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.

Satz: 3w+p GmbH, Rimpar
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 4

Anwendungsbereich und Verfahrensgarantien allgemeiner Vorschriften der Beschlagnahme und Durchsuchung 223

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
BGBl. I	Bundesgesetzblatt Teil I
BGH	Bundesgerichtshof
BGHSt	Entscheidungssammlung des *BGH* in Strafsachen
BGHZ	Entscheidungssammlung des *BGH* in Zivilsachen
BKA	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)
K-MRK	Südkoreanische Nationale Menschenrechtskommission
K-OGH	Südkoreanischer Oberster Gerichtshof
K-OGHE	Entscheidungen des *K-OGH*
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
K-VerfG	Südkoreanisches Verfassungsgericht
K-VerfGE	Entscheidungen des *K-VerfG* (Zitiert: *K-VerfGE* Band-Nummer, erste S., betroffene S.; z. B. *K-VerfGE* 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
NStZ	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. *Singelnstein*, 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 1879[4] 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-

- Im Jahre 1968 wurden die §§ 100a, b StPO a. F. als Rechtsgrundlage zur Überwachung des Fernmeldeverkehrs durch das G 10[7] geschaffen. Gestützt auf die Vorschriften wurde die Echtzeitüberwachung des Telefonverkehrs ermöglicht. Zwar wurde sie damals mit dem G 10 verrechtlicht, jedoch unterscheiden sich beide Maßnahmen nach ihrem Zweck voneinander. Bei einer TKÜ zum Zwecke der Gefahrenabwehr nach dem G 10 handelt es sich nicht um das Ermittlungsverfahren, wobei die Befugnis zur TKÜ den Nachrichtendiensten wie den Verfassungsschutzbehörden des Bundes und der Länder (BfV und LfV), dem MAD und dem BND zusteht.
- Durch das Änderungsgesetz, das am 1. April 1987 in Kraft trat,[8] wurde § 163d StPO als Rechtsgrundlage zum maschinellen Abgleich personenbezogener Daten zahlreicher Bürger (sog. „Schleppnetzfahndung") geschaffen. Dies entspricht den Grundsätzen des Volkszählungsurteils des *BVerfG* von Ende 1983. Nach dem Urteil dürfen personenbezogene Daten, die individualisiert werden können, nur unter besonders strengen Anforderungen erhoben, gespeichert und verarbeitet werden.
- Am 22. September 1992 ist das OrgKG[9] in Kraft getreten. Damit wurden §§ 100c, d StPO a. F. zur akustischen Überwachung außerhalb von Wohnraum (sog. „Kleiner Lauschangriff") und zu den Bildaufnahmen und dem Einsatz sonstiger technischer Mittel außerhalb von Wohnraum für Observationszwecke in der StPO erstmals als technische Ausspähungsmethoden außer der TKÜ begründet. Dazwischen wurde die Position der Ermächtigungsnorm jeder Maßnahme in der StPO durch das Gesetz zur Reform akustischer Wohnraumüberwachung von 2005 und das TKÜG von 2008 geändert: Kleiner Lauschangriff von § 100c Abs. 1 S. 1 Nr. 2 StPO a. F. zu § 100f StPO sowie die Bildaufnahmen und der Einsatz sonstiger technischer Mittel von § 100c Abs. 1 S. 1 Nr. 1 StPO a. F. (über § 100f StPO a. F.) zu § 100h StPO. Hierbei hat sich aber nichts i. R. d. Eingriffsvoraussetzungen und der Verfahrenskontrolle jeder Maßnahme inhaltlich geändert. Jedoch haben sich Verfahrensgarantien nach § 101 StPO (Kennzeichnung, Löschung und Sperrung erhobener Daten sowie Benachrichtigung und nachträglicher Rechtsschutz bei verdeckten Maßnahmen) bis zu solchen Maßnahmen erweitert: Also sind die Verfahrenssicherungen, die früher nur für den Einsatz sonstiger technischer Mittel galten, durch das TKÜG auf die Bildaufnahmen übertragen worden.[10] Dabei wurden andererseits auch die §§ 98a ff. und §§ 110a ff. StPO eingeführt.[11]

---

prozessuale Maßnahme ist als staatlicher Hoheitsakt i. d. R. neuralgisch, verwickelt sich unmittelbar in einen Grundrechtseingriff.

[7] Art. 2 G 10 vom 13. August 1968 (BGBl. I S. 949).

[8] Art. 2 Paßgesetz und Gesetz zur Änderung der StPO vom 19. April 1985 (BGBl. I S. 537).

[9] Art. 3 Nr. 6 OrgKG vom 15. Juli 1992 (BGBl. I S. 1302).

[10] *Wolter/Greco*, SK-StPO, § 100h Rn. 1.

[11] *Wolter/Jäger*, SK-StPO, § 110a Rn. 1 und 3. Bei §§ 110a–c StPO handelt sich es um menschliche Datenerhebungen, nämlich Spionagemethoden.

- Mit dem OrgKVerbG, das am 9. Mai 1998 in Kraft trat,[12] hat der Gesetzgeber §§ 100c Abs. 1 Nr. 3, 100d–f StPO a. F. (in der vom 9. Mai 1998 bis zum 30. Juni 2005 geltenden Fassung) zur akustischen Wohnraumüberwachung (sog. „Großer Lauschangriff") geschaffen; kurz davor hat er am 1. April 1998 durch das Änderungsgesetz des GG[13] Art. 13 Abs. 3–6 GG eingefügt, um die Verfassungsgrundlage zum Großen Lauschangriff zum Zweck der Strafverfolgung – und auch der Gefahrenabwehr – bereitzustellen. In den Vorschriften der StPO zur Durchführung der akustischen Überwachung von Wohnraum waren zwar ziemlich strenge Eingriffsvoraussetzungen und Schutzvorkehrungen enthalten, das *BVerfG* hat aber dennoch in seiner Entscheidung vom 2004 ausgeführt, dass die Vorschriften den verfassungsrechtlichen Anforderungen im Hinblick auf den Schutz der Menschenwürde, den Grundsatz der Verhältnismäßigkeit, die Gewährung effektiven Rechtsschutzes und den Anspruch auf rechtliches Gehör nicht in vollem Umfang genügen. Demzufolge wurden sie für verfassungswidrig und nichtig erklärt.[14] Danach ist eine Novelle, die den Inhalt der Entscheidung völlig aufgenommen hat, am 24. Juni 2005 durch den Gesetzgeber verabschiedet worden: §§ 100c–e StPO a. F. (in der vom 01. 07. 2005 bis zum 31. 12. 2007 geltenden Fassung).[15] Aus diesem Anlass wurde damals der Große Lauschangriff, der Einsatz sonstiger technischer Mittel und der Kleine Lauschangriff in §§ 100c–e, § 100f Abs. 1 und § 100f Abs. 2 StPO a. F. jeweils isoliert vorgesehen. Diese Regelungen wurden sowohl durch das TKÜG, das am 1. Januar 2008 in Kraft trat, als auch durch das Änderungsgesetz der StPO, das am 24. August 2017 in Kraft trat, inhaltlich kaum geändert.
- Mit dem StVÄG 1999, das am 1. November 2000 in Kraft trat,[16] wurde in die StPO die sog. „längerfristige Observation"[17] eingeführt, die bis dahin auf §§ 161, 163 StPO gegründet war und durch die Rechtsprechung geregelt wurde (vgl. § 163f StPO).[18] Fällt eine Maßnahme für Observationszwecke, z. B. eine Maßnahme nach § 100h Abs. 1 StPO, unter die Voraussetzungen des § 163f Abs. 1 StPO, muss sie einer Verfahrenskontrolle des § 163f Abs. 3 StPO unterzogen werden.

---

[12] Art. 2 OrgKVerbG vom 4. Mai 1998 (BGBl. I S. 845).

[13] Gesetz zur Änderung des GG (Art. 13) vom 26. März 1998 (BGBl. I S. 610).

[14] *BVerfGE* 109, 279, Tenor 6.

[15] Art. 1 Nr. 1 Gesetz zur Umsetzung des Urteils des BVerfG vom 03. März 2004 (akustische Wohnraumüberwachung) vom 24. Juni 2005 (BGBl. I S. 1841).

[16] Art. 1 Nr. 8 Strafverfahrensänderungsgesetz (StVÄG) 1999 vom 2. August 2000 (BGBl. I S. 1253).

[17] BT-Drs. 14/1484, S. 17; M-G/*Schmitt*, StPO, § 163f Rn. 1.

[18] Für den präventiv-polizeilichen Bereich ist die Maßnahme der längerfristigen Observation bereits geregelt; im BKAG und im BGSG im Bund, in den Polizeigesetzen in den Ländern. Die im Wesentlichen mit § 163f StPO gleichlautenden Regelungen bezeichnen eine Observation als längerfristige Observation, wenn diese länger als 24 Stunden dauert oder an mehr als zwei Tagen stattfindet (§ 23 Abs. 2 Nr. 1 BKAG, § 28 Abs. 2 Nr. 1 BGSG; BT-Drs. 14/1484, S. 24).

- Durch das Änderungsgesetz der StPO, das am 1. Januar 2002 in Kraft trat,[19] wurde die Rechtsgrundlage für die Erhebung der Verkehrsdaten aus bestehendem § 12 FAG a. F.[20] durch neu geschaffene §§ 100g, h StPO a. F. ersetzt. Außerdem wurde im August desselben Jahres § 100i StPO geschaffen, der den Einsatz des „IMSI-Catchers" zur Vorbereitung einer Maßnahme nach § 100a StPO sowie zur vorläufigen Festnahme oder Ergreifung eines Täters ausdrücklich legitimiert.[21]
- Am 1. Januar 2008 trat das TKÜG in Kraft, das den Inhalt der RL 2006/24/EG[22] in nationales Recht umsetzt und die TKÜ und andere verdeckte Ermittlungsmaßnahmen nach den Entscheidungen des *BVerfG* neu regelt.[23] Dabei wurde vor allem die Rechtsgrundlage zu einer „vorsorglich anlasslosen Speicherung von TK-Verkehrsdaten und deren Verwendung" (sog. „Vorratsdatenspeicherung"), die damals hinsichtlich ihrer Zulässigkeit heißumstritten war, in StPO und TKG eingeführt: §§ 100g, h StPO a. F. und §§ 113a – b TKG a. F. Bald nach der Inkraftsetzung dieser Novelle wurden Verfassungsbeschwerden gegen die verdeckten Maßnahmen im 8. Abschnitt des Ersten Buches der StPO erhoben, davon

[19] Art. 1 Gesetz zur Änderung der StPO vom 20. Dezember 2001 (BGBl. I S. 3879). Nach diesem Gesetz waren die neuen §§ 100g, h StPO von vornherein nur für begrenzte Zeit (drei Jahre) gültig und sollten am 1. Januar 2005 außer Kraft treten (Art. 2 & 4). Es wurde jedoch seitdem erweitert, weiterhin durch das TKÜG vom 1. Januar 2008 vollständig überarbeitet und schließlich in die StPO integriert.

[20] Das FAG geht ursprünglich auf das Gesetz über das Telegraphenwesen des Deutschen Reichs, das am 1. Januar 1928 in Kraft trat, zurück. Seit dem ersten Inkrafttreten des FAG bestand § 12 a. F., um den Ermittlungsbehörden zum Zweck der Strafverfolgung detaillierte Kenntnis von den Umständen der TK, nicht von ihren Inhalten, zu ermöglichen. Während das Gesetz zwar nach der Entwicklung der Telekommunikationstechnologie mehrmals geändert wurde, wurde die Vorschrift bis Ende 2001 ohne wesentliche inhaltliche Änderungen beibehalten, jedoch ist sie schließlich am 1. Januar 2002 durch die §§ 100g, h StPO a. F. ersetzt worden (vgl. Art. 4 Gesetz zur strafverfahrensrechtlichen Verankerung des Täter-Opfer-Ausgleichs und zur Änderung des FAG vom 20. Dezember 1999, BGBl. I S. 2491). Der Wortlaut des § 12 FAG a. F. beim Außerkrafttreten mit Ablauf der Frist ist wie folgt: „In Strafgerichtlichen Untersuchungen kann der Richter und bei Gefahr im Verzug auch die StA Auskunft über die TK verlangen, wenn die Mitteilungen an den Beschuldigten gerichtet waren oder wenn Tatsachen vorliegen, aus denen zu schließen ist, dass die Mitteilungen von dem Beschuldigten herrührten oder für ihn bestimmt waren und dass die Auskunft für die Untersuchung Bedeutung hat. Das Grundrecht des Art. 10 des GG wird insoweit eingeschränkt" (dies letztmals durch § 99 Abs. 1 Nr. 2 des TKG, das am 01. August 1996 in Kraft trat (BGBl. I S. 1120), geändert worden ist).

[21] Art. 1 Nr. 3 Gesetz zur Änderung der StPO vom 6. August 2002 (BGBl. I S. 3018); BT-Drs. 14/9088, S. 7. Dann war die Maßnahme nach der Vorschrift zur Vorbereitung der Verkehrsdatenerhebung, zur Unterstützung von Observationsmaßnahmen und zur Ermittlung des Standorts des Täters nicht gestattet.

[22] Nach dieser Richtlinie sind zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten (Art. 1) Anbieter elektronischer Kommunikationsdienste verpflichtet, für einen Zeitraum von mindestens sechs Monaten und höchstens zwei Jahren (Art. 6) Verkehrs- und Standortdaten, die im Zuge der Bereitstellung ihrer Kommunikationsdienste erzeugt oder verarbeitet werden (Art. 5), auf Vorrat zu speichern (Art. 3) und erforderliche Informationen unverzüglich an die zuständigen Behörden auf deren Anfrage hin weiterzuleiten (Art. 8).

[23] TKÜG vom 21. Dezember 2007 (BGBl. I S. 3198).

wurde das Verfahren über die Verfassungsbeschwerden von §§ 113a, b TKG a. F. und § 100g StPO a. F. für die VDS vom *Ersten Senat* und dasjenige von §§ 100a Abs. 2 und 4, 100f a. F. und §§ 101 Abs. 4 – 6, 110 Abs. 3, 160a StPO für sonstige Maßnahmen vom *Zweiten Senat* abgetrennt übernommen. Im Jahre 2010 hat zuerst der *Erste Senat* entschieden, dass die VDS als solche zwar nicht verfassungswidrig ist, aber § 100g Abs. 1 S. 1 StPO a. F. i. V. m. §§ 113a, b TKG a. F. wegen des Verstoßes gegen den Grundsatz der Verhältnismäßigkeit, insb. die Verhältnismäßigkeit i. e. S., verfassungswidrig und nichtig sind: Unzulänglichkeit eines besonders hohen Standards der Datensicherheit, der normenklaren Begrenzung und der Transparenz der Datenverwendung und eines effektiven Rechtsschutzes.[24] Im Anschluss daran hat im Jahre 2011 der *Zweite Senat* eine Entscheidung getroffen, dass §§ 100a, b StPO a. F. und §§ 101, 160a StPO durch ihre materielle Prüfung verfassungsmäßig sind.[25] Im Jahre 2014 hat auch der *EuGH* daneben festgestellt, dass die das TKÜG ausgelöste RL 2006/24/EG wegen des Verstoßes gegen das Recht auf Achtung des Privatlebens in Art. 7 GRCh und das Recht auf Schutz personenbezogener Daten in Art. 8 GRCh ungültig ist.[26] Dabei sind die Begründungen mit den in der *BVerfG*-Entscheidung vom 2010 dargelegten Gründen zumeist vereinbar; insb. die Anforderung eines besonders hohen Schutz- und Sicherheitsniveaus und die Begrenzung der Maßnahme auf schwere Straftaten.[27] Erst im Jahre 2015 hat der Gesetzgeber die Ermächtigungsvorschriften zur VDS entsprechend dem Inhalt der Rspr. des *BVerfG* neu geregelt.[28] Daher hat er die Erhebung von Verkehrsdaten in Echtzeit oder in Zukunft (§ 100g Abs. 1 StPO n. F. i. V. m. § 96 TKG) und von solchen, die nach Beendigung der TK gespeichert wurden (§ 100g Abs. 2 StPO n. F. i. V. m. § 113b TKG n. F.), getrennt geregelt, wobei die Vorkehrungen für letzten Fall strenger ausgestaltet wurden.

- Am 1. Juli 2013 hat der Gesetzgeber § 100j StPO zur Auskunft über Bestandsdaten geschaffen.[29] Das kommt von der Entscheidung des *BVerfG* vom 2012, dass bei Erhebung und Verwendung der Bestandsdaten ein „Doppeltürenmodell" erforderlich ist und sich eine Besonderheit bei der Auskunft über Zugangssicherungscodes ergibt.[30]

---

[24] *BVerfGE* 125, 260.

[25] *BVerfGE* 129, 208.

[26] *EuGH* (Große Kammer), Urteil vom 08. 04. 2014 – C293/12, C594/12 (= *EuGH*, NJW 2014, 2169).

[27] M-G/*Schmitt*, StPO, § 100g Rn. 5.

[28] Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 (BGBl. I S. 2218).

[29] Art. 2 Gesetz zur Änderung des TKG und zur Neuregelung der Bestandsdatenauskunft vom 20. Juni 2013 (BGBl. I S. 1602).

[30] *BVerfGE* 130, 151.

- Durch das am 24. August 2017 in Kraft getretene Änderungsgesetz[31] hat der Gesetzgeber in die StPO die Quellen-TKÜ und Online-Durchsuchung eingeführt, die von der Ermittlungsbehörde lange schon verlangt würden. Allerdings wurde zwar die Zulässigkeit der Maßnahmen als solche bereits von der Entscheidung des *BVerfG* vom 2008[32] festgestellt, jedoch bleibt wegen des verfassungsrechtlichen Bedenkens hinsichtlich ihrer konkreten gesetzlichen Ausgestaltung, d. h. der Lückenhaftigkeit der vom *BVerfG* gebotenen technischen Vorkehrungen und einer besonders hohen Eingriffsintensität der Online-Durchsuchung, diese Legitimierung noch umstritten.
- Jüngst, am 25. November 2019, trat das Gesetz in Kraft, die RL (EU) 2016/680 und die VO (EU) 2016/679 in nationales Recht umzusetzen.[33] Damit hat der Gesetzgeber eine Ermächtigungsgrundlage für die Erhebung gespeicherter (retrograder) Standortdaten genau umschrieben (§ 100g Abs. 3 StPO). Außerdem bestätigt er, dass auch für andere verdeckte Maßnahmen als solche nach §§ 100a bis 100c StPO, nämlich akustische Überwachung außerhalb von Wohnraum, weitere Maßnahmen außerhalb von Wohnraum, einen Einsatz eines Verdeckten Ermittlers und längerfristige Observation, gilt, dass Erkenntnisse aus dem Kernbereich privater Lebensgestaltung nicht erlangt oder verwertet werden dürfen (vgl. §§ 100f Abs. 4, 100h Abs. 4, 110a Abs. 1 S. 5, 163f Abs. 2 S. 2 i. V. m. § 100d Abs. 1, 2 StPO).

Dagegen hat sich an der „offenen Durchsuchung und Beschlagnahme" gemäß §§ 94 ff., 102 ff. StPO bis Ende 2020 fast nichts geändert. Allerdings hat der Gesetzgeber durch das TKÜG eine Rechtsgrundlage geschaffen, dass sich die Durchsuchung elektronischer Daten bis auf „räumlich getrennte Speichermedien" erweitern kann (§ 110 Abs. 3 StPO), aber es gab keine darüber hinausgehenden Versuche zur Gesetzgebung.

2. Entstehung und Entwicklung betreffender Vorschriften in Südkorea

Als Ermächtigungsgrundlage zur Beweissicherung zum Zweck der Strafverfolgung in Südkorea gibt es die §§ 106 ff. i. V. m. §§ 215, 219 K-StPO,[34] die allgemeine

[31] Art. 3 Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017 (BGBl. I S. 3202).

[32] *BVerfGE* 120, 274; vgl. für die Unzulässigkeit der verdeckten Online-Durchsuchung mangels einer Ermächtigungsgrundlage (im damaligen deutschen Gesetz), *BGHSt* 51, 211, 212 und 217 f.

[33] Gesetz zur Umsetzung der RL (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die VO (EU) 2016/679 vom 20. November 2019 (BGBl. I S. 1724).

[34] Sie entsprechen den Vorschriften von §§ 94 ff., 102 ff. StPO. Die Struktur von K-StPO und der Inhalt jeder Vorschrift sind im Wesentlichen aus der Perspektive des Gerichts gebildet. Daher werden gerichtliche Zwangsmaßnahmen (z. B. Untersuchungshaft, Beschlagnahme und Durchsuchung) zunächst im 10. Abschnitt Ersten Buches der K-StPO festgelegt (§§ 68 bis 145),

Vorschriften der Durchsuchung und Beschlagnahme sind, und das K-KGSG, das Maßnahmen wie Zensur der Postsendungen, TKÜ, Abhören von Gesprächen, Kenntnisnahme von den Umständen der TK etc. regelt.[35] Auch in Südkorea wirkt sich die rasante Ausbreitung der IuK-Technologie erheblich auf die Durchsuchung und Beschlagnahme im Ermittlungsverfahren aus, und sie bringt noch immer große rechtliche und politische Debatten mit sich. Hier scheint Südkorea jedoch im Vergleich zu Deutschland passiver gegenüber Reformen durch die Gesetzgebung zu sein und Lösungen durch konkrete Maßnahmen in Einzelfällen von Gerichten und Ermittlungsbehörden zu bevorzugen. Dies ist im Wesentlichen auf die Haltung des südkoreanischen Gesetzgebers sowie vom *K-OGH* und *K-VerfG* zurückzuführen, die dazu neigen, das Ermessen der StA und der Gerichte im Ermittlungsverfahren weitgehend zu garantieren. Das K-KGSG, das starke Eingriffsmaßnahmen wie TKÜ und Gesprächsüberwachung regelt, ist ein Sondergesetz der allgemeinen Bestimmungen über die Durchsuchung und Beschlagnahme in der StPO, aber seine Kontrolle ist in der Praxis nicht so streng. Aus diesem Grund werden der Inhalt und die Anwendung des Gesetzes seit seiner Gründung im Schrifttum ständig kritisiert, und es wurde mehrfach überarbeitet. Diese Änderungen waren früher hauptsächlich auf schwache Inhalte des Gesetzes zurückzuführen, neuerdings beziehen sie sich jedoch häufig auch auf fortschrittliche IuK-Technologie und auf die Eingriffsvoraussetzungen und Verfahrensgarantien einzelner Maßnahmen. Hingegen wurden die allgemeinen Vorschriften zur Beschlagnahme und Durchsuchung der StPO bisher nur einmal bezüglich der Verfahrenskontrolle bei der Sicherung elektronischer Daten überarbeitet. Die Geschichte der Schaffung und Änderung der allgemeinen Vorschriften und des K-KGSG kann wie folgt umrissen werden:

---

und diese Vorschriften gelten individuell entsprechend für die Untersuchungen der Ermittlungsbehörde im 1. Abschnitt Zweiten Buches der K-StPO, insb. Zwangsmaßnahmen (etwa § 200e für eine vorläufige Festnahme durch richterliche Anordnung, § 209 für eine Untersuchungshaft, § 213a für eine Festnahme auf frischer Tat, § 219 für eine Durchsuchung und Beschlagnahme). Diese seltsame Systemstruktur stammt aus der alten Strafprozessordnung Japans (*Son/Kim*, Durchsuchungs- und Beschlagnahmeverfahren, 24). Dieses Gesetz, das 1890 in Japan erlassen und in Kraft gesetzt wurde, hatte eine Institution der Voruntersuchung und diese wurde während der Kolonialherrschaft des japanischen Imperialismus auf Korea angewendet (*Dong-Woon Shin*, SLJ, 27-1, 1986, 149, 150 f.). Derzeit ist ein solches Regulierungssystem jedoch nicht mehr angemessen, da gerichtliche Durchsuchung und Beschlagnahme in der Praxis sehr selten ist, und daher ist die Schaffung eigener Regelungen seitens der Ermittlungsbehörde erforderlich (*Son/Kim*, a. a. O.; *Sungsoo Ahn*, KoK-StPO, vor § 106, 555). Wegen dieser Struktur der K-StPO werden ohnehin in der vorliegenden Arbeit diesbezügliche (Referenz-)Vorschriften als „Relevante Vorschriften i. V. m. § 219 K-StPO" bezeichnet.

[35] Das K-KGSG ist eine Sondervorschrift der K-StPO und daher wird diese nicht berücksichtigt, wenn das K-KGSG angewendet wird. In der Vergangenheit war unter der Diktatur oder dem autoritären System Südkoreas die Überwachung von Postsendungen und (Tele-) Kommunikationen durch Ermittlungsbehörden – als verdeckte Maßnahme – ein offenes Geheimnis, und es gab keine individuelle Rechtsgrundlage dafür. *Young-sam Kim* (Amtszeit: 02.1993 – 02.1998), der 1992 in der Präsidentschaftswahl gewählt wurde, hat jedoch kurz nach der Wahl das K-KGSG verabschiedet, um das Abhören (von Gesprächen) zu legalisieren und zu kontrollieren, das während der Wahl ein Problem war (*Kuk Cho*, KCR, 15-4, 2004, 103, 103 f.; *Hyung-Joon Kim*, JCL, Nr. 24, 2005, 213, 214).

- Die K-StPO (Gesetz Nr. 341), die durch eine parlamentarische Verabschiedung am 19. März 1954 und eine Verkündung am 23. September desselben Jahres geschaffen wurde, enthielt bereits einige detaillierte Regelungen für die Beschlagnahme und Durchsuchung. Im Ermittlungsverfahren wurde ihre Einhaltung jedoch im autoritären und diktatorischen Zeitalter praktisch häufig vernachlässigt, und außerdem wurden trotz der Veränderungen durch die Entwicklung der Technologie seit Langem keine Anstrengungen unternommen, um mit der Realität Schritt zu halten.[36] Nach der Machtübernahme der fortschrittlichen liberal-demokratischen politischen Kräfte Ende des 20. Jahrhunderts und der anschließenden Debatten über die Reform des Strafverfahrens wurde die K-StPO durch die am 1. Juni 2007 beschlossene und am 1. Januar 2008 in Kraft getretene Änderung teilweise verbessert (Gesetz Nr. 8496; im Folgenden als „K-StPO-Reform 2007").[37] Dabei wurden die Verwahrung und Vernichtung von beschlagnahmten Gegenständen (§§ 130, 132 K-StPO) und die Beschlagnahme und Durchsuchung ohne richterliche Anordnung bei vorläufiger Festnahme im Eilfall (§ 217 K-StPO)

[36] In der Zeit des Autoritarismus in Korea, die bis Ende der 90er Jahre andauerte, waren übermäßige Verletzungen der Freiheit des Lebens, der körperlichen Unversehrtheit oder der Gedanken-, Meinungs- und Versammlungsfreiheit üblicher als die Verletzung der Unverletzlichkeit von Wohnraum, der Fernmeldegeheimnisse und des informationellen Selbstbestimmungsrechts. Aus diesem Grund waren bis 2000 die Kontrolle der Zwangsmaßnahmen im Zusammenhang mit der persönlichen Haft und mit illegalen Handlungen bezüglich der Erstellung des Vernehmungsprotokolls des Beschuldigten hauptsächlich problematisch, und die K-StPO wurde diesbezüglich nur teilweise überarbeitet (*Jin-Yeon Chung*, SLR, Band 18, 2007, 73, 102; *Oung-Seok Jeong*, The Justice, Nr. 101, 2007, 205, 206; *Tae-Hoon Ha*, JCL, 23-1, 2011, 3, 4 f.). Seit den 2000er Jahren ist jedoch unter der wiederhergestellten freiheitlichen demokratischen Grundordnung und dem erhöhten Menschenrechtsbewusstsein mit der Entwicklung der IuK-Technologie die Kontrolle einer übermäßigen Erfassung personenbezogener Daten durch die Ermittlungsbehörden zum Kern der Diskussionen über Strafverfahren geworden.

[37] Diese Reform ist eines der Ergebnisse des Dursts nach einer liberalen Demokratie, die in Südkorea unterdrückt wurde. Sie geschah ab 2003 durch die Ausarbeitung eines Regierungsvorschlags für drei Jahre und eine einjährige parlamentarische Überprüfung. An der Bildung dieses Vorschlags haben Vertreter des Justizministeriums, der StA, des Gerichts, der Rechtsanwaltskammer, der Rechtswissenschaftler (aus The Korean Criminal Law Association) und der nichtstaatlichen Organisationen mitgewirkt. Er wurde insb. durch den „Ausschuss für Justizreform" der Regierung und des Gerichts und den darauffolgenden „Präsidialausschuss zur Förderung der Justizreform" konzipiert und geplant und durch die Konkretisierung des Justizministeriums festgesetzt (*Oung-Seok Jeong*, The Justice, Nr. 101, 2007, 205, 207 ff.). Das Parlament hat ihn in kurzer Zeit intensiv erörtert und nach teilweiser Überarbeitung beschlossen (Gesetz Nr. 8496). Zu diesen Änderungen gehören die Stärkung des Verteidigungsrechts des Beschuldigten, die Verbesserung der Institution von Festnahme und Untersuchungshaft, die Stärkung des Hauptverfahrens, die Stärkung des Schutzes der Opfer, die Ausweitung des Umfangs der Offenlegung festgesetzter Gerichtsakte usw. (*Oung-Seok Jeong*, a. a. O. 212 ff.; *Jin-Yeon Chung*, SLR, Band 18, 2007, 73, 77 ff.; *Yang-Kyun Shin*, JCL, 26-2, 2014, 447, 452 f.). Dies war die umfassendste Reform seit der Gründung von K-StPO. Parallel dazu wurde das „Gesetz über die Teilnahme der Bürger an den Kriminal-Gerichtsverfahren" (Gesetz Nr. 8495) geschaffen, um eine neue Art von strafrechtlicher Verhandlung einzuführen, in der die Elemente des Jury- und Schöffensystems teilweise gemischt werden.

teilweise überarbeitet. Durch diese Reform wurde u. a. das Prinzip des Ausschlusses von illegal erlangten Beweisen (im Folgenden „Ausschlussprinzip"), das eine grundlegende Änderung in der Struktur des Beweisrechts darstellt, eingeführt; vgl. dazu eingehend Kapitel 2, C. II.

- Erst durch die Änderung, die am 18. Juli 2011 beschlossen und am 1. Januar 2012 in Kraft getreten ist, wurden die Vorschriften der Beschlagnahme und Durchsuchung in der K-StPO sinnvoll verbessert (Gesetz Nr. 10864: im Folgenden als „K-StPO-Änderung 2011"). Zunächst wurde die Beschränkung der Durchsuchung und Beschlagnahme nur auf verfahrensrelevante Informationen durch Klartext hervorgehoben, um die in der Praxis häufig durchgeführte übermäßige Erfassung personenbezogener Daten zu begrenzen (vgl. §§ 106 Abs. 1, 107 Abs. 1, 109 Abs. 1 i. V. m. §§ 215, 219 K-StPO).[38] Bezüglich der Beschlagnahme und Durchsuchung elektronischer Daten wurden der Umfang und die Methode ihrer Durchführung und die Pflicht zur Benachrichtigung des von Daten Betroffenen über die Maßnahme gesetzlich festgelegt (§ 106 Abs. 3, 4 K-StPO). Daneben wurden im Zusammenhang mit der Beschlagnahme der Daten, die auf Servern Dritter gespeichert sind, die Wörter „Postsendungen oder Telegramme" als Gegenstände durch die Wörter „Postsendungen oder Telekommunikation gemäß § 2 Nr. 3 K-KGSG" ersetzt (§ 107 Abs. 1 K-StPO). Dabei muss die „Erstellungsperiode" der TK in dem Beschlagnahme- und Durchsuchungsbeschluss des Gerichts angegeben werden (§ 114 Abs. 1 S. 2 K-StPO). Darüber hinaus wurde ein Anspruch des Eigentümers etc. auf (Quasi-)Rückgabe des Originals und ein damit zusammenhängendes Einspruchsrecht festgelegt (§ 218a K-StPO).
- Das K-KGSG (Gesetz Nr. 4650), das am 27. Dezember 1993 erlassen wurde und am 28. Juni 1994 in Kraft getreten ist, wurde ohne ausreichende Überprüfung nicht nur rasch fertiggestellt, sondern war auch inhaltlich sehr schlecht. Damals wurde vielfach kritisiert, dass das Gesetz das Geheimnis der Kommunikation nicht schützt, sondern seinen Eingriff ohne angemessene Kontrolle rechtfertigt.[39] Aus diesem Grund wurden übermäßige Anwendungen bzw. Missbräuche des Gesetzes im Jahr 1998, vier Jahre nach seiner Durchsetzung, im Untersuchungsausschuss des Parlaments stark kritisiert, und es hat sich eine öffentliche Meinung über die Überarbeitung gebildet.[40] Was hierbei besonders problematisch war, waren ein großer Umfang von Katalogstraftaten, auf die die TKÜ anzuwenden ist, und eine

[38] In jede Vorschrift wurden die Worte „beschränkt auf das, was als für den vorliegenden Fall relevant anzusehen ist" eingefügt. Natürlich wurde bereits vor dieser Änderung die Relevanz für die Beschlagnahme und Durchsuchung durch die Auslegung der Vorschriften anerkannt und gefordert (*K-OGHE* vom 23. 4. 2004 – 2003 Mo 126; *ders.* vom 26. 5. 2011 – 2009 Mo 1196; *Whankyu Lee*, CRCL, Nr. 48, 2015, 90, 133; *Seungsoo Chun*, CRCL, Nr. 49, 2015, 37, 39 f.; *Son*/*Kim*, Durchsuchungs- und Beschlagnahmeverfahren, 27 f.; *Joo-Won Rhee*, K-StPO, 146).

[39] Repräsentativ, *Kuk Cho*, KCR, 15-4, 2004, 103, 106: Das Gesetz kontrolliert die illegale Überwachung nicht wirklich, sondern verkleidet sie mit einem legitimen Mantel.

[40] *Huigi Shim*, KCR, 10-3, 1999, 5, 6-15; *Il-Whan Kim*, KJC, 16-1, 2004, 25, 38.

nicht strenge Verfahrenskontrolle,[41] die Missbräuche der Eil-TKÜ[42] oder das Fehlen eines Verfahrens der Benachrichtigung des Betroffenen.[43]

- Infolgedessen wurde das K-KGSG durch eine Änderung, die am 29. Dezember 2001 beschlossen und am 30. März 2001 in Kraft getreten ist, erheblich überarbeitet (Gesetz Nr. 6456, im Folgenden als „K-KGSG-Änderung 2001"). Zuerst wurde die Anzahl der Katalogtaten um etwa 40 reduziert (§ 5 Abs. 1 K-KGSG);[44] die Maßnahme muss für die jeweiligen Verdächtigen im Einzelnen beantragt und zugelassen werden; der Ort und die Art und Weise ihrer Durchführung müssen im Schriftsatz des Antrags und der Zulassung angegeben werden, und die längste Ausführungsfrist in der Zulassung und Verlängerung wurde von drei Monaten auf zwei Monate verkürzt (§ 6 Abs. 1-7 K-KGSG).[45] Weiter sind die Voraussetzungen und das Verfahren der TKÜ im Eilfall erheblich strenger (§ 8 K-KGSG). Diesbezüglich wurden zu der bestehenden einfachen zeitlichen Dringlichkeit dringende Umstände wie die Planung und Durchführung schwerer Verbrechen wie Staatsschutzdelikte, Straftaten, die Leben oder Leib einer Person gefährden können, und organisierte Kriminalität etc. hinzugefügt (Abs. 1). Hinsichtlich des Verfahrens muss die Ermittlungsbehörde unverzüglich nach Beginn ihrer Vollstreckung ihre Zulassung beim Gericht beantragen, und wenn die Zulassung nicht eingeholt wird, muss die Maßnahme zügig innerhalb von 36 Stunden eingestellt werden (Abs. 2).[46] Schließlich wurde eine Bestimmung zur nachträglichen Benachrichtigung des Betroffenen über die TKÜ (auch im Eilfall) geschaffen (§ 9a K-KGSG).[47] Diese drei Änderungen wurden bis heute ohne große Änderungen beibehalten.

---

[41] *Huigi Shim*, KCR, 10-3, 1999, 5, 37 f.; *Kuk Cho*, KCR, 15-4, 2004, 103, 109.

[42] *Huigi Shim*, KCR, 10-3, 1999, 5, 7 und 16 f. In der Literatur wird darauf hingewiesen, dass die TKÜ im Eilfall praktisch oft in der Weise missbraucht werden, dass sie innerhalb von 48 Stunden ohne richterliche Kontrolle durchgeführt und dann beendet werden, und außerdem wird kritisiert, dass es in rechtssystematischer Hinsicht problematisch ist, dass eine Eilmaßnahme, die bei Durchsuchung und Beschlagnahme nicht zulässig ist, bei der TKÜ, die im Vergleich dazu intensiver ist, zulässig ist (a. a. O. 17 f.).

[43] *Huigi Shim*, KCR, 10-3, 1999, 5, 33-35.

[44] *Kuk Cho*, KCR, 15-4, 2004, 103, 109. In der Literatur wird jedoch immer noch kritisiert, dass die Zahl der Katalogtaten zu hoch ist (*Hyung-Joon Kim*, JCL, Nr. 24, 2005, 213, 222; *Kil-Young Oh*, DLS, Nr. 34, 2007, 357, 379 ff.; *Sung-Gi Hwang*, JML, 14-1, 2015, 1, 24; vgl. *Byoung-Hyo Moon*, PLLR, Band 45, 2009, 503, 507: Die Zahl beträgt immer noch insgesamt etwa 280).

[45] Dabei wurden für die TKÜ zur Staatssicherheit (§ 7 K-KGSG) die Wörter „soweit ein erhebliches Risiko (gegenüber der Staatssicherheit) erwartet wird" zu ihren Zulassungsvoraussetzungen hinzugefügt (Abs. 1) und die maximale Durchführungsdauer für solche Maßnahme und deren Verlängerung wurde von 6 Monaten auf 4 Monate verkürzt (Abs. 2).

[46] Diesbezüglich war die Frist vor der Überarbeitung auf 48 Stunden festgesetzt. Im Schrifttum wird jedoch kritisiert, dass auch nach dieser Änderung die TKÜ noch 36 Stunden ohne gerichtliche Kontrolle durchgeführt werden kann (*Hyung-Joon Kim*, JCL, Nr. 24, 2005, 213, 226).

[47] Die Unzulänglichkeit ihres Inhalts wird aber erheblich kritisiert (vgl. ausführlich Kapitel 3, D. II. 1. d)).

In der K-KGSG-Änderung 2001 wurden daneben die Ermächtigungsnormen für die Erhebung von Daten zur Bestätigung des Sachverhalts bezüglich der TK, nämlich Verkehrsdaten, geschaffen (vgl. §§ 13, 13a K-KGSG). Bis dahin wurden die Daten aufgrund von § 54 Abs. 3 K-TKGG a. F. ohne besondere Verfahren oder Einschränkungen auf Verlangen an die Ermittlungsbehörden übermittelt.[48] Mit zunehmender Bedeutung und Verwendung solcher Daten im Ermittlungsverfahren wurde jedoch das Fehlen von Verfahrenskontrollen über ihre Erhebung infrage gestellt,[49] und durch die Änderung 2001 wurde die Ermächtigung dazu in das K-KGSG eingeführt; § 13 K-KGSG regelt die Auskunftserteilung zur Ermittlung und § 13a K-KGSG regelt dieselbe zur gerichtlichen Entscheidung. Zur Auskunft über Verkehrsdaten zur Strafverfolgung musste die Ermittlungsbehörde grundsätzlich vorab eine Genehmigung des „zuständigen LOStA" erhalten (§ 13 Abs. 1 und Abs. 3 S. 1 K-KGSG a. F.), jedoch konnte diese in dringenden Fällen – ausnahmsweise – nach dem Verlangen bzw. der Erfassung der Daten eingeholt werden (§ 13 Abs. 3 S. 2 K-KGSG a. F.). Eine solche Aufsichtskontrolle, die nicht von einer unabhängigen und neutralen Instanz und nur hausintern erfolgt, wurde aber faktisch u. a. wegen des Auskunftsersuchens im Eilfall tatsächlich ausgehöhlt. Daher wurde in der Literatur darauf hingewiesen, dass eine Einschaltung eines Gerichts erforderlich ist.[50] Vor diesem Hintergrund wurde §§ 13 ff. K-KGSG a. F. im Mai 2005 überarbeitet (Gesetz Nr. 7503): grundsätzliche Anforderung einer vorherigen Zulassung des Gerichts und Vernichtung der erhobenen Daten bei Nichteinholung nachträglicher Genehmigung im Auskunftsersuchen im Eilfall. Dabei wurde auch eine Vorschrift zur Benachrichtigung des Betroffenen von der Erhebung der Verkehrsdaten geschaffen (§ 13b K-KGSG).[51]

- Darüber hinaus wurde durch die Änderung vom 28. Mai 2009 (Gesetz Nr. 9752) § 9b K-KGSG neu eingefügt, bei dem es sich um eine Benachrichtigung über die Durchsuchung und Beschlagnahme nach K-StPO handelt, die sich auf die nach Abschluss des Übermittlungsvorgangs auf dem Server des Anbieters gespeicherten Daten richtete. Diese Vorschrift wird heute im Schrifttum in rechtssys-

[48] § 54 Abs. 3 K-TKGG a. F. (in der vom 11. Dezember 1991 bis zum 31. März 2000 geltenden Fassung) [Schutz des Kommunikationsgeheimnisses] Werden Personen oder Unternehmen, die geschäftsmäßig TK-Dienste erbringen oder daran mitwirken, aufgrund des Untersuchungsbedarfs von der zuständigen Behörde schriftlich aufgefordert, Unterlagen bezügliche der Erbringung der TK-Dienste Einsicht zu nehmen und sie einzureichen, dann können sie der Aufforderung nachkommen. Diese Vorschrift stellte damals auch eine Rechtsgrundlage für die Auskunft sowohl über Bestandsdaten als auch über Verkehrsdaten dar. Nach der Überarbeitung im Jahr 2000 regelte sie jedoch nur die Auskunft über Bestandsdaten, und im Jahr 2010 wurde diese Regelung ohne inhaltliche Änderung auf § 83 K-TKGG umgestellt.

[49] *Huigi Shim*, KCR, 10-3, 1999, 5, 27 – 29. Prof. *Shim* bestand damals auf der Schaffung einer Vorschrift, die es ermöglichen würde, die Auskunftserteilung unter der Kontrolle des Gerichts auf einer geringeren Ebene als bei der TKÜ zuzulassen (a. a. O. 29 – 31).

[50] *Kuk Cho*, KCR, 15-4, 2004, 103, 116 ff.

[51] Dabei wurde die Ermächtigungsnorm zur Erhebung von Verkehrsdaten zur Staatssicherheit als Maßnahme der Gefahrenabwehr (§ 13 Abs. 2 K-KGSG a. F.) getrennt und in eigene Vorschriften übertragen (§ 13-4 KKGSG).

tematischer Hinsicht häufig kritisiert. Dies liegt daran, dass die Benachrichtigung über die Maßnahmen aufgrund der K-StPO im K-KGSG festgelegt ist.[52]

- Danach wurde die Änderung des K-KGSG im Parlament mehrmals angestrebt, aber es gab keinen Erfolg. Erst durch die am 31. Dezember 2019 beschlossenen und in Kraft getretenen Änderungen (Gesetz Nr. 16849) wurde einerseits bezüglich der TKÜ eine Regelung eingefügt, um die gesamte Verlängerungsfrist zu begrenzen (§ 6 Abs. 8 K-KGSG), und andererseits wurden bezüglich der Erhebung von Verkehrsdaten die Eingriffsvoraussetzung zur Ortung in Echtzeit und zur Funkzellenabfrage (§ 13 Abs. 2 K-KGSG) sowie das Verfahren der Benachrichtigung (§ 13b K-KGSG) strenger. Diese Änderungen sind auf die Entscheidungen des *K-VerfG* zurückzuführen: für Ersteres der Beschluss vom 28. Dezember 2010,[53] für Letzteres die beiden Beschlüsse vom 28. Juni 2018.[54] Bald darauf wurde durch die am 24. März 2020 beschlossene und in Kraft getretene Änderung (Gesetz Nr. 17090) eine Vorschrift eingeführt, die eine gerichtliche Kontrolle über die Verwertung und Verwahrung der durch Paket-Überwachung (sog. „Deep Packet Inspection (DPI)“) erlangten Daten ermöglicht (§ 12a K-KGSG). Dies ist auf den Beschluss vom *K-VerfG* vom 30. August 2018 zurückzuführen.[55]

Das K-KGSG wird seit seiner Gründung immer noch in der Literatur wegen der inhaltlichen Fehler in rechtsstaatlicher Hinsicht und der strukturellen Mängel in theoretischer Hinsicht vielfach kritisiert und die Notwendigkeit seiner – umfassenden – Neustrukturierung wird ständig angesprochen.[56] Hingegen widersetzt sich die Ermittlungsbehörde durch organisatorischen und politischen Einfluss dieser Reformforderung und versucht, die vorhandenen Inhalte und Formate beizubehalten. Dies liegt daran, dass die Lücken in der Kontrolle gegen die unangemessenen Er-

---

[52] *Seok-soon Im*, KCR, 27-2, 2016, 203, 206: seltsame Form. In der Gesetzesbegründung gibt es aber für diese Änderung keine besondere Erwägung, und somit wird daraus keine besondere legislative Notwendigkeit oder Zweckmäßigkeit abgeleitet (a. a. O. 218 f.).

[53] *K-VerfGE* vom 28. 12. 2010 – 2009 HunGa 30 (22-, 545, 558 f.).

[54] *K-VerfGE* vom 28. 6. 2018 – 2012 HunMa 191 etc. (30-1, 564); *ders.* vom 28. 6. 2018 – 2012 HunMa 538 (30-1, 596).

[55] *K-VerfGE* vom 30. 8. 2018 – 2016 HunMa 263 (30-2, 481, 482 f. und 500).

[56] Seit Ende der 1990er Jahre, als die Nutzung von Internet und IuK-Technik rasant zugenommen hat, wurde auch die Anwendung des K-KGSG in Südkorea praktisch rasch ausgeweitet. Dessen inhaltliche und strukturelle Mängel werden in zahlreichen Publikationen ständig kritisiert: *Huigi Shim*, KCR, 10-3, 1999, 5; *Kuk Cho*, KCR, 15-4, 2004, 103; *Byoung-Hyo Moon*, PLLR, Band 45, 2009, 503; *Sung-Gi Hwang*, JML, 14-1, 2015, 1; *Kil-Young Oh*, DLS, Nr. 34, 2007, 357; *ders.*, JML, 14-1, 2015, 33; *Gi-Young Cho*, JCL, 26-4, 2014, 105; *Seok-soon Im*, KCR, 27-2, 2016, 203; *Jina Cha*, KLAJ, 67-2, 2018, 366; *Hojung Lee*, JPL, 17-1, 2019, 35 m. w. N. Insb. nach einigen Literaturauffassungen sollte das K-KGSG deshalb umfassend und grundlegend reformiert werden, weil sein gesamtes Regulationssystem als solches bereits schwerwiegende Fehler beim Schutz der Grundrechte hat (*Hojung Lee*, a. a. O. 48). Auch eine Mindermeinung (Richter *Dae-Hyun Cho*) im Beschluss des *K-Verf* vom 2010 (2009 HunGa 30) erklärt, dass das K-KGSG generell rekonstruiert werden sollte, um diese Verfassungswidrigkeit zu beseitigen (*K-VerfGE* 22-2, 545, 561).

mittlungshandlungen, die sich aus diesen Rechtsfehlern ergeben, der Behörde ein weites Ermessen einräumen.

B. Forschungsziel und Gang der Untersuchung

Der Fortschritt der IuK-Technologie führt zu unendlichen Debatten über die staatliche Erhebung und Verwendung personenbezogener Daten und ihre Grenzziehung. Zuerst ist umstritten, unter welchen Voraussetzungen vielfältige verdeckte Ermittlungsmaßnahmen zur Datenerfassung mit Blick auf das Rechtsstaatsprinzip zu rechtfertigen sind.[57] Diesbezüglich stellen sich die Fragen, ob sowohl neuartige Maßnahmen, die durch den Fortschritt der Technik ermöglicht werden, als auch herkömmliche Maßnahmen, die aus demselben Grund eingriffsintensiver werden als früher, unter bestehende Ermächtigungsnormen subsumiert werden können, oder ob eine neue Ermächtigung dafür erforderlich ist.[58] Die Beantwortung dieser Fragen und die Aktualisierung der einschlägigen Vorschriften tragen zur Bildung eines rechtsstaatlichen Strafverfahrens bei. Eine Serie von Gesetzesänderungen in Deutschland und Südkorea, die oben aufgezeigt wurden, liegen auch im Prozess einer solchen Bildung. Zum anderen können personenbezogene Daten heute auch bei einer einfachen Durchsuchung und Beschlagnahme jederzeit umfassend erhoben werden, und dies kann zum schweren Eingriff in das Persönlichkeitsrecht führen. Dies wirft die Frage auf, wie die allgemeinen Vorschriften der Beschlagnahme und Durchsuchung in der StPO auszulegen und anzuwenden und eventuell zu novellieren sind, um mit der Verfassung in Einklang zu stehen. Es ist oft sehr zweifelhaft, ob die Kontrolle der umfassenden Durchsuchung und Beschlagnahme elektronischer Daten nur durch einfachen Richtervorbehalt und nachträglichen Rechtsschutz erreicht werden kann. In der Praxis wird u. a. der Grundsatz der Verhältnismäßigkeit nicht zureichend eingehalten und die Vorschriften des Strafprozessrechts werden vielfach umgangen. Vor diesem Hintergrund beschäftigt sich die vorliegende Arbeit damit, einen besseren Ansatz i. R. d. Auslegung und Anwendung der Ermächtigungsgrundlagen der Zwangsmaßnahmen zur Beweissicherung im Ermittlungsverfahren durch den Rechtsvergleich zwischen Deutschland und Südkorea zu finden.

Die Untersuchung ist in 5 Kapitel unterteilt. Kapitel 1 dient zur Einführung in die Thematik, und hier wird u. a. die historische Entwicklung der einschlägigen Vorschriften in Korea und Deutschland skizziert. Anschließend werden in Kapitel 2 zunächst die Veränderungen der Realität und die rechtsstaatlichen Grenzen untersucht, die den Hintergrund dieser Untersuchung bilden (Abschnitt A.), und dann

[57] Vgl. *Kasiske*, StraFo 6/2010, 228, 231: „*Die besonderen Gefahren eines vergeheimdienstlichten Ermittlungsverfahrens, das sich vor allem heimlicher Methoden zur Ausspähung des Beschuldigten bedient, haben erst seit kurzem die ihnen gebührende Aufmerksamkeit in der Diskussion erhalten.*“

[58] Vgl. *Singelnstein*, NStZ 2012, 593, 594.

werden die davon betroffenen Grundrechte eingehend überprüft (Abschnitt B.). Im ersten Abschnitt werden die Ausweitung der Nutzung von IT, die niemand vermeiden kann, und die Forderung nach rechtsstaatlicher Kontrolle über die dadurch verursachten Gefahren und im letzteren Abschnitt der Datenschutz zum Persönlichkeitsschutz und die verfassungsrechtlichen Kriterien für seine Verletzungen analysiert. In Abschnitt C werden ein eigenes Verständnis des Rechts auf informationelle Selbstbestimmung und des Schutzes von Kommunikationsgeheimnissen sowie Diskussionen über das Ausschlussprinzip in Südkorea zusammen mit den Entscheidungen von *K-VerfG* und *K-OGH* vorgestellt. In Kapitel 3 werden heimliche Zwangsmaßnahmen zur Beweissicherung in Deutschland und Südkorea zusammen mit der Rechtsgrundlage ausführlich erörtert. Zunächst wird argumentiert, dass solche Maßnahmen aufgrund ihrer Heimlichkeit und erhöhter Eingriffsintensität qualifiziert kontrolliert werden sollten (Abschnitt A.). Anschließend werden die Ermächtigungsgrundlagen im 8. Abschnitt des Ersten Buches der StPO und die darauf beruhenden Maßnahmen mit den Entscheidungen des *BVerfG* im Einzelnen beleuchtet (Abschnitt B.), wobei ein verdeckter Zugang zu den auf dem Server der Anbieter der Dienste wie E-Mail, soziale Netzwerke oder Cloud-Computing gespeicherten Daten gesondert überprüft wird (Abschnitt C.). In Abschnitt D. wird zum Rechtsvergleich detailliert beschrieben, welche Art von heimlichen Zwangsmaßnahmen zur Beweissicherung in Südkorea unter welchen Eingriffsvoraussetzungen und Verfahrenskontrollen zulässig ist. In Kapitel 4 werden der Anwendungsbereich und die Verfahrensgarantien der allgemeinen Vorschriften der Beschlagnahme und Durchsuchung in Deutschland und Südkorea verglichen. I. R. d. Vorschriften der StPO wird einerseits diskutiert, ob sie eine heimliche Beschlagnahme und Durchsuchung zulässig machen und eine offene Sicherstellung der auf dem Server des Providers vorhandenen Daten rechtfertigen (Abschnitt B.), andererseits, wie wirksam der Richtervorbehalt in der Praxis ist und ob das Anwesenheitsrecht des Betroffenen und seines Verteidigers bei der vorläufigen Sicherstellung gemäß § 110 StPO zu gewährleisten ist (Abschnitt C.). In Abschnitt D. wird beschrieben, wie diese Streitpunkte in Südkorea diskutiert werden. Schließlich werden in Kapitel 5 die Zwischenergebnisse der vorangegangenen Kapitel zusammengefasst.

Kapitel 2

Fortschritt der Informationstechnik, Rechtsstaatsprinzip und maßgebliche Grundrechte

A. Fortschritt der Informationstechnik und Rechtsstaatsprinzip

I. Änderung der Realität und neue Gefährdungen

1. Informationstechnik und ihre Bedeutung für die Persönlichkeitsentfaltung

Die Veränderungen des Lebensumfelds, die die Entwicklung der Informationstechnik mit sich gebracht hat, sind in allen Bereichen bereits weit fortgeschritten. In letzter Zeit hat die Tragweite und Bedeutung dieser Technologie durch eine Vernetzung informationstechnischer Systeme[1] und elektronischer, informationstechnische Komponenten enthaltender Geräte, nämlich die Konvergenz von Informations- und Telekommunikationstechnik, weiter zugenommen.[2] Heutzutage kann jeder die informationstechnischen Systeme und die sie miteinander verbindenden Netzwerke wie das Internet und Intranet nutzen und damit unabhängig von der Entfernung große Mengen von Daten schnell und einfach austauschen und verarbeiten. Die hochmoderne Informations- und Kommunikationstechnologie verändert alle Lebensbedingungen epochal.[3] Zuerst kann der Einzelne im Allgemeinen mithilfe informations-

[1] „Informationstechnische Systeme" meint elektronische Geräte, mit denen man digitale Daten erzeugen, verarbeiten oder speichern kann. Darunter fallen etwa sowohl Personalcomputer (PCs) und Mobiltelefone einschließlich mobiler Geräte in Form von Smartphones oder Tablet-PCs als auch Datenträger. Zu Letzteren gehören nicht nur interne oder externe Festplatte und sonstige tragbare Speicherlaufwerke (z. B. USB-Sticks), die meist persönlicher Nutzung des Einzelnen dienen, sondern auch Business-Server, die geschäftlicher Nutzung von Unternehmen, Organisationen und Regierungen dienen.

[2] *BVerfGE* 120, 274, 304.

[3] *Schertz*, NJW 2013, 721; auch *Blechschmitt*, MMR 2018, 361, 362 am Anfang. Da vor allem in den letzten zwanzig Jahren das repräsentative informationstechnische System „Smartphone" und das integrierte Netz „Internet" die Bedingungen der Realität, die Voraussetzungen zur Rechtsanwendung darstellen, durchaus verändert haben und dies auch heute noch gilt, sind die Bezeichnungen wie „Internetzeitalter", „Zeit smarter Technologien" (*Heckmann*, NJW 2012, 2631) oder „digitale Gesellschaft" (*Papier*, NJW 2017, 3025) nicht mehr gekünstelt.

technischer Systeme und des Internets personenbezogene Daten[4] erstellen und verarbeiten, mit anderen kommunizieren, Waren und Dienstleistungen kaufen und Finanztransaktionen durchführen. Auf der anderen Seite stellt „jeder, der ganz oder teilweise geschäftsmäßig oder öffentlich Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt", (im Folgenden, „(Dienst-)Anbieter" oder „ISP (Internet service provider)"),[5] dem Einzelnen über die Systeme und das Internet verschiedene Dienste (z. B. sowohl – reine – Kommunikationsdienste wie E-Mail-Verkehr oder Cloud-Computing als auch Online-Handel) zur Verfügung. Diese voneinander abhängige Struktur gilt gleichermaßen für Unternehmen und Länder, die personenbezogene Daten ihrer Mitarbeiter oder Bürger auswerten. Die Unternehmen speichern und verwalten geschäftsbezogene Daten auf einem integrierten Server und ermöglichen es ihren Mitarbeitern, die Daten über informationstechnische Systeme wie PCs oder Smartphones oder das Intranet abzurufen und zu nutzen. Auch die Staaten speichern und verwalten zur Erfüllung öffentlicher Aufgaben oder zur Erbringung öffentlicher Dienstleistungen auf ihrem Server personenbezogene Daten der Bürger, zu denen die Beamten Zugang haben. Heute sind verschiedene komplexe informationstechnische Systeme und komplexe Netzwerke, insb. das Internet,[6] für die Lebensführung der Bürger und für die Arbeit von Unternehmen und Staaten unverzichtbar geworden, und diese Abhängigkeit wird sich in Zukunft noch vertiefen.[7]

Heute ist der Markt für TK-Dienste, der von ISPs geführt wird, wettbewerbsintensiv, sodass bestehende Dienste nicht nur schnell durch neue ersetzt werden, sondern auch zahlreiche neue Arten von Diensten weiter entstehen. Die E-Mail hat zunächst bereits herkömmliche Post, Telegraf und -fax weitgehend ersetzt, und die Internet-Telefonie wie *Skype* (sog. „IP-Telefonie" oder „VoIP (Voice over IP)") ersetzt derzeit herkömmliche Telefone allmählich. Außerdem ersetzt und ergänzt ein Internet-Chat/Online-Chat wie etwa *WhatsApp*, *Facebook Messenger*, in dem zwei oder mehrere Nutzer mittels geschriebenem Text in Echtzeit Kommunikation führen

[4] Vgl. § 3 Abs. 1 BDSG: Die Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

[5] Vgl. § 3 Nr. 6 TKG. Aus § 3 Nr. 10 TKG ergibt sich, dass Dienstanbieter sein kann, wer keine Gewinnerzielungsabsicht verfolgt. Von diesem Anbieter erfasst ist, wer seine Dienste nur innerhalb geschlossener Benutzergruppen und damit nicht jedermann, sondern nur den Mitgliedern dieser Gruppen anbietet (*Schütz*, in: Geppert/Schütz, Beck'scher TKG-Komm, § 3 Rn. 15). Mitwirkende sind Erfüllungsgehilfen oder externe Hilfspersonen, also Mitarbeiter oder Subunternehmer des Erbringers (*Lünenbürger/Stamm*, in: Scheurle/Mayen, TKG-Komm, § 3 Rn. 12; *Schütz*, a. a. O.). In vorliegender Arbeit enthält „(Dienst-)Anbieter" oder „ISP" nicht nur die Unternehmen, die TK-Dienste bereitstellen, sondern auch die sonstigen Unternehmen bzw. die öffentlichen Hände, die über das TK-Netz weitere Dienste anbieten.

[6] Vgl. *Schertz*, NJW 2013, 721, 722: Das Internet, wo moderne IuK-Technologie implementiert ist, hat die Reichweite des Persönlichkeitsrechts erheblich ausgedehnt.

[7] Vgl. *Szesny*, WiJ 2012, 228: das papierlose Büro in der Zukunft.

können, die E-Mail und die Telefonie in nicht geringem Ausmaß.[8] In sozialen Netzwerken wie z. B. *Facebook* und *Instagram* können viele Nutzer – die zumindest voneinander als „Freunde" anerkannt werden – ihre persönlichen Daten zeitversetzt, aber tatsächlich in Echtzeit, miteinander austauschen.[9] Einen damit vergleichbaren Dienst kann man auch durch (geschlossene) Internet-Foren nutzen, die einen virtuellen Platz zum Austausch und zur Archivierung von Gedanken, Meinungen und Erfahrungen darstellen.[10] In letzter Zeit wird auch Cloud-Computing zunehmend verwendet, in dem die Verwahrung und Verwaltung der Daten durch den von ISPs bereitgestellten Server durchgeführt wird, ohne dass jeder Dienstbenutzer sie selbst vornehmen muss. Des Weiteren werden das IoT (Internet der Dinge), das alle Objekte mit Elementen aus der IuK-Technologie ausstattet und damit jedem Benutzer eine individuell und optimal abgestimmte Nutzungsumgebung bietet, und die AI (artifizielle Intelligenz), die die von jedem Einzelnen hinterlassenen Informationen sofort analysiert und zur Bereitstellung anderer Dienste nutzt, schrittweise umfassend eingeführt.

Zusammengefasst bietet die Nutzung der IT heute dem Einzelnen unvergleichlich mehr Möglichkeiten der Persönlichkeitsentfaltung als zuvor, andererseits ist dies aber zumindest für die Mehrheit der Bürger keine Wahl mehr, sondern eine Notwendigkeit. So hat sie i. R. d. Persönlichkeitsentfaltung eine früher nicht absehbare Bedeutung erlangt.[11] In der modernen Informationsgesellschaft ist die Nutzung der IT selbst und der informationstechnischen Systeme zur Erhaltung der Würde des Menschen (Art. 1 Abs. 1 GG) und zur freien Entfaltung der Persönlichkeit (Art. 2 Abs. 1 GG) „Schlüsselmittel" und „unvermeidliche Voraussetzung".

2. Ansammlung und Konzentration von Daten und neuartige Gefährdungen

a) Ansammlung und Konzentration von Daten – Eigenschaften elektronischer Daten und Arten der Telekommunikationsdaten

(1) Elektronische Daten bzw. Computerdaten in digitaler Form, die einerseits die zu schützenden Rechtsgüter im materiellen Strafrecht und andererseits sicherzu-

[8] Vgl. *Klesczewski*, ZStW 123 (2011), 737, 752: Der Internet Relay Chat (IRC). Heute ist zwar die Verwendung dieses Dienstes in der Regel unter einem Pseudonym/Nickname möglich, aber dafür ist eine Registrierung und eine Anmeldung über ein Benutzerkonto (fast) stets erforderlich.

[9] Durch diesen Informationsaustausch und Beziehungsaufbau entsteht eine sog. „Online-Community", die eine organisierte Gruppe von Menschen darstellt.

[10] Sie werden auch als Web-Foren, Online-Foren, Diskussionsforen oder Bulletin-Board bezeichnet. In der Literatur werden teilweise die sozialen Netzwerke und die Internet-Foren zusammen auch als „Newsgroups" bezeichnet (vgl. *Klesczewski*, ZStW 123 (2011), 737, 739 und 753).

[11] *BVerfGE* 120, 274, 303.

stellende Beweismittel im Strafverfahrensrecht darstellen, haben – im Vergleich zu herkömmlichen Tatobjekten oder Beweismitteln wie z. B. Gegenständen, Papieren, Körpern – eigene Eigenschaften: Unkörperlichkeit bzw. Unsichtbarkeit, Datenfülle, einfache Möglichkeit der Vervielfältigung, Netzwerkbezogenheit und Flüchtigkeit bzw. Nicht-Flüchtigkeit etc.[12] Solche Daten werden mit hundertprozentiger Genauigkeit verarbeitet und u. a. können sie nach dem Fortschritt der Technik nicht nur auf einen kleinen Datenträger nahezu unbegrenzt und kumulativ gespeichert, sondern auch in Sekunden kopiert, übermittelt und gelöscht werden. Fast alle neu produzierten Informationen sind derzeit entweder digital oder in dieses Format konvertierbar, und darüber hinaus werden auch die vorhandenen Informationen in elektronische Form konvertiert.[13] Um sie sichtbar zu machen, ist dabei ein Prozess notwendig, sie durch informationstechnische Systeme und ein spezifisches Programm zum Ausdruck zu bringen, und bis dahin kann man den Inhalt und Umfang der Daten nicht kennen.

Zum anderen werden in der Informationsgesellschaft, wo die Erstellung, Verarbeitung und Übermittlung der Daten technisch in PCs oder Smartphones und das Internet integriert ist, elektronische Spuren persönlichen Verhaltens in allen Lebensbereichen, die bei der Nutzung der IuK-Technologie hinterlassen werden („e-Spähre“[14]), unabhängig davon, ob ein Benutzer es wünscht oder nicht, in informationstechnischen Systemen, insb. lokalen Endgeräten und Servern des Dienstanbieters nach dem Zeitablauf sehr genau aufgezeichnet. Außerdem werden sie normalerweise dauerhaft gespeichert, es sei denn, dass sie i. d. R. absichtlich gelöscht werden. Zudem werden solche persönlichen Spuren bei IoT bzw. AI oft ohne TK-Partner nur aus der Vernetzung bzw. der Kommunikation zwischen Menschen und (smarten) Geräten erzeugt und auf die informationstechnischen Systeme gespeichert. Somit werden in der modernen Informationsgesellschaft detaillierte Informationen über die persönlichen Verhältnisse und die Lebensführung des Einzelnen (wie z. B. Worte, Verhalten und Gewohnheiten einschließlich tagebuchartiger intimer Aufzeichnungen) auf alle IT-Geräte und ihre internen und externen Speichermedien nicht nur „umfassend, kumulativ und dauerhaft gespeichert“, sondern sie „übertreffen auch herkömmliche Informationsquellen an Umfang und Vielfältigkeit bei

[12] *Kudlich*, StV 2012, 560, 560 f. Diesbezüglich, als Phänomene bzw. Charaktere in dem digitalen Ermittlungsumfeld, bei dem es sich um Kriminalität und Strafverfolgung im Internet handelt, weist *Sieber* auf Globalität und Ubiquität von Computerdaten, Anonymität des Internets, Kontrollresistenz der Informationstechnik, Größe des auszuwertenden Datenvolumens, Geschwindigkeit und Komplexität hin (*Sieber*, 69. DJT 2012, C 35 ff.).

[13] Vgl. *BVerfGE* 141, 220, 304 [Rn. 210]: „*Tagebuchartige Aufzeichnungen, intime Erklärungen oder sonstige schriftliche Verkörperungen des höchstpersönlichen Erlebens, Film- oder Tondokumente werden heute zunehmend in Dateiform angelegt, gespeichert und teilweise ausgetauscht.*“

[14] *Vogel*, ZIS 2012, 480, 481. Hier bezeichnet *Vogel* die elektronischen Spuren als „e-Sphäre“ eines Menschen. Sie bedeuten alle persönlichen Daten in digitaler Form, die zum privaten Bereich gehören.

weitem".[15] Angesichts des rasanten Fortschritts der Technologie, der wettbewerbsfähigen Dienstleistungen durch ISPs und der anspruchsvollen Nachfrage nach Annehmlichkeiten des Einzelnen etc. wird sich dieses Phänomen weiter verschärfen. Doch es kann tatsächlich zumeist nicht von einer Einzelperson umgangen werden[16], und außerdem können die auf ISPs gespeicherten Daten manchmal von dem Nutzer nicht endgültig gelöscht werden.[17]

(2) Werden personenbezogene Daten von Dienstanbietern verarbeitet oder übermittelt, so werden i. d. R. drei Arten von Daten erzeugt und gespeichert (im Folgenden, „Telekommunikationsdaten" oder „TK-Daten"). Jeder Nutzer gibt zur Nutzung der TK-Dienste zuerst den Anbietern seine Personalien wie z. B. Namen, Anschriften und Geburtsdaten (sog. „Bestandsdaten"[18]) an; zu diesem Begriff können ggf. „Zugangssicherungscodes"[19] wie Passwörter gehören, mittels deren der Zugriff auf Endgeräte selbst oder derselbe auf Speichereinrichtungen, die in ihnen oder hiervon räumlich getrennt eingesetzt sind, geschützt wird. Danach werden Telekommunikationsinhalte wie z. B. Worte, Stimmen, Bemerkungen und Fotos, die bei Nutzung der Dienste durch den Nutzer erstellt, verarbeitet, übermittelt und gespeichert werden, (sog. „Inhaltsdaten"[20]) i. d. R. in allen genutzten und zwischengeschalteten Systemen und Netzwerken automatisch gespeichert. Dann unterscheiden sich die durch den Nutzer heruntergeladenen und gespeicherten Inhaltsdaten aufgrund der Natur von Digitaldaten anscheinend nicht mehr von Daten, die der Nutzer – unabhängig von der Kommunikation – selbst angelegt hat.[21] Letztlich

[15] *BVerfGE* 120, 274, 322 f.; *Blechschmitt*, MMR 2018, 361, 362; dazu *Kudlich*, GA 2011, 193, 208: „*Informationen sind in einer Dichte und Vielfalt zusammengeführt, wie dies in der Vor-EDV-Zeit kaum denkbar war.*" In jüngster Zeit werden Waren und Dienstleistungen aller Art überwiegend über das Internet angeboten oder gehandelt, und Unternehmen sammeln große Menge an Daten, die in diesem Prozess hinterlassen werden, (sog. „Big Data") für wirtschaftliche und kommerzielle Zwecke. Diese Daten sagen viel über Dienstnutzer aus, z. B. Auskunft über ihr Verhalten und ihre Gedanken und Bedürfnisse.

[16] Vgl. *BVerfGE* 125, 260, 318 f. [Rn. 210]: „*Die Speicherung bezieht sich dabei auf Alltagshandeln, das im täglichen Miteinander elementar und für die Teilnahme am sozialen Leben in der modernen Welt nicht mehr verzichtbar ist. … Eine reguläre Ausweichmöglichkeit für den Bürger eröffnet dies (jedoch) nicht.*"

[17] Vgl. *BVerfGE* 125, 260, 319; auch *Brodowski*, JR 2009, 402, 403 [Tz. (iii)].

[18] §§ 3 Nr. 3, 111 Abs. 1 TKG.

[19] § 113 Abs. 1 S. 2 TKG. Die Daten, die dem Schutz vor unbefugtem Zugriff auf informationstechnische Systeme oder Speichereinrichtungen dienen, bezeichnet man als „Zugangssicherungscode", „Zugangscode", „Zugangsdaten" oder „Sicherungscode", wobei sie insb. bei Endgeräten zur TK-PIN (Personal identification number, persönliche Identifikationsnummer) und PUK (Personal Unblocking Key, persönlicher Entsperrungsschlüssel) heißen (*BVerfGE* 130, 151, 208 [Rn. 184]; *Bruns*, KK-StPO, § 100j Rn. 3; *Greco*, SK-StPO, § 100j Rn. 9; M-G/*Schmitt*, StPO, § 100j Rn. 3).

[20] Der Begriff von Inhaltsdaten ist gesetzlich – auch in § 3 TKG – nicht definiert. Sie sind der eigentliche Inhalt der TK, nämlich die Informationen, deren Übermittlung die Intention des TK-Vorganges ist (*Bruns*, KK-StPO, § 100a Rn. 15; *Neuhöfer*, JR 2015, 21, 22).

[21] *BVerfGE* 115, 166, 185 [Rn. 76]; dazu *Singelnstein*, NStZ 2012, 593, 602: „*Aus rechtlicher Sicht ergeben sich (heutzutage) für den Zugriff auf nicht aus TK kommende Daten im*

werden die Daten über nähere Umstände des Kommunikationsvorgangs wie z. B. Zeit und Standort des Erstellens, Modifizierens und Übermittelns der Nachrichten (sog. „Verkehrsdaten“[22] und „Standortdaten“[23]) auf den informationstechnischen Systemen des Nutzers und der Anbieter in zeitlicher Reihenfolge detailliert gespeichert. Dadurch, dass neuerlich die Arten der von Anbietern angebotenen TK-Dienste wettbewerblich vielfältig werden, werden auch allein aus diesen Daten – ohne Inhaltsdaten – durch eine umfassende und automatisierte Auswertung „tiefe Einblicke in das soziale Umfeld und die individuellen Aktivitäten“ eines Einzelnen möglich gemacht. In dieser Hinsicht können heute die Verkehrsdaten im Einzelfall einen eigenen Aussagegehalt haben.[24] In der Entscheidung zur VDS hat das *BVerfG* wie folgt ausgeführt:

> „Angesichts der … gesteigerten Aussagekraft der über 6 Monate systematisch vorsorglich erhobenen Verkehrsdaten hat ihr Abruf ein ungleich größeres Gewicht. Da eine Auswertung dieser Daten tief in das Privatleben eindringende Rückschlüsse und unter Umständen detaillierte Persönlichkeits- und Bewegungsprofile ermöglicht, kann insoweit nicht ohne weiteres davon ausgegangen werden, dass der Rückgriff auf diese Daten grundsätzlich geringer wiegt als eine inhaltsbezogene TKÜ.“[25]

b) Neuartige Gefährdungen

Die Ansammlung und Konzentration von Daten und die Einfachheit des Zugriffs darauf führt neuartige Gefährdungen herbei, dass personenbezogene Daten von Dritten unbegrenzt oder unverhältnismäßig erhoben und verwendet werden können. Die herkömmlichen Fernmeldeverkehre wie Telefongespräch, Post etc. sind temporär und punktuell und ihre Gebrauchsspuren blieben nur teilweise und ungenau,

Herrschaftsbereich des Betroffenen im Vergleich mit dem speziellen Bereich der TK-Daten kaum Besonderheiten.“

[22] §§ 3 Nr. 30, 96 Abs. 1 TKG. Der Rechtsausdruck der Verkehrsdaten, durch den die früheren TK-„Verbindungsdaten“ ersetzt werden, wurde durch das völlig neugefasste TKG vom 22. Juni 2004 (BGBl. I S. 1190) erstmals eingeführt und hierauf wird er durch die Inkraftsetzung des TKÜG vom 1. Januar 2008 auch in der StPO anstelle der „Verbindungsdaten“ genutzt. In der vergangenen Zeit waren die Verbindungsdaten definiert als „personenbezogene Daten eines an der TK Beteiligten, die bei der Bereitstellung und Erbringung von TK-Diensten erhoben werden“ (§ 2 Nr. 4 TK-Datenschutzverordnung (TDSV) a. F. i. V. m. § 89 Abs. 1 TKG a. F.). Auf jeden Fall wird der Ausdruck „Verbindungsdaten“ seit dem TKÜG nicht mehr in deutschem Recht verwendet (vgl. *Kudlich*, GA 2011, 293, 200 [Fn. 35]).

[23] §§ 3 Nr. 19, § 96 Abs. 1 Nr. 1, 98 Abs. 1 TKG. Standortdaten können eine Art der Verkehrsdaten sein.

[24] *BVerfGE* 107, 299, 320; 115, 166, 183 [Rn. 71]; 125, 260, 319 [Rn. 211]. Nach einer Meinung sind Verkehrsdaten nicht so sensibel wie Inhaltsdaten (*Kudlich*, GA 2011, 193, 200). In der Entscheidung des Falls *Edathy* hat aber das *BVerfG* entschieden: Dass das *LG* bei der Anordnung der Durchsuchung und Beschlagnahme von E-Mails (Inhaltsdaten) und Verkehrsdaten nicht durchweg zwischen beiden Daten unterschieden hat, ist im Hinblick auf die parallelen Anforderungen hinsichtlich dieser beiden Kategorien nicht zu beanstanden (NJW 2014, 3085, 3089 [Rn. 47]).

[25] *BVerfGE* 125, 260, 328 [Rn. 227].

während in der aktuellen (Tele-)Kommunikation alle Spuren detailgenau aufgezeichnet und gespeichert werden. Heute kann daher nicht nur der – verdeckte – Zugriff auf einen „laufenden" Telekommunikationsvorgang, sondern auch der – verdeckte oder offene – Zugriff auf „gespeicherte" frühere Kommunikation vertiefende Eingriffe in die Grundrechte hervorrufen. Mit Blick auf den Inhalt und Umfang der erfassten Daten hat sich das Gewicht des letzteren Eingriffs in einem Maße erhöht, das in der Vergangenheit undenkbar gewesen wäre. Durch nur einen einzigen Zugriff auf informationstechnische Systeme oder Datenträger können Ermittlungsorgane sensible Informationen wie Daten mit Kernbereichsbezug, Daten im Besitz von Geheimnisträgern bzw. Zeugnisverweigerungsberechtigten und wichtige interne Informationen von Organisationen oder Unternehmen umfassend erheben.[26] Im Zuge der Auffindung verfahrensrelevanter Daten zur Strafverfolgung werden nicht nur die potenziell beweiserheblichen und so zu beschlagnahmenden Daten, sondern auch die zu dem Kernbereich zählenden oder nach § 97 StPO beschlagnahmefreien Daten und die verfahrensirrelevanten Daten von Ermittlungsbehörden praktisch vielfach pauschal sichergestellt. Demzufolge sind Bürger und Unternehmen um den möglichen Missbrauch belastender Daten besorgt, die in den Informationen, die freiwillig herausgeben oder zwangsweise beschlagnahmt werden, enthalten sein können. Außerdem können sie in der Tat anlasslos dem Risiko weiterer Ermittlungen ausgesetzt werden. Dies führt zum Problem, dass es den Einzelnen zwingt, in Rechnung zu stellen, dass seine wichtigen Daten jederzeit vom Staat überwacht werden können, und dadurch eine unbefangene Wahrnehmung seiner Grundrechte beeinträchtigt wird.[27] Die Erhebung und Verwendung von so umfassenden Daten, die zur erkennbaren Rekonstruierbarkeit aller Aktivitäten der Bürger führen können, sog. „Rundum- oder Totalüberwachung", ist unter dem GG zwar nicht zulässig,[28] jedoch kann der – heimliche oder offene – Zugriff auf die Datenbestände in der modernen Informationsgesellschaft stets zur „umfangreichen Erhebung personenbezogener Daten" und damit zu „schweren Verletzungen des Persönlichkeitsrechts und der Menschenwürde" führen. Also bedrohen die Risiken i. R. d. modernen Informationstechnologie über den Aspekt der Integrität von Computersystemen hinaus die Privatsphäre der Bürger in fundamentaler Weise.[29]

Wie das *BVerfG* bereits herausgestellt hat, begründet zwar der Fortschritt der IT und ihr universeller Einsatz für den Einzelnen neben neuen Möglichkeiten der Persönlichkeitsentfaltung auch neue Persönlichkeitsgefährdungen, aber ein wirkungsvoller sozialer oder technischer Selbstschutz vor dieser Gefährdung ist er-

[26] Der Angeklagte wird im Ergebnis zum „gläsernen Angeklagten" (*Blechschmitt*, MMR 2018, 361).

[27] Vgl. *BVerfGE* 125, 260, 320.

[28] *BVerfGE* 109, 279, 323; 112, 304, 319; 130, 1, 24; 141, 220, 317 f.; *Roxin/Schünemann*, § 36 Rn. 2; dazu *BVerfGE* 125, 260, 324 [Rn. 218]: „*Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland.*"

[29] *Sieber*, 69. DJT 2012, C 10.

heblich schwieriger und eine zumindest für die durchschnittlichen Bürger übermäßige Forderung.[30]

II. Aufgaben des Staates und rechtsstaatliche Grenzen

1. Aufgaben des Staates und Anpassung an die Veränderung der Realität

Wie unter dem GG der Achtung der Menschenwürde (Art. 1 Abs. 1 S. 1) und dem Recht auf die freie Entfaltung der Persönlichkeit (Art. 2 Abs. 1) ein hoher Rang zugewiesen wird (vgl. unten B. II. 1.), werden auch der Sicherheit des Staates und der Bevölkerung (Art. 2 Abs. 1 S. 1 und Art. 1 Abs. 1 S. 2) hohe Verfassungswerte zugemessen.[31] Daher obliegt es dem Staat, die verfassungsmäßige Ordnung wie die freiheitliche demokratische Grundordnung oder die Rechtsstaatlichkeit, den Bestand und die Sicherheit des Bundes und der Länder sowie Leib, Leben und Freiheit der Person zu garantieren. Das *BVerfG* hebt wiederholt die unabweisbaren Bedürfnisse einer wirksamen Strafverfolgung und Verbrechensbekämpfung hervor[32] und bezeichnet die wirksame Aufklärung schwerer Straftaten als einen wesentlichen Auftrag eines rechtsstaatlichen Gemeinwesens.[33] Die Sicherung des Rechtsfriedens durch Strafrecht ist seit jeher eine wichtige Aufgabe staatlicher Gewalt.[34] Daneben ist das deutsche Strafverfahrensmodell auf das Prinzip der materiellen Wahrheit gegründet.[35] Da die Umsetzung der Gerechtigkeit durch die Bestrafung von Straftätern die Verwirklichung des materiellen Schuldprinzips darstellt, die durch ein gerechtes Urteil garantiert wird, das die materielle Wahrheit voraussetzt, ist das zentrale Anliegen des Strafprozesses die Ermittlung des wahren Sachverhalts.[36] Daher stellt die Erforschung der materiellen Wahrheit im Strafverfahren unverzichtbare Werte bzw. Rechtsgüter dar[37], und auch das *BVerfG* betont das öffentliche Interesse an einer „möglichst vollständigen Wahrheitsermittlung" im Strafverfahren.[38]

---

[30] *BVerfGE* 120, 274, 305 f. [Rn. 177 und 180].

[31] *BVerfGE* 120, 274, 319 [Rn. 220]; 141, 220, 267 f. [Rn. 100]; *Vogelgesang*, Grundrecht auf informationelle Selbstbestimmung?, 192.

[32] *BVerfG* 19, 342, 347; 33, 367, 383; 77, 65, 76; 107, 299, 316; 113, 29, 54 [Rn. 111]; 115, 166, 192 [Rn. 98]; insb. 109, 279, 336 [Rn. 200].

[33] *BVerfGE* 29, 183, 194; 33, 367, 383; 77, 65, 76; 107, 299, 316; 139, 245, 278 [Rn. 93]; insb. 109, 279, 336 [Rn. 200]. Der Verhinderung und Aufklärung von Straftaten kommt nach dem GG hohe Bedeutung zu (*BVerfGE* 113, 29, 54 [Rn. 111]; 115, 166, 192 [Rn. 98]).

[34] *BVerfGE* 113, 29, 54 [Rn. 111]; 115, 166, 192 [Rn. 98].

[35] *Roxin/Schünemann,* § 15 Rn. 3; *Volk/Engländer*, § 18 Rn. 15.

[36] Vgl. *BVerfG* 122, 248, 270 [Rn. 66]; 130, 1, 26 [Rn. 113]; insb. 133, 168, 199 [Rn. 56] und 221 [Rn. 95].

[37] Vgl. *Roxin/Schünemann*, § 15 Rn. 6: „*Der Strafprozess kann nur durch das Verfahrensziel der materiellen Wahrheitsfindung legitimiert werden.*"

Die moderne IuK-Technologie übt auch auf Kriminelle und Ermittlungsbehörden Einfluss aus. Täter begehen mittels informationstechnischer Systeme ein Verbrechen und arbeiten effektiv miteinander zusammen.[39] Tatsächlich werden heute fast alle Arten von Verbrechen im Bereich sowohl der normalen Kriminalität wie z. B. Betrug oder Untreue als auch der Cyberkriminalität, wie z. B. Ausspähen oder Abfangen von Daten, unter direkter und indirekter Nutzung der IT verübt. Der Zugang zu Daten, die in informationstechnischen Systemen und im Internet hinterlassen wurden, und die Rekonstruktion des Sachverhalts sind daher für eine wirksame Strafverfolgung von entscheidender Bedeutung. Aus Sicht der Ermittlungsbehörden ist die „e-Sphäre" von Verdächtigen hoch interessant, weil sie potenziell hoch ergiebiges Mittel zur Aufklärung von Straftaten darstellt.[40] In der Praxis wird die Durchsuchung von Mobiltelefonen, PCs und Servern schon üblicherweise als erste Standardmaßnahme getroffen.[41] Weil im Fall der organisierten Kriminalität (z. B. die Rauschgiftkriminalität oder extremistische Straftaten wie Terrorismus)[42] oder der Wirtschaftskriminalität (z. B. Steuerhinterziehung oder Korruption) offene Ermittlungsmaßnahmen nur von begrenztem Wert sind, ist es dabei zur Sachverhaltsaufklärung notwendig und wirksam, Informationen in der e-Sphäre ohne Wissen des Betroffenen zu erheben.[43] Für die Befriedung und Wahrung der wichtigen Rechtsgüter des Einzelnen und des Staates ist die Funktionstüchtigkeit der Strafrechtspflege[44] stets von aktueller Bedeutung.[45] Daher sollen zur Gewährleistung der funktionstüchtigen Strafrechts-

[38] *BVerfG* 32, 373, 381; 33, 367, 383; 77, 65, 76; 109, 279, 336 [Rn. 200]; 130, 1, 27 [Rn. 114].

[39] Vgl. *BVerfGE* 123, 43, 63 f.: „*Moderne Kommunikationstechniken werden im Zusammenhang mit der Begehung unterschiedlichster Straftaten zunehmend eingesetzt und tragen zur Effektivierung krimineller Handlungen bei*"; auch *Hofmann*, NStZ 2005, 121.

[40] *Vogel*, ZIS 2012, 480, 481; auch *Blechschmitt*, MMR 2018, 361, 363; *Singelnstein*, NStZ 2012, 593, 599 [Tz. 5] und 603 am Anfang.

[41] *Vogel*, ZIS 2012, 480, 481 f.

[42] Vgl. für den Begriff und die Art der „Organisierten Kriminalität" BT-Drs. 12/989, S. 20 f.; *Bruns*, KK-StPO, § 110a Rn. 3 f.; für ihre Merkmale *BGHSt* 32, 115, 120: „*Die Vorgehensweise der Täter im Rahmen dieses ‚organisierten Verbrechens' ist darauf angelegt, die Hauptpersonen möglichst nicht nach außen in Erscheinung treten zu lassen.*"

[43] *BGHSt* NJW 1997, 1934, 1935. Eine effektive, aber am Gebot der Rechtsstaatlichkeit ausgerichtete und dem Datenschutz angemessen Rechnung tragende Strafverfolgung muss sich diesen technischen Veränderungen stellen und staatliche Ermittlungsmaßnahmen dem technischen Fortschritt anpassen (BT-Drs. 18/12785, S. 48 a. E.).

[44] Vgl. *Hassemer*, StV 1982, 275, 276 ff. Unter dem Begriff der „Funktionstüchtigkeit der Strafrechtspflege" versteht hier *Hassemer* systematisch, dass der Topos das Strafverfahren zugunsten der Strafverfolgungsinteressen und zulasten der Justizförmigkeit verkehrt wird, und er übt an seiner Richtigkeit Kritik (zust. *Roxin/Schünemann,* § 1 Rn. 7). Außerdem betonen *Roxin/Schünemann*, dass die Funktionstüchtigkeit unter rechtsstaatlicher Strafrechtspflege mit voller Wahrung der Justizförmigkeit verbunden und der Widerstreit zwischen den Bedürfnissen der Effizienz und des Beschuldigtenschutzes im Ergebnis nach einer Gesamtabwägung gelöst werden muss (a. a. O.).

[45] *Landau*, NStZ 2007, 121.

pflege[46] auch Ermittlungsmethoden und Fachkräfte zur Strafverfolgung entsprechend den technologischen und sozialen Veränderungen geändert bzw. angepasst werden. Wie der Einzelne zur Ausübung seiner Grundrechte der Persönlichkeitsentfaltung mit der technischen Entwicklung Schritt hält, sollte sich der Staat zur Wahrnehmung seiner Aufgaben der Strafverfolgung und Verbrechensbekämpfung an sie anpassen.[47]

Zusammengefasst bewirkt die Veränderung der Realität durch IT zwar einerseits für den Einzelnen neue Persönlichkeitsgefährdungen (vgl. oben I.), aber sie erlegt andererseits dem Staat „neue Herausforderungen der Verbrechensbekämpfung durch effektive Strafverfolgung" auf. Damit die Ermittlungsbehörden solche Herausforderungen bewältigen und zugleich eine funktionstüchtige Strafrechtspflege aufrechterhalten, ist eine Modernisierung der Ermittlungsmethoden, nämlich eine Anpassung der Leistungsstärke der Ermittlungsorgane und der Strafverfolgungsstrategien an die gewandelte Realität, erforderlich,[48] was verfassungsrechtlich geboten ist.

2. Strafverfahrensrecht im Rechtsstaat

a) Rechtsstaatsprinzip und Grenzen der Ermittlungshandlungen

In dem liberal-demokratischen Verfassungssystem ist die Rechtsstaatlichkeit eines der zentralen verfassungsrechtlichen Prinzipien[49], und in das GG ist nicht nur seine tradierte formale Seite, sondern auch die materiale Seite schon aufgenommen (Art. 28 Abs. 1 S. 1 i. V. m. Art. 20 Abs. 2 und 3).[50] Indem die formelle Rechtsstaatlichkeit der Staatsgewalt durch verfahrens- und organisationsrechtliche Vor-

---

[46] *BVerfGE* 33, 367, 383; 130, 1, 26; 133, 168, 199 m. w. N.; M-G/*Schmitt*, StPO, Einl. Rn. 18.

[47] *BVerfGE* 115, 166, 193 [Rn. 102]; 123, 43, 64 [Rn. 71]: „*Das Schritthalten der Strafverfolgungsbehörden mit der technischen Entwicklung … ist vor dem Hintergrund der Verlagerung herkömmlicher Kommunikationsformen hin zum elektronischen Nachrichtenverkehr einschließlich der anschließenden digitalen Verarbeitung und Speicherung zu sehen*"; dazu *Roxin/Schünemann*, § 69 Rn. 1: „*Es ist … fast selbstverständlich, dass die Modernisierung der Gesellschaft auch eine Modernisierung ihres Strafverfahrens erfordert.*"

[48] *Schünemann*, ZStW 114 (2002), 1, 17 f.; *Sieber*, 69. DJT 2012, C 127 [Tz. 11].

[49] *Grzeszick*, in: Maunz/Dürig, GG-K, Art. 20 VII Rn. 1 und 2; vgl. *BVerfGE* 133, 168, 198 [Rn. 55].

[50] *Grzeszick*, in: Maunz/Dürig, GG-K, Art. 20 VII Rn. 16 und 22 ff. Aus dem Regelungszusammenhang und der Entstehungsgeschichte des GG kann geschlossen werden, dass davon ausgegangen wurde, dass die BRD qua Verfassung ein Rechtsstaat sein soll (a. a. O. Rn. 31). Der Begriff des Rechtsstaats bezeichnet im allgemeinsten Sinne denjenigen Staat, in dem staatliche Gewalt nur aufgrund und im Rahmen des Rechts ausgeübt wird, und er zielt auf den Schutz der Freiheit durch die rechtliche Begründung und Begrenzung öffentlicher Gewalt ab (*Huster/Rux*, in: Epping/Hillgruber, BeckOK GG, Art. 20 Rn. 138).

kehrungen Grenzen setzt[51] und die materielle Rechtsstaatlichkeit die Ausübung der Staatsgewalt nach dem Organisations- und Verfahrensrecht inhaltlich an Verfassung und Grundrechte bindet,[52] werden die Grundrechte der Bürger geschützt. Der Staat nimmt eine Aufgabe des Schutzes der Grundlagen der Verfassungsordnung unter Einhaltung des Rechtsstaatsprinzips wahr, sodass er auch für die Verfolgung der fundamentalen Staatszwecke der Sicherheit und des Schutzes der Bevölkerung die rechtsstaatlichen Mittel einsetzen muss.[53] Das Rechtsstaatsprinzip und die Unterprinzipien, wie Gewaltenteilung, Gesetzesvorbehalt, Normenklarheit, Verhältnismäßigkeit und gerichtliche Kontrolle, sind im Strafprozessrecht, das i. d. R. staatliche grundrechtseingreifende Handlungen erlaubt, von besonderer Bedeutung.[54] Für kriminalistische Zwangsmaßnahmen sind gesetzliche Ermächtigungen erforderlich, die sich mit den Grundsätzen decken können (Art. 103 Abs. 2 GG).[55]

Heute führt die Verstärkung eines strafrechtlichen Sicherheitsdenkens bzw. das starke Bedürfnis nach der Bekämpfung der organisierten Kriminalität unabwendbar und zwangsläufig zur Erweiterung der eingriffsintensiven Ermittlungsmethoden: u. a. die umfassende Sicherstellung personenbezogener Daten und die neu konzipierten und erweiterten technischen Ausspähungsmethoden. Dies erschüttert jedoch die bestehende Festigkeit der Rechtsstaatlichkeit.[56] Die materielle Wahrheitsfindung muss auch in der modernen Informationsgesellschaft dem rechtsstaatlichen Grundsatz und dem Verfahrensrecht folgen.[57] Wie der *BGH* schon längst erklärt hat, ist es kein Grundsatz der StPO, dass die Wahrheit um jeden Preis erforscht werden

[51] *Grzeszick*, in: Maunz/Dürig, GG-K, Art. 20 VII Rn. 36 und Rn. 23 ff.: Zu diesem Inbegriff gehören die Grundsätze der Gewaltenteilung, der Bindung von Justiz und Verwaltung an das Gesetz, der Gesetzesvorbehalt der Beschränkung der Grundrechte, die gerichtliche Kontrolle des Handelns der Exekutive sowie die Grundsätze einer Staatshaftung. Dieser Rechtsstaatlichkeit werden auch Vorgaben für die Ausgestaltung von Organisation und Verfahren der Ausübung von Staatsgewalt entnommen (a. a. O. Rn. 129).

[52] *Grzeszick*, in: Maunz/Dürig, GG-K, Art. 20 VII Rn. 37. Zu dieser Rechtsstaatlichkeit gehört das Prinzip der Rechtssicherheit, das Prinzip des Vertrauensschutzes, das Verbot rückwirkender Gesetze, das Prinzip der Klarheit und das Übermaßverbot bzw. der Grundsatz der Verhältnismäßigkeit (a. a. O. Rn. 27).

[53] *BVerfGE* 115, 320, 358 [Rn. 127 f.]; auch a. a. O. [Rn. 130]: der Rechtsstaat gewährleistet sowohl die Sicherheit des Bürgers durch den Staat als auch Freiheitsrechte des Bürgers gegen den Staat: eine Doppelfunktion (*Papier*, NJW 2017, 3025, 3026).

[54] Vgl. *Roxin/Schünemann*, § 2 Rn. 1: Das Strafverfahrensrecht ist der Seismograph der Staatsverfassung.

[55] Vgl. *Neuhöfer*, JR 2015, 21, 23: eine geeignete gesetzliche Grundlage; auch *Kudlich*, GA 2011, 193, 195: Für das Strafverfahrensrecht gilt zwar der Gesetzlichkeitsgrundsatz nicht streng, jedoch unterliegen strafprozessuale Zwangsmaßnahmen als besonders scharfe Formeln staatlicher Eingriffe dem allgemeinen Vorbehalt des Gesetzes; dazu *Sieber*, 69. DJT 2012, C 11: bei eingriffsintensiven Maßnahmen in grundrechtssensiblen Bereichen; auch *Vogel*, ZIS 2012, 480, 482.

[56] Vgl. *Huster/Rux*, in: Epping/Hillgruber, BeckOK GG, Art. 20 Rn. 138.1: die aktuelle Herausforderung rechtsstaatlicher Errungenschaften.

[57] Vgl. *Vogel*, ZIS 2012, 480, 482 f.

müsste,[58] und gibt es im Strafverfahren Interessen, die der Wahrheitssuche im Wege stehen und die in einem Rechtsstaat dennoch geschützt werden müssen.[59] Nicht jedes Mittel, welches zur Wahrheitsfindung beitragen könnte, kann daher – unbeschränkt – akzeptiert werden, und sie darf grundsätzlich nur nach strafprozessualen Vorschriften, nämlich durch justizförmige Weise, erreicht werden (vgl. unten b)).

Zusammengefasst: Wie nach dem Fortschritt der IT zum Schutz der Rechtsgüter eine Anpassung der Fähigkeit der Ermittlungsbehörde an veränderte technische Gegebenheiten von Bedeutung ist (vgl. oben 1.), ist ebenfalls zum Schutz der Grundrechte auch eine Kontrollierung der Ermittlungshandlungen gestützt auf das Rechtsstaatsprinzip von Bedeutung.[60] Sowohl die Modernisierung der Ermittlungsmethoden und der Strafverfolgungsstrategien als auch die rechtsstaatliche Aktualisierung der dementsprechenden Ermächtigungsgrundlagen ist zugleich geboten. Ggf. ist es insoweit erforderlich, Abwägung zwischen der Freiheit und der Sicherheit und eine sachgemäße Verfahrensbalance erneut zu konzipieren.[61]

b) Fair-Trial-Grundsatz und Justizförmigkeit des Strafverfahrens

(1) Der Grundsatz des *fair trial* ist wie bekannt der angloamerikanische Rechtsgrundsatz. Er ist derzeit in Art. 6 Abs. 1 S. 1 EMRK verankert und genießt auch in Deutschland Verfassungsrang.[62] Der Anspruch/das Recht eines Beschuldigten und eines Angeklagten auf ein faires Verfahren ist zwar im GG und in der StPO ausdrücklich nicht erwähnt, aber wird aufgrund des Rechtsstaatsprinzips (Art. 20 Abs. 3 GG) i. V. m. dem allgemeinen Freiheitsrecht (Art. 2 Abs. 1 GG) anerkannt.[63] Dieser Grundsatz ist allgemeines Prinzip des Verfahrensrechts, weil ein gerechtes Urteil ein faires, ordnungsgemäßes Verfahren voraussetzt.[64] Doch darf er nicht an die Stelle von Vorschriften der StPO oder von Verfahrensgrundsätzen gesetzt werden.[65]

---

[58] *BGHSt* 14, 358, 365; dazu *BVerfGE* 115, 320, 358 [Rn. 128]: „*Das schließt die Verfolgung des Zieles absoluter Sicherheit aus, welche ohnehin faktisch kaum, jedenfalls aber nur um den Preis einer Aufhebung der Freiheit zu erreichen wäre*"; auch *Roxin/Schünemann*, § 24 Rn. 19: „*Die Wahrheitserforschung ist daher im Strafverfahren kein absoluter Wert.*"

[59] *BGHSt* 19, 324, 329; *Volk/Engländer*, § 3 Rn. 1.

[60] Zust. *Schünemann*, ZStW 114 (2002), 1, 17 f.: „*fehlt im Ermittlungsverfahren keine rechtsstaatliche Kontrolle, ist es der echte Polizeistaat*".

[61] *Sieber*, 69. DJT 2012, C 11; vgl. *BVerfGE* 115, 320, 358 [Rn. 128]: „*Die Verfassung verlangt vom Gesetzgeber, eine angemessene Balance zwischen Freiheit und Sicherheit herzustellen.*" Insb. bei eingriffsintensiven Maßnahmen in grundrechtssensiblen Bereichen muss es gesetzlich garantiert sein, dass die Freiheiten und Persönlichkeitsrechte der Bürger nicht unverhältnismäßig eingeschränkt werden (Vorbehalt des Gesetzes, vgl. *Sieber*, a. a. O.).

[62] M-G/*Schmitt*, StPO, Einl. Rn. 19; *Roxin/Schünemann*, § 2 Rn. 9 und § 11 Rn. 4.

[63] *BVerfGE* 26, 66, 71; 57, 250, 274; 118, 212, 231; 122, 248, 271; 133, 168, 200 [Rn. 59] m. w. N.

[64] *Volk/Engländer*, § 3 Rn. 1.

[65] M-G/*Schmitt*, StPO, Einl. Rn. 19. Das Recht auf faires Verfahren bedarf der Konkretisierung, die in erster Linie Aufgabe des Gesetzgebers und i. R. d. gesetzlichen Vorschriften der

Demzufolge entsteht aus dem Verstoß gegen den Fair-Trial-Grundsatz i. d. R. kein Verfahrenshindernis als Rechtsfolge.[66] Ergibt sich aus einer Gesamtschau auf das Verfahrensrecht, dass rechtsstaatlich zwingende Folgerungen nicht gezogen wurden oder rechtsstaatlich Unverzichtbares preisgegeben wurde, so liegt eine Verletzung dieses Grundsatzes vor[67], und weiter kann dies ggf. zu einem Beweisverwertungsverbot führen.

Der Grundsatz des fairen Verfahrens verlangt insb. Waffengleichheit zwischen den Strafverfolgungsbehörden und den Beschuldigten oder Angeklagten (das Prinzip der Waffengleichheit).[68] Allerdings bedeutet er nicht, dass im Strafverfahren die Handlungsmöglichkeiten von StA und Verteidigung in jeder Beziehung ausgeglichen werden müssten.[69] Da im Strafverfahren die Stellung der Strafverfolgungsbehörde derjenigen des Beschuldigten oder Angeklagten wesentlich überlegen ist, muss aber einerseits dem Beschuldigten und seinem Verteidiger im Ermittlungsverfahren die Möglichkeit gewährleistet werden, eine Beschwerde gegen die Rechtmäßigkeit der Datenerhebung und -verwendung der Ermittlungsbehörden an das Gericht zu richten, und andererseits dem Angeklagten und seinem Verteidiger in der Hauptverhandlung die Möglichkeit gegeben werden, die vorgebrachten Belastungsbeweise angemessen zu überprüfen und zu kritisieren.[70] So müssen zur Verfahrensgestaltung, die eine zuverlässige Wahrheitserforschung gewährleistet, der Beschuldigte und sein Verteidiger am Ermittlungsverfahren und der Angeklagte und sein Verteidiger an der Hauptverhandlung teilnehmen dürfen.

Das Gebot des fairen Verfahrens und die darauf basierende Idee der Waffengleichheit scheinen aber heute zumindest im Ermittlungsverfahren ernsthaft in Gefahr zu geraten. Im heutigen Strafverfahren, in dem die Untersuchungsergebnisse nahezu uneingeschränkt in die Hauptverhandlung überführt werden, handelt es sich beim Ermittlungsverfahren nicht mehr um das lediglich ihr vorangehende, sie vorbereitende Verfahren. Vielmehr ist es inzwischen in vielen Fällen zum Kernstück des Strafprozesses geworden,[71] hingegen wurde dann die gerichtliche Hauptverhandlung

jeweils zuständigen Gerichte ist (*Hofmann*, in: Schmidt-Bleibtreu/Hofmann/Henneke, K zum GG, Art. 2 Rn. 47).

[66] *Roxin/Schünemann*, § 11 Rn. 9 f.

[67] *BVerfGE* 122, 248, 272; 133, 168, 200; M-G/*Schmitt*, StPO, Einl. Rn. 19.

[68] *Grzeszick*, in: Maunz/Dürig, GG-K, Art. 20 VII Rn. 144; M-G/*Schmitt*, StPO, Einl. Rn. 88; *Roxin/Schünemann*, § 11 Rn. 7: Das wird besser durch die Idee der Verfahrensbalance ausgedrückt.

[69] *BVerfGE* 122, 248, 272; 133, 168, 200; dazu 109, 279, 368 f. [Rn. 311]; vgl. *Roxin/Schünemann*, § 11 Rn. 7: Eine wirkliche Waffengleichheit wäre weder mit deutscher Verfahrensstruktur zu vereinbaren noch auch in einem reinen Parteiprozess durchführbar.

[70] *Roxin/Schünemann*, § 11 Rn. 7; dazu *BVerfGE* 133, 168, 200 [Rn. 59]: Das Recht auf ein faires Verfahren gewährleistet dem Beschuldigten, prozessuale Rechte und Möglichkeiten mit der erforderlichen Sachkunde wahrnehmen und Übergriffe der staatlichen Stellen oder anderer Verfahrensbeteiligter angemessen abwehren zu können.

[71] *Roxin/Schünemann*, § 39 Rn. 1: Der Ausgang einer Hauptverhandlung ist oft durch die Ermittlungsergebnisse des Vorverfahrens vorgezeichnet.

zu einer Formalität degradiert.[72] In dieser Hinsicht sollte über eine richterliche Intervention im Ermittlungsverfahren (Richtervorbehalt) hinaus dem Beschuldigten die Möglichkeit gegeben werden, zur Wahrung seiner Rechte auf den Gang und das Ergebnis des Ermittlungsverfahrens – auch nur teilweise – einen Einfluss zu nehmen, nämlich die Möglichkeit einer geordneten und effektiven Verteidigung.[73]

(2) Aufgabe des Strafprozesses ist es, den Strafanspruch des Staates um des Schutzes der Rechtsgüter Einzelner und der Allgemeinheit willen in einem justizförmigen Verfahren durchzusetzen und zugleich dem Beschuldigten bzw. Angeklagten eine wirksame Sicherung seiner Grundrechte zu gewährleisten.[74] Eine rechtsstaatliche Strafrechtspflege fordert, dass die beiden gegensätzlichen, aber gleichrangig gestellten Werte abgewogen werden.[75] Deswegen sind diese Forderungen im staatlichen Strafverfahren angemessen auszugleichen und das Strafprozessrecht ist eine Richtlinie dafür.[76] In diesem Sinne bezieht sich das prozessordnungsgemäße Strafverfahren auf ein Verfahren, bei dem die im Rechtsstaat verfassungsrechtlich geschützten Interessen angemessen berücksichtigt und ausbalanciert werden; es ist ein Wert an sich und schafft „Gerechtigkeit durch Verfahren", nämlich „prozedurale Gerechtigkeit".[77] Nur durch prozessuale Gerechtigkeit darf materielle Gerechtigkeit umgesetzt werden.[78] So kennzeichnen die Grenzen und Beschränkungen der staatlichen Eingriffsbefugnis die Justizförmigkeit des Strafverfahrens,[79] die den Schutz der Grundrechte im Verfahren bezweckt. Nach alledem sind die Regeln in der StPO nicht Formalismus, sondern ein Schutzmechanismus für die Interessen, die ein Rechtsstaat wahren muss (Institutsgarantie der Justizförmigkeit).[80]

Die Pflicht, nach dem Grundsatz des fairen Verfahrens im Einzelnen das Strafverfahrensrecht auszugestalten, ist in erster Linie dem Gesetzgeber aufgelegt[81], und

[72] Vgl. *Roxin*/*Schünemann*, § 69 Rn. 1: der Funktionsverlust der Hauptverhandlung.

[73] *Grzeszick*, in: Maunz/Dürig, GG-K, Art. 20 VII Rn. 144.

[74] *BVerfGE* 133, 168, 199 [Rn. 56]; Aufgaben und Ziel des Strafverfahrensrechts sind Abwägung zwischen materieller Richtigkeit, der Justizförmigkeit des Verfahrens und der Strafbarkeit (*Roxin*/*Schünemann*, § 1 Rn. 2 f.; *Volk*/*Engländer*, § 3 Rn. 5).

[75] *Roxin*/*Schünemann*, § 1 Rn. 7. Daher verhindert die Verfahrensförmlichkeit – mit dem Verhältnismäßigkeitsgrundsatz – eine Strafverfolgung um jeden Preis (*Dauster*, StraFo 1999, 186), im rechtsstaatlichen Strafverfahren ist aber ihre Wahrung nicht weniger wichtig als die Verurteilung Schuldiger und die Wiederherstellung des Rechtsfriedens (*Roxin*/*Schünemann*, § 1 Rn. 2).

[76] Vgl. *Roxin*/*Schünemann*, § 1 Rn. 6 ff.; auch *Volk*/*Engländer*, § 3 Rn. 5.

[77] *Volk*/*Engländer*, § 3 Rn. 5; vgl. *Roxin*/*Schünemann,* § 11 Rn. 5: Der Grundsatz des *fair trial* meint die Verfahrensgerechtigkeit.

[78] Im Ergebnis ist die Einhaltung der Vorschriften in der StPO, die „zu schützende Formen" darstellen, notwendige, aber auch ausreichende Bedingung für staatliches Strafen (*Hamm*, StV 2001, 81, 82).

[79] *Roxin*/*Schünemann*, § 1 Rn. 2.

[80] *Volk*/*Engländer*, § 3 Rn. 5.

[81] *BVerfGE* 133, 168, 200 [Rn. 59].

dieser stellt abstrakt das Spannungsverhältnis zwischen gegensätzlichen öffentlichen und privaten Interessen ein. Dieses rechtlich ausgestaltete und so justizförmige Strafverfahren wird aber in der Praxis manchmal oder teilweise vernachlässigt. Die Möglichkeit einer heimlichen bzw. umfassenden Erfassung der persönlichkeitsrelevanten Informationen infolge der Entwicklung der IT sowie die quantitative und qualitative Zunahme der organisierten und wirtschaftlichen Kriminalität sind entscheidende Ursachen für die Schwächung der normativen Wirkung der StPO und gefährden die Justizförmigkeit des Strafverfahrens. Daneben wollen die Ermittlungsbehörden, die als Vertreter des öffentlichen Interesses die Aufgabe wahrnehmen, die Wahrheit zu erforschen und Unrechtmäßigkeiten zu bestrafen, tendenziell die Grundrechte bzw. die prozessualen Rechte des Beschuldigten dem öffentlichen Interesse hintanstellen. So hängt die Ausgestaltung des Strafprozesses oft weniger von den Normen als vielmehr von der Wirklichkeit ab.[82] Es sollte versucht werden, diese Diskrepanz zwischen Norm und Realität zu schließen.

III. Normenbestimmtheit und -klarheit sowie Verhältnismäßigkeit

1. Gebot der Normenbestimmtheit und -klarheit[83]

a) Bedeutung

In einem Rechtsstaat sollen staatliche Hoheitsakte einerseits so klar und bestimmt und andererseits so beständig sein, dass sich der Bürger auf sie hinreichend verlassen kann.[84] Diese Anforderungen der Rechtssicherheit beziehen sich auf die Verlässlichkeit der Rechtsordnung, so soll bei der Gestaltung des Rechts das Vertrauen des Bürgers in die Vorgaben des Rechts in Rechnung gestellt werden.[85] Normen müssen daher inhaltlich hinreichend so klar und verständlich und so bestimmt formuliert sein, dass die Voraussetzungen und Folgen der Regelung für den Bürger als

[82] Vgl. *Roxin/Schünemann*, § 2 Rn. 7: In allen Fällen hängt die Ausgestaltung des Strafprozesses weniger von den Verfassungsnormen als vielmehr von der Verfassungswirklichkeit ab.

[83] Die „Klarheit" bezieht sich auf die inhaltlichen Aspekte des Rechts, während sich die „Bestimmtheit" auf die expressiven Aspekte des Rechts bezieht. Die beiden Angebote sind aber nicht eindeutig zu unterscheiden, sie zielen darauf ab, dass dem Bürger die Möglichkeit gegeben wird, sein Verhalten auf die Rechtsnormen einzustellen (*Grzeszick*, in: Maunz/Dürig, GG-K, Art. 20 VII Rn. 58). In der Rspr. wird durchgängig die Formulierung „Bestimmtheit und Klarheit der Norm" verwendet (z. B. *BVerfGE* 110, 33, 54; 113, 348, 376; 120, 274, 315 f.; 120, 378, 407 f. m. w. N.).

[84] *Grzeszick*, in: Maunz/Dürig, GG-K, Art. 20 VII Rn. 50. Es gehört zu den grundlegenden Aufgaben des Rechts, eine verlässliche Verhaltensordnung zu schaffen (*Huster/Rux*, in: Epping/Hillgruber, BeckOK GG, Art. 20 Rn. 181).

[85] *Grzeszick*, in: Maunz/Dürig, GG-K, Art. 20 VII Rn. 50; *Huster/Rux*, in: Epping/Hillgruber, BeckOK GG, Art. 20 Rn. 181.

Normadressat vorhersehbar sind.[86] Durch die Regelung soll der betroffene Bürger sich auf mögliche belastende Maßnahmen einstellen (Vorhersehbarkeit), die gesetzesausführende Verwaltung für ihr Verhalten steuernde und begrenzende Handlungsmaßstäbe vorfinden (wirksame Begrenzung) und sollen die Gerichte gegenüber der Verwaltung eine wirksame Rechtskontrolle durchführen können (Justitiabilität).[87] Die Bestimmbarkeit durch Rechtsbegriffe ist aber wegen der möglichen Vielgestaltigkeit der zu regelnden Sachverhalte zu beschränken. Wenn die zu erfassenden Einzelfälle sehr weitverbreitet sind oder wenn atypische Einzelfälle auch erfasst werden müssen, darf der Gesetzgeber bei der Gestaltung der Eingriffsvoraussetzungen einerseits abstrakte bzw. unbestimmte Rechtsbegriffe anwenden und andererseits dem Rechtsanwender einen Ermessensspielraum zur Gestattung und Bestätigung der Eingriffe einräumen.[88] Daher ist die Verwendung von unbestimmten Rechtsbegriffen,[89] Generalklauseln[90] und Ermessensermächtigungen[91] nicht untersagt.[92] Solange sich derartige Begriffe und Klauseln durch eine Auslegung der betreffenden Normen in juristischer Methodik hinreichend konkretisieren lassen und die im konkreten Anwendungsfall verbleibenden Ungewissheiten nicht so weit gehen, dass Vorhersehbarkeit und Justitiabilität des Verwaltungshandelns gefährdet sind, dann steht die Auslegungsbedürftigkeit als solche dem Bestimmtheitserfordernis nicht entgegen.[93]

Das Maß an gebotener Bestimmtheit und Klarheit der Norm hängt von der Grundrechtsrelevanz der jeweiligen Vorschrift (nach der Art und der Intensität des Eingriffs) und der Eigenschaft des jeweiligen Regelungsbereiches ab.[94] Je bedeutsamer die Norm ist, insbesondere je intensiver die damit verbundene Freiheitseinschränkung ist, und je eindeutiger, abgrenzbarer und vorhersehbarer der Regelungsgegenstand ist, desto höher ist das Maß der gebotenen Bestimmtheit der Norm.[95] Ist dagegen die Norm von geringer Bedeutung und ist der Regelungsgegenstand vielgestaltig, unübersichtlich und raschen Änderungen unterworfen, ist das

[86] *Grzeszick*, in: Maunz/Dürig, GG-K, Art. 20 VII Rn. 53 und 58.

[87] *BVerfGE* 110, 33, 53; 113, 348, 375 ff.; 124, 43, 60; 133, 277, 336; 141, 220, 265.

[88] *Grzeszick*, in: Maunz/Dürig, GG-K, Art. 20 VII Rn. 65.

[89] *BVerfGE* 31, 255, 264; 83, 130, 145; 110, 33, 56 f. m. w. N.

[90] *BVerfGE* 8, 274, 326; 13, 153, 161; 56, 1, 12.

[91] *BVerfGE* 8, 274, 326; 48, 210, 222; 110, 33, 54.

[92] *Huster/Rux*, in: Epping/Hillgruber, BeckOK GG, Art. 20 Rn. 182; vgl. *Grzeszick*, in: Maunz/Dürig, GG-K, Art. 20 VII Rn. 61 ff.

[93] *BVerfGE* 21, 73, 79 f.; 110, 33, 56 f. [Rn. 115]; 118, 168, 188 [Rn. 100]; 120, 274, 316 [Rn. 210]. Dabei kann die Konkretisierung durch die lange und ständige Rechtsprechung erreicht werden (*BVerfGE* 76, 1, 74; *Grzeszick*, in: Maunz/Dürig, GG-K, Art. 20 VII Rn. 62).

[94] *BVerfGE* 110, 33, 55; *Huster/Rux*, in: Epping/Hillgruber, BeckOK GG, Art. 20 Rn. 182.

[95] *Grzeszick*, in: Maunz/Dürig, GG-K, Art. 20 VII Rn. 60; vgl. *Huster/Rux*, in: Epping/Hillgruber, BeckOK GG, Art. 20 Rn. 182.1: Für den grundrechtlich besonders sensiblen Bereich des Strafrechts liegen verschärfte Anforderungen an die Normbestimmtheit, insb. das Verbot von einer strafbegründenden analogen Auslegung des Strafgesetzes vor (Art. 103 Abs. 2 GG).

Maß der gebotenen Bestimmtheit nicht hoch.[96] Im Bereich des in die Freiheit des Bürgers (besonders) intensiv eingreifenden Staatshandelns wie des Strafverfahrens ist die rechtsstaatliche Bestimmtheit (besonders) streng. Insb. bezüglich der Befugnisse zur heimlichen Datenerhebung und -verarbeitung, die tief in die Privatsphäre hineinwirken können, wie etwa TKÜ, Wohnraumüberwachungen und Online-Durchsuchungen, kann ihr Gehalt nur sehr eingeschränkt im Wechselspiel von Anwendungspraxis und gerichtlicher Kontrolle konkretisiert werden.[97] Je ungenauer die Ziele eines Eingriffs und die tatsächlichen Voraussetzungen einer Maßnahme gesetzlich umschrieben sind, umso größer ist außerdem das Risiko unangemessener Maßnahmen im Einzelfall.[98] So kann bei den nicht hinreichend bestimmten Ermächtigungsnormen die Beurteilung der Abwägung bereits unausgewogen sein. Das heißt, Unklarheiten über die Ziele und die Voraussetzungen der Maßnahmen bergen das Risiko in sich, dass die rechtsstaatliche Begrenzungsfunktion des Abwägungsgebots verfehlt wird.[99] In diesem Sinne ist das Bestimmtheits- und Klarheitsgebot mit den jeweiligen materiellen Anforderungen der Verhältnismäßigkeit, insb. der Abwägung, eng verbunden (vgl. unten 2.).[100]

b) Zweckbindung und Verbot der Zweckänderung bzw. -entfremdung

Der Zweck von Erhebung, Verarbeitung, Verwendung und Speicherung personenbezogener Daten muss nach dem Gebot der Bestimmtheit und Klarheit der Norm bereichsspezifisch und präzise bestimmt werden.[101] Die Verarbeitung, Verwendung und Speicherung personenbezogener Daten sind grundsätzlich an den Zweck und an das Verfahren gebunden, für die sie erhoben wurden.[102] Bei der Ausgestaltung der Ermächtigungsgrundlage für solche Maßnahmen ist daher das Gebot der Bestimmtheit und Klarheit durch den „Grundsatz der Zweckbindung" und das „Verbot der Zweckänderung" geprägt.[103] Demzufolge steht die Durchsuchung und Beschlagnahme im „Strafverfahren" unter einer strengen Begrenzung auf den „Ermittlungszweck", wobei die Ermittlungen inhaltlich auf die „Erforschung des – für

[96] *Grzeszick*, in: Maunz/Dürig, GG-K, Art. 20 VII Rn. 60. Dies gilt für den Gesetzesvorbehalt.

[97] *BVerfGE* 141, 220, 265 [Rn. 94] und 269 [Rn. 105].

[98] *BVerfGE* 110, 33, 55 [Rn. 111]; 113, 348, 385 [Rn. 148].

[99] *BVerfGE* 113, 348, 385 f. [Rn. 148].

[100] Vgl. *BVerfGE* 141, 220, 265 [Rn. 94] und 269 [Rn. 105]; 113, 348, 376; auch 110, 33, 55 [Rn. 112].

[101] *BVerfGE* 65, 1, 46 [Rn. 161 f.]; 113, 29, 51 [Rn. 103]; 115, 320, 365 [Rn. 150].

[102] *BVerfGE* 100, 313, 360 [Rn. 166]; 109, 279, 375 [Rn. 333]; 130, 1, 33 [Rn. 133].

[103] Vgl. *BVerfGE* 65, 1, 62 [Rn. 203]; 100, 313, 360 [Rn. 166]; 109, 279, 375 [Rn. 333]; 130, 1, 33 f. [Rn. 133]; 133, 277, 372 f. [Rn. 225]; 141, 220, 324 ff. [Rn. 276 und 284].

bestimmte Personen – strafrechtlich relevanten Sachverhalts“ beschränkt werden (vgl. §§ 155 Abs. 1, 161 Abs. 1 S. 1 und 163 Abs. 1 S. 2 StPO).[104]

Zum anderen kann der Gesetzgeber eine weitere Nutzung und eine Übermittlung von Daten vorsehen, indem er hierfür eine eigene, formell und materiell verfassungsgemäße Rechtsgrundlage schafft.[105] Bei weiterer Nutzung der Daten zu anderem Zweck als den der ursprünglichen Datenerhebung (Zweckänderung bzw. -entfremdung) muss dem Eingriffsgewicht der neuen Datenerhebung[106] Rechnung getragen werden.[107] Für die Daten aus eingriffsintensiven Maßnahmen kommt es folglich darauf an, ob die Daten nach verfassungsrechtlichen Kriterien neu auch für den geänderten Zweck mit vergleichbar schwerwiegenden Mitteln erfasst werden dürften.[108] In dieser Hinsicht können die Daten, die durch besonders eingriffsintensive Maßnahmen wie z. B. TKÜ, Wohnraumüberwachung und Online-Durchsuchung erlangt wurden, nur zu entsprechenden gewichtigen Zwecken benutzt werden.[109] Zur Sicherung der Zweckbindung muss daneben eine gesetzliche Verpflichtung zur Kennzeichnung und Protokollierung bestehen.[110]

2. Grundsatz der Verhältnismäßigkeit

a) Bedeutung und Prüfungsstruktur

Der Grundsatz der Verhältnismäßigkeit wird im GG nicht ausdrücklich erwähnt.[111] Nach der ständigen Rechtsprechung des *BVerfG* ist er aber aus dem Rechtsstaatsprinzip und den Freiheitsrechten abzuleiten[112] und hat Verfassungs-

---

[104] *BVerfGE* 113, 29, 51 f. [Rn. 103 – 105]; 115, 166, 191 [Rn. 94 f.]; 124, 43, 61 [Rn. 64]; *Park*, § 1 Rn. 18; *Peters*, NZWiSt 2017, 465, 467 [Tz. b)].

[105] *BVerfGE* 109, 279, 375 f.; 125, 260, 333 [Rn. 236]; 130, 1, 33 [Rn. 133]; 141, 220, 324 [Rn. 277].

[106] Die Ermächtigung für die Datennutzung zu neuen Zwecken begründet einen neuen eigenständigen Eingriff (*BVerfGE* 109, 279, 375 [Rn. 333]; 133, 277, 372 f. [Rn. 225]; 141, 220, 327 [Rn. 285]).

[107] *BVerfGE* 141, 220, 326 f. [Rn. 284].

[108] *BVerfGE* 141, 220, 327 f. [Rn. 287]; vgl. auch 133, 277, 373 f. [Rn. 225 f.]; „hypothetischer Ersatzeingriff“ in 130, 1, 34 [Rn. 133]. In der früheren Rspr. des *BVerfG* wurde insoweit darauf abgestellt, ob die geänderte Nutzung mit der ursprünglichen Zwecksetzung unvereinbar sei (141, 220, 327 [Rn. 287]; vgl. 109, 279 376 [Rn. 334]; 125, 260, 333 [Rn. 236]; 130, 1, 33 [Rn. 133]).

[109] *BVerfGE* 109, 279, 377 [Rn. 338 ff.]; 133, 277, 372 f. [Rn. 225]; 141, 220, 327 [Rn. 286].

[110] *BVerfGE* 109, 279, 379 f. [Rn. 346 f.]; 125, 260, 333 [Rn. 236]; 130, 1, 34 [Rn. 133].

[111] *Huster/Rux*, in: Epping/Hillgruber, BeckOK GG, Art. 20 Rn. 189; vgl. *Grzeszick*, in: Maunz/Dürig, GG-K, Art. 20 VII Rn. 108.

[112] Vgl. *BVerfGE* 19, 342, 348 f. [Rn. 17]; 23, 127, 133 [Rn. 19]; 30, 1, 20 f. [Rn. 92]; 90, 145, 173 [Rn. 125] m. w. N.; *Huster/Rux*, in: Epping/Hillgruber, BeckOK GG, Art. 20 Rn. 190.

rang.[113] Dieser Grundsatz hat derzeit als die entscheidende materielle Vorgabe des Rechtsstaatsprinzips an Bedeutung gewonnen[114] und steht damit im Zentrum der Prüfung des Grundrechtseingriffs.[115] Er folgt aus dem Grundgedanken, dass der Staat den einzelnen Bürger in seiner Freiheitssphäre nur so weit beschränken darf, wie dies in gemeinem Interesse erforderlich ist,[116] und er wird in allen Fällen angewendet, wenn auf eine geschützte Rechtsposition des Grundrechtsträgers nachteilig eingewirkt wird.[117] In dieser Hinsicht zielt der Grundsatz der Verhältnismäßigkeit im Strafverfahren auf den Schutz der Grundrechte durch die Beschränkung eines unverhältnismäßigen Eingriffs der Strafverfolgungsorgane ab. Im Rahmen von schweren Grundrechtseingriffen wie Durchsuchung und Beschlagnahme ist der Verhältnismäßigkeitsgrundsatz nicht nur bei Beantragung bzw. bei Erlass des richterlichen Beschlusses, sondern auch bei seinem Vollzug zu berücksichtigen.[118]

Nach der Rechtsprechung des *BVerfG* und h. M. in der Literatur setzt sich die Verhältnismäßigkeitsprüfung aus vier Anforderungen zusammen: Einzelne Ermächtigungen und Maßnahmen müssen zur Erreichung eines legitimen Zwecks geeignet, erforderlich und angemessen, nämlich nicht übermäßig oder verhältnismäßig i. e. S., sein.[119] Bei der Beurteilung, ob eine Ermächtigungsnorm für strafprozessuale Zwangsmaßnahmen und ihre konkrete Durchführung im Einzelfall verfassungsrechtlich gerechtfertigt werden kann, kommt es i. d. R. kaum auf den legitimen Zweck und die Geeignetheit und Erforderlichkeit des Mittels an. Denn dabei ist der Zweck der Eingriffsmaßnahme bereits klar vorausgesetzt, und dem Befugten zu ihrer Anordnung bzw. Durchführung ist der Gestaltungs- und Beurteilungsspielraum für geeignete und erforderliche Maßnahmen breit eingeräumt. Bei der Überprüfung der Verhältnismäßigkeit spielt im Ergebnis die Angemessenheit (Übermaßverbot oder Verhältnismäßigkeit i. e. S.) die wichtigste Rolle. Hieraus leitet

[113] *BVerfGE* 19, 342, 348 [Rn. 17]; 23, 127, 133 [Rn. 19]; 30, 1, 21 [Rn. 94]: Verfassungsgrundsatz; NJW 1986, 767, 769 m. w. N.; *Fischer*, KK-StPO, Einl. Rn. 161; M-G/*Schmitt*, StPO, Einl. Rn. 20.

[114] *Grzeszick*, in: Maunz/Dürig, GG-K, Art. 20 VII Rn. 107.

[115] Vgl. *Huster/Rux*, in: Epping/Hillgruber, BeckOK GG, Art. 20 Rn. 189: die zentrale Figur der grundrechtlichen Eingriffsdogmatik.

[116] Vgl. *Roxin/Schünemann*, § 2 Rn. 7: Begrenzung der Eingriffsbefugnisse auf das nach den konkreten Umständen unumgängliche Ausmaß.

[117] *Grzeszick*, in: Maunz/Dürig, GG-K, Art. 20 VII Rn. 108. Dem staatlichen Handeln werden somit durch den Grundsatz der Verhältnismäßigkeit Grenzen gesetzt (*BVerfGE* 113, 29, 53). Vgl. *BGHSt* 51, 211, 219 [Rn. 22]: „*Der Grundsatz der Verhältnismäßigkeit begrenzt im Einzelfall gesetzliche Befugnisse, eine fehlende Ermächtigungsgrundlage kann er nicht ersetzen.*“

[118] Vgl. *Park*, § 2 Rn. 84. Es wird jedoch häufig kritisiert, dass der Grundsatz bei der Durchsuchung und Beschlagnahme in der Praxis nicht ausreichend berücksichtigt wird (a. a. O. § 2 Rn. 84 f., § 3 Rn. 486 f.).

[119] *BVerfGE* 30, 292, 316; 65, 1, 54; 115, 166, 192; 120, 274, 318 f.; 124, 43, 61 f.; 125, 260, 316; 141, 220, 265 m. w. N.; *Grzeszick*, in: Maunz/Dürig, GG-K, Art. 20 VII Rn. 110: dogmatische Struktur.

das *BVerfG* bei der verfahrensrechtlichen Ausgestaltung von Ermittlungs- und Überwachungsbefugnissen fast immer übergreifende Anforderungen ab.[120]

b) Verhältnismäßigkeit im engeren Sinne: Gesamtabwägung

Die Verhältnismäßigkeit i. e. S. verlangt, dass staatliche Grundrechtsbeschränkung nicht in unangemessenem Verhältnis zu ihrem Zweck steht (Übermaßverbot). Dieser Prüfungsmaßstab setzt eine Gesamtabwägung zwischen der Schwere des Grundrechtseingriffs einerseits und dem Gewicht der ihn rechtfertigenden Gründe (der zu schützenden Rechtsgüter) andererseits voraus.[121] Je intensiver der Grundrechtseingriff ist, desto gewichtiger muss der Zweck des Eingriffs als Gemeinwohlinteresse sein und desto strenger müssen die Voraussetzungen des Eingriffs sein.[122] Da das Maß an rechtsstaatlich gebotener Bestimmtheit und Klarheit der Norm und die Strenge der verfahrensrechtlichen Vorkehrungen auch von der Eingriffsintensität einzelner Maßnahmen abhängt, wirkt sich die Abwägung auch auf die Normenbestimmtheit und -klarheit und die detaillierte Ausgestaltung der Verfahrensgarantien aus (vgl. oben 1. a)).

Die Aufgabe, in dem Spannungsverhältnis zwischen den widerstreitenden Interessen des Einzelnen an den Grundrechtsschutz durch die Abwägung einen Ausgleich zu erreichen, kommt dem Staat zu. Zunächst ist es Aufgabe des Gesetzgebers, durch die Ausgestaltung der Ermächtigungsnorm abstrakt die Interessen auszubalancieren.[123] Die Aufgabe, aufgrund dieser Norm im Einzelfall eine angemessene Balance herzustellen, obliegt der Strafverfolgungsbehörde, die die Maßnahme konkret durchführt, und dem Richter, der sie vorab und nachträglich kontrolliert und einschränkt.[124] Das *BVerfG* überprüft die abstrakte Rechtsnorm und konkrete Maßnahme auf ihre Verfassungsmäßigkeit.[125] Weil in dem liberal-demokratischen Verfassungssystem die Wertungen der Abwägung grundsätzlich von der – objektivierbaren – demokratischen Mehrheit entschieden werden,[126] gilt das Gesetz, das

---

[120] *BVerfGE* 141, 220, 268 [Rn. 103].

[121] *BVerfGE* 113, 29, 54 [Rn. 110]; 115, 320, 345 [Rn. 88]; 120, 274, 321 f. [Rn. 227]; auch 109, 279, 359 [Rn. 275]: „eine umfassende Abwägung".

[122] *Huster/Rux*, in: Epping/Hillgruber, BeckOK GG, Art. 20 Rn. 197.

[123] *BVerfGE* 109, 279, 350 [Rn. 243]; 115, 320, 346 [Rn. 88]; 120, 274, 322 [Rn. 227] und 326 [Rn. 243]; 141, 220, 267 [Rn. 98]; auch 124, 43, 62 [Rn. 66]. Allerdings darf dabei die Balance zwischen Freiheit und Sicherheit vom Gesetzgeber neu justiert, die Gewichte dürfen jedoch von ihm nicht grundlegend verschoben werden (*BVerfGE* 115, 320, 360 [Rn. 135]).

[124] Vgl. *BVerfGE* 109, 279, 350 [Rn. 243]; 139, 245, 279 [Rn. 93]: Der Richtervorbehalt dient der Sicherstellung der Interessenabwägung.

[125] Vgl. Art. 93 Abs. 1 GG. Insoweit wird es mit Recht kritisiert, dass die Prüfung der Verhältnismäßigkeit i. e. S. in unangemessener Weise vom Gesetzgeber zum *BVerfG* verschoben wird (*Huster/Rux*, in: Epping/Hillgruber, BeckOK GG, Art. 20 Rn. 197.1).

[126] *Grzeszick*, in: Maunz/Dürig, GG-K, Art. 20 VII Rn. 118 f. Die Gewichtung der bei der Abwägung im Einzelnen in Betracht kommenden Aspekte und hiernach die Grenzziehung der

sich aus der Ausübung der Gesetzgebungsbefugnis ergibt, grundsätzlich als nicht übermäßig. Im Ergebnis nimmt das *BVerfG* einen Verstoß gegen das Gebot der Verhältnismäßigkeit i. e. S. nur bei deutlicher Unangemessenheit an.[127]

Die Verfassungsmäßigkeit der Ermächtigungsgrundlagen zu Grundrechtseingriffen zum Zwecke der Strafverfolgung hängt grundlegend vom Gebot der Abwägung ab, die schon längst ein wesentliches Mittel für die Argumentation des *BVerfG* darstellt.[128] Diesbezüglich ist zum einen im Allgemeininteresse das Gewicht der zu schützenden Rechtsgüter und die Wahrscheinlichkeit des Eintritts einer Rechtsgutverletzung zu berücksichtigen.[129] Sie sind dabei in grundlegende wesentliche Rechtsgüter wie die Sicherheit des Staates und der Bevölkerung (z. B. die verfassungsmäßige Ordnung, den Bestand und die Sicherheit des Bundes und der Länder sowie Leib, Leben und Freiheit der Person) und sonstige andere Rechtsgüter zu unterteilen.[130] Die Wahrscheinlichkeit der Rechtsgutbeeinträchtigung wird nach dem Grad des Tatverdachts bestimmt. Zum anderen ist im Individualinteresse die Bedeutung des verletzten Grundrechts und das Gewicht des Grundrechtseingriffs in Rechnung zu setzen.[131] Beim staatlichen Eingriff in personenbezogene Daten hängt das Gewicht insb. von der Art und Weise der Maßnahmen und der Intensität der Persönlichkeitsverletzung ab. Diese begriffliche bzw. abgestufte Differenzierung und die dadurch diskriminierende Behandlung stehen in Einklang mit dem Ziel des Grundsatzes der Verhältnismäßigkeit, das einen Grundrechtsschutz durch die Beschränkung der Staatsgewalt darstellt. Die Ermächtigungsnormen in der StPO sind derzeit in eine gleitende Skala, d. h. auf solche Weise, ausgestaltet, dass das Gewicht

Maßnahme beruhen auf subjektiven Wertungen, und zwar postuliert das *BVerfG* seine subjektiven Wertungen als verfassungsrechtlich verbindlich (a. a. O. 118).

[127] *Grzeszick*, in: Maunz/Dürig, GG-K, Art. 20 VII Rn. 120. In dieser Hinsicht handelt es sich bei der Prüfung des *BVerfG* nicht darum, ob die vom Gesetzgeber gewählte Lösung die gerechteste Lösung ist, sondern darum, ob sie nicht evident unangemessen ist (*Huster/Rux*, in: Epping/Hillgruber, BeckOK GG, Art. 20 Rn. 197.1).

[128] Vgl. *BVerfGE* 67, 157, 178 ff.: § 3 G 10 1968 a. F. (strategische Post- und Telefonkontrolle durch BND); 100, 313, 375 ff.: § 3 G 10 1994 a. F. (strategische Fernüberwachung durch BND); 107, 299, 318 ff.: §§ 100a und b StPO 1989 a. F. u. § 12 FAG (Auskunft über Telefonverbindungsdaten an Strafverfolgungsbehörden); 109, 279, 349 ff.: §§ 100c, d und e StPO 1998 a. F. (Großer Lauschangriff); 110, 33, 74 f.: § 39 – 41 AWG 2002 a. F. (Brief- und Telefonüberwachung durch Zollkriminalamt); 113, 29, 53 ff.: §§ 94 ff. und 102 ff. StPO (Beschlagnahme von Datenträgern); 113, 348, 382 ff.: § 33a Abs. 1 Nrn. 2 und 3 Nds. SOG 1994 (vorbeugende TKÜ durch Polizei); 115, 166, 192 ff.: §§ 94 ff. und 102 ff. StPO (Beschlagnahme von E-Mails); 115, 320, 345 ff.: § 31 NWPolG 1990 a. F. (präventive polizeiliche Rasterfahndung); 120, 274, 302 ff.: § 5 Abs. 2 Nr. 11 NWVerfSchG (Online-Durchsuchung); 124, 43, 61 ff.: §§ 94 ff. und 102 ff. StPO (Beschlagnahme von E-Mails); 125, 260, 318 ff.: § 100g StPO 2008 a. F. (Vorratsdatenspeicherung); 129, 208, 255 ff.: TKÜG-Neuregelung; 133, 277, 322 ff.: § 2 S. 1 ATDG; 141, 220, 267 ff.: §§ 20g, h und k BKAG 2009 a. F. (verschiedene heimliche Überwachungsmaßnahmen).

[129] *BVerfGE* 100, 313, 376 [Rn. 219]; 113, 348, 382 [Rn. 136]; 124, 43, 62 [Rn. 67].

[130] Vgl. *BVerfGE* 115, 320, 346 [Rn. 91]; 141, 220, 270 f. [Rn. 108].

[131] *BVerfGE* 113, 348, 382 f.; 115, 166, 194 [Rn. 105 f.]; 115, 320, 347 [Rn. 95]; 120, 274, 322 ff.; 124, 43, 62 [Rn. 67 f.]; 141, 220, 267 [Rn. 99] m. w. N.

des Vorwurfs und die Stärke des Verdachts gegen das Gewicht des Grundrechtseingriffs abgewogen werden.[132] Bei dieser Abwägungsprüfung sollte die gesetzgeberische Bemessung der Eingriffsintensität der Maßnahme aufseiten der Individualinteressen stets zuerst erfolgen.[133] Erst nach der Festlegung dieser Eingriffsintensität sind die Aspekte der öffentlichen Interessen verhältnismäßig und also abgestuft zu bestimmen.

c) Datenzugriff und Abwägung

Entscheidend ist die Abwägung auch bei der Bestimmung oder der gesetzlichen Ausgestaltung der Ermächtigungsnorm zur Erhebung oder Verwendung personenbezogener Daten. I. R. d. der Bewertung der Schwere des Eingriffs hat das *BVerfG* bisher in seiner Rspr. viele verschiedene Überlegungen vorgestellt: die Persönlichkeitsrelevanz, die Vielfältigkeit und den Umfang der erfassten Daten (ein Potential für die Ausforschung der Persönlichkeit), die Erwartungen an die Vertraulichkeit der Wohnung oder der TK, eine diffuse Furcht oder Bedrohlichkeit, die Heimlichkeit einer Eingriffsmaßnahme, die Nicht-Anonymität des Betroffenen, eine Unzahl unverdächtiger Grundrechtsträger (verdachtslose Grundrechtseingriffe mit großer Streubreite), die längerfristige bzw. laufende Erfassung, die Datenerhebung zu unbestimmten oder noch nicht bestimmbaren Zwecken, die Einwirkungsmöglichkeiten des Betroffenen auf seinen Datenbestand, die Entwicklung der IT etc.[134] Die letzte „Entwicklung der IT" ist der grundlegendste Hintergrund (vgl. unten aa)) und unter den daraus abgeleiteten untergeordneten Überlegungen sind die „Heimlichkeit einer Maßnahme" (vgl. unten bb)) und die „Möglichkeit der Persönlichkeitsausforschung durch einen umfassenden Datenzugriff" (vgl. unten cc)) am wichtigsten.[135] Die sonstigen Faktoren treten normalerweise begleitend oder unvermeidlich auf, wenn die Informationserfassung heimlich oder umfassend mithilfe der IT erfolgt.

---

[132] Vgl. *Roxin/Schünemann*, § 39 Rn. 16.

[133] Vgl. *BVerfGE* 107, 299, 318 ff. [Tz. (dd)]; 141, 220, 267 [Rn. 99]; insb. 109, 279, 345 [Rn. 229]: „*Nach der Einschätzung des verfassungsändernden Gesetzgebers stellt die akustische Wohnraumüberwachung im Spektrum der strafprozessualen Maßnahmen einen besonders schweren Grundrechtseingriff dar, der deshalb auch im Hinblick auf die Schwere der zu verfolgenden Straftat an besonders strenge Eingriffsvoraussetzungen gebunden worden ist.*" Das *BVerfG* verlangt 2009 in seiner Entscheidung zur Feststellung der Rechtsgrundlage der Sicherstellung und Beschlagnahme von E-Mails auf dem Mailserver des Providers in erster Linie, die Eingriffsintensität zum Auswahlkriterium der „richtigen" Ermächtigungsgrundlage zu bestimmen (*Zimmermann*, JA 5/2014, 321, 325; vgl. *BVerfGE* 124, 43, 62 [Rn. 67 f.]).

[134] Vgl. *BVerfGE* 113, 348, 382–385 [Rn. 137–144]; 115, 320, 347–357 [Rn. 93–124], 120, 274, 322–326 [Rn. 229–241]; 124, 43, 62–66 [Rn. 66–76]; 141, 220, 267 [Rn. 99] m. w. N.

[135] Vgl. *BVerfGE* 115, 320, 348 [Rn. 97 f.]: Die Eingriffsintensität ist hoch, wenn Informationen auf solche Weise erlangt werden, dass Vertraulichkeitserwartungen verletzt werden, wie etwa bei Eingriffen in das Grundrecht auf Unverletzlichkeit der Wohnung nach Art. 13 GG oder das Fernmeldegeheimnis nach Art. 10 GG, und wenn sie inhaltlich eine hohe Persönlichkeitsrelevanz haben.

aa) Informationstechnische Gegebenheiten – mitsamt einer Veränderung der Wahrnehmung der Realität des *BVerfG*

Bei der Bemessung der Intensität von Grundrechtseingriffen ist der aktuelle Stand der Informationstechnik von erheblicher Bedeutung. Das *BVerfG* berücksichtigt ihn auch in seinen Rechtsprechungen ziemlich klar.[136] Dies ist u. a. auch seinen Entscheidungen zur Schaffung des Rechts auf informationelle Selbstbestimmung im Jahr 1983 und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme im Jahr 2008 zu entnehmen (vgl. näher unten B. III.).

Das *BVerfG* hat im Jahre 1984 – kurz nach der Anerkennung des informationellen Selbstbestimmungsrechts – entschieden, dass die Voraussetzungen des § 2 G 10 1978 a. F.,[137] der zur Verhinderung, Aufklärung oder Verfolgung von Straftaten dient, aus damaligen technischen Gründen durch den Missbrauch des § 3 Abs. 2 S. 2 G 10 1968 a. F., der zulässig ist, dass die durch „strategische Überwachungsmaßnahmen" nach § 3 Abs. 1 G 10 1968 a. F. erlangten Kenntnisse ausnahmsweise zur Strafverfolgung bestimmter Personen – einschließlich der Nichtverdächtigen – verwendet werden, nicht zweckentfremdet werden können.[138] Hingegen hat es nur 10 Jahre später, im Jahre 1994, bei der Prüfung der Verfassungsmäßigkeit der strategischen Überwachungsmaßnahmen nach § 3 G 10 1994 a. F., deren Anwendungsbereich quantitativ durch den Art. 13 VerbrBekG[139] ausgeweitet worden war (die Hinzufügung der Nrn. 2 bis 6), vorausgesetzt, dass ihre Eingriffsintensität aufgrund der technischen Entwicklung erhöht wurde: Hierbei hat es begründet, bei der Intensität des Eingriffs in das Grundrecht des Art. 10 GG falle ins Gewicht, dass jeder Teilnehmer am internationalen Telekommunikationsverkehr – abgesehen von dem Telefonverkehr – ohne ein konkretes Fehlverhalten oder einen konkretisierten personenbezogenen Verdacht derartigen Überwachungsmaßnahmen ausgesetzt ist, dabei Kommunikationsbeiträge jeder Art inhaltlich in vollem Umfang erfasst werden und es weiter an Anonymität der Kommunikationsteilnehmer fehlt.[140] Daher sei diese Überwachung dann verhältnismäßig, wenn Identifizierungsmerkmale enthaltende Suchbegriffe als Vorkehrung zur technischen Begrenzung ihrer Reichweite eingesetzt werden (§ 3 Abs. 2 S. 2 G 10 1994 a. F.), es sei denn, dass die Gefahr einer im Ausland begangenen Geldfälschung vorliegt (§ 3 Abs. 1 Nr. 5 G 10 1994 a. F.).[141] Hierauf hat das

[136] *BVerfGE* 67, 157, 181 f.; 100, 313, 379 ff.; 107, 299, 318 ff.; 120, 274, 323 ff.; 125, 260, 318 ff.; 141, 220, 267 [Rn. 99] m. w. N.

[137] G 10 in der von 16. 9. 1978 geltenden Fassung (BGBl. I S. 1546).

[138] *BVerfGE* 67, 157, 181 [Rn. 72–73]. Da im Jahre 1978 die Wahrscheinlichkeit, von der strategischen Kontrolle getroffen zu werden, für den Einzelnen äußerst gering war und die von Maßnahmen Betroffenen in aller Regel anonym blieben, war die Intensität des Grundrechtseingriffs relativ geringfügig (a. a. O. 178 f. [Rn. 66 f.]; auch 100, 313, 378 [Rn. 226]).

[139] Verbrechensbekämpfungsgesetz vom 28. 10. 1994 (BGBl. I S. 3186).

[140] *BVerfGE* 100, 313, 380 f. [Rn. 231–234].

[141] *BVerfGE* 100, 313, 384 f. [Rn. 244 f.].

Gericht im Jahr 2005 im Verfahren über die Verfassungsbeschwerde gegen § 33a Abs. 1 Nrn. 2, 3 Nds. SOG 2003 a. F.[142] als gesetzliche Ermächtigungen zur Verhütung und zur Vorsorge für die Verfolgung von Straftaten durch Maßnahmen der TKÜ ausgeführt, dass die Vielzahl der i. R. d. modernen TK erfassbaren Daten zu einer besonderen Intensität der Eingriffe in das Fernmeldegeheimnis führt.[143] Schließlich hat das *BVerfG* im Jahre 2008 in der Prüfung der Zulässigkeit verdeckter Online-Durchsuchung erkannt, dass die Nutzung moderner Informationstechnik und informationstechnischer Systeme heute von anderer Bedeutung ist als in der Vergangenheit (vgl. unten B. III. 2.).

Hinsichtlich der Erhebung und Verwendung der Verkehrsdaten vertritt das *BVerfG* die gleiche Auffassung. Im Jahre 2003 hat es im Verfahren über die Verfassungsbeschwerde gegen richterliche Anordnungen zur Herausgabe von Verbindungsdaten der TK (= aktueller Verkehrsdaten) aufgrund des § 12 FAG a. F. festgestellt, dass sich die Bedeutung der Daten infolge der Entwicklung der Telekommunikationstechnik erheblich erhöht und konsequenterweise auch die Eingriffsintensität der Übermittlung, Erhebung und Verwendung der Daten stark zugenommen hat.[144] Bei Überprüfung der Verfassungsmäßigkeit der VDS von 2010, dass die in allen Arten von TK-Diensten praktisch sämtliche Verkehrsdaten aller Bürger sechsmonatig, vorsorglich anlasslos systematisch gespeichert und weiter übermittelt und verwendet werden, war es davon überzeugt, dass es sich bei einem solchen Eingriff um einen besonders schweren Eingriff mit einer Streubreite handelt, wie sie die Rechtsordnung bisher nicht kennt.[145] Hierbei hat es u. a. auf die weitreichende Aussagekraft dieser Daten, d. h. die Möglichkeit tiefer Einblicke in das soziale Umfeld und die individuellen Aktivitäten eines jeden Bürgers hingewiesen: Zwar werden mit der VDS der Inhalt der Kommunikation nicht festgehalten, jedoch lassen sich auch aus den gespeicherten Verkehrsdaten bei umfassender und automatisierter Auswertung bis in die Intimsphäre hineinreichende inhaltliche Rückschlüsse ziehen.[146]

---

[142] Gesetz zur Änderung des Niedersächsischen Gefahrenabwehrgesetzes vom 11. 12. 2003 (Nds. GVBl., S. 414).

[143] *BVerfGE* 113, 348, 365 [Rn. 82].

[144] *BVerfGE* 107, 299, 318 f. Allerdings ist der Eingriff in den Telekommunikationsinhalt i. d. R. gewichtiger als der in die Telekommunikationsumstände (a. a. O. 322), nunmehr stehen jedoch infolge der Digitalisierung in erheblichem Umfang Verbindungsdaten zur Verfügung, die für einen gewissen Zeitraum auch für Zwecke der Strafverfolgung nutzbar sind (a. a. O. 319).

[145] *BVerfGE* 125, 260, 318 – 320 [Rn. 210 – 212].

[146] *BVerfGE* 125, 260, 319 [Rn. 211]. Da eine Auswertung dieser Daten tief in das Privatleben eindringende Rückschlüsse und unter Umständen die Erstellung von detaillierten Persönlichkeits- und Bewegungsprofilen ermöglicht, kann insoweit nicht ohne Weiteres davon ausgegangen werden, dass der Rückgriff auf die Daten grundsätzlich geringer wiegt als eine inhaltsbezogene TKÜ (a. a. O. 328 [Rn. 227]).

bb) Heimlichkeit der Maßnahmen und umfassende Datenerhebung

Nach der festen Meinung der Rspr. des *BVerfG* erhöht die Heimlichkeit von Maßnahmen der Strafverfolgung i. d. R. die Intensität des Grundrechtseingriffs (vgl. Kapitel 3, A. I. 3.). Der Eingriff in das Fernmeldegeheimnis wie z. B. TKÜ wiegt schwer, weil er typischerweise heimlich erfolgt.[147] Die akustische Überwachung der Wohnung (Art. 13 Abs. 3 GG) stellt einen besonders schweren Grundrechtseingriff dar, weil sie nach der Art und Weise ihrer Durchführung zu einer Verletzung der Menschenwürde bzw. des Kernbereichs privater Lebensgestaltung führen kann.[148] Dies gilt auch bei einem heimlichen Zugriff auf ein informationstechnisches System, der den Zugang zu einem Datenbestand ermöglicht, der herkömmliche Informationsquellen an Umfang und Vielfältigkeit bei Weitem übertreffen kann.[149] Jedoch wird die Heimlichkeit aus Vorschriften in der StPO nicht begrifflich ersichtlich rückgeschlossen (vgl. Kapitel 3, A. II.).

Andererseits können im heutigen Ermittlungsverfahren, das als eine Ansammlung und Konzentration von Daten und eine Untersuchung mittels der IT bezeichnet wird (vgl. oben I. 2.), Untersuchungs- bzw. Aufklärungstätigkeiten der Ermittlungsbehörde stets zu einem tiefen Eingriff in die Privatsphäre durch eine umfassende Erhebung personenbezogener Daten führen: insb. Zugriff auf die Daten, deren Erhebung oder Beschlagnahme verfassungsrechtlich oder gesetzlich verboten oder beschränkt sind, wie die Daten, die den Kernbereich privater Lebensgestaltung betreffen, die Daten der Berufsgeheimnisträger nach § 53 StPO oder die nicht verfahrensrelevanten Daten. Hierbei handelt es sich nicht um die Heimlichkeit oder Offenheit der Maßnahme.[150] Heutzutage sind weitreichende Rückschlüsse auf die Persönlichkeit durch eine umfangreiche Datenerfassung auch durch einen offenen Zugriff auf die Daten in einem informationstechnischen System oder einem Datenbestand jederzeit möglich.[151]

---

[147] Vgl. *BVerfGE* 107, 299, 321 [Tz. (d)]; 110, 33, 53 [Rn. 105]; 113, 348, 383 [Rn. 141]; 115, 166, 194 [Rn. 106]; auch 124, 43, 65 [Rn. 76].

[148] *BVerfGE* 109, 279, 318 [Rn. 135] und 345 [Rn. 229].

[149] *BVerfGE* 120, 274, 322 ff. [Rn. 229 ff., insb. 231 – 234].

[150] Vgl. z. B. für die heimliche Erhebung der Inhaltsdaten, *BVerfGE* 113, 348, 365 [Rn. 82] und 115, 320, 347 – 357, insb. 349 f. [Rn. 102 f.]; für die heimliche Erhebung der Verkehrsdaten, 125, 260, 318 f. [Rn. 210 f.]; für den heimlichen Zugriff auf das informationstechnische System des Einzelnen, 120, 274, 323 [Rn. 229 – 232]; für die offene Durchsuchung und Beschlagnahme, 113, 29, 52 f. [Rn. 106 f.] (die in PC und Festplatte gespeicherten Daten), 115, 166, 192 f. [Rn. 100] (die in PC und Mobiltelefon gespeicherten Verkehrsdaten) und 124, 43, 63 [Rn. 69] (E-Mails, die außerhalb eines laufenden Kommunikationsvorgangs und auf dem Mailserver des Providers gespeichert sind).

[151] Vgl. *Singelnstein*, NStZ 2012, 593, 598.

IV. Zusammenfassung und Zwischenfazit

Die IT beeinflusst schon seit Langem das Strafverfahren und hat in letzter Zeit einen sehr großen Einfluss auf insb. das Ermittlungsverfahren. Derzeit werden alle persönlichen Selbstdarstellungen wie etwa Notizen, Fotos und Film- oder Tondokumente technisch präzis aufgezeichnet und kumulativ gespeichert, und sie werden ggf. zu sinnvolleren Beweismitteln im Strafverfahren als Aussagen von Verdächtigen oder Zeugen. Daher wollen die Ermittlungsbehörden sie stets umfassend erheben und verwenden. In vielen Fällen ist der – umfassende – Zugriff auf die e-Sphäre zur Suche nach Datenspuren des Beschuldigten bereits in der Praxis zur „ersten Standardermittlungsmaßnahme" der Strafverfolgungsbehörden geworden[152], und insb. im Bereich der organisierten Kriminalität sind heimliche Ermittlungsmaßnahmen besonders wirksam. Diese Maßnahmen können aber jederzeit zu weitreichenden Rückschlüssen auf die Persönlichkeit, nämlich zur Erstellung von Persönlichkeitsprofilen, führen. Eine effektive Strafverfolgung ist auch in der Informationsgesellschaft noch erforderlich, dies muss jedoch i. R. des GG und des der StPO immanenten Rechtsstaatsprinzips[153] geschehen.[154]

Bei der Prüfung der Verhältnismäßigkeit, die den Kern materieller Vorgabe des Rechtsstaatsprinzips darstellt, steht im Vordergrund eine Abwägung, die verlangt, dass die Einbußen grundrechtlich geschützter Freiheiten nicht in unangemessenem Verhältnis zu den Gemeinwohlzwecken stehen. Daher stehen dem Staat zum Schutz der wichtigsten Rechtsgüter wie Leib, Leben und Freiheit einer Person oder Bestand und Sicherheit des Bundes oder eines Landes – fast – alle eingriffsintensiven Mittel der Strafverfolgung zur Verfügung, die aber notwendig i. V. m. der materiellen Eingriffsschwelle und den Verfahrensvorkehrungen sein müssen, um die Eingriffsintensität hinreichend auszugleichen. In dieser Wechselbeziehung ist der Ausgangspunkt der Diskussion die Einschätzung der erhöhten Eingriffsintensität jeder Maßnahme. Danach können sowohl der Anwendungsbereich und der Inhalt der Verfahrensgarantien als auch das Maß an gebotener Bestimmtheit und Klarheit der Norm festgelegt werden. Insoweit ist bei der Erhebung und Verwendung personenbezogener Daten u. a. zu berücksichtigen: die Entwicklung der IT und auch die heimliche bzw. umfassende Datenerhebung.

Zum anderen wirken sich die verschiedenen neuen technischen Ausspähungsmethoden und die Möglichkeit umfassender Datenerhebung im Ermittlungsverfahren und die dadurch wie nie zuvor gestärkte Ermittlungsmacht auch auf die Struktur des Strafprozesses aus. Da im deutschen Strafverfahren herkömmlicherweise die Hauptverhandlung als Kern des gesamten Strafprozesses gilt, sind die Vorschriften zur Hauptverhandlung in der geltenden StPO unter dem Gesichtspunkt der Verfahrensbalance ausgestaltet, um Waffengleichheit zu gewährleisten. Dagegen

[152] *Vogel*, ZIS 2012, 480, 481.

[153] *BGH* NJW 1980, 1761.

[154] Vgl. *Papier*, NJW 2017, 3025: Auch in einer digitalen und globalisierten Gesellschaft sind die Rechtsstaatlichkeit und der Grundrechtsschutz noch von Bedeutung.

gilt dies bei solchen zum Ermittlungsverfahren nicht, in dem das Inquisitionsprinzip noch gilt. Dies ist aber unter dem Gesichtspunkt der Verhältnismäßigkeit zumindest bei heimlicher bzw. umfassender Erhebung der Daten nicht vertretbar. Denn infolge der gewaltigen Ermittlungsmacht durch neue Ermittlungstechniken und die fast einschränkungslose Transponierung von Ermittlungsergebnissen in die Hauptverhandlung ist inzwischen das Ermittlungsverfahren zum Kernstück des Strafprozesses geworden, außerdem hat sich der Einfluss der Strafverfolgungsbehörden auf das Gesamtergebnis enorm gesteigert.[155] Zur Wiederherstellung der beschädigten rechtsstaatlichen Struktur im Strafverfahren bedarf es dringend einer wirksamen Kontrolle über intensive Grundrechtseingriffe der Ermittlungsbehörde, wobei dies durch eine strikte Einhaltung des Richtervorbehalts und eine Möglichkeit zur Einwirkung auf das Ermittlungsverfahren durch den Beschuldigten und seinen Verteidiger zu erreichen ist.[156] Das heißt, die „checks and balances" sollen in gewissem Maß auch im Ermittlungsverfahren – wie in der Hauptverhandlung – durch eine institutionelle Kontrolle gegenüber der Ermittlungsmacht und eine Stärkung der Verteidigungsfunktion zustande kommen. Dies kann sich auch darauf stützen, dass in dem deutschen Strafverfahren, das auf den liberalen Rechtsstaat gegründet ist, der Beschuldigte kein bloßes Objekt des Verfahrens mehr ist, dem ein Geständnis abzuringen ist,[157] sondern die Stellung des Prozesssubjektes hat, das mit selbständigen Verfahrensrechten wie z. B. dem Anspruch auf rechtliches Gehör und der Selbstbelastungsfreiheit (Nemo-tenetur-Grundsatz) ausgestattet ist. Aus alledem sollte i. R. d. Erhebung und Verwendung personenbezogener Daten im Ermittlungsverfahren dem Beschuldigten, wenn auch nur beschränkt, die Möglichkeit gegeben werden, in den Gang und das Ergebnis des Verfahrens einzugreifen.

B. Maßgebliche Grundrechte

I. Vorrede

Unter dem GG stehen die Grundrechte im Mittelpunkt der rechtsstaatlichen Ordnung und sind als unmittelbar geltendes Recht für alle staatlichen Gewalten verbindlich (Art. 1 Abs. 3).[158] Daher setzen sie staatlichem Handeln Grenzen.[159]

---

[155] *Roxin/Schünemann*, § 39 Rn. 1; *Schünemann*, ZStW 114 (2002), 1, 34.

[156] *Park*, § 1 Rn. 4–9; teilweise *Roxin/Schünemann*, § 39 Rn. 1. Dem Beschuldigten muss die Möglichkeit gegeben werden, zur Wahrung seiner Rechte auf den Gang und das Ergebnis des Strafverfahrens Einfluss zu nehmen (*BVerfGE* 63, 380, 390). Ein Verteidiger nimmt eine öffentliche Aufgabe wahr, indem er in rechtlicher Hinsicht die Justizförmigkeit des Verfahrens überwacht (*Roxin/Schünemann*, § 19 Rn. 10).

[157] *BVerfGE* 63, 380, 390; 122, 248, 271; M-G/*Schmitt*, StPO, Einl. Rn. 24 und 80; *Roxin/Schünemann*, § 2 Rn. 4 und § 18 Rn. 1 ff.

[158] *Papier*, NJW 2017, 3025.

Auch in der digitalen und globalisierten Lebenswirklichkeit darf der Schutz der Menschenwürde und Persönlichkeit noch nicht seine verfassungsrechtliche Geltungs- und Durchsetzungskraft verlieren.[160] Da die Ermittlungsmaßnahmen in materielle Grundrechte der Art. 1 ff. GG eingreifen,[161] können sie nicht ohne Berücksichtigung der verfassungsrechtlichen Implikationen beantwortet werden. Daher sind zu einer gesetzlichen Ausgestaltung der strafprozessualen Eingriffsbefugnisse maßgebliche Grundrechte und ihre Eingriffsvoraussetzungen im System des Grundrechtsschutzes des GG vorrangig zu erwägen.

Im Folgenden werden die Schutzbereiche und die Eingriffsschwellen der Grundrechte überprüft, die im Zuge der rasanten Entwicklung der Technologie die Funktion des Persönlichkeitsschutzes innehaben: das (allgemeine) Persönlichkeitsrecht nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG in seiner eigenständigen Ausprägung als das Grundrecht auf informationelle Selbstbestimmung und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (sog. „Computer-Grundrecht"),[162] der Schutz des Fernmeldegeheimnisses nach Art. 10 GG und die Unverletzlichkeit der Wohnung nach Art. 13 GG.

II. Allgemeines Persönlichkeitsrecht und Schutz des Kernbereichs privater Lebensgestaltung

1. Allgemeines Persönlichkeitsrecht: Schutz des privaten Lebensbereichs

a) Rechtsgrundlage und Bedeutung

Die Menschenwürde wird als „tragendes Konstitutionsprinzip",[163] „oberster Wert des Grundgesetzes",[164] „Wurzel aller Grundrechte"[165] und „Staatsfundamentalnorm"

---

[159] *BVerfGE* 139, 245, 278 [Rn. 98]; *Neuhöfer*, JR 2015, 21, 22; vgl. *Papier*, NJW 2017, 3025: „*Nicht der absolute Staat, der ‚Leviathan', vielmehr der rechtsgebundene und machtbegrenzte Staat sichert den inneren und äußeren Frieden und damit die Sicherheit der Bürger.*"

[160] *Papier*, NJW 2017, 3025, 3031; vgl. *Schertz*, NJW 2013, 721: In der modernen Mediengesellschaft hat aber die technische Entwicklung die rechtlichen Schutzmechanismen des Individuums überholt.

[161] *Kudlich*, GA 2011, 193, 194 f.

[162] *Hofmann*, in: Schmidt-Bleibtreu/Hofmann/Henneke, K zum GG, Art. 2 Rn. 39; *Kudlich*, GA 2011, 193, 198; *Singelnstein/Derin*, NJW 2017, 2646, 2648; *Zimmermann*, JA 5/2014, 321, 323. Es wird auch als „IT-Grundrechte" bezeichnet (*Dalby*, CR 2013, 361, 367; *Gurlit*, NJW 2010, 1035, 1036).

[163] *BVerfGE* 6, 32, 36; 109, 279, 311.

[164] *BVerfGE* 6, 32, 41; 27, 1, 6; 96, 375, 399; 109, 279, 311; *Herdegen*, in: Maunz/Dürig, GG-K, Art. 1 Rn. 4; *Hillgruber*, in: Epping/Hillgruber, BeckOK GG, Art. 1 Rn. 1.

[165] *BVerfGE* 93, 266, 273.

bezeichnet[166], und die Unantastbarkeit der Menschenwürde (Art. 1 Abs. 1 GG; vgl. Art. 1 GRCh) bildet den Mittelpunkt des grundgesetzlichen Wertsystems.[167] Daher sollen die folgenden Grundrechte und alle Verfassungsnormen im Licht des Art. 1 Abs. 1 GG ausgelegt und ihre Reichweite festgelegt werden.[168] Das Recht auf die freie Entfaltung der Persönlichkeit (Art. 2 Abs. 1 GG) ist zum anderen die erste und allgemeinste Freiheitsgewährleistung des GG.[169] Nach vorherrschender Auffassung ist es ein selbstständiges Grundrecht und gewährleistet zum lückenlosen Grundrechtsschutz die „Handlungsfreiheit im umfassenden Sinne", die – im Vergleich mit speziellen Freiheitsrechten – als sog. „Auffanggrundrecht" oder „Komplementärrecht" fungiert.[170] Der *BGH* und das *BVerfG* haben schon in den Anfangsjahren der BRD durch ihre Entscheidungen aus dem Schutz eigenständige spezielle Freiheitsrechte abgeleitet.[171] Dabei haben sie das „allgemeine Persönlichkeitsrecht" aus Art. 1 Abs. 1 GG i. V. m. Art. 2 Abs. 1 GG als ein verfassungsmäßig gewährleistetes eigenständiges Grundrecht entwickelt, um das Recht auf Selbstbestimmung über die Verwertung äußerer persönlicher Selbstdarstellungen grundrechtlich zu schützen.[172] Der Schutz dieses Rechts betrifft die durch den Wortlaut von Art. 2 Abs. 1 GG ausdrücklich gewährleistete Persönlichkeitsentfaltung, wobei Art. 1 Abs. 1 GG nur als Auslegungsmaßstab für ihren Inhalt und Schutzumfang fungiert.[173]

Im Jahr 1954 erkannte der *BGH* in der sog. „Leserbrief-Entscheidung" erstmals das allgemeine Persönlichkeitsrecht[174] und zugleich auch die „Eigensphäre der

[166] *Herdegen*, in: Maunz/Dürig, GG-K, Art. 1 Rn. 4. Daher darf dieser Schutz gemäß Art. 79 Abs. 3 GG durch eine Verfassungsänderung nicht berührt werden (*BVerfGE* 30, 1, 25; *Sodan*, GG, Art. 1 Rn. 1).

[167] *BVerfGE* 35, 202, 225; 39, 1, 43; *Sodan*, GG, Art. 1 Rn. 1. Das GG hat – im Gegensatz zur Reichsverfassung von 1919 – eine wertgebundene Ordnung aufgerichtet, die die öffentliche Gewalt begrenzt (*BVerfGE* 2, 1, 12; 6, 32, 40).

[168] *Hofmann*, in: Schmidt-Bleibtreu/Hofmann/Henneke, K zum GG, Art. 1 Rn. 82.

[169] *Di Fabio*, in: Maunz/Dürig, GG-K, Art. 2 Abs. 1 Rn. 1.

[170] *Di Fabio*, in: Maunz/Dürig, GG-K, Art. 2 Abs. 1 Rn. 7, 15, 21; 6, 32, 36; seither ständige Rspr.

[171] *BVerfGE* 141, 186, 201 [Rn. 32]; *Di Fabio*, in: Maunz/Dürig, GG-K, Art. 2 Ab. 1 Rn. 127; *Hofmann*, in: Schmidt-Bleibtreu/Hofmann/Henneke, K zum GG, Art. 2 Rn. 1; *Lang*, in: Epping/Hillgruber, BeckOK GG, Art. 2 Rn. 1 und 31: zwei unterschiedliche grundrechtliche Gewährleistungen; *Sodan*, GG, Art. 2 Rn. 1.

[172] *BGHZ* 13, 334, 338; 27, 1, 7 f.; 27, 344, 351; 32, 373, 378 f.; 34, 238, 247; 72, 155, 170 [Tz. a)]; *BVerfGE* 80, 367, 373; *Di Fabio*, in: Maunz/Dürig, GG-K, Art. 2 Abs. 1 Rn. 127 ff. und insb. Rn. 128: „*Begriff und dogmatische Prägung des allgemeinen Persönlichkeitsrechts sind Schöpfungen der Rechtsprechung*"; *Hofmann*, in: Schmidt-Bleibtreu/Hofmann/Henneke, K zum GG, Art. 2 Rn. 1, 14; *Lang*, in: Epping/Hillgruber, BeckOK GG, Art. 2 Rn. 31 ff.; *Sodan*, GG, Art. 2 Rn. 5 ff. In Deutschland wurde der Schutz des Individuums durch das Persönlichkeitsrecht nicht durch Gesetze, sondern im Wesentlichen durch gerichtliche Entscheidungen eingeführt und etabliert (*Schertz*, NJW 2013, 721, 722).

[173] *BVerfGE* 27, 344, 350 f.; 32, 373, 378 f.; 34, 238, 245; *Di Fabio*, in: Maunz/Dürig, GG-K, Art. 2 Abs. 1 Rn. 128 und dazu Rn. 130: „*der in Art. 1 Abs. 1 GG wurzelnde Gedanke grundrechtlicher Autonomie gibt dem Schutzbereich eine besondere Auslegungsrichtung vor*".

[174] *Schertz*, NJW 2013, 721, 722.

Persönlichkeit“ bzw. die „geschützte Geheimsphäre“ jedes Menschen: jede „sprachliche Festlegung“ eines bestimmten Gedankeninhalts wie Briefe oder sonstige private Aufzeichnungen (mit Gesprächs- bzw. Verkehrspartner).[175] Dies gilt auch für „sprachliche Äußerungen“ (mit Gesprächs- bzw. Verkehrspartner).[176] Darüber hinaus hat er 1964 in seiner Entscheidung, bei der es sich um „tagebuchartige Aufzeichnungen“ (ohne Gesprächs- bzw. Verkehrspartner) handelte, entschieden, dass die Grundsätze erst recht gelten müssen.[177] Das gilt auch für Selbstgespräche (ohne Partner).[178] Außerdem hat er entschieden, dass auch die „persönliche Geheimsphäre, die durch Geheimhaltung gesetzlicher Geheimnisträger wie ein Arzt bewahrt wird“, in die Reichweite des Persönlichkeitsrechts fällt.[179]

Das *BVerfG* hat andererseits im Jahr 1957 zum ersten Mal aus Art. 1 und Art. 2 GG eine – letzte unantastbare – Sphäre privater Lebensgestaltung ableitet[180], und unter dieser Prämisse hat es 1969 entschieden, dass die „statistische Erhebung über Persönlichkeits- und Lebensdaten“ dann zulässig ist, wenn sie nur an das Verhalten des Menschen in der Außenwelt anknüpft und weiter die Anonymität hinreichend gesichert ist.[181] In der „Tonband-Entscheidung“ von 1973 hat das Gericht erklärt, dass Art. 2 Abs. 1 GG auch die für die freie Entfaltung der Persönlichkeit notwendigen Rechtspositionen (das allgemeine Persönlichkeitsrecht) schützt und dazu „das Recht am eigenen Bild und das Recht am gesprochenen Wort“ gehört. Es ist zu gewährleisten, dass grundsätzlich jedermann selbst und allein bestimmen darf, wer sein Wort aufnehmen soll sowie ob und vor wem seine auf einen Tonträger aufgenommene Stimme wieder abgespielt werden darf.[182] Schließlich hat das Gericht 1980 klargestellt, dass das allgemeine Persönlichkeitsrecht durch Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG verfassungsrechtlich gewährleistet wird, und seine Eigenart und Notwendigkeit konkret ausgeführt: „*Dieses ergänzt als ‚unbenanntes‘ Freiheitsrecht die speziellen (‚benannten‘) Freiheitsrechte, die, wie etwa die Gewissensfreiheit oder*

[175] *BGHZ* 13, 334, 338 f.

[176] *BGHZ* 27, 284, 289: eine heimliche Tonaufnahme eines Gesprächs; *BGHSt* 10, 202, 205: Tonbandaufnahme beim Schlussvortrag des Verteidigers; 14, 358, 360 f.: eine heimliche Tonbandaufnahme eines privaten Gesprächs. „Gespräch“ meint nur solche Äußerungen wenigstens im „Zwiegespräch“ (*BGHSt* 50, 206, 214 am Anfang; BT-Drs. 15/4533, S. 14).

[177] *BGHSt* 19, 325, 327 f.: Solche Aufzeichnungen müssen stärker geschützt werden als die o. g. Fälle, weil sie Meinungen, Gefühle, Erlebnisse und Erfahrungen des Verfassers für sich selber festhalten werden, ohne dass sie, von seltenen Ausnahmen abgesehen, zur Kenntnis anderer gelangen sollen.

[178] *BGHSt* 50, 206: ein im Krankenzimmer heimlich aufgezeichnetes Selbstgespräch; *BGHSt* 57, 71: ein in einem Kraftfahrzeug heimlich aufgezeichnetes Selbstgespräch.

[179] *BGHZ* 24, 72.

[180] *BVerfGE* 6, 32, 41.

[181] *BVerfGE* 27, 1, 6 f. Danach hat es entschieden, dass „Ehescheidungsakten“ (*BVerfGE* 27, 344, 351 f.) und „ärztliche Karteikarten“ (32, 373), nicht den unantastbaren Bereich privater Lebensgestaltung, sondern den privaten Lebensbereich der Ehepartner betreffen.

[182] *BVerfGE* 34, 238; danach 100, 313, 375 f.; 113, 348, 382.

die Meinungsfreiheit, ebenfalls konstituierende Elemente der Persönlichkeit schützen.“[183]

Bei Prüfung der Verletzung der Persönlichkeit ist das allgemeine Persönlichkeitsrecht grundsätzlich gleichberechtigt mit anderen Freiheitsrechten,[184] aber es wird nachrangig angewendet. Aufgabe dieses Grundrechts ist es, Elemente der Persönlichkeit, die nicht Gegenstand der besonderen Freiheitsgarantien des GG sind, diesen aber in ihrer konstituierenden Bedeutung für die Persönlichkeit nicht nachstehen, grundrechtlich zu schützen. Dabei handelte es sich anfangs um den Missbrauch der einzelnen Erhebung und Verwertung von Daten, während es sich gegenwärtig um den Eingriff in die Identität und Integrität des Einzelnen durch umfangreiche Datenerhebung handelt.[185] In dieser Hinsicht kommt dem Grundrecht eine lückenschließende Gewährleistungsfunktion zu, um neuartigen Gefährdungen zu begegnen, zu denen es im Zuge wissenschaftlich-technischen Fortschritts und gewandelter Lebensverhältnisse kommen kann.[186]

b) Verfassungsrechtliches Beweisverbot

Unter dem GG folgt aus der staatlichen Pflicht zur Achtung der Menschenwürde (Art. 1 Abs. 1 S. 2 Alt. 1) die Achtung der Subjektqualität des Einzelnen im Verfahrensrecht, woraus das Verbot der Erhebung von Beweisen in einer Weise, durch die von staatlichen Organen die Menschenwürde verletzt wird, und der Verwertung dieser erlangten Beweise folgt.[187] Diesbezüglich hat der Gesetzgeber Beweiserhebungsverbote (z. B. §§ 52–55, 136a Abs. 1, 2, 3 S. 1 und § 100d Abs. 1 StPO) und Beweisverwertungsverbote (z. B. §§ 136a Abs. 3 S. 2, 160a Abs. 1 S. 2 und §§ 108 Abs. 2, 3, 100d Abs. 2 StPO) bereits teilweise gesetzlich festgeschrieben. Daneben kann jedoch die Verwertung der in die Persönlichkeitssphäre bzw. Persönlichkeitsrechte (tief-)eingreifenden Beweismittel – die nicht zum Kernbereich privater Lebensgestaltung zählen – auch nach Grundrechten und Verfassungssätzen, insb. Abwägung, nicht nach der StPO verboten werden.[188] Da das Strafverfahrensrecht als

[183] *BVerfGE* 54, 148, 153 [Rn. 13]; danach 72, 155, 170; 95, 220, 241; 109, 279, 326; 141, 186, 201 m. w. N.

[184] *Lang*, in: Epping/Hillgruber, BeckOK GG, Art. 2 Rn. 54.

[185] *BVerfGE* 109, 279, 312 [Rn. 115 a. E.].

[186] *BVerfGE* 118, 168, 183 [Rn. 85]; 120, 274, 303 [Rn. 169]; 141, 186, 201 f. [Rn. 32]; *Di Fabio*, in: Maunz/Dürig, GG-K, Art. 2 Abs. 1 Rn. 127; *Lang*, in: Epping/Hillgruber, BeckOK GG, Art. 2 Rn. 54.

[187] Vgl. *BGHSt* 5, 332, 333; 19, 325, 330 f.; *Herdegen*, in: Maunz/Dürig, GG-K, Art. 1 Rn. 76.

[188] *Roxin/Schünemann*, § 24 Rn. 23 und 30 ff.; *BGHSt* 19, 325, 329 a. E. Hierbei wird das Interesse des Staates an der Tataufklärung dann überwiegen, wenn der Tatverdacht schwerer Angriffe auf das Leben, auf andere bedeutsame Rechtsgüter, auf den Staat oder um andere schwerere Angriffe auf die Rechtsordnung hinreichend begründet ist, und daher führt es nicht zum Verwertungsverbot (*BGHSt*, a. a. O. 332 f.).

angewandtes Verfassungsrecht verstanden wird,[189] kann das GG die Wirkung der StPO, die Grundrechte einschränkt, korrigieren.[190] Der *BGH* hat entschieden, dass tagebuchartige Aufzeichnungen, die als Beweismittel des Verdachts des „Meineids" zur StA gelangen,[191] und auch Tagebücher, die im Ermittlungsverfahren wegen des Tatverdachts „geheimdienstlicher Agententätigkeit" beschlagnahmt werden,[192] intime Papiere darstellen und aufgrund einer Abwägung nicht verwertet werden dürfen. Hingegen hat er erklärt, dass bei tagebuchartigen Aufzeichnungen, die als Beweismittel des Verdachts des „Mords" freiwillig zur Polizei gelangen, der Intimcharakter verloren gegangen ist und sie daher nach Abwägung verwertet werden können.[193] In dieser Hinsicht ist es immer noch unklar, ob in die Persönlichkeit eingreifende Beweismittel im Einzelfall in den Kern- oder Abwägungsbereich fallen.[194]

2. Schutz des Kernbereichs privater Lebensgestaltung

a) Rechtsgrundlage und Bedeutung

Das *BVerfG* erkennt seit seiner Rechtsprechung in den Anfangsjahren der BRD ständig an, dass das GG aus „jeweiligen betroffenen Grundrechten i. V. m. Art. 1 Abs. 1 GG"[195] dem einzelnen Bürger einen unantastbaren Bereich privater Lebensgestaltung, nämlich einen absolut geschützten Kernbereich, gewährt, der der Einwirkung der öffentlichen Gewalt entzogen ist.[196] Insb. verkörpert sich in der jüngsten Zeit i. R. d. Grundrechtseinschränkungen im Bereich der inneren Sicherheit die Garantie der Menschenwürde dogmatisch mit der Lehre vom Kernbereichsschutz.[197] Der Schutz des Kernbereichs ist eine stets zu wahrende Schranken-

[189] *BVerfGE* 32, 373, 383; M-G/*Schmitt*, StPO, Einl. Rn. 218.

[190] *BGHSt* 19, 325, 332.

[191] *BGHSt* 19, 325, 333 a. E.

[192] *BGHSt* NJW 1994, 1170.

[193] *BGHSt* 34, 397, 400 f.

[194] Vgl. *Roxin*/*Schünemann*, 27. Aufl. 2012, § 24 Rn. 56 a. E. In der Entscheidung des *BVerfG* stießen hingegen die Meinungen der Richter mit 4:4 aufeinander über die Frage, ob tagebuchartige Aufzeichnungen, die als Beweismittel des Verdachts des „Mords" nicht freiwillig abgegeben, sondern sichergestellt werden, zum Kernbereich gehören (*BVerfGE* 80, 367, 376 ff.). Dies steht aber der „Selbstgespräch-Entscheidung" des *BGH* (*BGHSt* 50, 206, 210) entgegen, die sogar eine direkt auf die vorgeworfene Tat bezogene Äußerung des Beschuldigten im Selbstgespräch zu solchem Bereich gerechnet hat (*Roxin*/*Schünemann*, a. a. O.).

[195] *BVerfGE* 141, 220, 276 [Rn. 120].

[196] *BVerfGE* 6, 32, 41; 27, 1, 6; 27, 344, 350 f.; 32, 373, 378; 34, 238, 245; 80, 367, 373; 109, 279, 313; 113, 348, 390; 120, 274, 335; 124, 43, 69 m. w. N. Nach heutiger h. M. wurzelt dieser Bereich nicht mehr im allgemeinen Persönlichkeitsrecht, sondern allein im Art. 1 Abs. 1 GG (*Gurlit*, NJW 2010, 1035, 1039; vgl. *BVerfGE* 109, 279, 313; 124, 43, 69; 141, 220, 276).

[197] *Hofmann*, in: Schmidt-Bleibtreu/Hofmann/Henneke, K zum GG, Art. 1 Rn. 51.

Schranke.[198] Da selbst überragende Interessen der Allgemeinheit somit einen Eingriff in den Kernbereich nicht rechtfertigen können, steht er nicht unter einem allgemeinen Abwägungsvorbehalt.[199] Es ist folglich dem Staat verwehrt, personenbezogene Daten, die diesem Bereich zuzuordnen sind, als Beweismittel zu erheben, aufzuzeichnen, zu speichern, zu übermitteln und zu verwerten.

Der verfassungsrechtliche Schutz des Kernbereichs privater Lebensgestaltung gewährleistet dem Individuum einen Bereich höchstpersönlicher Privatheit, und zur Entfaltung der Persönlichkeit in einem solchen Bereich gehört die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen: hierzu gehören insb. „die nichtöffentlichen Kommunikationen oder Gespräche" mit „Personen des höchstpersönlichen Vertrauens" oder mit „in einem besonderen, den Kernbereich betreffenden Vertrauensverhältnis stehenden Personen", wie z. B. Ehe- oder Lebenspartnern, Geschwistern und Verwandten in gerader Linie, vor allem, wenn sie im selben Haushalt leben, und Strafverteidigern, Ärzten, Geistlichen und engen persönlichen Freunden.[200] Dabei verlieren sie auch dann nicht ihren Charakter als insgesamt höchstpersönlich, wenn sich in ihnen Höchstpersönliches und Alltägliches vermischen.[201] Ob ein Sachverhalt dem unantastbaren Bereich privater Lebensgestaltung oder jenem Bereich des privaten Lebens, der unter bestimmten Voraussetzungen dem staatlichen Zugriff offen steht, zugeordnet wird, hängt nicht davon ab, ob eine soziale Bedeutung oder Beziehung überhaupt besteht, sondern welcher Art und wie intensiv sie im Einzelfall ist.[202] Die Frage, ob eine Entfaltung der Persönlichkeit höchstpersönlichen Charakter hat, kann nämlich befriedigend nur unter Berücksichtigung der Besonderheiten des einzelnen Falls beantwortet werden.[203] Enthält insoweit der Inhalt der Persönlichkeitsentfaltung Angaben über die Planung bevorstehender oder Berichte über begangene Straftaten, die in einem unmittelbaren Bezug zu konkreten strafbaren Handlungen stehen, dann gehört er nach der überzeugten Meinung des *BVerfG* nicht zum unantastbaren Bereich privater Lebensgestaltung, sondern hat Sozialbezug.[204]

---

[198] *Gurlit*, NJW 2010, 1035, 1038 f.; vgl. *BVerfGE* 109, 279, 318 [Rn. 134].

[199] *BVerfGE* 34, 238, 245 f.; 109, 279, 313 f.; 120, 274, 335; 141, 220, 276 f. [Rn. 120 und 122].

[200] *BVerfGE* 109, 279, 313 und 321 ff.; 120, 274, 335; 129, 208, 247; 141, 220, 276 [Rn. 120 f.]: Dieser Kreis deckt sich nur teilweise mit dem der Zeugnisverweigerungsberechtigten.

[201] *BVerfGE* 109, 279, 330; 113, 348, 391 f.; 141, 220, 276 f. [Rn. 121 a. E.].

[202] *BVerfGE* 80, 367, 374; 109, 279, 319.

[203] *BVerfGE* 34, 238, 248; 80, 367, 374 f.; 109, 279, 314; 124, 43, 70; NJW 2011, 2417, 2419; krit. *Roxin/Schünemann*, § 36 Rn. 45: Dadurch wird der Schutz des Kernbereichs weitgehend ausgeschaltet.

[204] *BVerfGE* 80, 367, 375; 109, 279, 319; 113, 348, 391; 124, 43, 70; 141, 220, 277 [Rn. 122].

b) Schwierigkeit des Schutzes in der Informationsgesellschaft

Das *BVerfG* betont in seiner jüngsten Rspr. ständig, dass in den Kernbereich privater Lebensgestaltung auch durch die Erhebung personenbezogener Daten durch den Einsatz technischer Mittel nicht eingegriffen werden darf.[205] In der modernen Informationsgesellschaft, in der sowohl geschäftlich als auch privat die Verwendung komplexer informationstechnischer Systeme fortwährend wächst, mit denen man höchstpersönliche Daten erzeugen, verarbeiten, übermitteln und speichern kann, erhöht aber der Zugriff auf die Systeme das Risiko, dass die dem Kernbereich zuzuordnenden Daten zusammen mit anderen erfasst werden.[206] Trotzdem kann eine Ermittlungsmaßnahme aus diesem Grund nicht von vornherein unterlassen werden. Dies wäre eine übermäßige Einschränkung der Ermittlungsmacht und würde u. a. die Ermittlungstätigkeiten in einem Maße einschränken, dass eine wirksame Strafverfolgung auch gerade im Bereich schwerer und schwerster Kriminalität nicht mehr gewährleistet wäre.[207] Daher ist im Strafverfolgungsverfahren die Erhebung und Durchsicht kernbereichsrelevanter Daten in der Praxis in gewissem Maß unvermeidlich.[208] Erst recht gilt dies heute mit Blick auf die Eigenschaften digitaler Daten wie Unsichtbarkeit, große Menge etc. sowie automatisierter Datenerhebung. Aus diesen Gründen steckt der angemessene Schutz des Kernbereichs tatsächlich in der Klemme[209] und seine praktische Umsetzung stößt auf Schwierigkeiten.[210] Um eine Garantie der Menschenwürde zu erreichen, bedarf es letzten Endes institutioneller und verfahrensrechtlicher Vorkehrungen, damit die Intensität der Kernbereichsverletzung so gering wie möglich bleibt. Insoweit hat das *BVerfG* im Jahre 1989 vor der Verallgemeinerung der Nutzung elektronischer Daten und digitaler Telekommunikationstechnik in seiner Entscheidung bezogen auf die Durchsicht von tagebuchartigen Aufzeichnungen des Beschuldigten ausgeführt:

> „Die Verfassung gebietet es deshalb nicht, Tagebücher oder ähnliche private Aufzeichnungen schlechthin von der Verwertung im Strafverfahren auszunehmen. Allein die Aufnahme in ein Tagebuch entzieht Informationen noch nicht dem staatlichen Zugriff. Vielmehr hängt die Verwertbarkeit von Charakter und Bedeutung des Inhalts ab. … Daraus folgt auch, daß i. R. d. Strafverfolgung nicht von vornherein ein verfassungsrechtliches Hindernis besteht, solche Schriftstücke daraufhin durchzusehen, ob sie der prozessualen Verwertung

[205] Vgl. *BVerfGE* 109, 279, 318 – 324 und 328 – 335; 120, 274, 335 – 339; 129, 208, 245 ff. [Rn. 209 ff.]; 141, 220, 276 ff. [insb. Rn. 119 ff.].

[206] Vgl. *Kudlich*, GA 2011, 193, 198: Im Blick auf heutige Gegebenheiten und bürgerliche Handlungsweise bezüglich der Nutzung der IuK-Technologie könnte sich nahezu alles, was zu diesem Kernbereich gehören kann, auf den Systemen befinden.

[207] *BVerfGE* 129, 208, 247 [Rn. 216].

[208] *BVerfGE* 141, 220, 278 [Rn. 124]; auch 129, 208, 245 [Rn. 211]: „*In vielen Fällen ist es (allerdings) praktisch unvermeidbar, dass die Ermittlungsbehörden Informationen zur Kenntnis nehmen, bevor sie deren Kernbereichsbezug erkennen.*"

[209] Vgl. *Gurlit*, NJW 2010, 1035, 1039: dilemmatisch; *Roxin/Schünemann*, § 36 Rn. 45, 47.

[210] Zust. *Vogel*, ZIS 2012, 480, 482 a. E.

zugängliche Informationen enthalten. Hierbei ist allerdings die größtmögliche Zurückhaltung zu wahren; dies ist durch geeignete Maßnahmen sicherzustellen."[211]

In dieser Rspr. hat das Gericht zwar erkannt, dass eine Kontrolle gegenüber dem Zugriff auf höchstpersönliche Informationen erforderlich ist, hierfür hat es indes nur auf den Richtervorbehalt zur Durchsicht – der in der Praxis kaum wirksam war – hingewiesen. Jedoch hat es 2003 in der Entscheidung zur akustischen Überwachung von Wohnungen verfassungsrechtliche Anforderungen an die gesetzliche Ausgestaltung verfahrensrechtlicher Vorkehrungen zum Schutz des Kernbereichs unter Berücksichtigung des aktuellen technischen Standes im Detail begründet.[212] Hier ist der Schlüssel dazu sog. ein „zweistufiges Schutzkonzept", das in den Schutz „auf der Ebene der Erhebung" und „auf der Ebene der Auswertung und Verwertung" der Daten unterteilt ist. Danach hat es in den Entscheidungen über Verfassungsmäßigkeit jeder Ermächtigung zur TKÜ und zur Online-Durchsuchung sowie jeder Maßnahme einfacher Beschlagnahme und Durchsuchung das wiederholt beschrieben:[213] Zuerst muss auf der Erhebungsebene die Erfassung von kernbereichsrelevanten Informationen durch eine vorgelagerte Prüfung und eine Vermutung von typischerweise vertraulichen Situationen jedenfalls insoweit ausgeschlossen werden, als sich diese im Vorfeld vermeiden lässt, des Weiteren muss die Durchführung der Maßnahme stets abgebrochen werden, wenn solche Informationen erkennbar werden. Danach müssen in der Auswertungsphase, also dann, wenn die Erfassung von kernbereichsrelevanten Informationen nicht vermieden werden konnte, zur Herausfilterung solcher Informationen die erfassten Daten durch eine unabhängige Stelle (wie StA oder Richter) eingesehen werden. Dabei müssen in jedem Fall ggf. erfasste höchstpersönliche Daten unverzüglich gelöscht und muss die Löschung in solcher Weise protokolliert werden, die eine spätere Kontrolle ermöglicht, und jegliche Verwendung muss ausgeschlossen werden.

c) § 100d StPO

Der Kernbereich privater Lebensgestaltung beansprucht zwar bei allen Überwachungsmaßnahmen Beachtung, das *BVerfG* betonte aber bei den Maßnahmen, bei denen der Eingriff in den Bereich hinreichend konkret absehbar ist, insb. TKÜ, Online-Durchsuchung und Wohnraumüberwachung, zum wirksamen Schutz die Notwendigkeit einer Schaffung normenklarer Regelungen.[214] Die verfassungsrechtlichen Anforderungen an die konkrete Ausgestaltung dieses Schutzes können allerdings je nach der Art der Informationserhebung und der dadurch zu erfassenden Informationen unterschiedlich sein.[215] Daraufhin hat der Gesetzgeber die Garantien

[211] *BVerfGE* 80, 367, 374 f. [Rn. 30].

[212] *BVerfGE* 109, 279, 318 – 324 und 328 – 335.

[213] *BVerfGE* 113, 348, 391 ff.; 120, 274, 337 ff.; 124, 43, 70; 129, 208, 245 f.; jüngste überschaubare Ausführung 141, 220, 278 – 280 [Rn. 125 – 129].

[214] *BVerfGE* 141, 220, 277 [Rn. 123].

[215] *BVerfGE* 120, 274, 337 [Rn. 276]; 129, 208, 245 [Rn. 210]; 141, 220, 279 [Rn. 127].

zum Schutz des Kernbereichs je nach Maßnahme in § 100d StPO individuell vorgesehen. Zunächst sind im Fall der TKÜ die Anforderungen an die gesetzliche Ausgestaltung nicht streng (Abs. 1 und 2). Hier ist es geboten, für hinreichenden Schutz in der Phase der Datenauswertung und nicht auf der Ebene der Erhebung, zu sorgen.[216] Hingegen wird für die Wohnraumüberwachung und die Online-Durchsuchung nach der Rspr. des *BVerfG* der Kernbereichsschutz durch ausdrückliche gesetzliche Vorkehrungen besonders streng verlangt.[217] Aus diesem Grund werden in der Phase der Durchführung und Beendigung dieser Maßnahmen richterliche Einschaltungen mehr verlangt. Bei der Online-Durchsuchung muss eine Entscheidung darüber, ob erlangte Erkenntnisse den Kernbereich privater Lebensgestaltung betreffen, d. h. über ihre Verwertbarkeit und Löschung, nicht durch die StA, sondern durch das anordnende Gericht getroffen werden (Abs. 3 S. 2). Bei der Wohnraumüberwachung muss die Entscheidung auch durch das Gericht gefällt werden, wenn die Erfassbarkeit der Äußerungen, die dem Kernbereich zuzurechnen sind, oder die Verwertbarkeit erlangter Erkenntnisse im Zweifel ist (Abs. 4 S. 4, 5). Diese Entscheidungen des Gerichts sind freilich für das weitere Verfahren bindend (Abs. 3 S. 3 und Abs. 4 S. 6).

Durch das Änderungsgesetz vom 20. 11. 2019 (siehe Kapitel 1, Fn. 32) hat der Gesetzgeber jüngst festgestellt, dass § 100d Abs. 1, 2 StPO außer bei den drei o. g. Maßnahmen auch auf akustische Überwachung außerhalb von Wohnraum, eine Herstellung von Bildaufnahmen und eine Verwendung sonstiger technischer Mittel für Observationszwecke, einen Einsatz eines Verdeckten Ermittlers und längerfristige Observation Anwendung findet (§§ 100f Abs. 4, 100h Abs. 4, 110a Abs. 1 S. 5, 163f Abs. 2 S. 2 i. V. m. § 100d Abs. 1, 2 StPO). Der Regelungsinhalt des § 100d Abs. 1, 2 StPO gilt – ungeachtet dieser Änderung – bereits unter dem GG zwar verfassungsrechtlich, gleichwohl betont der Gesetzgeber bei den verdeckten Ermittlungsmaßnahmen, die ein hohes Eingriffsrisiko für einen unantastbaren Intimbereich in sich bergen, durch diese Verankerung ihn erneut.[218]

3. Zusammenfassung

In dem GG ist zwar ein eigenständiges Persönlichkeitsrecht nicht ausdrücklich vorgeschrieben, jedoch haben es der *BGH* und das *BVerfG* zur Schließung der Lücken des Persönlichkeitsschutzes durch ihre Entscheidungen in den Anfangsjahren der BRD aufgrund der Art. 1 Abs. 1 und Art. 2 Abs. 1 GG anerkannt. Danach hat das *BVerfG* aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 und Art. 19 Abs. 2 GG exegetisch das allgemeine Persönlichkeitsrecht deduziert, dessen Schutzbereich parallel zur Ver-

[216] *BVerfGE* 129, 208, 246 f. [Rn. 212 und 216]: Ein von vornherein umfassendes Erhebungsverbot in der TKÜ erschwert die Gewährleistung einer wirksamen Strafverfolgung im Bereich schwerer und schwerster Kriminalität.

[217] *BVerfGE* 141, 220, 299 f. [Rn. 197] und 306 [Rn. 218].

[218] Vgl. für die Meinung, die für diese analoge Anwendung auf die Maßnahmen nach §§ 100f, 100h Abs. 1 StPO spricht, *Singelnstein*, NStZ 2014, 305, 311.

änderung der Realität erweitert werden kann.[219] Wie der Begriff der Persönlichkeit und der Eingriff darin beweglich sind, dient das allgemeine Persönlichkeitsrecht durch seine Entwicklungsoffenheit und Begriffserweiterung dem Grundrechtsschutz dynamisch.[220] Insb. bei dem Einschreiten gegen neue Gefährdungen der Persönlichkeit, die im Zuge gesellschaftlicher oder technischer Entwicklung verursacht sind, wurde das zu einem der wichtigsten Grundrechte.[221] Aus dem allgemeinen Persönlichkeitsrecht hat das *BVerfG* das Recht auf informationelle Selbstbestimmung und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme schrittweise abgeleitet (vgl. unten III.). Zum anderen stellt das *BVerfG* ständig fest, dass ein absolut geschützter Kernbereich vorhanden ist. Jedoch ist die Unterscheidung zwischen diesem Bereich und dem Abwägungsbereich lange Zeit unklar geblieben, was in der Praxis erhebliche Probleme mit sich bringt. Insb. bei dem heutigen Ermittlungsverfahren, in dem personenbezogene Daten in jedem Fall umfassend zu erheben sind, gilt dies erst recht.

III. Recht auf informationelle Selbstbestimmung und Computer-Grundrecht

1. Recht auf informationelle Selbstbestimmung: Volkszählungsurteil

a) Erkenntnis- bzw. Erwägungsgründe und Schutzbereich

Im Jahr 1983 hatte das *BVerfG* in dem sog. „Volkszählungsurteil", das Volkszählungsgesetz 1983[222] auf Verfassungsmäßigkeit zu überprüfen, aufgrund des allgemeinen Persönlichkeitsrechts die verfassungsrechtlichen Grundlagen des Datenschutzes umfassend beleuchtet. Hierzu hat es ausgeführt: Da die freie Entfaltung der Persönlichkeit gemäß Art. 2 Abs. 1 GG unter den Bedingungen der modernen automatisierten Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraussetzt, ist dieser Schutz von dem allgemeinen Persönlichkeitsrecht umfasst. Hieraus hat es das „Recht auf informationelle Selbstbestimmung" abgeleitet, das die Befugnis des Einzelnen gewährleistet, grundsätzlich selbst über die Preisgabe oder Verwendung seiner persönlichen Daten zu bestimmen.[223]

---

[219] *BVerfGE* 65, 1, 41; 118, 168, 183; 120, 274, 303 [Rn. 169].

[220] *Di Fabio*, in: Maunz/Dürig, GG-K, Art. 2 Abs. 1 Rn. 127 und 147; *Lang*, in: Epping/Hillgruber, BeckOK GG, Art. 2 Rn. 34.

[221] Vgl. *BVerfGE* 54, 148, 153; 65, 1, 41; 120, 274, 303; *Di Fabio*, in: Maunz/Dürig, GG-K, Art. 2 Abs. 1 Rn. 127.

[222] Volkszählungsgesetz vom 25. März 1982 (BGBl. I S. 369).

[223] *BVerfGE* 65, 1, 41 ff. [insb. Rn. 155]. Natürlich wurde dieses Recht ohne Hintergrund nicht plötzlich anerkannt. Der Gedanke, dass der Einzelne über seine persönlichen Angelegenheiten selbst zu bestimmen habe, und die Notwendigkeit seines grundrechtlichen Schutzes wurden bereits frühzeitig in den Rspr. zum allgemeinen Persönlichkeitsrecht vertreten (*Vo-*

Durch das informationelle Selbstbestimmungsrecht wird der grundrechtliche Schutz von Verhaltensfreiheit und Privatheit bis auf die Stufe der Persönlichkeitsgefährdung im Vorfeld konkreter Bedrohungen bestimmter Rechtsgüter flankiert und erweitert, in dieser Hinsicht geht es über den Schutz der Privatsphäre hinaus.[224] Eine aufgrund dieses Rechts zu schützende Persönlichkeitsgefährdung kann insb. dann entstehen, wenn personenbezogene Informationen in einer Art und Weise genutzt und verknüpft werden können, die der Betroffene weder überschauen noch verhindern kann.[225] Das heißt, dass heute die Verhaltensfreiheit, die über ein grundrechtlich geschütztes Geheimhaltungsinteresse hinausgeht, durch elektronische Datenverarbeitung beeinträchtigt werden kann.[226] In dieser Hinsicht kann in der modernen Informationsgesellschaft auch ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen, insoweit gibt es kein belangloses Datum mehr.[227] Zum Schluss beschränkt sich der Schutzumfang des Rechts auf informationelle Selbstbestimmung nicht auf Informationen, die bereits ihrer Art nach sensibel sind und schon deshalb grundrechtlich geschützt werden.[228]

Da der Schutz der Persönlichkeit bei der Datenverarbeitung „Datenschutz" darstellt,[229] muss die Selbstbestimmung personenbezogener Daten auch unter modernen Bedingungen der Datenverarbeitung aufrechterhalten werden können. Aus dieser Sicht ist das Recht auf informationelle Selbstbestimmung eine normative Barriere gegen alle Tendenzen, den Einzelnen in ein bloßes Informationsobjekt zu verwandeln.[230] Somit sind strenge gesetzliche Anforderungen für seine Einschränkung notwendig, die in dieser Entscheidung am wichtigsten sind.[231]

---

gelgesang, Grundrecht auf informationelle Selbstbestimmung?, 45 f.). In dieser Hinsicht ist das Recht teilweise Ausprägung eines sich an moderne Entwicklungen anpassenden Persönlichkeitsschutzes, dabei handelt es sich nicht um ein neues Grundrecht, sondern um die interpretatorische Fortschreibung des Selbstdarstellungsschutzes aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG (*Di Fabio*, in: Maunz/Dürig, GG-K, Art. 2 Abs. 1 Rn. 173; *Simitis*, NJW 1984, 398).

[224] *BVerfGE* 120, 274, 311 f. [Rn. 198].

[225] *BVerfGE* 120, 274, 312. Der Verarbeitungsprozess personenbezogener Daten muss daher in jedem Fall für ihn durchschaubar und nachvollziehbar sein (*Simitis*, NJW 1984, 398, 400).

[226] *BVerfGE* 65, 1, 42; 113, 29, 45 f.; 115, 320, 342; 120, 274, 312 [Rn. 199]; NJW 2007, 2464, 2466.

[227] *BVerfGE* 65, 1, 45.

[228] *BVerfGE* 118, 168, 184 f.; 120, 274, 312 [Rn. 198 a. E.].

[229] *Hofmann*, in: Schmidt-Bleibtreu/Hofmann/Henneke, K zum GG, Art. 2 Rn. 16.

[230] *Simitis*, NJW 1984, 398, 399.

[231] Vgl. *Simitis*, NJW 1984, 398, 400: „*Die wohl wichtigste Konsequenz ist in der Entscheidung des BVerfG deutlich ausgesprochen: Der einzelne mag nicht umhin können, Einschränkungen seiner informationellen Selbstbestimmung hinzunehmen, sie sind freilich gesetzlich abzusichern.*"

b) Eingriffsschwellen

Das Recht auf informationelle Selbstbestimmung kann im überwiegenden Allgemeininteresse beschränkt werden, wobei die rechtliche Grundlage dieser Beschränkungen u. a. organisatorische/verfahrensrechtliche Vorkehrungen enthalten muss, um neuartigen Gefährdungen zu begegnen, die sich aus automatischer und elektronischer Datenverarbeitung ergeben.[232] Insofern hat das *BVerfG* im Volkszählungsurteil die Intensität der Verletzung des Grundrechts je nach Art und Weise der Erhebung personenbezogener Daten unterschiedlich bewertet und nach dem Verhältnismäßigkeitsgrundsatz auch die Voraussetzungen jeder Beschränkung unterschiedlich aufgezeigt.[233] So wird die Eingriffsintensität abgestuft und die Erhebung und Verwendung individualisierter oder individualisierbarer Daten ist – anders als die Erhebung anonymisierter Daten für statistische Zwecke – nur unter besonders strengen Anforderungen zu rechtfertigen.[234] In diesem Fall müssen weitere verfahrensrechtliche Schutzvorkehrungen wie Aufklärungs-, Auskunfts-, Löschungspflichten etc. getroffen werden, u. a. ist für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung unter den Bedingungen der automatischen Datenverarbeitung eine Beteiligung „unabhängiger Datenschutzbeauftragter" von Bedeutung.[235] Dies bedeutet, dass bei staatlicher Erhebung und Verwendung personenbezogener Daten – neben gerichtlicher Kontrolle – eine administrative aufsichtliche Kontrolle durch eine unabhängige Stelle i. d. R. erforderlich ist.

2. Computer-Grundrecht: Urteil zur Online-Durchsuchung

a) Erkenntnis- bzw. Erwägungsgründe und Schutzbereich

Im Jahr 2008 hat das *BVerfG* in dem sog. „Urteil zur Online-Durchsuchung" über die Verfassungsbeschwerden gegen § 5 Abs. 2 Nr. 11 S. 1 Alt. 2 NWVerfSchG a. F., der den „heimlichen Zugriff auf informationstechnische Systeme" zuließ, erklärt, dass im Zuge des wissenschaftlich-technischen Fortschritts und gewandelter Lebensverhältnisse über herkömmliche Ausprägungen des allgemeinen Persönlichkeitsrechts hinaus eine neue Ausprägung erforderlich ist, um neuartigen Gefährdungen der Persönlichkeit zu begegnen und die Lücken ihres grundrechtlichen Schutzes auszufüllen. Dafür hat es das sog. Computer-Grundrecht, nämlich das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, geschaffen. In der Urteilsbegründung hat das Gericht – vor der Entscheidung über die Verfassungsmäßigkeit der verdeckten Online-Durchsuchung und deren gesetzlicher Ermächtigungsgrundlage – als technischen und sozialen Hintergrund die Bedeutung der informationstechnischen Systeme in der modernen

[232] *BVerfGE* 65, 1, 44; 115, 320, 344 ff.

[233] *BVerfGE* 65, 1, 45 ff.

[234] *Di Fabio*, in: Maunz/Dürig, GG-K, Art. 2 Abs. 1 Rn. 184.

[235] *BVerfGE* 65, 1, 45 f.

Informationsgesellschaft ausführlich erläutert:[236] Hiernach ermöglicht heute der Zugriff auf diese vernetzten Systeme, die eine noch größere Vielzahl und Vielfalt von Daten im Vergleich zu einem alleinstehenden System erzeugen, verarbeiten und speichern können, weitreichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung und kann weitgehende Kenntnisse über diese gewinnen,[237] jedoch ist es für den Einzelnen, zumindest den durchschnittlichen Nutzer, übertrieben und praktisch unmöglich, ein solches Risiko wirksam auszuschließen.[238] Daraus folgt zwar ein erhebliches Schutzbedürfnis für die informationstechnischen Systeme als solche und ihre Nutzung, aber dies kann mit den anderen Grundrechten – einschließlich des informationellen Selbstbestimmungsrechts – nicht hinreichend berücksichtigt werden.[239] Deshalb sei ein neues Konzept, nämlich ein Computer-Grundrecht, erforderlich, um einen wirksamen Schutz der Persönlichkeit unter den derzeitigen technischen und sozialen Bedingungen weiter zu gewährleisten.[240] Kurz gesagt, ist ein direkter Grund für die Anerkennung dieses Grundrechts, dass in der modernen Informationsgesellschaft, in der alle wichtigen Informationen einer Person umfassend in vernetzten informationstechnischen Systemen gespeichert werden, der Schutz der Persönlichkeit unmöglich ist, ohne die Vertraulichkeit und Integrität der Systeme zu schützen.

Das Computer-Grundrecht ist eine Abwehr gegen neue Persönlichkeitsgefährdungen, die nicht mit den bestehenden Grundrechten abgedeckt werden können. Nach Angaben des *BVerfG* werden durch einen Zugriff auf das informationstechnische System die Nutzungen des Systems als solche überwacht, die Speichermedien des Systems durchsucht[241] oder personenbezogene Daten in einem Umfang und in einer Vielfalt erhoben, die es ermöglichen, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person oder ein aussagekräftiges Bild der Persönlichkeit zu erhalten,[242] daher muss dies vom Grundrecht geschützt werden. Allerdings sollten nicht alle informationstechnischen Systeme, die personenbezogene Daten erzeugen, verarbeiten oder speichern können, durch dieses Grundrecht besonders geschützt werden.[243] Kann aber ein einmaliger Zugriff auf ein solches System zur Verschaffung eines potenziell äußerst großen und aussagekräftigen Datenbestands führen, ohne noch auf weitere Datenerhebung und -verarbeitung angewiesen zu sein, so übertrifft dies einzelne Datenerhebungen an Eingriffsintensität.[244] Das Grundrecht zielt auf einen grundrechtlichen Schutz auf den dem Einzelnen zustehenden Cyberspace –

[236] *BVerfGE* 120, 274, 303–306.
[237] *BVerfGE* 120, 274, 305 f.
[238] *BVerfGE* 120, 274, 306.
[239] *BVerfGE* 120, 274, 306–313.
[240] *BVerfGE* 120, 274, 313.
[241] *BVerfGE* 120, 274, 308 [Rn. 186].
[242] *BVerfGE* 120, 274, 314 [Rn. 203].
[243] *BVerfGE* 120, 274, 313 [Rn. 202].
[244] *BVerfGE* 120, 274, 313 [Rn. 200].

über einzelne Kommunikationsvorgänge oder gespeicherte Daten hinaus – ähnlich der Unverletzlichkeit des Wohnraums.

b) Eingriffsschwellen

Das Computer-Grundrecht ist nicht schrankenlos und kann zu präventiven Zwecken oder zur Strafverfolgung beschränkt werden. Insoweit hat aber das *BVerfG* u. a. erhöhte Eingriffsvoraussetzungen und Verfahrensvorkehrungen verlangt, die nach der Gesamtabwägung dem Grundrechtseingriff von hoher Intensität, der im heimlichen Zugriff auf ein informationstechnisches System liegt,[245] entsprechen.[246] Hierbei wird betont, dass hinreichende gesetzliche Vorkehrungen gegen die Gefahr, dass den absolut geschützten Kernbereich privater Lebensgestaltung betreffende Daten erhoben werden, erforderlich sind,[247] insofern wurde das zweistufige Schutzkonzept erklärt (vgl. oben II. 2. b)).

3. Verfassungsrechtliche Kriterien zum Datenschutz

Das *BVerfG* hat für den Schutz der Persönlichkeitssphäre anfänglich nur auf das allgemeine Persönlichkeitsrecht zurückgegriffen, doch danach durch seine speziellen Ausprägungen daraus das informationelle Selbstbestimmungsrecht und das Computer-Grundrecht nacheinander hergeleitet. Obwohl sich Zeitpunkte und Hintergründe der Schaffung jedes Grundrechts unterscheiden (z. B. das Niveau der IuK-Technologie, das Bewusstsein der Bürger über personenbezogene Daten etc.), sind die beiden Grundrechte im Wesentlichen auf den Persönlichkeitsschutz durch Beschränkung der Ausforschung der Persönlichkeit durch unbegrenzte Erhebung, Speicherung und Verwendung personenbezogener Daten ausgerichtet. Während das Computer-Grundrecht den Persönlichkeitsschutz darstellt, der ein persönliches digitales Endgerät voraussetzt, betrifft das informationelle Selbstbestimmungsrecht der Persönlichkeitsschutz den Schutz der Daten selbst. Nach der weichenstellenden Entscheidung hat das Recht auf informationelle Selbstbestimmung durch ständige Rspr. des *BVerfG* die Handlungsfreiheit und den Schutz der Privatsphäre erweitert, die nur im Einzelnen geschützt wurden. Mittlerweile hat sich das Grundrecht mit der rasanten Entwicklung der IT und der Förderung des Bewusstseins der Bürger für den Datenschutz zu einem starken Geäst des allgemeinen Persönlichkeitsrechts ausgewachsen[248], und der Datenschutz hat dadurch einen Verfassungsrang erhalten.[249] Obwohl das Gericht dieses Grundrecht ursprünglich im Blick auf neuartige Gefahren der automatisierten Datenverarbeitung entwickelt hat, schützt es nun darüber hinaus

[245] *BVerfGE* 120, 274, 322 ff. [Rn. 229 ff.].
[246] *BVerfGE* 120, 274, 326 ff. [Rn. 242 ff.].
[247] *BVerfGE* 120, 274, 335 ff. [Rn. 270 ff.].
[248] *Herdegen*, in: Maunz/Dürig, GG-K, Art. 1 Abs. 1 Rn. 84.
[249] *Vogelgesang*, CR 1995, 554, 555: verfassungsrechtliche Weihen.

vor jeder Form von Erhebung, Kenntnisnahme, Speicherung, Verwendung, Weitergabe und Veröffentlichung personenbezogener Daten, einschließlich der manuellen.[250] Angesichts heutiger informationstechnischer Gegebenheiten kann der Schutzbereich dieses Rechts – ebenso wie ein solcher des allgemeinen Persönlichkeitsrechts – nicht endgültig festgelegt werden, und es fungiert als Auffang-Grundrecht im Verhältnis zu anderen Grundrechten, insb. dem Schutz des Fernmeldegeheimnisses und der Unverletzlichkeit der Wohnung. Das informationelle Selbstbestimmungsrecht stellt heutzutage das „Grundrecht auf Datenschutz" dar.[251] Bis heute wurde dieses weitsichtige verfassungsrechtliche Datenschutzkonzept des *BVerfG* so weit entwickelt, dass es insb. bezüglich des staatlichen Datenzugriffs im Bereich des Polizei- und Sicherheitsrechts und auch der Strafverfolgung umfängliche Umbauarbeiten erforderlich macht.[252]

Das informationelle Selbstbestimmungsrecht hat einen festen Stellenwert bezüglich des Datenschutzes erlangt, und auch dessen Anwendungsbereich ist bereits erheblich erweitert. Dennoch hat das *BVerfG* darüber hinaus das Computer-Grundrecht anerkannt, weil unter den aktuellen technischen und sozialen Gegebenheiten der Schutz vor staatlichen Zugriffen auf informationstechnische Systeme und Datenbestände, auf denen personenbezogene Daten umfangreich gespeichert sind, grundrechtlich besonders gewährleistet werden muss. Insb. die Nutzung des Internets als konvergiertes Netzwerk und die Verbreitung der PCs und Smartphones als konvergente Informations- und Kommunikationsgeräte haben das bestehende Verständnis von Verletzungen und Schutz der Persönlichkeit grundlegend geändert. Allerdings wird die Schöpfung dieses Rechts im Schrifttum teilweise kritisiert.[253] Angesichts der weiteren Entwicklung der IuK-Technologie und der damit verbun-

[250] *BVerfGE* 67, 100, 143; 78, 77, 84; 103, 21, 32 f.; 113, 29, 45 f.; 115, 166, 190; 115, 320, 341 f.; 118, 168, 183 f.; 120, 378, 397; 130, 151, 178 ff. m. w. N.; *Di Fabio*, in: Maunz/Dürig, GG-K, Art. 2 Abs. 1 Rn. 176; *Vogelgesang*, Grundrecht auf informationelle Selbstbestimmung?, 25 f. und 55 f.

[251] *BVerfGE* 84, 239, 280 [Rn. 138]: auch *Simitis*, NJW 1984, 398, 399 [Tz. II]: „*Das Recht ist die Antwort des BVerfG auf die Frage nach der verfassungsrechtlichen Grundlage des Datenschutzes.*" Auf Bundesländerebene enthalten nur die Verfassungen einiger Bundesländer selbstständige Datenschutzvorschriften: Art. 11 Verfassung des Landes Brandenburg, Art. 33 Verfassung des Freistaates Sachsen, Art. 6 Abs. 2 Verfassung des Freistaats Thüringen, Art. 6 Abs. 1 Verfassung des Landes Mecklenburg-Vorpommern, Art. 33 Verfassung von Berlin, Art. 4 Abs. 2 Verfassung für das Land Nordrhein-Westfalen, Art. 2 S. 2 – 3 Verfassung des Saarlandes (vgl. *Vogelgesang*, CR 1995, 554, 556 ff.). Dies darf aber in sonstigen Bundesländern nicht zur Missachtung des informationellen Selbstbestimmungsrechts führen (a. a. O. 560).

[252] *Gurlit*, NJW 2010, 1035: insb. *Hamm*, StV 2001, 81, 82: Das Volkszählungsurteil, das Bestimmtheits- und Klarheitsgebot zu betonen, trug wesentlich dazu bei, dass der Gesetzgeber viele neue Eingriffsermächtigungen für die *praeter legem* längst praktizierten verdeckten Ermittlungsmethoden schafft.

[253] Vgl. *Gurlit*, NJW 2010, 1035, 1037: Der Anwendungsbereich des informationellen Selbstbestimmungsrechts wird durch die Schaffung des Computer-Grundrechts unvertretbar auf einzelne Datenerhebungen reduziert; abw. *Kutscha*, NJW 2008, 1042, 1043: Der Schutzumfang dieses Grundrechts ist noch alles andere als eindeutig.

denen Möglichkeit einer vollständigen Überwachung ist jedoch die Grundidee, die den Hintergrund für diese Neuschöpfung bildete, sinnvoll. In Zukunft wird sich der Anwendungsbereich dieses Grundrechts erheblich erweitern.[254]

IV. Der Schutz des Fernmeldegeheimnisses: Art. 10 GG

1. Spezifischer Schutzbedarf

Leitgedanke des Art. 10 GG ist der verfassungsrechtliche Schutz von Kommunikation über räumliche Distanzen hinweg. Nachrichten, die durch ein Kommunikationsmedium übermittelt werden, sind den erleichterten Zugriffsmöglichkeiten Dritter – auch des Staates – ausgesetzt[255] und aus dieser besonderen Gefährdungslagen des kommunikativen Übermittlungsvorgangs[256] ergibt sich die besondere Schutzbedürftigkeit.[257] Der Schutzzweck der Vorschrift ist – nicht die Möglichkeit des Kommunizierens, sondern – die Vertraulichkeit des Kommunikationsvorgangs, nämlich eines privaten, vor der Öffentlichkeit verborgenen Austausches von Informationen.[258] So erfolgen Eingriffe in den Schutz des Fernmeldegeheimnisses typischerweise heimlich, also ohne Wissen des Grundrechtsträgers.[259] Dieses Grundrecht sichert andererseits einen Teilausschnitt des grundrechtlichen Schutzes der Privatsphäre mittelbar und dient so dem Persönlichkeitsschutz.[260] Aus diesem Grund hat es in der modernen Informationsgesellschaft eine besondere Bedeutung im Grundrechtesystem erlangt und nimmt im GG hohen Rang ein.[261]

---

[254] Auch *Kutscha*, NJW 2008, 1042, 1043.

[255] Vgl. *BVerfGE* 115, 166, 184: „*Das Fernmeldegeheimnis knüpft an das Kommunikationsmedium an.*“

[256] Vgl. *BVerfGE* 115, 166, 182 ff.; *Durner*, in: Maunz/Dürig, GG-K, Art. 10 Rn. 43.

[257] Vgl. *BVerfGE* 100, 313, 358; 129, 208, 241 [Rn. 198].

[258] *BVerfGE* 67, 157, 171 [Rn. 51]; 115, 166, 182 [Rn. 64]; *Durner*, in: Maunz/Dürig, GG-K, Art. 10 Rn. 49 f.; *Sodan*, GG, Art. 10 Rn. 1. Heutzutage spricht Art. 10 Abs. 1 GG nicht vom Schutz des Fernmelde-„Verkehrs“, sondern vom Fernmelde-„Geheimnis“ (*Klesczewski*, ZStW 123 (2011), 737, 751; *Zimmermann*, JA 5/2014, 321, 324).

[259] *BVerGE* 107, 299, 321; *Durner*, in: Maunz/Dürig, GG-K, Art. 10 Rn. 43.

[260] *Durner*, in: Maunz/Dürig, GG-K, Art. 10 Rn. 41. Daher stellen sie den wesentlichen Bestandteil des Schutzes der Privatsphäre dar (*BVerfGE* 115, 166, 182 [Rn. 65]).

[261] *BVerfGE* 67, 157, 171 [Rn. 51]; 115, 166, 182 [Rn. 64]; *Baldus*, in: Epping/Hillgruber, BeckOK GG, Art. 10 Rn. 1; *Durner*, in: Maunz/Dürig, GG-K, Art. 10 Rn. 1 und dazu 42: „*sind die in Art. 10 Abs. 1 GG verbürgten Grundrechte in ihrem Kern Ausdruck der Menschenwürdegarantie des Art. 1 GG*“.

2. Schutzbereich

Das Fernmeldegeheimnis schützt die unkörperliche Übermittlung von Informationen an individuelle Empfänger mithilfe des Kommunikationsverkehrs,[262] der Schutz bezieht sich auf alle mittels der Fernmeldetechnik ausgetauschten Kommunikationen.[263] Die Gewährleistung der Vertraulichkeit räumlich distanzierter Kommunikation hat sich im Laufe der historischen Entwicklung von der Vertraulichkeit des Postverkehrs gegenwärtig bis hin zum Kommunikationsgeheimnis, insbesondere dem Telekommunikationsgeheimnis erweitert.[264] Dass personenbezogene Daten Dritten anvertraut werden, war früher nur bei Post, Telegraf und Telefon denkbar, ihre Menge war auch begrenzt. Heute, wo IuK-Technologie in alle Lebensbereiche eindringt, ist aber die Erweiterung der Reichweite des Art. 10 GG unvermeidlich und erforderlich. So erstreckt sich derzeit sein Schutzbereich auf alle Arten verfügbarer TK ungeachtet der Übertragungsart (Kabel, Funk, analog oder digital) und der Ausdrucksformen (Sprache, Bilder, Töne, Zeichen), einschließlich des Internets.[265] I. R. d. elektronischen Kommunikation sind der primäre Schutzgegenstand des Art. 10 Abs. 1 GG traditionell die Inhaltsdaten,[266] jedoch wird in den letzten Jahren auch der Wert von Verkehrs- und Standortdaten[267] immer wichtiger (vgl. oben A. I. 2. a)). Das *BVerfG* hat auch in Kenntnis des technologischen Fortschritts den Schutzbereich dieses Grundrechtes weiter ausgebaut.[268] Der Schutz des Fernmeldegeheimnisses ist noch entwicklungsoffen[269] und ständig zu aktualisieren, um potenziellen neuen Persönlichkeitsverletzungen zu begegnen.

Hierbei zählen i. R. d. digitalen TK die von dem Gerät ausgehenden technischen Signale zur Gewährleistung der Kommunikationsbereitschaft nicht zum Fernmeldegeheimnis i. S. d. GG Art. 10 Abs. 1, weil sie keine Kommunikationsinhalte und -umstände betreffen, – anders als Kommunikationsumstände – keinen Rückschluss auf Kommunikationsbeziehungen und -inhalte ermöglichen[270] und der Schutz des Fernmeldegeheimnisses personal an der Schutzbedürftigkeit aufgrund der Einschaltung Dritter in den Kommunikationsvorgang anknüpft.[271] So setzt die TK das Vorhandensein eines menschlichen Kommunikationspartners voraus. Dabei geht es u. a. um die Positionsmeldungen eines aktiv geschalteten, aber nicht telefonierenden

---

[262] *BVerfGE* 67, 157, 172; 106, 28, 35 f.; 115, 166, 182; 120, 274, 306 f.; 124, 43, 54.

[263] *BVerfGE* 100, 313 358; 107, 299, 313; 110, 33, 53; 113, 348, 364 f.

[264] *Durner*, in: Maunz/Dürig, GG-K, Art. 10 Rn. 7 ff.

[265] *BverfGE*, 113, 348, 383; 120, 274, 307; 124, 43, 54.

[266] Vgl. *BverfGE* 100, 313, 358; 106, 28, 36; 113, 348, 364; 115, 166, 182 f.; 124, 43, 54.

[267] Vgl. *BverfGE* 67, 157, 172; 100, 313, 358; 107, 299, 312; 113, 348, 364; 125, 260, 309 m. w. N.

[268] *Gurlit*, NJW 2010, 1035, 1036.

[269] *BVerfGE* 115, 166, 182.

[270] *BVerfG*, NJW 2007, 351, 353 [Rn. 57].

[271] *BVerfG*, NJW 2007, 351, 354 [Rn. 59]; *BGH*, NStZ 2018, 611, 612; a. A. *BGH-Ermi-Ri*, NJW 2001, 1587.

Mobilfunkendgeräts (vgl. § 100g Abs. 1 S. 4 StPO) und die Maßnahme nach § 100i StPO.

Bezüglich der Eröffnung des Schutzbereichs von Art. 10 Abs. 1 GG sollen heutzutage die neuen Gegebenheiten der Verwendung der IT, insb. Ansammlung und Konzentration von Daten (vgl. oben A. I. 2) berücksichtigt werden. So sind unter der modernen Informationstechnologie schutzwürdige Kommunikationen nicht mehr unbedingt dynamisch. Obwohl technische (Tele-)Kommunikationen noch flüssig sind, unterliegt ausschließlich dieser Zustand nicht dem Schutz des Fernmeldegeheimnisses. I. d. R. endet der Schutz des Fernmeldegeheimnisses bezüglich der TK-Daten – im laufenden Kommunikationsvorgang – in dem Moment, in dem die Nachricht beim Empfänger angekommen und der Übertragungsvorgang beendet ist (sog. „technikvergleichende Theorie").[272] Jedoch hängt er heute davon ab, in welchem Bereich die TK-Daten vorhanden sind und ob die TK-Teilnehmer selbst dort Schutzvorkehrungen treffen können. Dabei kommt die Kenntnisnahme des Nachrichteninhalts durch Empfänger nicht in Betracht, weil sie nichts mit einer besonderen Gefahrenlage aufgrund der Einschaltung Dritter zu tun hat. Konsequenterweise gilt dieser Schutz unabhängig davon, ob eine Nachricht gesendet oder empfangen sowie gelesen oder ungelesen, d. h. zwischen- oder endgespeichert ist.[273] Daraus soll i. R. d. Abgrenzung des Schutzbereichs des Art. 10 Abs. 1 GG der „Herrschaftsbereich/Beherrschbarkeit", bei dem es sich darum handelt, ob der Kommunikationsteilnehmer eigene Schutzmaßnahmen gegen den unerwünschten Zugriff Dritter ergreifen kann, ausschlaggebendes Kriterium sein;[274] sog. „schutzfunktionale Theorie".[275] Der Schutz des Fernmeldegeheimnisses beginnt ab dem Zeitpunkt, wo die Daten des Grundrechtsträgers im Bereich des ISP, nämlich seinem Server, verlassen (gespeichert) werden, und kommt erst dann zu Ende, wenn sie vollständig und endgültig aus ihm gelöscht sind.[276]

---

[272] *BVerfGE* 115, 166, 184; 120, 274, 307 f.; 124, 43, 54.

[273] *BVerfGE* 124, 43, 55; *Brodowski*, JR 2009, 402, 405; *Gaede*, StV 2009, 96, 97; *Kasiske*, StraFo 6/2010, 228, 229 f.; *Klesczewski*, ZStW 123 (2011), 737, 747; *Neuhöfer*, JR 2015, 21, 23; abw. *Sankol*, MMR 2007, 169, 170: Der Kommunikationsvorgang als solcher ist mit dem Ruhen einer E-Mail auf einem ISP-Server noch nicht vollständig beendet, sondern kommt nur vorübergehend zum Stillstand, und wird daher nicht von Art. 10 Abs. 1 GG erfasst (sog. „technische-funktionale Theorie"; vgl. unter Verweis auf *Brodowski*, JR 2009, 402, 404).

[274] Vgl. *BVerfGE* 115, 166, 183 ff.; 120, 274, 307 f.; insb. 124, 43, 55 f. [Rn. 47 f.]: „*Art. 10 Abs. 1 GG folgt indes nicht dem rein technischen Telekommunikationsbegriff des TKG, sondern knüpft an den Grundrechtsträger und dessen Schutzbedürftigkeit aufgrund der Einschaltung Dritter in den Kommunikationsvorgang an. … Ob Art. 10 Abs. 1 GG Schutz vor Zugriffen bietet, ist mit Blick auf den Zweck der Freiheitsverbürgung unter Berücksichtigung der spezifischen Gefährdungslage zu bestimmen. Die spezifische Gefährdungslage und der Zweck der Freiheitsverbürgung von Art. 10 Abs. 1 GG bestehen auch dann weiter, wenn die E-Mails nach Kenntnisnahme beim Provider gespeichert bleiben*"; zust. *Brodowski*, JR 2009, 402, 405; *Kasiske*, StraFo 6/2010, 228, 229.

[275] Vgl. *Brodowski*, JR 2009, 402, 403 ff.

[276] *Kudlich*, GA 2011, 193, 202; *Neuhöfer*, JR 2015, 21, 23.

Zum anderen sollte zwischen TKÜ von außen und Teilnahme an der TK unterschieden werden.[277] Das Grundrecht des Art. 10 Abs. 1 GG schützt lediglich das Vertrauen des Einzelnen darin, dass eine Fernkommunikation, an der er beteiligt ist, nicht von Dritten zur Kenntnis genommen wird. Dagegen ist das Vertrauen der Kommunikationspartner zueinander nicht Gegenstand des Grundrechtsschutzes.[278] Wenn daher nur einer von mehreren Beteiligten der Ermittlungsbehörde seinen Zugangscode freiwillig herausgibt, liegt kein Eingriff in das Telekommunikationsgeheimnis vor, und sie kann zu Recht die Kommunikationsinhalte erfassen (vgl.: Es ist bloß eine Enttäuschung des personengebundenen Vertrauens in den Kommunikationspartner).[279] Auf dem technisch vorgesehenen Weg, aber unautorisiert, d. h. mit der Ausnutzung eines ohne oder gegen den Willen der Kommunikationsbeteiligten (z. B. mittels Keylogging) erhobenen Zugangsschlüssels, zugangsgesicherte Kommunikationsinhalte zu überwachen, ist dagegen keine Teilnahme an der TK, sondern eine TKÜ,[280] hierfür bedarf es einer speziellen Ermächtigung.[281]

3. Verhältnis zum allgemeinen Persönlichkeitsrecht

Im Hinblick darauf, dass der Schutz des Fernmeldegeheimnisses in Art. 10 Abs. 1 GG im Wesentlichen durch den Schutz personenbezogener Daten die Menschenwürde und die Persönlichkeitsentfaltung gewährleistet, steht er in engem Verhältnis zum allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG (vgl. oben 1.). Soweit ein Eingriff in Fernkommunikation die Erhebung personenbezogener Daten betrifft, ist Art. 10 Abs. 1 GG gegenüber dem informationellen Selbstbestimmungsrecht eine besondere Garantie (Spezialitäts- oder Ergänzungsverhältnis).[282] Dies gilt auch für das Computer-Grundrecht.[283] Schließlich werden kommunikationsrelevante personenbezogene Daten vorrangig durch Art. 10 Abs. 1 GG geschützt und, soweit dies aus dessen Auslegung nicht möglich ist, durch das allgemeine Persönlichkeitsrecht.[284]

Bei der Abgrenzung des Anwendungsbereichs zwischen dem Schutz des Fernmeldegeheimnisses und dem allgemeinen Persönlichkeitsrecht handelt es sich in der Fallkonstellation um den Schutz von den Inhalts- oder Verkehrsdaten, die nach Abschluss des Übertragungsvorgangs im informationstechnischen System des

---

[277] *Singelnstein*, NStZ 2012, 593, 600.

[278] *BVerfGE* 120, 274 340.

[279] *BVerfGE* 120, 274 341 [Rn. 291 und 293].

[280] *BVerfGE* 120, 274 341 [Rn. 291 f.].

[281] Vgl. § 100a: *Klesczewski*, ZStW 123 (2011), 737, 752; M-G/*Schmitt*, StPO, § 100a Rn. 7; *Singelnstein*, NStZ 2012, 593, 600.

[282] *BVerfGE* 67, 157, 171; 100, 313, 358; 107, 299, 312; 115, 166, 188 f.; 124, 43, 56 f.; 125, 260, 310.

[283] *BVerfGE* 120, 274, 302 [Rn. 167].

[284] Vgl. *Durner*, in: Maunz/Dürig, GG-K, Art. 10 Rn. 56.

Kommunikationsteilnehmers oder im Server des Anbieters gespeichert sind. Dabei ist der Schutzbereich des Art. 10 GG primär festzulegen, hier ist der Herrschaftsbereich von entscheidender Bedeutung[285], und daher werden die auf dem „Server der Anbieter" vorhandenen Daten i. d. R. durch das Fernmeldegeheimnisses geschützt.[286] Sind die Daten auf dem „informationstechnischen System des Betroffenen" gespeichert, werden sie dagegen deshalb nach der Offenheit oder der Heimlichkeit des Zugriffs von dem informationellen Selbstbestimmungsrecht oder dem Computer-Grundrecht geschützt, weil es keinen technisch bedingten Mangel an Beherrschbarkeit gibt.[287]

V. Unverletzlichkeit der Wohnung: Art. 13 GG

1. Schutzbereich und Eingriffsart

Die Unverletzlichkeit der Wohnung des Art. 13 Abs. 1 GG (vgl. das Recht auf Achtung der Wohnung von Art. 8 Abs. 1 EMRK und Art. 7 GRCh) schützt die räumliche Privatsphäre.[288] Der Schutz von elementaren Lebensräumen dient ausdrücklich der Menschenwürdegarantie und dem Persönlichkeitsschutz.[289] Dieser Schutz stellt – wie der Schutz des Art. 10 GG – eine spezielle Gewährleistung gegenüber dem allgemeinen Persönlichkeitsrecht dar (*lex specialis*).[290] Neben allen privaten Wohnzwecken gewidmeten Räumlichkeiten wie z. B. Privatwohnungen fallen auch Betriebs- und Geschäftsräume in den Schutzbereich.[291] Träger dieses Grundrechts ist jeder Inhaber oder Bewohner eines Wohnraums, unabhängig davon, auf welchen Rechtsverhältnissen die Nutzung des Raums beruht,[292] dazu gehört jedoch der zufällig in einer Wohnung Anwesende nicht.

Eingriffe in das Grundrecht der Unverletzlichkeit der Wohnung beschränken sich heute nicht auf das körperliche Eindringen (Betreten) in die geschützten Räume

---

[285] Vgl. BT-Drs. 18/12785, S. 49: Der Schutzbereich des Art. 10 GG wird vom Schutzbereich des Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG nach „Herrschaftssphären" abgegrenzt.

[286] *BVerfGE* 124, 43, 54 f.

[287] *BVerfGE* 115, 166, 183 f.; a. A. *Kutscha*, LKV 2008, 481, 485: Sämtliche individualbezogenen Verkehrsdaten sollten unabhängig vom Ort ihrer Speicherung vom Art. 10 GG geschützt werden.

[288] *BVerfGE* 7, 230, 238; 65, 1, 40; 109, 279, 309: vgl. 103, 142, 150 f.; 120, 274, 309: die räumliche Sphäre, in der sich das Privatleben entfaltet.

[289] *BVerfGE* 109, 279, 313; *Kluckert*/*Fink*, in: Epping/Hillgruber, BeckOK GG, Art. 13 Rn. 1; *Papier*, in: Maunz/Dürig, GG-K, Art. 13 Rn. 1.

[290] *BVerfGE* 109, 279, 325; 115, 166, 187; 115, 320, 347; *Papier*, in: Maunz/Dürig, GG-K, Art. 13 Rn. 1.

[291] *BVerfGE* 96, 44, 51; 120, 274, 309 [Rn. 192]; *Kluckert*/*Fink*, in: Epping/Hillgruber, BeckOK GG, Art. 13 Rn. 1 und 3; *Papier*, in: Maunz/Dürig, GG-K, Art. 13 Rn. 10, 13 und 144.

[292] *BVerfGE* 109, 279, 326 [Rn. 162]: Bei mehreren Bewohnern einer Wohnung steht das Grundrecht jedem Einzelnen, bei Familien mithin jedem Familienmitglied zu.

gegen den Willen des Berechtigten.[293] Mit der Entwicklung der Technologien sind sie auch auf andere Weise möglich, insb. durch das Durchsehen oder Belauschen der Vorgänge in der Wohnung mit besonderen Hilfsmitteln, nämlich die „Wohnraumüberwachung mit technischen Mitteln".[294] Sie können in Form akustischer oder optischer Wohnraumüberwachung erfolgen, einerlei, ob sie durch technische Mittel erfolgt, die in den geschützten Räumen angebracht oder von außerhalb der Wohnung eingesetzt werden:[295] etwa über PCs oder Smartphones, auf denen Spyware installiert sind, unter Nutzung von Richtmikrophonen oder durch die Messung elektromagnetischer Abstrahlungen.[296] Das Grundrecht auf Unverletzlichkeit der Wohnung gilt aber nur insoweit, als die Überwachung von außen solche innerhalb der Wohnung stattfindenden Vorgänge erfasst, die der natürlichen Wahrnehmung von außerhalb des geschützten Bereichs entzogen sind.[297] Zum anderen, wenn der Zugriff auf das informationstechnische System als Begleiteingriff zur Wohnraumüberwachung „über das mit dem System verbundene Netzwerk" – heimlich – erfolgt, nämlich bei der Online-Durchsuchung, lässt er die durch die Abgrenzung der Wohnung vermittelte räumliche Privatsphäre unberührt; dieser Eingriff erfolgt unabhängig vom Standort des Systems.[298] Der grundrechtliche Schutz vor diesem Eingriff muss durch das Computer-Grundrecht geschützt werden (vgl. oben III. 2.).[299]

2. Verhältnis zu sonstigen Grundrechten

Der Schutzbereich des Art. 13 Abs. 1 GG muss von demjenigen des informationellen Selbstbestimmungsrechts und des Telekommunikationsgeheimnisses abgegrenzt werden. Dies ist vor allem dann problematisch, wenn Mitarbeiter der Strafverfolgungsbehörde in die Wohnung eindringen, um dort befindliche Papiere und informationstechnische Systeme oder die auf ihnen gespeicherten Daten zu

[293] *BVerfGE* 109, 279, 327 [Rn. 165]; 120, 274, 309 [Rn. 192]; *Kluckert*/*Fink*, in: Epping/Hillgruber, BeckOK GG, Art. 13 Rn. 6.

[294] *BVerfGE* 109, 279, 327 [Rn. 165]; 120, 274, 309 f. [Rn. 192 f.]. Unter heutigen technischen Gegebenheiten würde der Schutzzweck dieses Grundrechts dann vereitelt, wenn eine solche Überwachung der Wohnung (vgl. Art. 13 Abs. 3 bis Abs. 6 GG) nicht von der Gewährleistung des Abs. 1 umfasst wäre (109, 279, 309 [Rn. 105]).

[295] *BVerfGE* 109, 279, 327 [Rn. 166].

[296] *BVerfGE* 109, 279, 327 [Rn. 166]; 120, 274, 310 [Rn. 192 a. E.].

[297] *BVerfGE* 109, 279, 327 [Rn. 166].

[298] *BVerfGE* 120, 274, 310 f. [Rn. 194]: Der Standort ist in vielen Fällen für die Ermittlungsmaßnahme ohne Belang und oftmals für die Behörde nicht einmal erkennbar.

[299] Vgl. die Online-Durchsuchung betrifft als solche nicht das Grundrecht auf Unverletzlichkeit der Wohnung. Die Online- und Wohnungsdurchsuchung unterscheiden sich trotz ihrer sprachlichen Ähnlichkeit durch ihre Gegenstände (reale Räume gegenüber virtuellen Räumen) und sind auch grundrechtlich unterschiedlich (*Kluckert*/*Fink*, in: Epping/Hillgruber, BeckOK GG, Art. 13 Rn. 10). Insbesondere im Hinblick auf die Bedeutung des Cyberspace unter den modernen informationstechnischen Gegebenheiten ist die Eingriffsintensität der Online-Durchsuchung sehr stark und kann solche der akustischen Wohnraumüberwachung übertreffen (vgl. Kapitel 3, A. IV. 3. c) bb)).

durchsuchen, durchzusehen und zu beschlagnahmen. Zwar geht Art. 13 GG als spezielle Garantie grundsätzlich dem allgemeinen Persönlichkeitsrecht vor, jedoch wird er ausnahmsweise dort verdrängt, wo sich jeder Schutzbereich beider Grundrechte nur partiell überschneidet oder wo das allgemeine Persönlichkeitsrecht einen eigenständigen Bereich mit festen Konturen hat.[300] Werden die Wohnräume des Betroffenen im Strafverfahren von Ermittlungspersonen betreten und werden danach die dort vorhandenen Papiere und Daten durchgesehen, sichergestellt und beschlagnahmt (d. h. bei der typischen – offenen – Durchsuchung und Beschlagnahme), so soll sich somit die voraus liegende Wohnungsdurchsuchung und die nachher liegende Durchsicht, Sicherstellung und Beschlagnahme unter grundrechtlichem Gesichtspunkt unterscheiden; Ersteres ist ein Eingriff in das Grundrecht des Art. 13 Abs. 1 GG, Letzteres ist jedoch ein Eingriff in das informationelle Selbstbestimmungsrecht.[301]

3. Beschränkungen

In das Grundrecht in Art. 13 Abs. 1 GG darf nur unter den Voraussetzungen der Abs. 2 bis Abs. 7 eingegriffen werden.[302] Abs. 2 davon ist die verfassungsrechtliche Grundlage für die Durchsuchung im Strafverfolgungsverfahren (§§ 102 ff. StPO)[303] und Abs. 3 ist diejenige für den Einsatz technischer Mittel zur akustischen Überwachung von Wohnungen (§ 100c StPO). Nach dem Art. 13 Abs. 2 GG muss sie grundsätzlich mit dem Richtervorbehalt verbunden sein, ausnahmsweise nur bei Gefahr im Verzuge kann sie auch durch die in den Gesetzen vorgesehenen anderen Organe angeordnet werden, die im Vorverfahren die StA und ihre Ermittlungspersonen darstellen (§ 105 Abs. 1 S. 1 StPO). Da die „akustische Wohnraumüberwachung durch den Einsatz technischer Mittel zum Zweck der Strafverfolgung" in Art. 13 Abs. 3 GG in das Grundrecht – besonders – intensiv eingreift, werden besonders schwere Katalogstraftaten, konkretisierte Verdachtslage und Subsidiarität als Eingriffsvoraussetzungen erfordert (Satz 1) und qualifizierter Richtervorbehalt als Verfahrenskontrolle vorgesehen (Satz 3 bis 4).[304] Außerdem sieht Abs. 6 parlamentarische Kontrolle vor. Nach der Rspr. des *BVerfG* ist die Maßnahme des Art. 13 Abs. 3 GG daneben nur dann mit der Menschenwürdegarantie vereinbar, wenn sie mit einer konkreten Ausgestaltung von Vorkehrungen zum Schutz des Kernbereichs der privaten Lebensgestaltung verbunden ist, und daher ist die Vorschrift dahingehend zu verstehen, dass ihre einfachgesetzliche Ausgestaltung die Erhebung von dem

[300] *BVerfGE* 115, 166, 187 [Rn. 83]; vgl. 109, 279, 326 [Rn. 162]: Der Schutz des allgemeinen Persönlichkeitsrechts greift ein, soweit von der Wohnraumüberwachung Personen betroffen werden, die sich nicht auf Art. 13 Abs. 1 GG berufen können.

[301] *BVerfGE* 115, 166, 187 f. und 196; *Kluckert*/*Fink*, in: Epping/Hillgruber, BeckOK GG, Art. 13 Rn. 7.

[302] *BVerfGE* 103, 142, 150; 120, 274, 309.

[303] *Papier*, in: Maunz/Dürig, GG-K, Art. 13 Rn. 23 und 25 ff.

[304] *BVerfGE* 109, 279, 357 ff.

Kernbereich zuzuordnenden Informationen durch die Wohnraumüberwachung ausschließen muss.[305] Demnach sind gesetzliche Regelungen erforderlich, die unter Beachtung des Grundsatzes der Normenklarheit sicherstellen, dass die Art und Weise der akustischen Wohnraumüberwachung nicht zu einer Verletzung der Menschenwürde führt (vgl. § 100d StPO).[306]

VI. Zusammenfassung und Zwischenfazit

Heute ist die Sicherstellung von Beweismitteln zum Zwecke der Strafverfolgung nicht mehr auf den Schutzbereich von Art. 13 und 14 GG beschränkt.[307] Der Datenschutz dient in der Informationsgesellschaft dem Schutz der Menschenwürde (Art. 1 Abs. 1 GG) durch Persönlichkeitsschutz. Das *BVerfG* hat parallel zur Entwicklung der IT aus dem allgemeinen Persönlichkeitsrecht im Wege richterlicher Rechtsfortbildung das Recht auf informationelle Selbstbestimmung im Jahre 1983 und das Computer-Grundrecht im Jahre 2008 jeweils als eigenständiges Grundrecht anerkannt. Die beiden Grundrechte stehen vor dem Hintergrund einer besonderen Gefahr für die Persönlichkeit, die sich von der Vergangenheit grundlegend unterscheidet. Unter anderem, indem das Recht auf informationelle Selbstbestimmung bisher in der Prüfung von zahlreichen Verletzungen des Schutzes personenbezogener Daten immer wieder als maßgebliches Grundrecht herangezogen wird, hat es nun einen festen Status als Grundrecht auf Datenschutz erlangt, fungiert im Verhältnis zu anderen Grundrechten als Auffang-Grundrecht. Konsequenterweise gelten die Eingriffsvoraussetzungen des Grundrechts für alle Arten von Datenzugriff: überwiegendes Allgemeininteresse, die Normenklarheit, die Verhältnismäßigkeit und verfahrensrechtliche Schutzvorkehrungen.[308] In dieser Hinsicht handelt es sich heute nicht mehr um einschlägige Grundrechte, vielmehr um konkrete Ausgestaltung der Ermächtigungsgrundlage zur Rechtfertigung jedes Eingriffs, nämlich verfassungsgemäße Eingriffsvoraussetzungen und verfahrensrechtliche Vorkehrungen.[309] Das *BVerfG* vereinheitlicht zum Schritthalten mit den sich entwickelnden Informationstechnologien durch ständige Rspr. das Schutzniveau der Grundrechte bezüglich des Datenschutzes hoch und verhindert damit, dass die staatlichen Datenzugriffe

[305] *BVerfGE* 109, 279, 311 ff. [Rn. 122 und 134].

[306] *BVerfGE* 109, 279, 318 [Rn. 135].

[307] *Zimmermann*, JA 5/2014, 321, 325.

[308] Soweit ein Eingriff in den Schutz des Fernmeldegeheimnisses die Erlangung personenbezogener Daten betrifft, sind die Anforderungen, die für Eingriffe in das informationelle Selbstbestimmungsgrundrecht gelten, grundsätzlich auf Eingriffe in das speziellere Grundrecht aus Art. 10 GG zu übertragen (*BVerfGE* 100, 313, 359; 115, 166, 188 f.; 124, 43, 56 f.; 125, 260, 310).

[309] Die Vereinheitlichung des Schutzniveaus der Grundrechte auf der grundsätzlichen Ebene gewährleistet einen lückenlosen Grundrechtsschutz auf hohem Schutzniveau (*Durner*, in: Maunz/Dürig, GG-K, Art. 10 Rn. 57 f.). Tatsächlich ist das Schutzniveau im Wesentlichen identisch (a. a. O. Rn. 58).

ohne berechtigte Ermächtigung oder unverhältnismäßig erfolgen. Infolgedessen stellen die o. g. Beschränkungsvoraussetzungen heute dogmatische Kriterien dar, die für alle Arten der Eingriffe in den Datenschutz gleichermaßen gelten. Bei Diskussionen über die einschlägigen Grundrechte für Eingriffe in personenbezogene Daten sind daher die aus einer abstrakten Bewertung nach der Verhältnismäßigkeit folgenden Schutzstandards entscheidend, nicht die Eröffnung der Schutzbereiche.[310] Im Vordergrund steht insb. die Schwere eines Eingriffs in der Abwägungsprüfung bei der Entscheidung materieller Verfassungsmäßigkeit der Ermächtigung. Denn die Voraussetzungen und verfahrensrechtlichen Garantien einer Maßnahme müssen entsprechend ihrer Eingriffsintensität ausgestaltet werden. Heute stellt i. R. d. Datenerhebung im Strafverfahren die Bewertung des Eingriffsgewichtes des heimlichen oder umfassenden Zugriffs auf Datenbestände einen ersten Ansatzpunkt der Diskussion dar.

C. Verfassungsrechtlicher Datenschutz und strafverfahrensrechtliches Prinzip des Ausschlusses von illegal erlangten Beweisen in Südkorea

I. Vorrede

Die oben in Abschnitt A und B beschriebenen Inhalte können zumeist auch für die südkoreanische Situation gelten. Um die Diskussion in Korea genauer zu verstehen, sollten aber zwei grundlegende Prämissen im Voraus beachtet werden. Was die Gewährleistung der Grundrechte betrifft, so gibt es auch in Korea keine Meinungsverschiedenheiten darüber, dass personenbezogene Daten zum Schutz der Persönlichkeit in der modernen Informationsgesellschaft grundrechtlich geschützt werden müssen. Jedoch ist es umstritten, was die verfassungsrechtliche Grundlage für den Schutz personenbezogener Daten darstellt. Das liegt daran, dass das „Recht auf Selbstbestimmung personenbezogener Daten", nämlich das informationelle Selbstbestimmungsrecht, im Jahr 2005 durch den Beschluss des *K-VerfG* als eigenständiges – nicht in der Verfassung festgelegtes – Grundrecht anerkannt wurde, obwohl das allgemeine Persönlichkeitsrecht (Abs. 10 S. 1)[311] und das Recht auf Geheimnis und Freiheit des Privatlebens (Abs. 17)[312] bereits in der K-Verf vorge-

[310] Zust. *Brodowski*, JR 2009, 402, 405.

[311] Vgl. Art. 10 S. 1 K-Verf: Jeder Bürger hat die Würde und den Wert des Menschen und das Recht auf das Streben nach Glück. Daraus wird nach der Rspr. des *K-VerfG* und herrschender Auffassung das allgemeine Persönlichkeitsrecht abgeleitet (*Jaewan Moon*, WCLR, 19-2, 2013, 271, 277).

[312] Vgl. Art. 17 K-Verf: Niemand darf das Geheimnis und die Freiheit des Privatlebens verletzen. Diese Vorschrift wurde durch die Verfassungsänderung vom 1980 verankert und bis dahin gab es nur die Vorschriften zum Schutz der Freiheit der Wohnung und des Geheimnisses der Kommunikation. Die Einführung des Geheimnisses und der Freiheit des Privatlebens in die

sehen sind.[313] Außerdem wird der Schutzbereich vom Kommunikationsgeheimnis in Südkorea breiter verstanden als in Deutschland. Zum anderen wurde das Prinzip des Ausschlusses von illegal erlangten Beweisen (im Folgenden als „Ausschlussprinzip"), nämlich das Beweis(verwertungs)verbot, durch die K-StPO-Reform 2007 verankert (§ 308a). Diesbezüglich sind indes seine konkreten Anwendungsbereiche und Kriterien streitig.[314]

II. Verfassungsrechtlicher Datenschutz

1. Recht auf informationelle Selbstbestimmung: Fingerabdruckspeicherungsbeschluss

a) Hintergrund und verfassungsrechtliche Grundlage

Im Jahr 2005 hat das *K-VerfG* im Beschluss über Verfassungsbeschwerden gegen das Einwohnermeldegesetz, das die Erhebung, Speicherung, Digitalisierung und Verwendung der Daten der Fingerabdrücke erlaubt, das Recht auf informationelle Selbstbestimmung als neues eigenständiges Grundrecht geschaffen. Nach der Entscheidung bedeutet das Recht, dass der von den Daten Betroffene selbst entscheiden kann, wann, in welchem Umfang und von wem die Daten über ihn bekannt gemacht und verwendet werden, d. h. das Recht, dass der Daten-Eigentümer selbst über die Offenlegung und Verwendung seiner personenbezogenen Daten entscheidet.[315] Das *K-VerfG* hat die Veränderungen sozialer Bedingungen als Hintergrund für die Anerkennung dieses Rechts wie folgt ausgeführt:

> „Die menschliche Gesellschaft ist … durch die sprunghafte Entwicklung von Computern und TK-Technologien … in die Informationsgesellschaft eingetreten, und aufgrund der drastischen Veränderung des Datenumfelds ist die verfassungsrechtliche Frage des Schutzes der Privatsphäre i. R. d. Erhebung und Verarbeitung personenbezogener Daten zu einem interessanten Thema geworden. … insb. durch Computer kann die Verarbeitung und Verwendung solcher Daten ohne zeitliche und räumliche Beschränkung einfach und schnell

---

K-Verf wurde von der Diskussion über das Recht auf Privatsphäre (the right to privacy) in den Vereinigten Staaten beeinflusst (*Sang-Hyeon Jeon*, The Justice, Nr. 169, 2018, 5, 20).

[313] *K-VerfGE* vom 26. 5. 2005 – 99 HunMa 513 etc. (17-1, 668). Die genaue Bezeichnung dieses Grundrechts in Südkorea ist das Recht auf informationelle Selbstbestimmung des „Einzelnen". Auf jeden Fall scheint dieser Ausdruck jedoch von den Entscheidungen des *BVerfG* und den Diskussionen in Deutschland beeinflusst zu sein (*Geonbo Kwon*, The Justice, Nr. 144, 2014, 7, 14; *Sang-Hyeon Jeon*, The Justice, Nr. 169, 2018, 5, 25), und seine wesentliche Bedeutung ist gleich. Daher wird sie in vorliegender Arbeit wie in Deutschland nur als das „Recht auf informationelle Selbstbestimmung" zum Ausdruck gebracht.

[314] Das südkoreanische Ausschlussprinzip wird inhaltlich mehr von „principle of exclusion of illegally obtained evidence" der Vereinigten Staaten als von der „Beweisverbotslehre" Deutschlands beeinflusst. Aus diesem Grund wird es in Südkorea als „Ausschluss von illegal erlangten Beweisen" bezeichnet.

[315] *K-VerfGE* 17-1, 668, 682.

> erfolgen, und die Automatisierung der Datenverarbeitung und die Kombination der Dateien … führen zu einer neuen Informationsumgebung, in der die Personalien oder die verschiedenen Lebensdaten der Personen unabhängig von der Absicht der von Daten Betroffenen in der Hand Dritter unbegrenzt gestapelt und durch ihn verwendet oder offengelegt werden können und … die Möglichkeit, Einzelpersonen vom Staat zu überwachen, hat erheblich zugenommen, so dass er ihr tägliches Leben vollständig erfassen kann. Unter diesen Umständen kann die Genehmigung des informationellen Selbstbestimmungsrechts als Grundrecht als ein Mindesterfordernis verfassungsrechtlicher Garantie angesehen werden, um personenbezogene Daten vor der Gefahr zu schützen, die moderner IuK-Technologie innewohnt, und weiter, um damit die Freiheit der individuellen Entscheidungen zu gewährleisten, und schließlich, um die Möglichkeit zu verhindern, dass das Rückgrat der freiheitlichen demokratischen Grundordnung insgesamt beschädigt wird."[316] *(Übersetzung vom Autor)*

Kurz gesagt, das Recht auf informationelle Selbstbestimmung wurde auf der Grundlage neuer Risiken für die Persönlichkeit oder Privatsphäre, die durch die Entwicklung der IT verursacht werden, und der Notwendigkeit ihres grundrechtlichen Schutzes geschaffen. Vor diesem Hintergrund gibt es in Korea keine Meinungsverschiedenheiten darüber, dass das Recht ein Grundrecht darstellt und in der Natur des Persönlichkeitsrechts liegt.[317] Die obigen Ausführungen des *K-VerfG* sind jedoch nicht nur praktisch identisch mit dem Grund, warum das Privatleben grundrechtlich geschützt wird (vgl. Art. 17 K-Verf),[318] sondern stimmen auch mit dem Hintergrund des Auftretens des Rechts auf Privatsphäre in den Vereinigten Staaten und dem Grund für die Anerkennung des informationellen Selbstbestimmungsrechts in Deutschland (vgl. oben B. III. 1. a)) überein. Daher ist es umstritten, was die verfassungsmäßige Grundlage des informationellen Selbstbestimmungsrechts ist.

Das *K-VerfG* ist der Ansicht, dass das Recht auf informationelle Selbstbestimmung aus dem Recht auf Geheimnis und Freiheit des Privatlebens nach Art. 17 K-Verf und dem allgemeinen Persönlichkeitsrecht, das auf der Würde und dem Wert des Menschen sowie dem Recht auf das Streben nach Glück nach Art. 10 S. 1 K-Verf basiert, abgeleitet wird.[319] Es argumentiert jedoch nicht richtig im Detail.[320] Dies

---

[316] *K-VerfGE* 17-1, 668, 682 f.

[317] *Jaewan Moon*, WCLR, 19-2, 2013, 271, 279; *Geonbo Kwon*, The Justice, Nr. 144, 2014, 7, 13 und 15. Die Herausforderung des Schutzes personenbezogener Daten wird heute im Hinblick auf die Gewährleistung grundlegender Menschenrechte verstanden (*Geonbo Kwon*, a. a. O. 13).

[318] *Sang-Hyeon Jeon*, The Justice, Nr. 169, 2018, 5, 19 – 20. Seit 1980 ist der Schutz des Geheimnisses und der Freiheit des Privatlebens in die Liste der Grundrechte der K-Verf ausdrücklich aufgenommen.

[319] *K-VerfGE* 17-1, 668, 683; 17-2, 81, 90; 21-2, 372, 384 f.; 22-1, 323, 334; 24-2, 537; 30-1, 564, 575; 30-1, 596, 604 m. w. N. Daneben hat das *K-VerfG* im Fingerabdruckspeicherungsbeschluss, in dem das Recht auf informationelle Selbstbestimmung erstmals anerkannt wurde, auch auf die freiheitliche demokratische Grundordnung sowie das Prinzip der Volkssouveränität und der Demokratie, die in der Präambel der K-Verf stehen, als verfassungsrechtliche Grundlage verwiesen (*K-VerfGE* 17-1, 668, 683), aber danach nicht mehr. Zum anderen hat der

wird kritisiert, weil der Schutzbereich dieses Grundrechts nur durch ein Argument genau bestimmt werden kann. Aus diesem Grund ist es – trotz der Beschlüsse des *K-VerfG* – im Schrifttum immer noch umstritten, auf welcher verfassungsrechtlichen Grundlage das Grundrecht beruht, d. h. ob es nur auf Art. 10 S. 1 oder Art. 17 K-Verf oder auf beiden beruht. In Bezug auf das Verhältnis zwischen dem Art. 10 und dem Art. 17 K-Verf, die in der Verfassung verankert sind, wird von einem Teil der Lehre die Meinung vertreten, dass der Art. 17 K-Verf nur den Schutz des Geheimnisses und der Freiheit im Bereich des „Privatlebens" vorsieht, während der Art. 10 S. 1 K-Verf daneben auch die Verwirklichung der Würde und des Wertes des Menschen im „sozialen" Bereich gewährleistet.[321] Nach dieser Ansicht beruht das Recht auf informationelle Selbstbestimmung, die dem Schutz der Bedingungen für die Entfaltung der Persönlichkeit im sozialen Bereich (eigener Selbstbestimmung bezüglich des sozialen Persönlichkeitsbildes) dient, grundlegend auf Art. 10 K-Verf.[322] Der Schutz der Privatsphäre nach dem Art. 17 K-Verf ist ein Grundrecht, bei dem der Inhalt seiner Garantie beweglich ist, um den Veränderungen sozialer Realität und den damit verbundenen neuen Gefahren zu begegnen, und er schützt somit umfassend Teile, die im Bereich der Privatsphäre nicht durch traditionelle Grundrechte wie der Unverletzlichkeit der Wohnung nach Art. 16 K-Verf und dem Schutz des Kommunikationsgeheimnisses nach Art. 18 K-Verf geschützt sind.[323] Es ist weder klar noch wichtig, ob personenbezogene Daten heutzutage hinsichtlich ihrer Erstellung die private oder öffentliche Lebenssphäre betreffen.[324] Darüber hinaus wird aus dem Art. 17 K-Verf nicht nur das (passive) Abwehrrecht als Freiheitsrecht, sondern auch das (aktive) Anspruchsrecht auf die Verarbeitung personenbezogener Daten abgeleitet.[325] Vor allem im heutigen Grundrechtsschutzsystem zielen sowohl der Art. 10 als auch der Art. 17 K-Verf darauf ab, das Persönlichkeitsrecht, nämlich die freie Bildung und Entwicklung der Persönlichkeit, zu gewährleisten.[326] Nach alledem ist die Ansicht des *K-VerfG* überzeugend, dass das Recht auf informationelle Selbstbestimmung aus den beiden Vorschriften abgeleitet wird.[327]

K-OGH erklärt, dass der Art. 10 und der Art. 17 K-Verf nicht nur das passive Recht gewährleisten, dass die Privatsphäre nicht verletzt wird und nicht ohne Zustimmung veröffentlicht wird, sondern auch das aktive Recht, Informationen über sich selbst in einer modernen Informationsgesellschaft autonom zu kontrollieren (*K-OGHE* vom 24. 7. 1998 – 96 Da 42789).

[320] *Sang-Hyeon Jeon*, The Justice, Nr. 169, 2018, 5, 18 f.

[321] *Jaewan Moon*, WCLR, 19-2, 2013, 271, 280.

[322] *Jaewan Moon*, WCLR, 19-2, 2013, 271, 280 f.; abw. *Nak-In Sung*, K-Verfassungsrecht, 1349: Das Recht nach Art. 10 K-Verf ist Auffanggrundrecht, somit beruht das Recht auf informationelle Selbstbestimmung ergänzt auf Art. 17 K-Verf.

[323] *Soo-Woong Han*, CLR, Band 13, 2002, 623, 649.

[324] *Sang-Hyeon Jeon*, The Justice, Nr. 169, 2018, 5, 24 f.

[325] *Sang-Hyeon Jeon*, The Justice, Nr. 169, 2018, 5, 23 f.

[326] *Sang-Hyeon Jeon*, The Justice, Nr. 169, 2018, 5, 23; *Jaewan Moon*, WCLR, 19-2, 2013, 271, 280.

[327] A. A. *Sang-Hyeon Jeon*, The Justice, Nr. 169, 2018, 5, 23 und 25 f. Er argumentiert, dass der Art. 10 K-Verf von der verfassungsmäßigen Grundlage des informationellen Selbstbe-

b) Schutzbereich

Der Schutzbereich des informationellen Selbstbestimmungsrechts hängt vom Begriff der zu schützenden personenbezogenen Daten ab, und durch seine Bestimmung kann das Recht einen eigenen Schutzbereich haben, der sich von anderen Grundrechten unterscheidet, und erst dann kann sein verfassungsmäßiger Wert und seine Funktion anerkannt werden.[328] Laut dem Fingerabdruckspeicherungsbeschluss handelt es sich bei den personenbezogenen Daten, die durch dieses Recht zu schützen sind, um „Angaben, die die persönliche Subjektivität des Einzelnen wie Körper, Glauben, sozialer Status etc. einer Person kennzeichnen, d. h. um alle Informationen, die die Identität des Einzelnen kenntlich machen; darin sind nicht nur Informationen, die zum intimen oder privaten Bereich gehören, sondern auch die personenbezogenen Daten, die im öffentlichen Leben gebildet wurden oder bereits offengelegt wurden, enthalten“[329] (Übersetzung vom Autor). Welche personenbezogenen Daten durch das informationelle Selbstbestimmungsrecht geschützt werden, beurteilt das *K-VerfG* je nachdem, ob der von den Daten Betroffene durch sie bestimmt bzw. identifiziert werden kann: die personenbezogenen Daten, die eine bestimmte Person identifizieren können oder sich auf ihre Persönlichkeit beziehen.[330] Angesichts des

stimmungsrechts ausgeschlossen werden sollte, solange der Art. 17 K-Verf existiert. Denn heute liegt der Kerninhalt dieser Vorschrift, der durch die Wirkung der US-amerikanischen Diskussion über das Recht auf Privatsphäre geschaffen wurde, in der Kontrolle der eigenen Information, und dies entspricht im Wesentlichen dem Hintergrund, dass das *K-VerfG* im Fingerabdruckspeicherungsbeschluss von 2005 das Recht auf informationelle Selbstbestimmung anerkannt hat (a. a. O. 20 f.). Zum anderen ist in der GRCh der Schutz sowohl auf Achtung der Privatsphäre (Art. 7) als auch auf Schutz personenbezogener Daten (Art. 8) verankert, und in Einzelfällen wendet der *EuGH* die beiden Vorschriften übereinander an: z. B. bei Prüfung der Gültigkeit der RL 2002/58/EG (Urteil vom 8. 4. 2014 – C293/12, C594/12, Rn. 31) und der Entscheidung 2000/520/EG (Urteil vom 6. 10. 2015 – C362/14).

[328] *Jaewan Moon*, WCLR, 19-2, 2013, 271, 281; *Sang-Hyeon Jeon*, The Justice, Nr. 169, 2018, 5, 26.

[329] *K-VerfGE* 17-1, 668, 682. Außerdem stellen alle Handlungen wie Untersuchung, Erhebung, Speicherung, Verarbeitung und Verwendung der personenbezogenen Daten grundsätzlich Einschränkungen des Rechts auf informationelle Selbstbestimmung dar (a. a. O.).

[330] Sie sind begrifflich enger gefasst als die personenbezogenen Daten, die im K-DSG gesetzlich definiert sind, aber der Unterschied ist praktisch nicht groß (*Jaewan Moon*, WCLR, 19-2, 2013, 271, 187; *Geonbo Kwon*, PLJ, 18-3, 2017, 199, 209 f.). Nach § 2 Nr. 1 K-DSG sind „personenbezogene Daten“ Informationen über lebende Personen, und sie beziehen sich auf folgende Informationen: a) Informationen, die eine Person identifizieren können, wie Name, Registrierungsnummer und Bild; b) Informationen, die, selbst wenn eine bestimmte Person nur mittels ihrer nicht identifiziert werden kann, leicht mit anderen Informationen kombiniert werden können, um sie zu identifizieren, wobei i. R. d. Möglichkeit der Kombination Zeit, Kosten und Technologie, die zur Identifizierung der Person erforderlich sind, angemessen berücksichtigt werden sollten; c) Informationen in a und b, die teilweise gelöscht oder teilweise oder vollständig ersetzt werden, sodass eine bestimmte Person mittels ihrer nicht identifiziert werden kann. Das *K-VerfG* hat in seiner Entscheidung über die Verfassungsbeschwerde über die Erhebung und Verwendung von DNA-Daten zur Identifikation nach dem Begriff der personenbezogenen Daten des K-DSG beurteilt, ob es sich bei den Daten um personenbezogene Daten handelt, die durch das Recht auf informationelle Selbstbestimmung geschützt sind (*K-*

hohen Niveaus der heutigen IuK-Technologie und ihrer Nutzungsumgebung ist die Reichweite der personenbezogenen Daten, die durch das informationelle Selbstbestimmungsrecht zu schützen sind, jedoch sehr breit und es gibt praktisch kaum Informationen, die m Hinblick auf die Grundrechte nicht wichtig sind.[331] Daraus erschließt sich, dass das informationelle Selbstbestimmungsrecht als eigenständiges Grundrecht von Bedeutung ist. Es wird anerkannt, um Einzelpersonen vor der potenziellen Gefahr zu schützen, die von der Erfassung und Verwendung sog. „neutraler Informationen" ausgeht, die naturgemäß für sich genommen eine soziale Bewertung der Person nur schwer beeinflussen können, wie Fingerabdrücke, DNA-Daten zur Identifizierung, Registrierungsnummer des Bewohners, Name und Geburtsdatum etc.[332] Aus diesem Grund versteht die vorherrschende Ansicht die zentrale Bedeutung des Rechts auf informationelle Selbstbestimmung in Südkorea als Entscheidungsrecht („Kontrollkompetenz") über die Verarbeitung personenbezogener Daten.[333]

c) Beschränkung

Art. 37 Abs. 2 K-Verf sieht vor, dass alle Freiheiten und Rechte des Volkes nur dann gesetzlich eingeschränkt werden dürfen, wenn dies für die Staatssicherheit, die Erhaltung der Ordnung oder öffentliche Wohlfahrt erforderlich ist, aber in diesem Fall ihre wesentlichen Inhalte nicht beeinträchtigt werden dürfen. Nach dieser Vorschrift kann auch das Recht auf informationelle Selbstbestimmung beschränkt werden. Es ist nämlich i. R. d. Gemeinschaftsbezogenheit und -gebundenheit ohne Einwilligung des von den Daten Betroffenen unter den Grundsätzen des Gesetzesvorbehaltes, der Normenklarheit und der Verhältnismäßigkeit zu beschränken.[334]

VerfGE vom 28. 8. 2014 – 2011 HunMa 28 etc.: 26-2, 337, 363). Daneben sind die „Standortdaten der Personen" nach § 2 Nr. 2 K-StandODSG mit Informationen über Orte gemeint, an denen eine bestimmte Person zu einem bestimmten Zeitpunkt existiert oder existiert hat, und werden durch die Telekommunikationsanlagen nach K-TKGG erhoben. Dazu gehören auch Informationen, mittels deren der Standort der bestimmten Person nicht bestätigt werden kann, aber die leicht mit anderen Informationen kombiniert werden können, um ihn zu bestätigen. Aus diesem Grund stellen die Standortdaten der Personen Informationen dar, die mit der Persönlichkeit einer bestimmten Person verbunden sind, und gehören zu den personenbezogenen Daten i. S. d. § 2 Nr. 1 K-DSG (*Won-San Lee*, KCR, 23-2, 2012, 109, 113; *Bong-Su Kim*, CNLR, 32-3, 2012, 271, 273). Aus alledem ergibt sich, dass personenbezogene Daten in Südkorea mit der Persönlichkeit einer Person immer verbunden sind.

[331] *Geonbo Kwon*, The Justice, Nr. 144, 2014, 7, 17; *ders.*, PLJ, 18-3, 2017, 199, 203; *Aeryung Jung*, PLJ, 17-3, 2016, 51, 67; *Sang-Hyeon Jeon*, The Justice, Nr. 169, 2018, 5, 10.

[332] *Sang-Hyeon Jeon*, The Justice, Nr. 169, 2018, 5, 29.

[333] *Jaewan Moon*, WCLR, 19-2, 2013, 271, 280 f.; *Geonbo Kwon*, The Justice, Nr. 144, 2014, 7, 14; *ders.*, PLJ, 18-3, 2017, 199, 201; *Sang-Hyeon Jeon*, The Justice, Nr. 169, 2018, 5, 20 und 26; auch *K-OGHE* vom 24. 7. 1998 – 96 Da 42789.

[334] *Jaewan Moon*, WCLR, 19-2, 2013, 271, 283; *Geonbo Kwon*, The Justice, Nr. 144, 2014, 7, 21 – 25.

2. Schutz des Kommunikationsgeheimnisses: Art. 18 K-Verf

Art. 18 K-Verf[335] gewährleistet die Freiheit der Kommunikation als Grundrecht, wobei der Schutz des Kommunikationsgeheimnisses im Mittelpunkt steht.[336] Das Geheimnis und die Freiheit der Kommunikation in der Privatsphäre können freilich auch von dem Geheimnis und der Freiheit des Privatlebens nach Art. 17 K-Verf erfasst werden, aber es hat eine Stellung als eigenständiges Grundrecht in der K-Verf. Der Grund liegt darin, dass der Betrieb von Post oder Telekommunikation traditionell von staatlichen Monopolen ausgeht und dass die Möglichkeit des Eingriffs in die Kommunikation, die einen Austausch von Informationen zwischen Einzelpersonen voraussetzt, größer ist als solche in andere private Bereiche.[337]

Den Begriff und Schutzbereich des Kommunikationsgeheimnisses (Art. 18 K-Verf) versteht das *K-VerfG* teilweise anders, als dies in Deutschland verstanden wird. Es versteht die „Kommunikation" im Schutz des Kommunikationsgeheimnisses begrifflich als eine Datenübermittlung für den Informationsaustausch zwischen Menschen, nämlich einen „nicht offen interaktiven Informationsaustausch",[338] wobei es aber weder „räumliche Distanz" noch ein „Kommunikationsmedium" voraussetzt. Im Schrifttum wird kaum dagegen eingewendet, dass die Kommunikation i. S. d. Art. 18 K-Verf das Vorhandensein eines menschlichen Kommunikationspartners verlangt.[339] Es ist jedoch umstritten, ob sich der Begriff der Kommunikation durch die räumliche Distanz bzw. das Kommunikationsmedium kennzeichnet. Soweit Äußerungen ein direktes oder indirektes Gespräch zwischen zwei oder mehr Personen darstellen, werden sie nach der Stellungnahme des *K-VerfG* und seiner Befürworter vom Schutzbereich des Art. 18 K-Verf gedeckt.[340] Nach dieser Ansicht ist der Schutz des Kommunikationsgeheimnisses auf die „Heimlichkeit des menschlichen Informationsaustausches" ausgerichtet, während im Zentrum des Schutzes der Privatsphäre (Art. 17 K-Verf) personenbezogene Daten, Selbstgespräche, Verhalten etc. selbst stehen. Dazu kommt, dass es auch auf den Begriff der Kommunikation wirkt, dass Gesprächsüberwachungen durch das K-KGSG (§ 14) geregelt werden.[341] Dieses Verständnis behindert jedoch die Abgrenzung der Schutzbereiche der Grundrechte und seine theoretische Konstruktion. Nach einer anderen in der Literatur vertretenen Auffassung setzt Kommunikation – wie in Deutschland – die Datenübermittlung durch Medien Dritter voraus, und persönliche Gespräche werden durch das Geheimnis und den Schutz der Privatsphäre gewährleistet.[342] Somit geht

[335] Vgl. Art. 18 K-Verf: Niemand darf das Geheimnis der Kommunikation verletzen.

[336] *K-VerfGE* 13-1, 652, 658; 30-1, 564, 576; 30-1, 596, 605.

[337] *K-VerfGE* 13-1, 652, 658; 30-1, 564, 576; 30-1, 596, 605.

[338] *K-VerfGE* 13-1, 652, 661 – 662.

[339] *Sung-Gi Hwang*, JML, 14-1, 2015, 1, 8 ff.; *Kil-Young Oh*, JML, 14-1, 2015, 33, 47.

[340] *Il-Hwan Kim*, KJC, 16-1, 2004, 25, 33 f.; *Sung-Gi Hwang*, JML, 14-1, 2015, 1, 10 f.; *Nak-In Sung*, K-Verfassungsrecht, 1372; *Jinseoung Kong*, CNLR, 38-4, 2018, 67, 74 f.

[341] *Taesoo Kang*, KHLJ, 45-4, 2010, 287, 294.

[342] *Taesoo Kang*, KHLJ, 45-4, 2010, 287, 294 f.; *Jina Cha*, PLJ, 14-1, 2013, 39, 41.

diese Ansicht davon aus, dass die Regelung der Gesprächsüberwachung durch das K-KGSG darauf abzielt, Gespräche auf dem gleichen Niveau wie Telefongespräche zu schützen, und es nichts mit dem Schutzbereich des Grundrechts zu tun hat.[343]

Andererseits gewährleistet der Art. 18 K-Verf zur freien Kommunikation die Vertraulichkeit nicht nur von Kommunikationsinhalten, sondern auch äußerer Tatsachen, die bei dem konkreten Kommunikationsvorgang anfallen. Nach der Ausführung in der Entscheidung des *K-VerfG* beziehen sich diese Tatsachen auf die externe Gesamtsituation im Zusammenhang mit der Nutzung der TK, wozu nicht nur Beginn und Ende nach Datum und Uhrzeit, Standort, Anzahl der TK etc., sondern auch die Daten zur Feststellung der „persönlichen Identität" der Kommunikationsbeteiligten gehören.[344] Daher wird in Südkorea – anders als in Deutschland – davon ausgegangen, dass die Bestandsdaten zur Identifizierung i. d. R. durch das Recht auf informationelle Selbstbestimmung und den Schutz des Kommunikationsgeheimnisses zusammen gewährleistet werden,[345] und in der Verfassungsbeschwerde gegen den Zugriff auf die Daten prüft das *K-VerfG* nur die Verletzung des Schutzes des Kommunikationsgeheimnisses als eines speziellen Freiheitsrechts.[346]

3. Zusammenfassung und Zwischenfazit

Beim Verständnis des Schutzbereichs von Grundrechten erkennt das *K-VerfG* die Konkurrenz der Grundrechte an. Aus diesem Grund wird bei der Feststellung der Grundrechte, die durch die Erhebung, Verarbeitung und Verwendung elektronischer Daten bezüglich der TK im Strafverfolgungsverfahren verletzt werden, keine klare Unterscheidung zwischen dem Recht auf informationelle Selbstbestimmung und dem Schutz von Kommunikationsgeheimnissen versucht. Dies verhindert allerdings teilweise, den Schutzbereich der individuellen Grundrechte festzulegen. Mit Blick darauf, dass der grundrechtliche Begriff der „Kommunikation" mit der Entwicklung der IuK-Technologie immer unklarer und auch die Schutzbedürftigkeit zwischen TK-Daten und anderen Daten sich immer weniger unterscheidet, verursacht die Grundrechtskonkurrenz jedoch kein Problem. Andererseits wird in einiger Literatur das Computer-Grundrecht, das im Jahr 2008 von *BVerfG* anerkannt wurde, auch in Südkorea vorgestellt, aber es gibt kaum weitere Diskussionen. Angesichts der Möglichkeit einer Rundum- od. Totalüberwachung mittels IuK-Technologie, die sich schnell nähert und häufig sichtbarer ist, wird die Grundidee der Schaffung eines

[343] *Taesoo Kang*, KHLJ, 45-4, 2010, 287, 295.

[344] *K-VerfGE* 30-1, 564, 576; 30-1, 596, 605.

[345] Zust. *Sung-Gi Hwang*, JML, 14-1, 2015, 1, 12 f.

[346] *K-VerfGE* 30-1, 564, 575 – 576: Beschluss zur Echtzeit-Lokalisierung; 30-1, 596, 604 – 605: Beschluss zur Funkzellenabfrage; zust. *Jina Cha*, KLAJ, 67-2, 2018, 366, 380 f. Dies unterscheidet sich von der Stellungnahme des *BVerfG*, dass hierbei i. d. R. das informationelle Selbstbestimmungsrecht, aber bei Beauskunftung durch die Identifizierung der dynamischen IP-Adressen der Schutz von Kommunikationsgeheimnissen verletzt wird (*BVerfGE* 130, 151, 178 ff.).

solchen Grundrechts auch für Südkorea als sehr sinnvoll angesehen (vgl. oben B. III. 2.).

III. Prinzip des Ausschlusses von illegal erlangten Beweisen: § 308a K-StPO

1. Allgemeines

Die Lehre des Ausschlusses von illegal erlangten Beweisen in den Vereinigten Staaten ist zusammen mit der Lehre der Beweisverbote in Deutschland schon lange in Südkorea thematisiert und teilweise angenommen,[347] aber es gab keine ausdrückliche allgemeine Vorschrift darüber wie in den o. g. Ländern. Durch die K-StPO-Reform 2007 (siehe Kapitel 1, Fn. 36) wurde jedoch das Prinzip des Ausschlusses von illegal erlangten Beweisen kodifiziert (§ 308a K-StPO).[348] Diese Vorschrift gilt sowohl für „Beweismittel in Worten" bzw. „Aussage zum Beweis" als auch für „Beweismittel nicht in Worten" bzw. „Beweis in anderen Formen als Aussage" als allgemeine Klausel.[349] Für die Beweismittel in Worten befinden sich individuelle Regelungen, die die Beweisverwertung aufgrund der Beweiserhebungsverbote, insb. Beweismethodenverbote, verbieten. Art. 12 Abs. 7 Hs. 1 K-

[347] Im strafrechtlichen Bereich in Südkorea wurde das materielle Recht stark von Deutschland beeinflusst, während das prozessuale Recht stärker von den Vereinigten Staaten beeinflusst wurde. Daher hatte die US-amerikanische Diskussion über den Ausschluss von illegal erlangten Beweisen schon seit den 1960ern auf Südkorea eine erhebliche Wirkung, und dazu hat auch die deutsche Beweisverbotslehre, die auf dem Persönlichkeitsrecht beruht, Südkorea teilweise beeinflusst (*Yang-Kyun Shin*, JCL, 26-2, 2014, 447, 448).

[348] § 308a K-StPO [Abschluss von illegal erlangten Beweisen] Beweise, die ohne Befolgung legitimen Verfahrens erlangt wurden, dürfen nicht als Beweismittel dienen.

[349] *Kuk Cho*, Juris, Nr. 3, 2008, 198, 203; *Yang-Kyun Shin*, JCL, 26-2, 2014, 447, 458; *Joo-Won Rhee*, K-StPO, 364. I. R. d. Zulässigkeit der im Ermittlungsverfahren gewonnenen Beweise werden im südkoreanischen Strafprozessrecht Beweismittel in Worten und nicht in Worten unterschiedlich behandelt. Zu den Ersteren gehören Aussagen des Beschuldigten, der Zeugen oder der Sachverständigen wie Geständnisse, Zeugnisse oder Gutachten (personale Beweismittel) sowie Urkunden, in denen diese aufgezeichnet sind (z. B. Vernehmungs- oder Aussageniederschrift). Hingegen beziehen sich die Letzteren auf alle anderen sachlichen Beweismittel (z. B. Tatmittel wie Schwerter oder Waffen, Diebesgut, Betäubungsmittel, Kinderpornografie oder der menschliche Körper selbst oder dessen Teile oder dessen Inhalte), die auch die Schriftstücke enthalten, deren Inhalt und auch deren Vorliegen oder Zustand als Beweismittel dienen: Schriftstücke als Beweisgegenstände, z. B. Drohbriefe bei der Bedrohung, Vertragsurkunde oder Zahlungsdetails beim Betrug, ge- bzw. verfälschte Dokumente. Diese Unterscheidung ist im System des Beweisrechts des koreanischen Strafverfahrens sehr wichtig: Insb. bei Beweismitteln in Worten ist die Prüfung der Freiwilligkeit der Aussagen sehr streng (§§ 309, 317 K-StPO) und dann, wenn sie Beweise darstellen, die lediglich auf Hörensagen beruhen (hearsay evidence), sind sie grundsätzlich nicht als Beweismittel zulässig (§ 310a K-StPO), während dies nicht bei Beweismitteln nicht in Worten gilt (*Lee/Cho*, K-StPO, § 36 Rn. 11; *Joo-Won Rhee*, K-StPO, 343).

Verf[350] und § 309 K-StPO[351] sehen vor, dass die Geständnisse des Beschuldigten/Angeklagten, die durch eine illegale Vernehmung erhoben werden, als Beweismittel unzulässig sind, und § 317 Abs. 1, 2 K-StPO sieht vor, dass Aussagen oder Schriftstücke des Beschuldigten/Angeklagten oder anderer Personen nur dann als Beweismittel zu verwenden sind, wenn sie freiwillig vorgenommen wurden.[352] Darüber hinaus darf gemäß § 4 K-KGSG der Inhalt von Postsendungen oder TK nicht als Beweismittel verwertet werden, wenn er durch illegale Zensur oder Überwachung erhoben wurde (vgl. dazu eingehend Kapitel 3, D. I. 2.). Daneben schließt der *K-OGH* die Beweisfähigkeit der Niederschrift über die Beschuldigtenvernehmung, die unter Verletzung des Verfahrens erstellt wurde, strikt aus (unten 2.). Für die Beweismittel nicht in Worten gibt es andererseits im Strafverfahrensgesetz keine besonderen Vorschriften über die Beweisfähigkeit. Hierbei standen sich früher die Stellungnahmen von Literatur und Rspr. gegenüber, aber dies wurde durch die K-StPO-Reform und die Entscheidung im Plenum des *K-OGH* vom 2007 gelöst (unten 3.). Bei jüngsten Diskussionen über das Ausschlussprinzip in Südkorea handelt es sich meistens eher um Verfahrensstöße bei der Erhebung der Beweismittel nicht in Worten, insb. diejenigen bei dem Vollzug von Durchsuchung und Beschlagnahme. Um die Bedeutung und Wirkung des Ausschlussprinzips in Südkorea zu verstehen, ist es notwendig, die Diskussionen vor und nach der Einführung von § 308a K-StPO und den Inhalt der Entscheidung des *K-OGH* vom 15. November 2007 zu untersuchen.

2. Die Verankerung des Ausschlussprinzips und deren Sinn

a) Kontroverse vor der Verankerung: Grundlage des Ausschlussprinzips

Das Ausschlussprinzip in Südkorea wird im Wesentlichen von der US-amerikanischen Lehre des Ausschlusses von illegal erlangten Beweisen, die mit judikativer Integrität (judicial integrity) auf normativer Ebene und mit Abschreckung (deterrence) der illegalen polizeilichen Maßnahmen auf sachlicher Ebene begründet ist, beeinflusst und bei seiner konkreten Anwendung teilweise auch von der deutschen

[350] Art. 12 Abs. 7 K-Verf: Wird angenommen, dass das Geständnis des Angeklagten durch Folter, Gewalt, Bedrohung, unberechtigte Verlängerung körperlicher Haft, Täuschung oder auf andere Weise nicht freiwillig angegeben wird, so … ist das nicht als Beweismittel zur Verurteilung zulässig, oder aus diesem Grund darf er nicht bestraft werden.

[351] § 309 K-StPO [Beweisfähigkeit des Geständnisses durch Zwang etc.] Wird begründet in Zweifel gezogen, dass das Geständnis des Angeklagten durch Folter, Gewalt, Bedrohung, unberechtigte Verlängerung körperlicher Haft, Täuschung oder auf andere Weise nicht freiwillig angegeben wird, so ist das nicht als Beweismittel zur Verurteilung zulässig.

[352] § 317 K-StPO [Freiwilligkeit von Aussagen] (1) Aussagen des Angeklagten oder anderer Personen, die nicht freiwillig erfolgen, dürfen nicht als Beweismittel dienen. (2) Schriftstücke dürfen als Beweismittel nicht dienen, es sein denn, dass ihre Fertigstellung und die Freiwilligkeit ihrer Inhalte erwiesen werden.

Lehre der Beweisverbote, insb. der Abwägungslehre.[353] Die vorherrschende Ansicht der Literatur sprach sich dafür aus, dass das Prinzip in das südkoreanische Strafprozessrechtssystem aufgenommen werde,[354] und als verfassungsrechtliche und theoretische Grundlage dafür wurden i. d. R. die Garantie eines rechtsstaatlichen Verfahrens (Rechtsstaatsprinzip) und der Richtervorbehalt nach Art. 12 Abs. 1 und Abs. 3 K-Verf[355] sowie die abschreckende Wirkung auf illegale Ermittlungen durch Ermittlungsbehörden erwähnt.[356]

Alle Aussagen, die nicht freiwillig gemacht werden, oder alle Schriftstücke, in denen sie angegeben werden, durften – schon vor K-StPO-Reform 2007 – nicht als Beweismittel dienen (§ 317 K-StPO),[357] und die Beweisfähigkeit des Geständnisses, das eine Aussage des Beschuldigten darstellt, musste streng begrenzt werden (§ 309 K-StPO).[358] Die Geständnisse des Beschuldigten/Angeklagten, die durch – typische – rechtswidrige Ermittlungshandlungen wie Folter, Gewalt, Bedrohung etc. vorgenommen wurden, wurden auch bei Vorliegen begründeter Zweifel (keine

[353] *Mankee Min*, SKKLR, 24-2, 2012, 339; *Myung-Sun Roh*, CBLR, Band 37, 2012, 91, 93: eine Art Kompromiss; *Yang-Kyun Shin*, JCL, 26-2, 2014, 447, 466: Während sich die jüngsten Diskussionen in den Vereinigten Staaten auf die Abschreckung von rechtswidrigen Ermittlungen konzentrieren, liegt im Mittelpunkt der Diskussion in Südkorea die prozessuale Gerechtigkeit.

[354] *Young-Soo Han*, JCL, Band 11, 1999, 401, 407; *Kuk Cho*, SLJ, 45-2, 2004, 43, 44; *Wankyu Lee*, KJCCL, 8-1, 2006, 595, 596; *Jae-Sang Lee*, K-StPO, 544 f. m. w. N.; vgl. *Joo-Won Rhee*, K-StPO, 365.

[355] Art. 12 K-Verf (1) Jeder Bürger hat die Freiheit der Person. Niemand darf nicht gestützt auf ein Gesetz vorläufig festgenommen, verhaftet, beschlagnahmt, durchsucht oder untersucht werden, und nicht gestützt auf ein Gesetz und ein legitimes Verfahren bestraft werden oder der Maßregel oder Zwangsarbeit unterliegen. (3) Bei Festnahme, Verhaftung, Beschlagnahme und Durchsuchung muss der Anordnungsbeschluss, der nach dem legitimen Verfahren auf Antrag der StA durch Richter erlassen wird, vorgelegt werden. Bei Verfolgung auf frischer Tat oder im Fall, wenn Flucht- oder Verdunkelungsgefahr für den Verdächtigen einer Straftat, die eine Freiheitsstrafe von mehr als drei Jahren erwartet ist, besteht, kann er jedoch nachträglich beantragt werden.

[356] *Kuk Cho*, SLJ, 45-2, 2004, 43, 44; *Myung-Sun Roh*, CBLR, Band 37, 2012, 91, 93; *Joo-Won Rhee*, K-StPO, 364 f. Prof. *Cho* kritisiert insb., dass die strafrechtlichen, zivilen und administrativen Sanktionen nicht effektiv genug sind, um rechtswidrige Handlungen von Ermittlern bezüglich der Beschlagnahme und Durchsuchung zu unterdrücken, und dass sie faktisch auch wenig genutzt werden (*Kuk Cho*, a. a. O. 45 – 47). Daher behauptete er vor 2007 bereits, dass der *K-OGH* das Ausschlussprinzip durch Auslegung aufgrund von Art. 12 Abs. 1 und Abs. 3 K-Verf aufnehmen sollte wie in der Entscheidung Mapp v. Ohio vom *Obersten Gerichtshof der Vereinigten Staaten* von 1961 (367 U.S. 643) (a. a. O. 48 f.).

[357] Nach dem Urteil des *K-OGH* wird unter der Freiwilligkeit der Vorschrift verstanden, dass „es keine Umstände gibt, in denen die Freiwilligkeit der Aussage geleugnet wird, wie Folter, Gewalt, Bedrohung, unberechtigte Verlängerung körperlicher Haft, Täuschung oder andere Weise, d. h., es gibt keine Rechtswidrigkeit bei der Beweiserhebung“ (*K-OGHE* vom 8. 3. 1983 – 82 Do 3248; *Joo-Won Rhee*, K-StPO, 473 f.). Daher stimmt diese Freiwilligkeit begrifflich mit derjenigen von § 309 K-StPO überein.

[358] *Park/Tak*, Beweisfähigkeit von Geständnissen, 48; *Kuk Cho*, Juris, Nr. 3, 2008, 198, 205; *Bong-Su Kim*, KJCCL, 11-2, 2009, 189, 191.

Überzeugung) an solchen Handlungen ohne Abwägungsprüfung automatisch und pflichtmäßig von den Beweismitteln ausgeschlossen.[359] Nach h. M. beruhte die Vorschrift theoretisch auf der Garantie eines rechtsstaatlichen Verfahrens, und somit durften die durch rechtswidriges Verfahren erlangten Geständnisse unabhängig von der Freiwilligkeit nicht als Beweismittel verwertet werden.[360] Auf der gleichen Ebene lehnte der *K-OGH* ebenfalls ungeachtet der Freiwilligkeit der Aussage die Beweisfähigkeit in folgenden Fällen ab; etwa die Niederschrift der Beschuldigtenvernehmung, bei der das Recht auf ungehinderten Verkehr mit seinem Verteidiger (§§ 34, 89 i. V. m. § 209 K-StPO) verletzt wurde,[361] die Vernehmungsniederschrift des Beschuldigten, der sich nach einer rechtswidrigen Festnahme nicht auf freiem Fuß befindet,[362] oder die Aussage des Beschuldigten, die bei der Vernehmung ohne Belehrung über die Aussagefreiheit (Art. 12 Abs. 2 K-Verf,[363] § 244b K-StPO[364]) erfolgte.[365] [366] Nach den Entscheidungen des *K-OGH* war die Ablehnung der Zulässigkeit jedes Beweismittels nicht auf die (analoge) Anwendung des § 309 K-StPO, sondern auf Verfahrensverstöße wie die rechtswidrige Nichtzulassung oder Einschränkung des freien Verteidigerverkehrs, die Verletzung der Belehrung über die Aussagefreiheit oder die rechtswidrige Festnahme zurückzuführen. Darüber hinaus wurden die Inhalte von Postsendungen und TK, die durch Zensur und Überwachung, die nicht dem Verfahren entsprechen, erfasst wurden, nach § 4 K-KGSG ohne Abwägungsprüfung einheitlich von Beweismitteln ausgeschlossen. Nach alledem wurde im Schrifttum davon ausgegangen, dass der *K-OGH* i. R. d. „Beweismittel in Worten" auf der Grundlage der verfassungsrechtlichen Rechtsstaatlichkeit des Art. 12 Abs. 7 Hs. 1 K-Verf, des § 309 K-StPO und des § 4 K-KGSG das Aus-

[359] *Park/Tak*, Beweisfähigkeit von Geständnissen, 48; *Kuk Cho*, Juris, Nr. 3, 2008, 198, 205; abw. *Joo-Won Rhee*, K-StPO, 388: Er besteht auf einer umfassenden Überprüfung, aber erklärt, dass ein freiwilliges Geständnis im Falle eines Verfahrensverstoßes letztendlich nicht zulässig ist.

[360] Vgl. *Joo-Won Rhee*, K-StPO, 387 f.

[361] *K-OGHE* vom 24. 8. 1990 – 90 Do 1285: *ders.* vom 25. 9. 1990 – 90 Do 1586: Sie wird vor der Beurteilung der Freiwilligkeit der Aussagen ihre Zulässigkeit verweigert.

[362] *K-OGHE* vom 11. 6. 2002 – 2000 Do 5701.

[363] Art. 12 Abs. 2 K-Verf: Niemand darf gefoltert und strafrechtlich gezwungen werden, gegen sich selbst auszusagen.

[364] § 244b K-StPO [Belehrung des Aussageverweigerungsrechts] (1) Die StA und die Kriminalpolizei haben vor der Vernehmung den Beschuldigten darauf hinzuweisen, dass 1. er keinerlei oder nur auf einzelne Fragen Aussagen machen kann, 2. er nicht benachteiligt wird, auch wenn er keine Aussage macht, 3. die Aussagen, die er nach dem Verzicht auf das Recht auf Aussageverweigerung machte, vor Gericht als Beweismittel zur Verurteilung verwertet werden können, 4. er sich bei seiner Vernehmung des Beistands eines Rechtsanwalts bedienen kann, z. B. wie die Teilnahme seines Verteidigers an der Vernehmung.

[365] *K-OGHE* vom 23. 6. 1992 – 92 Do 682: Die Aussage ist nicht als Beweismittel zulässig, „auch wenn sie freiwillig erfolgt".

[366] Vgl. diese Entscheidungen wurden von der amerikanischen Rechtstheorie beeinflusst (*Wankyu Lee*, KJCCL, 8-1, 2006, 595, 606).

schlussprinzip schon früher anerkannt hat, obwohl dies nicht in seinen Entscheidungen zum Ausdruck gebracht wurde.[367]

Auf der anderen Seite hat der *K-OGH* vor der Reform von 2007 die Beweisfähigkeit von Gegenständen, die durch illegale Beschlagnahme und Durchsuchung sichergestellt wurden, nämlich Beweismittel nicht in Worten, aufgrund der Betrachtung der sog. „unveränderlichen Natur und Form" anerkannt.[368] Die herrschende Ansicht im Schrifttum war hingegen ziemlich kritisch und behauptete, dass das Ausschlussprinzip auch hier gelten sollte. Hierbei ist jedoch i. d. R. zu beachten, dass alle Formen der Illegalität im Verfahren der Beschlagnahme und Durchsuchung – anders als das Verbot der Verwertung von Geständnissen oder Aussagen – nicht automatisch und einheitlich zum Beweisverwertungsverbot führen können.[369] Das heißt, dass der grundsätzliche Ausschluss von illegal erlangten Beweismitteln nicht in Worten im Einzelfall durch richterliche Abwägungsprüfung unterbleiben kann: „diskretionärer" Ausschluss von illegal erlangten Beweisen.[370] Nach einer im Schrifttum vertretenen Auffassung sei die unterschiedliche Behandlung zwischen Beweismitteln in Worten und nicht in Worten i. d. R. durch das Gewicht des Grundrechtseingriffs,[371] den tatsächlichen Wert der erlangten Beweise und ggf. die Erwägung der Rechtsgüter des Opfers[372] zu rechtfertigen.

b) Der Sinn der Verankerung

Der § 308a K-StPO sieht vor, dass Beweise, die ohne Befolgung legitimen Verfahrens erlangt wurden, nicht als Beweismittel dienen dürfen.[373] Er ist eine allgemeine Vorschrift, die für die Beweismittel sowohl nicht in Worten als auch in Worten gilt. Dem Wortlaut zufolge haben die durch einen Verfahrensverstoß gewonnenen

---

[367] *Wankyu Lee*, KJCCL, 8-1, 2006, 595; *Kuk Cho*, Juris, Nr. 3, 2008, 198, 200 f.; *Joo-Won Rhee*, K-StPO, 365.

[368] *K-OGHE* vom 17. 9. 1968 – 68 Do 932; *ders.* vom 23. 6. 1987 – 87 Do 705; *ders.* vom 8. 2. 1994 – 93 Do 3318; *ders.* vom 28. 10. 2005 – 2004 Do 4731: „*Die beschlagnahmten Gegenstände sind als Beweismittel zulässig, auch wenn das Verfahren der Beschlagnahme illegal ist, da der Verfahrensverstoß nicht zur Änderung der Natur und Form der Gegenstände führt und daher sich ihr Beweiswert nicht ändert.*" (Übersetzung vom Autor).

[369] *Kuk Cho*, SLJ, 45-2, 2004, 43, 49; *Wankyu Lee*, KJCCL, 8-1, 2006, 595, 609 f.; *Lee/Cho*, K-StPO, § 39 Rn. 9.

[370] *Kuk Cho*, SLJ, 45-2, 2004, 43, 49; *Wankyu Lee*, KJCCL, 8-1, 2006, 595, 610.

[371] *Kuk Cho*, SLJ, 45-2, 2004, 43, 50 f.; *Wankyu Lee*, KJCCL, 8-1, 2006, 595, 608.

[372] *Wankyu Lee*, KJCCL, 8-1, 2006, 595, 607 ff.

[373] Im Gesetzgebungsvorgang wurde der Wortlaut dieser Vorschrift, insb. „ohne Befolgung legitimen Verfahrens", seitens der StA abgelehnt (*Wankyu Lee*, KJCCL, 8-1, 2006, 595, 596). Staatsanwalt Dr. *Wankyu Lee* kritisierte vor allem, dass aus der Auslegung des Wortlauts der Anwendungsbereich der Vorschrift unbegrenzt ist (d. h. sie kann auch bei geringfügigen Verfahrensverstößen angewendet werden), sodass sie in der Praxis keine klaren Kriterien vorlegt und der spezifische Anwendungsbereich letztendlich vollständig vom Gericht festgelegt wird (a. a. O. 610 – 614).

Beweise – unabhängig von der Freiwilligkeit oder Wahrheit/Falschheit und des Gewichts der Beweise, der Schwere der Straftat, der Absicht des Verstoßes – keine Beweisfähigkeit. Für die Beweismittel in Worten galt dies bereits vor Einführung der Vorschrift in erheblichem Ausmaß (vgl. oben a)). Daher ist insoweit die Schaffung des § 308a K-StPO nicht von Bedeutung, und er ist funktional nur eine allgemeine Vorschrift der Sonderregelungen wie §§ 309, 317 Abs. 1, 2 K-StPO und § 4 K-KGSG.[374] Hingegen schließt die Vorschrift die Lücke in der Regelung bezüglich der Beweismittel nicht in Worten.[375]

3. Das Ausschlussprinzip bei Beweismitteln nicht in Worten: Anwendungskriterien des § 308a K-StPO

a) Fragestellung

Wie in obigem Unterabschnitt 2 erläutert, ist die Einführung von § 308a K-StPO in der Tat für Beweismittel nicht in Worten von Bedeutung, aber in der Vorschrift ist nur ein „legitimes Verfahren" als Kriterium für den Ausschluss von Beweisen angeführt. Daher wurde sie erst einmal dahingehend ausgelegt, dass Beweise, die durch Verstöße gegen das „verfassungsrechtliche rechtsstaatliche Verfahren" (Art. 12 Abs. 1 K-Verf) gewonnen wurden, nicht als Beweismittel verwendet werden dürfen,[376] und nach dem Beschluss des *K-VerfG* ist dieses Verfahren ein „legitimes Verfahren zur Gewährleistung der Grundrechte der Angeklagten etc. bei der Verwirklichung des staatlichen Strafanspruchs", d. h. ein „Verfahren zur Gewährleistung grundlegender Fairness".[377] In dieser Hinsicht kann der § 308a K-StPO dann angewendet werden, wenn die rechtswidrigen Handlungen der Ermittlungsbehörde in die Grundrechte des Betroffenen eingreifen und die Verfahrensgerechtigkeit beschädigen. Dies ist jedoch nicht ausreichend, daher wird immer noch darüber diskutiert, was die spezifischen Anwendungskriterien sind.[378] Diesbezüglich hat der *K-OGH* Ende 2007, kurz vor dem Inkrafttreten von § 308a K-StPO, durch ein Urteil detailliertere Kriterien festgelegt.

---

[374] *Kuk Cho*, Juris, Nr. 3, 2008, 198, 203 f.

[375] *Kuk Cho*, Juris, Nr. 3, 2008, 198, 203; auch *Lee/Cho*, K-StPO, § 39 Rn. 1.

[376] *Kuk Cho*, Juris, Nr. 3, 2008, 198, 203; *Bong-Su Kim*, KJCCL, 11-2, 2009, 189, 203; *Yang-Kyun Shin*, JCL, 26-2, 2014, 447, 458; *Joo-Won Rhee*, K-StPO, 365.

[377] *K-VerfGE* 8-2, 808, 830.

[378] *Wankyu Lee*, KJCCL, 8-1, 2006, 595, 613; *Kuk Cho*, Juris, Nr. 3, 2008, 198, 203; *Mankee Min*, SKKLR, 24-2, 2012, 339, 340; *Myung-Sun Roh*, CBLR, Band 37, 2012, 91, 92; *Yang-Kyun Shin*, JCL, 26-2, 2014, 447, 458 f.; *Joo-Won Rhee*, K-StPO, 365 f. In dieser Hinsicht ist die Theorie des diskretionären Ausschlusses von illegal erlangten Beweisen (vgl. oben 2. a)) vor der Einführung solcher Vorschrift noch gültig.

b) K-OGHE *(Plenum) vom 15. 11. 2007 – 2007 Do 3061: „Grundsätzlicher Ausschluss, ausnahmsweise Zulässigkeit"*

Durch die Entschließung im Plenum vom 15. November 2007 hat der *K-OGH* die herkömmliche Betrachtung der unveränderlichen Natur und Form verworfen, die seit über 40 Jahren durchgehalten wurde, und gleichzeitig hat er entschieden, dass das Ausschlussprinzip mit seiner Fernwirkung (sog. „fruit of the poisoned tree doctrine") i. d. R. anerkannt werden sollte, um Grundrechte zu gewährleisten und illegale Ermittlungen abzuschrecken:[379]

> „Zur Gewährleistung von elementaren Menschenrechten sollte die normative Wirkung der K-Verf und der K-StPO … gewahrt bleiben. Die Beweise, die ohne Einhaltung des in der K-Verf und der K-StPO festgelegten Verfahrens erlangt wurden, sind grundsätzlich nicht als Beweismittel zu einer Verurteilung zulässig, da es nicht dem legitimen Verfahren zur Gewährleistung von elementaren Menschenrechten entspricht. Die effektivste und sicherste Gegenmaßnahme zur Unterdrückung der illegalen Beschlagnahme und Durchsuchung durch Ermittlungsbehörden und zur Verhinderung ihrer Wiederholung besteht darin, sicherzustellen, dass nicht nur die durch sie erhobenen Beweise, sondern auch die darauf gewonnenen sekundären Beweise nicht als Beweismittel dienen können." *(Übersetzung vom Autor)*

Daran anschließend erläuterte die Mehrheitsmeinung der Entscheidung die Beschränkung der Anwendung des Ausschlussprinzips und seiner Fernwirkung sowie die hier zu berücksichtigenden Umstände bezüglich der Durchsuchung und Beschlagnahme ausführlich. Danach ist die Verwertung illegal erlangter Beweise immerhin eine „Ausnahme", und hierzu sollten alle Umstände bezüglich des Verfahrens zur Beweissicherung insgesamt betrachtet und bei der Prüfung der Fernwirkung daneben auch die Unterbrechung bzw. Verdünnung des Kausalzusammenhangs berücksichtigt werden.

> „Dass die beschlagnahmten Gegenstände nur deswegen keine Beweisfähigkeit einheitlich haben, weil sie formal gesehen ohne Befolgung von dem rechtlich festgelegten Verfahren erhoben wurden, ist (auch) nicht mit dem Zweck der Regelung über das Strafverfahren von K-Verf und K-StPO vereinbar, da die Verwirklichung des berechtigten Strafanspruchs durch die Erforschung der materiellen Wahrheit auch ein wichtiges Ziel (Idee) ist, das die K-Verf und die K-StPO durch das Strafverfahren erreichen wollen. Daher können sie in Ausnahmefällen vor Gericht als Beweismittel zu einer Verurteilung verwendet werden, in denen die Verfahrensverstöße den wesentlichen Inhalt des rechtsstaatlichen Verfahrens nicht berühren, sondern der Ausschluss ihrer Beweisfähigkeit so bewertet wird, dass er zu einem Ergebnis führt, das dem Zweck der K-Verf und der K-StPO entgegensteht, der durch die Regelung über das Strafverfahren einen Ausgleich zwischen dem Prinzip des rechtsstaatlichen Verfahrens und der Sachverhaltsaufklärung erreichen und damit strafrechtliche Gerechtigkeit verwirklichen will; umfassend zu berücksichtigen sind dabei alle Umstände

[379] Vgl. die vorherrschende Meinung der Literatur stimmt auch zu, dass die Fernwirkung anerkannt werden sollte, da ansonsten das Ausschlussprinzip selbst ausgehöhlt wird (*Kuk Cho*, Juris, Nr. 3, 2008, 198, 214 f.; *Bo-Hack Suh*, KCR, 20-3, 2009, 31, 39 f.; *Yang-Kyun Shin*, JCL, 26-2, 2014, 447, 463).

hinsichtlich der Verfahrensverstöße, die im Zuge der Beweiserhebung durch die Ermittlungsbehörde vorgenommen wurden, nämlich der Zweck der Verfahrensregelungen, der Inhalt, die Intensität, der konkrete Verlauf und die Vermeidbarkeit ihres Verstoßes, die Natur und der Verletzungsgrad der durch die Regelungen geschützten Rechte oder Rechtsgüter und ihre Relevanz für den Beklagten, der Kausalzusammenhang zwischen den Verfahrensverstößen und Beweiserhebung, die Wahrnehmung und Absicht der Ermittlungsbehörde etc. Dies gilt auch für die sekundären Beweise, die auf Basis der ohne Befolgung des legitimen Verfahrens erlangten Beweise gewonnen wurden, und unter umfassender Berücksichtigung aller Umstände bezüglich der sekundären Beweiserhebung können sie daher in Ausnahmefällen vor Gericht als Beweismittel zu einer Verurteilung verwendet werden; zu berücksichtigen sind dabei insb. Unterbrechung oder Verdünnung des Kausalzusammenhangs zwischen der primären und der sekundären Beweiserhebung."[380] *(Übersetzung vom Autor)*

4. Zusammenfassung und Zwischenfazit

Seit dem Inkrafttreten der – geltenden – Verfassung 1987 in Südkorea werden illegal erlangte Beweismittel in Worten aufgrund des Grundrechts auf körperliche Unversehrtheit und persönliche Freiheit und des Gebots des rechtsstaatlichen Verfahrens nach Art. 12 K-Verf bereits recht streng ausgeschlossen. Hingegen wurde ein solcher Ausschluss i. R. d. Beweismittel nicht in Worten durch die Schaffung von § 308a K-StPO und das proaktive Urteil von *K-OGH* im Jahr 2007 verwirklicht. Das Ausschlussprinzip ist in der Vorschrift verankert und der *K-OGH* hat in seinem Urteil klar erklärt, dass die Verwertung von illegal erlangten Beweisen eine Ausnahme darstellt. Dies ist eine Warnung an eine Praxis, die nur auf die materielle Wahr-

[380] Zust. *Kuk Cho*, Juris, Nr. 3, 2008, 198, 215; *Yang-Kyun Shin*, JCL, 26-2, 2014, 447, 460. Das Sondervotum des *K-OGH* in der Entscheidung unterscheidet sich etwas von der Mehrheitsansicht: „*Bei der Beurteilung der Beweisfähigkeit der beschlagnahmten Gegenstände sollte ein Gleichgewicht aufrechterhalten werden, die Gebote des rechtsstaatlichen Verfahrens und der Sachverhaltsaufklärung auszugleichen. Die Kriterien der Mehrheitsmeinung sind jedoch nicht nur unklar, sondern auch zu streng … , so dass eine Sorge besteht, dass es unmöglich oder zu schwierig sein könnte, ein anderes Ziel der Strafjustiz, nämlich die angemessene Ausübung des Strafanspruchs durch die Aufklärung von Sachverhalten, zu erreichen. Daher … angesichts aller Umstände bezüglich des Verfahrens zur Beweissicherung … wenn die Gründe für die Verfahrensverstöße so schwerwiegend sind, dass Geist und Zweck des Richtervorbehalts vernachlässigt werden, können die Gegenstände nicht als Beweismittel dienen; aber wenn solche Gründe nicht so schwer sind, sollten sie als Beweismittel dienen können.*" (Übersetzung vom Autor); zust. *Lee/Cho*, K-StPO, § 39 Rn. 10; *Mankee Min*, SKKLR, 24-2, 2012, 339, 365 ff.; *Myung-Sun Roh*, CBLR, Band 37, 2012, 91, 96 f. Das Sondervotum stimmt der Aufnahme des Ausschlussprinzips zu, aber betont, dass illegal erlangte Beweise nur bei schwerwiegenden Verfahrensverstößen nach Abwägung ausgeschlossen werden können, nicht dass sie grundsätzlich ausgeschlossen werden sollten. In dieser Hinsicht ist der Umfang des Ausschlusses der Beweise im Vergleich zur Mehrheitsmeinung eng (*Kuk Cho*, a. a. O.). Andererseits behauptet Prof. *Bong-su Kim*, dass illegal erlangte Beweise – nicht nach Ermessen, sondern – obligatorisch und automatisch ausgeschlossen werden sollten, wenn das Verfahren zur Gewährleistung grundlegender Fairness verletzt wird, z. B. bei der Durchsuchung und Beschlagnahme ohne richterliche Anordnung oder durch fehlerhafte Anordnung (*Bong-Su Kim*, KJCCL, 11-2, 2009, 189, 200 ff.).

heitsfindung ausgerichtet war, und bestätigt die Bedeutung der Verfahrensgerechtigkeit. Danach hat der *K-OGH* in vielen Entscheidungen weiterhin den grundsätzlichen Ausschluss und die ausnahmsweise Zulassung der Verwertung von illegal beschlagnahmten Gegenständen bestätigt.[381] Durch diese Entscheidungen wird das Ausschlussprinzip i. R. d. Durchsuchung und Beschlagnahme elektronischer Daten konkretisiert, und dabei handelt es sich insb. um ein Verfahren zur Durchführung der Maßnahme und zur Sicherstellung nur verfahrensrelevanter Daten. Daneben hat der Gerichtshof in der Entscheidung von 2009 über die Auswirkungen von Verstößen gegen die Anweisungen des Durchsuchung- und Beschlagnahmebeschlusses und das Durchführungsverfahren der K-StPO (2008 Do 763) ausgeführt, dass die ausnahmsweise Verwertung solcher Gegenstände sorgfältig gestattet werden sollte und das Vorhandensein konkreter und spezifischer Umstände dafür durch den Staatsanwalt nachgewiesen werden muss.[382] Schließlich kann jeder den Ausschluss illegal erlangter Beweise geltend machen, und sie dürfen trotz der Einwilligung des Angeklagten weder als Beweismittel noch als bestärkender/entlastender Hilfsbeweis verwendet werden.[383] Aus alledem ist ersichtlich, dass in Südkorea derzeit die prozessuale Gerechtigkeit nicht nur bei Beweismitteln in Worten, sondern auch bei Beweismitteln nicht in Worten erheblich betont wird.

[381] *K-OGHE* vom 12. 3. 2009 – 2008 Do 11437; *ders.* vom 24. 12. 2009 – 2009 Do 11401; *ders.* vom 28. 4. 2011 – 2009 Do 10412; *ders.* vom 11. 7. 2019 – 2018 Do 20504 m. w. N.

[382] *K-OGHE* vom 12. 3. 2009 – 2008 Do 763: „*Die unüberlegte Genehmigung dieser Ausnahmefälle kann … zu einer Verletzung des Prinzips führen, und daher haben Gerichte dies bei der Beurteilung zu berücksichtigen, ob ein bestimmter Fall unter den Ausnahmefall fällt. Darüber hinaus … muss der Staatsanwalt nachweisen, dass konkrete und besondere Umstände für solche Ausnahmefälle vorliegen.*“ (Übersetzung vom Autor); weiter *ders.* vom 28. 4. 2011 – 2009 Do 10412; *ders.* vom 11. 7. 2019 – 2018 Do 20504 m. w. N.

[383] *Joo-Won Rhee*, K-StPO, 368: In dieser Hinsicht ist das Ausschlussprinzip ein „schwarzes Loch“ im Beweisrecht.

Kapitel 3

Heimliche Zwangsmaßnahmen

A. Heimliche Ermittlungen und Zwangsmaßnahmen

I. Zulässigkeit heimlicher Ermittlungen und kriminalistische Zwangsmaßnahmen

1. Zulässigkeit heimlicher Ermittlungen

Sind heimliche Ermittlungen, insb. heimliche Erhebungen personenbezogener Daten, mit dem Rechtsstaatsprinzip vereinbar? Die Heimlichkeit von Maßnahmen der Strafverfolgung verstößt als solche nicht gegen das im Fair-Trial-Grundsatz wurzelnde Täuschungsverbot[1] und ist kein Umstand, die Unzulässigkeit der ergriffenen Maßnahmen zu begründen.[2] Vielmehr ist sie in vielen Fällen eine unabdingbare Voraussetzung des Erfolgs der Strafverfolgung.[3] Schon seit Langem werden heimliche Ermittlungen als notwendig und legitim anerkannt, um nicht nur die organisierte Kriminalität, sondern auch viele andere Formen schwerer Kriminalität zu bekämpfen.[4] Sie erfolgen nicht nur für wichtige Rechtsgüter wie den Bestand oder die Sicherheit des Staates, die freiheitliche demokratische Grundordnung oder Leib, Leben oder Freiheit einer Person oder nur durch heimliche Tonband- oder Bildaufnahme mit technischen Mitteln. Nach dem Grundsatz der freien Gestaltung des Ermittlungsverfahrens (§§ 161 Abs. 1, 163 Abs. 1 StPO) dürfen die Ermittlungsbehörden i. d. R. alle zulässigen Maßnahmen, zur Aufklärung der Straftat beizutragen, ergreifen[5] und haben breiten Spielraum für kriminalistische Taktik und den Einsatz von Kriminaltechnik.[6] Daher können vielfältige heimliche Ermittlungen zur Erforschung des Sachverhalts erfolgen. Sobald die Ermittlungsbehörden eine

[1] *BVerfGE* 109, 279, 324 [Rn. 156].

[2] *BVerfG* NJW 2009, 1405, 1407 [Rn. 28]; *BGHSt* 39, 335, 346; 42, 139, 150; M-G/*Schmitt*, StPO, § 161 Rn. 7.

[3] *BVerfGE* 109, 279, 325 [Rn. 156]; NJW 2009, 1405, 1407 [Rn. 28].

[4] Vgl. *BVerfG* NJW 1985, 1767: Bei der Bewertung der Rechtmäßigkeit polizeilicher Lockspitzel sollen die Bedürfnisse einer wirksamen Strafrechtspflege in Betracht kommen; *BGH* NJW 1980, 1761: „*i. R. d. Bekämpfung besonders gefährlicher und schwer aufklärbarer Kriminalität, insb. auch der Rauschgiftkriminalität, kann auf den polizeilichen Lockspitzel (agent provocateur) nicht verzichtet werden.*"

[5] *BVerfG* NJW 2009, 1405, 1407 [Rn. 26]; M-G/*Schmitt*, StPO, § 161 Rn. 7.

[6] M-G/*Schmitt*, StPO, § 163 Rn. 64.

Maßnahme treffen, die erkennbar darauf abzielt, gegen jemanden strafrechtlich vorzugehen, ist das Ermittlungsverfahren eingeleitet, wobei es gleichgültig ist, ob das dem Beschuldigten bekannt ist.[7] Vielmehr wird es meist ohne Wissen des Betroffenen durch Strafantrag oder –anzeige oder amtliche Wahrnehmung einer Straftat eingeleitet.[8] Im Allgemeinen ist es oft zweckmäßig und erforderlich, dass Ermittlungen – mindestens an ihrem Anfang – ohne Wissen des Beschuldigten eingeleitet oder durchgeführt werden.[9] In der modernen Informationsgesellschaft werden – online – heimliche Ermittlungen durch das Internet, um personenbezogene Daten auf informationstechnischen Systemen oder im Netzwerk verdeckt zu erheben, in der Praxis immer wichtiger, weil die dort gewonnene Daten in vielen Fällen sachlich der Aufklärung von Straftaten dienen. Die Heimlichkeit der Ermittlungen steht nicht schlechthin ihrer Zulässigkeit entgegen.[10]

2. Kriminalistische Zwangsmaßnahmen

Strafrechtlicher Zwang darf nur angewandt werden, soweit das Strafverfahrensrecht dies zulässt (vgl. § 136a Abs. 1 S. 2 StPO).[11] Jedoch dürfen §§ 161 Abs. 1, 163 Abs. 1 StPO als Ermittlungsgeneralklausel keine Rechtsgrundlage zu kriminalistischen Zwangsmaßnahmen sein (vgl. unten B. I. 1.). Diese stellen nämlich nur die Vorschriften zur Zuständigkeit bzw. Aufgabenverteilung dar, in dem Sinne, dass der StA und der Polizei allgemeine Ermittlungsbefugnis erteilt wird. Für Beschlagnahme, Durchsuchung, Verhaftung und vorläufige Festnahme als typische Zwangsmaßnahmen liegen daher eigenständige Rechtsgrundlagen in der StPO vor (vgl. §§ 94 ff., 102 ff., 112 ff., 127 ff.). Nach h. M. setzt der Begriff des „Zwangs" keine physische Verletzung notwendig voraus, sondern er ist durchweg mit dem Eingriff in ein Grundrecht verbunden,[12] die ‚Eingriffsqualität' der Maßnahmen ist

---

[7] M-G/*Schmitt*, StPO, Einl. Rn. 60.

[8] Vgl. *Roxin*/*Schünemann*, § 39 Rn. 2 ff.

[9] M-G/*Schmitt*, StPO, § 161 Rn. 8: Kriminaltaktischer Gesichtspunkt. Auch die „Vorermittlungen", um aufgrund eines besonders schwachen Anfangsverdachts das Vorliegen von (einfachem) Anfangsverdacht (§ 152 Abs. 2 StPO) zu begründen (M-G/*Schmitt*, StPO, § 152 Rn. 4b; *Roxin*/*Schünemann*, § 39 Rn. 17), erfolgen durchgängig ohne Wissen des Betroffenen. Sie sind zu unterscheiden von den „Vorfeldermittlungen", die dazu dienen, im zweifelhaften Umfeld (noch) ohne den Anfangsverdacht einer Straftat Informationen zu beschaffen, und die daher nach der StPO nicht gestattet sind (*Roxin*/*Schünemann*, § 39 Rn. 18: Dazu gehören geheimdienstliche Tätigkeiten oder polizeiliche Maßnahmen i. R. d. Gefahrenabwehr; vgl. M-G/*Schmitt*, a. a. O.: Diese sind in strafprozessualer Hinsicht unzulässig). Bei den Vorermittlungen dürfen keine Zwangsmittel ergriffen werden und auch der Ermittlungsumfang ist nach dem Verhältnismäßigkeitsgrundsatz begrenzt (M-G/*Schmitt*, StPO, a. a. O.; *Roxin*/*Schünemann*, § 39 Rn. 17).

[10] *Hofmann*, NStZ 2005, 121, 123.

[11] Vgl. M-G/*Schmitt*, StPO, Einl. Rn. 45 und § 163 Rn. 32.

[12] *Ameldung*, Rechtsschutz, 15 f.; *Roxin*/*Schünemann*, § 29 Rn. 3; *Park*, § 1 Rn. 23; vgl. BT-Drs. 7/2600, S. 13: „*Richterliche Untersuchungshandlungen sind einmal dann erforderlich,*

dann anzunehmen, wenn ihre Intensität „eine bestimmte Schwelle überschreitet".[13] Dem Gesetzgeber steht die Aufgabe zur primären Bewertung und gesetzlichen Ausgestaltung darüber grundsätzlich zu. Bei der normativen Ausgestaltung zur Rechtfertigung der Zwangsmaßnahmen liegen die entscheidenden Eingriffsvoraussetzungen auf der materiellen Seite, nämlich die Schwere der Straftat und die Stärke des Tatverdachts, und eine Kontrolle gegenüber den Strafverfolgungsbehörden auf der prozessualen Seite ist von entscheidender Bedeutung. Im letzteren Fall ist – unter dem Strafjustizsystem des Akkusationsprinzips – die Kontrolle durch Gericht als unabhängige und neutrale Instanz wie Richtervorbehalt und effektiver Rechtsschutz traditionell von größter Bedeutung.[14] Der Richtervorbehalt als präventive Kontrolle dient der Legitimierung der Zwangsmaßnahmen und gerichtlicher Rechtsschutz als nachträgliche Kontrolle trägt zum lückenlosen Grundrechtsschutz bei. Im Rechtsstaat darf den Strafverfolgungsbehörden das gesamte rechtliche Instrumentarium eines Überwachungsstaates nur unter einer reinen In-Sich-Kontrolle nicht in die Hand gegeben werden.[15]

3. Heimliche Zwangsmaßnahmen

a) Ausnahmsweiser und eigenständiger Charakter

In einem Rechtsstaat ist die Heimlichkeit staatlicher Eingriffsmaßnahmen ausnahmsweise und bedarf besonderer Rechtfertigung.[16] Dies ist zumindest insoweit durchaus zumutbar, als Maßnahmen zum Zwecke der Strafverfolgung in Grundrechte schwer eingreifen.[17] Erfahren die Bürger als Grundrechtsträger von einer

wenn die Ermittlungsmaßnahmen über den prozessualen Bereich hinaus in die vom GG geschützte Persönlichkeitssphäre des Betroffenen wirken, also bei Zwangsmaßnahmen."

[13] *Park*, § 1 Rn. 25. Aufgrund dieser Unklarheit entzünden strafprozessuale Zwangsmaßnahmen häufig Streit (vgl. *Michalke*, StraFo 3/2014, 89).

[14] Vgl. *BGHSt* 54, 69, 106 [Rn. 103]; auch *Roxin/Schünemann*, § 29 Rn. 6 ff. In der StPO sind die Durchsuchung und Beschlagnahme und sonstige individuelle heimliche Ermittlungsmaßnahmen zu zwangsmäßigen Ermittlungen i. d. R. mit dem Richtervorbehalt verbunden (z. B. §§ 98 Abs. 1, 105 Abs. 1, 100 Abs. 1, 100e Abs. 1 und 2 StPO). In dieser Hinsicht ist der grundrechtsbeeinträchtigende Zwang im Strafverfahren allein dem Richter in vollem Umfang gestattet, dagegen der StA und ihren Ermittlungspersonen nur in eingeschränktem Maße (*Roxin/Schünemann*, § 39 Rn. 26 f.).

[15] Vgl. *Schünemann*, ZStW 114 (2002), 1, 38.

[16] *BVerfGE* 118, 168, 197 [Rn. 134]; 120, 274, 325 [Rn. 238]; dazu *Kasiske*, StraFo 6/2010, 228, 231; *Zerbes/El-Ghazi*, NStZ 2015, 425, 432 [Tz. c)]. Jedoch ist mit Blick auf die sich weiterentwickelnden technischen Möglichkeiten das „Regel-Ausnahme-Verhältnis von offenen und verdeckten Maßnahmen" teilweise infrage gestellt, dadurch besteht eine Bedenklichkeit von „Vergeheimdienstlichung des Strafverfahrens" (*Singelnstein*, NStZ 2012, 593).

[17] Zwar darf der Grundsatz der Offenheit – der zu den Transparenzanforderungen zählt – für die Gefahrenabwehr und die Wahrnehmung der Aufgaben der Nachrichtendienste und für die damit verbunden Vorfeldermittlung im Bereich der Staatsschutzdelikte verfassungsrechtlich vertretbar ausgeschlossen werden, jedoch gilt dies für die Strafverfolgung nicht (*BVerfGE* 125, 260, 336 [Rn. 243]; 133, 277, 369 [Rn. 213]; 141, 220, 283 [Rn. 137]).

staatlichen Maßnahme vor ihrer Durchführung, können sie mit der Möglichkeit, auf den Gang der Ermittlung einzuwirken, ihre Interessen wahrnehmen.[18] Bei offenen Datenerhebungen kann der Betroffene – ggf. unter Hinzuziehung anwaltlichen Beistandes – bereits der Durchführung der Maßnahme entgegentreten, wenn es an den gesetzlichen Voraussetzungen fehlt, oder er kann zumindest die Einhaltung der im Durchsuchungsbeschluss gezogenen Grenzen einschließlich der Richtlinien der Beschlagnahme selbst überwachen und sich gegen Ausuferungen des Vollzugs der richterlichen Anordnungen wenden.[19] Hingegen ist das bei einer heimlichen Maßnahme nicht möglich. Hier kann der Betroffene gegen die Maßnahmen frühestens dann mit rechtlichen Mitteln vorgehen, wenn sie bereits vollzogen sind, und dies auch nur, wenn er darüber informiert wird oder auf andere Weise Kenntnis erlangt. Eingriffe dieser Art bergen daher durch den Ausschluss rechtlicher Abwehrmöglichkeiten und einer Einflusschance hohe Risiken für die Rechte der Betroffenen in sich[20] und erhöhen das Gewicht des Grundrechtseingriffs.[21] In dieser Hinsicht haben eingriffsintensive heimliche Ermittlungsmaßnahmen, nämlich „heimliche Zwangsmaßnahmen", einen neuen, eigenständigen Charakter.[22]

Aus Ermittlungshandlungen, die zur Festlegung des Verdachts vielfältige Herausforderungen erfüllen müssen, heimliche Ermittlung begrifflich klar abzugrenzen und weiter einheitlich zu regeln, ist (fast) unmöglich.[23] Aus der Sicht des Grundrechtsschutzes sind ausnahmsweise und speziell allein die „heimlichen Ermittlungsmaßnahmen." Insoweit muss zuerst die Heimlichkeit klar definiert werden, und nur so kann auch die Bestimmung der Ermächtigungen derartiger Maßnahmen ermöglicht werden (vgl. unten II.).

---

[18] *BVerfGE* 118, 168, 197 f. [Rn. 134]; 120, 274, 325 [Rn. 238].

[19] *BVerfGE* 115, 166, 194 f. [Rn. 106]; auch *BGHSt* 51, 211, 215 [Rn. 10]: „*Die offene Durchführung gibt dem Betroffenen die Möglichkeit, je nach den Umständen die Maßnahme durch Herausgabe des gesuchten Gegenstands abzuwenden bzw. in ihrer Dauer und Intensität zu begrenzen, ferner ihr – gegebenenfalls mit Hilfe anwaltlichen Beistands – bereits während des Vollzugs entgegenzutreten, wenn es an den gesetzlichen Voraussetzungen fehlt, oder aber zumindest die Art und Weise der Durchsuchung zu kontrollieren, insbesondere die Einhaltung der im Durchsuchungsbeschluss gezogenen Grenzen zu überwachen. Die heimliche Durchsuchung nimmt dem Betroffenen diese Möglichkeiten.*"

[20] *BVerfGE* 113, 348, 384; auch 107, 299, 321: „spezifische Risiken für die Rechte der Betroffenen".

[21] *BVerfGE* 107, 299, 321 [Tz. (d)]; 113, 348, 383 [Rn. 141]; 115, 166, 194 f. [Rn. 106]; 118, 168, 198 [Rn. 134]; 120, 274, 325 [Rn. 238]; 124, 43, 62 [Rn. 68] m. w. N.; *BGHSt* 51, 211, 215; *Zimmermann*, JA 5/2014, 321, 323: „*Verdeckte Maßnahmen bedeuten gerade aufgrund ihrer Heimlichkeit eine erhebliche Eingriffsvertiefung gegenüber ihrem offen vollzogenen Pendant.*"

[22] *Roxin/Schünemann*, § 36 Rn. 2; für Online-Durchsuchung, *BGHSt* 51, 211, 215 [Rn. 10]: „*Jede heimliche Durchsuchung ist im Vergleich zu der in §§ 102 ff. StPO geregelten offenen Durchsuchung wegen ihrer erhöhten Eingriffsintensität eine Zwangsmaßnahme mit einem neuen, eigenständigen Charakter.*"

[23] Vgl. *Hamm*, StV 2001, 81: Er versteht den Begriff der „heimlichen Ermittlungen" so weit, dass alle Fälle, in denen im Strafverfahren Strafbarkeitsvoraussetzungen nicht offen erhoben werden, darunter subsumiert werden.

b) Verfassungsrechtliche Rechtfertigung – Ausschluss von Rundumüberwachung

Indem eine Maßnahme nur heimlich getroffen wird, führt dies stets ohne Weiteres nicht zur Verletzung der absolut geschützten Menschenwürde.[24] Neben dem Grundrechtsschutz müssen auch wirksame Ermittlungstätigkeiten zur Bekämpfung schwerer organisierter und wirtschaftlicher Straftaten in Betracht gezogen werden.[25] So dürfen nach den Rspr. des *BVerfG* auch besonders eingriffsintensive, verdeckte Ermittlungsmaßnahmen wie z. B. akustische Wohnraumüberwachung, TKÜ, Online-Durchsuchung oder VDS nur wegen ihrer Heimlichkeit verfassungsrechtlich nicht verboten werden, vielmehr ist die Ermächtigungsgrundlage zu jeder Maßnahme durch strenge Eingriffsvoraussetzungen und verfahrensrechtliche Vorkehrungen, mit denen ihre besonders hohe Eingriffsintensität ausgeglichen werden kann, rechtsstaatlich auszugestalten.[26] Dabei hebt das Gericht „das Verbot der Rundumüberwachung" wiederholt hervor, was, obwohl keine ausdrückliche Regelung existiert, „*zur Wahrung eines in der Menschenwürde wurzelnden unverfügbaren Kerns der Person unmittelbar von Verfassung wegen gilt*".[27] Daher ist es unter dem GG verboten, personenbezogene Daten umfassend zu speichern und dadurch persönliches Verhalten umfassend wiederherzustellen.[28] Die heimlichen Maßnahmen müssen nach der Verhältnismäßigkeit (i. e. S.) mit erhöhten Eingriffsvoraussetzungen und besonders strengen verfahrensrechtlichen Vorkehrungen verbunden sein. In diesem Sinne hängt ihre verfassungsrechtliche Rechtfertigung ab von der gesetzlichen Ausgestaltung solcher Anforderungen (vgl. unten III.).

---

[24] Vgl. *BVerfGE* 109, 279, 313 [Rn. 118]: „*Ein heimliches Vorgehen des Staates führt an sich noch nicht zu einer Verletzung des absolut geschützten Achtungsanspruchs. Wird jemand zum Objekt einer Beobachtung, geht damit nicht zwingend eine Missachtung seines Wertes als Mensch einher.*"

[25] Vgl. für die Online-Durchsuchung, *BVerfGE* 120, 274, 320 f. [Rn. 221 und 223]: „*Bei der Beurteilung der Eignung ist dem Gesetzgeber ein beträchtlicher Einschätzungsspielraum eingeräumt. … (Weiter) ist die Eignung der geregelten Befugnis auch nicht deshalb zu verneinen, weil möglicherweise der Beweiswert der Erkenntnisse, die mittels des Zugriffs gewonnen werden, begrenzt ist.*"

[26] Vgl. *BVerfGE* 109, 279, 310 ff. (Großer Lauschangriff); 120, 274, 315 ff. (Online-Durchsuchung); 125, 260, 325 ff. (VDS); 129, 208, 240 ff., 250 ff. (TKÜ); 141, 220, 267 ff. (BKAG). Zulässigkeit und Reichweite dieser heimlichen Ermittlungsmaßnahme ist Sache der Rechtspolitik und daher durch die Gesetzgebung zu bestimmen (zust. *Vogel*, ZIS 2012, 480, 482).

[27] *BVerfGE* 141, 220, 317 [Rn. 254]; 109, 279, 315 [Rn. 124]; 323 [Rn. 150]; vgl. *BGHSt* 54, 69, 102 ff.

[28] Vgl. *BVerfGE* 125, 260, 324 [Rn. 218]: In der BRD dürfen die Handlungen der Bürger nicht total erfasst und aufgezeichnet werden.

II. „Heimlichkeit" bei heimlichen Zwangsmaßnahmen

1. Durchführung „ohne Wissen des Betroffenen"

(1) Der Grund, warum die heimlichen Zwangsmaßnahmen besonders behandelt werden sollten, liegt, wie bereits erwähnt, darin, dass zum Zeitpunkt eines schwerwiegenden Eingriffs in die Grundrechte dem Betroffenen als Grundrechtsträger und Prozesssubjekt seine Möglichkeiten, seine Interessen zu schützen und die Durchführung zu überwachen, bereits genommen sind und dass sie daraufhin aus Sicht des Rechtsstaatsprinzips immer zu übermäßigen Eingriffen führen können (vgl. oben I. 3. a)). Unter den heimlichen Zwangsmaßnahmen versteht man mit Recht, dass die Ermittlungsbehörden „zum Zeitpunkt der Durchführung" „ohne Wissen des Betroffenen, nämlich heimlich", seine Daten erheben bzw. verwenden.[29]

Ermittlungsmaßnahmen zum Datenzugriff betreffen nicht nur einen direkten Adressaten der Maßnahme, sondern auch weitere Personen, nämlich die von erhobenen, gespeicherten und verwendeten Daten betroffenen Personen. Eher sind die Letzteren entscheidend. Bei der Datenerhebung, die sich direkt gegen den Beschuldigten richtet, ist der von Daten Betroffene zugleich der Adressat der Maßnahme: z. B. bei eigenständiger TKÜ durch die Ermittlungsbehörden (§ 100a Abs. 1 StPO), bei Online-Durchsuchung (§ 100b StPO), bei akustischer Wohnraumüberwachung (§ 100c StPO), bei akustischer Überwachung außerhalb von Wohnraum (§ 100f StPO), bei Erhebung von Verkehrs- und Standortdaten in Echtzeit (§ 100g Abs. 1 StPO), bei Bildaufnahmen und Einsatz sonstiger technischer Mittel für Observationszwecke (§ 100h StPO) und bei – offener – Durchsuchung und Beschlagnahme gegen den Beschuldigten (§§ 94, 102 StPO). Bei der Datenerhebung, die sich gegen Dritte als Nichtverdächtige richtet, stellt hingegen der von Daten Betroffene meistens keinen Adressaten der Maßnahme dar: z. B. bei TKÜ durch die Mitwirkung des Dienstanbieters (§ 100a Abs. 1 S. 1 i. V. m. Abs. 4 StPO),[30] bei Erhebung von vorsorglich gespeicherten Verkehrs- und Standortdaten (§ 100g Abs. 2 StPO) und bei – offener – Durchsuchung und Beschlagnahme der beim Anbieter gespeicherten Daten (§§ 94, 103 StPO, insb. bei Maßnahme nach § 110 Abs. 3 StPO). In den letzteren Fällen ist es daher noch fraglich, nach welchem der Betroffenen die Heimlichkeit der Maßnahme gemessen werden soll. Heute sind personenbezogene Daten in vielen Fällen beim Dienstanbieter als Dritte umfangreich gespeichert und

[29] Vgl. *Roxin/Schünemann*, § 39 Rn. 29: „*Das Ermittlungsverfahren ist grundsätzlich geheim. Jedoch gewährt die StPO auch dem Beschuldigten und seinem Verteidiger gewisse Beteiligungsrechte und wird in diesem Umfang ‚parteiöffentlich'.*"

[30] Zwar wird die Überwachung gemäß §§ 100a, 100g StPO üblicherweise unter Mitwirkung des ISP durchgeführt (§§ 100a Abs. 4, 101a Abs. 1 StPO), aber ist sie ohne seine Hilfe auch nur von der Strafverfolgungsbehörde selbstständig durchzuführen, z. B. bei der W-LAN-Überwachung (*Meininghaus*, Der Zugriff auf E-Mails, 2007, 116 f.; M-G/*Schmitt*, StPO, § 100a Rn. 8; *Singelnstein*, NStZ 2012, 593, 599; *Zimmermann*, JA 5/2014, 321, 323). Auch die Quellen-TKÜ gemäß § 100a Abs. 1 S. 2 und 3 StPO richtet sich unmittelbar an den Beschuldigten.

die Ermittlungsbehörden müssen sie von ihm erhalten. Dabei ist er aber gesetzlich verpflichtet, auf Verlangen der Behörden Auskunft zu erteilen, und seine Kenntnisnahme von Maßnahmen ist zumeist in seinem grundrechtlichen Interesse nicht entscheidend. Hierbei hängt somit die Heimlichkeit eng mit der Wahrnehmung der Maßnahme des von Daten Betroffenen („Daten-Eigentümer“[31]) zusammen, nicht des Dienstanbieters, eines einfachen Gewahrsamsinhaber der Daten darstellt („Eigentümer des Speichers“). Hat eine Ermittlungsbehörde ohne Anhörung und Benachrichtigung des Beschuldigten beim unverdächtigen Anbieter die Daten sichergestellt, so soll diese Maßnahme aus einem solchen Grund noch als heimlich durchgeführt angesehen werden.[32] Zum Schluss ist für die Heimlichkeit der Maßnahme die Kenntnisnahme des Beschuldigten zum Zeitpunkt der Erfassung der Daten durch die Ermittlungsbehörde entscheidend;[33] der Dienstanbieter ist lediglich ein Adressat der Maßnahme. Dies ist dem Wortlaut und der Auslegung von Vorschriften der StPO zu entnehmen. Betroffener i. S. d. § 98 Abs. 2 StPO, bei dem es sich um die gerichtliche Bestätigung bzw. Entscheidung für nichtrichterliche Beschlagnahme handelt, ist zuerst jeder, dessen Rechtsposition durch die Beschlagnahme berührt ist.[34] Dazu zählen nach h. M. nicht nur Gewahrsamsinhaber, Eigentümer und Besitzer der Gegenstände, sondern auch der Betroffene, dessen personenbezogene Daten das beschlagnahmte Beweismittel enthält:[35] z. B. der Kontoinhaber bei der Beschlagnahme von Kontounterlagen in einem Kreditinstitut, der Geschäftsinhaber bzw. der Geheimnisgeschützte bei der Beschlagnahme von Geschäftsunterlagen oder der Absender bzw. Empfänger bei der Beschlagnahme von Briefen (§ 101a Abs. 4 S. 1 Nr. 2

---

[31] Vgl. *Wicker*, MMR 2013, 765, 766 [Tz. II.].

[32] Vgl. *Klesczewski*, ZStW 123 (2011), 737, 749; *BVerfGE* 107, 299, 321: „*Die Auskunft wird … ohne Anhörung des Betroffenen angeordnet und damit ohne Kenntnisnahme heimlich vollzogen*“; auch *BGH* NJW 2010, 1297, 1298 [Rn. 19]: „*… um offene Ermittlungsmaßnahmen, deren Anordnung den Betroffenen und Verfahrensbeteiligten bekannt zu machen ist (§§ 33 Abs. 1, 35 Abs. 2 StPO). Der Beschuldigte ist deshalb auch dann von der Beschlagnahme der in seinem elektronischen Postfach gelagerten E-Mail-Nachrichten zu unterrichten, wenn die Daten auf Grund eines Zugriffs beim Provider auf dessen Mailserver sichergestellt wurden*“; a. A. *Brunst*, CR 2009, 584, 592 [Tz. a) a. E.]: „*Die Offenheit einer Maßnahme kann sich (daher) in bestimmten Fällen also darauf beschränken, dass die Strafverfolgungsbehörden den Betroffenen im Nachhinein über die Tatsache einer vorher bereits durchgeführten E-Mail-Beschlagnahme informieren*“; dazu *Singelnstein*, NStZ 2012, 593, 596: nur bei drohender Zweckverfehlung. *Brunst* ist der Ansicht, dass im Rahmen einer Sicherstellung der Daten beim Provider eine vorherige Benachrichtigung des Betroffenen eine Ausnahme darstellt, und *Singelnstein* ist der Ansicht, dass die Unterrichtung ausnahmsweise verschoben werden darf, aber so früh wie möglich erfolgen muss. In diesem Fall sollte man jedoch annehmen, dass die Maßnahmen nicht mehr offen, sondern heimlich erfolgen.

[33] Obwohl die Durchsuchung geheim vorbereitet wurde, führt sie nicht zu einer heimlichen Ermittlungsmaßnahme (M-G/*Schmitt*, StPO, § 105 Rn. 13).

[34] *Greven*, KK-StPO, § 98 Rn. 18; *Park*, § 3 Rn. 502; *Wohlers*/*Greco*, SK-StPO, § 98 Rn. 48.

[35] *Greven*, KK-StPO, § 98 Rn. 18; M-G/*Schmitt*, StPO, § 98 Rn. 15 und 20; *Park*, § 3 Rn. 502; *Wohlers*/*Greco*, SK-StPO, § 98 Rn. 48; dazu *Singelnstein*, NStZ 2012, 593, 603: wer in seiner informationellen Selbstbestimmung beeinträchtigt wird.

StPO). Dies gilt auch für die Auslegung des § 101 StPO zur Regelung nachträglicher Benachrichtigung bei den verdeckten Maßnahmen in §§ 99 ff. StPO. Betroffene der TKÜ in der Vorschrift sind die Beteiligten der überwachten TK (vgl. § 101a Abs. 4 S. 1 Nr. 2 StPO). Bei der Entscheidung der „Heimlichkeit" der heimlichen Zwangsmaßnahmen zur Datensicherung im Ermittlungsverfahren ist nach alledem die „Kenntnisnahme des von Daten Betroffenen zum Zeitpunkt der Durchführung der Maßnahme" von entscheidender Bedeutung.

(2) Zum anderen stellt sich die Frage, ob auch die Kenntnisnahme des Dienstanbieters, der einen Gewahrsamsinhaber der Daten als Dritter darstellt, hierbei zu berücksichtigen ist. Dürfen die serverbasiert gespeicherten Daten so – nicht nur gegenüber dem von Daten Betroffenen, sondern – auch gegenüber ihm geheim erhoben werden?[36] Eine Ansicht verweist darauf, dass der Zugriff auf solche Daten typischerweise gegenüber dem Dienstanbieter offen erfolgt und außerdem ein Zugriff, der mittels Zugangssicherungscodes des von der Durchsuchung Betroffenen – etwa wenn den Ermittlungsbehörden Benutzername und Passwort bekannt sind – ohne Wissen des Anbieters erfolgt, nicht nur unzulässig, sondern auch (theoretisch denkbar, aber) angesichts § 100a Abs. 4 StPO (= § 100b Abs. 3 StPO a. F.) und § 110 TKG regelmäßig nicht erforderlich ist.[37] Der Anbieter ist zunächst grundlegend als Zeuge dazu verpflichtet, ihm bekannte Tatsachen auszusagen (§§ 48 Abs. 1 S. 2, 161a Abs. 1 S. 1 StPO) und als Gewahrsamsinhaber von Beweisgegenständen dazu verpflichtet, sie vorzulegen und auszuliefern (§ 95 Abs. 1 StPO). Auch gemäß § 110 TKG und TKÜV ist daneben jeder, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, zur Mitwirkung bei der Datenerhebung der Ermittlungsbehörden verpflichtet (vgl. § 100a Abs. 4 StPO für die TK-Überwachung, § 101a Abs. 1 S. 1 StPO für die Erhebung der Verkehrsdaten und § 100j Abs. 5 StPO für die Erhebung der Bestandsdaten und Zugangssicherungscodes). Hiernach stellt die Datenerhebung beim Dienstanbieter seinerseits stets offene Ermittlung dar.

Dies ist aber nicht immer so und sollte auch nicht so sein. Zuerst ergibt sich aus dem Wortlaut des § 100a Abs. 4 StPO, dass der Anbieter zur Mitwirkung bei den Ermittlungsbehörden verpflichtet ist, während diese zur Mitwirkung nicht verpflichtet sind. Außerdem können bei der heimlichen Online-Durchsuchung nach § 100b StPO, die in jüngster Zeit eingeführt wurde, die Ermittlungsbehörden über das infiltrierte informationstechnische System des Betroffenen ohne Wissen des Anbieters auf dessen Server zugreifen. Daneben ist es auch nach § 110 Abs. 3 StPO, der am 1. Januar 2008 schon in Kraft trat, zulässig, – mindestens zum Zeitpunkt der Durchführung der Maßnahme – ohne Wissen oder ohne Zustimmung des Dienst-

[36] Praktisch erfolgt die exemplarische TK-Überwachung, etwa der Eingriff in laufende (Internet-)Telefonie, meist ohne Wissen und Hilfe des Anbieters; abw. *Zerbes/El-Ghazi*, NStZ 2015, 425, 432: Das Abfragen der Nachrichten beim Anbieter ist gesetzgeberisches Konzept.

[37] *Brodowski*, JR 2009, 402, 403 [Tz. b) (ii)] und 411 [Tz. 2. b)]; dazu *Singelnstein*, NStZ 2012, 593, 596 a. E.: „*Gegenüber dem Anbieter … hat die Maßnahme ohne Ausnahme offen zu erfolgen. Daher ist (etwa der) … verdeckte Zugriff auf Daten in einer Cloud durch Überwinden des Passwortschutzes nicht von der StPO gedeckt.*"

anbieters auf durch ihn in Verwahrung genommene Daten zuzugreifen.[38] So ist es zweifelhaft, ob ein Zugriff durch die Erweiterung der Durchsicht aufgrund des § 110 Abs. 3 StPO, die eine offene Maßnahme, die sich unmittelbar an den von Daten Betroffenen richtet, voraussetzt (vgl. Kapitel 4, C. III. 2. a) cc)), auch dem Anbieter als schlichtem Verwahrer der Daten stets bekannt werden muss.[39] Unter heutigen informationstechnischen Gegebenheiten ist nämlich die Kenntnisnahme des Anbieters für die Wahrung der Heimlichkeit oder Offenheit der Maßnahmen nicht entscheidend. Mindestens bei der TK-Überwachung nach § 100a StPO oder der Online-Durchsuchung nach § 100b StPO ist die Offenheit der Maßnahme gegenüber dem Anbieter nicht unbedingt gefordert.

2. Verhältnis zum Recht auf rechtliches Gehör

Die Heimlichkeit einer Zwangsmaßnahme kollidiert nicht als solche mit dem Anspruch auf rechtliches Gehör (Art. 103 Abs. 1 GG & Art. 6 EMRK), das auf der Pflicht zur Wahrung der Menschenwürde basiert und sich aus dem Rechtsstaatsgedanken ableitet. Denn dieser kann ausnahmsweise ausgeschlossen werden. Durch die Gewährleistung rechtlichen Gehörs kann der Mensch zum bloßen Objekt des Verfahrens gemacht werden und ihm muss die Möglichkeit gegeben werden, vor Entscheidungen, die seine Rechte betreffen, zu Wort zu kommen und damit auf den Gang und das Ergebnis des Strafverfahrens Einfluss zu nehmen.[40] Danach dürfen sich gerichtliche Entscheidungen grundsätzlich nicht auf solche Tatsachen oder Beweisergebnisse stützen, zu denen der Beschuldigte noch nicht gehört worden ist.[41] Die nähere Ausgestaltung des rechtlichen Gehörs bleibt aber den einzelnen Verfahrensvorschriften überlassen,[42] und für das Strafverfahren ist dies in § 33 StPO ausgeprägt. Gemäß der Vorschrift muss – bei allen Zwangsmaßnahmen, die mit dem Richtervorbehalt verbunden sind – das richterliche Gehör grundsätzlich vor der Entscheidung gewährleistet werden (Art. 103 Abs. 1 GG, § 33 Abs. 1–3 StPO), jedoch darf es ausnahmsweise ausgeschlossen werden, sofern die vorherige Anhö-

[38] Vgl. *Zimmermann*, JA 5/2014, 321, 325; auch *Kudlich*, GA 2011, 193, 207.

[39] Vgl. *Brodowski/Eisenmenger*, ZD 3/2014, 119, 125 [Tz. 5]: Diese Durchsicht ist nur gegenüber dem unmittelbar Betroffenen eine offene Maßnahme, aber der Betreiber des Speichermediums erfährt zunächst nichts. Gleichwohl bleibt auf jeden Fall hier die Offenheit der Maßnahme gegenüber dem Anbieter – unvollständig – bestehen. Denn der die Durchsicht durchführende Beamte hat nach der Vorschrift binnen drei Tagen die gerichtliche Bestätigung zu beantragen (§ 110 Abs. 3 S. 2 Hs. 2 i. V. m. § 98 Abs. 2 S. 1 StPO; BT-Drs. 16/6979, S. 45; M-G/*Schmitt*, StPO, § 110 Rn. 8), und der Anbieter ist im Verlauf einer gesetzlichen Anhörung (§ 33 Abs. 3 und 4 StPO) von der Maßnahme zu benachrichtigen (BT-Drs. a. a. O.; M-G/*Schmitt*, a. a. O.; *Park*, § 4 Rn. 820).

[40] *BVerfGE* 1, 418, 429 [Rn. 51]; 63, 380, 390; 86, 133, 144 [Rn. 35]; 89, 28, 35 m. w. N.

[41] M-G/*Schmitt*, StPO, Einl. Rn. 29; *Roxin/Schünemann*, § 18 Rn. 4.

[42] *BVerfGE* 9, 89, 95 f.; 67, 208, 211; 74, 228, 233.

rung den Zweck der Anordnung gefährden würde (§ 33 Abs. 4 S. 1 StPO).[43] Nach der Literatur ist eine derartige Gefährdung anzunehmen, wenn aufgrund von Tatsachen im Einzelfall oder nach der Lebenserfahrung naheliegt oder zumindest die Gefahr besteht, dass der Betroffene bei vorheriger Anhörung die Anordnung etwa von Durchsuchung, Beschlagnahme oder TKÜ vereiteln würde, z. B. durch Verstecken, Vernichtung oder Löschung der zu beschlagnahmenden Gegenstände.[44] Nach h. M. darf somit das Gehör nicht nur bei Fällen der Untersuchungshaft (§§ 112 ff. StPO) und der Beschlagnahme (§§ 94 ff. StPO), die in der Vorschrift ausdrücklich aufgezählt sind, sondern auch bei Fällen der Durchsuchung (§§ 102 ff. StPO), der Beschlagnahme von Postsendungen und Telegrammen (§ 99 StPO), der TKÜ (§ 100a StPO) oder der verdeckten Ermittler (§ 110a StPO) wegen der „Notwendigkeit überraschender Maßnahmen" unterbleiben.[45] Insoweit würde diese Gefährdung insb. für heimliche Maßnahmen der §§ 99 ff. StPO die „Notwendigkeit heimlicher Maßnahmen" bedeuten und eine solche Abweichung ist eine gesetzgeberische Entscheidung. In der Praxis wird aber bei – offener – Beschlagnahme und Durchsuchung diese vorherige Anhörung fast ausnahmslos zugunsten überraschender Maßnahmen ausgeschlossen.[46] Zum Schließen dieser Lücke ist daher dem Betroffenen mindestens die Möglichkeit nachträglichen rechtlichen Gehöres, d. h. die Gelegenheit des Rechtsbehelfs gegen die Anordnung als solche sowie die Art und Weise ihres Vollzugs, zu verschaffen.

3. Verhältnis zur Bekanntmachung und Benachrichtigung

(1) Im Rahmen der kriminalistischen Zwangsmaßnahmen, die richterlich angeordnet[47] und offen durchgeführt werden, ergibt sich der Grundsatz der Offenheit

---

[43] *BGH* NJW 2010, 1297, 1298 [Rn. 13]; *Maul*, KK-StPO, § 33 Rn. 12; M-G/*Schmitt*, StPO, § 33 Rn. 16; *Roxin*/*Schünemann*, § 18 Rn. 10 und § 23 Rn. 8; weiter für die Durchsuchung *Bruns*, KK-StPO, § 105 Rn. 5; M-G/*Schmitt*, StPO, § 105 Rn. 4; *Wohlers*, SK-StPO, § 105 Rn. 30.

[44] M-G/*Schmitt*, StPO, § 33 Rn. 16.

[45] *Maul*, KK-StPO, § 33 Rn. 12; M-G/*Schmitt*, StPO, § 33 Rn. 15 und § 100e Rn. 10. Dagegen darf von der Anhörung nicht deshalb abgesehen werden, weil der dazu erforderliche Aufwand unverhältnismäßig wäre (*Maul*, a. a. O. Rn. 13; M-G/*Schmitt*, a. a. O. Rn. 17; *Park*, § 2 Rn. 71).

[46] Vgl. *BGH* NJW 2010, 1297, 1298 [Rn. 13]. Jedoch scheint die Gewährung rechtlichen Gehörs praktisch völlig außer Acht gelassen zu werden. Laut *Park „hat sich dieses Regel-Ausnahme-Verhältnis in der Praxis völlig umgekehrt und die Frage der Anhörung des Betroffenen wird fast ausnahmslos mit keinem Wort erwähnt*" (§ 2 Rn. 72 und § 3 Rn. 473). Die Umstände, die die Anwendung des § 33 Abs. 4 S. 1 StPO veranlasst haben, sind in dem Beschluss darzulegen, wenn sie nicht offensichtlich sind (BT-Drs. 18/5088, S. 36; M-G/*Schmitt*, StPO, § 33 Rn. 16 und § 101a Rn. 32). So ist diese Praxis bedenklich (*Park*, § 2 Rn. 73 und § 3 Rn. 474).

[47] Bei richterlicher Anordnung nach dem Antrag auf Anordnung von Zwangsmaßnahmen der StA handelt es sich funktionell um Akte der Rechtsprechung (M-G/*Schmitt*, StPO, § 162 Rn. 1).

verfassungsrechtlich aus Anforderungen an Transparenz (vgl. eingehend unten III. 3. a)) und fachrechtlich auch aus §§ 33 Abs. 4 S. 1, 35 und 106 StPO.[48] Absehen von vorheriger Anhörung nach § 33 Abs. 4 S. 1 StPO muss sich von dem Gebot der Bekanntmachung der Entscheidung „vor der Durchführung der Maßnahme" nach § 35 Abs. 2 StPO unterscheiden. Eher hat die Offenheit richterlicher Zwangsmaßnahmen näher mit § 35 Abs. 2 StPO als mit § 33 Abs. 4 StPO zu tun.[49] In der ersteren Vorschrift ist nicht – anders als in der letzteren für rechtliches Gehör – die Zurückstellung oder das Absehen von einer Bekanntmachung/Benachrichtigung vorgesehen. Diesbezüglich gilt nach der Entscheidung des *BGH* und dem Schrifttum für die – offene – Durchsuchung und Beschlagnahme gemäß §§ 94 ff., 102 ff. StPO die weitere Zurückstellung bzw. das endgültige Absehen von der Benachrichtigung wegen Gefährdung des Untersuchungszwecks nach § 101 Abs. 5 StPO für die heimlichen Ermittlungsmaßnahmen nicht entsprechend.[50] Die Bekanntmachung der Anordnung an den Betroffenen bei einfacher Beschlagnahme und Durchsuchung darf daher wegen der „Notwendigkeit überraschender Maßnahmen" „nur bis unmittelbar vor Beginn ihrer Durchführung" „zurückgestellt" werden.[51] Wenn personenbezogene Daten des Beschuldigten wie etwa E-Mails durch die allgemeine Beschlagnahme und Durchsuchung aus dem Dienstanbieter-Server sichergestellt werden, ist er somit von solchen Maßnahmen spätestens „bis zum Beginn ihrer Durchführung", also „unmittelbar vor der Herausgabe der Daten" zu unterrichten.[52] Wenn sonst diese Bekanntgabe unter entsprechender Anwendung des § 101 Abs. 5 und 6 StPO auch nach dem Schluss der Durchführung noch weiter zurückgestellt

---

[48] *BVerfGE* 125, 260, 335 f. [Rn. 243]; auch *Zimmermann*, JA 5/2014, 321, 322; abw. *Wohlers*/*Greco*, SK-StPO, § 94 Rn. 27 [Fn. 100]: „*§ 35 StPO findet nur auf richterlich angeordnete Beschlagnahmen Anwendung und es stellt sich ferner die Frage, was man unter der Offenheit einer Maßnahme versteht.*" Jedoch soll die Offenheit auch für die durch die StA oder ihre Ermittlungspersonen angeordnete Durchsuchung und Beschlagnahme bei Gefahr im Verzug (§ 98 Abs. 1 S. 1 Alt. 2, § 105 Abs. 1 S. 1 Alt. 2 StPO) gelten. Es gibt keinen Grund, die grundsätzlich geforderte Bekanntmachung/Benachrichtigung im Ausnahmefall der Anordnung von Ermittlungsbehörden auszuschließen (*argumentum a maiore ad minus*; vgl. § 98 Abs. 2 S. 5 StPO).

[49] Vgl. *Obenhaus*, NJW 2010, 651, 653 [Tz. 2.]: Die Benachrichtigung dient der Wahrung des Charakters als offener Datenzugriff.

[50] *BGH* NJW 2010, 1297, 1298 [Rn. 19]; NStZ 2015, 704, 705; *Greven*, KK-StPO, § 98 Rn. 21; *Kasiske*, StraFo 6/2010, 228, 232; M-G/*Schmitt*, StPO, § 98 Rn. 10; *Singelnstein*, NStZ 2012, 593, 596.

[51] *Greven*, KK-StPO, § 98 Rn. 21; M-G/*Schmitt*, StPO, § 98 Rn. 10 und § 105 Rn. 4; *Wohlers*/*Jäger*, SK-StPO, § 105 Rn. 30.

[52] *BVerfGE* 124, 43, 71 f.; *BGH* NJW 2010, 1297, 1298 [Rn. 19]; M-G/*Schmitt*, StPO, § 98 Rn. 10; *Wohlers*/*Greco*, SK-StPO, § 98 Rn. 23; abw. *Sieber*, 69. DJT 2012, C 111: Unmittelbar nach der Durchführung ausnahmslos bekanntgegeben werden; a. A. *Brunst*, CR 2009, 584, 592 [Tz. a)]; vgl. *Wohlers*/*Greco*, SK-StPO, § 94 Rn. 27 [Fn. 100]. Insb. laut *Brunst* ist eine solche Vorabbekanntmachung in der Praxis eher eine Ausnahme, und darüber hinaus werde die Offenheit einer Maßnahme dadurch erreicht, dass die Strafverfolgungsbehörden den Betroffenen im Nachhinein über sie informieren. Dies steht jedoch im Widerspruch zu der Auslegung der StPO und dem vorigen Urteil des *BVerfG*.

oder endgültig ausgeschlossen wird, so kollidiert dies deswegen mit der Offenheit der Maßnahme, denn ein solcher Eingriff stellt keine offene Maßnahme mehr dar, sondern er ist eine heimliche.[53] Wird eine Zwangsmaßnahme, die richterlich anzuordnen ist, vor Ort zum Zeitpunkt des Beginns ihrer Durchführung oder zum Zeitpunkt des Erhalts der Daten vom Anbieter (fern)schriftlich, (fern)mündlich oder telefonisch dem Beschuldigten oder dem Gewahrsamsinhaber, Eigentümer, Besitzer der durchsuchten Räume bzw. der beschlagnahmten Sache bekannt gemacht, dann erfolgte sie nicht heimlich, und lediglich die vorherige Anhörung nach § 33 Abs. 4 S. 1 StPO wurde ausgeschlossen. Diesbezüglich hat das *BVerfG* bereits zutreffend ausgeführt:

> „Werden in einem Postfach auf dem Mailserver des Providers eingegangene E-Mails sichergestellt, ist zum Schutz des Postfachinhabers … zu fordern, dass er im Regelfall zuvor von den Strafverfolgungsbehörden unterrichtet wird, damit er jedenfalls bei der Sichtung seines E-Mail-Bestands seine Rechte wahrnehmen kann. … Diesen Anforderungen wird durch § 35 StPO und § 98 Abs. 2 S. 6 StPO Rechnung getragen. … (Jedoch) sind richterliche Anordnungen von Durchsuchungen … und Beschlagnahmen in jedem Fall dem Betroffenen vor Durchführung der Maßnahmen gemäß § 35 StPO bekannt zu geben. Im Falle einer vorläufigen Sicherstellung oder Beschlagnahme durch die StA oder ihre Ermittlungspersonen wegen Gefahr im Verzuge ist der Betroffene gemäß § 98 Abs. 2 S. 6 StPO über sein Antragsrecht nach § 98 Abs. 2 S. 2 StPO zu belehren."[54]

Bei verdeckter Ermittlungsmaßnahme hat andererseits der Betroffene keinen Anspruch auf Kenntnis von der Datenerhebung. Bei heimlichen Zwangsmaßnahmen, für denen der Richtervorbehalt vorausgesetzt ist, muss freilich der Betroffene zum effektiven Rechtsschutz (Art. 19 Abs. 4 GG) gemäß § 101 Abs. 4 S. 1–2 StPO grundsätzlich nach der Beendigung der Durchführung jeder Maßnahme, also nachträglich benachrichtigt werden. Diese Mitteilung darf aber ausnahmsweise nach der Abwägung zurückgestellt oder ausgeschlossen werden (§ 101 Abs. 4 S. 3, Abs. 5 S. 1 StPO und § 101a Abs. 6 StPO). Bei anderen als der Maßnahme nach § 100g StPO bleibt insofern die Zuständigkeit für die Zurückstellung der Benachrichtigung für das erste Jahr nach Beendigung jeder Maßnahme bei den Ermittlungsbehörden, insbesondere dem Staatsanwalt, während dieselbe für weitere Zurückstellung und endgültiges Absehen dem Gericht zugewiesen wird (§ 101 Abs. 5 und Abs. 6 S. 1 StPO). Bei Erhebung der Verkehrsdaten nach § 100g StPO hingegen bedarf es für die

---

[53] Daher erscheint es paradox, dass grundsätzliche Offenheit der Maßnahme wegen – rechtswidrigen – Absehens bzw. Verbotes der vorherigen Unterrichtung an den Betroffenen in der Praxis kritisiert wird (*Brunst*, CR 2009, 584, 592 [Tz. a)]).

[54] *BVerfGE* 124, 43, 71 f. [Rn. 94 f.]: S. 6 ist ein Schreibfehler von S. 5. Ein Teil der Ausführungen des Beschlusses (Rn. 94 S. 2–4: „*Ausnahmen von der Unterrichtungspflicht können geboten sein, wenn die Kenntnis des Eingriffs in das Fernmeldegeheimnis dazu führen würde, dass dieser seinen Zweck verfehlt. Werden auf dem Mailserver des Providers gespeicherte E-Mails ausnahmsweise ohne Wissen des Postfachinhabers sichergestellt, so ist dieser so früh, wie es die wirksame Verfolgung des Ermittlungszwecks erlaubt, zu unterrichten.*") ist dabei unsachgemäß, da er eine heimliche Maßnahme betrifft (vgl. *Wohlers*/*Greco*, SK-StPO, § 94 Rn. 27 [Fn. 100]).

Zurückstellung und das Absehen stets einer Anordnung des zuständigen Gerichts (§ 101a Abs. 6 S. 2 i. V. m. § 101 Abs. 4 – 7 StPO).

(2) Die Entscheidung darüber, ob die Beweiserhebung zum Zwecke der Strafverfolgung heimlich oder offen erfolgen soll, steht i. d. R. im Ermessen der Ermittlungsbehörden. Auch wenn eine Zwangsmaßnahme grundsätzlich bzw. endlich durch richterliche Anordnung angeordnet werden muss, steht eine solche Entscheidung daher dem Staatsanwalt zu, der Herr des Ermittlungsverfahrens ist und die Anordnung beantragt. Daher muss er sich zur Offenheit der Maßnahme spätestens bis zum Zeitpunkt des Antrags auf ihre Anordnung entschließen; hier beschränkt sich die richterliche Prüfung auf die Zulässigkeit und Grenzen der beantragten Maßnahme. Ermittlungsmaßnahmen, die in einzelnen Fällen ergriffen werden, werden dabei nicht bündelweise, sondern isoliert bewertet.[55]

Mit Blick auf die Justizförmigkeit des Strafverfahrens sowie das Gewicht des Eingriffs und verfahrensrechtliche Kontrolle ist es rechtsstaatlich unzulässig, gestützt auf richterliche Anordnung, die zur offenen Ermittlung erlassen wird (§§ 98 Abs. 1, 105 Abs. 1 StPO), ohne Benachrichtigung des von Daten Betroffenen die Durchsuchung und Beschlagnahme vorzunehmen. Dies ist die Vermeidung der legitimen, aber strengeren Ermächtigungsnorm. Etwa, wenn zwar die Erhebung personenbezogener Daten wie E-Mails aufgrund der §§ 94 ff., 103 ff. StPO angeordnet wurde, aber die Mitteilung des Eingriffs wegen der Gefährdung des Ermittlungszwecks auch nachträglich weiter zurückgestellt oder endgültig ausgeschlossen wird, so ist die Maßnahme rechtswidrig. Ein Verstoß gegen diese Regelungen führt jedoch nach der Rechtsprechung des *BGH* und einer Stellungnahme in der Literatur i. d. R. nicht zu einem Beweisverwertungsverbot.[56] Hingegen wäre das Gegenteil ggf. – bei dringenden Fällen – möglich (*argumentum a maiore ad minus*).

4. Exkurs: Heimlichkeit in der Verkehrsdatenerhebung (§§ 100g, 101a StPO)

In den Gesetzesmaterialien zur Novelle der Ermächtigungsnorm zur Erhebung der Verkehrsdaten, die auf die Rechtsprechung des *BVerfG* vom 2. März 2010 zurückgeführt ist, wird i. R. d. Transparenzanforderungen und der darauf begründeten Qualifizierung der Verkehrsdatenabfrage[57] wie folgt ausgeführt:

> „Durch die Streichung der Worte ‚auch ohne Wissen des Betroffenen' wird deutlich gemacht, dass es sich bei der Verkehrsdatenerhebung nach § 100g StPO-E grundsätzlich nicht

[55] Vgl. *BGHSt* 51, 211, 219 [Rn. 22]: „*Es ist unzulässig, einzelne Elemente von Eingriffsermächtigungen zu kombinieren, um eine Grundlage für eine neue technisch mögliche Ermittlungsmaßnahme zu schaffen. Dies würde dem Grundsatz des Gesetzesvorbehalts für Eingriffe in Grundrechte (Art. 20 Abs. 3 GG) sowie dem Grundsatz der Normenklarheit und Tatbestandsbestimmtheit von strafprozessualen Eingriffsnormen widersprechen.*"

[56] *BGH* NJW NStZ 2015, 704, 705; *Greven*, KK-StPO, § 98 Rn. 21.

[57] Vgl. *BVerfGE* 125, 260, 334 ff. [Rn. 240 – 245].

um eine heimliche Maßnahme handelt. Soweit möglich muss die Verwendung der Daten offen erfolgen“[58] und: „In § 101a StPO n. F. wird das Verfahren zur Erhebung von Verkehrsdaten an Verfahren zur Anordnung offener Maßnahmen angeglichen.“[59]

Es ist jedoch zweifelhaft, ob die obigen Ausführungen theoretisch vertretbar sind. Da allerdings nach den Transparenzanforderungen die Erhebung und Nutzung von personenbezogenen Daten i. d. R. offen erfolgen soll (§§ 33, 35, 102, 103, 106 StPO), ist der Betroffene vor der Abfrage bzw. Übermittlung seiner Daten zu benachrichtigen.[60] Jedoch wird die offene Erhebung der Verkehrsdaten zum Zwecke der Strafverfolgung eher die Ausnahme sein, worauf im Schrifttum zutreffend hingewiesen wird: Die Daten werden in der Praxis im Normalfall zu einem frühen Zeitpunkt erhoben, in dem die Ermittlungen noch heimlich geführt werden, etwa um eventuell tatbeteiligte Personen zu identifizieren oder weiter verdeckte Maßnahmen wie eine Telefonüberwachung vorzubereiten.[61] So wird die Echtzeitüberwachung der Verkehrsdaten nach § 100g Abs. 1 StPO zwangsläufig von Natur aus – ausnahmslos – verdeckt erfolgen. Auch die Erhebung der gespeicherten Verkehrsdaten gemäß § 100g Abs. 2 StPO, nämlich die VDS, erfolgt fast immer verdeckt, wobei die vorherige Anhörung i. d. R. nach § 33 Abs. 4 S. 1 StPO geschehen wird. Dies zeigt sich auch daran, dass für den § 101a Abs. 6 StPO, die Benachrichtigung des Betroffenen bei der Verkehrsdatenerhebung zu bestimmen, der § 101 Abs. 4 bis 7 StPO, dieselbe bei sonstigen heimlichen Maßnahmen zu regeln, abgesehen von der Zuständigkeit fast vollständig entsprechend gilt. Eine derartige Regelung steht im Widerspruch dazu, dass die Erhebung der Verkehrsdaten grundsätzlich eine offene Maßnahme sein soll, für die § 35 StPO gilt. Dieses Verständnis ist außerdem in rechtssystematischer Hinsicht sinnvoll. Denn die Eingriffsvoraussetzungen und Verfahrensgarantien zur Verkehrsdatenerhebung (§§ 100g, 101a und b StPO) sind strenger als dieselben zu einfacher Beschlagnahme und Durchsuchung (§§ 94 ff., 102 ff. StPO) und vielmehr mit denselben der TKÜ (§§ 100a, d und e StPO) vergleichbar. Wenn eine Ermittlungsbehörde daher die auf dem ISP gespeicherten Verkehrsdaten – in der Praxis nur wenig oder gar nicht – „offen“ erheben will, so muss dies aufgrund der §§ 94 ff., 102 ff. i. V. m. § 35 StPO zu rechtfertigen sein, nicht aufgrund der §§ 100g, 101a StPO. Ansonsten können die Interessen der Strafverfolgung unverhältnismäßig verletzt werden. In dieser Hinsicht ist die Anwendung von § 35 oder § 101 StPO zur Bekanntmachung oder Benachrichtigung als ein Kriterium anzusehen, das zwischen grundsätzlich offenen und ursprünglich heimlichen Maßnahmen unterscheidet. Aus alledem soll die Verkehrsdatenerhebung gemäß § 100g StPO von Natur aus als eine heimliche Maßnahme behandelt werden.

[58] BT-Drs. 18/5088, S. 31; M-G/*Schmitt*, StPO, § 100g Rn. 11. Damit hat der Gesetzgeber § 100g StPO aus den heimlichen Maßnahmen, die dem § 101 StPO unterliegen, herausgenommen und stattdessen die eigenständigen Regelungen in § 101a Abs. 6 StPO n. F. eingefügt (vgl. BT-Drs. a. a. O. S. 33 f.).

[59] BT-Drs. 18/5088, S. 34.

[60] *BVerfGE* 125, 260, 335 f.

[61] M-G/*Schmitt*, StPO, § 101a Rn. 32.

III. Zulässigkeitsvoraussetzungen zu den heimlichen Zwangsmaßnahmen – i. R. d. Erhebung und Verwendung personenbezogener Daten

1. Vorrede

Zwar sind heimliche Ermittlungsmaßnahmen erforderlich und zulässig, jedoch sind sie nicht alle so grundrechtsinvasiv, dass sie immer durch eine eigenständige Ermächtigung geregelt und stets gerichtlich kontrolliert werden müssen. Wie bereits erwähnt, sollten die „heimlichen Zwangsmaßnahmen" speziell behandelt werden (vgl. oben I. 3.). Dabei ist der Grundsatz der Verhältnismäßigkeit bereits in der Phase der Gesetzgebung zu berücksichtigen (Gesetzesvorbehalt bzw. Parlamentsvorbehalt)[62], und die Rechtsgrundlage für jede Maßnahme ist im Verhältnis zu ihrer Eingriffsintensität individuell auszugestalten. I. R. d. Eingriffsvoraussetzungen der Ermittlungsmaßnahmen werden zum einen die „Schwere der Straftat" und die „Stärke des Tatverdachts" berücksichtigt.[63] Hierbei kommt bei den vom Datenzugriff betroffenen Maßnahmen nicht nur die potenzielle Beweisbedeutung der sicherzustellenden Daten, sondern auch der Grad des auf die Daten bezogenen Auffindeverdachts in Betracht.[64] Daneben gehört zu solchen Voraussetzungen die Subsidiarität,[65] die die *ultima ratio* darstellt, die sich aus der Erforderlichkeit und Verhältnismäßigkeit ergibt. Die heimlichen Ermittlungsmaßnahmen gehen nämlich i. d. R. den gleichrangigen offenen nach. Zum anderen wird verfahrensrechtlichen Vorkehrungen Rechnung getragen. Sie müssen ein ausreichendes Mittel sein, um im Strafverfolgungsverfahren den übermäßigen Datenzugriffen oder unbefugten bzw. unrechtmäßigen Verwendungen zu begegnen, und die Eingriffsintensität hinreichend auszugleichen. Die Voraussetzungen des Eingriffs und die verfahrensrechtlichen Vorkehrungen für – technische – heimliche Ermittlungsmethoden (z. B. §§ 99 ff.

[62] Vgl. für die akustische Wohnraumüberwachung *BVerfGE* 109, 279, 343 [Rn. 226]; für § 81g StPO *OLG Jena*, NJW 1999, 3571 und dazu M-G/*Schmitt*, StPO § 81g Rn. 7a: Indem der Wortlaut der Straftaten von erheblicher Bedeutung in der Regelung eingelegt wurde, wurde der Grundsatz der Verhältnismäßigkeit bereits bei der Gesetzgebung berücksichtigt.

[63] *BVerfGE* 113, 29, 53 [Rn. 108]; 115, 166, 197 [Rn. 117]; 124, 43, 66 [Rn. 79]; M-G/*Schmitt*, StPO, § 94 Rn. 18 und § 102 Rn. 15a.

[64] *BVerfGE* 115, 166, 197 f. [Rn. 117 f.]; 124, 43, 66 [Rn. 79]. Im Einzelfall können daher die Geringfügigkeit der zu ermittelnden Straftat, eine geringe Beweisbedeutung der zu beschlagnahmenden Daten oder die Vagheit eines Auffindeverdachts einer zwanghaften Sicherstellung des Datenbestands entgegenstehen (115, 166, 198 [Rn. 119]; 124, 43, 67 [Rn. 79]).

[65] Vgl. §§ 98a Abs. 1, 100a Abs. 1, 100b Abs. 1, 100c Abs. 1, 100f Abs. 1 – 2, 100g Abs. 1 – 2, 100h Abs. 1 – 2, 110a Abs. 1, 163f Abs. 1 StPO: „wenn (die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Täters/des Beschuldigten) auf andere Weise [erheblich] weniger erfolgversprechend (Erfolg versprechend), aussichtslos oder [wesentlich, unverhältnismäßig] erschwert wäre." Nach der Art und Qualität der Datenerhebung oder der Eingriffsintensität der Maßnahme erhält ein Teil der Ermächtigungsnormen nach §§ 99 ff. StPO diese Klausel nicht: etwa § 100i StPO für technische Ermittlungsmaßnahmen bei Mobilfunkendgeräten und § 100j Abs. 1 S. 1 StPO für die Bestandsdatenauskunft.

StPO) sind i. d. R. strenger als die solchen für einfache Beschlagnahme und Durchsuchung (§§ 94 ff., 102 ff. StPO).[66]

2. Qualifizierte Eingriffsvoraussetzungen

Heimliche Zwangsmaßnahmen sind nur zum Schutz gewichtiger Rechtsgüter zulässig.[67] Die Rechtfertigung jeder Maßnahme ist somit von der Schwere und der Bedeutung der aufzuklärenden Straftat abhängig, die auf die Reichweite jeder Ermächtigungsnorm einwirken.[68] Derzeit schlägt sich das Gewicht der Straftaten – i. R. d. verdeckten Zwangsmaßnahmen – in der StPO mit folgenden drei Bezeichnungen nieder:[69] „besonders schwere Straftaten“,[70] „schwere Straftaten“[71] und „Straftaten von erheblicher Bedeutung“.[72] Die zwei ersteren sind zwar in jeder Vorschrift konkret katalogisiert (Straftatenkatalog; § 100a Abs. 2 sowie § 100b Abs. 2 und § 100g Abs. 2 S. 2 StPO), bei letzteren ist das aber nicht der Fall. Insoweit wird teilweise wegen seiner Unbestimmtheit und Unklarheit die Verfassungsmäßigkeit seiner Verwendung in Zweifel gezogen,[73] jedoch verwendet ihn der Gesetzgeber seit 1992 zur Begrenzung bestimmter Maßnahmen kontinuierlich. Auch das *BVerfG* erkannte den Begriff grundsätzlich als legitime Schwelle solcher Maßnahmen an.[74] Die Entscheidung über die Bestimmung der Rechtsgüter von qualifiziertem Gewicht wird zunächst dem Gesetzgeber nach eigenem Ermessen

[66] Vgl. *Roxin/Schünemann*, § 29 Rn. 5: In der StPO sind die Ermächtigungsgrundlagen zu zwanghaften Ermittlungsmaßnahmen nach dem Verhältnismäßigkeitsgrundsatz schematisch auf einer gleitenden Skala vorgesehen, wobei drei „Kautelen,“ nämlich das „Gewicht des Vorwurfs,“ die „Stärke des Tatverdachts“ und die „Dignität der anordnenden Stelle“ berücksichtigt werden.

[67] *BVerfGE* 141, 220, 270 [Rn. 106 ff.].

[68] Vgl. *BVerfGE* 100, 313, 375 f. [Rn. 219]; 107, 299, 321 [Tz. (2)].

[69] Vgl. *BVerfGE* 109, 279, 344 ff. [Rn. 228 ff.]; 141, 220, 270 [Rn. 107]. Dogmatisch sind die Begriffe dem Verhältnismäßigkeitsgrundsatz und dessen Untermerkmal des Übermaßverbotes zuzuordnen (vgl. *Rieß*, GA 2004, 623, 631 am Anfang: Straftaten von erheblicher Bedeutung).

[70] Der Begriff wurde durch die Änderung des Art. 13 Abs. 3 GG vom 26. März 1998 (BGBl. I S. 610) und den daraus sich ergebenden § 100c Abs. 1 Nr. 3 StPO a. F. (BGBl. I S. 845) in die StPO eingeführt.

[71] Der Begriff wurde zum ersten Mal in der StPO bei der Einführung der §§ 100a und b StPO a. F. vorgesehen, die zur Überwachung des Fernmeldeverkehrs zum Zwecke der Strafverfolgung durch G 10 (Art. 2), das am 1. November 1968 in Kraft trat (BGBl. I S. 949), geschaffen wurden.

[72] Dieser Rechtsbegriff wurde vom OrgKG von 1992 in die StPO eingeführt.

[73] *Rieß*, GA 2004, 623, 624.

[74] Nach überwiegender Auffassung muss eine Straftat von erheblicher Bedeutung mindestens dem Bereich der mittleren Kriminalität zuzurechnen sein, den Rechtsfrieden empfindlich stören und dazu geeignet sein, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen. (*BVerfGE* 103, 21, 34 [Rn. 52]; 107, 299, 322; 109, 279, 344 [Rn. 228]; 112, 304, 305 f. [Rn. 48]; 124, 43, 64 [Rn. 73]; *LG Mannheim* StV 2001, 266; M-G/*Schmitt*, StPO, § 81g Rn. 7a).

überlassen, wobei aber Mindestanforderungen vom *BVerfG* nach Prüfung der Verfassungsmäßigkeit durch die Normenkontrolle gestellt werden können.[75]

Zum anderen ist in der StPO die Stärke des Tatverdachts auch aufgrund des Verhältnismäßigkeitsgrundsatzes nach dem Gewicht der Grundrechtsbeeinträchtigung abgestuft.[76] Sofern „zureichende tatsächliche Anhaltspunkte" in allgemeinen Strafsachen vorliegen, wird zuerst ein sog. „Anfangsverdacht" angenommen (§ 152 Abs. 2 StPO),[77] der für die Einleitung der Strafverfolgung erforderlich und ausreichend ist.[78] Daher wird er nicht nur in den Fällen, in denen er zum Ausdruck kommt (z. B. §§ 98a – c, § 110a Abs. 1 und § 163f Abs. 1 StPO), sondern auch in den Fällen, in denen ein Gesetzwortlaut keine besondere Bedingung über den Verdacht enthält (z. B. §§ 94 f., 102 f., § 99 und § 100h Abs. 1 S. 1 Nr. 1 StPO), verlangt. So ist bei Vorliegen des Anfangsverdachts eine einfache Durchsuchung und Beschlagnahme möglich und zulässig, damit kann die Ermittlung eingeleitet werden.[79] In den Fällen von etwa §§ 100a Abs. 1, 100b Abs. 1, 100c Abs. 1, 100f Abs. 1, 100g Abs. 1 und 2, 100i Abs. 1 und 163d Abs. 1 StPO wird andererseits der durch „bestimmte Tatsachen" begründete Verdacht verlangt (sog. „qualifizierter Tatverdacht").[80] Für ihn muss eine konkretisierte Verdachtslage, d. h. konkrete und in gewissem Umfang verdichtete Umstände, als Tatsachenbasis vorhanden sein.[81] Dieser Verdacht unterliegt höheren Anforderungen als der bloße Anfangsverdacht, jedoch wird nicht verlangt, dass er den Grad eines „hinreichenden" für die Anklageerhebung (§ 170 StPO) und die Eröffnung des Hauptverfahrens (§ 203 StPO) oder gar „dringenden" Tatverdachts für die Untersuchungshaft (§ 112 StPO) und die vorläufige Festnahme (§ 127 StPO) erreicht.[82] Denn obwohl die Maßnahmen der §§ 100a ff. StPO in Grundrechte intensiv eingreifen, zielen sie auf die Erhebung verfahrensrelevanter Daten zur Anklageerhebung ab, und ist auch ihre Intensität geringer als Eingriffe in die persönliche Freiheit.

---

[75] Vgl. *BVerfGE* 125, 260, 328 f. [Rn. 227 – 229].

[76] *Roxin/Schünemann*, § 39 Rn. 16.

[77] Für diesen Verdacht müssen offenkundigen Tatsachen es nach den kriminalistischen Erfahrungen als möglich erscheinen lassen, dass eine verfolgbare Straftat vorliegt (*BGH* NJW 1989, 96, 97; *Diemer*, KK-StPO, § 152 Rn. 7; M-G/*Schmitt*, StPO, § 152 Rn. 4; vgl. *BVerfG* NJW 2015, 851: Berücksichtigung kriminalistischer Erfahrungssätze; *Roxin/Schünemann*, § 35 Rn. 5: Begründung in gesicherter kriminalistischer Erfahrung).

[78] *Diemer*, KK-StPO, § 152 Rn. 7; M-G/*Schmitt*, StPO, § 152 Rn. 4; *Roxin/Schünemann*, § 39 Rn. 15.

[79] M-G/*Schmitt*, StPO, § 94 Rn. 8, auch § 160 Rn. 5.

[80] Vgl. *BVerfGE* 141, 220, 325 [Rn. 280].

[81] *BVerfGE* 100, 313, 395; 109, 279, 350 f. [Rn. 247]; 129, 268 [Rn. 273].

[82] *BVerfGE* 109, 279, 350 [Rn. 247]; 129, 208, 268 [Rn. 273]; *Diemer*, KK-StPO, § 152 Rn. 7; M-G/*Schmitt*, StPO, § 152 Rn. 4; *Wolter*, SK-StPO, § 100c Rn. 41.

3. Strenge verfahrensrechtliche Sicherungen

a) Anforderungen an Transparenz

In den jüngsten Entscheidungen, bei denen es sich um heimliche, tief in die Privatsphäre bzw. den Datenschutz eingreifende Ermittlungsmaßnahmen wie TKÜ, VDS oder Online-Durchsuchung handelt, setzt das *BVerfG* die Gewährleistung von Transparenz der Datenerhebung, -verarbeitung und -verwendung als verfassungsrechtliches Gebot voraus und stellt deshalb zur verfahrensrechtlichen Kontrolle jeder Maßnahme neben den Richtervorbehalt Anforderungen an individuellen Rechtsschutz, aufsichtliche Kontrolle und die Löschungs- und Protokollierungspflicht.[83] Diese Anforderungen ergeben sich aus dem Verhältnismäßigkeitsgrundsatz und dem jeweiligen Grundrecht i. V. m. Art. 19 Abs. 4 GG.[84] Die Transparenz der Datenverarbeitung soll dazu beitragen, dass Vertrauen und Rechtssicherheit entstehen können und der Umgang mit Daten in einen demokratischen Diskurs eingebunden bleibt.[85] So hat der Gesetzgeber wegen der Transparenz zum einen durch die Gewährleistung subjektiven Rechtsschutzes des Betroffenen (die subjektivrechtliche Kontrolle durch die Gerichte), zum anderen durch die Ergänzung eines hinreichend wirksamen aufsichtsrechtlichen Kontrollregimes (die objektivrechtliche Kontrolle in der Verwaltungspraxis) eine diffuse Bedrohlichkeit geheimer staatlicher Beobachtung aufzufangen.[86] Dabei hat die letztere Kontrolle umso größeres Gewicht, je weniger die erstere Kontrolle wegen der Heimlichkeit oder der Art und Weise der Maßnahme sichergestellt werden kann, und sie flankiert den individuellen Rechtsschutz.

b) Richtervorbehalt

Nach der Anforderung an Transparenz unterliegen strafprozessuale Maßnahmen zur Erhebung und Nutzung personenbezogener Daten dem Grundsatz der Offenheit, und so ist der Betroffene vor der Verwendung seiner Daten grundsätzlich zu benachrichtigen (vgl. oben II. 3.).[87] In diesem Fall darf eine heimliche Verwendung der

---

[83] Die erste detaillierte Einführung hierzu *BVerfGE* 125, 260, 334 ff. [Rn. 239 ff.]; und weiter 129, 208, 250 f. [Rn. 226 f.]; 133, 277, 365 ff. [Rn. 204 ff.]; 141, 220, 282 ff. [134 ff.].

[84] *BVerfGE* 125, 260, 335 [Rn. 242]; 133, 277, 366 [Rn. 206]; 141, 220, 282 [Rn. 134].

[85] *BVerfGE* 133, 277, 366 [Rn. 206]; 141, 220, 282 [Rn. 135].

[86] *BVerfGE* 125, 260, 335 [Rn. 242]; 141, 220, 282 [Rn. 135]; auch 133, 277, 366 f. [Rn. 207] und 369 [Rn. 214].

[87] Für die Gefahrenabwehr und die Wahrnehmung der Aufgaben der Nachrichtendienste ist das Absehen von dem Grundsatz der Offenheit grundsätzlich anzunehmen; andernfalls wird hier allgemein der Zweck der Untersuchung vereitelt (*BVerfGE* 125, 260, 336 [Rn. 243]). Daneben gilt dieser Grundsatz für die Informationsanbahnung zur Vorbereitung weiterer Ermittlungen i. R. d. Gefahrenabwehr im Bereich der Staatsschutzdelikte (141, 220, 283 [Rn. 137]; dazu 133, 277, 369 [Rn. 213]: „*Angesichts des Zwecks der Antiterrordatei ist dies (jedoch) verfassungsrechtlich gerechtfertigt. … Dass solche Ermittlungen grundsätzlich nicht dem Grundsatz der Offenheit folgen können, liegt auf der Hand. … ist das Absehen von spezifischen Benachrichtigungspflichten verfassungsrechtlich vertretbar.*“; a. A. *Hofmann*, NStZ

Daten durch das Absehen von vorheriger Benachrichtigung nur vorgesehen werden, wenn sie im Einzelfall erforderlich und richterlich angeordnet ist (Richtervorbehalt)[88] Für heimliche Zwangsmaßnahmen ist aus dem Verhältnismäßigkeitsgrundsatz verfassungsrechtlich eine vorbeugende/vorherige Kontrolle durch eine unabhängige Stelle geboten: etwa in Form einer richterlichen Anordnung.[89] Kann der Betroffene selbst seine Interessen wegen der Heimlichkeit der Maßnahme im Vorweg nicht wahrnehmen, so kann die Kontrolle gewährleisten, dass bei der Entscheidung über eine heimliche Ermittlungsmaßnahme die Interessen des Betroffenen hinreichend in Rechnung gestellt werden: vgl. die „kompensatorische Repräsentation" der Interessen des Betroffenen.[90] Bei Grundrechtseingriffen von besonders hohem Gewicht wie Online-Durchsuchung, VDS, TKÜ etc. reduziert sich u. a. der Spielraum des Gesetzgebers dahingehend, dass solche Maßnahmen grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen sind.[91]

Der Richtervorbehalt beschränkt sich aber auf die gesetzliche Zulässigkeit, nämlich die Rechtmäßigkeit der Maßnahme, daher ist diese Kontrolle nicht dazu geeignet, die Mängel einer zu unbestimmt geregelten oder zu niedrig angesetzten Eingriffsschwelle (z. B. §§ 94 ff., 102 ff. StPO) auszugleichen. Bei heimlichen Ermittlungsmaßnahmen von hoher Eingriffsintensität hat der Gesetzgeber das Gebot vorbeugender richterlicher Kontrolle in spezifischer und normenklarer Form mit „strengen Anforderungen an den Inhalt und die Begründung der gerichtlichen Anordnung" zu verbinden.[92] Dafür bedarf es zunächst einer hinreichend substantiierten Begründung und Begrenzung des Antrags auf Anordnung, insb. der vollständigen Information seitens der antragstellenden Behörde über den zu beurteilenden Sachstand.[93] Nur dadurch kann sich das Gericht als die unabhängige Stelle erst eigenverantwortlich ein Urteil darüber bilden, ob solche Maßnahmen die gesetzlichen Voraussetzungen, also die gesetzlich vorgeschriebenen Eingriffsvoraussetzungen

2005, 121, 123 f.: „*Zumindest im Bereich der organisierten Kriminalität und der Terrorismusdelikte ist das verdeckte Führen der Ermittlungen die Regel und durch die Pflicht zur Erforschung der Wahrheit nach § 160 Abs. 1 StPO sowie durch das im Rechtsstaatsprinzip verankerte Gebot einer effektiven Strafverfolgung.*"). In diesen Fällen ist auch ein Richtervorbehalt kein verfassungsrechtlich gebotenes, geeignetes Mittel (a. a. O. [Rn. 213])**.** Für die Gefahrenabwehr und die Wahrnehmung der Aufgaben der Nachrichtendienste kommt im Ergebnis der Gewährleistung einer effektiven aufsichtlichen Kontrolle umso größere Bedeutung zu (a. a. O. [Rn. 214]; 141, 220, 284 [Rn. 140]).

[88] *BVerfGE* 125, 260, 336 [Rn. 243 a. E.].

[89] *BVerfGE* 141, 220, 275 [Rn. 117]: die eingriffsintensiven Überwachungs- und Ermittlungsmaßnahmen. Für Maßnahmen akustischer Wohnraumüberwachung ist der Richtervorbehalt schon in Art. 13 Abs. 2 bis 4 GG vorgesehen.

[90] *BVerfGE* 120, 274, 331 f. [Rn. 258]; vgl. 100, 313, 361 [Rn. 171].

[91] BVerfGE 120, 274, 332 [Rn. 259]; 125, 260, 337 [Rn. 248]; vgl. 141, 220, 275 f. [Rn. 118]: „Hierfür die notwendigen sachlichen und personellen Voraussetzungen zu schaffen, obliegt der Landesjustizverwaltung und dem Präsidium des zuständigen Gerichts."

[92] *BVerfGE* 125, 260, 338 [Rn. 249]; 141, 220, 275 [Rn. 118]; vgl. 109, 279, 358 f.

[93] *BVerfGE* 141, 220, 275 [Rn. 118]; auch 125, 260, 338 [Rn. 249]; vgl. 103, 142, 152 f. [Rn. 30].

und -schwelle, befolgen.[94] Danach muss der Anordnungsbeschluss des Gerichts gehaltvoll begründet werden. Dabei sind die zu erhebenden oder zu übermittelnden Daten hinreichend selektiv und in klarer Weise zu bezeichnen, sodass die Ermittlungsbehörde und ggf. auch der Dienstanbieter als der Verpflichtete zur Mitwirkung (vgl. § 100a Abs. 4 S. 1, § 101a Abs. 1 i. V. m. § 100a Abs. 4 StPO) eine eigene Sachprüfung nicht vornehmen müssen.[95] Insoweit trifft § 100e Abs. 3 und 4 StPO für die TKÜ, die Online-Durchsuchung und die akustische Wohnraumüberwachung, § 100f Abs. 4 i. V. m. § 100e Abs. 3 StPO für die Überwachungen außerhalb von Wohnungen und § 101a Abs. 1 S. 1, Abs. 2, Abs. 3 S. 1 und 2 i. V. m. § 100e Abs. 3 und 4 StPO für die Erhebung der Verkehrsdaten jeweilige konkrete Regelungen. Zum anderen ist für die TKÜ, Online-Durchsuchung, Wohnraumüberwachung und Verkehrsdatenerhebung, die einen schwerwiegenden Grundrechtseingriff bewirken, vorgesehen, dass das anordnende Gericht nach Beendigung der Maßnahme über deren Ergebnisse, bei Wohnraumüberwachung und Online-Durchsuchung auch über den Verlauf zu unterrichten ist (vgl. §§ 100e Abs. 5, 101a Abs. 1 StPO), um zügig zu überprüfen, ob sie nach der richterlichen Anordnung durchgeführt wurden. Dies garantiert die Wirksamkeit des Richtervorbehalts und trägt dazu bei, übermäßige Persönlichkeitsverletzungen so früh wie möglich zu verhindern.[96]

c) Effektiver Rechtsschutz

Der Transparenz bedarf auch die Bildung der Voraussetzungen für einen wirksamen Rechtsschutz.[97] Nur durch den Anspruch des Betroffenen auf Kenntnis von Maßnahmen kann der Schutz gewährleistet werden („Auskunftsansprüche"). Werden den Betroffenen zumindest nachträgliche Kenntnis hinsichtlich der sie betreffenden Datenverarbeitung nicht verschafft, können sie weder eine Unrechtmäßigkeit der Datenverwendung noch etwaige Rechte auf Löschung, Berichtigung oder Genugtuung geltend machen.[98] Daher gehören Regelungen zur Information der von Datenzugriffen Betroffenen allgemein zu den elementaren Instrumenten des grundrechtlichen Datenschutzes.[99] Außerdem müssen die Betroffenen nach dieser Benachrichtigung in zumutbarer Weise eine gerichtliche Rechtmäßigkeitskontrolle

[94] *BVerfGE* 125, 260, 338 [Rn. 249].

[95] Vgl. *BVerfGE* 125, 260, 338 [Rn. 249].

[96] Die gerichtliche Überprüfung durch diese Unterrichtung wird jedoch auch die Arbeitsbelastung des Richters erhöhen (vgl. Kapitel 4, C. II. 3.).

[97] *BVerfGE* 125, 260, 335 [Rn. 242]; 129, 208, 250 [Rn. 226]; 133, 277, 366 [Rn. 206].

[98] *BVerfGE* 125, 260, 335 [Rn. 242]; 129, 208, 250 [Rn. 226]; 133, 277, 366 [Rn. 206].

[99] *BVerfGE* 129, 208, 250 [Rn. 226]; dazu 125, 260, 335 [Rn. 242]: Diese Auskunft gegenüber den Betroffenen „*mindert eine sich aus dem Nichtwissen um die tatsächliche Relevanz der Daten ergebende Bedrohlichkeit, wirkt verunsichernden Spekulationen entgegen und schafft den Betroffenen die Möglichkeit, solche Maßnahmen in die öffentliche Diskussion zu stellen*".

erwirken können (Art. 19 Abs. 4 GG).[100] Insofern sieht das GG nichts für ihre verfahrensrechtliche Ausgestaltung vor,[101] der Gesetzgeber hat aber Regelungen zur nachträglichen Benachrichtigung und zur gerichtlichen Rechtmäßigkeitskontrolle zu schaffen.[102] Dabei müssen die Zurückstellung und Ausschließung der Benachrichtigung mit Blick auf die Rechtsschutzlücken, die durch ihre Beschränkung entstehen, der Kontrolle des Gerichts als unabhängiger Stelle unterstehen.[103] Das *BVerfG* hat Anforderungen an die gesetzliche Ausgestaltung dieser Benachrichtigungspflicht in einer Kette von Entscheidungen über den Großen Lauschangriff, VDS und TKÜ im Einzelnen ausgeführt[104] und insb. in der Entscheidung von 2010 übersichtlich umrissen.[105] Nach der Meinung des *BVerfG* sind die Regelungen des § 101 Abs. 4–6 StPO i. d. R. mit diesen Vorgaben vereinbar.[106]

---

[100] *BVerfGE* 141, 220, 283 f. [Rn. 138]; vgl. 125, 260, 335 [Rn. 242]. Allerdings ergibt sich aus diesem Anspruch neben dem gerichtlichen Rechtsschutz ein spezifisches Datenschutzrecht, das gegenüber der informations- und datenverarbeitenden staatlichen Stelle geltend gemacht werden kann (100, 313, 361 [Rn. 169]; vgl. unten d) und f)).

[101] Vgl. *BVerfGE* 100, 313, 361 [Rn. 170 f.]: etwa Art. 10 Abs. 2 GG.

[102] Vgl. *BVerfGE* 125, 260, 335 [Rn. 244] und 339 [Rn. 251]. Insoweit hat sich das *BVerfG* schon vor langer Zeit in seiner Entscheidung zur Gewährleistung und Einschränkungen einer vorherigen Anhörung bei der Untersuchungshaft ausdrücklich erklärt (9, 89, 98 [Rn. 29]): „*… kann eine Ausnahme von dem Grundsatz vorheriger Anhörung nur zulässig sein, wenn dies unabweisbar ist, um nicht den Zweck der Maßnahme zu gefährden. … Außerdem verlangt der Rechtsstaatsgedanke, daß der Betroffene in solchem Fall Gelegenheit erhält, wenigstens nachträglich sich gegen die angeordneten Maßnahmen zu wehren. Es muß also auf Verlangen des Betroffenen zu einem Nachverfahren kommen, in dem ihm rechtliches Gehör gewährt und über die Berechtigung der getroffenen Maßnahmen entschieden wird.*“

[103] Vgl. *BVerfGE* 100, 313, 361 [Rn. 171].

[104] *BVerfGE* 109, 279, 363 ff.; 125, 260, 336 f.; 129, 208, 251; 141, 220, 282 f.

[105] *BVerfGE* 125, 260, 336 f. [Rn. 244 f.]: „*Ausnahmen von der Benachrichtigungspflicht kann der Gesetzgeber in Abwägung mit verfassungsrechtlich geschützten Rechtsgütern Dritter vorsehen. Sie sind jedoch auf das unbedingt Erforderliche zu beschränken. Bei der Strafverfolgung sind Ausnahmen von den Benachrichtigungspflichten denkbar, wenn beispielsweise die Kenntnis des Eingriffs in das Telekommunikationsgeheimnis dazu führen würde, dass dieser seinen Zweck verfehlt, wenn die Benachrichtigung nicht ohne Gefährdung von Leib und Leben einer Person geschehen kann oder wenn ihr überwiegende Belange einer betroffenen Person entgegenstehen, etwa weil durch die Benachrichtigung von einer Maßnahme, die keine weiteren Folgen gehabt hat, der Grundrechtseingriff noch vertieft würde (Zurückstellung der Benachrichtigung). Liegen zwingende Gründe vor, die auch eine nachträgliche Benachrichtigung ausschließen, ist dieses richterlich zu bestätigen und in regelmäßigen Abständen zu prüfen (Absehen von der Benachrichtigung). Darüber hinaus ist es verfassungsrechtlich nicht geboten, vergleichbar strenge Benachrichtigungspflichten gegenüber Personen zu begründen, die nur zufällig von einer Ermittlungsmaßnahme gegen einen Beschuldigten betroffen sind und somit nicht Ziel des behördlichen Handelns sind. Eine Benachrichtigung kann ihnen gegenüber im Einzelfall den Eingriff vielfach sogar vertiefen. In diesen Fällen kann eine Benachrichtigung grundsätzlich schon dann unterbleiben, wenn die Betroffenen von der Maßnahme nur unerheblich betroffen wurden und anzunehmen ist, dass sie kein Interesse an der Benachrichtigung haben. Einer richterlichen Bestätigung dieser Abwägungsentscheidung bedarf es nicht*“; dazu 129, 208, 251 [Rn. 227].

Die Eröffnung eines nachträglichen Rechtsschutzverfahrens gegen die in § 101 Abs. 1 StPO aufgezählten heimlichen Ermittlungsmaßnahmen ist andererseits in Abs. 7 S. 2–4 vorgesehen und diese Vorschrift ist eine Sonderregelung des § 98 Abs. 2 S. 2 (vgl. Kapitel 4, C. II. 2. e)).[107] Daher kann der von einer Maßnahme Betroffene (§ 101 Abs. 4 S. 1 StPO) – anders als im Fall des § 98 Abs. 2 S. 2 StPO – bei dem für die Anordnung zuständigen Gericht „auch nach Beendigung der Maßnahme" „bis zu zwei Wochen" nach der Benachrichtigung die Überprüfung der Rechtmäßigkeit der Maßnahme – „richterlich oder nichtrichterlich" – sowie der Art und Weise ihres Vollzugs beantragen.[108] Dabei beginnt die zweiwöchige Ausschlussfrist[109] mit der Benachrichtigung, auch wenn der Betroffene schon anderweitig Kenntnis von der Maßnahme erlangt hat.[110] Nach dem Wort „auch" kann der Antrag jedoch schon vor Beendigung der Maßnahme[111] und auch nach ihrer Erledigung[112] gestellt werden. Insbesondere im letzten Fall kann eine nachträgliche richterliche Überprüfung erfolgen, ohne dass ein konkretes Rechtsschutzbedürfnis nachgewiesen werden müsste.[113] Somit soll diese Vorschrift zum effektiven Grundrechtsschutz gegen heimliche Maßnahmen analog anwendbar sein.[114]

[106] *BVerfGE* 129, 208, 251 ff. [Rn. 228 ff.]; vgl. für die Verkehrsdatenerhebung gemäß § 100g StPO, § 101a Abs. 6 S. 2 StPO: Es bedarf für das Unterbleiben und die Zurückstellung der Benachrichtigung nach § 101 Abs. 4 S. 3 und Abs. 5 S. 1 StPO der Anordnung des zuständigen Gerichts (125, 260, 354 [Rn. 282]).

[107] M-G/*Schmitt*, StPO, § 98 Rn. 23 a. E. und § 101 Rn. 26a; *Roxin/Schünemann*, § 29 Rn. 24; vgl. *Wolter/Jäger*, SK-StPO, § 101 Rn. 39: ergänzender Charakter.

[108] M-G/*Schmitt*, StPO, § 101 Rn. 25; vgl. *Roxin/Schünemann*, § 29 Rn. 24; *Wolter/Jäger*, SK-StPO, § 101 Rn. 38a. Die Feststellung über die Rechtmäßigkeit oder Rechtswidrigkeit durch das Gericht hat keine Bindungswirkung für die im Hauptverfahren vom erkennenden Gericht zu beurteilende Entscheidung über die Verwertbarkeit der aus der Maßnahme gewonnenen Erkenntnisse (BT-Drs. 16/5846, S. 62; *Bruns*, KK-StPO, § 101 Rn. 30: ausgenommen die Entscheidung nach § 100d Abs. 4 S. 5, 6 StPO; M-G/*Schmitt*, a. a. O. Rn. 26). Freilich kann dies umgekehrt den Angeklagten nicht an der Geltendmachung ihres Verwertungsverbots im Hauptverfahren hindern (*Bruns*, a. a. O. Rn. 35a; M-G/*Schmitt*, a. a. O.). Zur Art und Weise des Maßnahmenvollzugs gehört anderseits auch die Rechtmäßigkeit der Benachrichtigung inklusive ihrer Rechtzeitigkeit (*OLG Celle* StraFo 2012, 183 = NStZ 2013, 60; *OLG Stuttgart* StraFo 2016, 413), die freilich regelmäßig nicht zu einem Verwertungsverbot führt (vgl. *Bruns*, a. a. O. Rn. 30).

[109] BT-Drs. 16/5846, S. 62: „bis zu"; *Bruns*, KK-StPO, § 101 Rn. 30; M-G/*Schmitt*, StPO, § 101 Rn. 25; *Wolter/Jäger*, SK-StPO, § 101 Rn. 40.

[110] *Bruns*, KK-StPO, § 101 Rn. 30; M-G/*Schmitt*, StPO, § 101 Rn. 25. Die Benachrichtigung ist aber keine Rechtsschutzvoraussetzung und hat allein fristauslösende Wirkung, daher setzt der Antrag sie nicht notwendig voraus (M-G/*Schmitt*, a. a. O.; *Wolter/Jäger*, SK-StPO, § 101 Rn. 39 a. E.). Jedoch ist ein verfristeter Antrag unzulässig (M-G/*Schmitt*, a. a. O.).

[111] M-G/*Schmitt*, StPO, § 101 Rn. 25; a. A. *Singelnstein*, NStZ 2009, 481, 482 und *Wolter/Jäger*, SK-StPO, § 101 Rn. 39: § 98 Abs. 2 S. 2 StPO entsprechend bzw. § 304 StPO.

[112] *BGHSt* 53, 1; M-G/*Schmitt*, StPO, § 101 Rn. 26a; *Singelnstein*, NStZ 2009, 481, 482.

[113] *Roxin/Schünemann*, § 29 Rn. 24; *Wolter/Jäger*, SK-StPO, § 101 Rn. 39.

[114] *Singelnstein*, NStZ 2009, 481, 483; *Roxin/Schünemann*, § 29 Rn. 24; *Wolter/Jäger*, SK-StPO, § 101 Rn. 39; a. A. M-G/*Schmitt*, StPO, § 101 Rn. 26a a. E.: Der Rechtsschutz der nicht in § 101 Abs. 4 S. 1 StPO genannten Personen richtet sich nach den allgemeinen Vorschriften.

d) Administrative aufsichtliche Kontrolle

Die aufsichtliche Kontrolle dient der Gewährleistung der Gesetzmäßigkeit der Verwaltung insgesamt und flankiert damit die subjektivrechtliche Kontrolle durch die Gerichte objektivrechtlich.[115] Sie betrifft i. d. R. heimliche Überwachungs- und Ermittlungsmaßnahmen und hat umso größeres Gewicht, je weniger eine subjektivrechtliche Kontrolle sichergestellt werden kann.[116] Die Gewährleistung einer wirksamen aufsichtlichen Kontrolle bedarf der Einrichtung einer mit wirksamen Befugnissen und technischen und organisatorischen Mitteln ausgestatteten Aufsichtsinstanz und der angemessenen Durchführung der Kontrollbefugnis. Insoweit hat das *BVerfG* in seinen Entscheidungen wie folgt angegeben:

> „Die Gewährleistung einer wirksamen aufsichtlichen Kontrolle setzt zunächst eine mit wirksamen Befugnissen ausgestattete Stelle – wie nach geltendem Recht die Bundesdatenschutzbeauftragte – voraus. Dazu ist erforderlich, dass die Datenerhebungen vollständig protokolliert werden. … Angesichts der Kompensationsfunktion der aufsichtlichen Kontrolle für den schwach ausgestalteten Individualrechtsschutz kommt deren regelmäßiger Durchführung besondere Bedeutung zu und sind solche Kontrollen in angemessenen Abständen – deren Dauer ein gewisses Höchstmaß, etwa zwei Jahre, nicht überschreiten darf – durchzuführen. Dies ist bei der Ausstattung der Aufsichtsinstanz zu berücksichtigen. Die Gewährleistung der verfassungsrechtlichen Anforderungen einer wirksamen aufsichtlichen Kontrolle obliegt dem Gesetzgeber und den Behörden gemeinsam.“[117]

e) Berichtspflichten gegenüber Parlament

Daneben verlangt das *BVerfG* für eingriffsintensive heimliche Überwachungs- und Ermittlungsmaßnahmen zur Gewährleistung von Transparenz eine gesetzliche Regelung von Berichtspflichten gegenüber dem Parlament.[118] Diese Berichte müssen hinreichend so gehaltvoll sein, dass eine öffentliche Diskussion über Art und Ausmaß der auf die Befugnisse zu den Maßnahmen gestützten Datenerhebung und auch eine demokratische Kontrolle und Überprüfung darüber ermöglicht wird.[119] Diesbezüglich gibt es § 101b StPO, der für die TKÜ (Abs. 2), die Online-Durchsuchung (Abs. 3), die akustische Wohnraumüberwachung (Abs. 4) und die Erhebung von TK-Verkehrsdaten (Abs. 5) gilt.

f) Löschungs- und Protokollierungspflicht

Eine Verwendung personenbezogener Daten, die durch heimliche Überwachungs- und Ermittlungsmaßnahmen erhoben werden, beschränkt sich auf die

[115] *BVerfGE* 133, 277, 366 [Rn. 207].
[116] *BVerfGE* 133, 277, 366 f. [Rn. 207].
[117] *BVerfGE* 133, 277, 370 f. [Rn. 215, 217]; 141, 220, 284 [Rn. 141].
[118] *BVerfGE* 133, 277, 372 [Rn. 221 f.]; 141, 220, 285 [Rn. 142 f.].
[119] *BVerfGE* 133, 277, 372 [Rn. 222]; 141, 220, 285 [Rn. 143].

festgelegten Zwecke und ist nach deren Erledigung nicht mehr möglich (Gebot der Zweckbindung; vgl. Kapitel 2, A. III. 1. b)). Daher ist eine Vernichtungs- und Löschungspflicht einschließlich einer diesbezüglichen Protokollierungspflicht gesetzlich vorzusehen: § 101 Abs. 8 StPO.[120]

IV. Zwischenfazit – Bedarf an qualifizierter Kontrolle gegen heimliche Zwangsmaßnahmen

Da Ermittlungshandlungen i. d. R. mit einer Grundrechtsbeeinträchtigung verbunden sind, müssen sie nach dem Rechtsstaatsprinzip, insb. dem Grundsatz der Verhältnismäßigkeit, angemessen beschränkt werden. Insofern muss u. a. bei kriminalistischen Zwangsmaßnahmen, die einen nicht geringfügigen Eingriff in Grundrechte bewirken, ihre Rechtmäßigkeit zum Schutz der Grundrechte sowohl vorbeugend als auch nachträglich geprüft werden können. Zum anderen sind heimliche Ermittlungen mit Blick auf die Effektivität der Strafrechtspflege notwendig und gestattet, jedoch haben sie im Allgemeinen wegen ihrer Heimlichkeit im Vergleich zu offenen Ermittlungen ein erhöhtes Eingriffsgewicht. Daher sollen unter dem Rechtsstaatsprinzip zum effektiven Grundrechtsschutz die „heimlichen Zwangsmaßnahmen" speziell bearbeitet werden. Hierbei hängt die „Heimlichkeit" entscheidend davon ab, dass die Maßnahmen zur Zeit ihrer Durchführung „ohne Wissen des von erhobenen Daten Betroffenen" erfolgen. Da derartige Maßnahmen i. d. R. intensiver sind als die offenen, werden zudem dafür nach dem Verhältnismäßigkeitsgrundsatz engere Eingriffsvoraussetzungen und verfahrensrechtliche Sicherungen verlangt als diejenigen nach §§ 94 ff., 102 ff. StPO. Insb. eine Rechtfertigung von tief in die Privatsphäre eingreifenden Maßnahmen ist von einer konkreten Ausgestaltung der verfahrensrechtlichen Schutzvorkehrungen abhängig.

B. Ermächtigungsgrundlagen für „zwangsmäßige bzw. heimliche Ermittlungsmaßnahmen" im 8. Abschnitt des Ersten Buches der StPO

I. Allgemeines

1. Konstruktion der Ermächtigungsgrundlagen zur Beweissicherung in der StPO

Im Bereich der Suche und der Sicherstellung der Beweismittel im Strafverfolgungsverfahren bildet die StPO ein abgestuftes Normensystem nach der Art und

[120] *BVerfGE* 100, 313, 362 [Rn. 172]; 133, 277, 372 [Rn. 223]; 141, 220, 285 f. [Rn. 144] und 322 f. [Rn. 269 ff.]; vgl. 65, 1, 46 [Rn. 162].

Weise und der Eingriffsintensität der Maßnahmen. Zuerst gibt es Generalklauseln der „Ermittlung" (§§ 161 Abs. 1, 163 Abs. 1 StPO) und allgemeine Vorschriften der „Beschlagnahme und Durchsuchung" (§§ 94 ff., 102 ff. StPO). Daneben liegen selbstständige Ermächtigungsnormen, um neuartige Maßnahmen zu regeln, die durch den Fortschritt der Technologie ermöglicht werden (§§ 99 ff. StPO).[121] Den Generalklauseln und den allgemeinen Vorschriften fehlt es an Beschränkung bezüglich der Art und Weise der Durchführung der Maßnahmen – wie die Bezeichnung „General-" bzw. „allgemein" schon zeigt. Hingegen setzen die Maßnahmen nach §§ 99 ff. StPO nicht nur qualifizierte Eingriffsvoraussetzungen voraus, sondern das Verfahren ihrer Anordnung und Durchführung ist auch mit strengen verfahrensrechtlichen Sicherungen verbunden. Sie haben wegen erhöhter Eingriffsintensität aufgrund der Art und Weise ihrer Durchführung einen neuen eigenständigen Charakter, so wird eine individuelle Rechtfertigung dafür verlangt (vgl. oben A. I. 3.). Aus dem abgestuften Normensystem ergibt sich, dass die Ermittlungsgeneralklauseln, die allgemeinen Vorschriften der Durchsuchung und Beschlagnahme sowie jede gesonderte Ermächtigungsnorm zueinander im Sonder- bzw. Subsidiaritätsverhältnis stehen.[122]

Zunächst sehen §§ 161 Abs. 1, 163 Abs. 1 StPO nur eine Aufgabe bzw. Pflicht und eine Befugnis der Ermittlungsbehörden vor.[123] Nach Rspr. und h. M. folgt aus solchen Klauseln der „Grundsatz der freien Gestaltung des Ermittlungsverfahrens".[124] und gestützt darauf können die Behörden Ermittlungen jeder Art – ungeachtet ihrer Offenheit oder Heimlichkeit – vornehmen. Jedoch erlauben sie nur Ermittlungshandlungen, die von einer speziellen Eingriffsermächtigung der StPO nicht erfasst werden und keinen Eingriffscharakter haben oder lediglich geringfügig in die Grundrechte eingreifen (sog. „Auffang-Rechtsgrundlage").[125] Da nach dem Grundsatz des Gesetzesvorbehalts der Zwang im Strafverfahren nur dann möglich ist, wenn das Strafverfahrensrecht ihn zulässt,[126] dürfen sie nicht zur Rechtsgrund-

[121] In vorliegender Arbeit werden lediglich Vorschriften zur Sicherstellung von Beweismitteln im 8. Abschnitt des Ersten Buches der StPO (§§ 94 – 110a StPO), abgesehen von maschinellem Abgleich und der Übermittlung personenbezogener Daten (§§ 98a – c StPO), und zur längerfristigen Observation (§ 163f StPO) berücksichtigt.

[122] Vgl. *BVerfGE* 124, 43, 58 f. [Rn. 58]; abw. *Singelnstein*, NStZ 2012, 593, 603: Ein solches systematisches Verständnis hat sich indes noch nicht vollständig durchgesetzt.

[123] *Volk*/*Engländer*, § 10 Rn. 1.

[124] M-G/*Schmitt*, StPO, § 161 Rn. 7 und § 163 Rn. 64; *Roxin*/*Schünemann*, § 39 Rn. 23; *Volk*/*Engländer*, § 10 Rn. 1.

[125] *BGHSt* 51, 211, 218 [Rn. 21]; 55, 138, 143 [Rn. 18]: auch mit „weniger intensiven" Grundrechtseingriffen; M-G/*Schmitt*, StPO, § 161 Rn. 1; *Kudlich*, GA 2011, 193, 198; *Soiné*, NStZ 2014, 248, 251 [Tz. IV.]; *Wohlers*, SK-StPO, § 161 Rn. 4; vgl. *BVerfG* NJW 2009, 1405, 1407 [Rn. 26]: Diese Klauseln bilden die Rechtsgrundlage für die allgemeine Erhebung personenbezogener Daten und damit für eine Ermittlungsanfrage gegenüber privaten Stellen, also Datenabfrage bei Kreditkartenunternehmen (*Singelnstein*, NStZ 2012, 593, 603; vgl. *LG Koblenz* wistra 9/2002, 359: Zu den Ermittlungen zählt auch ein auf § 95 Abs. 1 StPO gestütztes Herausgabeverlangen).

[126] M-G/*Schmitt*, StPO, Einl. Rn. 45 und § 163 Rn. 32.

lage für Zwangsmaßnahmen dienen. Zum anderen sind für die heimlichen Ermittlungsmaßnahmen, die aufgrund eigener individueller Ermächtigungsnormen (z. B. §§ 99 ff. StPO) anzuordnen sind, sowohl die Art und Weise ihrer Durchführung als auch die Eingriffsvoraussetzungen und das Anordnungsverfahren gesetzlich konkret beschrieben. Schließlich gehen die §§ 94 ff., 102 ff. StPO, die mit bestimmten Verfahrensregelungen verbunden sind, den Ermittlungsgeneralklauseln vor,[127] jedoch werden sie von den speziellen Ermächtigungsnormen verdrängt. In dieser Hinsicht kann ihr Anwendungsbereich zwischen §§ 161 Abs. 1, 163 Abs. 1 StPO und §§ 99 ff. StPO abstrakt und begrifflich festgelegt werden. So werden durch die Vorschriften die Maßnahmen gedeckt, die mit einer solchen Gewalt, die sich aufgrund der Generalklauseln nicht rechtfertigen lässt, in Grundrechte eingreifen, die aber milder sind als Eingriffe gemäß §§ 99 ff. StPO oder deren Art und Weise darunter nicht subsumiert werden kann. Im Einzelfall ist diese Abgrenzung jedoch nicht immer klar und sie wird zum Grundrechtsschutz nach dem Grundsatz der Verhältnismäßigkeit relativ getroffen. Hierbei ist u. a. eine Differenzierung zwischen der Anwendung der allgemeinen Vorschriften der Beschlagnahme und Durchsuchung und derjenigen individueller Ermächtigungsnormen der §§ 99 ff. StPO problematisch. Dabei handelt es sich um eine Umgehung der strengeren Verfahrensvorschriften durch die Ermittlungsbehörden. Eine Ermächtigung einzelner Maßnahmen muss auf Grundlage der Art und Weise ihres Vollzugs – einschließlich der Heimlichkeit oder Offenheit – und der daraus sich ergebenden Eingriffsintensität sowie der dementsprechenden Eingriffsschwellen bestimmt werden.[128]

2. Die allgemeinen Vorschriften der Beschlagnahme und Durchsuchung: §§ 94 ff., 102 ff. StPO

Diese Vorschriften enthalten die materiellen Voraussetzungen der Beschlagnahme und Durchsuchung (§§ 94, 102, 103 StPO). Hierin wird aber ihr Gegenstand nur abstrakt erwähnt und es bestehen keine Beschränkungen nach der Schwere der Straftaten und dem Gewicht des Tatverdachts, auch die Art und Weise der Durchführung ist nicht bestimmt. Die Vorschriften gelten daher für die Verfolgung aller Straftaten und verlangen nur den Anfangsverdacht.[129] Sie regeln daneben den Richtervorbehalt (§§ 98, 105 Abs. 1 StPO), das Durchführungsverfahren der Durchsuchung (§§ 105 Abs. 2, 106 bis 100 StPO), Herausgabepflicht (§ 95 StPO) und Beschlagnahmeverbote (§ 97 StPO). In diesen allgemeinen Vorschriften werden u. a. bezüglich des Richtervorbehalts etwa die Form und der Inhalt richterlicher Anordnung und die Grenze nichtrichterlicher Anordnung – anders als in §§ 99 ff. StPO – gesetzlich nicht geregelt; dies wird vielmehr durch die Auslegung der

[127] *Singelnstein*, NStZ 2012, 593, 603.

[128] Siehe Kapitel 4, B. III. 2.

[129] *BVerfGE* 124, 43, 65 [Rn. 74]; M-G/*Schmitt*, StPO, § 94 Rn. 8, § 102 Rn. 2 und § 152, Rn. 4; *Roxin*/*Schünemann*, § 39 Rn. 15 und § 34 Rn. 5.

Rechtsprechung und Literatur reguliert.[130] Für die Strafverfolgungsbehörden, die in der Praxis sich auf unterschiedliche Sachverhalte einstellen und gleichzeitig die Beweismittel sicherstellen müssen, ist die Beschlagnahme und Durchsuchung nach diesen Vorschriften das grundlegendste, aber wichtigste Mittel.[131] Dies gilt auch heute noch, wo personenbezogene Daten häufig umfassend eingesehen und gesichert werden. Sie müssen angepasst an veränderte Bedingungen manchmal flexibel oder manchmal streng angewandt werden, darüber hinaus können bestehende Ansätze durch neue ersetzt oder ergänzt werden.[132] Vgl. Kapitel 4 bezüglich ihrer Reichweite und Grenze.

Die Eingriffsvoraussetzungen und verfahrensrechtlichen Vorkehrungen zu technischen Ausspähungsmethoden im 8. Abschnitt des Ersten Buches der StPO sind im Vergleich zu denselben der allgemeinen Vorschriften zur Beschlagnahme und Durchsuchung höher. In dieser Hinsicht fungieren diese als standardmäßige Vorschrift der Ermächtigungsgrundlagen für Zwangsmaßnahmen zur Sicherstellung der Beweismittel.

II. Eigene Ermächtigungen: §§ 99 bis 101b, 110a und 163f StPO

1. Überblick

Unter dem 8. Abschnitt des Ersten Buches der StPO liegen selbstständige Ermächtigungen als Rechtsgrundlage der Zwangsmaßnahmen zur Beweissicherung vor: § 99 StPO für die Beschlagnahme von Postsendungen und Telegrammen, § 100a StPO für TKÜ, § 100b StPO für die Online-Durchsuchung, § 100c StPO für die akustische Wohnraumüberwachung, § 100f StPO für die akustische Überwachung außerhalb von Wohnungen, § 100g StPO für die Erhebung der Verkehrs- und Standortdaten, § 100h StPO für die Herstellung von Bildaufnahmen und die Verwendung technischer Mittel für Observationszwecke, § 100i StPO für technische Ermittlungsmaßnahmen bei Mobilfunkendgeräten, § 100j StPO für die Auskunft der Bestandsdaten und Zugangscodes, § 110a StPO für den Einsatz verdeckter Ermittler, § 163d StPO für die Speicherung und Abgleich von Daten aus Kontrollen, § 163e StPO für die Ausschreibung zur Beobachtung bei polizeilichen Kontrollen und § 163f StPO für die längerfristige Observation. Jede Vorschrift regelt die von ihr zugelassenen Maßnahmen nach deren Eingriffsintensität unter dem Grundsatz der Verhältnismäßigkeit durch eine recht genaue und rechtliche Ausgestaltung.[133] Die o. g. Maßnahmen können nach ihrer Eingriffsintensität und der dementsprechenden

[130] Vgl. *Kemper*, wistra 5/2006, 171, 175: derzeit beruht die Beschlagnahme und Durchsuchung einer Menge an Papieren zum weitaus größten Teil auf der Auslegung durch die Rspr.

[131] *Park*, § 1 Rn. 1.

[132] Vgl. M-G/*Schmitt*, StPO, Einl. Rn. 190 ff.: Die Strenge der Auslegung im Verfahrensrecht ist etwas lockerer als im materiellen Recht.

[133] Vgl. *Roxin*/*Schünemann*, § 36 Rn. 1.

Strenge der Kontrolle schätzungsweise in der Reihenfolge der Online-Durchsuchung, der Wohnraumüberwachung, der VDS, der TKÜ und der akustischen Überwachung außerhalb von Wohnraum, der Erhebung von Verkehrsdaten in Echtzeit, der technischen Ermittlungsmaßnahmen bei Mobilfunkendgeräten, Postbeschlagnahme, einfacher Beschlagnahme und Durchsuchung, des Einsatzes sonstiger technischer Mittel und der Herstellung von Bildaufnahmen für Observationszwecke und schließlich der Erhebung von Bestandsdaten (abgesehen von Zugangssicherungscodes) angeordnet werden.

In jeder Ermächtigung spiegelt sich die Schwere der aufzuklärenden Straftat nach dem Gewicht der Grundrechtsbeeinträchtigung abgestuft:[134] „besonders schwere Straftaten" für die Online-Durchsuchung (§ 100b Abs. 2 StPO), den Großen Lauschangriff (§ 100c Abs. 1 i. V. m. § 100b Abs. 2 StPO) und die Nutzung von anlasslos vorsorglich gespeicherten Verkehrsdaten (§ 100g Abs. 2 S. 2 StPO); „schwere Straftaten"[135] für die TKÜ (§ 100a Abs. 2 StPO), den Kleinen Lauschangriff (§ 100f Abs. 1 StPO i. V. m. § 100a Abs. 2 StPO), die Erhebung von Verkehrsdaten in Echtzeit (§ 100g Abs. 1 i. V. m. § 100a Abs. 2 StPO) und den Einsatz technischer Ermittlungsmaßnahmen bei Mobilfunkendgeräten (§ 100i Abs. 1 i. V. m. § 100a Abs. 2 StPO); schließlich „Straftaten von erheblicher Bedeutung" für die Verwendung technischer Mittel für Observationszwecke (§ 100h Abs. 1 S. 1 Nr. 2 StPO; abgesehen von der Herstellung von Bildaufnahmen gemäß Nr. 1), den Einsatz verdeckter Ermittler (§ 110a Abs. 1 StPO), die längerfristige Observation (§ 163f Abs. 1 StPO). Außerdem ist der Grad des Tatverdachts abgestuft: „Anfangsverdacht" und „qualifizierter Verdacht". Des letzteren Verdachts bedarf es für die restlichen Maßnahmen abgesehen von §§ 110a Abs. 1, 163f Abs. 1 StPO.

Die verfahrensrechtlichen Vorkehrungen für heimliche Zwangsmaßnahmen können sich in vorherige bzw. nachträgliche Kontrolle gliedern. Die vorbeugende Kontrolle wird wie bei einfacher Beschlagnahme und Durchsuchung allein durch Richter als unabhängige Stelle durchgeführt (Richtervorbehalt; vgl. oben A. III. 2. b)). Doch ist der konkrete Inhalt der Kontrolle restriktiver.[136] Dazu gehört etwa die Beschränkung der Eilzuständigkeit (z. B. §§ 100 Abs. 1, 100e Abs. 1 S. 2 und Abs. 2 S. 2, 100f Abs. 4, 100i Abs. 3 S. 1, 101a Abs. 1 S. 1 StPO) und deren Wirksamkeit (z. B. §§ 100 Abs. 2, 100e Abs. 1 S. 3 und Abs. 2 S. 3, 100f Abs. 4, 100i Abs. 3 S. 1 StPO) sowie strenge Anforderungen an Form und Inhalt bzw. Begründung der gerichtlichen Anordnung(z. B. §§ 100e Abs. 3 und 4, 100f Abs. 4, 100i Abs. 3 S. 1,

[134] Vgl. *BVerfGE* 141, 220, 270 [Rn. 107].

[135] Obwohl in dem § 100b Abs. 2 und dem § 100g Abs. 2 der Wortlaut gleich ist, nämlich „besonders schwere Straftaten", decken sich die in jeder Bestimmung aufgeführten Straftaten teilweise nicht.

[136] Für die Maßnahmen wie die Herstellung von Bildaufnahmen und den Einsatz technischer Mittel für Observationszwecke, deren Eingriffsintensität geringer eingeschätzt wird als die allgemeine Durchsuchung und Beschlagnahme, ist aber keine vorherige Kontrolle durch die Gerichte vorbehalten, sondern nur eine nachträgliche Überprüfung der Rechtmäßigkeit möglich.

101a Abs. 1 und 2 StPO). Zum anderen erfolgt die nachträgliche Kontrolle nicht nur vom Gericht, sondern von den Strafverfolgungsbehörden selbst und einer nichtgerichtlichen Einrichtung, insb. einem Parlament (vgl. oben A. III. 3. c)–f)). Die Wichtigste davon ist die gerichtliche Überprüfung zum effektiven Rechtsschutz und dafür die Benachrichtigung des Betroffenen. Diesbezüglich wurden durch das TKÜG von 2008 die Regelungen, die die Vernichtungs- und Kennzeichnungspflicht, die Benachrichtigung und ihre weitere Zurückstellung sowie die Überprüfung der Rechtmäßigkeit betreffen, was bis dahin nur für die akustische Wohnraumüberwachung galt (vgl. § 100d Abs. 5 und 7 bis 10 StPO a. F.), auf § 101 StPO, der eine allgemeine Vorschrift zum Rechtsschutzverfahren bei verdeckten Ermittlungsmaßnahmen darstellt, umgestellt (vgl. § 101 Abs. 2 bis 8 StPO n. F.).[137] Damit wurde das System des nachträglichen Rechtsschutzes für heimliche Maßnahmen in dieser Vorschrift vereinheitlicht. Daneben verlangt der Gesetzgeber, auch das *BVerfG*, für tief in die Privatsphäre eingreifende Maßnahmen eine unübliche, gerichtliche und administrative aufsichtliche Kontrolle. In den Ermächtigungen für diese Maßnahmen ist nach deren Beendigung die Unterrichtung des Gerichts über deren „Ergebnisse" vorgesehen (§§ 100e Abs. 5 S. 1–2 und 101a S. 1 StPO), zudem insb. in der Online-Durchsuchung und der Wohnraumüberwachung auch die Unterrichtung über deren „Verlauf" (§ 100e Abs. 5 S. 3 StPO). Derartige Kontrollen können zwar einerseits die freie Gestaltung des Ermittlungsverfahrens, nämlich eine Ermessensentscheidung der StA oder konkrete Handlungen ihrer Ermittlungspersonen, unmittelbar beschränken, andererseits dienen sie der Aufsicht und Überwachung der staatsanwaltlichen oder polizeilichen Durchführung durch die Gerichte oder StA. Für die Maßnahmen, die sich an „inhaltliche Informationen" wie kommunizierende Nachrichten oder gesprochene Worte richten, etwa die TKÜ, die Online-Durchsuchung, die akustische Wohnraumüberwachung, akustische Überwachung außerhalb von Wohnraum, die Herstellung von Bildaufnahmen und die Verwendung sonstiger technischer Mittel für Observationszwecke, den Einsatz eines Verdeckten Ermittlers und längerfristige Observation, sind darüber hinaus verfahrensrechtliche Vorkehrungen zum effektiven Schutz des Kernbereichs privater Lebensgestaltung vorgesehen (§ 100d und §§ 100f Abs. 4, 100h Abs. 4, 110a Abs. 1 S. 5, 163f Abs. 2 S. 2 i. V. m. § 100d Abs. 1 und 2 StPO). Durch die Maßnahmen kann nämlich auf die zum Kernbereich gehörenden Informationen typisch zugegriffen werden (vgl. Kapitel 2, B. II. 2.).

2. Wohnraumüberwachung und Online-Durchsuchung

Die Online-Durchsuchung (§ 100b StPO) und die akustische Wohnraumüberwachung (§ 100c StPO), deren Eingriffsintensität nunmehr unter den individuellen heimlichen Ermittlungsmaßnahmen in der StPO als die schwersten eingestuft wer-

[137] Diejenigen für die Erhebung der Verkehrs- und Standortdaten sieht § 101a StPO durch die Novellierung vom Dezember 2015 (BGBl. I S. 2218) isoliert vor. Ihr Inhalt ist aber praktisch identisch mit § 101 StPO (vgl. oben A. II. 4.).

den,[138] unterliegen „besonders engen" Eingriffsvoraussetzungen und „sehr strengen" verfahrensrechtlichen Sicherungen (§§ 100d, e, 101, 101b StPO).

a) Wohnraumüberwachung

(1) Die akustische Wohnraumüberwachung betrifft das Abhören und Aufzeichnen nichtöffentlich gesprochener Worte in einer Wohnung (§ 100c Abs. 1 StPO). Sie richtet sich auf alle Lebensäußerungen, die in der „Privatwohnung", die einen engen Bezug zur Menschenwürde hat und ein räumliches Substrat darstellt (Art. 13 Abs. 1 GG), mit „bestimmten Gesprächspartnern" geführt werden.[139] Daher ermöglicht sie eine zeitliche und räumliche Rundumüberwachung, die aber verfassungsrechtlich verboten ist. Danach verlangte das *BVerfG* in seiner Entscheidung von 2004 zu ihrer Rechtfertigung eine gesetzliche Ausgestaltung, um dem Kernbereich der privaten Lebensgestaltung zuzuordnende Sachverhalte so bald als möglich aus dem Verfahren auszuklammern oder ihre Aufzeichnungen wenn auch verspätet zu vernichten bzw. deren Verwendung zu untersagen.[140] Hierzu fordert es nach Art. 13 Abs. 3 GG und dem Verhältnismäßigkeitsgrundsatz erhöhte Eingriffsvoraussetzungen, die Einsetzbarkeit der Wohnraumüberwachung als eines „besonders schweren Grundrechtseingriffs" auf gesetzlich bestimmte „besonders schwere Straftaten" zu beschränken, und Verfahrensvorkehrungen, um ihre Eingriffsintensität hinreichend aufzuwiegen.[141] Die geltende Ermächtigung ist auf das Änderungsgesetz, das den Inhalt dieses Urteils widergespiegelt hat und am 1. Juli 2005 in Kraft getreten ist (siehe Kapitel 1, Fn. 14), zurückgeführt.

(2) Zuerst ist i. R. d. Richtervorbehalts für die Anordnung der Wohnraumüberwachung grundsätzlich nicht der Ermittlungsrichter des Amtsgerichts, sondern die mit drei Richtern besetzte Kammer des Landgerichts (vgl. § 74a Abs. 4 GVG; sog. die „Sonderstrafkammer für Staatsschutzsachen"[142]), ausnahmsweise auch bei Gefahr im Verzug nicht die StA und ihre Ermittlungspersonen, sondern der Vorsitzende der Kammer zuständig (Art. 13 Abs. 3 S. 3 – 4 GG und § 100e Abs. 2 S. 1 – 2 StPO = § 100d Abs. 1 S. 1 – 2 StPO a. F.). Außerdem ist eine Anordnung und eine Verlängerung der Maßnahme auf höchstens einen Monat befristet (§ 100e Abs. 2 S. 4 – 5 StPO = § 100d Abs. 1 S. 4 – 5 StPO a. F.); wenn sie auch nach sechs Monaten weiter zu verlängern ist, so entscheidet darüber das OLG (§ 100e Abs. 2 S. 6 StPO = § 100d Abs. 1 S. 6 StPO a. F.). Kurzum darf die akustische Wohnraumüberwachung auch in Eilfällen nicht von der Strafverfolgungsbehörde angeordnet werden.[143] Darin, dass

[138] Insb. für Online-Durchsuchung *Singelnstein/Derin*, NJW 2017, 2646, 2647; *Soiné*, NStZ 2018, 497.

[139] M-G/*Schmitt*, StPO, § 100c Rn. 2 f.

[140] *BVerfGE* 109, 279, 324 [Rn. 152] und 328 – 335 [Rn. 169 – 196].

[141] *BVerfGE* 109, 279, 335 ff. [Rn. 197 ff., insb. Rn. 225 f.] und 357 ff. [Rn. 269 ff.].

[142] *Roxin/Schünemann*, § 36 Rn. 50.

[143] Vgl. BT-Drs. 13/8651, S. 14; *Papier*, in: Maunz/Dürig, GG-K, Art. 13 Rn. 78. Für die Online-Durchsuchung, die zu ihrer Durchführung regelmäßig einen erheblichen Zeitaufwand

auch die Eilkompetenz der StA ausgeschlossen ist, unterscheidet sich dieser qualifizierte Richtervorbehalt von demjenigen sonstiger verdeckter Maßnahmen ausdrücklich. Bezüglich der Form und des Inhalts der Anordnung sind im richterlichen Beschluss (soweit möglich) die Personalien des von der Maßnahme Betroffenen, der Tatvorwurf, Art, Umfang, Dauer und Endzeitpukt der Maßnahme, die Art der zu erhebenden Informationen und ihre Bedeutung für das Verfahren und schließlich die zu überwachenden Wohnräume (bei der Online-Durchsuchung, eine möglichst genaue Bezeichnung des zu überwachenden, informationstechnischen Systems) anzugeben (§ 100e Abs. 3 S. 1, S. 2 Nrn. 1–4, 6, 7 StPO = § 100d Abs. 2 StPO a. F.). Dabei sind in der Begründung die wesentlichen Abwägungsgesichtspunkte darzulegen, die die bestimmten Tatsachen, die einen Verdacht begründen, und die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme enthalten (§ 100e Abs. 4 StPO = § 100d Abs. 3 StPO a. F.).[144]

Der Gesetzgeber zielt daneben darauf ab, dass sich das Gericht i. R. d. Wohnraumüberwachung nicht nur bei ihrer Anordnung, sondern auch nach Beendigung ihrer Durchführung – unabhängig von subjektivem Rechtsschutz – in die Prüfung ihrer Rechtmäßigkeit konkret einschaltet. Nach Beendigung der Maßnahme muss die Ermittlungsbehörde daher je nach den Umständen des Einzelfalls über deren Ergebnisse und auch deren Verlauf, aber mindestens über Erfolg und Misserfolg der Maßnahme, ggf. Bedenken gegen die Fortsetzung oder gegen die Art, den Umfang und die Dauer der Maßnahme das anordnende Gericht unterrichten (§ 100e Abs. 5 S. 1–3 StPO = § 100d Abs. 4 S. 1 StPO n. F.).[145] Liegen die Voraussetzungen der Anordnung nicht mehr vor, so ist die Maßnahme unverzüglich zu beenden und daher hat das Gericht den Abbruch der Maßnahme anzuordnen, sofern der Abbruch nicht bereits durch die StA veranlasst wurde; dies kann auch durch den Vorsitzenden allein erfolgen (§ 100e Abs. 5 S. 1, 4–5 StPO = § 100d Abs. 4 S. 2–3 StPO a. F.). Damit die Maßnahme wieder angeordnet wird, ist ein neuer Anordnungsbeschluss erforderlich.[146] Zum anderen dürfen die durch die Wohnraumüberwachung erlangten personenbezogenen Daten für andere Zwecke verwendet werden, jedoch ist dies nur unter mit § 100c Abs. 1 StPO vergleichbaren Bedingungen zugelassen (§ 100e Abs. 6 StPO = § 100d Abs. 5 StPO a. F.). Die Daten dürfen in anderen Strafverfahren, die die Katalogstraftaten nach § 100b Abs. 2 StPO betreffen (§ 100e Abs. 6 Nr. 1), nur zur Abwehr einer dringenden Gefahr für hochrangige Rechtsgüter (etwa für Leben, Leib oder Freiheit einer Person, für die Sicherheit oder den Bestand des Staates oder für Gegenstände von bedeutendem Wert oder für sonstige bedeutende Vermögenswerte) (Nr. 2) verwendet werden. Wenn die Daten umgekehrt durch Maßnahmen zur Gefahrenabwehr erlangt wurden, dürfen sie ebenfalls nur in den Strafverfahren, die sich gegen die Katalogtaten des § 100b Abs. 2 StPO richten,

verlangt, dürfte die Eilfallregelung regelmäßig nicht anwendbar sein (*Roggan*, StV 2017, 821, 828).

[144] M-G/*Schmitt*, StPO, § 100e Rn. 17.

[145] M-G/*Schmitt*, StPO, § 100e Rn. 20.

[146] M-G/*Schmitt*, StPO, § 100e Rn. 19.

verwendet werden (Nr. 3). Nach Beendigung der Maßnahmen ist der dadurch Betroffene nach § 101 StPO nachträglich zu benachrichtigen und daraufhin steht ihm die Möglichkeit des Rechtsschutzes offen.

Nach der Meinung des *BVerfG* sind bei der akustischen Wohnraumüberwachung, auch der Online-Durchsuchung, sowohl die Strafverfolgungsbehörden als auch das Gericht verpflichtet, die Verwertbarkeit und Löschung der Daten, die den Kernbereich privater Lebensgestaltung betreffen, zu beurteilen (§ 100d Abs. 3 S. 2–3 und Abs. 4 S. 4–6 StPO; vgl. § 100c Abs. 5 S. 6 und Abs. 7 StPO a. F.).[147] Dies zieht die Möglichkeit in Betracht, dass höchstpersönliche Daten durch solche Maßnahmen erhalten werden und der wirksame Kernbereichsschutz nach der willkürlichen Beurteilung der Strafverfolgungsbehörden vereitelt wird. Hierbei bedarf es einer eindeutigen Regelung, wer diese Entscheidung beim Gericht zu beantragen hat.[148] Andernfalls liegt die Entscheidung in den Händen der Strafverfolgungsbehörden und diese werden i. d. R. die Fortführung der Maßnahme bzw. die Nutzung der Daten bestätigen.[149]

b) Online-Durchsuchung

Die Online-Durchsuchung, mit technischen Mitteln in von dem Betroffenen genutzte informationstechnische Systeme heimlich einzugreifen und dessen Nutzung zu überwachen bzw. dort gespeicherte Inhalte aufzuzeichnen, wurde trotz praktischer Anforderungen erst kürzlich durch die Novelle, die am 24. August 2017 in Kraft getreten ist, wegen des besonders hohen Risikos einer Persönlichkeitsverletzung gesetzlich geregelt (siehe Kapitel 1, Fn. 30; vgl. für das Computer-Grundrecht als maßgebliches Grundrecht, Kapitel 2, B. III. 2.). Die Eingriffsvoraussetzungen und die verfahrensrechtlichen Vorkehrungen für diese Maßnahme sind auf gleicher Höhe wie diejenigen der Wohnraumüberwachung gebildet. Durch die Gesetzänderung vom 2017 wurden die für die Überwachung der Wohnräume geltenden, bestehenden Anforderungen (§ 100c Abs. 4 bis 7 StPO a. F.) auf die Online-Durchsuchung (§§ 100b, d, e StPO n. F.) erweitert. Dies basiert auf einer gesetzgeberischen Erwägung, dass die Eingriffsintensität beider Maßnahmen vergleichbar ist.[150] Angesichts der Abweichung der Eingriffsintensität zwischen den beiden Maßnahmen wird eine solche Regelung jedoch beanstandet; vgl. eingehend unten c).

---

[147] Vgl. für die akustische Wohnraumüberwachung *BVerfGE* 109, 279, 333 [Rn. 191].

[148] Vgl. *BVerfGE* 109, 279, 334 [Rn. 193].

[149] Diese Verfahrenssicherungen gelten jedoch nach der Rspr. des *BVerfG* nicht in der TKÜ, wobei die StA selbst über die Verwendbarkeit der gewonnenen Erkenntnisse entscheiden kann (vgl. unten 3. a)).

[150] BT-Drs. 18/12785, S. 54; vgl. *BVerfGE* 141, 220, 304 [Rn. 210 a. E.]; *Niedernhuber*, JA 3/2018, 169, 171. Bei der Entscheidung über Verfassungsbeschwerden, die sich gegen Regelungen des BKAG richten, die als Unterabschnitt 3a durch das Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt vom 25. Dezember 2008 (BGBl. I S. 3083) mit Wirkung zum 1. Januar 2009 eingefügt wurden, sieht das *BVerfG* hinsichtlich des Eingriffsgewichts die Wohnraumüberwachung sowie den Zugriff auf informa-

Vor der Gesetzgebung von 2017 stellte die Online-Durchsuchung als solche nach höchstgerichtlicher Rspr. sowie h. M. in der Literatur kein verfassungswidriges Ermittlungsmittel dar, jedoch durfte sie auf der Grundlage von §§ 94 ff., 102 ff. StPO bzw. §§ 100a ff. StPO (a. F.) nicht zugelassen werden.[151] Diese Maßnahme geht nämlich über die Reichweite herkömmlicher TKÜ weit hinaus. Damit können nicht nur neu hinzukommende Kommunikationsinhalte, sondern auch alle auf einem informationstechnischen System bereits erzeugten und gespeicherten Inhalte sowie auch das gesamte Nutzungsverhalten einer Person überwacht werden.[152] Daher muss sie sich von der Quellen-TKÜ, in der zur Überwachung verschlüsselter Kommunikation in das System technisch eingegriffen wird, und die sich nur gegen die Daten, die auch während des laufenden Übertragungsvorgangs hätten überwacht und aufgezeichnet werden können, richtet, sowohl begrifflich als auch rechtlich unterscheiden (vgl. unten 3. b)). Die beiden Maßnahmen werden aber auf technischer Seite[153] allgemein in der Weise vorgenommen, dass Ermittler in den Herrschaftsbereich des Betroffenen, d. h. in von dem Betroffenen genutzte informationstechnische Systeme, eingreifen (etwa durch den heimlichen Einsatz staatlicher Schadsoftware zur Computerspionage, nämlich Spionage-Software [sog. „Staatstrojaner"]).[154] Aus diesem Grund werden die technischen Sicherungen und Protokollierungspflichten, die für die Quellen-TKÜ gelten, auch auf die Online-Durchsuchung übertragen (§ 100b Abs. 4 i. V. m. § 100a Abs. 5 – 6, abgesehen von Abs. 5 S. 1 Nr. 1 StPO).[155]

c) Kritik an der Gesetzgebung zur Online-Durchsuchung (und Quellen-TKÜ)

(1) Die Gesetzgebung des Jahres 2017 wird viel kritisiert.[156] Nach der Literatur hat der Gesetzgeber quasi „durch die Hintertür",[157] aber „nicht zimperlich"[158] die Er-

tionstechnische Systeme für besonders tief in die Privatsphäre eindringend (a. a. O. 269) und achtet i. R. v. Anforderungen an Eingriffsschwellen und wirksame verfahrensrechtliche Kontrolle übergreifend gleich (a. a. O. 270 ff. und 275 ff.); krit. *Roggan*, StV 2017, 821, 826 f.

[151] Vgl. *BVerfGE* 120, 274, 308 f.; *BGHSt* 51, 211, 212 ff., 217 f.; BT-Drs. 16/5846, S. 64; M-G/*Schmitt*, StPO, § 100a Rn. 7c; *Sieber*, 69. DJT 2012, C 104; a. A. *Hofmann*, NStZ 2005, 121, 123 ff.

[152] BT-Drs. 18/12785, S. 54; *Roggan*, StV 2017, 821, 825.

[153] Vgl. „mit technischen Mitteln" in § 100a Abs. 2 S. 2 und § 100b Abs. 1 StPO. Eine Befugnis, die Wohnung des Betroffenen zum Zweck der Aufbringung der Überwachungssoftware heimlich zu betreten, ist daher mit der Befugnis nach den Vorschriften nicht verbunden (BT-Drs. 18/12785, S. 52; *Roggan*, StV 2017, 821, 822; *Singelnstein/Derin*, NJW 2017, 2646, 2647; auch *Niedernhuber*, JA 3/2018, 169, 171).

[154] *Beukelmann*, NJW-Spezial 2017, 440; *Blechschmitt*, MMR 2018, 361, 364. In dieser Hinsicht stellt die Online-Durchsuchung ein „staatliches Hacken" dar (vgl. BT-Drs. 16/5846, S. 64 am Anfang).

[155] BT-Drs. 18/12785, S. 54.

[156] Vgl. *Beukelmann*, NJW-Spezial 2017, 440; *Roggan*, StV 2017, 821; *Singelnstein/Derin*, NJW 2017, 2646; *Freiling/Safferling/Rückert*; JR 2018, 9; *Blechschmitt*, MMR 2018, 361; *Soiné*, NStZ 2018, 497 m. w. N.

mächtigungsnormen zur Online-Durchsuchung und der Q-TKÜ in die StPO eingefügt.[159]

Im Gesetzestext des § 100a Abs. 1 S. 2, 3 zur Quellen-TKÜ und § 100b Abs. 1 StPO zur Online-Durchsuchung fehlt es an einer Eingrenzung der technischen Mittel für das Eindringen in ein informationstechnisches System. Insoweit fehlt es auch an abstrakten Vorgaben zu den spezifischen technischen Anforderungen an die Überwachungssoftware und im Text liegt nur der Wortlaut „nach dem Stand der Technik" vor (§ 100a Abs. 5 S. 2 und 3 i. V. m. § 100b Abs. 4 StPO). Dies trägt der rasanten Entwicklung im Computer-Bereich Rechnung[160] und die Vorschriften wurden in technischer Hinsicht entwicklungsoffen, nämlich „technikoffen", konzipiert. Ebenso bleiben jedoch auch konkrete technische Vorkehrungen offen, um eine Lücke in der Sicherheit zu schließen. Vor diesem Hintergrund werden zwei Punkte besonders kritisiert. Nur mit neu rechtsetzenden Vorschriften scheidet die Gefährdung einer Bildung von Persönlichkeitsprofilen durch die Online-Durchsuchung, auch die Quellen-TKÜ, nicht technisch aus, und zudem ist unklar, ob nunmehr in der Praxis eine Überwachungssoftware, die mit technischen Vorkehrungen ausgestattet ist, die verhindern, dass die Quellen-TKÜ für eine Online-Durchsuchung genutzt wird, tatsächlich verwertet werden kann (unten (2)). Außerdem stellt sich die Frage noch, ob die Online-Durchsuchung gegenwärtig zum Zweck der Strafverfolgung erforderlich ist (unten (3)).[161] Mit dieser Maßnahme kann nämlich ein informationstechnisches System komplett durchleuchtet werden[162], und dadurch wird eine Rundumüberwachung, die verfassungsrechtlich unzulässig ist, ermöglicht.

(2) In den Neuregelungen werden vor allem keine technischen Voraussetzungen zur einzusetzenden Überwachungssoftware festgelegt, die den Kern der Durchführung dieser Maßnahmen bildet (vgl. § 100a Abs. 5 StPO).[163] Zuerst kann durch die Quellen-TKÜ, die eine funktionale Äquivalenz zur herkömmlichen TKÜ darstellt, ausschließlich „laufende" „inhaltliche" Kommunikation überwacht und aufgezeichnet werden (vgl. § 100a Abs. 5 S. 1 Nr. 1 StPO). Um dies in zeitlicher Hinsicht zu gewährleisten, sieht S. 1 Nr. 1 lit. b vor, dass nur zukünftige Kommunikationsinhalte, d. h. dieselben, die „ab dem Zeitpunkt der Anordnung" nach § 100e Abs. 1

---

[157] *Beukelmann*, NJW-Spezial 2017, 440 am Anfang.

[158] *Blechschmitt*, MMR 2018, 361, 366.

[159] Der Inhalt des Gesetzentwurfs wurde zwar bereits im Verlauf des Gesetzgebungsverfahrens von zahlreichen Sachverständigen scharf kritisiert, aber dennoch ohne ausreichende Debatte in der Ausschussfassung vom Bundestag angenommen (*Beukelmann*, NJW-Spezial 2017, 440; *Singelnstein/Derin*, NJW 2017, 2646).

[160] M-G/*Schmitt*, StPO, § 100a Rn. 14k; auch *Blechschmitt*, MMR 2018, 361, 365.

[161] Vgl.: Während im Bereich der Gefahrenabwehr der Einsatz von Überwachungstechniken mittels einer speziellen Software den Polizeibehörden schon seit längerer Zeit ausdrücklich eingeräumt wird, um schwere Gefahren abzuwehren, ist dies im Bereich der Strafverfolgung bis vor dieser Gesetzgebung nicht der Fall gewesen (BT-Drs. 18/12785, S. 46).

[162] Zust. *Niedernhuber*, JA 3/2018, 169, 171.

[163] M-G/*Schmitt*, StPO, § 100a Rn. 14i ff.

StPO anfallen, erhoben werden dürfen.[164] Demnach muss die für die Quellen-TKÜ zu verwendende Software so konstruiert/programmiert sein, in technischer Hinsicht diesen Anforderungen zu genügen. So muss sie anhand der Meta-Daten, die etwa die Absende-, Empfangs- und Lesezeitpunkte enthalten, die einzelnen Textnachrichten unterscheiden können.[165] Nach S. 1 Nr. 2 und 3 sind zudem an dem zu infiltrierenden System nur Veränderungen vorzunehmen, die für die Datenerhebung unerlässlich sind, und die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig zu machen. Des Weiteren ist nach S. 2 die eingesetzte Überwachungssoftware nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Daher werden die Online-Durchsuchung und die Quellen-TKÜ auf die Erhebung von Daten beschränkt und hier ist die eigenständige Erzeugung von Daten und die Veränderung gespeicherter Daten unzulässig.[166] So ist insb. bei der Online-Durchsuchung nur eine passive Kenntnisnahme von Daten, die sich bereits in dem System befinden, gestattet, dagegen ist eine aktive Aktivierung des Systems, z. B. die (über das optische (Live-)Beobachten hinausgehende) Erfassung der Umgebung durch die Inbetriebnahme einer Webcam, verboten.[167] Kann bei Durchführung der Online-Durchsuchung und der Quellen-TKÜ nicht sichergestellt werden, dass die Überwachungssoftware das infiltrierte System vor unbefugter Nutzung und Manipulationen Dritter zuverlässig – und nach dem Stand der aktuellen Technik – schützt, so werden *a priori* nur unzuverlässige Beweise erhoben.[168] Daher setzt die Rechtfertigung der Maßnahmen in technischer Hinsicht eine den o. g. Anforderungen genügende Software voraus. Ob diese zum Zeitpunkt der Rechtssetzung überhaupt bereits zur Verfügung stand, ist aber unklar,[169] und dies gilt auch im Moment. Auch die Ausführung der Gesetzesbegründung ist nicht ganz frei von Zweifeln hieran.[170] Nach der Begründung werde durch Protokollierungspflichten des

---

[164] BT-Drs. 18/12785, S. 50 – 53. Daher unterliegen der Quellen-TKÜ auch die Kommunikationen, die nach einer Anordnung aber vor der Installation der Überwachungssoftware geführt wurden, d. h. solche, die im Zeitraum zwischen dem Erlass des richterlichen Beschlusses und dem Aufbringen der Software nach Abschluss des Übertragungsvorgangs auf dem informationstechnischen System des Betroffenen gespeichert wurden (a. a. O. S. 51 f.; zust. *Roggan*, StV 2017, 821, 823 f.: nach dem § 100a Abs. 1 S. 3 StPO).

[165] BT-Drs. 18/12785, S. 53: Daher „*dürfen ältere Messenger-Nachrichten nur im Rahmen einer Maßnahme nach § 100b StPO-E (Online-Durchsuchung) ausgeleitet werden*".

[166] Vgl. *Niedernhuber*, JA 3/2018, 169, 172.

[167] *Roggan*, StV 2017, 821, 826: „Nutzungsüberwachung"; auch *Niedernhuber*, JA 3/2018, 169, 172; *Singelnstein/Derin*, NJW 2017, 2646, 2647: Ermittlungsbehörde darf etwa Kamera oder Mikrofon der überwachten Endgeräte (eigenständig) nicht aktivieren und auch keine Bild- oder Ton-Aufnahmen machen.

[168] *Roggan*, StV 2017, 821, 825 und 827; auch M-G/*Schmitt*, StPO, § 100a Rn. 14k.

[169] Vgl. *Niedernhuber*, JA 3/2018, 169, 175: „*Derzeit ist es äußerst zweifelhaft, ob eine Abgrenzung zwischen der Quellen-TKÜ und der Online-Durchsuchung technisch exakt umzusetzen ist*"; dazu *Roggan*, StV 2017, 821, 822. *Roggan* findet, dass die Neuregelung die unzweideutigen Vorgaben des BVerfG missachtet bzw. vermissen lässt (a. a. O. 824).

[170] *Roggan*, StV 2017, 821, 822 [Tz. II.]; vgl. BT-Drs. 18/12785, S. 53: „*Soweit eine den Anforderungen des Abs. 5 S. 1 Nr. 1 genügende Software … nicht zur Verfügung stehen sollte, …*

§ 100a Abs. 6 StPO die nachträgliche Überprüfung ermöglicht, ob eine Software verwendet wurde, die den Anforderungen des § 100a Abs. 5 S. 1 Nr. 1 lit. b StPO genügt hat,[171] jedoch ist gegenwärtig zweifelhaft, ob diese Pflichten unter technischem Aspekt tatsächlich erfüllt werden können.[172]

Daneben kann aus kompetenzrechtlicher Sicht problematisch sein, wer zu prüfen und zertifizieren hat, ob die einzusetzende Software zu solchen konkreten technischen Vorkehrungen geeignet ist: eine Zuständigkeit für eine Prüfung und Zertifizierung, ob die Software der Anforderung an den Schutz nach dem Stand der Technik des § 100a Abs. 5 S. 2 und 3 StPO gerecht wird. Angesichts der Bedeutung, die die Software in diesen Maßnahmen hat, ist eine solche Prüfung nicht einer einfachen Privatperson zu übertragen. Sie sollte einer unabhängigen, mit Sachkunde ausgestatteten Stelle überlassen bleiben, nicht aber dem die Maßnahme anordnenden Ermittlungsrichter (vgl. § 100e Abs. 1 StPO).[173] Denn für eingriffsintensive Maßnahme bedarf es zuverlässiger externer Kontrollen.

(3) Auch wenn die o. g. Anforderungen vorweg technisch eindeutig sichergestellt werden, ist es noch sehr zweifelhaft, ob die Online-Durchsuchung im Ermittlungsverfahren überhaupt gerechtfertigt werden kann.[174] Da sie sich vor allem an PCs und Smartphones, die Bürger täglich privat und beruflich nutzen, richtet, deckt der Datenumfang, der dadurch erlangt werden kann, nicht nur alle Informationen aus TKÜ, akustischer Wohnraumüberwachung und Überwachung außerhalb von Wohnungen ab, vielmehr geht er weit darüber hinaus.[175] Überwacht werden alle auf einem

ist die Maßnahme unter den Voraussetzungen des § 100a StPO unzulässig. Insoweit kommt allerdings die Durchführung einer Online-Durchsuchung gemäß § 100b StPO in Betracht."

[171] Vgl. BT-Drs. 18/12785, S. 52: Bei der Vorbereitung, Durchführung und Nachbereitung der Maßnahme wird verfahrenstechnisch sichergestellt, dass die Vorgaben des Gesetzes in vollem Umfang eingehalten werden.

[172] *Freiling/Safferling/Rückert*, JR 2018, 9, 19 f.; M-G/*Schmitt*, StPO, § 100b Rn. 13. Es scheint weiter, dass die Informationen, die gesetzlich protokolliert werden müssen, für die nachträgliche Überprüfung der Rechtsmäßigkeit der Art und Weise der Durchführung der Maßnahme (vgl. § 101 Abs. 7 S. 2 StPO) nicht ausreichend sind (*Singelnstein/Derin*, NJW 2017, 2646, 2647); es fehlt etwa an der Protokollierung der kompletten Löschung des eingesetzten Programms und ihres Zeitpunkts. Für den weiteren Einsatz der Überwachungssoftware ist dabei allerdings die Offenlegung ihres Quellcodes aber nicht erforderlich (*Freiling/Safferling/Rückert*; JR 2018, 9, 12; M-G/*Schmitt*, StPO, § 100a Rn. 14m).

[173] Zust. *Roggan*, StV 2017, 821, 824 a. E.; vgl. M-G/*Schmitt*, StPO, § 100a Rn. 14k: Insoweit besteht keine gesetzliche Verpflichtung zur Verwendung staatlicherseits programmierter Software wegen fehlender Regulierung.

[174] Zust. *Roggan*, StV 2017, 821, 827. Nach *Roggan* beziehen sich die bisherigen Entscheidungen des *BVerfG* auf Befugnisse zur Gefahrenabwehr und es hat sich nicht zu den verfassungsrechtlichen Schranken geäußert, die bei repressiv-rechtlichen Eingriffsregelungen zu beachten sind; daher lassen sich die in den Entscheidungen genannten Beschränkungen nicht ohne Weiteres auf eine strafprozessuale Regelung übertragen (a. a. O.).

[175] *Roggan*, StV 2017, 821, 826; dazu *Blechschmitt*, MMR 2018, 361, 365: Wenn sich die Online-Durchsuchung an smarte Geräte (z. B. *Echo Show*) und eine bestimmte Anwendung wie z. B. *Alexa* von *Amazon* richtet, so ermöglicht dies in der Tat akustische Wohnraumüberwachung.

Computer-System gespeicherten Daten und die hinzukommenden Kommunikationsinhalte sowie das gesamte Nutzungsverhalten des Betroffenen, und darüber hinaus ist ein „Live-Zugriff", nämlich der „heimliche Blick über die Schulter" möglich; außerdem können durch diese Maßnahme auch Zugangscodes wie Benutzernamen und Passwörter erhoben werden, die mittels Keylogging oder Screen-/Applicationshots erlangt werden.[176] Insofern ermöglicht sie für sich allein, unabhängig von weiteren Datenerhebungen und -verarbeitungen, besonders tief in die Privatsphäre eindringende Eingriffe.[177] So ermöglicht zwar die Online-Durchsuchung – technisch auch die Quellen-TKÜ – eine (fast) grenzenlose Überwachung, die verfassungsrechtlich verboten ist,[178] aber die Gewährleistung der Einhaltung dieses Verbots ist in technischer Hinsicht nicht klar.

Daraus folgt, dass die potenzielle Eingriffsintensität einer Online-Durchsuchung viel tiefer ist als diejenige einer Wohnraumüberwachung nach § 100c StPO. Sie ist eher mit wiederholt durchführbaren heimlichen Hausdurchsuchungen vergleichbar.[179] So ist dem Gesichtspunkt des *BVerfG* in seiner Entscheidung zum BKAG und der Gesetzesbegründung zur Gesetzesänderung vom 2017, die Eingriffsintensität beider Maßnahmen gleich zu achten, nicht zuzustimmen. Dies verstößt gegen den Verhältnismäßigkeitsgrundsatz, weil die Online-Durchsuchung angesichts des Gewichts des Grundrechtseingriffs viel stärker ist als die Wohnraumüberwachung.[180] Durch die Einführung der Online-Durchsuchung in den Bereich der Strafverfolgung wird u. a. die Grenze zwischen Prävention und Repression weiter verwischt.[181] Insofern hat *Sieber* schon am 69. DJT zu Recht gesagt:

> „Bei einer angemessenen Regelung der Quellen-TKÜ sind gegenwärtig (jedoch) keine überzeugenden Gründe für die Rechtfertigung einer Online-Durchsuchung oder Online-Überwachung zu rein repressiven Zwecken der Strafverfolgung ersichtlich."[182]

---

[176] *Roggan*, StV 2017, 821, 825.

[177] *Roggan*, StV 2017, 821, 826; auch *BVerfGE* 120, 274, 323 [Rn. 232]: Naheliegendes Risiko, weitreichende Rückschlüsse auf die Persönlichkeit des Betroffenen zu ermöglichen.

[178] *Blechschmitt*, MMR 2018, 361, 365; *Roggan*, StV 2017, 821, 826.

[179] *Roggan*, StV 2017, 821, 826 a. E.

[180] Zudem ist zweifelhaft, ob der Straftatenkatalog in § 100b Abs. 2 StPO, der keineswegs nur Schwerkriminalität erfasst (z. B. Diebstahls- und Hehlereidelikt), den Anforderungen der Verhältnismäßigkeit gerecht wird (zust. *Roggan*, StV 2017, 821, 827; *Singelnstein*/*Derin*, NJW 2017, 2646, 2647).

[181] *Beukelmann*, NJW-Spezial 2017, 440; *Roggan*, StV 2017, 821, 827.

[182] *Sieber*, 69. DJT 2012, C 108, dazu weiter C. 109: „*Momentan sollten eher vor einer repressiven Regelung die Erfahrungen mit der präventiven Online-Durchsuchung und deren weiterer Normierung in den Landespolizeigesetzen abgewartet werden.*"

3. TKÜ und Postbeschlagnahme

a) TKÜ

(1) Die TKÜ, die es auf die Erfassung der Inhaltsdaten der TK anlegt (§§ 100a, 100d Abs. 1, 2, 100e Abs. 1, 3, 4 StPO = §§ 100a – b StPO a. F.), stellt die praktisch am weitesten verbreitete heimliche Ermittlungsmaßnahme im Bereich der organisierten Kriminalität dar. Zunächst benutzt die StPO nach dem BegleitG zum TKG, das am 24. Dezember 1997 in Kraft trat,[183] nicht mehr den Begriff „Fernmeldeverkehr", sondern die begrifflich weitere „Telekommunikation".[184] So ist der Anwendungsbereich der TKÜ vorerst gemäß § 100a Abs. 1 S. 1 StPO (= § 100a Abs. 1 StPO a. F.) i. d. R. durch den Begriff der TK i. S. d. § 3 Nr. 22 und 23 TKG zu bestimmen.[185] Nunmehr können nach h. M. nicht nur der herkömmliche Fernsprechverkehr, sondern auch jede Art der Nachrichtenübermittlung mittels technischer Einrichtungen oder Systemen wie SMS-Dienste, E-Mail-Verkehr, soziale Netzwerke und Internet-Telefonie etc. nach § 100a StPO überwacht werden.[186] Wie weit der Begriff der TK des § 100a Abs. 1 StPO reicht, ist somit noch nicht abschließend geklärt[187] und nach der Entwicklung der IuK-Technologie ist er entwicklungsoffen.[188] Diesbezüglich wurde die Quellen-TKÜ durch die StPO-Reform vom August des Jahres 2017 in § 100a Abs. 1 S. 2 und 3 StPO verrechtlicht (vgl. unten b)),[189] es ist hingegen noch nicht eindeutig, ob ein „verdeckter" Zugriff auf die „auf dem Server des Dienstanbieters gespeicherten" Kommunikationsinhalte/Inhaltsdaten stets durch § 100a StPO gerechtfertigt werden kann (vgl. unten C.).

(2) Da der heimliche Zugriff auf Inhaltsdaten und ihre Erfassung als solche ein schwerwiegenden Grundrechtseingriff darstellen, unterliegt die TKÜ dem Richtervorbehalt und die Eilzuständigkeit bei Gefahr im Verzug ist auch beschränkt; hierbei ist nur die StA zur Anordnung befugt, nicht aber ihre Ermittlungspersonen (§ 100e

---

[183] Das TKG, das eine gesetzgeberische Maßnahme zur Öffnung und Liberalisierung der Märkte der TK darstellt (BT-Drs. 13/4438, S. 1), trat am 1. August 1996 in Kraft (BGBl. I S. 1120), und demnach wird verlangt, dass andere Rechtsgebiete diesen veränderten rechtlichen Rahmenbedingungen (z. B. Terminologie) angepasst werden. Dabei wurde i. R. d. Strafverfahrensrechts die Gesetzesänderung zur Schließung von Strafbarkeitslücken sowie der Sicherstellung der Überwachbarkeit von TK (BT-Drs. 13/8016, S. 1) durch das BegleitG zum TKG vom 17. 12. 1997 (BGBl. I S. 3018) vorgenommen.

[184] Vgl. *Roxin/Schünemann*, § 36 Rn. 3.

[185] Vgl. *BGH* NJW 2009, 1828; *Bruns*, KK-StPO, § 100a Rn. 4; M-G/*Schmitt*, StPO, § 100a Rn. 6; *Roxin/Schünemann*, § 36 Rn. 3; *Kasiske*, StraFo 6/2010, 228, 229: ein enger technischer TK-Begriff.

[186] *Bruns*, KK-StPO, § 100a Rn. 16 ff.; M-G/*Schmitt*, StPO, § 100a Rn. 6 – 7a; *Roxin/Schünemann*, § 36 Rn. 3 m. w. N.

[187] *Niedernhuber*, JA 3/2018, 169, 172.

[188] *Bruns*, KK-StPO, § 100a Rn. 4: mit Rücksicht auf die Praktikabilität der §§ 100a ff. StPO.

[189] Vgl. M-G/*Schmitt*, StPO, § 100a Rn. 6: Ein solcher Kommunikationsinhalt gehört nicht zur „TK" i. S. d. Abs. 1 S. 1.

Abs. 1 S. 1–2 StPO = § 100b Abs. 1 S. 1–2 StPO a. F.). Außerdem ist die Anordnung der Maßnahme und ihre Verlängerung befristet (jeweils höchstens 3 Monate; § 100e Abs. 1 S. 4–5 StPO = § 100b Abs. 1 S. 4–5 StPO a. F.)[190], und die Entscheidungsformel der Anordnung muss sowohl (soweit möglich) den Namen und die Anschrift des Betroffenen, den Tatvorwurf, Art, Umfang, Dauer und Endzeitpunkt der Maßnahme und die Art der zu erhebenden Informationen und ihre Bedeutung für das Verfahren als auch die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgerätes[191] enthalten (§ 100e Abs. 3 S. 1, S. 2 Nrn. 1–5 StPO = § 100b Abs. 2 StPO a. F.). Daneben wurde durch die Novellierung 2017 umschrieben, dass auch beim Anordnungsbeschluss der TKÜ – ebenfalls wie bei Online-Durchsuchung und akustischer Wohnraumüberwachung – die bestimmten Tatsachen, die den Verdacht begründen, und die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme anzugeben sind (§ 100e Abs. 4 S. 2 Nrn. 1 und 2 StPO). Des Weiteren muss die Ermittlungsbehörde nach Beendigung der TKÜ über die „Ergebnisse" der Maßnahme das anordnende Gericht unterrichten (§ 100e Abs. 5 S. 2 StPO = § 100b Abs. 4 S. 2 StPO a. F.); aber – anders als bei Online-Durchsuchung und akustischer Wohnraumüberwachung – nicht über deren Verlauf.

Da sich die TKÜ an Inhaltsdaten richtet, wird sie – mit der Online-Durchsuchung und der akustischen Wohnraumüberwachung – durch die Vorschrift zum Schutz des Kernbereichs privater Lebensgestaltung, den sie einer unmittelbaren Gefahr aussetzt, geregelt (§ 100d Abs. 1–2 StPO = § 100a Abs. 4 StPO a. F.). Jedoch ist hier anders als bei anderen beiden Maßnahmen (vgl. § 100d Abs. 3–4 StPO) die Zuständigkeit zur Beurteilung der Verwertbarkeit der gewonnenen Erkenntnisse nicht in der Vorschrift bestimmt, daher wird sie i. d. R. der StA als Herrin des Ermittlungsverfahrens gegeben. Diesbezüglich hat das *BVerfG* in seiner Entscheidung über die Verfassungsmäßigkeit des TKÜG ausgeführt, dass dies aufgrund des Richtervorbehalts, der Unterrichtung des Gerichts über das Ergebnis der Maßnahme und der Gewährleistung der nachträglichen, gerichtlichen Überprüfung verfassungsrechtlich nicht infrage steht.[192] Dies liegt im Wesentlichen daran, dass das Risiko, dass die zum

[190] Auch die Quellen-TKÜ unterliegt als funktionale Äquivalenz zur herkömmlichen TKÜ dieser zeitlichen Begrenzung. Daher ist sie zunächst nur für die Dauer von drei Monaten zulässig. Dies reduziert die Gefahr, dass der Zeitraum zwischen dem Erlass des richterlichen Beschlusses und dem Aufbringen der Software unbegrenzt lang ist und ein rückwirkendes Ausleiten daher erhebliche Zeiträume umfasst. Wird die Software innerhalb dieses Zeitraums auf dem Gerät eingesetzt, ist ohne Bedeutung, wann sie aufgebracht wird. Kann sie innerhalb des Zeitraums künftig nicht aufgebracht werden, wird aber der Beschluss ungültig und die Maßnahme darf nicht mehr durchgeführt werden (BT-Drs. 18/12785, S. 51 f.).

[191] Zu anderen Kennungen des Anschlusses gehören z. B. IMSI, IP-Adresse, elektronisches Postfach und zu der Gerätekennung gehören z. B. IMEI (*Bruns*, KK-StPO, § 100e Rn. 14; M-G/*Schmitt*, StPO, § 100e Rn. 14).

[192] *BVerfGE* 129, 208, 249 f. [Rn. 221–224]: „*(Entgegen der Auffassung der Beschwerdeführer) ist es von Verfassungs wegen nicht geboten, zusätzlich zu den staatlichen Ermittlungsbehörden eine unabhängige Stelle einzurichten, die über die (Nicht-)Verwendbarkeit der gewonnenen Erkenntnisse im weiteren Ermittlungsverfahren entscheidet. … In seinem Be-*

Kernbereich gehörenden Informationen erhoben werden, bei der TKÜ geringer ist als bei der Online-Durchsuchung und der akustischen Wohnraumüberwachung, und dass die TKÜ in der modernen Informationsgesellschaft häufiger verwendet und weiter verbreitet ist (Nützlichkeit in der Praxis).

b) Quellen-TKÜ

(1) Um in der letzten Zeit die kriminalistischen Hindernisse zu überwinden, die sich aus der Ausweitung der verschlüsselten Datenübertragung insb. bei der Nutzung von Internet-Telefonie wie *skype* ergeben,[193] wurde in der Praxis die Notwendigkeit der Quellen-TKÜ immer wieder bekräftigt[194] und sie ist nunmehr ausdrücklich gestattet (§ 100a Abs. 1 S. 2–3 StPO). Diese Maßnahme ist – wie schon in ihrer Bezeichnung (Quellen-„TKÜ") deutlich wird – von Natur aus eine TKÜ und sollte es sein,[195] jedoch unterscheidet sie sich von einer allgemeinen TKÜ darin, dass sie auf die Kommunikationsinformationen abzielt, die nach Beendigung des Übertragungsvorgangs auf einzelnen informationstechnischen Systemen gespeichert sind.[196] So ist zwar die Quellen-TKÜ eine funktionale Äquivalenz zur herkömmlichen

---

schluss zur akustischen Wohnraumüberwachung hat es ausgeführt, dass es einer unabhängigen Stelle obliege, die Verwertbarkeit der gewonnenen Erkenntnisse … zu beurteilen. Die von Verfassungs wegen geforderten verfahrensrechtlichen Sicherungen gebieten jedoch nicht, dass in allen Fallkonstellationen neben staatlichen Ermittlungsbehörden weitere unabhängige Stellen eingerichtet werden, um die Einhaltung der gesetzlichen Bestimmungen zu gewährleisten."

[193] *Bruns*, KK-StPO, § 100a Rn. 42; *Klesczewski*, ZStW 123 (2011), 737, 742; M-G/*Schmitt*, StPO, § 100a Rn. 7a; *Niedernhuber*, JA 3/2018, 169, 170; *Sieber*, 69. DJT 2012, C 103 f.; *Singelnstein*, NStZ 2012, 593, 598; *Wolter/Greco*, SK-StPO, § 100a Rn. 28.

[194] Vgl. *Sieber*, 69. DJT 2012, C 38; auch *Hofmann*, NStZ 2005, 121: Wirkungslosigkeit der TKÜ nach § 100a StPO durch diverse Verschlüsselungstechnologien und die Erforderlichkeit der Online-Durchsuchung. Insoweit ist zwar als Mittel und Weg zur Überwindung der Verschlüsselung neben der Quellen-TKÜ eine Verpflichtung der Anbieter zur Herausgabe der automatisch generierten, temporären Schlüssel bzw. die Implementierung von Hintertüren für Behörden bereits in den Programmen durch deren Anbieter (sog. „back doors") denkbar, jedoch steht sie in Widerspruch zu geltenden Vorschriften. Denn es steht entgegen, dass die TKÜ ausschließlich in den Katalogtaten des § 100a Abs. 2 StPO zulässig ist (BT-Drs. 18/12785, S. 48 f.). Unter anderem wird die Verwirklichung solcher Mittel den direkten Weg zum Überwachungsstaat darstellen.

[195] Vgl. *Singelnstein/Derin*, NJW 2017, 2646, 2647; *Niedernhuber*, JA 3/2018, 169, 170: insb. Sprach- und Videotelefonie, Nachrichten in Form von E-Mails, SMS oder MMS und Kommunikationsinhalte (Nachrichten und Multimediadaten) über IP-basierte instant-Messaging-Dienste wie z. B. *WhatsApp, Facebook Messenger, Threema, Telegram, Google Talk* oder *Jabber.*

[196] *Niedernhuber*, JA 3/2018, 169, 170 f. Dabei ist keine Schutzwirkung des Art. 10 Abs. 1 GG mehr zu entfalten, stattdessen handelt es sich um das Allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. GG in der Ausprägung des Grundrechts auf informationelle Selbstbestimmung und des Computer-Grundrechts (zust. a. a. O. 171; auch *Roggan*, StV 2017, 821, 824).

TKÜ,[197] aber sie wird in technischer Hinsicht auf die gleiche Weise wie bei der Online-Durchsuchung nach § 100b StPO, d. h. durch die Infiltration in das Endgerät des Betroffenen, durchgeführt.[198] Deswegen war ihre Zulässigkeit vor der Gesetzesänderung von 2017 stark umstritten, d. h., ob sie aufgrund des § 100a Abs. 1 StPO a. F. (= § 100a Abs. 1 S. 1 StPO n. F.) überhaupt zulässig ist. Bei dieser Debatte handelt es sich auch um das Problem, ob ein heimliches Eindringen in lokale informationstechnische Systeme zur Installation des Staatstrojaners, der zur Durchführung der Quellen-TKÜ erforderlich ist, als „typische Begleitmaßnahme" der TKÜ von §§ 100a und b StPO a. F. zu erfassen ist.[199]

In den Rspr. von ein paar Instanzgerichten und in Teilen der Literatur wurde für eine Übergangszeit – bis zu einer gesetzlichen Regelung – die Auffassung vertreten, dass die Quellen-TKÜ gestützt auf §§ 100a und b StPO a. F. zulässig sei.[200] Hingegen wurde mehrheitlich in der Literatur aus Gründen der Voraussetzungen der Zulässigkeit der Quellen-TKÜ, die in der Entscheidung des *BVerfG* zur Online-Durchsuchung gefordert werden, dies zu Recht abgelehnt:[201] die Sicherstellung technischer Vorkehrungen und rechtlicher Vorgaben, um die Überwachung „ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang" zu beschränken.[202] Denn es ist nicht nur unklar, ob diese Begrenzung nach heutigem Stand der Technik überhaupt möglich ist,[203] sondern auch zweifelhaft, ob sie rechtlich sicherzustellen ist.[204] Daraus folgt, dass die verdeckte Infiltration in informationstechnische Systeme zur Durchführung der Quellen-TKÜ keine primäre Maßnahme bzw. keine Begleitmaßnahme der TKÜ darstellen kann. So ist sie ohne technische und rechtliche Si-

[197] BT-Drs. 18/12785, S. 50.

[198] Vgl. *Singelnstein/Derin*, NJW 2017, 2646, 2647: „*Technisch besehen ist auch die Quellen-TKÜ eine Online-Durchsuchung … Der Unterschied besteht alleine im Umfang der erhobenen Daten*"; auch *Roggan*, StV 2017, 821, 825.

[199] *Klesczewski*, ZStW 123 (2011), 737, 743 f.; *Kudlich*, GA 2011, 193, 206 f.: primäre Maßnahme; *Sieber*, 69. DJT 2012, C 104: Begleiteingriff; vgl. *Bruns*, KK-StPO, § 100a Rn. 46; *Singelnstein*, NStZ 2012, 593, 598 f.: Annexkompetenz zur Überwachungsanordnung; *Wolter/Greco*, SK-StPO, § 100a Rn. 28 f.

[200] *LG Hamburg* MMR 2011, 693; *LG Landshut* MMR 2011, 690; *AG Bayreuth* MMR 2010, 266; M-G/*Schmitt*, StPO, 60. Aufl. 2017, § 100a Rn. 7a f. Teilweise wird dies damit begründet, dass nach § 100b Abs. 2 S. 2 Nr. 2 StPO a. F. die Überwachung im Endgerät möglich ist und die TKÜ lediglich unter Mitwirkung des Dienstanbieters nicht durchzuführen ist (vgl. *Klesczewski*, ZStW 123 (2011), 737, 743 f.; *Wolter/Greco*, SK-StPO, 5. Aufl. 2016, § 100a Rn. 28 f.).

[201] *Gercke*, GA 2012, 474, 48; *Klesczewski*, ZStW 123 (2011), 737, 743 f.; *Kudlich*, GA 2011, 193, 205 ff.; StV 2012, 560, 565; *Roxin/Schünemann*, § 36 Rn. 3; *Sieber*, 69. DJT 2012, C 104 f.; *Singelnstein*, NStZ 2012, 593, 598 f.; *Vogel/Brodowski*, StV 2009, 632 ff.; *Wolter/Greco*, SK-StPO, § 100a Rn. 29 m. w. N.

[202] *BVerfGE* 120, 274, 309 [Rn. 190].

[203] *Roxin/Schünemann*, § 36 Rn. 3; *Singelnstein*, NStZ 2012, 593, 598: Die Erfahrung mit dem „bayerischen Staatstrojaner" vom Oktober 2011 hat gezeigt, dass die technischen Anforderungen des BVerfG praktisch nicht umsetzbar sind (auch *Sieber*, 69. DJT 2012, C 109).

[204] *Singelnstein*, NStZ 2012, 593, 598 f.

cherungen viel eingriffsintensiver als die TKÜ des Haupteingriffs.[205] Daher war es verfassungswidrig, wenn die Quellen-TKÜ vor der Gesetzesänderung in der Praxis – als Übergangsbonus – gestützt auf §§ 100a und b StPO a. F. praktiziert wurde.[206] Im Ergebnis ist zu ihrer Legitimierung eine spezielle gesetzliche Regelung erfordert, die mit ähnlichen technischen Schutzmaßnahmen wie eine Online-Durchsuchung ausgestattet ist, und zugleich eine technische Begutachtung.[207] Vor diesem Hintergrund hat der Gesetzgeber bei Einführung der Quellen-TKÜ in die StPO normative Vorgaben, um sie von der Online-Durchsuchung abzugrenzen und weiter das Verbot der Übertragung auf diese zu gewährleisten, vorgesehen (vgl. § 100a Abs. 5 StPO); vgl. zu dem Zweifel und der Kritik daran, oben 2. C. (2).

Die Zieldaten beider Maßnahmen werden durch die Wörter jeder Ermächtigung voneinander klar unterschieden. Während sich die Quellen-TKÜ an die laufende TK (Abs. 5 S. 1 Nr. 1 lit. a) oder an die Inhalte und Umstände der Kommunikation, die auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz hätten überwacht und aufgezeichnet werden können (lit. b), richtet, betrifft die Online-Durchsuchung die auf einem von dem Betroffenen genutzten informationstechnischen System bereits gespeicherten Daten (§ 100b Abs. 1 StPO). Daher macht die Quellen-TKÜ konkret die über Messenger-Dienste versandten und mittlerweile regelmäßig verschlüsselten „Kommunikationsinhalte" zum Gegenstand des Eingriffs, und diese – gespeicherten – Nachrichten dürfen erst ab dem Zeitpunkt der Anordnung durch das Gericht oder in Eilfällen durch den Staatsanwalt ausgeleitet werden, aber nicht erhoben werden, wenn sie nicht mehr als aktuelle Kommunikation gelten können.[208] Hingegen betrifft die Online-Durchsuchung alle auf dem Endgerät des Betroffenen gespeicherten Nachrichten ohne solche zeitlichen und inhaltlichen Begrenzungen.[209] Kann eine Trennung der Messenger-Nachrichten nach einzelnen Zeitpunkten aber technisch durch die zu verwendende Software nicht vorgenommen werden oder existiert eine solche Software (noch) nicht, ist die Maßnahme unzu-

---

[205] *Klesczewski*, ZStW 123 (2011), 737, 743 f.; *Sieber*, 69. DJT 2012, C 104; *Wolter/Greco*, SK-StPO, § 100a Rn. 29.

[206] Zust. *Klesczewski*, ZStW 123 (2011), 737, 743 f. und 754; auch *Roxin/Schünemann*, 29. Aufl. 2017, § 36 Rn. 3 a. E.: Erhebliche Fragwürdigkeit ihrer Rechtmäßigkeit; dazu *Wolter/Greco*, SK-StPO, 5. Aufl. 2016, § 100a Rn. 30: „*Dass insoweit die Strafverfolgung in einem wesentlichen Bereich vorübergehend punktuell durch Erhebungs- und Verwertungsverbote lahmgelegt wird, ist zumeist bis zur etwaigen Aufnahme angemessener gesetzgeberischer Bemühungen hinzunehmen.*"

[207] *Sieber*, 69. DJT 2012, C 105 f.

[208] BT-Drs. 18/12785, S. 50 f.; dazu *Niedernhuber*, JA 3/2018, 169, 171 f.: „*Der Zeitpunkt der Anordnung der Maßnahme bildet auch die zeitliche Grenze zwischen der Quellen-TKÜ und der Online-Durchsuchung.*" Entwürfe von Nachrichten, die noch nicht abgeschickt wurden, werden von der Maßnahme nicht erfasst (BT-Drs. a. a. O.; *Niedernhuber*, a. a. O.; *Singelnstein/Derin*, NJW 2017, 2646, 2648).

[209] BT-Drs. 18/12785, S. 50 a. E. Ältere Nachrichten, die vor Erlass des richterlichen Beschlusses versandt wurden, dürfen ausschließlich durch die Online-Durchsuchung auf der Grundlage des § 100b StPO erhoben werden (eine rückwirkende Erhebung, a. a. O. S. 52).

lässig;[210] sie hat zu unterbleiben.[211] Der Verstoß gegen die technischen Vorgaben wird zum Verwertungsverbot erhobener Daten führen.[212]

(2) Die Quellen-TKÜ zielt auf die Ergänzung herkömmlicher TKÜ ab, indem sie einer von den Kommunikationspartnern verschlüsselt geführten Kommunikation entgegenwirkt. Sie ist daher nach dem Verhältnismäßigkeitsgrundsatz im Verhältnis zur herkömmlichen TKÜ grundsätzlich nur subsidiär zulässig.[213] Dies manifestiert sich im Wortlaut des § 100a Abs. 1 S. 2 StPO (vgl. „wenn dies notwendig ist").[214] Außerdem lässt sich die Subsidiarität auch aus § 100a Abs. 1 S. 3 StPO ziehen (vgl. § 100a Abs. 5 S. 1 Nr. 1 lit. b StPO).[215] Jedoch wird die Quellen-TKÜ trotz alledem binnen kurzem angesichts derzeitiger Kommunikationsgewohnheiten als standardmäßige TKÜ-Methode gelten und dürfte die klassischen TKÜ-Maßnahmen quantitativ sogar überholen.[216] Nach heutigem Stand der Technik ist die Entschlüsselung entweder extrem zeitaufwendig oder sogar gänzlich ausgeschlossen.[217] Das legt auch die Gesetzesbegründung nahe.[218]

c) Postbeschlagnahme

§ 99 StPO ist – zusammen mit § 100a StPO – der grundlegendste Tatbestand für den Eingriff in das Fernmeldegeheimnis nach Art. 10 Abs. 1 GG.[219] §§ 99 f. StPO sind eine Sonderregelung der §§ 94, 98 StPO für allgemeine Beschlagnahme.[220] Der § 99 StPO stellt „im Verhältnis zum § 94 StPO" die spezielle Gefahr des Übertragungsvorgangs von Postsendungen und Telegrammen, nämlich die Verletzlichkeit, in Rechnung. Er kann sich daher bei seiner Anwendung nicht mit dem § 94 StPO

---

[210] BT-Drs. 18/12785, S. 52 & 53; M-G/*Schmitt*, StPO, § 100a Rn. 14i.

[211] M-G/*Schmitt*, StPO, § 100a Rn. 14j.

[212] Zust. M-G/*Schmitt*, StPO, § 100a Rn. 35a.

[213] BT-Drs. 18/12785, S. 51; *Roggan*, StV 2017, 821, 822; *Singelnstein*/*Derin*, NJW 2017, 2646, 2648: wegen ihres durch die Infiltration gesteigerten Eingriffscharakters gegenüber der einfachen TKÜ.

[214] Abw. *Roggan*, StV 2017, 821, 822.

[215] BT-Drs. 18/12785, S. 51; auch *Roggan*, StV 2017, 821, 822 a. E.

[216] *Roggan*, StV 2017, 821, 822 a. E.

[217] BT-Drs. 18/12785, S. 46 a. E. und 48; auch *Roggan*, StV 2017, 821, 822.

[218] Vgl. BT-Drs. 18/12785, S. 48: „*Nachdem inzwischen ein Großteil der Kommunikation IP-basiert erfolgt und zahlreiche VoIP- und Messenger-Dienste die Kommunikationsinhalte mit einer Verschlüsselung versehen, werden den Ermittlungsbehörden bei der Überwachung und Aufzeichnung im öffentlichen Telekommunikationsnetz oft nur verschlüsselte Daten geliefert.*"

[219] Der ursprüngliche Rahmen und Inhalt der §§ 99 f. StPO (Gesetz, betreffend Änderungen des Gerichtsverfassungsgesetzes und der StPO vom 17. 5. 1898) wird bis heute ohne wesentliche Änderungen beibehalten. Der § 100a StPO (vom 13. 8. 1968: BGBl. I S. 949), der zum Zeitpunkt seiner Gründung auf die Überwachung von Fernmeldeverkehr, insb. von Telefonen abzielte, wurde seitdem mit der Entwicklung der TK-Technologie mehrmals überarbeitet und im Detail ausdifferenziert.

[220] *Park*, § 3 Rn. 684; *Roxin*/*Schünemann*, § 34 Rn. 31.

überschneiden[221] und die Beschlagnahme nach der Vorschrift ist nur zum Zwecke der Gewinnung der Beweisgegenstände i. S. d. § 94 StPO zulässig.[222] Nach h. M. wird der Begriff der „Postsendungen" nach § 4 Nr. 5 i. V. m. Nr. 1 PostG definiert und der Begriff der „Telegramme" im Zusammenhang mit der TK nach § 3 Nr. 22 TKG beschränkend ausgelegt.[223] Daher sind nur traditionelle, verkörperte Nachrichten unter §§ 99 f. StPO zu subsumieren, dagegen elektronische wie E-Mail nicht;[224] vgl. dazu eingehend unten C. III. 1.

Die Eingriffsintensität der Beschlagnahme gemäß § 99 StPO ist zwar einerseits wegen des Eingriffs in das Fernmeldegeheimnis schwerwiegend, aber sie ist andererseits etwas geringer als bei der TKÜ gemäß § 100a StPO, weil hierbei die Informationen nicht durch automatische Datenverarbeitung erhoben werden und so eine Gefährdung der Persönlichkeitsverletzung durch die umfassende Datenbeschaffung wie bei elektronischen Daten kaum besteht.[225] Daher enthalten die Eingriffsvoraussetzungen des § 99 StPO – wie diejenigen des § 94 StPO, aber anders als diejenigen des § 100a StPO – weder die Eingrenzung nach der Schwere der Straftat und der Stärke des Verdachts noch die Subsidiaritätsklausel. Hingegen ist seine verfahrensrechtliche Kontrolle strenger als die der einfachen Beschlagnahme gemäß § 98 StPO; z. B. durch den Ausschluss polizeilicher Eilkompetenz bei Gefahr im Verzug (§ 100 Abs. 1 StPO), das Außerkrafttreten der Eilanordnungen ohne gerichtliche Bestätigung (Abs. 2) und die grundsätzliche Zuweisung der Zuständigkeit der Öffnung der Postsendungen an das Gericht (Abs. 3).

4. Erhebung von Verkehrs- und Standortdaten

(1) Die Ermächtigung zur Erhebung und Verwendung der Verkehrs- und Standortdaten zum Zwecke der Strafverfolgung ist in zwei Arten unterteilt, je nachdem, ob die Maßnahme auf künftige Daten bzw. Echtzeitdaten oder auf (vorsorglich anlasslose) gespeicherte Daten abzielt (§ 100g Abs. 1 und Abs. 2 StPO). Der Grund dieser differenzierten Regelung liegt darin, dass sich das *BVerfG* im Jahre 2010 dafür ausgesprochen hat, dass die Speicherung und Verwendung von vorsorglich flächendeckend und langfristig gespeicherten Verkehrs- und Standortdaten – insb. hinsichtlich der Datensicherheit, des Umfangs der Datenverwendung, der Transparenz und des Rechtsschutzes – strengeren Voraussetzungen und Verfahrensgarantien unterliegen muss als dieselbe von solchen Daten in Zukunft bzw. in Echt-

[221] *BVerfGE* 124, 43, 60 [Rn. 58]: auch § 100a; *BGH* NJW 2009, 1828.

[222] M-G/*Schmitt*, StPO, § 99 Rn. 1; *Wohlers*/*Greco*, SK-StPO, § 99 Rn. 1.

[223] *Greven*, KK-StPO, § 99 Rn. 7; M-G/*Schmitt*, StPO, § 99 Rn. 5; abw. *Wohlers*/*Greco*, SK-StPO, § 99 Rn. 12.

[224] *Greven*, KK-StPO, § 99 Rn. 7; M-G/*Schmitt*, StPO, § 99 Rn. 5; *Neuhöfer*, JR 2015, 21, 26; a. A. *LG Ravensburg* MMR 2003, 679: in analoger Anwendung der §§ 94, 98, 99 StPO; *Bär*, MMR 2003, 679, 681: auch eine direkte Anwendung des § 99 StPO möglich.

[225] M-G/*Schmitt*, StPO, § 99 Rn. 14; *Roxin*/*Schünemann*, § 34 Rn. 31.

zeit.[226] Aus diesem Grund sind die Eingriffsvoraussetzungen und verfahrensrechtlichen Vorkehrungen der ersteren Maßnahme so streng ausgestaltet, dass sie fast vergleichbar mit Online-Durchsuchung und Wohnraumüberwachung sind, hingegen sind dieselben der Letzteren parallel zu der TKÜ (vgl. §§ 100g, 101a und b StPO). Auf jeden Fall liegt der Grund, warum der Zugriff auf Verkehrs- und Standortdaten, aber nicht auf Inhaltsdaten, so streng kontrolliert wird, – wie das *BVerfG* bereits in seiner Rspr. ausgeführt hat – darin, dass die Aussagekraft der Verkehrsdaten, die langfristig umfangreich und kumulativ gespeicherten werden, unter den modernen informationstechnischen Gegebenheiten weitreichend ist.[227]

(2) Die Erhebung der künftig anfallenden Verkehrsdaten oder in Echtzeit darf im Rahmen ihrer Eingriffsvoraussetzungen für die Straftaten von auch im Einzelfall erheblicher Bedeutung, insb. für die in § 100a Abs. 2 S. 2 StPO katalogisierten Straftaten („schwere Straftaten") oder mittels TK begangene Straftaten angeordnet werden (§ 100g Abs. 1 S. 1 StPO i. V. m. § 96 Abs. 1 TKG). Die Verkehrsdaten des § 96 Abs. TKG dürfen zu geschäftlichen Zwecken soweit erforderlich von Dienstanbietern gespeichert werden, die keine gesetzliche Verpflichtung zu einer solchen Speicherung haben. Da es somit hierbei keine obligatorische Speicherungsfrist gibt und die Abrufbarkeit dieser Daten von den technischen und geschäftlichen Zwecken jedes Anbieters abhängig ist, ist ihre Verwendung vom Standpunkt der Ermittlungsbehörde nicht sicher.[228] Im Rahmen der Verfahrenskontrollen gilt zwar zuerst qualifizierter Richtervorbehalt, jedoch ist die Eilkompetenz der StA bei Gefahr im Verzug zulässig (vgl. *argumentum e contrario* aus § 101a Abs. 1 S. 2 i. V. m. § 100e Abs. 1 S. 2 StPO). Außerdem sind in der gerichtlichen Entscheidungsformel die Personalien des Betroffenen, der Tatvorwurf, die Art der Maßnahme und die Art und der Zeitraum der zu übermittelnden Verkehrsdaten sowie ihre Bedeutung anzugeben (§ 101a Abs. 1 S. 1 Nr. 1 i. V. m. § 100e Abs. 3 S. 2 StPO), in der Begründung der Anordnung sind die bestimmten Tatsachen, die den Verdacht begründen, und die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme zu nennen (§ 101a Abs. 1 S. 1 i. V. m. § 100e Abs. 4).[229] Hierzu kommt, dass die Ermittlungsbehörde das anordnende Gericht nach Erhalt der Daten über dessen „Ergebnisse" unterrichten muss (§ 101a Abs. 1 S. 1 i. V. m. § 100e Abs. 5 StPO). Die (nachträgliche) Benachrichtigung und die Gewährleistung eines effektiven Rechtsschutzes wird – nicht von § 101 StPO, sondern – von § 101a Abs. 6 StPO abgetrennt geregelt. Ursprünglich waren diese Regelungen auch in § 101 StPO a. F. (§ 101 Abs. 4 S. 1 Nr. 6 in der vom 1. 1. 2008 bis zum 17. 12. 2015 geltenden Fassung) enthalten, wurden jedoch in der Revision vom Dezember 2015 von der Vorschrift gestrichen. Nach § 101a Abs. 6 StPO gelten aber für die Erhebung der Verkehrs- und

[226] *BVerfGE* 125, 260, 325 ff. [Rn. 220 ff.].

[227] *BVerfGE* 125, 260, 319 f. [Rn. 211 f.]. Außerdem können solche Verkehrsdaten im Zusammenspiel mit anderen vorhandenen Dateien zur Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger führen (a. a. O. 324 [Rn. 218]).

[228] Vgl. *Bruns*, KK-StPO, § 100g Rn. 4.

[229] Vgl. M-G/*Schmitt*, StPO, § 101a Rn. 9, 11 und 13.

Standortdaten die Regelungen für die Benachrichtigung und den Rechtsschutz im § 101 Abs. 4 – 7 StPO umfassend entsprechend. Hierbei ist allerdings für das Unterbleiben und die Zurückstellung der Benachrichtigung nach § 101 Abs. 4 S. 3 und Abs. 6 S. 1 StPO das Gericht stets zuständig. Insofern wird der von dieser Maßnahme Betroffene stärker geschützt als ein von der Wohnraumüberwachung oder Online-Durchsuchung Betroffener. Angesichts des Schutzniveaus, das der Eingriffsintensität entsprechen muss, kann dies jedoch aus Sicht der Ermittlungsbehörde infrage gestellt werden. Hierfür werden schließlich auch der Bericht an das Bundesamt für Justiz und den Deutschen Bundestag und die Veröffentlichung der Übersicht im Internet verlangt (§ 101b Abs. 1 und 5 StPO).

Die VDS, die zur Strafverfolgung die Verwendung der Daten über die Umstände des Kommunikationsvorgangs, die vorsorglich anlasslos und umfassend langfristig (für zehn Wochen, aber für vier Wochen bei Standortdaten; vgl. § 113b Abs. 1 TKG) gespeichert sind, ermöglicht, ist mit strengeren Eingriffsvoraussetzungen und verfahrensrechtlichen Sicherungen ausgestattet als bei der obigen Erhebung der Verkehrsdaten in Zukunft oder in Echtzeit (vgl. §§ 100g Abs. 2, 101a, b StPO und §§ 113a – g TKG). Die Maßnahme darf nur für einen begrenzteren Straftatenkatalog („besonders schwere Straftaten“) angeordnet werden (§ 100g Abs. 2 S. 2 StPO), dessen Bereich gegenüber der Online-Durchsuchung und der akustischen Wohnraumüberwachung weiter ist. Für ihre Verfahrensgarantien gibt es neben den Vorkehrungen gegen die Erhebung in Zukunft oder in Echtzeit zusätzliche Kontrollen. Die TK-Dienstanbieter sind zuerst verpflichtet, die bestimmten Verkehrsdaten zu speichern und sie an die Strafverfolgungsbehörde auf deren Verlangen im Einzelfall zu übermitteln (§§ 113a – c TKG), und sie haben dafür einen besonders hohen Sicherheitsstandard zu gewährleisten (vgl. §§ 113d – g TKG).[230] Des Weiteren unterliegt die Verwendung der gespeicherten Verkehrsdaten zur Strafverfolgung stets dem Richtervorbehalt; so ist die staatsanwaltliche Eilanordnung aufgrund von Gefahr im Verzug nicht zulässig (ein „absoluter“ Richtervorbehalt;[231] § 101a Abs. 1 S. 2 StPO). Die Verkehrsdaten des § 113b TKG sind nämlich bereits bei Anbietern gespeichert, sodass die Eilkompetenz nicht eingeräumt werden kann. Bei der Erhebung von Verkehrsdaten nach § 100g Abs. 2 StPO ist das Absehen von Daten im Besitz von Zeugnisverweigerungsberechtigten streng zu kontrollieren (§ 100g Abs. 4 StPO) und die Verwendung der erhobenen Daten in anderen Strafverfahren oder ihre Übermittlung zu Zwecken der Gefahrenabwehr ist nur unter strengen Bedingungen zulässig (§ 101a Abs. 4 StPO).

(3) Die Standortdaten eines Mobiltelefons, die zu den Verkehrsdaten gehören (§ 96 Abs. 1 Nr. 1 TKG) und die Ermittlung des Aufenthaltsorts eines Beschuldigten in der Vergangenheit (z. B. zur Tatzeit) oder die Bestimmung des aktuellen Standorts ermöglichen, sind auch unter den Voraussetzungen des § 100g Abs. 1 und Abs. 2 StPO zu erheben (§ 100g Abs. 1 S. 3, 4 StPO). Indem die Daten die Erstellung von

[230] Vgl. *BVerfGE* 125, 260, 325 – 327 [Rn. 221 – 225].

[231] M-G/*Schmitt*, StPO, § 101a Rn. 6.

Bewegungsprofilen des Betroffenen ermöglichen, sind sie besonders sensible Daten und daher wird ihre Erhebung streng beschränkt.[232] Zuerst ist die Erhebung von Standortdaten nach Abs. 1 S. 4 im Fall des Abs. 1 S. 1 Nr. 1 – abgesehen von Nr. 2 – nur für künftig anfallende Verkehrsdaten oder in Echtzeit zulässig. Das heißt, diese Vorschrift regelt nicht gespeicherte Standortdaten (in Echtzeit), die eine (Echtzeit-) Lokalisierung des Beschuldigten ermöglichen; dies ist u. a. beim sog. „IP-Catching" praktisch relevant.[233] Darüber hinaus können durch diese Vorschrift auch die Standortdaten eines eingeschalteten, aber nicht genutzten Mobiltelefons, nämlich „Standortdaten im Stand-by-Betrieb", in Echtzeit erhoben werden und eine solche ständige Ortung ermöglicht eine Erstellung eines aktuellen Bewegungsbildes des Betroffenen, nämlich Observationsmaßnahmen.[234] Nach § 100g Abs. 1 S. 3 StPO, der durch das Gesetz vom 20. 11. 2019 neu eingefügt wurde,[235] ist die Erhebung gespeicherter (retrograder) Standortdaten andererseits nur unter den Voraussetzungen des Abs. 2 zulässig. Damit wurden die insoweit bestehende Regelungslücke beseitigt.[236]

(4) § 100g Abs. 3 StPO sieht zum anderen die sog. Funkzellenabfrage vor, die als die Erhebung aller – zu einer bestimmten Zeit – in einer bestimmten Funkzelle angefallenen Verkehrsdaten definiert wird. Ist eine Zielperson oder ihre Nummer oder sonstige Kennung noch nicht bekannt, dann ist diese Ermittlungsmethode zu nutzen, um sie zu bestimmen. Daher wird diese Maßnahme üblicherweise im Frühstadium einer Untersuchung verwendet, und sie zielt nicht auf die Erhebung der Standortdaten eines bestimmten Beschuldigten ab. Durch die Maßnahme können die Verkehrsdaten aller Mobilfunkendgeräte, die zu einer bestimmten Zeit in einer bestimmten Funkzelle aktiv eingeschaltet sind, erfasst werden und daher wird dann in unvermeidbarer Weise eine Vielzahl von Personen betroffen.[237] Bis zur Gesetzesänderung von 2015 (vgl. siehe Kapitel 1, Fn. 27) hat sie sich auf § 100g Abs. 2 S. 2 StPO a. F. gestützt,[238] jedoch hat der Gesetzgeber durch die Änderung ihre Rechtsgrundlage festgelegt: § 100g Abs. 3 StPO. Dabei wurden nach dem Sinn der BVerfG-Entscheidung von 2010 die nach § 96 Abs. 1 TKG zu geschäftlichen Zwecken ge-

[232] *Bruns*, KK-StPO, § 100i Rn. 1; M-G/*Schmitt*, StPO, § 100g Rn. 21.

[233] M-G/*Schmitt*, StPO, § 100g Rn. 21a.

[234] M-G/*Schmitt*, StPO, § 100g Rn. 9. Der Einsatz „stiller SMS" zur Erzeugung von Standortdaten im betriebsbereiten Standby-Modus ist nach der jüngsten Rspr. des *BGH* unter den Voraussetzungen des § 100i Abs. 1 Nr. 2 zulässig (vgl. unten 6. b)).

[235] Art. 1 Nr. 5 Gesetz zur Umsetzung der RL (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die VO (EU) 2016/679 vom 20. November 2019 (BGBl. I S. 1724).

[236] M-G/*Schmitt*, StPO, § 100g Rn. 21b; vgl. BT-Drs. 19/4671, S. 61.

[237] BT-Drs. 16/5846, S. 55; *Bruns*, KK-StPO, § 100g Rn. 11; M-G/*Schmitt*, StPO, § 100g Rn. 36.

[238] BT-Drs. 16/5846, S. 83; vgl. § 100g Abs. 2 S. 2 a. F.: … genügt im Falle einer Straftat von erheblicher Bedeutung eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der TK, wenn … die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre.

speicherten Verkehrs- und Standortdaten sowie die nach § 113b TKG obligatorisch auf Vorrat zu speichernden differenziert und die Voraussetzungen der Maßnahme strenger ausgestaltet. Diese Maßnahme muss deswegen unter den Voraussetzungen des § 100g Abs. 1 S. 1 Nr. 1 StPO in einem angemessenen Verhältnis zur Bedeutung der Sache stehen und unterliegt verstärkter Subsidiarität („soweit die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre"), weil sie sich auf eine Vielzahl von unverdächtigen Dritten bezieht.[239]

5. Auskunft über Bestandsdaten und Zugangssicherungscodes

a) Bestandsdatenauskunft

Die Erhebung und Verwendung der Bestandsdaten (§ 95 StPO i. V. m. § 3 Nr. 3 und § 111 Abs. 1 S. 1 TKG) sollte zuerst anders gehandhabt werden als dieselbe der Inhalts- und Verkehrsdaten.[240] Weil ein solcher Eingriff eine Verwendung der Identifizierungsdaten darstellt, kann seine Intensität nicht als geringfügig angesehen werden, jedoch ist sie deswegen keineswegs schwer, weil die Daten nur eine beschränkte Aussagekraft haben.[241] Daher kann er – obwohl er in aller Regel heimlich erfolgt – wesentlich von den Ermittlungsgeneralklauseln der §§ 161 Abs. 1, 163 Abs. 1 StPO erfasst werden.[242] Dass dennoch diese Auskunft mit eigenständiger Ermächtigungsgrundlage (vgl. § 100j Abs. 1 S. 1 StPO) geregelt wird, ist darauf zurückzuführen, dass das *BVerfG* in seiner Entscheidung von 2012 nach den Anforderungen der Normenklarheit das sog. „Doppelungsmodell" verlangt hat.[243] Demnach müssen die „Datenübermittlung" seitens der auskunftserteilenden Stelle und der „Datenabruf" seitens der auskunftssuchenden Stelle jeweils selbstständig geregelt werden, daher ist dafür neben einer Norm zur Datenübermittlung („erste Tür"; § 95 Abs. 1 S. 3 und § 111 Abs. 1 S. 1 TKG) eine Norm für den Datenabruf („zweite Tür"; § 100j Abs. 1 S. 1 StPO) separat erforderlich. Da die Erteilung und

[239] Vgl. M-G/*Schmitt*, StPO, § 100g Rn. 37 f.

[240] Da sich die Daten keinesfalls auf TK beziehen, werden sie nicht durch das Telekommunikationsgeheimnis, sondern durch das Recht auf informationelle Selbstbestimmung geschützt (*BVerfGE* 130, 151, 178 f. und 183). Soweit die Datenauskunft aufgrund zu einem bestimmten Zeitpunkt zugeordneter, dynamischer IP-Adressen erteilt wird (vgl. § 100j Abs. 2 StPO), begründet sie aber einen Eingriff in Art. 10 Abs. 1 GG (a. a. O. 181 f. [Rn. 116 ff.]).

[241] *BVerfGE* 130, 151, 188 ff. und 196 f.

[242] Vgl. *BVerfGE* 130, 151, 209 [Rn. 185]. In der modernen Informationsgesellschaft, in der die Nutzung verschiedener TK-Dienste vorherrscht, kann die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten gewöhnlich, insb. im Cyberspace, nur mit dem Erwerb dieser grundlegenden Personendaten beginnen, die die Anbieter bereits für geschäftliche Zwecke besitzen. In dieser Hinsicht spielt die Bestandsdatenauskunft in der Praxis zu Beginn der Ermittlung eine wichtige Rolle (*Bär*, MMR 2013, 700, 700 f.; *Greco*, SK-StPO, § 100j Rn. 1).

[243] *BVerfGE* 130, 151, 184 [Rn. 123]; vgl. *Bär*, MMR 2013, 700; *Bruns*, KK-StPO, § 100j Rn. 1; *Dalby*, CR 2013, 361, 362 ff.

Verwendung der Bestandsdaten aufgrund der Identifizierung von dynamischen IP-Adressen in das Telekommunikationsgeheimnis eingreift, bedarf es hierbei auch einer eigenen Norm zur Identifizierung (vgl. § 100j Abs. 2).[244]

Für die Bestandsdatenauskunft fehlt es aus diesem Grund nicht nur an Eingriffsschwellen nach der Schwere der Straftat und der Stärke des Tatverdachts und an einer Subsidiaritätsklausel (§ 100j Abs. 1 S. 1 StPO),[245] sondern auch an verfahrensrechtlichen Sicherungen wie z. B. Richtervorbehalt und Benachrichtigung (vgl. *argumentum e contrario* aus § 100j Abs. 3 und 4 StPO).[246] Soweit beim Bestehen eines Anfangsverdachts für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten die Rufnummern und andere Anschlusskennungen, der Namen und die Anschrift des Anschlussinhabers, die statische IP-Adresse, IMEI, IMSI etc. erforderlich sind, dürfen somit die Strafverfolgungsbehörden – ohne Wissen des Betroffenen und ohne Anordnung des Gerichts – von den Dienstanbietern die Auskünfte verlangen,[247] und damit kann die Ermittlung eingeleitet werden. Da die Beauskunftung durch die Identifizierung der dynamischen IP-Adressen in das Telekommunikationsgeheimnis eingreift, ist sie i. d. R. zu benachrichtigen (§ 100j Abs. 4 S. 1 StPO). Soweit sich aber die erhobenen Bestandsdaten auf nicht beschuldigte Dritte beziehen,[248] gibt es angesichts der geringen Eingriffsintensität der Maßnahme in der Benachrichtigung darüber keine schutzwürdigen Belange (Abs. 4 S. 3; vgl.: Dies ist parallel zu der Regelung des § 101 Abs. 4 S. 4 – 5 StPO).

b) Beschaffung der Zugangssicherungscodes

(1) Zum anderen ist die Erhebung und Verwendung der Zugangssicherungscodes zur Strafverfolgung, die dem Schutz vor unbefugtem Zugriff auf Endgeräte oder (externe) Speichereinrichtungen dienen, anders zu behandeln (§ 100j Abs. 1 S. 2 StPO i. V. m. § 113 Abs. 1 S. 2 TKG). Mittels dieser Daten können die Ermittlungsbehörden nicht nur die Daten, die in den privaten Endgeräten oder Speichereinrichtungen (z. B. PCs, Smartphones oder Festplatten) oder in hiervon räumlich getrennt eingesetzten Speichermedien, d. h. auf Speicherräumen im Internet oder

[244] *BVerfGE* 130, 151, 204 f. [Rn. 172 – 174] und dazu 181 [Rn. 116]: Auf der Grundlage von § 113 Abs. 1 S. 1 TKG a. F. dürfte auch die Identifizierung der Bestandsdaten von dynamischen IP-Adressen deswegen nicht erfolgen, weil dafür die Anbieter in einem Zwischenschritt zur Sichtung der Verbindungsdaten ihrer Kunden auf konkrete Telekommunikationsvorgänge zugreifen müssen.

[245] Für den Erwerb des Bestandsdaten durch eine Identifizierung dynamischer IP-Adressen (Abs. 2) gibt es auch keine Subsidiaritätsregelung, angesichts deren ohnehin beschränkten Werts ist dies jedoch kaum zu beanstanden (*Greco*, SK-StPO, § 100j Rn. 6).

[246] M-G/*Schmitt*, StPO, § 100j Rn. 5 a. E.

[247] M-G/*Schmitt*, StPO, § 100j Rn. 2; *Greco*, SK-StPO, § 100j Rn. 14.

[248] Abw. *Greco*, SK-StPO, § 100j Rn. 7: Nach § 100j StPO ist es nicht gestattet, Daten Dritter einzuholen, auch wenn er unvermeidbar betroffen ist (*argumentum e contrario* aus §§ 100a Abs. 3, 100b Abs. 3, 100c Abs. 2, 100f Abs. 2, 100h Abs. 3, 100i Abs. 2 StPO).

anderen Netzwerken (z. B. E-Mail- oder SNS-Server oder Cloud-Speicher), gespeichert sind, erfassen,[249] sondern auch die Daten aus einem laufenden Telekommunikationsvorgang.[250] Die Nutzung dieser Daten gehört für eine effektive Strafverfolgung zu einem staatlichen legitimen Interesse,[251] heutzutage ist aber die Entschlüsselung digitaler Kryptographie oft unmöglich oder erfordert einen erheblichen zeitlichen und finanziellen Aufwand[252], und die zugangsgeschützten Daten können meist nur mithilfe derjenigen Personen, die über die entsprechenden Zugangscodes verfügen, wie z. B. ISPs oder Unternehmen, zugänglich gemacht werden.[253] Die Ermittlungsbehörden dürfen daher von den Dienstanbietern Auskunft über die Sicherungscodes verlangen.[254] Vor der Neuregelung konnten sie auf der Grundlage von §§ 161 Abs. 1, 163 Abs. 1 StPO nach § 113 Abs. 1 S. 2 TKG a. F. erhoben werden.[255] Jedoch erfolgt die Erlangung dieser Codes, die unter der modernen Informationstechnik eine weitreichende Beschlagnahme personenbezogener Daten ermöglichen, nicht nur zumeist heimlich,[256] sondern sie kann auch sehr viel brisanter sein als eine einzelne Datenerhebung.[257] Sie muss nicht nur mit einem Richtervorbehalt notwendig verbunden sein, sondern es sind auch sie rechtfertigende Sonderregeln erforderlich. Insofern bedarf es insb. nach der Rspr. des *BVerfG* für die Erhebung der Zugangscodes aus dem Verhältnismäßigkeitsgrundsatz – neben den Normen für Datenherausgabe und -abruf – weiteren Voraussetzungen für die

[249] *Bruns*, KK-StPO, § 100j Rn. 3; M-G/*Schmitt*, StPO, § 100j Rn. 3.

[250] *BVerfGE* 130, 151, 208 [Rn. 184].

[251] *BVerfGE* 130, 151, 208 [Rn. 183].

[252] Die Ermittlungsbehörden können die Codes mit ihren eigenen technischen Mitteln entschlüsseln (unmittelbarer Zwang; vgl. Kapitel 4, C. III. 2. a) cc)).

[253] *Sieber*, 69. DJT 2012, C 119; *Bäumerlich*, NJW 2017, 2718 [Tz. II.]; auch M-G/*Schmitt*, StPO, § 95 Rn. 3a. Die Schlüssel sind aus Sicherheitsgründen ggf. ausschließlich dem Betroffenen bekannt (*Sieber*, a. a. O. C 120). In letzter Zeit werden Biometriescanner – etwa durch Fingerabdruck- und Irisscanner – bei den Smartphones zusätzlich eingesetzt (*Bäumerlich*, a. a. O. 2718 f.).

[254] Die erstrebten Gegenstände sind jedoch keine Sicherungscodes selbst, sondern die durch diese gesicherten Daten. Also sollte im Grunde eine „Verpflichtung bzw. Anordnung zur unverschlüsselten Herausgabe von Daten" nach §§ 95, 98 Abs. 1 StPO in Rechnung gestellt werden (vgl. Kapitel 4, B. III. 4.).

[255] *Bruns*, KK-StPO, § 100j Rn. 3; *Dalby*, CR 2013, 361, 364.

[256] Abw. *Dalby*, CR 2013, 361, 366: notwendigerweise heimlich. Die „heimliche" Erhebung der Zugangssicherungscodes ist nur zum Zweck der „heimlichen" Ermittlungsmaßnahmen wie etwa TKÜ (§ 100a StPO) oder Online-Durchsuchung (§ 100b StPO) möglich (vgl. *Zimmermann*, JA 5/2014, 321, 325). Daher dürfen die Gerichte oder die Ermittlungsbehörden bei der Durchsuchung nach §§ 103, 105 StPO den Anbietern oder Unternehmen nicht anordnen, die Codes „im Voraus/präventiv" vorzulegen, um sich auf ein Scheitern ihrer Erfassung vorzubereiten. Dies macht nämlich tatsächlich die heimliche Erhebung der Daten möglich.

[257] *Sieber*, 69. DJT 2012, C 121: Unter moderner Informationstechnik ist der Zugangscode ein wirkungsmächtiges Datenwerkzeug.

„Nutzung der erfassten Daten“ als „dritte Tür“ (vgl. § 100j Abs. 1 S. 2).[258] So ist die Erhebung und Verwendung der Codes an jeweilige gesetzliche Eingriffsbedingungen für die Nutzung der durch sie geschützten Daten geknüpft.[259] Soll ihre Nutzung etwa die Überwachung eines noch nicht abgeschlossenen Telekommunikationsvorgangs ermöglichen (vgl. heimliche Maßnahme), dann setzt dies die Einhaltung der strengen materiellen Anforderungen des § 100a StPO voraus; soll man jedoch mit den Codes auf beschlagnahmten Mobiltelefonen oder PCs abgelegte Daten einsehen bzw. diese auslesen (vgl. offene Maßnahme), dann können geringere Eingriffsschwellen ausreichen (vgl. §§ 94, 98 StPO).[260]

(2) Das Verlangen der Zugangssicherungscodes darf nur auf Antrag der StA durch das Gericht angeordnet werden (§ 100j Abs. 3 S. 1 StPO), und bei Gefahr im Verzug kann die Anordnung ausnahmsweise auch durch die StA oder ihre Ermittlungspersonen getroffen werden (S. 2). In diesem Fall ist jedoch die gerichtliche Entscheidung unverzüglich nachzuholen (S. 3). Wollen die Ermittlungsbehörden daher mittels der Codes etwa die allgemeine Beschlagnahme und Durchsuchung nach §§ 94 ff., 102 ff. StPO, die TKÜ nach § 100a StPO oder die Online-Durchsuchung nach § 100b StPO durchführen, so bedarf es eines „doppelten Richtervorbehalts“.[261] Diese gesetzliche Ausgestaltung bezüglich des Richtervorbehalts erscheint aber nicht angemessen. Denn sie ist inhaltlich parallel zu dem einfachen Richtervorbehalt (vgl. §§ 98 Abs. 1, 105 Abs. 1 StPO). Wenn die Ermittlungsbehörden zur Vorbereitung auf eine heimliche Maßnahme wie etwa die TKÜ oder die Online-Durchsuchung, bei denen die Eilkompetenz von StA bzw. Polizei ausgeschlossen ist, die Zugangscodes verlangen, so können die verhältnismäßigen gesetzlichen Ausgestaltungen des Richtervorbehalts und der Eilkompetenz in jeder Vorschrift umgangen werden (vgl. § 100e Abs. 1 – 2 StPO). Dies gilt auch für die Verfahrenskontrollen des § 100e Abs. 3 – 4 StPO. Unter anderem vor dem Hintergrund, dass ein Zugriff auf diese Codes zu einem schweren Eingriff in die Geheim- bzw. Intimsphäre des Betroffenen oder die Integrität des informationstechnischen Systems führen kann,[262] sind die momentanen Regelungen nicht zureichend. Zudem besteht das Risiko, dass die Ermittlungsbehörde, die die Codes bereits erhalten hat, die Einhaltung des Verfahrens für die Maßnahmen, bei denen ein qualifizierter Richtervorbehalt verlangt wird, vernachlässigen.

Zum anderen kann gemäß Abs. 3 S. 4 StPO die Anwendung der S. 1 – 3 ausnahmsweise ausgeschlossen werden (S. 4), wenn der Betroffene vom Auskunfts-

[258] *BVerfGE* 130, 151, 208 f. [Rn. 183 – 185]; *Bruns*, KK-StPO, § 100j Rn. 3a; *Dalby*, CR 2013, 361, 364; *Greco*, SK-StPO, § 100j Rn. 10 und dazu Rn. 9: Die Vorschriften stellen einen Rechtfertigungsgrund für das Ausspähen von Daten (§ 202a StGB) dar.

[259] M-G/*Schmitt*, StPO, § 100j Rn. 3; vgl. *Sieber*, 69. DJT 2012, C 122: Dabei wird auch eine Subsidiarität als materielle Voraussetzung verlangt.

[260] *BVerfGE* 130, 151, 208 f.; *Bruns*, KK-StPO, § 100j Rn. 3a; M-G/*Schmitt*, StPO, § 100j Rn. 3.

[261] *Dalby*, CR 2013, 361, 366.

[262] *Sieber*, 69. DJT 2012, C 120 f.

verlangen bereits Kenntnis hat oder haben muss (1. Alt.) oder wenn die Nutzung der Daten bereits durch eine gerichtliche Entscheidung gestattet wird (2. Alt.). Das Vorliegen solcher Voraussetzungen ist aktenkundig zu machen (S. 5). In diesen Fällen bedarf es nämlich keines eigenständigen richterlichen Beschlusses für das Verlangen der Auskunft über die Codes. Jedoch ist die 1. Alt. ziemlich und auch die 2. teilweise fragwürdig.[263]

Zuerst ist zweifelhaft, ob die 1. Alt. zu rechtfertigen ist. Nach den Gesetzesmaterialien ist dies dann der Fall, wenn der Betroffene in die Nutzung der Zugangssicherungscodes ausdrücklich eingewilligt hat oder er mit ihr rechnen muss; dazu gehören z. B. die Fälle, wenn das entsprechende Endgerät – nach §§ 94 Abs. 2, 98 Abs. 1 StPO – bei ihm beschlagnahmt wurde oder ein Auskunftsverlangen unter Hinweis auf die Möglichkeit der Abfrage beim Provider zuvor an ihn persönlich gerichtet wurde.[264] Bei der Erhebung und Nutzung der Zugangssicherungscodes, die – bei ihrem etwaigen Missbrauch – sogar die TKÜ oder Online-Durchsuchung ermöglichen, ist es aber nicht angebracht, dass der Richtervorbehalt nur deswegen schlichtweg ausgeschlossen wird, weil sie unter der bloßen Wahrnehmung oder Vorhersage des Beschuldigten erfolgt.[265] Auch wenn Endgeräte vom Beschuldigten nach den allgemeinen Beschlagnahme- und Durchsuchungsvorschriften sichergestellt wurden oder wenn er sie freiwillig herausgegeben hat, kann nicht davon ausgegangen werden, dass er freiwillig auch die Zugangssicherungscodes i. S. d. § 100j Abs. 1 S. 2 StPO mitgeteilt hat.

Zur 2. Alt. gehören danach etwa die Fälle, wenn eine gerichtliche Beschlagnahme- und Durchsuchungsanordnung zur Sicherstellung der auf Endgeräten oder Speichermedien des Einzelnen gespeicherten Daten schon erlassen wurde (z. B. offene Maßnahme nach §§ 94, 98, 102, 105 StPO oder heimliche Maßnahme nach §§ 100a Abs. 1 S. 2 – 3, 100b StPO) oder wenn ein gerichtlicher Beschluss gefasst wurde, um auf E-Mail- bzw. Cloud-Server von Dienstanbietern oder auf Nachrichten in einem laufenden Telekommunikationsvorgang zuzugreifen (z. B. offene Maßnahme nach § 110 Abs. 3 StPO oder heimliche Maßnahme nach § 100a Abs. 1 StPO). Dabei kann davon ausgegangen werden, dass die Nutzung der Zugangssicherungscodes bereits aufgrund einer richterlichen Entscheidung über die Sicherstellung der gesicherten Daten gestattet wurde. In diesem Sinne ist dies keine Ausnahme, sondern die Nutzbarkeit der Codes wurde bereits vom Gericht geprüft. Jedoch ist auch hier – wie bei der 1. Alt. – zu beachten, dass es zwischen der Beschlagnahme der Endgeräte selbst und dem Zugriff auf das externe Speichermedium, auf das von den Geräten aus zugegriffen werden kann, aber das durch die Sicherheitsdaten geschützt ist, unterschieden werden muss. So dürfen die Ermittlungsbehörden nur aufgrund des § 110 Abs. 3 StPO weder vom Betroffenen noch von An-

[263] Zust. *Greco*, SK-StPO, § 100j Rn. 16: Beide Alternativen sind fragwürdig.

[264] BT-Drs. 17/12879, S. 11; *Bruns*, KK-StPO, § 100j Rn. 5; *Greco*, SK-StPO, § 100j Rn. 16; M-G/*Schmitt*, StPO, § 100j Rn. 5.

[265] *Greco*, SK-StPO, § 100j Rn. 16.

bietern oder Unternehmen die Vorlegung der Passwörter als solcher verlangen, auch wenn eine richterliche Durchsuchungsanordnung gestützt auf §§ 102, 103 105 Abs. 1 StPO bereits ergangen ist.[266] Allerdings kann dabei der von der Durchsuchung Betroffene als Daten-Eigentümer seine Zugangscodes freiwillig herausgeben.

6. Sonstige verdeckte Maßnahmen

a) Akustische Überwachung außerhalb von Wohnraum

Zur Erforschung eines Sachverhalts oder der Ermittlung des Aufenthaltsortes eines Beschuldigten dürfen die Ermittlungsbehörde ohne Wissen der betroffenen Personen „außerhalb von Wohnungen" das nichtöffentlich gesprochene Wort „mit technischen Mitteln" abhören und aufzeichnen (§ 100f Abs. 1 StPO). Diese Maßnahme ist nur unter vergleichbaren Eingriffsvoraussetzungen und Verfahrenssicherungen mit der TKÜ nach § 100a StPO zulässig.[267] Der § 100f Abs. 1 StPO regelt das heimliche Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes außerhalb von Wohnungen i. S. d. Art. 13 GG.[268] So ist diese Maßnahme gestattet nur außerhalb aller Räume, die der allgemeinen Zugänglichkeit durch eine räumliche Abschottung entzogen und zur Stätte privaten Lebens und Wirkens gemacht sind. Demnach ist sie nicht erlaubt in z. B. nicht allgemein zugänglichen Büro- und Geschäftsräumen, Krankenzimmern, Vereinshäusern, wohl aber in Pkw, Hafträumen einer Justizvollzugsanstalt oder Besuchsräumen einer U-Haftvollzugsanstalt etc.[269] Sowohl Abhören durch technische Mittel wie Wanzen, Mikrophone etc. als auch Mithören ohne technische Mittel, z. B. das zufällige oder arrangierte Belauschen, können durch die Vorschrift gedeckt werden.[270] Außerdem sind in Ansehung der Entscheidung des *BGH* über den Einsatz technischer Mittel nach § 100h Abs. 1 Nr. 1 StPO[271] auch Begleitmaßnahmen, die mit der Anbringung dieser Mittel typisch verbunden sind, aufgrund des § 100f StPO zulässig.[272]

Bei Gefahr im Verzug darf die akustische Überwachung außerhalb von Wohnraum auch von der StA angeordnet werden (§ 100f Abs. 4 i. V. m. § 100e Abs. 1

---

[266] Zust. *Park*, § 4 Rn. 817; dazu *Wohlers/Jäger*, SK-StPO, § 110 Rn. 10: Die Vorschrift des § 110 Abs. 3 selbst legt ohne Weiteres für den von der Durchsuchung Betroffenen bzw. den Provider keine Pflicht auf, den Ermittlungsbehörden Passwörter herauszugeben.

[267] M-G/*Schmitt*, StPO, § 100f Rn. 2.

[268] *Bruns*, KK-StPO, § 100f Rn. 1 f.; M-G/*Schmitt*, StPO, § 10 f Rn. 1. Sie stellt einen Rechtfertigungsgrund für die Verletzung der Vertraulichkeit des Wortes nach § 201 Abs. 2 Nr. 1 StGB dar (*Bruns*, a. a. O. Rn. 2).

[269] *Bruns*, KK-StPO, § 100f Rn. 4 f.; M-G/*Schmitt*, StPO, § 100f Rn. 2; *Roxin/Schünemann*, § 36 Rn. 54.

[270] M-G/*Schmitt*, StPO, § 100f Rn. 4.

[271] *BGHSt* 46, 366, 273 f. [Rn. 18].

[272] *M-G/Schmitt*, StPO, § 100f Rn. 4: auch Mitwirkung der durch die Ermittlungsbehörde beigezogenen Personen, z. B. Stromableser, Schornsteinfeger etc.

StPO) und in ihrer Entscheidungsformel sind die Personalien des von der Maßnahme Betroffenen, der Tatvorwurf, Art, Umfang, Dauer und Endzeitpukt der Maßnahme, die Art der zu erhebenden Informationen und ihre Bedeutung für das Verfahren und die zu überwachenden Orte außerhalb von Wohnraum anzugeben (§ 100f Abs. 4 i. V. m. § 100e Abs. 3 StPO). Doch die wesentlichen Abwägungsgesichtspunkte müssen nicht begründet werden und nach Beendigung der Maßnahme ist die Unterrichtung des Gerichts über deren Ergebnisse nicht erforderlich (vgl. *argumentum e contrario* aus § 100f Abs. 4 StPO).

b) Technische Ermittlungsmaßnahmen bei Mobilfunkendgeräten

§ 100i StPO regelt die Erfassung von Positions- und Standortmeldungen von Mobilfunkendgeräten: die Ermittlung von IMSI und IMEI (Abs. 1 Nr. 1) sowie Standort (Nr. 2) eines Mobiltelefons. Nr. 1 ermöglicht die Ermittlung von IMSI und IMEI eines „aktiv eingeschalteten" Mobilfunkendgerätes (sog. „IMSI-Catcher") und Nr. 2 erlaubt die heimliche Lokalisierung des Standorts des Gerätes (insb. Einsatz sog. „Stiller SMS" bzw. „stealth ping").[273] Zum Merkmal „technischer Mittel" i. S. d. Abs. 1 gehört zwar u. a. der IMSI-Catcher,[274] aber der Gesetzgeber hat durch seine Wahl dem technischen Fortschritt Rechnung getragen und damit die Anwendbarkeit des § 100i StPO auch für weitere kriminaltechnische Neuerungen offengehalten.[275] Daneben hat er inzwischen durch das TKÜG den Wortlaut „nur zur vorläufigen Festnahme oder Ergreifung des Täters auf Grund eines Haft- oder Unterbringungsbefehls" gestrichen.[276]

Bei IMSI-Catchern handelt sich um Geräte, mit denen die auf der Mobilfunk-Karte eines „empfangsbereiten" Mobiltelefons gespeicherte IMSI und IMEI ausgelesen und sein Standort innerhalb einer Funkzelle eingegrenzt werden können.[277] Der IMSI-Catcher ist daher etwa dann als Ermittlungsinstrument von Bedeutung, wenn die Rufnummer des Betroffenen nicht erkennbar ist, weil er eine SIM-Karte unter falschen Personalien gekauft, die Karte getauscht oder ein unter dem Namen einer fremden Person registriertes Mobiltelefon benutzt hat.[278] Soweit dabei mit ihm die laufenden Gespräche des Mobiltelefons mitgehört werden, bedarf es zusätzlich

[273] *BGHSt* 63, 82 = NStZ 2018, 611, 613; zust. *Bruns*, KK-StPO, § 100i Rn. 1; M-G/*Schmitt*, StPO, § 100i Rn. 4; a. M. *Rückert* NStZ 2018, 611, 614: § 100i StPO ist eindeutig auf den IMSI-Catcher zugeschnitten. Nach der Bundesregierung wurde die Stille SMS in der Praxis unterstützt von den Ermächtigungsnormen zur TKÜ (§§ 100a, b StPO a. F.) i. V. m. den §§ 161, 163 StPO zugelassen (BT-Drs. 18/2695, S. 3).

[274] BT-Drs. 14/9088, S. 7.

[275] *BGH* NStZ 2018, 611, 613.

[276] *BGH* NStZ 2018, 611, 613. Damit hat der Gesetzgeber ausdrücklich darauf abgezielt, dass die technischen Mittel i. S. d. § 100i Abs. 1 StPO auch zur Erhebung der Standortdaten nach § 100g Abs. 1 S. 3 oder 4 StPO oder zur Unterstützung von Observationsmaßnahmen nach § 100h Abs. 1 S. 1 Nr. 2 StPO eingesetzt werden können (a. a. O.).

[277] *Bruns*, KK-StPO, § 100i Rn. 2.

[278] *Bruns*, KK-StPO, § 100i Rn. 2; M-G/*Schmitt*, StPO, § 100i Rn. 1.

einer Anordnung nach § 100a StPO.[279] Zum anderen werden bei stiller SMS durch die Versendung einer speziellen Kurzmitteilung, die zwar eine Verbindung mit dem angewählten Mobiltelefon erzeugt, jedoch von dessen Nutzer nicht bemerkt werden kann, Standortdaten des kontaktierten Mobiltelefons erzeugt, womit das Mobiltelefon geortet werden kann.[280] Sie ist in der Praxis eine der bedeutsamsten technischen Ermittlungsmaßnahmen zur Standortbestimmung von Personen[281] und wird zur Zeit laut statistischer Angaben vom BKA und der Bundespolizei weitgehend verwendet.[282] Schließlich fallen die Maßnahmen nach § 100i StPO nicht in den Schutzbereich des Art. 10 Abs. 1 GG; denn TK setzt das Vorhandensein eines menschlichen Kommunikationspartners voraus, jedoch ist die Erhebung der Daten durch die Maßnahmen nicht abhängig von einem tatsächlich stattfindenden oder zumindest versuchten Kommunikationsvorgang zwischen Menschen, sondern sie ist nur einen Datenaustausch zwischen technischen Gräten (vgl. Kapitel 2, B. IV. 2.).[283]

Diese Maßnahmen werden i. d. R. zur Vorbereitung der Überwachung nach § 100a oder § 100g StPO, die Observation nach § 100h Abs. 1 S. 1 Nr. 2 StPO oder die längerfristige Observation nach § 163f StPO eingesetzt, außerdem kann die Ermittlungsbehörde damit auch den Beschuldigten festnehmen oder ergreifen.[284] Daher sind ihre Anordnungsvoraussetzungen und Verfahrenssicherungen den o. g. Maßnahmen gegenüber weitgehend gelockert; z. B. keine obligatorischen Angaben des richterlichen Anordnungsbeschlusses, kein Bedarf der Unterrichtung des Gerichts über die Ergebnisse der Maßnahme und die Befristung ihrer Anordnung und Verlängerung auf höchstens sechs Monate (§ 100i Abs. 3 i. V. m. §§ 100a Abs. 3, 100e Abs. 1 S. 1 – 3, Abs. 3 S. 1, Abs. 5 S. 1 StPO).

---

[279] *Bruns*, KK-StPO, § 100i Rn. 6: die ausgehenden Gespräche der eingebuchten Mobiltelefone; M-G/*Schmitt*, StPO, § 100i Rn. 3. Dementsprechend sind die den Sicherheitsbehörden des Bundes zur Verfügung stehenden Geräte so eingerichtet, dass weder TK-Inhalte noch Verbindungsdaten erfasst werden können (*Bruns*, a. a. O.).

[280] *BGH* NStZ 2018, 611, 611 – 612; *Bruns*, KK-StPO, § 100i Rn. 6a; M-G/*Schmitt*, StPO, § 100i Rn. 4.

[281] *Rückert*, NStZ 2018, 611, 613; *Ruppert*, JR 2019, 297, 300.

[282] Netzpolitik, Viele „Stille SMS" bei Bund und Ländern, 10. 2. 2020, <https://netzpolitik.org/2020/viele-stille-sms-bei-bund-und-laendern/#vorschaltbanner>, Abruf: 31. 10. 2020.

[283] *BVerfG* NJW 2007, 351, 353 [Rn. 57]; *BGH* NStZ 2018, 611, 612 [Tz. b)]; *Bruns*, KK-StPO, § 100i Rn. 1; M-G/*Schmitt*, StPO, § 100i Rn. 2; *Roxin*/*Schünemann*, § 36 Rn. 4. Der Nutzer digitaler Telekommunikationsgeräte muss gewärtigen, dass die Bereitschaft zu ihrer Nutzung die Erfassung der IMSI und der IMEI sowie seiner Identität sowie seines ungefähren Aufenthaltsorts ermöglicht, wobei es sich um das Recht auf informationelle Selbstbestimmung und eine allgemeine Handlungsfreiheit handelt, nicht um den Schutz des Telekommunikationsgeheimnisses (*BVerfG* a. a. O. 354 [Rn. 59 f.]).

[284] *Bruns*, KK-StPO, § 100i Rn. 3 f.; M-G/*Schmitt*, StPO, § 100i Rn. 1; vgl. § 100i Abs. 1 Nr. 2 StPO in der vom 14. 8. 2002 bis zum 31. 12. 2007 geltenden Fassung (BGBl. I S. 3018).

c) Verdeckter Ermittler und längerfristige Observation

Die Vorschriften gelten nur dann, wenn eine Ermittlungshandlung nach den Zulässigkeitsvoraussetzungen jeder Vorschrift vorgenommen wird. Daher wird der Einsatz eines Polizeibeamten als Verdeckten Ermittlers (sog. „VE") nach §§ 100a und b StPO geregelt, nur soweit er unter einer „Legende" ermittelt,[285] und § 163f StPO gilt für eine Beobachtung des Beschuldigten, die durchgehend länger als 24 Stunden dauert oder an mehr als zwei Tagen stattfindet.[286] Dagegen wird der Einsatz eines nicht offen ermittelnden Polizeibeamten (sog. „NoeP"), die Tätigkeit von Vertrauenspersonen (sog. „V-Leute") oder Informanten und eine kurzfristige Observation von den Vorschriften nicht erfasst, sondern ist durch die Ermittlungsgeneralklauseln der §§ 161 Abs. 1, 163 Abs. 1 StPO zu rechtfertigen.[287] Die Beschränkungen der §§ 110 a ff. StPO über VE, insb. der Richtervorbehalt, sind somit auf V-Leute nicht entsprechend anzuwenden, ihnen stehen Eingriffsbefugnisse des VE nicht zu.[288] Andererseits gilt der § 163f StPO auch für die Beobachtung des Beschuldigten, die zwar nicht von vornherein auf eine Überschreitung der in Abs. 1 S. 1 Nrn. 1, 2 genannten Fristen gerichtet ist, aber aus kriminalistischer Sicht auf dem Weg die Fristen überschreiten muss; in diesem Fall muss die Polizei daher dem Verfahren nach Abs. 3 folgen, sobald sich die Notwendigkeit der Fristüberschreitung ergibt.[289] Wenn kurzfristige Observationen mehrfach wiederholt werden, kann praktisch unklar sein, zu entscheiden, ob es jeweils ein einzelne abgrenzbare kurzfristige oder eine langfristige Observation ist.

Für den Einsatz eines Verdeckten Ermittlers gemäß § 110a Abs. 1 StPO ist grundsätzlich die Zustimmung der StA und ggf. des Gerichts erforderlich, bei Gefahr im Verzug kann ihn die Polizei und ggf. die StA selbstständig anordnen (§ 110b Abs. 1 – 2 StPO). Der letztere Einsatz ist zu beenden, wenn ihm nicht binnen drei Werktagen von der StA oder dem Gericht zugestimmt wird (§ 110b Abs. 1 S. 2, Abs. 2 S. 4 StPO). Die längerfristige Observation nach § 163f Abs. 1 StPO darf anderseits nur durch das Gericht, bei Gefahr im Verzug auch durch die StA und ihre Ermittlungspersonen angeordnet werden (§ 163f Abs. 3 S. 1 StPO). Auch in diesem Fall tritt die letztere Anordnung außer Kraft, wenn sie nicht binnen drei Werktagen von dem Gericht bestätigt wird (§ 163f Abs. 3 S. 2 StPO). Die Anordnung derartiger Observation und ihre Verlängerung ist auf höchstens drei Monate zu befristen und sie

[285] *Bruns*, KK-StPO, § 110a Rn. 5; *Roxin/Schünemann*, § 37 Rn. 2; *Wolter/Jäger*, SK-StPO, § 110a Rn. 12.

[286] M-G/*Schmitt*, StPO, § 163f Rn. 1; *Roxin/Schünemann*, § 36 Rn. 35. Da § 163f StPO ungeachtet der Art der Überwachungsmethode ausschließlich auf die Dauer der Observation abstellt, gilt er für jede längerfristige Observation unabhängig von der Verwendung technischer Mittel nach § 100h Abs. 1 S. 1 Nr. 2 StPO (*BGHSt* 46, 266, 278 [Rn. 29]).

[287] *BGHSt* 41, 42; *Bruns*, KK-StPO, § 110a Rn. 6 und 9; M-G/*Schmitt*, StPO, § 110a Rn. 4 f. und § 161 Rn. 1; *Roxin/Schünemann*, § 37 Rn. 6 und 9.

[288] *BGHSt* 41, 42, 45 [Rn. 8 f.].

[289] M-G/*Schmitt*, StPO, § 163f Rn. 1a.

muss schriftlich ergehen (§ 163f Abs. 3 S. 3 i. V. m. § 100e Abs. 1 S. 4, 5, Abs. 3 S. 1 StPO).

d) Herstellung von Bildaufnahmen und Einsatz sonstiger technischer Mittel

Nach § 100h Abs. 1 S. 1 StPO dürfen die Ermittlungsbehörden „außerhalb von Wohnungen" „zum Zwecke der Observation"[290] heimlich Bildaufnahmen herstellen (Nr. 1) und sonstige besondere technische Mittel verwenden (Nr. 2). Die Maßnahme von Nr. 1 ist nicht mit schweren Straftaten oder einem qualifizierten Tatverdacht verbunden, jedoch wird sie wird durch das Gebot der Subsidiarität und Verhältnismäßigkeit geregelt.[291] Die Vorschrift gilt auch für die Fertigung von Bildaufnahmen oder Videoaufzeichnungen mit Kameras zur Verfolgung von Ordnungswidrigkeiten im Straßenverkehr.[292] Nr. 2 regelt den Einsatz eines sonstigen technischen Mittels, der von der TKÜ, der Online-Durchsuchung, der akustischen Überwachung inner- und außerhalb von Wohnraum und dem Einsatz technischer Ermittlungsmaßnahmen bei Mobilfunkendgeräten nach §§ 100a – c, 100f, 100i StPO sowie den Bildaufnahmen nach Nr. 1 nicht gedeckt wird.[293] Nach der Angabe des *BVerfG* kollidiert das Merkmal „besondere für Observationszwecke bestimmte technische Mittel" in der Nr. 2 nicht mit den Anforderungen an Normenklarheit und Tatbestandsbestimmtheit, die sich aus dem Rechtsstaatsprinzip ergeben.[294] Der Gesetzgeber kann u. a. mit dem Begriff des „technischen Mittels" dem technischen Fortschritt Rechnung tragen.[295] Die Strafverfolgungsbehörden haben unter Beachtung des Verhältnismäßigkeitsgrundsatzes eine Annexkompetenz für die den Einsatz des technischen Mittels

[290] Nach dem Wortlaut der Vorschrift ist die Anfertigung von Bildaufnahmen der Nr. 1 – im Gegensatz zu Nr. 2 – keineswegs nur auf Observationszwecke beschränkt (vgl. *OLG Bamberg* NJW 2010, 100, 101 [Tz. aa)]; *OLG Brandenburg* NJW 2010, 1471, 1472 [Tz. a)]; *OLG Stuttgart* NJW 2010, 1219, 1220). Nach h. M. in der Literatur ist aber diese Voraussetzung auch für die Nr. 1 erforderlich (*OLG Düsseldorf* NJW 2010, 1216, 1217 [Tz. cc)]; M-G/*Schmitt*, StPO, § 100h Rn. 1; *Wolter/Greco*, SK-StPO, § 100h Rn. 4; dazu *Bruns*, KK-StPO, § 100h Rn. 2; vgl. *Singelnstein*, NStZ 2014, 305, 306: aufgrund der Verweisung auf das Wort der Nr. 2 „sonstige"). Demnach gilt die Vorschrift nicht für die Fertigung von Lichtbildern am Tatort zur Beweissicherung (Spurensicherung) (M-G/*Schmitt*, a. a. O.).

[291] M-G/*Schmitt*, StPO, § 100h Rn. 1. Freilich ist ein Anfangsverdacht erforderlich (*Bruns*, KK-StPO, § 100h Rn. 4).

[292] *BVerfGE* NJW 2010, 2717; *Bruns*, KK-StPO, § 100h Rn. 4; M-G/*Schmitt*, StPO, § 100h Rn. 1 a. E.; *Singelnstein*, NStZ 2014, 305, 306.

[293] Vgl. *BGHSt* 46, 266, 271 f. [Rn. 14]; NStZ 2018, 611, 612; vgl. *BVerfGE* 112, 304, 317 [Rn. 53]: Der Gesetzgeber hat in § 100c Abs. 1 StPO a. F. die optischen und akustischen Überwachungstätigkeiten systematisch abgegrenzt und damit hat er einen Bereich hinreichend bestimmt abgegrenzt, in dem jede moderne Kriminaltechnik zur Anwendung kommen darf.

[294] *BVerfGE* 112, 304, 316 f. [Rn. 49 – 52].

[295] *BGHSt* 46, 266, 272 [Rn. 15]; *BVerfGE* 112, 304, 316 f. [Rn. 51]. Darüber hinaus können die Ermittlungsbehörde und die Gerichte nach dem Fortschritt der Technik diesen offenen Gesetzesbegriff konkret ausfüllen, jedoch kann der Gesetzgeber bei Fehlentwicklungen korrigierend eingreifen (*BVerfGE* a. a. O.).

notwendigen Begleitmaßnahmen.[296] Die Anwendung von technischen Mitteln wie z. B. Ferngläser und Sprechfunkgeräte bedarf i. d. R. keiner ausdrücklich gesetzlichen Regelung (vgl. §§ 161, 163 StPO),[297] aber wenn eine Maßnahme mittels technischer Mittel eine nicht geringe Beeinträchtigung für die Privatsphäre auslöst, nämlich beim Einsatz von z. B. Nachtsichtgeräten, Bewegungsmeldern, Peilsendern bzw. GPS,[298] Drohnen[299] etc., so ist dies durch § 100h Abs. 1 StPO zu rechtfertigen.

Von dieser Auslegung sind die Maßnahmen nach § 100h Abs. 1 StPO nur außerhalb des Schutzbereichs des Art. 13 Abs. 1 GG zulässig[300], und sie dürfen auch nur zur Observation eingesetzt werden. Sie schränken i. d. R. das allgemeine Persönlichkeitsrecht bzw. das Recht auf informationelle Selbstbestimmung ein, dürfen aber in den Kernbereich ihres Schutzes nicht eingreifen (vgl. § 100h Abs. 4 i. V. m. § 100d Abs. 1, 2 StPO). Nach der Entscheidung des *BGH* ist es unverhältnismäßig, soweit eine Maßnahme gemäß Nr. 2 (der Einsatz der GPS-Technik) mit anderen isoliert betrachtet je für sich zulässigen Überwachungsmethoden zusammentrifft und dies zur Erstellung eines umfassenden Persönlichkeitsprofils führt. Daher ist bei der Anordnung jeder einzelnen Maßnahme zu prüfen, ob ihre Durchführung unter Berücksichtigung bereits angeordneter Überwachungsmethoden insgesamt noch verhältnismäßig ist.[301]

Bezüglich der Eingriffsvoraussetzungen gibt es in § 100h StPO zunächst keine Beschränkung nach der Schwere der Straftat und der Stärke des Tatverdachts, und darin liegt nur eine einfache Subsidiaritätsklausel vor. Weil die Maßnahmen des Abs. 1 S. 1 Nr. 2 aber i. d. R. eingriffsintensiver sind als die Bildaufnahmen der Nr. 1, beschränken sie sich auf Straftaten von erheblicher Bedeutung (Abs. 1 S. 2).[302] Danach bleiben die Maßnahmen der Nrn. 1 und 2 nicht dem Richter vorbehalten, sondern dürfen nach Ermessen der StA oder der Polizei angeordnet werden.[303]

---

[296] *BGHSt* 46, 266, 273 f. [Rn. 18]: eine heimliche Wegnahme eines Pkw zum Einbau eines Empfängers in einer Werkstatt.

[297] Vgl. *Bruns*, KK-StPO, § 100h Rn. 1 und 5; auch M-G/*Schmitt*, StPO, § 100h Rn. 2.

[298] *BVerfGE* 112, 304; *BGHSt* 46, 266, 271 ff.; M-G/*Schmitt*, StPO, § 100h Rn. 2. In den Gesetzesmaterialien des § 100c Abs. 1 Nr. 1 lit. b StPO a. F. ist der Peilsender, der vor der GPS universal verwendet wurde, als Beispiel für die technischen Mittel angeführt (BT-Drs. 12/989, S. 39).

[299] *Bruns*, KK-StPO, § 100h Rn. 5; M-G/*Schmitt*, StPO, § 100h Rn. 2.

[300] *Bruns*, KK-StPO, § 100h Rn. 3 (Nr. 1) und Rn. 5 (Nr. 2); M-G/*Schmitt*, StPO, § 100h Rn. 1.

[301] *BGHSt* 46, 266, 277 [Rn. 27 a. E.]: Bei der insoweit vorgenommenen Abwägung ist das Gewicht der aufzuklärenden Straftat von besonderer Bedeutung.

[302] *OLG Bamberg* NJW 2010, 100, 101 [Tz. aa)].

[303] *Roxin/Schünemann*, § 36 Rn. 55; *Wolter/Greco*, SK-StPO, § 100h Rn. 9. Dabei darf die Anordnung der Polizei nur dann ergehen, wenn die StA alsbald nicht erreichbar ist, danach ist die Einhaltung dieser Subsidiarität nur durch die Zustimmung der StA zu bestätigen (*Wolter/Greco*, a. a. O.). Soweit eine einzelne Beobachtungsmaßnahme die zeitlichen Grenzen des § 163f StPO überschreitet, sind aber die Voraussetzungen dieser Norm, u. a. der Richtervorbehalt, zu beachten (*Singelnstein*, NStZ 2014, 305, 310).

Demnach liegen in der Vorschrift keine Bestimmungen über Form, Inhalt und Begründung der Anordnung sowie über die Unterrichtung des Gerichts nach Beendigung der Maßnahmen.[304] Wird eine Videoüberwachung oder eine Observation durch die Verwendung technischer Mittel von den Voraussetzungen des § 163f StPO erfasst, unterliegt sie freilich dem Richtervorbehalt und der zeitlichen Beschränkung der Maßnahme nach § 163f Abs. 3 StPO.[305] Es ist dennoch fragwürdig, dass es in der Ermächtigungsnorm überhaupt keine Garantie gibt. Die Fertigung von Bildaufnahmen oder die Verwendung technischer Mittel können nämlich über die Observationszwecke hinaus zur Beweissicherung durch die Auszeichnung von Gespräch oder Wort, d. h. der Überwachung und Aufzeichnung von Gespräch oder Wort i. S. d. §§ 100a Abs. 1, 100c Abs. 1, 100f Abs. 1 StPO, führen.[306] Da heute u. a. die Technik der Aufnahme und Wiedergabe von Bild und Ton – als Schlüsselfunktion des Smartphones – immer noch fortschreitet, bedarf es für ihre Verwendung zu Ermittlungszwecken zumindest einer wirksamen nachträglichen Kontrolle über ihre Rechtmäßigkeit: z. B. Protokollierungs- bzw. Dokumentations- und Begründungspflichten.

III. Zusammenfassung und Zwischenfazit

Heimliche Zwangsmaßnahmen und ihre Ermächtigungsnormen sind nur dann mit dem GG in Einklang zu bringen, wenn sie mit Eingriffsvoraussetzungen und verfahrensrechtlichen Vorkehrungen verbunden sind, die nach Maßgabe des Verhältnismäßigkeitsgrundsatzes mit ihrer Eingriffsintensität gleichgerichtet werden. Dabei ist u. a. eine konkrete gesetzliche Ausgestaltung von Verfahrensgarantien entscheidend, um die Eingriffsintensität jeder Maßnahme entsprechend auszugleichen. Die Verfassungsmäßigkeit von Ermächtigungen, die durch verdeckte bzw. umfassende Erhebung personenbezogener Daten einen bestimmten einschneidenden Eingriff ermöglichen, hängt von dem Inhalt der verfahrensrechtlichen Garantien als Kontrollsysteme ab, seine Eingriffsintensität ausgleichen zu können.[307] Dies gilt sowohl für TKÜ, Überwachungen außerhalb von Wohnungen, Wohnraumüberwachungen

[304] *Wolter/Greco*, SK-StPO, § 100h Rn. 9 f. und 16.

[305] *BGHSt* 46, 266, 278 [Rn. 29]; *Bruns*, KK-StPO, § 100h Rn. 3.

[306] *Wolter/Greco*, SK-StPO, § 100h Rn. 20.

[307] Im Hinblick auf eine effektive Strafverfolgung in den Bereichen der organisierten Kriminalität und des Terrorismus sowie der Wirtschafts- und Steuerdelikte kann heute eine bestimmte Ermittlungsmaßnahme lediglich wegen der besonderen Intensität des Grundrechtseingriffs nicht von vornherein vollständig ausgeschieden werden, es sei denn, dass sie auf eine umfassende Datenbeschaffung durch eine langfristige und vollständige Überwachung des Einzelnen abzielt. Dies lässt sich auch den Entscheidungen des *BVerfG* über die Wohnraumüberwachung und die Online-Durchsuchung (*BVerfGE* 109, 297; 120, 274; 141, 220) entnehmen. Bei der Kontroverse über neue technische Ermittlungsmethoden steht daher nicht die Verfassungsmäßigkeit einer Maßnahme selbst im Vordergrund, sondern eine verhältnismäßige Ausgestaltung ihrer Eingriffsschwelle und Vorkehrungen.

und VDS als auch für (jüngste) Quellen-TKÜ und Online-Durchsuchungen, was in den letzten Jahrzehnten in die StPO nacheinander eingeführt wurde. Insofern dienen die allgemeinen Vorschriften zur Beschlagnahme und Durchsuchung der §§ 94 ff., 102 ff. StPO als Standard für die Ausgestaltung verfahrensrechtlicher Vorkehrungen der jeweiligen Befugnisnormen. Für einen Grundrechtseingriff kann der Betroffene – nach dem jeweiligen Grundrecht i. V. m. Art. 19 Abs. 4 GG – grundsätzlich nachträglich nach der Benachrichtigung die Überprüfung der Rechtmäßigkeit der Maßnahme sowie der Art und Weise ihres Vollzugs beantragen (vgl. § 101 Abs. 7, 101a Abs. 6 StPO). Die Kontrolle über bereits gewonnene Daten ist jedoch nur begrenzt wirksam: insb. bei heimlichen Zwangsmaßnahmen. Von größter Bedeutung ist daher zur Erreichung des Grundrechtsschutzes in den Ermittlungsverfahren der Richtervorbehalt, der die proaktive Kontrolle durch Richter darstellt. Jedoch sieht sich er heutzutage dem Zweifel und der Kritik an der Aushöhlung seiner Funktion und Wirkung in der Praxis ausgesetzt (vgl. dazu eingehend unten C. II. 3.).

C. Ermächtigungsgrundlagen für heimlichen Zugriff auf die auf dem Server des Dienstanbieters gespeicherten Daten

I. Fragestellung

Dadurch, dass alle Arten von Daten derzeit zumeist in informationstechnischen Systemen (lokalen Endgeräten oder Servern der Dienstanbieter) „gespeichert" bleiben, unterscheiden sich moderne Telekommunikationsumstände von früheren entscheidend (vgl. Kapitel 2, A. I.). Die Strafverfolgungsbehörden können diese tagtäglichen, umfassend kumulativ hinterlassenen Datenspuren der Bürger von dem Betroffenen selbst oder von Anbietern erhalten. Dabei hängen die Bestimmung bzw. die Ausgestaltung der Ermächtigungsnorm für jede Maßnahme von ihrer Eingriffsintensität ab, die nach der Art und Weise der Durchführung unterschiedlich bewertet wird. Erfolgt der Zugriff auf die auf einem lokalen System vorhandenen Daten und ihre Sicherstellung mit Wissen des Betroffenen, dann gelten dafür §§ 94 ff., 102 ff. StPO (vgl. Kapitel 4), erfolgt das aber ohne Wissen des Betroffenen, so gilt § 100b StPO (vgl. heimliche Online-Durchsuchung; oben B. II. 2. b)). Umstritten ist dagegen der Zugriff auf serverbasiert gespeicherte Daten und ihre Sicherstellung. Erfolgen sie offen, kann dies aufgrund der §§ 94 ff., 102 ff. StPO gerechtfertigt werden (vgl. näher dazu Kapitel 4, B. III.).[308] Es ist aber noch unklar und unbestimmt, auf welcher Ermächtigungsgrundlage der „ohne Wissen des (von Daten) Betroffenen durchgeführten Zugriff auf Nachrichteninhalte in Webseiten"

[308] Vgl. *BVerfGE* 124, 43, 58 f. [Rn. 57].

und ihre „Sicherstellung“ möglich ist.[309] In der Praxis ist dies insbesondere in folgenden Fällen problematisch: bei E-Mail-Verkehr zum Zweck des Datenaustausches mit einem bestimmten Beteiligten und bei sozialen Netzwerken und Internet-Foren, in denen viele (un)bestimmte Teilnehmer Daten miteinander austauschen, und bei Cloud-Computing, bei dem externe Speichermedien über das Internet – i. d. R. ohne den Zweck des Datenaustauschs – verwendet werden. Hinsichtlich der Fallkonstellation, Inhaltsdaten zu erfassen, die von Anbietern der Dritten verwahrt werden und nur unter dem Nutzerkonto erreicht werden können, scheinen alle Zugriffe einander ähnlich zu sein. Die Eingriffsintensität jeder Maßnahme wird aber unterschiedlich bewertet, und daher müssen auch Ermächtigungsnormen dementsprechend festgelegt werden. Bei Betrachtung der heute weitverbreiteten Nutzung dieser TK-Dienste ist die Bestimmung der Ermächtigung für den jeweiligen Fall den Ermittlungsbehörden von großer faktischer Relevanz.

II. Technische Vorgänge nach Kommunikationsart sowie einschlägige Grundrechte

Im Rahmen der Zugriffe auf die über TK-Dienstanbieter kommunizierenden Daten sind nach technischen Phasen der TK und der Art und Weise des Eingriffs die Grundrechte von Art. 10 Abs. 1, Art. 13 Abs. 1 oder Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG in Rechnung zu stellen. Zunächst kommt beim Eingriff in die bei ihnen gespeicherten Daten – wie bei dem in einen laufenden Kommunikationsvorgang – nur der Schutz des Fernmeldegeheimnisses in Betracht. Denn die außerhalb des Herrschaftsbereichs der Kommunikationsteilnehmer bestehenden Daten werden – ungeachtet des technischen Übermittlungsvorganges – wegen der spezifischen Gefährdungslage allemal durch dieses Grundrecht primär geschützt. Damit sind die serverbasierten privaten Nachrichten mittels eines Benutzerkontos i. d. R. unabhängig von ihrer Art in allen Facetten in den Schutzbereich des Fernmeldegeheimnisses einbezogen.[310] Hingegen werden die Daten, die im Herrschaftsbereich des Nutzers wie etwa in PC oder Handy vorhanden sind, normalerweise durch die Unverletzlichkeit der Wohnung oder das informationelle Selbstbestimmungsrecht und bei einem verdeckten Zugriff durch das Computer-Grundrecht geschützt. Entscheidend ist aber bei verfassungsrechtlicher Rechtfertigung der Eingriffe in per-

[309] *Bär*, NStZ 2009, 397, 398 f.; *Brodowski*, JR 2009, 402, 406 [Tz. III.]: insb. im Lichte der bisherigen Rechtsprechung zur Normenklarheit und -bestimmtheit; *Kasiske*, StraFo 6/2010, 228, 230 ff.; *Klesczewski*, ZStW 123 (2011), 737, 746 ff.; *Kudlich*, GA 2011, 193, 202; *Neuhöfer*, JR 2015, 21, 23 ff.; *Park*, § 4 Rn. 802 ff. [insb. Rn. 807 ff.]; *Sieber*, 69. DJT 2012, C 109 ff.; *Zimmermann*, JA 5/2014, 321, 324 f. In der letzten Zeit wird die „Ermächtigungsgrundlage für den Zugriff auf serverbasiert gespeicherte Nachrichteninhalte“ – einschließlich der E-Mails – zum Hauptgegenstand der juristischen Auseinandersetzung (vgl. *Neuhöfer*, a. a. O. 21). Dies wurde schon in der Praxis mit der Verbreitung von Webmail-Service, Internet-Foren und -Newsgroups wichtig.

[310] *Neuhöfer*, JR 2015, 21, 23.

sonenbezogene Daten nunmehr keine Eröffnung des Schutzbereichs des Grundrechts mehr, sondern die Eingriffsintensität nach Art und Weise der Durchführung jeder Maßnahme und die gesetzliche Ausgestaltung dementsprechender Eingriffsvoraussetzungen und Verfahrenssicherungen.

1. E-Mail-Verkehr

Die Kommunikation per E-Mail kann in mehreren Stadien unterteilt werden und in der Literatur ist dies je nach Ansicht unterschiedlich.[311] Der Hauptgrund für diese Unterteilung liegt aber in der Bestimmung des betroffenen Grundrechts und der einschlägigen Ermächtigung in jeder Phase. So kann der Übertragungsweg der E-Mail in vier Phasen wie folgt eingeteilt werden (teilweise Veränderung des Sechs-Phasen-Modells von *Zimmermann*).[312]

- Phase 1: Herstellung des Entwurfs der E-Mail auf dem Endgerät des Senders. Hierbei sind die zwei technischen Möglichkeiten zu unterscheiden: ein Fall, dass der Entwurf auf dem Endgerät des Senders abgefasst wird („clientbasiert" – Variante 1), und ein anderer Fall, dass die Rohdaten in Echtzeit oder gelegentlich als Sicherungskopie auf den Server des Mail-Providers übertragen und dort gespeichert werden („serverbasiert" – Variante 2). Die beiden Alternativen können je nach dem Verhalten des Absenders oder der technischen Möglichkeit nebeneinander bestehen.
- Phase 2: Absenden der E-Mail und Übermittlung über den Mail-Provider des Senders an den Mail-Provider des Empfängers.
- Phase 3: Zwischenspeicherung der eingegangenen E-Mail auf dem Mail-Server des Empfängers.
- Phase 4: Abruf der E-Mail durch den Empfänger. Auch hierbei gibt es die zwei technischen Möglichkeiten: Ein Fall, dass die E-Mail auf den Empfängerbereich heruntergeladen und gleichzeitig im Server des Mail-Providers gelöscht wird (Variante 1), und ein anderer Fall, dass die E-Mail auf dem Server nicht gelöscht wird und gespeichert bleibt, und weiter dort gelesen und verwaltet wird (Variante 2). Ebenfalls können die beiden Alternativen nebeneinander bestehen.

Zur Variante 1 in Phase 1 und 4 gehören E-Mail-Programme wie *MS Outlook* und *Mozilla Thunderbird.* Dies basiert technisch auf POP3 (Post Office Protocol 3). Hier wird zwar die gesendete E-Mail zunächst auf dem ISP-Server zwischengelagert, bis

[311] Z. B. *Bär*, NStZ 2009, 397, 398: 4 Phasen; *Brodowski*, JR 2009, 402: 7 Phasen; *Bruns*, KK-StPO, § 100a Rn. 18 f.: 3 Phasen; *Kasiske*, StraFo 6/2010, 228: 3 oder 4 Phasen; *Klesczewski*, ZStW 123 (2011), 737, 744 f.: 4 Phasen; *Park*, § 4 Rn. 803 und 806: 4 Phasen; *Zimmermann*, JA 5/2014, 321, 321 f.: 6 Phasen.

[312] Vgl. *Zimmermann*, JA 5/2014, 321, 321 f. Unabhängig davon, ob dieser Prozess in verschiedene Phasen unterteilt wird, sind drei Zustände rechtlich von Bedeutung: die Übertragung der E-Mail und die Speicherung bei einem Beteiligten oder dem TK-Anbieter (*Singelnstein*, NStZ 2012, 593, 596).

sie durch das E-Mail-Programm vom Empfänger abgeholt wird, jedoch wird sie nach dem Abholvorgang im Server gelöscht und als digitale Kopie ausschließlich auf dem lokalen Computer des Empfängers gespeichert. Daher verbleiben auf dem Server nur E-Mails, die zum Zeitpunkt der Durchsuchung nicht abgerufen wurden. Die Variante 2 in Phase 1 und 4 heißt „Webmail-Service", bei dem die E-Mail (oder deren Entwurf) normalerweise im Mail-Server des Providers gelesen, gespeichert und verwaltet wird (z. B. *gmx*, *hotmail*, *gmail*). Er fußt technisch auf IMAP (Internet message access protocol). Hierbei hat zwar der Teilnehmer ein E-Mail-Postfach auf dem Mail-Server, auf den er überall von einem beliebigen Endgerät aus über das Internet zugreifen kann,[313] jedoch sind die Nachrichteninhalte nur beim Anbieter gespeichert.[314] Beim Webmail-Service ist es tatsächlich üblicherweise nicht feststellbar und auch ohne Bedeutung, ob die entgegengenommene E-Mail abgerufen oder gelesen wurde. Somit ist hier die Abgrenzung zwischen der Phase 3 und der Variante 2 in Phase 4 nicht sinnvoll. Im Frühstadium der E-Mail-Dienste war die Variante 1 weit verbreitet, jedoch wird der Webmail-Service heute durchgängig verwendet.[315] Daher ist es nunmehr bezüglich der Bestimmung des betroffenen Grundrechts und der Rechtsgrundlage für den Zugriff auf die auf dem Server des Anbieters vorhandenen E-Mails gleichgültig, ob sie zwischen- oder endgespeichert sind.[316]

Die Variante 1 in Phase 1 und 4 betrifft die Unverletzlichkeit der Wohnung oder das informationelle Selbstbestimmungsrecht oder ggf. das Computer-Grundrecht, die sonstigen Phasen und Varianten den Schutz des Fernmeldegeheimnisses.[317] Im Rahmen der Ermächtigung liegt Eingriffen in Phase 2 als – typische – TKÜ unbeanstandet § 100a Abs. 1 S. 1 StPO zugrunde. Es ist aber umstritten, aufgrund welcher Ermächtigung Zugriffe auf die E-Mails in der Variante 2 in Phase 1 und 4 sowie in Phase 3 zu rechtfertigen sind (vgl. unten III. 1.).

2. Nachrichten in sozialen Netzwerken und Internet-Foren

Eine Kenntnisnahme öffentlich zugänglicher Informationen ist dem Staat grundsätzlich nicht verwehrt. Daher liegt dann kein Eingriff in Grundrechte vor,[318]

---

[313] *Neuhöfer*, JR 2015, 21, 22: „rein serverbasiert" oder „durchweg internetbasiert"; *Park*, § 4 Rn. 804.

[314] *Bruns*, KK-StPO, § 100a Rn. 19; *Brunst*, CR 2009, 584, 591; *Sieber*, 69. DJT 2012, C 109. Der Nutzer hat freilich jederzeit die Möglichkeit, E-Mails in lokale Ordner zu verschieben (*Sieber*, a. a. O. C. 109 f.).

[315] Vgl. *Bruns*, KK-StPO, § 100a Rn. 19; *Kemper*, NStZ 2005, 538, 543; *Kasiske*, StraFo 6/2010, 228, 229; *Klesczewski*, ZStW 123 (2011), 737, 745; *Park*, § 4 Rn. 804; *Sieber*, 69. DJT 2012, C 109.

[316] Vgl. *BVerfGE* 124, 43, 55 f. [Rn. 46–48]: bei Festlegung des verletzten Grundrechts.

[317] BT-Drs. 18/12785, S. 49 f.; vgl. *BVerfGE* 124, 43, 54 [Rn. 45].

[318] *BVerfGE* 120, 274, 344 f. [Rn. 308]: kein Eingriff in das allgemeine Persönlichkeitsrecht liegt vor.

wenn eine staatliche Stelle im Internet verfügbare Kommunikationsinhalte erhebt, die sich an jedermann richten (sog. „Online-Streife“[319]): etwa, wenn die Behörde – unter Zuhilfenahme der verfügbaren Suchmaschinen wie beispielhaft *google.de* – eine allgemein zugängliche Webseite aufruft, eine jedem Interessierten offenstehende Mailingliste abonniert oder offene Chats beobachtet. Wenn diese Internetaufklärung gezielt zu einer Person erfolgt und die erhobenen Daten mit anderen Daten abgeglichen werden, so kann ein Eingriff in das Recht auf informationelle Selbstbestimmung bestehen und hierfür bedarf es einer Ermächtigungsgrundlage.[320] Nach h. M. sind aber dabei die Ermittlungsgeneralklauseln der §§ 161 Abs. 1, 163 Abs. 1 StPO ausreichend.[321] Dies alles gilt ebenfalls für den Zugriff auf „offene“ soziale Netzwerke und Internet-Foren.

Heute muss man sich zur Verwendung sozialer Netzwerke und Internet-Foren fast immer anmelden, und auf die darauf vorhandenen Daten können nur durch geschlossene Benutzergruppen zugegriffen werden. Jedoch ist die Überprüfung zumeist nur formell, außerdem kann man i. d. R. unter Verwendung von Pseudonymen wie Nicknamen an der TK teilnehmen.[322] So sind hier die Daten in Webseiten zugangsgesichert, aber eine unbestimmte Mehrheit kann jederzeit pseudonym darauf zugreifen, und hierbei stehen auch keinerlei Überprüfungsmechanismen für das Vertrauen eines Kommunikationsteilnehmers in die Identität und Wahrhaftigkeit seiner Partner bereit.[323] Aus diesem Grund besteht in sozialen Netzwerken und Internet-Foren, in denen es mehr als zwei, aber meist Hunderte bis Zehntausende von registrierten Nutzern gibt, im Vergleich zur Telefonie oder zum E-Mail-Verkehr, in denen durchgängig zwei bestimmte Personen kommunizieren, i. d. R. kein grundrechtlich schutzwürdiges Vertrauen des Betroffenen in die Identität und die Moti-

[319] *Klesczewski*, ZStW 123 (2011), 737, 739; M-G/*Schmitt*, StPO, § 163 Rn. 28a; *Singelnstein*, NStZ 2012, 593, 600; auch *Kudlich*, GA 2011, 193, 198: „elektronische Streifenfahrt durch das Internet“; *Sieber*, 69. DJT 2012, C 125: die einfache „Streife im Netz“. Dies stellt ein „Aufklären im Internet“ dar, es bedeutet das heimliche Aufzeichnen der Inhalte von Internetkommunikation gerade auf dem dafür technisch vorgesehenen Wege; abzugrenzen ist es von der „Online-Durchsuchung“ (*Klesczewski*, a. a. O. 739 f.).

[320] *BVerfGE* 120, 274, 345 [Rn. 309].

[321] *Brodowski/Eisenmenger*, ZD 3/2014, 119, 125; *Bruns*, KK-StPO, § 100a Rn. 24; *Klesczewski*, ZStW 123 (2011), 737, 739; *Kudlich*, GA 2011, 193, 198 f.; M-G/*Schmitt*, StPO, § 100a Rn. 7; *Sieber*, 69. DJT 2012, C 125 f.; *Singelnstein*, NStZ 2012, 593, 600 am Anfang m. w. N.

[322] *Bruns*, KK-StPO, § 110a Rn. 23 f.; *Soiné*, NStZ 2014, 248, 249 [Tz. 4.]; auch *Klesczewski*, ZStW 123 (2011), 737, 753; *Kudlich*, GA 2011, 193, 198 f. Im Internet wird auf die Verwendung von Klarnamen oder Bezeichnungen, die auf existente Personen hindeuten, so vielfach verzichtet und dabei wissen die Beteiligten regelmäßig nicht, wer sich hinter diesen Bezeichnungen verbirgt (*Soiné*, a. a. O.; dazu *Klesczewski*, a. a. O.: dies zählt zu den Usancen des Internets). Insb. bei z. B. *Facebook* und *Instagram*, das sich heutzutage weit verbreitet und viel verwendet ist, kann man sich unter einem falschen oder fremden Namen und mit falscher und fremder Adresse anmelden, weiter sind sämtliche Inhalte unter einem bestimmten Konto nach Einstellung der Teilnehmer in der Tat allen Mitgliedern zugänglich.

[323] *BVerfGE* 120, 274, 345; M-G/*Schmitt*, StPO, § 163 Rn. 28a; *Soiné*, NStZ 2014, 248, 249.

vation von Kommunikationspartnern.[324] Daher stellen hierbei die Daten keine rechtlich – etwa durch das Recht auf informationelle Selbstbestimmung und das Datenschutzrecht – zu schützenden personenbezogenen Daten dar, die Ermittlungsbehörde kann mittels anonymer bzw. pseudonymer Identität eine (reine) Internetaufklärung vornehmen.[325] So hat die Erhebung der Daten keinen Eingriffscharakter.[326] Das Vertrauen eines Kommunikationsteilnehmers darauf, dass er nicht im Internet mit einer staatlichen Stelle kommuniziert, ist nicht schutzwürdig.[327] Im Ergebnis gehört dies auch begrifflich zur „Online-Streife“[328] und wird in dieser Arbeit nicht behandelt.

Erfolgt hingegen die Anmeldung zu einer Gruppe bzw. der Zugriff auf bestimmte Inhalte – obwohl es nicht üblich ist – nur mit der Angabe von echten Daten, z. B. unter „Klarnamen“ und auf der Grundlage einer mehr oder weniger „intensiven Prüfung“, dann ist dieser Eingriff eher dem Zugriff auf bei E-Mail-Servern gespeicherte Nachrichten gleichzustellen.[329] In der Kommunikation, die in so hohem Maße zugangsgesichert ist, besteht i. d. R. – ebenfalls wie beim E-Mail-Verkehr – ein spezielles, den persönlichen Bereich betreffendes Vertrauensverhältnis zwischen Kommunikanten. So kann insofern die Fragestellung des „Zugriffs auf serverbasiert gespeicherte E-Mail-Inhalte“ rechtlich ohne Weiteres auf die Diskussion über den „Zugriff auf bei qualifiziert zugangsgesicherten sozialen Netzwerken bzw. Internet-Foren gespeicherte Nachrichteninhalte“ übertragen werden (vgl. unten III. 1.).[330] Auch hier ist Art. 10 Abs. 1 GG betroffen.

3. Cloud-Computing

Bei Cloud-Computing, dessen Nutzung seit Anfang der 2010er-Jahre rasant zugenommen hat, werden die Daten in einem Speicherplatz des Servers der Dienstprovider wie z. B. *Microsoft, Google, Dropbox, Amazon* gespeichert und verwaltet,

[324] *Klesczewski*, ZStW 123 (2011), 737, 739 und 753; *Singelnstein*, NStZ 2012, 593, 599 f.; *Soiné*, NStZ 2014, 248, 248 f.; vgl. *BVerfGE* 120, 274, 340 f. [Rn. 290 – 293].

[325] Vgl. *Sieber*, 69. DJT 2012, C 125: Die Anonymität in Computernetzen kommt nicht nur Straftätern zugute, sondern kann auch von Strafverfolgungsbehörden zu verdeckten Ermittlungen genutzt werden.

[326] *Soiné*, NStZ 2014, 248, 248 f. Vgl. § 3 Abs. 6 und 6a BDSG.

[327] *BVerfGE* 120, 274, 345 f. [Rn. 311]; *Soiné*, NStZ 2014, 248, 249.

[328] Vgl. *BVerfGE* 120, 274, 344 f. [Rn. 308]: „*im Internet verfügbare Kommunikationsinhalte, die sich an jedermann oder zumindest an einen nicht weiter abgegrenzten Personenkreis richten*“.

[329] In diesem Fall können die Daten aus Internet-Foren oder sozialen Netzwerken ggf. mehr und vielseitiger sein als dieselben aus E-Mail-Beständen.

[330] *Klesczewski*, ZStW 123 (2011), 737, 752 ff.; *Neuhöfer*, JR 2015, 21, 21 f.; *Sieber*, 69. DJT 2012, C 111; *Singelnstein*, NStZ, 2012, 593, 597 und 599. Hierbei können die Daten – anders als bei E-Mail – bei ihrem Abruf nur temporär im Browser des Nutzers angezeigt, nicht jedoch auf seinen lokalen Rechner heruntergeladen werden (*Neuhöfer*, a. a. O. 22; *Sieber*, a. a. O.).

wobei die Benutzer über das Netzwerk auf den Server zugreifen und danach die erforderlichen Informationen verwenden können. Zurzeit wird dieser Service zumeist nach der Registrierung (der Eröffnung des Nutzerkontos) ohne oder gegen Entgelt (aber kleine Gebühr) erbracht. Die Nutzer können jederzeit von jedem Ort über das Internet auf diesen Cloud-Speicher, eine sog. „virtuelle Festplatte", zugreifen[331] und damit ihre Dateien der Inhaltsdaten hinauf- oder herunterladen und löschen. Die außengelagerte Festplatte ersetzt daher die gewöhnliche des heimischen PC.[332] Zwar werden ggf. die beiden Speicher automatisch abgeglichen, nämlich synchronisiert, aber die im Cloud-Speicher gespeicherten Daten sind von den auf privaten Computersystemen oder mobilen Datenträgern wie z. B. USB-Stick jedes Nutzers gespeicherten zu unterscheiden.[333] Unter dem Gesichtspunkt der Herrschaftsbereich-Theorie befinden sich nämlich die Ersteren in der Sphäre des von Daten Betroffenen, dagegen die Letzteren im Bereich des Netzbetreibers eines Dritten.[334]

Zwar erfolgt die Durchsicht und Sicherstellung von Datenträgern und den hierauf gespeicherten Daten meist zusammen mit der Wohnungsdurchsuchung, aber sie stehen mit Eingriffen in den Schutz des Art. 13 GG in keiner Beziehung. Denn die Unverletzlichkeit der Wohnung schützt die „durch die Abgrenzung der Wohnung vermittelte – physische – räumliche Privatsphäre" gegen ein Eindringen darin von außen, jedoch keine Speichermedien eines informationstechnischen Systems, nämlich „einen virtuellen Raum".[335] Hier handelt es sich daher eher um den Schutz der Privatsphäre durch das Recht auf informationelle Selbstbestimmung oder das Computer-Grundrecht und ggf. die Gewährleistung des Telekommunikationsgeheimnisses. Hierbei wird für die im Herrschaftsbereich der Anbieter vorhandenen Daten dem Schutz durch Art. 10 Abs. 1 GG deshalb vorzugsweise Rechnung getragen, weil er gegenüber den anderen Grundrechten eine spezielle Garantie darstellt.[336]

---

[331] *Brodowski/Eisenmenger*, ZD 3/2014, 119, 121; auch *Sieber*, 69. DJT 2012, C 107: ein virtueller Raum.

[332] *Dalby*, CR 2013, 361, 367; vgl. *Kudlich*, GA 2011, 193, 207: Hierbei handelt es sich um eine Art Outsourcing von Computerdiensten auf dezentralen Systemen, deren größere Flexibilität, Kapazität und Lastverteilung vom Kunden genutzt wird.

[333] *Sieber*, 69. DJT 2012, C 106: Beim Cloud-Computing sind die Dateien des Verdächtigen nicht mehr auf dessen eigenem Rechner, sondern (oft nur noch) auf den Systemen eines Dienstleisters gespeichert.

[334] In neuerer Zeit führt dieser Dienst über eine bloße Verteilung des Speicherplatzes hinaus zur Auslagerung ganzer Benutzeroberflächen (*Roggan*, StV 2017, 821, 823). In diesem Fall gibt es für die Benutzung keinen Unterschied mehr, ob die Daten auf einem lokalen PC oder auf einem externen Cloud-Server gespeichert sind.

[335] *BVerfGE* 120, 274, 309 ff.; *Brodowski/Eisenmenger*, ZD 3/2014, 119, 121.

[336] *Brodowski/Eisenmenger*, ZD 3/2014, 119, 121 a. E. und weiter 122: Ein „Zugriff auf räumlich getrennte Speichermedien nach § 110 Abs. 3 StPO" ist am Maßstab des Art. 10 GG zu messen.

III. Ermächtigungsgrundlagen

Für den „heimlichen" Zugriff auf die serverbasiert gespeicherten Telekommunikationsinhalte oder (Inhalts-)Daten und ihre Erhebung sind *de lege lata* nur §§ 99, 100a oder 100 b StPO anzuwenden. Im Schrifttum wird die Anwendbarkeit von § 99 oder § 100a StPO für E-Mails und soziale Netzwerke einerseits (vgl. unten 1.) und diejenige von § 100a oder § 100b StPO für Cloud-Computing andererseits (vgl. unten 2.) erörtert.

1. Zugriff auf beim E-Mail- und Soziales-Netzwerk-Server gespeicherte Nachrichteninhalte

a) Anwendbarkeit von § 99 StPO

(1) Ist § 99 StPO für einen Zugriff auf beim E-Mail-Server gespeicherte Nachrichteninhalte „direkt" heranzuziehen? Nach einer Meinung kann die E-Mail ohne Schwierigkeiten vom sprachlichen Verständnis her, nämlich ohne damit die mögliche Grenze des Wortsinns in der Auslegung zu überschreiten, unter den Begriff der Postsendungen i. S. d. § 99 StPO subsumiert werden, weil es auch hierbei – wie bei der herkömmlichen Post – um eine Sicherstellung während der Beförderungsphase geht.[337] Nach h. M. bezeichnen dagegen „Postsendungen" ausschließlich körperliche Gegenstände, und auch „Telegramme" werden beschränkend ausgelegt, sodass E-Mails und SNS-Nachrichten nicht unter den Begriff der Postsendungen und Telegramme zu subsumieren seien. Vor allem sei der Wortlaut „Telekommunikation" seit dem BegleitG zum TKG, das am 24. Dezember 1997 in Kraft trat, in § 100a StPO ausdrücklich verankert.[338]

Zum anderen ist es problematisch, ob § 99 StPO hierfür „entsprechend" gelten kann. Dafür hat der *BGH* in seiner Entscheidung vom 31. März 2009 über die Beschlagnahme von E-Mails bei einem E-Mail-Provider gesprochen:

> „(Vielmehr) ist die Beschlagnahme … auch unter Berücksichtigung des heutigen Kommunikationsverhaltens in jeder Hinsicht vergleichbar mit der Beschlagnahme anderer Mitteilungen, welche sich zumindest vorübergehend bei einem Post- oder Telekommunikationsdienstleister befinden, beispielsweise von Telegrammen, welche gleichfalls auf dem Telekommunikationsweg dorthin übermittelt wurden. Daher können beim Provider gespeicherte … E-Mails – auch ohne spezifische gesetzliche Regelung – jedenfalls unter den Voraussetzungen des § 99 StPO beschlagnahmt werden. … muss aber gewährleistet sein,

[337] *Bär*, MMR 2003, 679, 681.

[338] *Neuhöfer*, JR 2015, 21, 26: Aliud-Verhältnis zwischen Brief- und Telekommunikationsgeheimnis, auch bei den Ermächtigungsgrundlagen; auch *Brodowski*, JR 2009, 402, 408; a. A. *Bär*, MMR 2003, 679, 681: „*Nachdem der Gesetzgeber bei der Neufassung des § 99 StPO durch das BegleitG zum TKG von 1997 als Adressat einer Beschlagnahme neben Unternehmen, die Postdienste erbringen, auch ausdrücklich die Anbieter von TK-Diensten aufführt, bestehen daher hier keine Zweifel, auch die Internetprovider darunter einzuordnen.*"

dass eine Maßnahme nach § 99 StPO auch durchsetzbar ist. Deshalb gilt auch hier der in § 95 Abs. 1 und 2 StPO seine Ausprägung gefundene allgemeine Grundsatz, …“[339]

Darauf folgend hat das *AG Reutlingen* im Jahr 2011 das Denken des *BGH* fortgeführt, sodass es im Ermittlungsverfahren wegen des Verdachts einer Beihilfe zum Wohnungseinbruchsdiebstahl die Beschlagnahme vollständiger Registrierungsdaten und vollständiger Datensätze einschließlich ein- und ausgehender sowie als Entwürfe erstellter Nachrichten („Messages“, „Chats“, „Friends“, „Notes“, „sämtliche Lichtbilder“ etc.), die unter dem *Facebook*-Konto des Beschuldigten gespeichert waren, in entsprechender Anwendung von § 99 StPO ohne sein Wissen angeordnet hat.[340]

Grundlegend ergibt sich dieser Blickwinkel des *BGH* und des *AG Reutlingen* aus der Erkenntnis, dass der E-Mail-Verkehr nicht der Informationsübermittlung via Fernsprecher, vielmehr dem traditionellen Postverkehr vergleichbar ist.[341] Für die Ermittlungsbehörden ist dies in mancherlei Hinsicht vorteilhaft. Denn wenn die Nachrichteninhalte beim E-Mail- und SNS-Server unter den Voraussetzungen des § 99 StPO – heimlich – beschlagnahmt werden können, fehlt es dabei nicht nur an formellen Hürden hinsichtlich der Schwere der Straftat, des Verdachtsgrades und der Subsidiarität, sondern auch hinsichtlich des Kernbereichsschutzes.[342]

---

[339] *BGH* NJW 2009, 1828; abw. *LG Ravensburg* MMR 2003, 679: in analoger Anwendung der §§ 94, 98 und 99 StPO.

[340] *AG Reutlingen*, ZD 4/2012 178 = StV 2012, 462: „*Diese beim Provider … befindlichen und sicherzustellenden Messages und Chat-Nachrichten sind insoweit einer Briefsendung oder einem Telegramm im Gewahrsam des Postdienstleisters vergleichbar und damit in entsprechender Anwendung der Voraussetzungen des § 99 StPO zu beschlagnahmen*“; krit. *Meinicke*, StV 2012, 462, 463; *Neuhöfer*, ZD 4/2012 178; *Zimmermann*, JA 5/2014, 321, 327.

[341] Dies zeigt der Beschluss von *LG Ravensburg* aus dem Dezember 2002 deutlicher (MMR 2003, 679): „*Das E-Mail ersetzt nicht den Schriftverkehr, sondern vereinfacht ihn. … Durch die E-Mail-Technik wird der Briefverkehr nicht ersetzt, sondern verkürzt. Schon das Wortgebilde E-Mail zeigt, dass es sich um Post (das deutsche Wort Post wird durch das englische Wort Mail ersetzt) handelt. Statt schriftlicher Post liegt elektronische Post vor.*“ Zum anderen hat der *BGH* in der Mitte der 90er-Jahre, als die Verwendung von E-Mails noch nicht üblich war, in seiner Entscheidung, den Antrag des Generalbundesanwaltes zu prüfen, um auf die in den Mailboxen gespeicherten Daten heimlich zuzugreifen, entschieden, dass ein derartiger Zugriff unter den Voraussetzungen der Telefonüberwachung nach § 100a StPO grundsätzlich zulässig ist (NJW 1997, 1934 1935): „*Der Bezug des Zugriffs auf eine … Mailbox zur Telefonüberwachung ergibt sich aus folgendem: Soweit es um den Zugriff auf gesicherte Daten geht, stellt das Endgerät mit dem Speichermedium einen Teil der Fernmeldeanlage dar, …. Nachrichtenübermittlung von und zu dieser Mailbox ist deshalb … Fernmeldeverkehr i. S. der §§ 100a, 100b StPO (a. F.). Auch der heimliche … vorgenommener Zugriff auf den Datenbestand der Mailbox erfolgt – wie auch sonst bei der Telefonüberwachung – ausschließlich über die Fernmeldeanlage von außen.*“ Vermutlich hat das Gericht in der Vergangenheit, als die Übermittlung/Kommunikation von Text und Sprache klar in Post und Telefon unterteilt war, § 99 StPO als Ermächtigung für die Überwachung der Textkommunikation und § 100a StPO als die für die Überwachung der Sprachkommunikation angesehen.

[342] *Zimmermann*, JA 5/2014, 321, 324.

(2) Dass der heimliche Zugriff auf die auf E-Mail- oder SNS-Server gespeicherten Nachrichten nach § 99 StPO direkt oder analog zulässig ist, verstößt aber gegen den Grundsatz der Verhältnismäßigkeit und ist auch unter rechtssystematischem Gesichtspunkt unvertretbar.[343] Heute besteht vor allem keine vergleichbare Situation mehr zwischen der Beschlagnahme der Postsendungen und Telegrammen nach § 99 StPO und der Sicherstellung der Nachrichteninhalte beim Server der Provider der TK-Dienste.[344] Nun ersetzen der E-Mail-Verkehr und die SNS-Kommunikation aus funktioneller Sicht teilweise die herkömmliche Post, jedoch teilweise auch das Telefon. Hier werden die Nachrichten einfach tatsächlich in Echtzeit kommuniziert und ihre Inhalte betreffen alle Lebensbereiche einschließlich der Intimsphäre. Außerdem kann der Zugriff auf die Nachrichten beim Server ggf. eine große Datenmenge betreffen, die bis hin zur Bildung von Persönlichkeitsprofilen führen kann, ferner eine Unzahl unverdächtiger Dritter.[345] Hingegen setzt § 99 StPO die Beschlagnahme von maximal nur einigen Nachrichten voraus. Schließlich sind im Hinblick auf die rechtliche Bewertung unter Berücksichtigung der IuK-Technologie E-Mails und SNS-Nachrichten beim Server wesentlich anders zu behandeln als herkömmliche Postsendungen und Telegramme.[346] Hinzu kommt, dass im Hinblick auf die erhöhten Anforderungen, die das *BVerfG* für „offenen" Zugriff auf serverbasiert gespeicherte E-Mails in seiner Rechtsprechung vom 16. Juni 2009 – nach dem Verhältnismäßigkeitsgrundsatz – aufstellt, die Kautelen der §§ 99 f. StPO für „verdeckten" Zugriff darauf keinesfalls genügen dürften.[347]

b) Anwendbarkeit von § 100a StPO und Anforderung an eine Neuregelung

(1) Nach den oben angeführten Argumenten kann sich der heimliche Zugriff auf bei E-Mail- und SNS-Servern gespeicherte Nachrichteninhalte derzeit nur auf § 100a StPO stützen. Laut Schrifttum liegt dies daran, dass er den Schutz des Art. 10 Abs. 1 GG berühre[348] oder § 100a StPO *de lege lata* hierfür die einzig denkbare Ermäch-

[343] Dazu *Neuhöfer*, JR 2015, 21, 26.

[344] Für die E-Mail *Singelnstein*, NStZ 2012, 593, 597 am Anfang; *Neuhöfer*, JR 2015, 21, 27; für soziale Netzwerke *Neuhöfer*, ZD 4/2012 178, 179 [Tz. 1.]: Es gibt nicht eine vergleichbare Interessenlage als Analogievoraussetzung.

[345] *Singelnstein*, NStZ 2012, 593, 597 [Fn. 66]; *Neuhöfer*, JR 2015, 21, 27.

[346] *Brodowski*, JR 2009, 402, 408; dazu *Zimmermann*, JA 5/2014, 321, 327: Die Nachrichteninhalte, die bei sozialen Netzwerken wie *Facebook* (als neuartige Mischform) ausgetauscht oder angezeigt werden, sind angesichts der Vielfalt und des Umfangs der Daten zumindest nicht mit den Postsendungen oder Telegrammen i. S. d. § 99 StPO vergleichbar.

[347] *Kasiske*, StraFo 6/2010, 228, 234.

[348] Für einen verdeckten Zugriff auf E-Mails beim ISP *Kudlich*, GA 2011, 193, 203; *Roxin/Schünemann*, § 36 Rn. 6; vgl. *Kasiske*, StraFo 6/2010, 228, 234: „Da sowohl hinsichtlich der betroffenen Grundrechte als auch im Hinblick auf den heimlichen Charakter der Maßnahme in einem solchen Fall keine Unterschiede zu einer TKÜ nach § 100a StPO ersichtlich sind, dürfte diese Norm deshalb in diesen Fällen auch die einschlägige Eingriffsgrundlage darstellen."

tigungsgrundlage sei.[349] Da es sich u. a. in struktureller Hinsicht bei der in Rede stehenden Sache um einen „heimlichen Zugriff" auf die „außerhalb des Herrschaftsbereichs des Betroffenen" liegenden „Nachrichteninhalte" handelt, kann sie i. R. d. geltenden Vorschriften mit den Eingriffsvoraussetzungen des § 100a StPO übereinstimmen. Für die Anordnung einer solchen Maßnahme muss daher ein qualifizierter Verdacht der in § 100a Abs. 2 StPO aufgeführten Straftaten vorausgesetzt werden[350], und ihr Verfahren unterliegt gesetzlichen Beschränkungen nach § 100d Abs. 1 und 2 StPO zum Schutz des Kernbereichs privater Lebensgestaltung und strengen Sicherungen nach § 100e StPO wie qualifizierter Eilkompetenz und deren Wirksamkeit sowie Dauer, Form und Begründung der Anordnung.

Für die Umsetzung dieser Maßnahmen wird eine Mitwirkung des Dienstanbieters in aller Regel verlangt (vgl. § 100a Abs. 4 StPO).[351] Insofern ist es umstritten, ob dieser Zugriff „zumindest ‚mit Wissen' bzw. ‚mit Hilfe' des Dienstanbieters" erfolgen soll.[352] Wie schon erwähnt ist seine Kenntnisnahme bei der Entscheidung über Heimlichkeit der Maßnahme weder erforderlich noch maßgeblich (vgl. oben A. II. 1.). Danach ist bezüglich seiner Mitwirkung der Wortlaut der StPO durchaus offen formuliert (vgl. § 100e Abs. 3 S. 2 Nr. 5 und § 100a Abs. 4 StPO = § 100b Abs. 2 S. 2 Nr. 2 und Abs. 3 StPO a. F.). Die Vorschriften sehen streng genommen nur die Mitwirkungspflicht des Anbieters – bei Bedarf – vor und sagen nichts darüber aus, ob die Ermittlungen immer auf eine bestimmte Weise abzulaufen haben.[353] So sind die Strafverfolgungsbehörden berechtigt, den Zugangscode zum E-Mail- oder SNS-Konto ohne seine Hilfe aus eigener Kraft zu gewinnen und die Überwachung durchzuführen;[354] etwa wenn die Behörden – nicht üblich, aber – auf andere Weise,

[349] *Neuhöfer*, ZD 4/2012 178, 179 [Tz. 4.]; *Zimmermann*, JA 5/2014, 321, 327. Letztlich machen sie eine gesetzgeberische Lösung *de lege ferenda* geltend.

[350] Demzufolge könnte im Fall des *AG Reutlingen*, dass zur Aufklärung eines Wohnungseinbruchsdiebstahls, der nicht in den Straftatenkatalog des § 100a Abs. 2 StPO fällt, eine Beschlagnahme ohne Wissen des Betroffenen angeordnet wurde (siehe Fn. 340), die Maßnahme der Beweissicherung nur nach §§ 94 ff. StPO angeordnet und durchgeführt werden kann, nicht nach § 99 oder § 100a StPO (vgl. *Zimmermann*, JA 5/2014, 321, 327 und dazu 324: Beispielsfall 1 [Verdacht einer allein begangenen Vergewaltigung]).

[351] BT-Drs. 18/12785, S. 48: Er erfolgt zumeist i. d. R. bei den Telekommunikationsunternehmen; vgl. für den eingehenden Vorgang und Inhalt, *Bruns*, KK-StPO, § 100a, Rn. 36 und 41.

[352] Genau genommen überschneiden sich zwar die (zwei) Fragen teilweise, ob die TKÜ nach § 100a StPO mit „Wissen" bzw. mit „Hilfe" des Anbieters vorzunehmen ist, jedoch sind sie nicht völlig gleich. Denn nach dem Wortlaut des Abs. 4 ist er nur zur Mitwirkung verpflichtet, daneben muss er „zum Zeitpunkt der Durchführung" der Maßnahme nicht unbedingt von ihr wissen.

[353] *Kudlich*, JA 4/2010, 310, 312; *ders.*, GA 2011, 193, 207; *Wolter/Greco*, SK-StPO, § 100b Rn. 19; auch *Zerbes/El-Ghazi*, NStZ 2015, 425, 432.

[354] BT-Drs. 16/5846, S. 47; M-G/*Schmitt*, StPO, § 100a Rn. 8; *Singelnstein*, NStZ 2012, 593, 599 und 600; vgl. dazu *Bruns*, KK-StPO, § 100a Rn. 37: Dies sollte im Anordnungsbeschluss klargestellt werden (vgl. § 100e Abs. 3 S. 2 Nr. 3 StPO); a. A. *Wolter/Greco*, SK-StPO, § 100b Rn. 19.

z. B. bei der Durchsuchung der Wohnung oder der Durchsicht von Papieren das Passwort gewinnen.[355] Die Ermittlungsbehörden verlangen jedoch regulär vom Anbieter die Auskunft der Codes und greifen damit auf den Server zu. Nunmehr ist dies nur unter den Voraussetzungen des § 100j Abs. 1 S. 2, Abs. 2 – 5 StPO gestattet.[356] Dabei ist die Verwendung von Benutzerkennung und Passwort strikt zu beschränken. Dies gilt u. a. für den Fall, dass die Ermittlungsbehörden mittels der Codes auf das Konto des Beschuldigten „wiederholt" zugreifen. Dann kann nämlich die einfache TKÜ nach § 100a Abs. 1 S. 1 StPO in der Tat auf die Quellen-TKÜ nach § 100a Abs. 1 S. 2 und 3 StPO ohne Beschränkungen des § 100a Abs. 5 und 6 StPO bzw. auf die Online-Durchsuchung nach § 100b StPO übertragen werden. Dies läuft der Verhältnismäßigkeit und auch dem Richtervorbehalt zuwider. Um diese Bedenklichkeit und die Gefahr der Übertragung zu vermeiden wird die Intervention des Dienstanbieters, die in § 100b Abs. 4 S. 2 StPO a. F. vorgesehen ist, der bis zum 31. Dezember 2007 gültig war, jedoch ersatzlos gestrichen wurde,[357] berücksichtigt werden.[358] Hierbei kann er auch zum Datenschutz seiner Kunden rechtlich gestattete sachgemäße Vorsorge treffen. Darüber hinaus darf ein solcher Zugriff bei den Kommunikationsteilnehmern selbst, d. h. in einer Weise, nicht erfolgen, dass er über von ihnen genutzte PCs oder Smartphones zum Server gelangt. Hierbei können nämlich weder die Tatbestände der Quellen-TKÜ nach § 100a Abs. 1 S. 2 und 3 StPO noch die technischen Vorgaben in Abs. 5 eingehalten werden.

(2) Insofern stellt sich aber die Frage, ob die Eingriffsvoraussetzungen und die verfahrensrechtlichen Vorkehrungen gemäß §§ 100a, d und e StPO noch ausreichend sind.[359] Dies ist auf die heutige Situation zurückzuführen, dass E-Mail und soziale Netzwerke bereits von Bürgern sowohl privat als auch beruflich weit verwendet werden und alle in der Zwischenzeit entstandenen Daten unbegrenzt auf den Servern des Dienstanbieters gespeichert werden. Allerdings ist nach dem Verhältnismäßigkeitsgrundsatz der dauerhafte Zugriff auf den gesamten Datenbestand bzw. die Beschlagnahme sämtlicher gespeicherter Daten i. d. R. nicht erlaubt und je nach den Umständen des Einzelfalls müssen unterschiedliche, miteinander kombinierbare Möglichkeiten der materiellen Datenzuordnung, die etwa themen-, zeit- oder personenbezogen oder mittels bestimmter Suchbegriffe erfolgen, stets in Betracht gezogen werden.[360] Hinsichtlich der Eingriffsintensität stellt sich aber daneben die Frage, ob entsprechende Schutzvorkehrungen „gesetzlich" zu treffen sind; insb. weil

[355] *Klesczewski*, ZStW 123 (2011), 737, 752.

[356] Jedoch kommt § 100j Abs. 3 S. 1 – 2 StPO, der einen Richtervorbehalt zur Bereitstellung des Zugangscodes regelt, unter Verhältnismäßigkeitsgesichtspunkten infrage (vgl. oben B. III. 5. b)).

[357] Vgl. § 100b Abs. 4 S. 2 StPO bis zum 31. 12. 2007 geltenden Fassung: Die Beendigung (der Maßnahmen) ist dem Richter und dem nach Absatz 3 Verpflichteten mitzuteilen.

[358] Vgl. *Wolter/Greco*, SK-StPO, § 100b Rn. 19; auch *Singelnstein*, NStZ 2012, 593, 600: sehr gute systematische Gründe.

[359] Auch *Neuhöfer*, JR 2015, 21, 28.

[360] Vgl. *BVerfG* 124, 43, 67 f.

sich ein derartiger Eingriff mit Blick auf die Vielfalt und den Umfang der zu erhebenden Daten von einer Telefonüberwachung unterscheidet, die i. d. R. nur auf punktuelle Telekommunikationsinhalte oder in einer kurzen Zeit vorgenommen wird.[361] Außerdem ist diese Fragestellung auch in rechtssystematischer Hinsicht auf den ersten Blick deswegen nachvollziehbar, weil §§ 100a, d und e StPO für die heimliche Erhebung von gespeicherten „Inhaltsdaten" mit milderen Eingriffsvoraussetzungen und Sicherungen als §§ 100g Abs. 2 und 101a StPO für dieselbe von gespeicherten „Verkehrsdaten" verbunden sind.

Diesbezüglich erklärt sich das *BVerfG* noch nicht ausdrücklich.[362] Es hat aber in der Prüfung der Verhältnismäßigkeit der obigen Entscheidung von 2009 nochmals klargestellt, dass i. R. d. verdeckten Zugriffs auf gespeicherte Nachrichteninhalte eine Heimlichkeit, eine Relevanz der Daten für Dritte und ein Fehlen von Einwirkungsmöglichkeit die Schwere eines Eingriffs erhöhen,[363] Kommunikationsinhalte im Vergleich zu Verkehrsdaten in höherem Maße schutzwürdig sind[364] und Einzelmaßnahmen zur Erlangung der beim Provider gespeicherten Verkehrsdaten auf Straftaten von erheblicher Bedeutung zu beschränken sind.[365] Außerdem hat das Gericht im Urteil zur VDS vom 2. März 2010 entschieden, dass eine solche Datenerhebung, die bis in die Intimsphäre hineinreichende inhaltliche Rückschlüsse bzw. die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile jeden Bürgers ermöglicht, einen besonders schweren Eingriff mit sich bringt,[366] und dass daher zu dieser Datennutzung zum Zwecke der Strafverfolgung zumindest der durch bestimmte Tatsachen begründete Verdacht einer schweren Straftat[367] sowie die Gewährleistung eines effektiven Rechtsschutzes und adäquater Sanktionen[368] erforderlich sind.[369] Aus diesen Entscheidungsinhalten ist zu schließen, dass die Anordnungsvoraussetzungen und Verfahrensvorkehrungen der hier in Rede stehenden Eingriffe mindestens die Anforderungen von §§ 100a, d und e StPO erfüllen sollten. Zum Schluss kann eine solche Maßnahme *de lege lata* nach diesen Vorschriften vorgenommen werden, es ist jedoch aus Sicht des Rechtssystems sinnvoller, in

[361] *Neuhöfer*, JR 2015, 21, 28 [Tz. f)].

[362] *Zimmermann*, JA 5/2014, 321, 325.

[363] *BVerfGE* 124, 43, 62 [Rn. 68].

[364] *BVerfGE* 124, 43, 63 [Rn. 70].

[365] *BVerfGE* 124, 43, 65 [Rn. 75].

[366] *BVerfGE* 125, 260, 319 [Rn. 211].

[367] *BVerfGE* 125, 260, 328 f. [Rn. 228].

[368] *BVerfGE* 125, 260, 337 ff. [Rn. 246 ff.].

[369] Daneben erbringt das *BVerfG* im Urteil das Risiko von Bürgern, ohne Anlass weiteren Ermittlungen ausgesetzt zu werden, die Missbrauchsmöglichkeiten und ein diffus bedrohliches Gefühl des Beobachtetseins als Gründe des besonderen Gewichts des Eingriffs (*BVerfGE* 125, 260, 319 f. [Rn. 212]), verlangt dementsprechend von Aufsichtsbehörden und Dienstanbietern die gesetzliche Gewährleistung eines besonders hohen Standards der Datensicherheit (a. a. O. 325 ff. [Rn. 221 ff.]).

Zukunft eine eigenständige Ermächtigung zu schaffen.[370] Erforderlich sind etwa ein Straftatenkatalog, der mit dem Katalog für die VDS in § 100g Abs. 2 S. 2 StPO vergleichbar ist, Sicherungen, die dem Verfahren nach § 101a StPO gleichkommen oder Regelungen zum Schutz des Kernbereichs, der zu den Inhalten des § 100d Abs. 3 und 4 StPO parallel ist.

c) Sonstige verdeckte Ermittlungsmaßnahmen bei geschlossenen sozialen Netzwerken und Internet-Foren

Wie bereits bemerkt, greift die Internetaufklärung bei der Ermittlungsbehörde i. d. R. nicht in Grundrechte ein, oder auch wenn sie in sie eingreift, wird die Eingriffsintensität meist als gering eingeschätzt, und daher ist dies aufgrund der Ermittlungsgeneralklauseln der §§ 161, 163 StPO zu rechtfertigen (vgl. oben II. 2.). Die Online-Streife durch anonym und pseudonym eingesetzte NoeP oder V-Leute ist ohne eine spezielle Ermächtigung möglich.[371] Dies kann jedoch für die sozialen Netzwerke und Internet-Foren nicht gelten, in denen ein spezielles Vertrauensverhältnis zwischen den Kommunikationsbeteiligten vorliegt. Dafür ist dem Einsatz eines (virtuellen) Verdeckten Ermittlers nach § 110a StPO Rechnung zu tragen.[372] Allerdings liegt i. d. R. kein Eingriff in das Recht auf informationelle Selbstbestimmung schon dann vor, wenn sich ein Ermittler unter einer Legende nach § 110a StPO in eine Kommunikationsbeziehung zu einem Grundrechtsträger begibt. Aber, wenn er dabei ein schutzwürdiges Vertrauen des Betroffenen in die Identität und die Motivation seines Kommunikationspartners ausnutzt, um persönliche Daten zu erheben, die er ansonsten nicht erhalten würde, so besteht ein Eingriff in das Recht.[373] Die Schutzwürdigkeit dieses Vertrauens hängt davon ab, ob der Betroffene darauf vertrauen darf, dass Identität und Motivation der verdeckt ermittelnden Person authentisch sind.[374] Trotz allem ist es aber in der Praxis wegen der Anonymität im

---

[370] *Neuhöfer*, ZD 4/2012 178, 179 [Tz. 4.]; *ders.*, JR 2015, 21, 28 [Tz. f)]; *Zimmermann*, JA 5/2014, 321, 327: eine technikunabhängige Datenzugriffs-Generalklausel.

[371] *Singelnstein*, NStZ 2012, 593, 600; *Soiné*, NStZ 2014, 248, 249 ff.: unter pseudonymer Kennung. In der Praxis dürfte der Schwerpunkt auf Einsätzen von NoeP liegen (*Soiné*, a. a. O. 251 [Tz. IV.]).

[372] *Bruns*, KK-StPO, § 110a Rn. 7; *Kudlich*, GA 2011, 193, 199: bei sozialen Netzwerken; *Sieber*, 69. DJT 2012, C 126; *Singelnstein*, NStZ 2012, 593, 600. Vgl.: Nach der Rspr. des *BGH* ist ein verdecktes Verhör dem Ermittler gestattet, jedoch nicht einem NoeP und den V-Leuten (*BGHSt* 55, 138, 143 f. [Rn. 18]: Ein verdecktes Verhör mit dem Ziel, eine selbstbelastende Äußerung eines noch nicht förmlich vernommenen Beschuldigten herbeizuführen, erscheint als Ermittlungshandlung von nicht unerheblicher Eingriffsintensität; *Roxin/Schünemann,* § 37 Rn. 5 und 10). Nicht gedeckt ist dagegen von § 110a StPO die Maßnahme, dass ein Ermittler unter heimlicher Verwendung der Identität einer realen Person in deren sozialem Umfeld Kontakt zu Dritten aufnimmt, sog. „verdeckte Identitätsübernahme" (*Sieber*, a. a. O.).

[373] *BVerfGE* 120, 274, 345 [Rn. 310]; *Klesczewski*, ZStW 123 (2011), 737, 753: In diesem Fall liegt eine Art Rasterfahndung vor.

[374] *Soiné*, NStZ 2014, 248, 249 [Tz. 4.]. Daher ist i. d. R. das Vertrauen auf Nutzer von Pseudonymen wie Nicknamen nicht schutzwürdig, dagegen besteht das schutzwürdige Ver-

Internet ungeklärt, ob und wann schutzwürdiges Vertrauen in einen Kommunikationspartner entstehen kann,[375] darüber hinaus kommt all dies eher kaum in Betracht.[376]

2. Zugriff auf beim Cloud-Speicher gespeicherte Daten

(1) Die Nutzung von Cloud-Computing, das zu einer neuen Art von „TK-Diensten" gehört, wird in jüngster Zeit erheblich erweitert und § 100b StPO für verdeckte Online-Durchsuchung wurde erst 2017 in die StPO eingefügt. Bis dahin wurde in der Literatur hauptsächlich diskutiert, ob der Zugriff auf die im Cloud-Speicher gespeicherten Daten aufgrund des § 100a StPO zu rechtfertigen ist: insb. in Hinsicht darauf, dass das Cloud-Computing unter dem Begriff „Telekommunikation" i. S. d. § 100a Abs. 1 StPO subsumiert werden kann.[377] Dies ist im Wesentlichen darauf zurückzuführen, dass nur § 100a StPO seinerzeit auf ihn – direkt oder analog – anwendbar war.[378]

Nach h. M. kann aber der verdeckte – unmittelbare – Zugriff auf die im Cloud-Speicher gespeicherten Daten und ihre Erhebung unter den Voraussetzungen und nach dem Verfahren der verdeckten Online-Durchsuchung (vgl. §§ 100b, d und e

trauen dann, wenn sich Kommunikationspartner persönlich unter Klar- und Nicknamen kennen oder wenn polizeiliche Ermittlungen über einen längeren Zeitraum unter einer Legende vorgenommen werden, z. B. zu Treffen in der realen Welt führen; somit kann dabei in das informationelle Selbstbestimmungsrecht eingegriffen werden (a. a. O.).

[375] *Sieber*, 69. DJT 2012, C 126.

[376] *Soiné*, NStZ 2014, 248, 249 f.

[377] Vgl. *Sieber*, 69. DJT 2012, C 106 ff.; *Dalby*, CR 2013, 361, 368.

[378] Nach dem formalen Gesichtspunkt, dass Cloud-Nutzer und -Provider zwei unterschiedliche Personen sind, besteht zwischen ihnen eine Telekommunikationsbeziehung, daher ist § 100a StPO darauf anzuwenden (sog. „Kommunikationslösung"; *Kudlich*, GA 2011, 193, 199; beim Up- und Download; *Singelnstein*, NStZ 2012, 593, 594 f.: auch beim Online-Banking; vgl. *Sieber*, 69. DJT 2012, C 107). Nach h. M. kann § 100a StPO hingegen deswegen nicht angewendet werden, weil es hierbei – anders als bei (echten) Kommunikationsvorgängen – keine Kommunikation von Dateninhalten gibt (eine funktionale Betrachtungsweise; *Dalby*, CR 2013, 361, 368; auch M-G/*Schmitt*, StPO, § 100a Rn. 14f; *Roggan*, StV 2017, 821, 823; *Sieber*, 69. DJT 2012, C 107; vgl. *Roxin/Schünemann,* § 36 Rn. 4: TK (des § 100a StPO) setzt das Vorhandensein eines menschlichen Kommunikationspartners voraus). Der Cloud-Speicher wird nämlich i. d. R. nicht zur Kommunikation zwischen Kommunikationspartnern, sondern zur Ersetzung oder Ergänzung lokaler Datenspeicher verwendet (vgl. oben II. 3.). Insofern hat die *3. Kammer* des *2. Senats* des *BVerfG* jedoch in letzter Zeit entschieden, dass auch die Nutzung des Internets durch Abrufen von Webseiten, nämlich „Surfen" und die Eingabe von Suchbegriffen, als „TK" i. S. d. § 100a StPO anzusehen ist (NJW 2016, 3508, 3509 f. [Rn. 29 ff.]). Nach diesem Beschluss ist der § 100a StPO auch auf das Cloud-Computing deswegen anzuwenden, weil damit der Telekommunikationsbegriff von einer sozialen Interaktion im Sinne eines (Daten)Austausches zwischen mindestens zwei Individuen losgelöst wird (*Roggan*, a. a. O.). Gleichwohl ist es zweifelhaft, ob sich der verdeckte Zugriff auf den Cloud-Speicher unter Verhältnismäßigkeitsgesichtspunkten noch auf § 100a Abs. 1 StPO stützen kann, insb. weil er in qualitativer Hinsicht noch eine besonders hohe Eingriffsintensität hat (zust. *Roggan*, a. a. O.). Wie schon erwähnt ist die Ermächtigung nicht mehr von einschlägigem Grundrecht abhängig, sondern sie ist nach der eigenen Eingriffsintensität zu bestimmen.

StPO), die den heimlichen Eingriff in lokale informationstechnische Systeme und die Erhebung dort gespeicherter Daten darstellt, angeordnet werden.[379] Der Cloud-Speicher stellt die virtuelle Festplatte dar und so kann der Zugriff darauf i. d. R. über die Inhalte der Individualkommunikation hinaus die Daten aus dem Kernbereich privater Lebensgestaltung sichtbar machen und weiter bis hin zu einer Bildung eines Persönlichkeitsprofils des Nutzers führen. Gerade aus diesem Grund ist die heimliche – umfangreiche – Erhebung der Cloud-Daten viel eingriffsintensiver als die allgemeine TKÜ nach § 100a Abs. 1 StPO, sodass sie sowohl qualitativ als auch funktional mit der Online-Durchsuchung nach § 100b StPO vergleichbar ist.[380] Dies ergibt sich auch aus den Entscheidungen des *BVerfG.* Das Gericht hat das zuerst in seinen Entscheidungen über Online-Durchsuchung von 2008 und über die Verfassungsmäßigkeit von §§ 100a und b StPO a. F. (= §§ 100a, d und e StPO n. F.) vom 12. Oktober 2011 mittelbar zum Ausdruck gebracht. Im ersteren Fall hat es hat entschieden, dass das Computer-Grundrecht anzuwenden ist, wenn die Eingriffsermächtigung Systeme erfasst, die eine noch größere Vielzahl und Vielfalt von Daten enthalten können,[381] und im letzteren Fall hat es angenommen, dass i. R. d. Schutzes des Kernbereichs privater Lebensgestaltung die inhaltliche TKÜ keine so strenge Kontrolle wie bei der Online-Durchsuchung (bzw. Wohnraumüberwachung) verlangt.[382] Daran anschließend hat *BVerfG* in der Entscheidung zum BKAG von 2016 ausdrücklich erklärt, dass die heimliche Online-Durchsuchung ein Mittel für die Überwachung des Cloud-Computings sein kann:

> „… die geheime Durchführung von Online-Durchsuchungen, mit denen private, von den Betroffenen auf eigenen oder vernetzten fremden Computern (wie etwa der sog. Cloud) abgelegte oder hinterlassene Daten erhoben und deren Verhalten im Netz nachvollzogen werden kann."[383]

Da hierbei (inländische) Cloud-Dienstanbieter „anderen Personen" i. S. d. § 100b Abs. 3 S. 2 zugerechnet werden können, ist ein derartiger Zugriff nur dann zulässig, wenn aufgrund bestimmter Tatsachen anzunehmen ist, dass der Beschuldigte das informationstechnische System eines Anbieters benutzt, und dass die Subsidiarität

---

[379] *Bruns*, KK-StPO, § 100b Rn. 13; M-G/*Schmitt*, StPO, § 100b Rn. 10; *Roggan*, StV 2017, 821, 825 f.; auch *Sieber*, 69. DJT 2012, C 107 f.; *Dalby*, CR 2013, 361, 368. Letzte zwei Autoren haben damals die Lösung durch die Schaffung der neuen Ermächtigung zur Online-Durchsuchung verlangt.

[380] M-G/*Schmitt*, StPO, § 100a Rn. 14f, § 100b Rn. 10; *Roggan*, StV 2017, 821, 823; dazu *Sieber*, 69. DJT 2012, C 107 f.: Im Falle der Synchronisation des lokalen Computers mit einem Cloud-Speicher entspricht der heimliche Zugriff auf diesen Speicher funktional der („großen") Online-Durchsuchung.

[381] *BVerfGE* 120, 274, 314 [Rn. 203].

[382] Vgl. *BVerfGE* 129, 208, 249 f. Daraus ist zu entnehmen, dass das Gericht hinsichtlich der Persönlichkeitsrelevanz zwischen persönlich gegenseitig austauschenden und der nur für sich selbst erstellten oder eingesehenen Daten unterscheidet.

[383] *BVerfGE* 141, 220, 303 [Rn. 209].

i. S. d. Nr. 2 vorliegt.[384] Im gerichtlichen Durchsuchungsbeschluss ist zu bestimmen, in welcher Art und Weise die Maßnahme durchgeführt wird, und ob das lokale informationstechnische System oder der Cloud-Speicher zum Gegenstand der Maßnahme gehören.[385] So können die Ermittlungsbehörden im privaten System, das während verdeckter Online-Durchsuchung infiltriert wird, über das Cloud-Konto des Betroffenen auf den Server des Anbieters zugreifen. Ein derartiger Zugriff ist eine Vorgehensweise, die der Ausweitung der Durchsuchung nach § 110 Abs. 3 StPO – die eine offene Maßnahme darstellt – entspricht. Auch hier können die Ermittlungsbehörden mit dem Zugangssicherungscode, der vom Dienstanbieter bereitgestellt wurde, von ihrem Computer aus auf den Cloud-Speicher heimlich zugreifen (vgl. oben 1. b)).

(2) Wenn Cloud-Computing zum Zwecke der Kommunikation verwendet wird, z. B., wenn ein Nutzer den Zugangssicherungscode für den Zugriff auf Cloud-Speicher mit Dritten teilt, so kann die Anwendung von § 100a StPO nach einer Ansicht in Betracht gezogen werden, da hier das bloße Ablegen von serverbasierten (passwortgeschützten) Daten einen Telekommunikationsvorgang darstellen kann.[386] Hierbei wird der Kommunikationsdienst jedoch bloß „atypisch" von den Nutzern verwendet. Gehört diese Fallgestaltung zur TKÜ nach § 100a StPO, so kann dies zu einer unangemessenen Folge führen, dass alle Fälle, in denen ein Passwort an einen Dritten weitergegeben wird, von der Vorschrift erfasst werden können.[387] Können solche Fälle allerdings aufgrund bestimmter Tatsachen angenommen werden, so können sie gesondert berücksichtigt und gemäß § 100a StPO gerechtfertigt werden. Jedoch kann dies in der Praxis nur sehr eingeschränkt nachgewiesen werden.[388] Umgekehrt, wenn ein E-Mail-Nutzer zum Zweck der Datenspeicherung, nicht aber des Datenaustausches über seine E-Mail-Adresse mit sich selbst kommuniziert, d. h. wenn der E-Mail-Server wie ein Cloud-Speicher verwendet wird, dann können die darauf gespeicherten Daten aus dem gleichen Grund gestützt auf § 100a StPO erhoben werden.

---

[384] *Bruns*, KK-StPO, § 100b Rn. 13; M-G/*Schmitt*, StPO, § 100b Rn. 10; *Soiné*, NStZ 2018, 497, 499 f.; vgl. *Roggan*, StV 2017, 821, 825 f.: sofern aufgrund bestimmter Tatsachen anzunehmen ist, dass der Beschuldigte dort Daten speichert (zust. *Soiné*, a. a. O. 500). Vgl.: Insoweit kann § 100b StPO, der als Ermächtigungsgrundlage für den Eingriff in das Computer-Grundrecht geschaffen wird, i. R. d. Cloud-Computings als dieselbe für den Eingriff in Art. 10 Abs. 1 GG dienen.

[385] *Bruns*, KK-StPO, § 100e Rn. 12 und 16; M-G/*Schmitt*, StPO, § 100e Rn. 12 und 15.

[386] *Zimmermann*, JA 5/2014, 321, 326.

[387] *Soiné*, NStZ 2018, 497, 500 am Anfang: ein bloßer Nebeneffekt.

[388] *Dalby*, CR 2013, 361, 368 [Fn. 68]; auch *Brodowski*, JR 2011, 533, 536: nur ausgesprochen restriktiv.

IV. Zusammenfassung und Zwischenergebnisse

Heute werden immer mehr Informationen auf Webseite gespeichert. Daher sollten heimliche Zugriffe auf darauf gespeicherte Inhaltsdaten angesichts der Vielfalt und des Umfangs der zu erhebenden Daten je nach Art von Telekommunikationsdiensten individuell behandelt werden. Der Zugriff auf die Nachrichteninhalte des E-Mail- oder SNS-Servers ist nur unter den Voraussetzungen zumindest der §§ 100a, d und e StPO oder solchen vergleichbaren der §§ 100g Abs. 2 und 101a StPO (*de lege ferenda*) zulässig und der auf die Daten beim Cloud-Speicher ist nach den Voraussetzungen der §§ 100b, d und e StPO möglich. Dabei ist stets die Ausführung des *BVerfG* zu beachten, dass die Freiheitswahrnehmung der Bürger nicht total erfasst und aufgezeichnet werden darf und dies zur verfassungsrechtlichen Identität der *Bundesrepublik Deutschland* gehört.[389]

D. Ermächtigungsgrundlagen für heimliche Ermittlungsmaßnahmen in Südkorea

I. Vorrede – Hintergrundwissen zum Verständnis der Diskussionen in Südkorea

1. Übersicht

(1) Das System der Ermächtigungsgrundlagen zur Beweissicherung im Ermittlungsverfahren in Südkorea ist nicht so abgestuft ausgestaltet und weiter nicht nach der Art der Maßnahme aufgeteilt wie das im 8. Abschnitt des Ersten Buches der StPO (vgl. oben B. I. 1.). Dies ist einerseits auf das koreanische Gesetzgebungsumfeld zurückzuführen, das dazu tendiert, eine konkrete Lösung im Einzelfall zu suchen, indem man der StA und den Gerichten viel Ermessensspielraum einräumt, und andererseits auf die Haltung des *K-VerfG*, die nicht streng bei der Prüfung der Verfassungsmäßigkeit der Ermächtigungen ist. Dies verhindert jedoch teilweise, dass das Rechtsstaatsprinzip in Strafverfahren konkret berücksichtigt wird und die Grundrechte wirksam geschützt werden. Insbesondere ist dies in Hinsicht auf Normenklarheit und Verhältnismäßigkeit nicht ausreichend.

Die „heimlichen Ermittlungsmaßnahmen", die neuerdings in der südkoreanischen Literatur i. d. R. ausführlich behandelt werden, umfassen etwa die TKÜ und die Zensur von Postsendungen, die Erhebung von Verkehrs- und Standortdaten, Bestandsdatenauskunft, das Abhören von nichtöffentlichen Gesprächen, den Einsatz von (eigenständigen) GPS-Trackern. Natürlich werden andere geheime Ermittlungsmethoden wie Online-Durchsuchung und Quellen-TKÜ, IMSI-Catcher, Stille

[389] *BVerfGE* 125, 260, 324.

SMS und der Einsatz verdeckter Ermittler, die in Deutschland diskutiert werden, auch mit ihren Rechtsgrundlagen und den Inhalten der betroffenen Urteile vorgestellt,[390] aber es ist noch nicht zu einer weiter in die Tiefe gehenden Diskussion gekommen. Es gibt auch keinen konkreten Versuch, sie auf parlamentarischer Ebene zu legalisieren. Dafür mag es mehrere Gründe geben, aber u. a. einerseits, weil es – zumindest aus den Inhalten von Rspr. oder Literaturen – nicht klar ist, ob solche Maßnahmen in der Praxis von koreanischen Ermittlungsbehörden oder Nachrichtendiensten verwendet werden,[391] und andererseits, weil i. d. R. – vom Justizministerium und der StA – davon ausgegangen wird, dass sie von bestehenden Vorschriften abgedeckt werden können.[392] Andererseits wird die Erhebung und Verwendung von Zugangssicherungscodes in Südkorea kaum diskutiert. Das liegt daran, dass die vom *BVerfG* verlangten gesetzlichen Sonderanforderungen wie Doppeltürenmodell bzw. dritte Tür in der Literatur oder Rspr. überhaupt nicht berücksichtigt werden. Wichtiger ist vielmehr, ob bei der Erfassung von Bestandsdaten ein Richtervorbehalt erforderlich ist.

Daher wird sich der vorliegende Abschnitt nur mit den heimlichen Ermittlungsmaßnahmen beschäftigen, die in Südkorea ausführlich erörtert werden, nämlich der Erhebung der Daten der Inhalte und Umstände der Kommunikation, der Erhe-

[390] Zum Beispiel für die Online-Durchsuchung und die Quellen-TKÜ, *Hee-Young Park*, WKLR, 28-3, 2012, 153; *Won-Sang Lee*, CRCL, Nr. 38, 2013, 174; *Hwang Heo*, CRCL, Nr. 58, 2018, 94; *Hee-Young Park*/*Sang-Hak Lee*, KCR, 30-2, 2019, 113 m. w. N.; für den IMSI-Catcher und die Stille SMS, *Hee-Young Park*, PLR, 61-2, 2020, 137; für den Einsatz von VE oder V-Leuten, *Sung-Ryong Kim*, KJCCL, 7-2, 2005, 275.

[391] Kürzlich hat der *K-OGH* jedoch in der Entscheidung über die im Staatssicherheitsgesetz bezeichnete Straftat ausgeführt, dass „*Bildaufnahmen der Handlungen des Angeklagten und Bildschirminhalte auf dessen Tablet-PCs durch Installation und Verwendung einer Netzwerkkamera gegen Verhältnismäßigkeit und Angemessenheit sowie Richtervorbehalt verstoßen, sodass die daraus gewonnenen Bildmaterialien nicht als Beweismittel dienen dürfen*“ (Übersetzung vom Autor) (*K-OGHE* vom 29. 11. 2017 – 2017 Do 9747). In dieser Hinsicht ist ersichtlich, dass die südkoreanischen Geheimdienste derzeit zumindest bei der Ermittlung der Staatsschutzdelikte eine Art der Online-Durchsuchung verwenden. Eine solche Ermittlungshandlung sollte jedoch als verfassungswidrig angesehen werden. Um diese Maßnahme zu rechtfertigen, ist angesichts des Gesetzesvorbehalts, des Richtervorbehalts und des Grundsatzes der Verhältnismäßigkeit eine Ermächtigung erforderlich, um ihre Eingriffsintensität auszugleichen. Selbst in der Literatur, in der behauptet wird, dass auch in Südkorea die Online-Durchsuchung erforderlich ist, gibt es keine Ansicht, dass sie durch bestehende Ermächtigungen gerechtfertigt werden kann. (vgl. *Hee-Young Park*, WKLR, 28-3, 2012, 153, 180; *Won-Sang Lee*, CRCL, Nr. 38, 2013, 174, 210; *Hwang Heo*, CRCL, Nr. 58, 2018, 94, 124 – 129; *Hee-Young Park*/*Sang-Hak Lee*, KCR, 30-2, 2019, 113, 137 ff.). Prof. *Hwang Heo* macht geltend, dass die Online-Durchsuchung angesichts der Situation in Südkorea, das immer noch militärisch mit Nordkorea konfrontiert ist und auch vor Terrorismus nicht mehr sicher ist, einzuführen ist, aber sie nur unter strengeren Anforderungen gerechtfertigt werden kann, als diejenigen von §§ 5 ff. K-KGSG zur TKÜ (*Hwang Heo*, a. a. O. 130 ff.).

[392] Der Grund dafür könnte außerdem darin liegen, dass in Südkorea oft eine Frage über eine individuelle Zwangsmaßnahme in Ermittlungsverfahren i. d. R. erst dann akademisch gestellt wird, wenn sie zuerst in der Politik oder in den Medien zum Thema geworden ist.

bung der Bestandsdaten, dem Abhören des Gesprächs und dem Einsatz eines GPS-Trackers zur Ortung in Echtzeit (vgl. unten II.).

(2) Als Ermächtigungsgrundlagen zu heimlichen Ermittlungsmaßnahmen zur Beweissicherung im koreanischen Strafprozessrecht gibt es die Generalklauseln der Ermittlung (§§ 195 – 197, 199 K-StPO[393]) oder allgemeine Vorschriften der Beschlagnahme und Durchsuchung (§§ 106 ff. i. V. m. §§ 215, 219 K-StPO) sowie das K-KGSG und den § 83 K-TKGG, bei denen es sich um die Beschränkung des Kommunikationsgeheimnisses handelt.[394]

Die Ermittlungsgeneralklauseln sehen – wie §§ 161 Abs. 1, 163 Abs. 1 StPO – inhaltlich nur die Aufgaben und Befugnisse der Ermittlungsbehörden vor, aber sie sind eine Rechtsgrundlage für alle Arten von Ermittlungen ohne Zwang (z. B. Untersuchung durch Zustimmung oder Mitwirkung des Verdächtigen).[395] Zwangsmaßnahmen sind daher nur dann zulässig, wenn es eine besondere Vorschrift gibt, die sie zulässt (vgl. § 199 Abs. 1 S. 2 K-StPO).[396] Dies ist nach der K-StPO-Reform 2007 von Bedeutung, die es ermöglicht, das Ausschlussprinzip auch auf Beweismittel nicht in Worten anzuwenden. Denn wenn die Eingriffsvoraussetzungen jeder Maßnahme wie Beschlagnahme, Durchsuchung und TKÜ sowie das Verfahren und die Art ihrer Durchführung gesetzlich festgelegt werden, müssen die Ermittlungs-

[393] § 195 K-StPO [Verhältnisse zwischen Staatsanwalt und Kriminalpolizei usw.] (1) Staatsanwalt und Kriminalpolizei müssen bei der Ermittlung und der Erhebung und Fortsetzung der öffentlichen Klage miteinander zusammenarbeiten. (2) Angelegenheiten bezüglich der allgemeinen Untersuchungsregeln, die für die Ermittlung nach Abs. 1 zu beachten sind, werden in der DVO vorgeschrieben.

§ 196 K-StPO [Ermittlung des Staatsanwalts] Hält der Staatsanwalt den Verdacht einer Straftat für begründet, so untersucht er Täter, Sachverhalt und Beweise.

§ 197 K-StPO [Kriminalpolizei] (1) Polizeirat, Erster Polizeihauptkommissar, Polizeihauptkommissar, Polizeioberkommissar, Polizeikommissar untersuchen als Kriminalpolizei Täter, Sachverhalt und Beweise, wenn sie den Verdacht einer Straftat für begründet halten. (2) Polizeihauptmeister, Polizeiobermeister, Polizeimeister müssen als Kriminalpolizei die Ermittlungen unterstützen.

§ 199 K-StPO [Ermittlung und erforderliche Untersuchungen] (1) Um den Zweck der Ermittlung zu erreichen, können erforderliche Untersuchungen durchgeführt werden. Zwangsmaßnahmen sind jedoch nur dann zulässig, soweit sie gesetzlich besonders geregelt sind, und dürfen nur im erforderlichen Mindestmaß durchgeführt werden. (2) Zum Zwecke der Ermittlung sind Staatsanwalt und Kriminalpolizei befugt, von allen Behörden und öffentlichen oder privaten Einrichtungen um Auskunft zu ersuchen.

[394] Daneben gibt es § 4 Abs. 1 des Gesetzes über Finanztransaktionen unter Klarnamen (Kurztitel: Klarname-Finanztransaktionsgesetz), der vorsieht, dass die Informationen oder Materialien zum Inhalt von Finanztransaktionen aufgrund richterlicher Anordnung beschlagnahmt und durchsucht werden dürfen, was aber der Natur nach zur allgemeinen Beschlagnahme und Durchsuchung nach §§ 106 ff. i. V. m. §§ 215, 219 K-StPO gehört. In der vorliegenden Arbeit wird dies nicht gesondert behandelt.

[395] *Joo-Won Rhee*, K-StPO, 99.

[396] *Young-Seok Cha*, Die Welt von Staatsexamen, 1988/2, 14; *Wankyu Lee*, KoK-StPO (II), § 199, 96; *Joo-Won Rhee*, K-StPO, 100.

behörden dies einhalten, sonst werden ihre Ermittlungshandlungen rechtswidrig.[397] Nach h. M. und der Rspr. gelten die allgemeinen Vorschriften der Beschlagnahme und Beschlagnahme nicht nur für offene Maßnahmen. Die Beschlagnahme und Beschlagnahme, die ohne Wissen des Betroffenen durchgeführt wird, kann auch auf die Vorschriften beruhen. In diesem Fall können i. R. d. Erhebung von Informationen die Verfahrensgarantien wie die Bekanntmachung an den von der Maßnahme Betroffenen und die Teilnahme an der Durchführung der Durchsuchung ausgeschlossen werden (vgl. Kapitel 4, D. III. 2.), und eine nachträgliche Benachrichtigung erfolgt nach § 9b K-KGSG nach dem Beschluss bezüglich einer Anklageerhebung.[398] Das typischste Beispiel hierfür ist die heimliche Beschlagnahme und Durchsuchung der Daten, die nach Abschluss des Übertragungsvorgangs im Server des TK-Anbieters gespeichert sind (z. B. E-Mail, Messenger-Nachrichten etc.). Diese allgemeinen Vorschriften werden daneben als Auffang-Ermächtigungsnormen für die verdeckten Ermittlungsmaßnahmen angesehen, die i. d. R. in Grundrechte nicht unerheblich eingreifen, deren Ermächtigungen jedoch nicht vorhanden oder nicht klar sind. Das K-KGSG regelt durch qualifizierte Eingriffsvoraussetzungen und Verfahrenssicherungen die Eingriffe in das Geheimnis und die Freiheit der Kommunikation bzw. des Gesprächs. Die nach dem Gesetz zulässigen Maßnahmen sind die TKÜ und die Postzensur, die Erhebung von Verkehrs- und Standortdaten und das Abhören des Gesprächs etc. Die Bestandsdaten werden aufgrund des § 83 K-TKGG erhoben.

In diesem Abschnitt stehen die Regelungsinhalte des K-KGSG und des § 83 K-TKGG und die von ihnen zugelassenen Maßnahmen im Mittelpunkt.

2. Eigene Merkmale von K-KGSG

Das K-KGSG hat seit seiner Schaffung viele Mängel im Blick auf Begriffe/Terminologien, Inhalte und Struktur (vgl. Kapitel 1, A. II. 2.), die trotz mehrerer Überarbeitungen in der Zwischenzeit immer noch vorhanden sind. Um das K-KGSG zu verstehen, sollte man daher zunächst auf einige damit verbundene besondere Merkmale – im Vergleich zu StPO und TKG – achten.

(1) Im K-KGSG werden die Postzensur und die TK-Überwachung (§ 2 Nr. 1 – 4, 6, 7, 9, 10[399]) als „Maßnahmen zur Beschränkung der Kommunikationen“ (im fol-

[397] *Young-Seok Cha*, Die Welt von Staatsexamen, 1988/2, 14. In Südkorea ist der Begriff der Zwangsmaßnahme im Ermittlungsverfahren umstritten, aber nach h. M. ist sie praktisch zu bestimmen und wird – wie in Deutschland – i. d. R. als eine Maßnahme verstanden, die einen nicht geringfügigen Eingriff in Grundrechte bewirkt (*Wankyu Lee*, KoK-StPO (II), § 199, 96, 104; auch *Yang-Kyun Shin*, JCL, 26-2, 2014, 447, 662).

[398] *K-VerfGE* vom 17. 12. 2012 – 2011 HunBa 225 (24-2, 467, 473).

[399] § 2 K-KGSG [Begriffsbestimmungen] Im Sinne dieses Gesetzes ist oder sind: 1. „Kommunikation“ Postsendungen und Telekommunikation, 2. „Postsendung“ Post und Paket, 3. „Telekommunikation (TK)“ das Senden oder Empfangen aller Arten von Ton, Text, Zeichen oder Bildern auf drahtgebundene, drahtlose, optische oder andere elektronische Weise wie Telefon, E-Mail, Auskunftsdienst für Mitglieder, Telefax, Funkruf etc., 4. die „Betroffenen“

genden „KBeschMaß“) bezeichnet (§ 3 Abs. 2[400]), die unter denselben Eingriffsvoraussetzungen und verfahrensrechtlichen Vorkehrungen reguliert sind (§§ 4 – 6, 8 – 9a, 11, 12). Dieser Terminus wird jedoch im Schrifttum teilweise kritisiert, da er eine Verwirrung bei der Abgrenzung von den Begriffen „Kommunikationen“, „Überwachung“ und „Abhören von Gesprächen“ verursacht und nicht mit alltäglichen Ausdrücken übereinstimmt.[401] Außerdem ist die Postzensur in der jüngsten Praxis kaum problematisch. Aus diesen Gründen wird in der Literatur und Rspr. normalerweise stattdessen die Bezeichnung „TKÜ“ verwendet. In der vorliegenden Arbeit wird der Ausdruck „KBeschMaß“ nur bei Bedarf verwendet, und i. d. R. wird „TKÜ“ verwendet. Andererseits gelten die meisten Vorschriften zur TKÜ entsprechend für das Abhören von Gesprächen, bei dem nichtöffentliche persönliche Gespräche zwischen anderen Personen mit technischen Mitteln geheim aufgezeichnet und abgehört werden (§ 14 Abs. 2).[402] Schließlich sind die Postzensur, die TKÜ und das Abhören von Gesprächen in Südkorea unter denselben Eingriffsvoraussetzungen und Verfahrensgarantien erlaubt.

Im K-KGSG werden die Daten über die Umstände der TK als „Daten zur Bestätigung des Sachverhalts bezüglich der TK“ (im folgenden „TK-Bestätigungsdaten“) bezeichnet, zu denen der Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit, die (Kunden-)Nummer oder Kennungen von Teilnehmern wie die Rufnummer der beteiligten Anschlüsse etc., die Nutzungshäufigkeit (der TK), die Logdateien über den Sachverhalt bezüglich der Nutzung von Computernetzwerk oder Internet, die Daten zur geographischen Ortung von Funkzellen und die Daten, die die geografische Lage des Computernetzwerk- oder Internetanschlusses bestä-

---

Absender und Empfänger von Postsendungen oder TK, 6. „Zensur“ das Öffnen von Postsendungen ohne Einwilligung der Betroffenen oder die Kenntnisnahme, das Aufzeichnen oder das Verwahren ihres Inhalts auf andere Weise, 7. „Überwachung“ die Kenntnisnahme oder das Aufzeichnen des Inhalts der TK durch Abhören und Lesen von Ton, Text, Zeichen oder Bildern mit der Verwendung elektronischer oder technischer Mittel ohne Einwilligung der Betroffenen, oder das Stören von Senden oder Empfangen der TK auf eine solche Weise, 9. „E-Mail“ das Übertragen von Nachrichten über ein Computernetzwerk oder die gesendeten Nachrichten, 10. „Auskunftsdienst für Mitglieder“ der Informationsdienst, der bestimmten Mitgliedern oder Vertragspartnern bereitgestellt wird, oder ein solches Netzwerk.

[400] § 3 K-KGSG [Schutz des Geheimnisses der Kommunikation und des Gesprächs] (2) Die Postzensur und die TK-Überwachung (im Folgenden „KBeschMaß“) müssen zum Zwecke der Ermittlung von Straftaten oder der Staatssicherheit als ergänzende Maßnahmen verwendet werden, wobei Ermittlungsbehörden dafür sorgen sollten, Eingriffe in das Geheimnis der Kommunikation zu minimieren.

[401] Vgl. *Kil-Young Oh*, JML, 14-1, 2015, 33, 39.

[402] § 14 K-KGSG [Verbot des Eingriffs in das Geheimnis des Gesprächs anderer Personen] (2) Für die Aufzeichnung und das Abhören nach Abs. 1 gelten §§ 4 – 8, § 9 Abs. 1 S. 1, Abs. 3, § 9a, § 11 Abs. 1, 3 und 4 sowie § 12 K-KGSG. Der Grund, warum das Abhören von Gesprächen vom K-KGSG geregelt wird, scheint darin zu liegen, dass es, nicht TKÜ, der politische Hintergrund für die Schaffung des Gesetzes im Jahr 1994 war (siehe Kapitel 1, Fn. 34). Auf jeden Fall führt dies in der Literatur teilweise zu einem anderen Verständnis des Schutzbereichs von Kommunikationsgeheimnissen in Deutschland und Südkorea (vgl. Kapitel 2, C. II. 2.).

tigen können, gehören (§ 2 Nr. 11 K-KGSG[403]). Sie entsprechen begrifflich den Verkehrsdaten i. S. v. § 3 Nr. 30 TKG und auch der dazugehörige Umfang der Daten ist nahezu identisch mit dem der Verkehrsdaten (vgl. § 96 Abs. 1 und § 113b TKG). Daher wird der Ausdruck „TK-Bestätigungsdaten" in der vorliegenden Arbeit nur bei Bedarf verwendet und i. d. R. wird „Verkehrsdaten" verwendet. Zum anderen werden die Bestandsdaten i. S. d. § 3 Nr. 3 TKG in Südkorea als „Grunddaten der TK" bezeichnet und sie sind aufgrund des § 83 K-TKGG[404] – nicht K-KGSG – zu erheben. Ihr Begriff ist im K-TKGG nicht rechtlich definiert, aber die dazugehörigen Daten sind im § 83 Abs. 3 K-TKGG einzeln aufgeführt (vgl. unten II. 3.). Diese sind fast identisch mit den in § 111 Abs. 1 TKG genannten Informationen. In der vorliegenden Arbeit wird auch der Ausdruck „Grunddaten der TK" nur bei Bedarf verwendet.

(2) Nach dem Wortlaut von § 6 und § 9a K-KGSG ist die TKÜ nicht nur für den Beschuldigten, sondern auch für „den von Vorermittlung Betroffenen" zulässig. Dies gilt auch bei der Erhebung der Verkehrsdaten (§ 13 Abs. 9 K-KGSG). Nach einer Meinung der Literatur sei dies auf die Praxis zurückzuführen, in der die Unterscheidung zwischen Ermittlung und Vorermittlung in der Vergangenheit nicht klar war und somit ihr Begriff gemischt verwendet wurde.[405] Dabei handelt es sich jedoch meiner Meinung nach nicht um einen legislativen Fehler, und es wird davon ausgegangen, dass der Gesetzgeber es darauf angelegte, bei Staatsschutzdelikten bereits im Vorermittlungsstadium den Nachrichtendiensten die TKÜ und die Verkehrsdatenerhebung zu ermöglichen. Dennoch ist dies nicht damit zu vereinbaren, dass solche Maßnahmen Zwangsmaßnahmen darstellen, die einen Richtervorbehalt explizit voraussetzen. Dies liegt daran, dass nach h. M. in Südkorea zwangsmäßige Ermittlungen im Vorermittlungsstadium nicht zulässig sind.[406] Der Wortlaut sollte unter dem Gesichtspunkt der rechtsstaatlichen Normenklarheit dringend gestrichen werden, und die Möglichkeit der Maßnahmen für die Staatssicherheit sollten durch andere unabhängige Vorschriften gerechtfertigt werden.

---

[403] § 2 K-KGSG [Begriffsbestimmungen] Im Sinne dieses Gesetzes ist oder sind: 11. „Daten zur Feststellung des Sachverhalts bezüglich der TK" die Daten, die unter eine der folgenden lit. fallen, a) Datum und Uhrzeit der TK, b) der Beginn und das Ende der jeweiligen TK-Verbindung nach Datum und Uhrzeit, c) die (Kunden-)Nummer oder Kennungen von Teilnehmern wie die Rufnummer der beteiligten Anschlüsse etc., d) die Nutzungshäufigkeit, e) die Logdateien über den Sachverhalt bezüglich der Nutzung von Computernetzwerk oder Internet, f) die Daten zur Standortverfolgung von Funkzellen, die es ermöglichen, die geografische Lage der mit dem IT-Netzwerk verbundenen IT-Geräte zu bestätigen, und g) die Daten zur Standortverfolgung von Anschlüssen, die es ermöglichen, die geografische Lage der IT-Geräte zu bestätigen, die zur Verbindung mit dem IT-Netzwerk verwendet werden.

[404] Der Inhalt dieser Vorschrift befand sich früher in § 54 K-TKGG a. F. (in der vom 1. April 2000 bis zum 21. September 2010 geltenden Fassung), aber er wurde durch eine Änderung, die am 2. März 2010 beschlossen und am 22. September 2010 in Kraft getreten ist, ohne wesentliche Änderung des Inhalts in § 83 verschoben (Gesetz Nr. 10166).

[405] *Wankyu Lee*, TPCP, 7-1, 2015, 33, 44 f.

[406] *Kyung-Sik Oh*, CRCL, Nr. 34, 2012, 48, 66; *Wankyu Lee*, TPCP, 7-1, 2015, 33, 39 ff.; *Yang-Kyung Shin*/*Gi-Young Cho*, JCL, 23-3, 2011, 181, 195 ff.; a. A. *Soung-Jin Chung*, KLR, Nr. 9, 1997, 93, 115; *Mungyu Hwang*, KCR, 22-3, 2011, 217, 239.

(3) Nach Vorschriften des K-KGSG werden die Postzensur, die TKÜ, die Verkehrsdatenerhebung und das Abhören von Gesprächen nicht nur zum Zwecke der Strafverfolgung, sondern auch zum Zwecke der geheimdienstlichen Gefahrenabwehr erlaubt (vgl. §§ 7, 8 Abs. 8–9, 9a Abs. 3, § 13c K-KGSG). Im südkoreanischen Rechtssystem haben – anders als in Deutschland – Geheimdienste, etwa der Nationale Nachrichtendienst, polizeiliche Geheimdienstabteilungen und militärische Geheimdienste (z. B. das Oberkommando zur Militärischen Sicherheitsunterstützung), Ermittlungsbefugnisse in Bezug auf bestimmte Straftaten. Zu den koreanischen Ermittlungsbehörden gehören daher i. d. R. sowohl StA und Polizei als auch Geheimdienste. Die Vorschriften tragen diesem System Rechnung. Diese Maßnahmen nach dem K-KGSG unterliegen natürlich gerichtlicher Kontrolle. In der Literatur wird jedoch u. a. kritisiert, dass die Eingriffsvoraussetzungen nicht klar sind (vgl. § 7 Abs. 1 K-KGSG: „wenn eine erhebliche Gefahr für die Staatssicherheit erwartet wird oder wenn Antiterror-Maßnahmen nach dem Gesetz zur Terrorismusbekämpfung (Gesetz Nr. 17466) erforderlich sind"), dass die maximale Überwachungsfrist (4 Monate) zu lang und die Verlängerung unbeschränkt zulässig ist (vgl. Abs. 2) und dass die nachträgliche Benachrichtigung des Betroffenen in der Tat auf unbestimmte Zeit zurückgestellt werden kann (vgl. § 9a Abs. 3, 4, 6 K-KGSG).[407] Schließlich werden derzeit in Südkorea Überwachungen für die Staatssicherheit praktisch kaum kontrolliert, nachdem sie anfangs vom Richter genehmigt wurden. Dies scheint jedoch aus Sicherheitsgründen politisch angenommen zu werden. In der vorliegenden Arbeit wird die TKÜ zum Zwecke der Gefahrenabwehr nicht gesondert behandelt.

(4) Das K-KGSG gehört hinsichtlich Struktur und Inhalt zum Sonderrecht. Verboten sind zuerst die Postzensur, die TKÜ, die Verkehrsdatenerhebung und die Gesprächsüberwachung, die nicht auf dem Gesetz beruhen (§ 3 Abs. 1 K-KGSG, für das Abhören von Gesprächen § 14 Abs. 1 K-KGSG),[408] und Verstöße gegen dieses Verbot und die Veröffentlichung und Offenbarung von Informationen, die durch die Maßnahmen gewonnen werden, werden strafrechtlich bestraft (§ 16 Abs. 1 K-KGSG; jedoch nicht bei den Verkehrsdaten). Jede Eingriffsmaßnahme ist nur aufgrund von §§ 5–12a, 13–13d, 14 K-KGSG als Vorschriften zur Rechtfertigung

[407] *Byoung-Hyo Moon*, PLLR, Band 45, 2009, 503; *Sung-Gi Hwang*, JML, 14-1, 2015, 1, 24 f. Daher wird in der Literatur häufig die Wirksamkeit der Kontrolle über die Tätigkeiten von Geheimdiensten durch dieses Gesetz infrage gestellt (*Il-Whan Kim*, KJC, 16-1, 2004, 25, 43 f.), dies ist jedoch im Wesentlichen auf die Situation zurückzuführen, in der die beiden Koreas politisch und militärisch konfrontiert sind.

[408] § 3 K-KGSG [Schutz des Geheimnisses der Kommunikation und des Gesprächs] (1) Niemand darf Postsendungen zensieren, TK überwachen, TK-Bestätigungsdaten erteilen oder nichtöffentliche Gespräche zwischen anderen Personen aufzeichnen oder abhören, es sei denn, dies beruht auf anderen Vorschriften in diesem Gesetz, der K-StPO oder des Militärgerichtsgesetzes.

§ 14 K-KGSG [Verbot des Eingriffs in das Geheimnis des Gesprächs anderer Personen] (1) Niemand darf nichtöffentliche Gespräche zwischen anderen Personen aufzeichnen oder mithilfe von technischen Mitteln abhören.

zulässig. Die Inhalte von Postsendungen, TK oder Gesprächen, die durch Verletzungen der Vorschriften gewonnen wurden, dürfen nicht als Beweismittel in Gerichts- oder Disziplinarverfahren verwendet werden (§ 4 K-KGSG, für das Abhören von Gesprächen § 14 Abs. 2 i. V. m. § 4 K-KGSG; jedoch nicht bei den Verkehrsdaten).[409]

(5) Das K-KGSG stellt eine Ermächtigungsnorm für heimliche Zwangsmaßnahmen dar, aber seine Eingriffsvoraussetzungen und Verfahrensgarantien sind überall nicht so streng und gradweise ausgestaltet, verglichen mit §§ 99 – 101b StPO. Zuerst werden i. R. d. Eingriffsvoraussetzungen der Maßnahmen die „Schwere der Straftat" und die „Stärke des Tatverdachts" nur bei Postzensur, TKÜ und Gesprächsüberwachung berücksichtigt (§ 5 und § 14 Abs. 2 K-KGSG),[410] aber nicht bei der Erhebung von Verkehrs- und Standortdaten (§ 13 Abs. 1, 2 K-KGSG). Außerdem wird die „Subsidiarität" bei den ersteren Maßnahmen immer angefordert, aber bei der letzteren Maßnahme nur teilweise für die Ortung in Echtzeit und die Funkzellenabfrage (§ 13 Abs. 2 K-KGSG). Andererseits wird i. R. d. verfahrensrechtlichen Vorkehrungen die Kontrolle durch Gericht als unabhängige und neutrale Instanz nicht ausreichend gewährleistet. Die Regelungen für die Benachrichtigung, die es den von Maßnahmen Betroffenen ermöglicht, einen nachträglichen effektiven Rechtsschutz zu eröffnen, sind nicht nur unangemessen (§§ 9a, 13b K-KGSG), sondern es gibt auch darin u. a. keine Rechtsgrundlage für die nachträgliche Überprüfung der Rechtmäßigkeit der Art und Weise der Durchführung der Maßnahmen (vgl. unten II. 1. d)). All dies ist im Hinblick auf die Rechtsstaatlichkeit problematisch.

II. Heimliche Ermittlungsmaßnahmen zur Beweissicherung und ihre Ermächtigungen

1. TKÜ und Postzensur

Wie bereits erwähnt, werden TKÜ und Postzensur im K-KGSG als Maßnahmen zur Beschränkung der Kommunikationen bezeichnet und sind völlig gleich geregelt, aber diese Art der Regulierung ist sowohl in der Literatur als auch in der Praxis keineswegs fragwürdig. Im Folgenden werden die einschlägigen Bestimmungen des Gesetzes mit Schwerpunkt auf TKÜ dargestellt (vgl. a) – c)). Dazu werden die Probleme der Benachrichtigungsvorschriften und das Fehlen der Möglichkeit

[409] K-KGSG § 4 [Verbot der Beweisverwertung des Inhalts von Postsendungen aufgrund illegaler Zensur und von TK aufgrund illegaler Überwachung] Der Inhalt von Postsendungen oder TK, der unter Verstoß gegen die Vorschrift des § 3 durch illegale Zensur erlangt oder durch illegale Überwachung zur Kenntnis genommen oder aufgezeichnet wurde, darf nicht als Beweismittel in Gerichts- oder Disziplinarverfahren verwendet werden.

[410] Nach § 14 Abs. 2 K-KGSG gilt der § 5 Abs. 1 K-KGSG, in dem die Straftaten, für die die Postzensur und die TKÜ zulässig sind, begrenzt aufgezählt sind, entsprechend für das Abhören von Gesprächen.

nachträglichen Rechtsschutzes (vgl. d)) sowie die Regelung über „Paket-Überwachung“ (vgl. e)) gesondert überprüft.

a) Eingriffsvoraussetzungen und präventive Verfahrenskontrolle

aa) Eingriffsvoraussetzungen: § 5 K-KGSG

(1) Die TKÜ kann nur dann subsidiär erlaubt werden, wenn der Verdacht einer im K-KGSG bezeichneten bestimmten Straftat zureichend begründet ist (§ 5 Abs. 1 K-KGSG), und sie richtet sich an bestimmte TK, die vom Verdächtigen gesendet und empfangen wurden, oder solche TK für einen bestimmten Zeitraum (Abs. 2).[411] Der Anwendungsbereich von TKÜ nach § 5 K-KGSG hängt vom Begriff TKÜ ab, und nach § 2 K-KGSG bedeutet diese „die ‚Kenntnisnahme‘ oder das ‚Aufzeichnen‘ des Inhalts der TK (das ‚Senden oder Empfangen‘ aller Arten von Ton, Text, Zeichen oder Bilder auf drahtgebundene, drahtlose, optische oder andere elektronische Weise wie Telefon, E-Mail, Auskunftsdienst für Mitglieder, Telefax, Funkruf etc.) mit der Verwendung elektronischer oder technischer Mittel ohne Einwilligung der Betroffenen als ‚Absender und Empfänger‘ der TK, oder das ‚Stören‘ von Senden oder Empfangen der TK auf eine solche Weise“ (Nrn. 3, 4, 7). Da „TK“ und „Überwachung“ umfassend und offen definiert sind, können alle Arten von TK und Überwachungsmethoden, die bereits bestehen oder in Zukunft neu entwickelt werden, begrifflich von „Überwachung der TK“ abgedeckt werden.[412] Doch wegen der Wortlaute in der Verlaufs- bzw. Gegenwartsform der Begriffsbestimmung

[411] § 5 K-KGSG [Voraussetzungen der Erlaubnis zur KBeschMaß zur Ermittlung der Straftaten] (1) Die KBeschMaß können nur dann erlaubt werden, wenn zureichende Gründe für den Verdacht bestehen, dass die folgenden Straftaten geplant oder begangen werden oder begangen wurden, und soweit die Verhinderung ihrer Begehung, die Festnahme des Verdächtigen oder die Erhebung von Beweismitteln auf andere Weise erschwert wäre; die Straftaten sind: 1. aus dem Strafgesetzbuch: …, 2. aus dem Militärstrafrecht: …, 3. die im Staatssicherheitsgesetz bezeichneten Straftaten, 4. die im Gesetz zum Schutz militärischer Geheimnisse bezeichneten Straftaten, 5. die im Gesetz zum Schutz militärischer Stützpunkte und Einrichtungen bezeichneten Straftaten, 6. aus dem Betäubungsmittelgesetz: …, 7. aus dem Gesetz zur Bestrafung von Gewalttaten etc.: …, 8. aus dem Gesetz zur Kontrolle von Waffen, Schwertern und Sprengstoffen: …, 9. aus dem Gesetz zur verschärften Bestrafung für bestimmte Straftaten: …, 10. aus dem Gesetz zur verschärften Bestrafung für bestimmte Wirtschaftsstraftaten: …, 11. die Straftaten, die gegen die Gesetze zur Verschärfung der Bestrafung von Straftaten der Abs. 1 und 2 verstoßen, 12. aus dem Gesetz zur Bestechungsbekämpfung im internationalen Geschäftsverkehr: … (2) Die KBeschMaß kann für bestimmte TK, die vom Verdächtigen i. S. d. Abs. 1 gesendet und empfangen wurden, oder solche TK für einen bestimmten Zeitraum, erlaubt werden.

[412] Wie bereits erwähnt, sind § 3 Abs. 1 i. V. m. § 16 Abs. 1 K-KGSG Vorschriften zur Bestrafung derjenigen, die illegale TKÜ durchgeführt haben. Daher ist die „Überwachung der TK“ i. S. d. § 2 Nrn. 3, 7 K-KGSG ein Tatbestandsmerkmal der Strafvorschrift. Eine Verfassungsbeschwerde gegen das Merkmal wurde erhoben, weil es wegen seines umfassenden Begriffs gegen die Normenklarheit verstößt, aber das *K-VerfG* entschied, dass es durch andere Vorschriften ausreichend konkret beschrieben werden kann (*K-VerfGE* vom 25. 11. 2004 – 2002 HunBa 85: 16-2, 345, 352 f.).

(„Kenntnisnahme/Aufzeichnen“, „Senden/Empfangen“ und „Stören“) ist der Anwendungsbereich umstritten.

(2) Zunächst stellt sich die Frage, ob die nach Abschluss des Übermittlungsvorgangs auf dem Server des TK-Diensteanbieters gespeicherten Kommunikationsinhalte wie E-Mails oder Messenger-Nachrichten (Internet-Chat) in den Begriff der „TK“ nach § 2 Nr. 3 K-KGSG einbezogen werden können. Dabei handelt es sich um die Abgrenzung des Anwendungsbereichs zwischen der TKÜ nach §§ 5 ff. K-KGSG und allgemeiner Beschlagnahme und Durchsuchung nach §§ 106 ff. i. V. m. §§ 215, 219 K-StPO. Die Anwendung der beiden Ermächtigungsnormen unterscheidet sich nicht nur im Umfang der Straftaten, für die jede Maßnahme zulässig ist, sondern auch in der Strenge der Verfahrenskontrolle und des Beweisverwendungsverbots. Aus diesem Grund wollen die Ermittlungsbehörden in der Praxis womöglich Daten aufgrund der allgemeinen Vorschriften der K-StPO erheben. Hierbei erklärt *K-OGH* ständig, dass die TKÜ gestützt auf die Legaldefinitionen des § 2 Nrn. 3, 7 K-KGSG (Wortlaute von „Kenntnisnahme/Aufzeichnen“, „Senden/Empfangen“ und „Stören“) die Gleichzeitigkeit/Parallelität bzw. Gegenwärtigkeit ihrer Durchführung voraussetzen muss und dass die Erhebung der nach Beendigung des Übertragungsvorgangs auf dem Server des Anbieters vorhandenen E-Mails oder Nachrichten auf K-StPO, nicht auf K-KGSG, beruhen muss: ein technischer TK-Begriff.

> „Im Lichte der Begriffsbestimmung der ‚Überwachung‘ bezieht sich die TKÜ auf den Fall der Kenntnisnahme oder des Aufzeichnens der TK-Inhalte in Echtzeit während des laufenden Übertragungsvorgangs und den Fall der unmittelbaren Störung des Sendens und Empfangens der TK, aber dazu gehört nicht die Einsicht in die Aufzeichnungen oder Inhalte der TK, die nach dem Empfang verbleiben.“[413] *(Übersetzung vom Autor)*

Dies wird jedoch neuerdings im Schrifttum kritisiert. Weil der Zugang auf die Inhalte von E-Mails und Messenger-Nachrichten, die auf dem Server gespeichert sind, in vielen Fällen hinsichtlich der Menge und Vielfalt der Daten schwerwiegender ist als die Überwachung in Echtzeit, sollten die auf dem Server vorhandenen TK-Inhalte aufgrund der §§ 5 ff. K-KGSG erhoben werden.[414] Diese Kritik ist teilweise vertretbar, aber es sollte vermieden werden, dass die Interessen einer wirksamen Strafverfolgung übermäßig eingeschränkt werden. Daher sollte die Bestimmung der Ermächtigung zum Zugriff auf solche Daten danach unterschieden werden, ob er heimlich oder offen erfolgt. Heutzutage ist dieser Zugriff zur Sachaufklärung in

[413] Für die E-Mail *K-OGHE* vom 26. 7. 2012 – 2011 Do 12407 vom 29. 11. 2012 – 2010 Do 9007 und vom 29. 11. 2017 – 2017 Do 9747 m. w. N.; für die Messenger-Nachricht *ders.* vom 13. 10. 2016 – 2016 Do 8137; dazu *Kil-Young Oh*, JML, 14-1, 2015, 33, 43 f.: Diese Stellungnahme des *K-OGH* steht im Einklang mit dem Wortlaut von § 9b K-KGSG.

[414] *Kuk Cho*, KJC, 22-1, 2010, 99, 120; vgl. im gleichen Sinne *Hojung Lee*, JPL, 17-1, 2019, 35, 43. Andererseits zieht Prof. *Kil-Young Oh* in Zweifel, dass sich angesichts der Eigenschaften elektronischer Daten, die sich nach dem Ende der Übertragung nicht verflüchtigen, sondern gespeichert bleiben, die Ermächtigungsgrundlage für diese Maßnahme danach unterscheidet, ob diese in der Übertragungsphase oder nach ihrer Beendigung ergriffen wird. Er sagt jedoch, dass die Stellungnahme des *K-OGH* unter Berücksichtigung des Wortlauts von K-KGSG gültig ist (*Kil-Young Oh*, JML, 14-1, 2015, 33, 43 f.).

vielen Ermittlungsverfahren unerlässlich, unabhängig von der Schwere der Straftaten. Dass er nur bei begrenzten Straftaten erlaubt ist, kann eine wirksame Strafverfolgung erheblich behindern. In dieser Hinsicht sollten „offene Ermittlungen", die den Betroffenen mindestens zeitgleich oder unmittelbar nach ihrer Durchführung mitgeteilt werden, auf den allgemeinen Vorschriften der Beschlagnahme und Durchsuchung beruhen können, deren Anwendungsbereich nicht beschränkt ist und die keine Subsidiaritätsregelung enthalten. Dies gilt jedoch nicht für die heimlichen Maßnahmen, die zu einem intensiveren Grundrechtseingriff führen und umso mehr für die TKÜ in Südkorea, bei der der Betroffene erst nach dem Beschluss in Bezug auf Anklageerhebung über ihren Vollzug informiert wird. In diesem Fall sind enge Eingriffsvoraussetzungen und strenge verfahrensrechtliche Vorkehrungen nach §§ 5 ff. K-KGSG erforderlich.[415] Insbesondere der § 12b K-KGSG, der gerichtliche Kontrolle über die Verwendung und Speicherung von durch Paket-Überwachung erfassten Daten vorsieht (vgl. unten e), sollte entsprechend auch für die Erhebung und Verwendung der auf dem Server umfassend gespeicherten Inhalte von E-Mails und Messenger-Nachrichten gelten.

Auf der anderen Seite wird derzeit in Südkorea kaum die Frage diskutiert, unter welcher Ermächtigungsnorm bzw. unter welchen Eingriffsvoraussetzungen ein „heimlicher" Zugriff auf „die im Cloud-Speicher der Dienstanbieter vorhandenen Daten" erlaubt werden kann. In der Praxis scheint dies genauso behandelt zu werden wie der heimliche Zugriff auf die auf dem Mail- oder SNS-Server des Providers gespeicherten E-Mails oder Nachrichteninhalte; d. h., sie werden aufgrund der allgemeinen Vorschriften der Beschlagnahme und Durchsuchung erhoben. Natürlich wird in der Literatur auf die durch Cloud-Computing verursachten Veränderungen und die Grenzen bei der Anwendung der allgemeinen Vorschriften der K-StPO und ihre Verbesserungen in legislativer Hinsicht ständig eingegangen, aber diese Diskussionen setzen im Grunde offene Beschlagnahme und Durchsuchung voraus (vgl. Kapitel 4, D. II.). Nach einer in der Literatur vertretenen Auffassung kann die Einführung der Ermächtigung zur Online-Durchsuchung – wie in Deutschland – für den verdeckten Zugriff auf den Cloud-Speicher in Betracht gezogen werden, aber wegen ihrer hohen Eingriffsintensität bedarf es der Unterstützung der öffentlichen Meinung und einer gesetzgeberischen Entscheidung.[416]

(3) Darüber hinaus stellt sich die Frage, ob es durch § 5 K-KGSG abzudecken ist, dass ein Teilnehmer der TK, insb. Telefongespräche – einschließlich IP-Telefonie –, den TK-Inhalt selbst oder unter Mitwirkung eines Dritten ohne Wissen der TK-

[415] A. A. *Joo-Won Rhee*, ALR, Nr. 37, 2012, 151, 187 ff.: In diesem Fall ist die Schwere der Straftaten oder die Subsidiarität nicht erforderlich, und es genügt, dass ein qualifizierterer Tatverdacht als bei allgemeiner Beschlagnahme und Durchsuchung und die Beschränkung des Umfangs der Beschlagnahme durch den Sendungs- und Empfangszeitpunkt gesetzlich geregelt wird.

[416] *Won-Sang Lee*, CRCL, Nr. 38, 2013, 174, 207 ff. Außerdem argumentiert er, dass bei der Gesetzgebung die Maßnahme nur dann erlaubt werden sollte, wenn sie das einzige und letzte Mittel ist (a. a. O. 210).

Partner aufzeichnen kann. Sie ist auch auf den Gesetzestext zurückzuführen. Gemäß § 2 Nr. 7 K-KGSG bedeutet die Überwachung die Kenntnisnahme oder das Aufzeichnen des TK-Inhalts ohne Einwilligung der „Betroffenen", d. h. des Absenders „und" Empfängers der TK (Nr. 4). Erfolgt die Telefonüberwachung daher entweder von einem der Telefonteilnehmer selbst oder von einem Dritten mit dessen Einwilligung, ist umstritten, ob dies unter § 5 K-KGSG subsumiert werden kann. Dieses Problem wird in Südkorea auf derselben Ebene behandelt wie das Abhören nichtöffentlichen Gesprächs: vgl. unten 4.

bb) präventive Verfahrenskontrolle: § 6 K-KGSG

§ 6 K-KGSG schreibt das Verfahren der Erlaubnis zur TKÜ vor. Die Ermittlungsbehörde muss beim Gericht die Erlaubnis der TKÜ für jeden Verdächtigen im Einzelnen beantragen (Abs. 1 und 2). Dieser Antrag ist in schriftlicher Form unter Angabe von Art, Zweck, Gegenständen, Umfang und Zeitraum und Durchführungsort und -methode der TKÜ sowie Gründen, die die Eingriffsvoraussetzungen von § 5 Abs. 1 K-KGSG erfüllen (Antragsbegründung), zu stellen, wobei ihm erläuternde Unterlagen für die Antragsbegründung beizulegen sind (Abs. 4 S. 1: „Antragsschrift").[417] Er wird vom Landgericht entschieden, in dessen Bezirk die Straftat begangen wurde, oder die von Maßnahmen Betroffenen oder die an der Straftat Beteiligten ihren Wohn- und Aufenthaltsort haben (Abs. 3). Das Gericht muss die TKÜ für jeden Betroffenen im Einzelnen erlauben und einen Schein dafür ausstellen (Abs. 5: „Erlaubnisschein"), in dem Art, Zweck, Gegenstände, Umfang, Zeitraum und Durchführungsort und -methode der TKÜ angegeben werden müssen (Abs. 6). Die TKÜ darf zwei Monate nicht überschreiten und muss sofort beendet werden, wenn das Ziel der Maßnahme in diesem Zeitraum erreicht wird (Abs. 7 S. 1). Wenn jedoch die Anforderungen von § 5 Abs. 1 K-KGSG bestehen, kann die Ermittlungsbehörde unter Beifügung von erläuternden Unterlagen eine Verlängerung um einen Zeitraum von weniger als zwei Monaten beantragen (Abs. 7 S. 2). Dabei darf die gesamte Verlängerungsfrist i. d. R. ein Jahr nicht überschreiten, aber bei Straftaten bezüglich der Staatssicherheit oder der öffentlichen Ruhe, Ordnung und Sicherheit unter den in § 5 Abs. 1 Nrn. 1, 2 K-KGSG genannten Straftaten und bei Straftaten in Nrn. 3 – 5 darf sie drei Jahre nicht überschreiten (Abs. 8).[418] Wird der

[417] Wurde die TKÜ dabei bereits für dieselbe Tatsache und dieselbe Person beantragt oder erlaubt, müssen der Zweck und die Gründe für einen erneuten Antrag angegeben werden (Abs. 4 S. 2).

[418] Der Abs. 8 wurde am 31. Dezember 2019 neu eingeführt (Gesetz Nr. 16849). Dies ist auf dem Beschluss von *K-VerfG* zurückzuführen. Das Gericht entschied am 28. Dezember 2010, dass § 6 Abs. 7 K-KGSG, der die Gesamtdauer oder der Anzahl der Verlängerungen nicht begrenzt, gegen die Anforderungen der *ultima ratio* und die Abwägung aus dem Verhältnismäßigkeitsprinzip verstößt und verfassungswidrig ist, und dass er somit nur vorläufig angewendet werden kann (2009 HunGa 30, *K-VerfGE* 22-2, 545). Aber das Gericht hat hier einen Fehler begangen, keine Frist für die vorläufige Anwendung festzulegen. Aus diesem Grund hat

Antrag auf die TKÜ nach Abs. 1, 2 und deren Verlängerung nach Abs. 7 S. 2 als unbegründet angesehen, lehnt das Gericht ihn ab und teilt dies dem Antragsteller mit (Abs. 9).

b) TKÜ im Eilfall: § 8 K-KGSG

§ 8 K-KGSG sieht vor, dass die Ermittlungsbehörde für eine Person, die die Eingriffsvoraussetzungen nach § 5 Abs. 1 erfüllt, ohne Erlaubnis des Gerichts die TKÜ durchführen darf, soweit ein dringender Grund besteht, das Verfahren gemäß § 6 nicht durchlaufen zu können. Diese Eil-TKÜ setzt dringende Situationen voraus, wie die Planung oder Ausführung von schwerwiegenden Straftaten wie Verschwörungen, die die Staatssicherheit bedrohen, oder Straftaten, die eine Gefahr von direkten Todesfällen oder schweren Körperverletzungen verursachen, oder organisierter Kriminalität (Abs. 1). Aus diesen Anforderungen ist ersichtlich, dass sie – meist im Bereich der Staatssicherheit oder der öffentlichen Ruhe, Ordnung und Sicherheit – zum Zwecke der Strafverfolgung oder der Gefahrenabwehr erlaubt wird. Diese TKÜ wird jedoch vom Gericht kontrolliert, da sie von der Ermittlungsbehörde jederzeit missbraucht werden kann. Die Behörde muss unverzüglich nach Beginn ihrer Vollstreckung gemäß § 6 das Gericht um Erlaubnis ersuchen und die Maßnahme dann sofort einstellen, wenn sie innerhalb von 36 Stunden nach dem Zeitpunkt der Vollstreckung keine Erlaubnis erhält (Abs. 2). Wenn die Polizei die Eil-TKÜ ausführt, muss diese grundsätzlich im Voraus vom Staatsanwalt befohlen werden, aber in dringenden Fällen kann diese staatsanwaltliche Genehmigung nach Beginn ihrer Vollstreckung unverzüglich eingeholt werden (Abs. 3). Eine TKÜ im Eilfall ohne gerichtliche Erlaubnis ist eine rechtswidrige Ermittlungsmaßnahme und die durch diese gewonnenen TK-Inhalte dürfen als illegal erlangte Beweise nicht dienen.[419] Bei dieser TKÜ muss die sie durchführende Behörde ein „Formular zur Eil-TKÜ“ ausfüllen und in ihrem Organ oder ihrer Einrichtung muss ein „Buch zur Eil-TKÜ“ gehalten werden (Abs. 4). Wenn eine Eil-TKÜ innerhalb von 36 Stunden beendet wird und somit keine gerichtliche Genehmigung erforderlich ist, muss der zuständige LOStA an das entsprechende Gericht innerhalb von 7 Tagen ein „Unterrichtungsschreiben der Eil-TKÜ“ übersenden, das durch die durchführende Behörde erstellt wird (Abs. 5). Darin sind nicht nur Zweck, Gegenstände, Umfang, Zeitraum und Durchführungsort und -methode der Eil-TKÜ, sondern auch die Gründe, warum der Antrag nicht gestellt werden konnte, anzugeben (Abs. 6).

In Bezug auf den o. g. Regelungsinhalt wird u. a. kritisiert, dass eine TKÜ für 36 Stunden ohne gerichtliche Kontrolle durchgeführt werden kann. Die Ermittlungsbehörde kann die TKÜ absichtlich innerhalb von 36 Stunden beenden, um eine gerichtliche Überwachung zu vermeiden. Außerdem sieht der § 8 K-KGSG nur vor, dass die Eil-TKÜ, die nicht gerichtlich genehmigt wurde, unverzüglich eingestellt

der Gesetzgeber diesen verfassungswidrigen Zustand liegen lassen und erst am 31. Dezember 2019 den Sinn und Zweck des Beschlusses von 2010 in das Gesetz umgesetzt.

[419] *Joo-Won Rhee*, K-StPO, 167.

werden soll (Abs. 2), und er erwähnt nicht die Verwertbarkeit von Daten, die zwischenzeitlich gewonnenen wurden. Die Daten, die durch die TKÜ gewonnen wurden, die innerhalb von 36 Stunden beendet wurde oder wegen Erfolglosigkeit der Einholung gerichtlicher Genehmigung eingestellt wurde, sind daher nicht illegal, sodass die Ermittlungsbehörde sie verwenden kann.[420] Dies ist ein erheblicher Rechtsfehler und bedarf es einer umgehenden Überarbeitung.

c) Durchführung sowie Schweigepflichten und Einschränkung der Verwertung: §§ 9, 11, 12, 15 K-KGSG

(1) Die Ermittlungsbehörde kann die TKÜ (auch im Eilfall) nicht nur selbst durchführen, sondern auch den TK-Dienstanbieter mit ihrer Durchführung beauftragen oder ihn um eine Mitwirkung zur Durchführung ersuchen (§ 9 Abs. 1 K-KGSG).[421] Im letzteren Fall muss sie dem Anbieter eine Abschrift des Deckblattes des Erlaubnisscheins nach § 5 Abs. 5 K-KGSG bzw. des Formulars zur Eil-TKÜ nach § 8 Abs. 4 K-KGSG aushändigen und er muss sie für den in der DVO festgelegten Zeitraum aufbewahren (Abs. 2). Der Anbieter, der eine TKÜ durchführt oder bei der Durchführung mitwirkt, muss schriftlich Zweck und Gegenstände der Maßnahme sowie Datum und Uhrzeit ihrer Durchführung dokumentieren und die Dokumentation für den in der DVO festgelegten Zeitraum verwahren (Abs. 3). Wenn bei Durchführung die Zielrufnummer der TKÜ, die im Erlaubnisschein oder Formular angegeben ist, nicht mit ihrem Inhaber übereinstimmt, kann der Anbieter die Durchführung verweigern, und keinesfalls sind Zugangscodes zu offenbaren (Abs. 4).

Bezüglich des Verstoßes gegen das Durchführungsverfahren der TKÜ und des daraus resultierenden Beweisverwertungsverbots hat *K-OGH* am 13. Oktober 2016 eine sinnvolle Entscheidung getroffen.[422] Nach dem Sachverhalt der Entscheidung erhielt die Ermittlungsbehörde am 1. März 2014 gemäß § 6 Abs. 1 K-KGSG eine gerichtliche Erlaubnis zur Überwachung eines von einem Verdächtigen verwendeten Messenger-Dienstes (*Kakao-Talk*), und im Erlaubnisschein sind die abgesendeten oder empfangenen Nachrichten vom 3. März 2014 bis zum 2. Mai 2014 als Gegenstände angegeben bezüglich des Verdachtes auf einen Verstoß gegen das

[420] *Hyung-Joon Kim*, JCL, Nr. 24, 2005, 213, 227.

[421] Vgl. § 15a K-KGSG [Mitwirkungspflicht des TK-Dienstanbieters] (1) Der TK-Dienstanbieter muss bei der KBeschMaß und der Auskunft über TK-Bestätigungsdaten, die vom Staatsanwalt oder dem Leiter von Kriminalpolizei oder Geheimdiensten nach diesem Gesetz durchgeführt werden, mitwirken. (2) Im DVO werden die Mitwirkungen zur Durchführung der KBeschMaß gemäß Abs. 1, die Dauer der Speicherung von Verkehrsdaten oder sonstige erforderliche Mitwirkungen festgelegt.

§ 41 DVO des K-KGSG [Mitwirkungspflicht des TK-Dienstanbieters] (1) Nach § 15a K-FGSG muss der Anbieter dabei mitwirken, dass die KBeschMaß und die Auskunft über TK-Bestätigungsdaten dann zügig durchgesetzt werden können, wenn es dringende Gefahr für Leben oder Körper einer Person wie Mord, Geiselnahme etc. gibt.

[422] *K-OGHE* vom 13. 10. 2016 – 2016 Do 8137.

Staatssicherheitsgesetz. Die Ermittlungsbehörde hat den Dienstanbieter mit der Durchführung dieser TKÜ beauftragt. Er hatte jedoch keine Einrichtung, die die Inhalte der TK in Echtzeit abfangen konnte, und sie wurden regelmäßig 3 bis 7 Tage nach der Speicherung auf dem Server gemäß seinen Anweisungen gelöscht. Aus diesem Grund hat der Anbieter während des im Erlaubnisschein beschriebenen Überwachungszeitraums regelmäßig alle 3 bis 7 Tage nur die Inhalte, die Gegenstände darstellen, getrennt und diese an die Ermittlungsbehörde übergeben. Der Angeklagte argumentierte, dass die durch eine solche Durchführung der TKÜ erlangten Daten nicht als Beweismittel zulässig seien, da sie gegen die §§ 6, 9 K-KGSG und die im Erlaubnisschein angegebene Durchführungsmethode verstoße. Diesbezüglich hat der *K-OGH* vorausgesetzt, dass bei der Durchführung der TKÜ die Gleichzeitigkeit bzw. Gegenwärtigkeit (vgl. oben a. bb) nicht nur begrifflich, sondern auch tatsächlich erforderlich sind, und entscheiden, dass die dagegen verstoßende Durchführungsmethode illegal ist.

> „Im Erlaubnisschein sind Art, Zweck, Gegenstände, Umfang, Zeitraum und Durchführungsort und -methode der TKÜ bestimmt anzugeben (§ 6 Abs. 6 K-KGSG) und die Ermittlungsbehörde muss unter Einhaltung der im Schein angegebenen Vorgaben die TKÜ vollziehen. Dabei … ist es selbstverständlich, dass der mit dem Vollzug Beauftragte (nach § 9 Abs. 1, 2 K-KGSG) die im Schein angegebene Durchführungsmethode einhalten muss, wie wenn die Ermittlungsbehörde es selbst durchführt. Daher … darf es nicht auf andere Weise durchgeführt werden. Andererseits, wenn die Ermittlungsbehörde den TK-Dienstanbieter mit der Durchführung der TKÜ beauftragt, muss sie die erforderlichen Einrichtungen für die Durchführung bereitstellen (§ 21 Abs. 3 DVO des K-KGSG). Wenn der beauftragte TK-Anbieter nicht über die für die Durchführung erforderlichen Einrichtungen verfügt, muss er somit die Ermittlungsbehörde auffordern, die Einrichtung bereitzustellen, und wenn er die TKÜ ohne diese Aufforderung und ohne Einhaltung der im Schein beschriebenen Weisungen durchgeführt hat, sind die durch eine solche Durchführung erlangten Inhalte der TK … Beweise, die ohne Befolgung legitimen Verfahrens erlangt wurden, und daher dürfen sie nicht als Beweismittel dienen.“ *(Übersetzung vom Autor)*

(2) Beamte und Angestellte von Dienstanbietern, die sich an der Erlaubnis, Durchführung, Benachrichtigung von TKÜ und Erstellung diesbezüglicher Dokumente beteiligen oder daran beteiligt haben, dürfen Informationen, die sie dienstlich erfahren haben, nicht veröffentlichen und offenbaren, es sei denn, sie werden gemäß § 12 K-KGSG verwendet (§ 11 Abs. 1, 2 K-KGSG). Dies gilt auch für alle anderen, die die Informationen kennen (Abs. 3).

Nach § 12 K-KGSG dürfen die durch die TKÜ gemäß § 9 K-KGSG erlangten Inhalte von Postsendungen oder TK nur in folgenden Fällen verwendet werden: 1. wenn sie zur Ermittlung, Verfolgung oder Verhinderung einer in § 5 Abs. 1 K-KGSG genannten Straftat, aufgrund deren die TKÜ erlaubt wurde, und den damit zusammenhängenden Straftaten verwendet werden, 2. wenn sie in Disziplinarverfahren wegen Straftaten nach Nr. 1 verwendet werden, 3. wenn sie in einer Klage auf Schadenersatz verwendet werden, die von dem von der Maßnahme Betroffenen eingereicht wird, 4. wenn sie nach den Bestimmungen anderer Gesetze verwendet werden. Der „Zusammenhang“ von Straftaten in der Nr. 1 versteht der *K-OGH*

genauso wie die Bedeutung von „Relevanz“, die die Grenzen des Umfangs der Beschlagnahme und Durchsuchung bestimmt.[423] Das heißt, der Gerichtshof versteht die „Relevanz“ i. S. v. §§ 106 Abs. 1, 109 Abs. 1, 215 K-StPO, die ein Kriterium für den Umfang der Gegenstände der Beschlagnahme ist, die bei der allgemeinen Durchsuchung und Beschlagnahme rechtmäßig sichergestellt werden können, und den „Zusammenhang“ i. S. d. § 12 Nr. 1 K-KGSG, der maßgebend für den Umfang der Verwertung der durch die TKÜ erlangten Informationen ist, begrifflich gleich (vgl. dazu eingehend Kapitel 4, D. II. 2.).[424]

Schließlich wird die TKÜ auch von dem Parlament beaufsichtigt. Der zuständige Ausschuss des Parlaments kann nämlich bei Bedarf beim Leiter der Behörde für Gerichtsverwaltung und der Ermittlungsbehörde einen Bericht über TKÜ anfordern und außerdem die Orte bezüglich der Überwachung selbst untersuchen und in Augenschein nehmen (§ 15 K-KGSG).

d) Benachrichtigung und effektiver Rechtsschutz: §§ 9a, 9b und 13b K-KGSG[425]

aa) Übersicht über die Inhalte der Vorschriften

Die Ermittlungsbehörde muss i. R. d. Durchführung der TKÜ gemäß § 6 Abs. 1, 2 und § 8 Abs. 1 K-KGSG „innerhalb von 30 Tagen ab dem Datum des Beschlusses, die öffentliche Klage zu erheben oder davon abzusehen, ausgenommen des Beschlusses zur Verfahrenseinstellung, (zum maßgeblichen Zeitpunkt der Benachrichtigung)“ „den TK-Teilnehmer, an den sich die Maßnahme richtete“, „von ihrer Durchführung, Durchführungsbehörde und -zeitraum etc.“ schriftlich benachrichtigen (§ 9a Abs. 1, 2 K-KGSG).[426] Diese Benachrichtigung kann jedoch zurückgestellt werden, wenn erhebliche Bedenken bestehen, dass sie „die Staatssicherheit oder die öffentliche Ruhe, Ordnung und Sicherheit gefährden oder eine schwere Gefährdung des Lebens oder des Körpers einer Person“ herbeiführen würde (Abs. 4). Dazu muss die Ermittlungsbehörde im Voraus die „Genehmigung des zuständigen LOStA“ einholen (Abs. 5). Werden die Gründe für die Zurückstellung nach Abs. 4 aufgelöst, muss die Ermittlungsbehörde innerhalb von 30 Tagen ab dem Datum der

[423] *K-OGHE* vom 25. 1. 2017 – 2016 Do 13489; vgl. *ders.* vom 5. 12. 2017 – 2017 Do 13458.

[424] *Joo-Won Rhee*, K-StPO, 160 f.

[425] § 9a K-KGSG regelt die Benachrichtigung über die Durchführung von KBeschMaß, § 9b K-KGSG dieselbe über die (heimliche) Durchführung von Beschlagnahme und Durchsuchung der bereits gesendeten und empfangenen TK aufgrund der K-StPO und § 13b K-KGSG dieselbe über die Erhebung von Verkehrsdaten. Diese Vorschriften sehen nachträgliche Benachrichtigung über heimliche Maßnahmen vor, und ihr Inhalt ist im Wesentlichen identisch. Daher werden sie hier zusammen beschrieben.

[426] Vgl.: § 9a Abs. 3 K-KGSG sieht die Benachrichtigung über die Durchführung von KBeschMaß durch Geheimdienste vor. Nach der Vorschrift ist die Durchführung der Maßnahme „innerhalb von 30 Tagen ab dem Datum ihrer Beendigung“ „dem TK-Teilnehmer, an den sich die Maßnahme richtete“, schriftlich mitzuteilen.

Auflösung benachrichtigen (Abs. 6). § 9b K-KGSG sieht die Benachrichtigung über die – heimliche – Durchführung der Durchsuchung und Beschlagnahme der bereits gesendeten oder empfangenen TK vor, die auf allgemeinen Vorschriften von K-StPO beruht. Hier sind die zu benachrichtigende Person, der maßgebliche Zeitpunkt und der Inhalt der Benachrichtigung auf dieselbe Weise wie in § 9a Abs. 1, 2 K-KGSG vorgesehen, aber es gibt keine Regelung über die Zurückstellung der Benachrichtigung. Hinsichtlich der Normenklarheit ist auch hier eine Rechtsgrundlage erforderlich.

Andererseits sieht § 13b K-KGSG eine Benachrichtigung des Betroffenen über die Erhebung von Verkehrsdaten vor. Diese Vorschrift wurde am 31. Dezember 2019 nach dem Beschluss von K-VerfG vom 28. Juni 2018 (2012 HunMa 191 etc.)[427] geändert (Gesetz Nr. 16849).[428] Die Ermittlungsbehörde muss i. R. d. Verkehrsdatenerhebung gemäß § 13 K-KGSG „den Betroffenen, an den sich die Maßnahme richtete", „von ihrer Durchführung, Durchführungsbehörde und -zeitraum" nach folgenden Maßgaben schriftlich benachrichtigen (Abs. 1): innerhalb von 30 Tagen ab dem Datum des Beschlusses, die öffentliche Klage zu erheben oder davon abzusehen (Nr. 1), innerhalb von 30 Tagen nach einem Jahr (nach 3 Jahren für die Straftaten, bei denen die TKÜ gemäß § 6 Abs. 8 K-KGSG für maximal 3 Jahre zulässig ist) ab dem Datum des Beschlusses zur Verfahrenseinstellung (Nr. 2), innerhalb von 30 Tagen nach einem Jahr (nach 3 Jahren für die Straftaten, bei denen die TKÜ gemäß § 6 Abs. 8 K-KGSG für maximal 3 Jahre zulässig ist) ab dem Datum der Verkehrsdatenerhebung, wenn die Ermittlung noch nicht beendigt wird (Nr. 3). In den Abs. 2 bis 4 ist die Zurückstellung der Benachrichtigung vorgesehen, deren Inhalt fast dem Inhalt von § 9a Abs. 4 bis 6 entspricht. Hinzukommen aber als Gründe für die Zurückstellung die Risiken, ein faires Justizverfahren zu hemmen, wie Gefahr der Verdunkelung, der Flucht, der Bedrohung von Zeugen etc., und die Ehre oder die Privatsphäre des Beschuldigten, des Opfers oder anderer Verfahrensbeteiligten zu beeinträchtigen (Abs. 2). Abs. 5 – 6 schreibt das Verfahren zur Benachrichtigung über „Gründe für die Maßnahme" vor. Dies ist nicht im Inhalt der ersten Benachrichtigung gemäß Abs. 1 enthalten und der von Maßnahme Betroffene kann nach Erhalt der Mitteilung über die Verkehrsdatenerhebung nur deren Gründe durch ein gesondertes Verfahren beantragen (Abs. 5). Die Ermittlungsbehörde hat sie dabei innerhalb von 30 Tagen nach Eingang des Antrags schriftlich mitzuteilen, es sei denn, die oben genannten Gründe für die Zurückstellung der Benachrichtigung liegen vor (Abs. 6).

[427] *K-VerfGE* 30-1, 564: Beschluss zur Echtzeit-Lokalisierung.

[428] Bis dahin wurde § 9a K-KGSG hierauf einfach entsprechend angewendet (§ 13b Abs. 2 K-KGSG a. F.).

bb) Probleme und Kritik

Die o. g. Vorschriften zur Benachrichtigung werden in der Literatur wegen ihres unzureichenden Inhalts stark kritisiert. Vor allem widersprechen sie übergreifend dem Sinn und Zweck des Benachrichtigungssystems, das dem nachträglichen Rechtsschutz des Betroffenen bei heimlichen Zwangsmaßnahmen dient.

Zuerst sollten bezüglich der Adressaten der Benachrichtigung die Formulierung „den TK-Teilnehmer" aus §§ 9a, 9b K-KGSG durch die Formulierung „den Betroffenen (der Maßnahme)" aus § 13b K-KGSG ersetzt werden, denn auch eine Person, die keinen TK-Teilnehmer darstellt, aber Nachrichten tatsächlich gesendet oder empfangen hat, soll über die Verletzung ihrer Grundrechte unterrichtet werden können.[429] Die TK wird i. d. R. als Informationsaustausch von zwei oder mehr Personen, die räumlich getrennt sind, verstanden und daher greift die TKÜ nicht nur in das Grundrecht des Beschuldigten, an den sich die Maßnahme richtete, sondern auch in das der anderen Beteiligten der betroffenen TK. Aber wenn sich die beteiligte Person der TK, die tatsächlich überwacht wurde, nicht auf den untersuchten Sachverhalt bezieht und für die Benachrichtigung eine Nachforschung zur Feststellung ihrer Identität erforderlich ist, sollte die Benachrichtigung nach dem Grundsatz der Verhältnismäßigkeit gesetzlich ausgeschlossen werden können.[430]

Zudem sollten bezüglich des maßgeblichen Zeitpunkts der Benachrichtigung die Formulierung „innerhalb von 30 Tagen ab dem Datum des Beschlusses, die öffentliche Klage zu erheben oder davon abzusehen, ausgenommen des Beschlusses zur Verfahrenseinstellung," aus §§ 9a Abs. 1, 2, 9b, 13b Abs. 1 Nr. 1 K-KGSG durch die Formulierung „sofort am Tag der Beendigung (der Maßnahme)" ersetzt werden. Nach den geltenden Vorschriften hängt nämlich die Wahrnehmung der Verletzung der Grundrechte durch den Betroffenen vom Beschluss der StA ab, wobei die Gefahr

[429] *Hyung-Joon Kim*, JCL, Nr. 24, 2005, 213, 228; *Chan-Keol Park*/*Dong-Wook Kang*, JLPR, 20-1, 2014, 315, 322 f.; *Seok-soon Im*, KCR, 27-2, 2016, 203, 215 f.; *Joongwook Park*, CRCL, Nr. 68, 2020, 97, 119.

[430] *Kil-Young Oh*, JML, 14-1, 2015, 33, 49 [Fn. 51]; *Jina Cha*, KLAJ, 67-2, 2018, 366, 406–408; *Joongwook Park*, CRCL, Nr. 68, 2020, 119. Andererseits hat das *K-VerfG* am 26. April 2018 eine Verfassungsbeschwerde überprüft, dass der § 9b K-KGSG, in dem vorgesehen ist, dass nur der „TK-Teilnehmer (meist Beschuldigte)", an den sich die Maßnahme unmittelbar richtete, abgesehen von dem „TK-Partner", an den sich die Maßnahme mittelbar richtete, benachrichtigt wird, verfassungswidrig sei (*K-VerfGE* vom 26. 4. 2018. – 2014 HunMa 1178: 30-1, 675). In dieser Entscheidung erklärte das Gericht, dass der Adressat der Maßnahme im Strafverfahren nach dem Rechtsstaatsprinzip vom Art. 12 K-Verf über ihre Durchführung angemessen informiert werden und ihm die Gelegenheit zur Abgabe schriftlicher oder mündlicher Erklärung gegeben werden sollte (a. a. O. 681), aber dass zur Gewährleistung der Heimlichkeit der Ermittlung es nicht problematisch ist, dass der andere TK-Partner nicht als die zu benachrichtigende Person bestimmt ist (a. a. O. 682). Das Gericht betont jedoch durch ergänzende Erklärung die Notwendigkeit einer institutionellen Garantie, um den Eingriff in Grundrechte des TK-Partners zu minimieren. Wenn höchstpersönliche oder sensible Informationen des unverdächtigen Partners im beschlagnahmten oder durchsuchten TK-Inhalt enthalten sind, sollte er darüber informiert werden, dass die Informationen von der Ermittlungsbehörde erhoben wurden, um ihrem Missbrauch zu begegnen (a. a. O. 682–684).

besteht, dass er nach Willkür der StA erfolgt.[431] Fasst die StA u. a. nach Beendigung der Maßnahme über einen längeren Zeitraum keinen Beschluss bezüglich der öffentlichen Klage oder fasst sie einen Beschluss, das Verfahren einzustellen, so befindet sich der Betroffene weiterhin, in der Tat unbegrenzt, in einem unbilligen Zustand, in dem er den staatlichen Eingriff in seine Grundrechte nicht zur Kenntnis nimmt.[432] Dies widerspricht dem Sinn und Zweck der Benachrichtigung des Grundrechtsschutzes und greift i. V. m. dem Mangel des K-KGSG, insb. dem Fehlen eines nachträglichen effektiven Rechtsschutzes (vgl. unten cc)), erheblich in Grundrechte ein.[433] Darüber hinaus sollte die Frist der Benachrichtigung von 30 Tagen und von 1 Jahr oder 3 Jahren gemäß § 13b Abs. 1 K-KGSG gestrichen werden, da sie einfach aus einer Denkweise zugunsten der Ermittlungsbehörde stammt.[434] Soll die Benachrichtigung nach Beendigung der Maßnahme zurückstellt werden, reicht es aus, dass dies nach den Vorschriften zur Zurückstellung erfolgt.[435]

Es gibt aber auch mehrere Probleme mit der Regelung für die Zurückstellung der Benachrichtigung (§ 9a Abs. 4 – 6 und § 13b Abs. 2 – 4 K-KGSG). Zuerst ist die Zurückstellung nur mit einer administrativen aufsichtlichen Kontrolle, nämlich mit der Genehmigung vom LOStA, ohne gerichtliche Intervention zulässig. Dies berücksichtigt jedoch nicht, dass für wirksamen Rechtsschutz bei heimlichen Ermittlungsmaßnahmen eine nachträgliche Benachrichtigung vorausgesetzt werden muss.[436] Dies steht u. a. im Widerspruch zur Ausführung im Beschluss zur Echtzeit-Lokalisierung des K-VerfG, dass für die Zurückstellung der Benachrichtigung eine Genehmigung einer unabhängigen und neutralen Instanz erforderlich ist.[437] Insofern kann gesagt werden, dass der Gesetzgeber in der Novellierung des § 13b K-KGSG im Dezember 2019 dem Sinn des Beschlusses des K-VerfG vom Juni 2018 nicht ausreichend Rechnung getragen hat. Darüber hinaus sind die Zurückstellungsgründe wie die Staatssicherheit oder die öffentliche Ruhe, Ordnung und Sicherheit sowie eine schwere Gefährdung des Lebens oder des Körpers einer Person zu abstrakt und umfassend.[438] Dies ist – i. V. m. der oben erwähnten Zuständigkeit des LOStA –

[431] *Seok-soon Im*, KCR, 27-2, 2016, 203, 212; *Joongwook Park*, CRCL, Nr. 68, 2020, 97, 120.

[432] *K-VerfGE* 30-1, 564, 584; 30-2, 481, 501 und dazu 513 [Minderheitsmeinung]; *Kyung-Sin Park*, IHLR, 13-2, 2010, 265, 281; *Seok-soon Im*, KCR, 27-2, 2016, 203, 211; *Jina Cha*, KLAJ, 67-2, 2018, 366, 403 f.; *Joongwook Park*, CRCL, Nr. 68, 2020, 97, 120.

[433] *K-VerfGE* 30-2, 481, 501.

[434] *Jina Cha*, KLAJ, 67-2, 2018, 366, 404 und 409; *Heun-Jae Lee*, KLAJ, 68-4, 2019, 497, 520 f.; *Joongwook Park*, CRCL, Nr. 68, 2020, 97, 120 f.

[435] *Heun-Jae Lee*, KLAJ, 68-4, 2019, 497, 520 f.; *Joongwook Park*, CRCL, Nr. 68, 2020, 97, 121.

[436] *Joongwook Park*, CRCL, Nr. 68, 2020, 97, 122; vgl. *BVerfGE* 109, 279, 364 [Rn. 292].

[437] *K-VerfGE* 30-1, 564, 585. Im Beschluss über die Paket-Überwachung von 2018 hat die Minderheitsmeinung i. R. d. § 9a K-KGSG auf das gleiche Problem hingewiesen (*K-VerfGE* 30-2, 481, 514).

[438] *Hyung-Joon Kim*, JCL, Nr. 24, 2005, 213, 229; *Seok-soon Im*, KCR, 27-2, 2016, 203, 213; *Heun-Jae Lee*, KLAJ, 68-4, 2019, 497, 521; *Joongwook Park*, CRCL, Nr. 68, 2020, 97,

praktisch so, als würde der StA eine Möglichkeit der unbegrenzten Zurückstellung gewährt.[439] Außerdem ist es auch problematisch, dass es keine Zurückstellungsdauer gibt; d. h., eine einmal zurückgestellte Benachrichtigung kann weiterhin zurückgestellt werden, es sei denn, die Ermittlungsbehörde hat erneut Interesse daran oder sie stellt selbst fest, dass die Gründe für die Zurückstellung gelöst wurden.[440] Aus alledem bleibt die Zurückstellung der Benachrichtigung nach den geltenden Vorschriften der StA praktisch uneingeschränkt vorbehalten.

Schließlich schreiben §§ 9a Abs. 1, 2, 9b, 13b Abs. 1 K-KGSG vor, dass „Durchführung, Durchführungsbehörde und -zeitraum etc." jeder Maßnahme mitgeteilt werden müssen. In der Praxis enthält dies jedoch keine „Gründe für die Maßnahme", nämlich die (angewendeten) Strafvorschriften, die Bezeichnung der Tat und den Inhalt des Verdachts.[441] Hinsichtlich des Zwecks des Benachrichtigungssystems ist dies fragwürdig, da eine Beschwerde des Betroffenen gegen die Maßnahme erheblich beschränkt ist, wenn er keine Gründe für ihre Durchführung kennt.[442] Diesbezüglich wurde durch die Änderung im Dezember 2019 eine neue Regelung eingeführt, die es dem bereits benachrichtigten Betroffenen, soweit es die Verkehrsdatenerhebung betrifft, ermöglicht, die Gründe für die Durchführung der Maßnahme abgesehen von bestimmten Fällen gesondert zu beantragen und darüber benachrichtigt zu werden. Aber ihr Inhalt scheint an sich widersprüchlich zu sein. Denn sie sieht vor, dass nur der „benachrichtigte" Betroffene die Gründe für die Maßnahme beantragen kann (Abs. 5), aber auch in diesem Fall nicht benachrichtigt werden kann, wenn Gründe für die Zurückstellung nach Abs. 2 vorliegen (Abs. 6). Die Ausnahme von Abs. 6 ist bedeutungslos oder gleichbedeutend damit, der Ermittlungsbehörde die Möglichkeit zu gewähren, die Benachrichtigung über die Gründe für die Maßnahme erneut auf unbestimmte Zeit zurückzustellen.[443]

---

122. Diese Kritik stimmt mit der Stellungnahme des *BVerfG* in der Entscheidung zur Wohnraumüberwachung von 2003 (*BVerfGE* 109, 279, 366 [Rn. 301]) überein, wonach der Begriff der „öffentlichen Sicherheit" wegen seiner Reichhaltigkeit keine Zurückstellung oder keinen Ausschluss der Benachrichtigung rechtfertigt. Andererseits ist die Gefährdung des Untersuchungszwecks nicht in den Zurückstellungsgründen in den Benachrichtigungsvorschriften des K-KGSG – anders als in § 101 Abs. 5 S. 1 StPO – enthalten. Denn im K-KGSG erfolgt die Benachrichtigung nach dem Beschluss, die öffentliche Klage zu erheben oder davon abzusehen, nämlich nach Beendigung der Ermittlung.

[439] *Joongwook Park*, CRCL, Nr. 68, 2020, 97, 122; vgl. *Heun-Jae Lee*, KLAJ, 68-4, 2019, 497, 521: Die Genehmigung von LOStA wird nur zu einer Formalität.

[440] *Hyung-Joon Kim*, JCL, Nr. 24, 2005, 213, 229; *Seok-soon Im*, KCR, 27-2, 2016, 203, 213; *Jina Cha*, KLAJ, 67-2, 2018, 366, 409; *Heun-Jae Lee*, KLAJ, 68-4, 2019, 497, 521; *Joongwook Park*, CRCL, Nr. 68, 2020, 97, 122.

[441] §§ 8, 15, 22 Richtlinien für Benachrichtigungen bzw. Unterrichtungen des K-KGSG; vgl. *K-VerfGE* 30-1, 564, 584; 30-2, 481, 513 f.

[442] *K-VerfGE* 30-1, 564, 585; *Joongwook Park*, CRCL, Nr. 68, 2020, 97, 123.

[443] *Joongwook Park*, CRCL, Nr. 68, 2020, 97, 124.

cc) Mangel an Verfahren zum nachträglichen Rechtsschutz

Im K-KGSG gibt es derzeit keine Rechtsgrundlage, die es dem benachrichtigten Betroffenen ermöglicht, nach Beendigung der Maßnahme die gerichtliche Überprüfung der Rechtmäßigkeit der Art und Weise ihres Vollzugs zu beantragen.[444] Wenn die nachträgliche Benachrichtigung bei heimlichen Ermittlungsmaßnahmen nicht mit der Anfechtbarkeit der Rechtmäßigkeit ihres Vollzugs verbunden ist, ist es jedoch praktisch unmöglich, einen Amtsmissbrauch bei der Datenerfassung durch die Ermittlungsbehörde zu verhindern und den Rechtsbehelf wirksam einzulegen.[445] Dies verstößt nicht nur gegen den effektiven Rechtsschutz aufgrund des Rechts auf Anrufung der Gerichte (Art. 27 Abs. 1 K-Verf[446]), sondern widerspricht auch u. a. der Ausführung des K-VerfG in jüngsten diesbezüglichen Beschlüssen:

> „Selbst wenn die Geheimhaltung der Ermittlungen gewährleistet werden soll, muss dem von Daten Betroffenen, an den sich die TKÜ richtete, wie etwa dem Beschuldigten, die Durchführung (der Maßnahme) in angemessener Weise mitgeteilt und eine Gelegenheit zur Stellungnahme tatsächlich gegeben werden, um einen Amtsmissbrauch der Ermittlungsbehörde zuverlässiger zu verhindern und die Grundrechte des Verdächtigen etc. zu schützen … Dies ermöglicht es dem Beschuldigten zu überprüfen, ob die Maßnahme nach einem legitimen Verfahren durchgeführt wurde, ob die erfassten Daten für den Zweck verwendet wurden oder ob sie nach dem in K-DSG etc. festgelegten Verfahren vernichtet wurden. Auf diese Weise kann der Beschuldigte bzw. der von Daten Betroffene, falls illegale oder unfaire Handlungen der Ermittlungsbehörde festgestellt werden, einen wirksamen Rechtsbehelf erhalten, etwa indem er bei der Ermittlungsbehörde oder dem Gericht Einspruch einlegt.“[447] *(Übersetzung vom Autor)*

Das Versäumnis des Gesetzgebers, in den aufeinanderfolgenden Änderungen von 31. Dezember 2019 und 24. März 2020, die nach den beiden Beschlüssen von 2018

---

[444] Vgl. § 101 Abs. 7 S. 2 StPO. In Südkorea kann der Betroffene i. d. R. gegen eine rechtswidrige Handlung einer Ermittlungsbehörde in der Ermittlungsphase beim Gericht Beschwerde einlegen (§ 417 K-StPO). Nach der ständigen Rspr. des *K-OGH* ist ein Einspruch nach dieser Vorschrift (entsprechende Beschwerde) jedoch nur bei den darin aufgeführten Maßnahmen zulässig, nämlich Verhaftung, Beschlagnahme, Rückgabe beschlagnahmter Gegenstände und einer Maßnahme gegen das Recht auf Verteidigerkonsultation oder dessen Anwesenheit bei der Vernehmung, aber er ist bei sonstigen Maßnahmen wie z. B. Durchsuchung, den Maßnahmen nach K-KGSG nicht gestattet (vgl. Kapitel 4, D. II. 4.).

[445] *Sung-Gi Hwang*, JML, 14-1, 2015, 1, 18 und 21; *Jina Cha*, KLAJ, 67-2, 2018, 366, 410 f.; *Sang-Hyun Shin*, HUFSLJ, 43-3, 2019, 93, 114; *Joongwook Park*, CRCL, Nr. 68, 2020, 97, 128 f.

[446] Art. 27 Abs. 1 K-Verf: Jeder Bürger hat das Recht, nach dem Gesetz vor Gericht zu stehen und rechtliches Gehör durch Richter zu erhalten, die nach der Verfassung und dem Gesetz qualifiziert sind.

[447] *K-VerfGE* 30-1, 564, 584. Bei diesem Beschluss handelt es sich um die Prüfung der Verfassungsbeschwerde am 28. Juni 2018 (2012 HunMa 191 etc.), ob die Erhebung von Standortdaten in Echtzeit nach §§ 13 ff. K-KGSG zulässig ist, und die Zitate im Text wurden i. R. d. Prüfung der Verfassungsmäßigkeit des § 13b K-KGSG geschrieben. Die gleiche Erklärung wiederholt sich auch in der Minderheitsmeinung der Entscheidung über die Paket-Überwachung (2016 HunMa 263) vom 30. August 2018 (*K-VerfGE* 30-2, 481, 513).

(2012 HunMa 191 etc. und 2016 HunMa 263) erfolgten, keine Rechtsgrundlage zum wirksamen Rechtsschutz nach der Benachrichtigung zu schaffen, verstößt daher nicht nur gegen das Recht des Betroffenen auf Anrufung der Gerichte, sondern auch gegen den Zweck und die Absicht der obigen Beschlüsse des K-VerfG. Es bedarf einer dringenden Gesetzesnovellierung für die Schaffung der Vorschrift zum Rechtsbehelf. Dies gilt auch bei Betrachtung des Gesetzes zur Verwendung und dem Schutz von DNA-Daten zur Identifikation (Kurztitel: DNA-Gesetz), das kürzlich vom K-VerfG aus demselben Grund für verfassungswidrig erklärt wurde. Im Beschluss vom 30. August 2018 (2016 HunMa 344 etc.) hat das Gericht aufgrund des Rechts auf Anrufung der Gerichte verlangt, dass im Zuge der Durchführung der richterlichen Anordnung für die Entnahme von Proben zur DNA-Identifizierung dem Betroffenen eine Gelegenheit zur Stellungnahme gewährleistet wird oder, falls nicht, ein wirksamer Rechtsbehelf geschaffen wird, um nach Beendigung der Maßnahme die Überprüfung der Rechtmäßigkeit der Art und Weise ihres Vollzugs zu beantragen.[448] Nach diesem Beschluss hat der Gesetzgeber am 21. Januar 2020 den § 8a DNA-Gesetz[449] zum Beschwerdeverfahren geschaffen (Gesetz Nr. 16866).

e) Paket-Überwachung

(1) Die Überwachung von Internetleitungen, die die über eine Internetleitung gesendete und empfangene TK umfassend erfasst, wird in Form einer sog. „Paket-Überwachung" durchgeführt, d. h., Pakete in Form elektronischer Signale während des Übertragungsvorgangs zu sichern, zu duplizieren und zu rekonstruieren, um ihren Inhalt zu erfassen.[450] Dabei erfolgt die Auswertung der Pakete technisch durch DPI (Deep Packet Inspection).[451] Gegenwärtig wird diese Maßnahme in Südkorea i. d. R. von Geheimdiensten zur Verhütung und Ermittlung von Straftaten bezüglich der Staatssicherheit oder der öffentlichen Ruhe, Ordnung und Sicherheit eingesetzt. Die Paket-Überwachung durch den Staat wurde erstmals im Jahr 2008 der Öffentlichkeit durch einen Fall vorgestellt, in dem die Verdächtigten wegen des Verstoßes

[448] *K-VerfGE* vom 30. 8. 2018 – 2016 HunMa 344 etc. (30-2, 516, 536 f.). Die Entnahme von Proben zur DNA-Identifizierung ist – anders als bei Maßnahmen des K-KGSG – eine offene Maßnahme, die es dem Betroffenen ermöglicht, ihre Durchführung zur Kenntnis zu nehmen und ggf. illegalen Ermittlungen zu begegnen.

[449] § 8a DNA-Gesetz [Beschwerdeverfahren] (1) Der Betroffene, von dem ein Probenmaterial durch richterliche Anordnung zur Entnahme von Proben zur DNA-Identifizierung nach § 8 Abs. 1 und 2 entnommen wurde, kann innerhalb von 7 Tagen ab dem Datum der Entnahme beim für den Durchführungsort zuständigen Gericht oder dem Gericht der zuständigen StA, der der Staatsanwalt angehört, die Aufhebung der Maßnahme beantragen. (2) Der Antrag nach Abs. 1 ist schriftlich beim zuständigen Gericht einzureichen. (3) Wird der Antrag nach Abs. 1 gestellt, gelten die Vorschriften der §§ 409, 413, 414, 415 K-StPO entsprechend.

[450] *Kil-Young Oh*, DLS, Nr. 41, 2009, 391, 410 f.; *Yangsub Kwon*, KorLR, Band 39, 2010, 177, 183.

[451] *Kil-Young Oh*, DLS, Nr. 41, 2009, 391, 411 ff.; *Yangsub Kwon*, KorLR, Band 39, 2010, 177, 184; *Hee-Young Park*, IIS, 2-1, 2011, 105, 106 ff.

gegen das Staatssicherheitsgesetz angeklagt wurden.[452] Der Kern der Kritik an der Paket-Überwachung besteht darin, dass sie de facto zur Zulassung einer „Generalermächtigung" führt, weil sie der Ermittlungsbehörde ermöglicht, alle Daten zu erfassen, die über die vom Betroffenen verwendete Internetleitung übertragen wurden.[453] Das heißt, selbst wenn ein Richter eine Paket-Überwachung mit der konkreten Bestimmung ihrer Zielperson und ihres Umfangs erlaubt, hat die Ermittlungsbehörde keine andere Wahl, als wegen ihrer technischen Eigenschaften im Zuge der Durchführung personenbezogene Daten umfassend zu erheben, aber im K-KGSG gibt es keine ausreichenden flankierenden Maßnahmen gegen diese Umstände. Daher wurde in der Literatur argumentiert, dass eine eigenständige Ermächtigungsnorm für die Paket-Überwachung[454] oder eine zusätzliche Vorkehrung für den Verlauf ihrer Durchführung[455] erforderlich ist.[456]

(2) Der K-OGH hat jedoch in seinem Urteil von 2012 festgestellt, dass die TK über die Internetleitung zur TK i. S. d. § 2 Nr. 3 K-KGSG gehört, und daher die Paket-Überwachung gemäß § 5 Abs. 1 K-KGSG zulässig ist.[457] Das K-VerfG hat hingegen in seinem Beschluss vom 30. August 2018 (2016 HunMa 263) erklärt, dass die bestehenden Vorschriften zur TKÜ aus §§ 5 ff. K-KGSG, soweit es die Paket-Überwachung betrifft, den Anforderungen der ultima ratio und Abwägung aus dem

[452] *Mankee Min*, CRCL, Nr. 53, 2016, 214, 227; *Gi-Young Cho*, JCL, 26-4, 2014, 105, 116; Der repräsentative Zeitungsartikel dazu ist Hankyoreh Shinmun, „Der Nationale Nachrichtendienst, er hat einen Blick auf Dein gesamtes Internet geworfen", 31. 8. 2009, <http://www.hani.co.kr/arti/society/rights/374120.html>, Abruf: 31. 12. 2020.

[453] *Kil-Young Oh*, DLS, Nr. 41, 2009, 391, 420 f.; *Yangsub Kwon*, KorLR, Band 39, 2010, 177, 190.

[454] *Kil-Young Oh*, DLS, Nr. 41, 2009, 391, 421 – 422; *Hee-Young Park*, IIS, 2-1, 2011, 105, 121; im gleichen Sinn *Gi-Young Cho*, JCL, 26-4, 2014, 105, 121 – 125: Dafür ist eine erneute umfassende Ausgestaltung der Ermächtigungsnorm zur Paket-Überwachung erforderlich. Im Vergleich zur allgemeinen TKÜ sollte der Umfang von Katalogstraftaten enger beschränkt werden und das Erlaubnisverfahren des Gerichts strenger gestärkt werden, wobei die Kontrolle des Gerichts über den Prozess der Vollstreckung und die erlangen Daten erforderlich ist.

[455] *Mankee Min*, CRCL, Nr. 53, 2016, 214, 259; vgl. *Yangsub Kwon*, KorLR, Band 39, 2010, 177, 192 f.: Die erlangen Pakete sollten von einem unabhängigen Dritten, nicht von der Ermittlungsbehörde, analysiert und dann nur sollten die von der Ermittlungsbehörde geforderten Inhalte geliefert werden.

[456] Der Ansicht, dass diese Maßnahme selbst verfassungswidrig ist, ist *Dong-seok Oh*, Verfassungsrechtliche Probleme von Paket-Überwachung, öffentliche Anhörung über Probleme und Verbesserungsvorschläge von Paket-Überwachung vom 1. Februar 2010, Die Demokratische Partei, 21 – 23. Demnach ermöglicht diese Maßnahme eine umfassende Überwachung von zahlreichen unbestimmten Personen unabhängig von richterlicher Anordnung, sodass die Intensität des Grundrechtseingriffs im Vergleich zum Untersuchungszweck übermäßig hoch ist und somit dies gegen die Grundsätze wie Gewaltenteilung, Verhältnismäßigkeit und Garantie eines rechtsstaatlichen Verfahrens verstößt.

[457] *K-OGHE* vom 11. 10. 2012 – 2012 Do 7455. In dieser Entscheidung sagte der Gerichtshof, dass die Rechtmäßigkeit der Paket-Überwachung „*nicht geändert wird, nur weil ihrer Natur nach Bedenken bestehen, dass TK-Inhalte, die für den Zweck der Untersuchung irrelevant sind, oder der TK-Inhalt Dritter auch überwacht werden könnten*" (Übersetzung vom Autor).

Verhältnismäßigkeitsprinzip nicht genügen.[458] In der heutigen internetbasierten IT-Umgebung sollte eine solche Überwachung für eine wirksame Ermittlung durch den § 5 K-KGSG abgedeckt werden können, aber sie ermöglicht es, in der tatsächlichen Durchführungsphase personenbezogene Daten über den vom Gericht angeordneten Umfang hinausgehend zu erheben, daher ist hierfür eine entsprechende Sicherung erforderlich. Die Meinung der Mehrheit des Beschlusses besagt, dass der Umfang der Paket-Überwachung durch §§ 5, 6 K-KGSG in der Zulassungsphase des Gerichts personen- und sachbezogen beschränkt werden kann, aber diese Beschränkungen in der tatsächlichen Durchführungsphase überschritten werden und daher nicht nur verfahrensirrelevante Daten des von Maßnahme Betroffenen, sondern auch Daten von Dritten, die dieselbe Internetleitung benutzen, durch die Ermittlungsbehörde weitgehend erhoben und gespeichert werden und schließlich sich die Paket-Überwachung wesentlich von anderen Arten der TKÜ angesichts der Menge und Vielfalt der erfassten Daten unterscheidet.[459] Auf dieser Grundlage verlangte das K-VerfG für die Paket-Überwachung verfahrensrechtliche Vorkehrungen, um es zu ermöglichen, im Verlauf oder nach Beendigung ihrer Durchführung die Verwahrung, Verwertung und Verarbeitung der erhobenen Daten zu überwachen und zu kontrollieren, um einen Amtsmissbrauch der Ermittlungsbehörde zu verhindern und die dadurch verursachten Grundrechtseingriffe zu minimieren.[460] Diesbezüglich hat das Gericht – neben den Beschränkungen der Datenverwertung gemäß §§ 11, 12 K-KGSG – eine nachträgliche Kontrolle durch Richter (objektive Kontrolle durch eine unabhängige Stelle) und eine Kontrolle durch Benachrichtigung der Betroffenen (subjektive Kontrolle durch den Betroffenen) über die durch die Überwachung erhobenen Daten vorgeschlagen.[461] Insbesondere bezüglich des Letzteren hat es in der folgenden Entscheidungsbegründung auf die Probleme von § 9a K-KGSG hingewiesen, dass der Inhalt der Benachrichtigung keine Gründe für die Maßnahme enthalten ist, dass sie in bestimmten Fällen auf unbestimmte Zeit zurückgestellt werden kann und dass es keinen Rechtsbehelf zur nachträglichen Überprüfung der Rechtmäßigkeit ihres Vollzugs gibt.[462]

Das K-VerfG hat jedoch im Tenor die oben erwähnten Entscheidungsbegründungen nicht ausreichend widergespiegelt.[463] Das heißt, das Gericht hat lediglich entschieden, dass die Paket-Überwachung nicht in die Maßnahme nach § 5 K-KGSG

[458] *K-VerfGE* 30-2, 481, 497 und 502 f. In der Entscheidung hat das *K-VerfG* entschieden, dass die Vorschriften unvereinbar mit der Verfassung sind, aber dass sie bis zum Ablauf des 31. März 2020 vorübergehend weiter anwendbar sind (a. a. O. 503). Zum anderen gibt es eine Gegenansicht von zwei Richtern, dass die Paket-Überwachung auch durch §§ 6, 9, 11, 12 K-KGSG im Verlauf ihrer Durchführung ausreichend kontrolliert werden kann und es daher vereinbar mit der Verfassung ist, dass sie aufgrund des § 5 K-KGSG zulässig ist (a. a. O. 504 ff.).

[459] *K-VerfGE* 30-2, 481, 499 f.

[460] *K-VerfGE* 30-2, 481, 500.

[461] *K-VerfGE* 30-2, 481, 500 f. Diesbezüglich verweist das *K-VerfG* auf die einschlägigen Vorschriften in den USA, Deutschland und Japan.

[462] *K-VerfGE* 30-2, 481, 501.

[463] *Joongwook Park*, CRCL, Nr. 68, 2020, 97, 105.

einbezogen werden kann, im Sinne, dass die Vorschriften zur Verfahrenskontrolle über die TKÜ (§§ 6, 9, 9a, 11, 12 K-KGSG) nicht genügen, um die Schwere des Eingriffs der Paket-Überwachung auszugleichen.[464] In diesem Tenor wurden aber nicht nur die Entscheidungsgründe nicht ausreichend berücksichtigt, sondern er führte auch dazu, dass wesentliche Mängel der Verfahrensgarantie für die TKÜ, nämlich mehrere Mängel des § 9a K-KGSG und das Fehlen einer Rechtsgrundlage zum effektiven Rechtsschutz, weiterhin liegen gelassen werden (vgl. oben d)). In der Novellierung vom 24. März 2020 zur Aufnahme des Beschlussinhalts über die Paket-Überwachung wurden keine Änderungen bezüglich der Benachrichtigung und des nachträglichen Rechtsschutzes vorgenommen, und nur eine Rechtsgrundlage geschaffen, die es ermöglicht, dass sich Richter in die Verwahrung und Verwertung der durch die Überwachung erlangten Daten einschalten (§ 12a K-KGSG).[465]

(3) § 12a K-KGSG ist eine Vorschrift, um die Verwahrung und Verwertung der Daten, die durch die Paket-Überwachung gewonnenen werden, durch die Einschaltung des Gerichts zu begrenzen. Wenn die StA die durch diese Überwachung erhobenen Daten nach § 12 Nr. 1 K-KGSG verwerten oder für diese Verwertung in Verwahrung nehmen will, muss sie innerhalb von 14 Tagen nach Abschluss ihrer Vollstreckung die erforderlichen Daten auswählen und dann bei dem Gericht, das die Maßnahme angeordnet hat, eine Genehmigung beantragen (Abs. 1). Dies gilt auch für die Polizei, jedoch muss diese es über die StA beantragen (Abs. 2). Dieser Antrag muss schriftlich gestellt werden, in dem der Verlauf der Paket-Überwachung, der Inhalt der erlangten Ergebnisse und die Gründe für die Verwertung oder Verwahrung angegeben sind, wobei ihm erläuternde Unterlagen für die Antragsbegründung sowie der Inhalt und das Verzeichnis der zu verwertenden oder zu verwahrenden Daten beizulegen sind (Abs. 3). Wird der Antrag als begründet angesehen, genehmigt das Gericht ihn schriftlich (Abs. 4). Wenn die Ermittlungsbehörde keinen Antrag nach Abs. 1, 2 stellt oder keine Genehmigung nach Abs. 4 erhält, sind die erhobenen Daten zu vernichten (Abs. 5), wobei ein Ergebnisbericht, in dem Gründe, Umfang, Datum und Uhrzeit der Vernichtung enthalten sind, erstellt, zu den Akten genommen

[464] *K-VerfGE* 30-2, 481, 488. In diesem Beschluss weist einer der zwei Richter mit abweichenden Meinungen auf die Probleme von § 9a K-KGSG bezüglich der nachträglichen Benachrichtigung und ihrer Verfassungswidrigkeit hin (a. a. O. 512 – 514) hin. Dieser Hinweis stimmt mit dem Inhalt überein, der im Beschluss zur Echtzeit-Lokalisierung vom 28. Juni 2018, nämlich kurz vor dem Beschluss, ausgeführt wurde (30-1, 564, 584 – 585), und vielmehr widerspricht der Tenor nach der Mehrheitsmeinung dem Inhalt.

[465] Diese Gesetzgebung ist im Wesentlichen darauf zurückzuführen, dass die Entscheidungsgründe des *K-VerfG* nicht vollständig berücksichtigt werden. Insbesondere ist diese Gesetzesänderung insofern sehr unangemessen, als die Verfassungswidrigkeit von § 13b K-KGSG, die dieselbe Funktion wie § 9a K-KGSG hat, bereits durch den Beschluss vom Juni 2018 bestätigt wurde (*K-VerfGE* 30-1, 564, 584 – 585). Dieser Gesetzgebungsakt ist auch aus Sicht der Rechtsstaatlichkeit und der Gewaltenteilung problematisch. Dies scheint grundlegend auf das politische Umfeld zurückzuführen zu sein, insb. den Einfluss des Justizministeriums und der StA, die aus Gründen der Staatssicherheit oder der öffentlichen Ruhe, Ordnung und Sicherheit die strikte Kontrolle über die Maßnahmen nach K-KGSG ablehnen.

und innerhalb von 7 Tagen an das Gericht, das die Paket-Überwachung angeordnet hat, gesendet wird (Abs. 6).

2. Erhebung von Verkehrs- und Standortdaten

a) Eingriffsvoraussetzungen und präventive Verfahrenskontrolle: § 13 Abs. 1, 3, 4 und 9 K-KGSG

(1) Die Ermittlungsbehörde darf die Bereitstellung von in § 2 Nr. 11 K-KGSG genannten Verkehrs- und Standortdaten (siehe Fn. 403) vom Dienstanbieter verlangen, soweit dies für die Ermittlung erforderlich ist (§ 13 Abs. 1 K-KGSG).[466] Dazu ist der Anbieter verpflichtet, die Daten nach Nr. 11 lit. a-d und lit. f für mehr als 12 Monate (Informationen zu inländischen Telefonanrufen für mehr als 6 Monate) und die nach Nr. 11 lit. e und g für mehr als 3 Monate zu speichern.[467] Die Eingriffsvoraussetzungen zu Verkehrs- und Standortdaten nach Abs. 1 haben die folgenden zwei Merkmale. Zuerst wird hierbei die Schwere der Straftaten und das Gewicht des Tatverdachts nicht berücksichtigt, und die Subsidiarität ist nur in bestimmten Fällen erforderlich (§ 13 Abs. 1 K-KGSG, vgl. unten c)).[468] Daher wird diese Maßnahme auf dem gleichen Niveau kontrolliert wie die allgemeine Beschlagnahme und Durchsuchung. In der Praxis scheint es jedoch tatsächlich lockerer zu sein. Bei einfacher Beschlagnahme und Durchsuchung hat der von der Maßnahme Betroffene u. a. das Teilnahmerecht nach § 122 K-StPO und das Recht auf Aushändigung des Beschlagnahmeverzeichnisses nach § 129 K-StPO (vgl. Kapitel 4, D. II. 3. b) und c)), aber er hat keine Verteidigungsrechte bei der Erhebung der Verkehrsdaten.[469] Dann hängen die Eingriffsvoraussetzungen des § 13 Abs. 1 K-KGSG – anders als bei § 100g StPO – nicht davon ab, ob die Daten von Dienstanbietern zu geschäftlichen Zwecken oder zur Mitwirkung bei der Ermittlung obligatorisch gespeichert wurden.[470] Das heißt, der § 13 Abs. 1 K-KGSG gilt unabhängig davon, ob die Verkehrsdaten in Echtzeit gespeichert werden oder bereits gespeichert sind. Dies unterscheidet sich auch von der TKÜ nach § 5 K-KGSG, die die Gleichzeitigkeit bzw. Gegenwärtigkeit der Durchführung der Maßnahme erfordert.

Bezüglich § 13 Abs. 1 K-KGSG wird in der Literatur teilweise kritisiert, dass die Eingriffsvoraussetzungen aus Sicht des Grundsatzes der Verhältnismäßigkeit nicht

---

[466] Aber für Echtzeit-Lokalisierung und Funkzellenabfrage, § 13 Abs. 2 K-KGSG: vgl. unten c).

[467] § 41 Abs. 2 DVO des K-KGSG. Daher ist die Speicherdauer der Verkehrsdaten des Diensteanbieters länger als in Deutschland (§ 113b Abs. 1 TKG: 10 oder 4 Wochen).

[468] Vgl. § 100g Abs. 1 Nr. 1 und Abs. 2 S. 2 StPO.

[469] *Hojung Lee*, JPL, 17-1, 2019, 35, 44 f.

[470] Dies ist die gleiche Form der Regulierung wie § 100g Abs. 1 StPO a. F., der bis zum 17. Dezember 2015 galt.

der Intensität des Grundrechtseingriffs entsprechen.[471] Aber in der meisten Literatur und in der Praxis werden diese nicht strengen Voraussetzungen kaum kritisiert. Vielmehr ist es nach h. M. nicht problematisch, weil die Erhebung von Verkehrs- und Standortdaten i. d. R. Grundrechte weniger verletzt als solche von Inhaltsdaten, und sie schon dem Richtervorbehalt unterliegt.[472] Die gilt jedoch nicht für die Echtzeit-Lokalisierung und die Funkzellenabfrage (vgl. unten c)). Kurz gesagt, werden die Verkehrs- und Standortdaten in Südkorea noch als von geringer Bedeutung angesehen, da es sich nicht um Inhaltsdaten handelt. Angesichts des heutigen Niveaus der IuK-Technologie ist diese Erkenntnis jedoch nicht angemessen. Auf jeden Fall wird jedoch üblicherweise kritisiert, dass die gerichtliche Kontrolle über diese Maßnahme de facto formal ist, sodass die Daten in der Praxis übermäßig erhoben werden.[473] Laut Statistik wurden zwischen 2010 und 2019 durchschnittlich 71.596 Anträge auf Erteilung der Verkehrsdaten jedes Jahr von den Ermittlungsbehörden beim Gericht gestellt, von denen etwa 94,3 % angenommen wurden; wenn hier eine teilweise Genehmigung enthalten ist, beträgt die Zahl etwa 98,5 %.[474] Darüber hinaus betrug die Anzahl der Dokumente, die den Ermittlungsbehörden von den Dienstanbietern aufgrund der gerichtlichen Erlaubnisse zur Verfügung gestellt wurden, im Jahr 2001,

[471] *Hojung Lee*, JPL, 17-1, 2019, 35, 45 und 47; *Heun-Jae Lee*, KLAJ, 68-4, 2019, 497, 519. Prof. *Hojung Lee*, der eine ähnliche Ansicht wie das *BVerfG* zur Bedeutung von Verkehrsdaten vertritt, argumentiert, dass die Ermächtigung zum Zugriff auf die Daten so streng sein sollte wie bei der TKÜ (a. a. O. 47 – 55).

[472] *Seong-Cheon Kim*, Öffentliche Anhörung zur teilweisen Überarbeitung des K-KGSG, 2009, 7, 12 ff. *K-MRK* befindet sich auch in einer vergleichbaren Stellungnahme (*K-MRK-Beschluss*, Verbesserungsvorschläge zur Bestandsdatenauskunft nach K-TKGG und zur Bereitstellung von TK-Bestätigungsdaten nach K-KGSG vom 10. Februar 2014, 13). Dies unterscheidet sich deutlich von Deutschland, wo im letzten Jahrzehnt große Kontroversen über die Einführung von VDS geführt wurden. In Südkorea wird jedoch allgemein davon ausgegangen, dass die Verkehrsdaten – abgesehen von Standortdaten in Echtzeit – immer noch unbedeutender sind als die Inhaltsdaten, und daher wird es als ausreichend angesehen, dass ihre Erfassung oder Verwendung von einem Richter kontrolliert wird. Daher wird in der Literatur i. d. R. der Inhalt der Vorschrift des § 100g StPO und der Entscheidungen von *BVerfG* und *EuGH* nur für den Fall der „Echtzeit-Lokalisierung" beigezogen (*Gi-Young Cho*, JCL, 26-4, 2014, 105, 133; *Heun-Jae Lee*, KLAJ, 68-4, 2019, 497, 517 f.); vgl. unten c).

[473] *K-MRK-Beschluss* (Fn. 472), 7 – 8; *Jina Cha*, KLAJ, 67-2, 2018, 366, 374 f. Prof. *Cha* behauptet, dass die Schwere der Straftaten und die Subsidiarität in die Eingriffsvoraussetzungen einbezogen werden sollte, um ein solches übermäßiges Verlangen zu unterdrücken (a. a. O. 392 f.).

[474] Statistischer Monatsbericht des Gerichts, <https://www.scourt.go.kr/portal/justicesta/JusticestaCodeAction.work?gubun_code=G01>, Abruf: 31. 12. 2020, ausgezogen aus den Statistiken jedes Jahres. Diese Zahl unterscheidet sich nicht wesentlich vom Fall der einfachen Beschlagnahme und Durchsuchung. Zwischen 2010 und 2020 wurden etwa 87,3 bis 91,7 % für den Antrag der Beschlagnahme und Durchsuchung angenommen, aber wenn hier eine teilweise Genehmigung enthalten ist, liegt die Zahl zwischen 98,1 und 99,1 % (*K-OGH*, Jahrbuch der Justiz, 2014, 681 und 2020, 729).

als diese Vorschrift erstmals erlassen wurde, 157.162, aber sie stieg weiter im Jahr 2008 auf 212.745 und im Jahr 2015 auf 300.942.[475]

(2) Zum Verlangen der Bereitstellung von Verkehrsdaten muss die Ermittlungsbehörde bei einem zuständigen Gericht in schriftlicher Form unter Angabe von Gründen für das Verlangen, der Relevanz bezüglich des von der Maßnahme Betroffenen und dem Umfang der erforderlichen Daten beantragen, und sie muss eine Erlaubnis des Gerichts einholen (§ 13 Abs. 3 S. 1 K-KGSG). In dringenden Fällen kann sie vom Dienstanbieter ohne gerichtliche Erlaubnis eine Auskunft verlangen, jedoch muss sie dann unverzüglich die Erlaubnis einholen (Abs. 3 S. 2), andernfalls müssen die bereitgestellten Verkehrsdaten sofort vernichtet werden (Abs. 4). Eine solche Eilkompetenz kann nur bei Erhebung von künftig anfallenden Verkehrsdaten oder in Echtzeit gelten. Bei gespeicherten Verkehrsdaten besteht keine Dringlichkeit. Das zuständige Gericht und die Inhalte, die in der Antragsschrift der Ermittlungsbehörde und auf dem Erlaubnisschein des Gerichts anzugeben sind, sind identisch mit dem Fall der TKÜ (§ 13 Abs. 9 i. V. m. § 6 Abs. 3 – 6 K-KGSG). Nach dem Abs. 9 K-KGSG gilt der § 6 Abs. 7, 8 K-KGSG, der die Frist und die Verlängerung der TKÜ beschränkt, nicht für die Erhebung von Verkehrsdaten, daher gibt es keine Beschränkung des Zeitpunkts der Speicherung bei der Erhebung der gespeicherten vergangenen Verkehrsdaten und keine Beschränkung der Durchführungsfrist bei der Erhebung der künftig anfallenden Verkehrsdaten oder in Echtzeit. Aus den Verkehrsdaten über einen langen Zeitraum können jedoch die Daten, die zum intimen Bereich des Einzelnen gehören, abgeleitet werden. Dies gilt umso mehr, als die Verwendung von Mobilfunkendgeräten wie Smartphones oder Tablet-PCs heutzutage üblich ist.[476] Daher sind auch für die Erhebung von Verkehrsdaten Beschränkungen des Zeitraums und der Verlängerung der Maßnahme erforderlich.[477] Darüber hinaus gilt dies auch angesichts des Beschlusses des K-VerfG von 2010, dass es dem Verhältnismäßigkeitsprinzip widerspricht, dass § 6 Abs. 7 K-KGSG a. F. keine Be-

[475] Ministerium für Wissenschaft, Technologie, Information und Kommunikation (im Folgenden „Ministerium für WTIC"), <https://www.msit.go.kr/web/msipContents/contents.do?mId=MTAxOA==>, Abruf: 31. 12. 2020, ausgezogen aus den Statusdaten der ersten und zweiten Hälfte jedes Jahres. Basierend auf der in einem Dokument aufgeführten Telefonnummern ist die Anzahl sogar noch höher. Sie betrug im Jahr 2008 446.900, stieg jedoch im Jahr 2009 auf 16.082.957 und im Jahr 2010 auf 39.391.220. Sie ist danach leicht gesunken und seit 2016 unter etwa 1,5 Millionen gefallen. Der Grund, warum den Ermittlungsbehörden eine so große Anzahl von Telefonnummern zur Verfügung gestellt wurde, liegt darin, dass Smartphones im Jahr 2009 sich weit verbreitet haben und die Behörden zur Funkzellenabfrage wahllos die Bereitstellung der Verkehrsdaten von Dienstanbietern verlangt haben (*K-MRK-Beschluss* (Fn. 472), 8 f.). Nach 2010 wurde diese Ermittlungsmethode erheblich kritisiert und dementsprechend ist die Zahl drastisch zurückgegangen (*Hojung Lee*, JPL, 17-1, 2019, 35, 48).

[476] Zust. *Jina Cha*, KLAJ, 67-2, 2018, 366, 396 f.; *Hojung Lee*, JPL, 17-1, 2019, 35, 45; *Heun-Jae Lee*, KLAJ, 68-4, 2019, 497, 519: Dies ist tatsächlich so, als ob eine elektronische Fußfessel angebracht ist.

[477] Vgl. § 101a Abs. 1 S. 1 Nr. 1 und Abs. 2 StPO: Zeitraum.

schränkung für die gesamte Verlängerungsfrist und die Anzahl der Verlängerungen enthalten war.[478]

b) Nachträgliche Aufsicht und Benachrichtigung: § 13 Abs. 5–8 und § 13d sowie § 13b K-KGSG[479]

Wenn die Ermittlungsbehörde Verkehrsdaten von einem Dienstanbieter erhalten hat, müssen in ihrem Organ oder ihrer Einrichtung die Unterlagen vorgehalten werden, in denen die Daten über Verlangen, Antrag, Erlaubnis usw. angegeben sind (§ 13 Abs. 5 K-KGSG), und auch das zuständige Gericht muss solche Unterlagen aufbewahren (Abs. 6). Wenn ein Anbieter die Daten übergeben hat, muss er die entsprechenden Unterlagen ab diesem Datum für 7 Jahre vorhalten und über den diesbezüglichen Status zweimal jährlich dem Minister für WTIK berichten (Abs. 7). Der Minister kann die Verwaltung der Unterlagen des Anbieters überprüfen (Abs. 8). Hier gibt es jedoch – anders als bei TKÜ – keine parlamentarische Aufsicht.[480] Andererseits gelten §§ 11, 12 K-KGSG auch entsprechend für die Auskunft über Verkehrsdaten (§ 13d K-KGSG).

Der Inhalt von § 13b K-KGSG, der eine Benachrichtigung des Betroffenen bei der Erhebung von Verkehrsdaten regelt, und die Kritik daran wurden bereits ausführlich dargelegt (vgl. oben 1. d)). Das *K-VerfG* hat im Beschluss vom 2018 die Verfassungswidrigkeit der Vorschrift bestätigt und eine gesetzgeberische Alternative, die nicht streng gegenüber der TKÜ ist, vorgeschlagen. Der Gesetzgeber hat sie indessen nur teilweise aufgenommen. Vor allem, dass keine Rechtsgrundlage zum nachträglichen Rechtsschutz geschaffen wurde, ist nicht nur hinsichtlich des Grundrechtsschutzes unangemessen, sondern verletzt auch das Recht auf Recht auf Anrufung der Gerichte schwerwiegend.

c) Echtzeit-Lokalisierung und Funkzellenabfrage: § 13 Abs. 2 K-KGSG

Mit der weitverbreiteten Verwendung von Mobiltelefonen mit GPS-Technik sind jüngst in Südkorea zwei Fragen hinsichtlich der Erhebung von Verkehrs- und Standortdaten zum Zwecke der Strafverfolgung am umstrittensten geworden: Können eine Echtzeit-Lokalisierung und eine Funkzellenabfrage durch § 13 Abs. 1 K-KGSG gerechtfertigt werden? Die Verfassungsbeschwerde für jeden Fall wurde einzeln erhoben und das *K-VerfG* hat am selben Tag, dem 28. Juni 2018 die Beschlüsse über die Echtzeit-Lokalisierung (2012 HunMa 191 etc.) und über die Funkzellenabfrage (2012 HunMa 538) gefasst. In ihnen hat das Gericht verlangt, dass

[478] *K-VerfGE* 22-2, 545.

[479] § 13a K-KGSG ist die Ermächtigung zur Erhebung von Verkehrsdaten zum Zwecke der gerichtlichen Entscheidung und § 13c K-KGSG dieselbe zum Zwecke der geheimdienstlichen Gefahrenabwehr.

[480] Krit. *Jina Cha*, KLAJ, 67-2, 2018, 366, 377.

die beiden Maßnahmen mit strengeren Eingriffsvoraussetzungen verbunden werden.[481] Nach den Beschlüssen hat der Gesetzgeber am 31. Dezember 2019 § 13 Abs. 2 K-KGSG eingefügt (Gesetz Nr. 16849). Nach dieser Vorschrift darf die Erteilung von Standortdaten in Echtzeit (Nr. 1)[482] und Verkehrsdaten von bestimmten Funkzellen (Nr. 2),[483] die in § 2 Nr. 11 lit. f und g K-KGSG bezeichnet werden, verlangt werden, soweit dies zum Zwecke der Ermittlung erforderlich ist und das Verhindern des Begehens der Straftat, die Auffindung oder Sicherung des Verdächtigen oder die Erhebung oder Sicherstellung von Beweismitteln auf andere Weise erschwert wäre (S. 1); dies gilt jedoch nicht für die in § 5 Abs. 1 K-KGSG aufgeführten Straftaten oder für Straftaten mittels der TK (S. 2).[484]

aa) Erhebung der Standortdaten in Echtzeit durch Mobiltelefone

Standortdaten sind geografische Informationen über Orte, an denen eine Person zu einem bestimmten Zeitpunkt sich aufgehalten hat oder aktuell sich aufhält, und ihre Erhebung, Verwertung oder Verwendung kann zu einer schweren Verletzung der Privatsphäre führen. Der Grund, warum die Erhebung oder Verwendung der Standortdaten besonders problematisch ist, liegt darin, dass der Einsatz von GPS-Technologie im privaten Bereich üblich ist und die Verwendung von Smartphones weit verbreitet ist. Seit 2005 ist die Erhebung und Verwendung der Standortdaten in Südkorea durch das StandODSG gesondert geregelt. Im Bereich der Strafverfolgung und der Gefahrenabwehr zur Staatssicherheit gehören diese Daten begrifflich zu den Verkehrsdaten (vgl. § 2 Nr. 11 lit. f und g K-KGSG) und werden wie andere Arten von Verkehrsdaten behandelt. Dies war in der Vergangenheit nicht besonders problematisch, da die erhaltenen Standortdaten nicht so genau waren, dass sie Grundrechte schwer beeinträchtigten konnten.[485] Durch die Verbindung der GPS-Technologie mit Mobiltelefonen sind die Standortdaten aber sehr wichtig geworden. Solche Daten sind sehr genau und können in Echtzeit erhoben werden, was einen schweren Eingriff in das Persönlichkeitsrecht ermöglicht.[486]

---

[481] In dem Beschluss der Echtzeit-Lokalisierung wurde entscheiden, dass auch § 13b K-KGSG a. F. zur Benachrichtigung für die Erhebung von Verkehrsdaten verfassungswidrig ist (siehe Fn. 427).

[482] Vgl. § 100g Abs. 1 S. 4 StPO.

[483] Vgl. § 100g Abs. 3 StPO: Funkzellenabfrage.

[484] Dies steht im Gegensatz zur Regulierung der StPO. Nach § 100g Abs. 1 – 3 StPO ist die Erhebung gespeicherter Verkehrs- und Standortdaten mit strengeren Eingriffsvoraussetzungen verbunden als die Erhebung von Verkehrs- und Standortdaten in Echtzeit.

[485] *Kil-Young Oh*, DLS, Nr. 34, 2007, 357, 370.

[486] *Kil-Young Oh*, DLS, Nr. 34, 2007, 357, 371 ff.; dazu *Hojung Lee*, JPL, 17-1, 2019, 35, 40: Die Standortdaten ermöglichen die Erstellung von Bewegungsprofilen des Betroffenen, und wenn sie mit anderen Verkehrsdaten kombiniert werden, erhöht dies die Gefahr einer vollständigen Überwachung der Persönlichkeit. Daher sind diese Daten von größerer Bedeutung als andere Verkehrsdaten (*Hojung Lee*, a. a. O. 45).

In der Literatur wird es kaum problematisiert, dass die gespeicherten „vergangenen" Standortdaten zu den Daten i. S. d. § 2 Nr. 11 lit. f und g K-KGSG gehören und somit aufgrund von § 13 K-KGSG erhoben werden können.[487] Umstritten ist hingegen, ob auch die Standortdaten „in Zukunft" oder „in Echtzeit" gestützt auf diese Vorschrift erhoben werden können. Dass eine Standortverfolgung in Echtzeit zur vorläufigen Festnahme, Untersuchungshaft, Vorbereitung der TKÜ, Überwachung etc.[488] erforderlich ist, wird i. d. R. nicht beanstandet.[489] Eine solche Maßnahme greift jedoch normalerweise in Grundrechte stärker ein als die Erhebung von anderen Verkehrsdaten oder gespeicherten Standortdaten, deswegen ist es erforderlich, dass sie demnach mit strengeren Eingriffsvoraussetzungen oder Vorkehrungen in Verbindung gebracht wird. Diesbezüglich äußerte die K-MRK im Jahre 2014 die Ansicht, dass die Erhebung der Standortdaten in Echtzeit unter den Voraussetzungen des § 13 Abs. 1 K-KGSG nur „subsidiär" zulässig sein sollte.[490] In der Literatur wird hingegen i. d. R. die Ansicht vertreten, dass strengere Eingriffsvoraussetzungen erforderlich sind, d. h. in gleichem oder vergleichbarem Maße wie bei der TKÜ; eine derartige Maßnahme sollte „auf schwere Straftaten" nur „subsidiär" anwendbar sein.[491] Aber das K-VerfG vertrat in seinem Beschluss von 2018 (2012 HunMa 191 etc.) dieselbe Auffassung wie die o. g. K-MRK:

> „Da die Standortdaten zur Echtzeit-Lokalisierung zwar keine Inhaltsdaten darstellen, aber den aktuellen Ort und den Bewegungsstatus des von Daten Betroffenen erbringen, können sie in sensible Daten, die ausreichend geschützt werden müssen, fallen. Trotzdem ist … (nach § 13 Abs. 1 K-KGSG) … möglich, dass die Erteilung der Standortdaten sowohl des Verdächtigten als auch von Dritten verlangt werden, auch wenn nur die Erforderlichkeit der Ermittlung ohne Subsidiarität besteht. Daher beschränkt die Vorschrift … Grundrechte des von Daten Betroffenen übermäßig. … Es ist möglich, seine Grundrechte weniger zu ver-

[487] *Daeho Choi*, KNULJ, Band 62, 2018, 213, 245; *Heun-Jae Lee*, KLAJ, 68-4, 2019, 497, 517 f.; vgl. *Gi-Young Cho*, JCL, 26-4, 2014, 105, 131 f.; abw. *Won-Sang Lee*, KCR, 23-2, 2012, 109, 122: Die Einbeziehung gespeicherter früherer GPS-Standortdaten in die „Daten zur Standortverfolgung von Funkzellen" (§ 2 Nr. 11 lit. f K-KGSG) sollte durch die Gesetzgebung erreicht werden. Aber Prof. *Won-Sang Lee* behauptet auch, dass die Erhebung solcher Standortdaten lediglich durch die Kontrolle des Gerichts gerechtfertigt werden kann (a. a. O. 127 f.).

[488] In der Praxis wird die Auskunft über Verkehrs- und Standortdaten in Zukunft oder in Echtzeit hauptsächlich bei einer Flucht nach der Ausstellung eines Haftbefehls oder nach einem rechtskräftigen Urteil oder gleichzeitig mit der Ausstellung eines Haftbefehls erlaubt (*Jina Cha*, KLAJ, 66-4, 2017, 237, 252).

[489] Laut der Aussage der Polizei im *K-MRK-Beschluss* ist die Verwendung von Standortdaten in Echtzeit mithilfe der GPS-Technologie in der Praxis nützlich (siehe Fn. 472, 22 f.), und diese werden nach dem Beschluss zur Echtzeit-Lokalisierung des *K-VerfG* bereits verwendet (*K-VerfGE* 30-1, 564, 570 f.).

[490] *K-MRK-Beschluss* (Fn. 472), 17.

[491] *Bong-Su Kim*, CNLR, 32-3, 2012, 271, 290 ff.; *Gi-Young Cho*, JCL, 26-4, 2014, 105, 133; *Daeho Choi*, KNULJ, Band 62, 2018, 213, 244 f.; auch *Hojung Lee*, JPL, 17-1, 2019, 35, 55 und *Heun-Jae Lee*, KLAJ, 68-4, 2019, 497, 519; dazu *Kil-Young Oh*, JML, 14-1, 2015, 33, 46: Die Standortverfolgung in Echtzeit verletzt Grundrechte in vergleichbarem Maße wie TKÜ; vgl. *Youngsung Min*/*Hee-Young Park*, KCR, 28-4, 2017, 203, 225; *Sang-Kyung Lee*, LCJ, 6-1, 2019, 77, 101. Die letzten beiden Autoren legen keine konkreten Eingriffsvoraussetzungen vor.

letzen, ohne die Erreichung des gesetzgeberischen Zwecks zu behindern. Z. B. kann es als Verbesserungsvorschlag betrachtet werden, dass ① die Bereitstellung der Standortdaten zur Echtzeit-Lokalisierung oder der Standortdaten einer unbestimmten Mehrzahl von Personen nur dann erlaubt wird, wenn dies für die Ermittlung nicht nur erforderlich, sondern auch subsidiär ist, d. h., soweit das Verhindern des Begehens der Straftat, die Auffindung oder Sicherung des Verdächtigen oder die Erhebung oder Sicherstellung von Beweismitteln auf andere Weise erschwert wäre, oder ② sie für andere als die in § 5 Abs. 1 K-KGSG genannten Straftaten nur subsidiär erlaubt wird … . Zur Erhebung von Verkehrsdaten ist die gerichtliche Erlaubnis erforderlich, … daher wird ein Amtsmissbrauch der Ermittlungsbehörde teilweise kontrolliert. Aber … Die Ablehnungsrate des Gerichts für den Antrag auf TKÜ beträgt etwa 4 %, während eine solche für den Antrag auf Erhebung von Verkehrsdaten nur etwa 1 % beträgt, was auch darauf zurückzuführen ist, dass die Vorschrift ohne Subsidiarität nur die Erforderlichkeit der Ermittlung vorsieht."[492] *(Übersetzung vom Autor)*

Kurz gesagt, hat das K-VerfG entschieden, dass die Standortdaten zur Echtzeit-Lokalisierung zu den sensiblen Daten gehören, und dass sie somit für die Ermittlung nur subsidiär erhoben oder verwendet werden können, aber dass diese Anforderung der Subsidiarität nach Ermessen des Gesetzgebers bei schweren Straftaten, bei denen die TKÜ zulässig ist, ausgeschlossen werden kann. Nach diesem Beschluss hat dieser gesetzlich festgelegt, dass solche Daten bei anderen Straftaten als den schweren des § 5 Abs. 1 K-KGSG oder bei solchen mittels der TK nur subsidiär erhoben und verwendet werden dürfen. In dieser Hinsicht kann man den Schluss ziehen, dass der südkoreanische Gesetzgeber mehr Gewicht auf effektive Strafverfolgung legt.

bb) Funkzellenabfrage

Die Funkzellenabfrage bezieht sich auf eine Ermittlungsmethode, bei der alle Verkehrsdaten einschließlich der von einer bestimmten Funkzelle gesendeten Standortdaten zu einem bestimmten Zeitraum bereitgestellt werden.[493] Es wird nicht bestritten, dass eine solche Maßnahme durch § 13 K-KGSG zulässig sein kann und dass sie in bestimmten Fällen zu Beginn der Ermittlung erforderlich ist, um Verdächtige zu bestimmen oder zu identifizieren.[494] Es wird jedoch kritisiert, dass sie von der Ermittlungsbehörde – unabhängig von der Schwere des Falles – übermäßig häufig verwendet wird, wodurch der Behörde die Verkehrsdaten von zahlreichen unverdächtigen Dritten zur Verfügung gestellt werden.[495] Aus diesem Grund wird in

[492] *K-VerfGE* 30-1, 564, 579 f.

[493] *K-VerfGE* 30-1, 596, 603.

[494] *K-MRK-Beschluss* (Fn. 472), 14; dazu *K-VerfGE* 30-1, 596, 603: „*Bei der Funkzellenabfrage … handelt es sich hauptsächlich um eine Ermittlungsmethode, um durch die Verfolgung der von der Funkzelle des Tatorts gesendeten Telefonnummern den Verdächtigen einzuengen, insb. wenn ein Serienverbrechen auftritt, bei dem die Ermittlungsbehörde den Verdächtigen nicht identifizieren kann, oder wenn Hinweise auf einen kriminellen Fall in mehreren Gebieten mit einer Zeitdifferenz gefunden werden. Diese Untersuchung hat … ihre Rechtsgrundlage in § 13 K-KGSG.*" (Übersetzung vom Autor).

[495] *Gi-Young Cho*, JCL, 26-4, 2014, 105, 127; *Hojung Lee*, JPL, 17-1, 2019, 35, 56; dazu *K-VerfGE* 30-1, 596, 603: „*Der Natur nach enthält ein Erlaubnisschein Tausende von Telefon-*

der Literatur argumentiert, dass diese Maßnahme auf schwere Straftaten beschränkt und nur subsidiär erlaubt werden sollte[496] oder dass die sichergestellten Verkehrsdaten von unverdächtigen Dritten unverzüglich gelöscht werden sollten.[497] Die *K-MRK* äußerte jedoch im Jahre 2014 nur die Meinung, dass die Funkzellenabfrage – wie bei der Standortverfolgung in Echtzeit – subsidiär erlaubt werden sollte.[498] In der Folge vertrat auch das *K-VerfG* im Beschluss von 2018 (2012 HunMa 538) dieselbe Auffassung:

> „Es besteht kein Zweifel, dass die sog. Funkzellenabfrage erlaubt sein sollte, … aber der Staat darf … keine Verkehrsdaten zahlreicher unbestimmter Personen unter dem Deckmantel einer strafrechtlichen Untersuchung leichtfertig verlangen. Das heißt, es ist ausnahmsweise zulässig …, dass die Daten von unverdächtigen Personen an Ermittlungsbehörden in großen Mengen bereitgestellt werden."[499]

> „Da das Verlangen der Bereitstellung von Verkehrsdaten vom Gericht erlaubt werden muss, kann … natürlich davon ausgegangen werden, dass ein Missbrauch aufgrund der Funkzellenabfrage ausreichend kontrolliert werden kann. Aber … die gerichtliche Ablehnungsrate dieses Erlaubnisantrags beträgt nur etwa 1 %, was darauf zurückzuführen ist, dass die Vorschrift (§ 13 Abs. 1 K-KGSG) nur die Erforderlichkeit ohne Subsidiarität als Eingriffsvoraussetzungen der Maßnahme vorschreibt. In Anbetracht dessen ist … es schwierig zu schließen, dass ein Missbrauch des Rechts auf Auskunftsverlangen von Ermittlungsbehörden lediglich durch den Richtervorbehalt ausreichend kontrolliert wird. Für die Erlaubnis der Funkzellenabfrage gibt es eine Möglichkeit, die Grundrechte von zahlreichen unbestimmten Personen weniger zu verletzen, ohne die Ermittlung zu stören, indem es als Verbesserungsvorschlag unabhängig oder überschneidend betrachtet wird, dass ① sich die Bereitstellung der Verkehrsdaten von Opfern oder Verdächtigen auf die unbedingt notwendigen Straftaten wie Staatsschutzdelikte oder Gewaltkriminalität wie Entführung, sexuelle Gewalt etc. beschränkt, ② neben diesen schweren Straftaten sie auch bei Straftaten mittels der TK zulässig ist, ③ dazu das Erfordernis, dass die Ermittlung der Straftaten auf andere Weise erschwert wäre (Subsidiarität), hinzugefügt wird oder diese Subsidiarität nur

---

nummern, aber nur 1–2 Telefonnummern, die für die Untersuchung von Bedeutung sind, werden herausgezogen und verwendet. Mit Stand von 2015 betrug der Erlaubnisschein zum Zwecke der Funkzellenabfrage insgesamt 1.394, was nur 0,46 % der gesamten Erlaubnisscheine (300.942) zur Bereitstellung der Verkehrsdaten im Jahr 2015 entspricht, aber die Anzahl der für die Funkzellenabfrage bereitgestellten Telefonnummern betrug etwa 4,97 Millionen, was 90,62 % der gesamten zur Bereitstellung der Verkehrsdaten bereitgestellten Telefonnummern (etwa 5,48 Millionen) entspricht." (Übersetzung vom Autor). Aus diesem Grund wirft eine Literatur Bedenken auf, dass die Polizei durch diese Maßnahme die Teilnehmer bestimmter Versammlungen in gleicher Weise wie Rasterfahndung untersuchen kann (*Gi-Young Cho*, a. a. O.).

[496] *Hojung Lee*, JPL, 17-1, 2019, 35, 56 f.

[497] *Heun-Jae Lee*, KLAJ, 68-4, 2019, 497, 520. Darüber hinaus argumentiert er, dass die Benachrichtigung zahlreicher Dritter, die nichts mit dem Fall zu tun haben, über die Erhebung ihrer Verkehrsdaten deshalb unterbleiben kann, weil es angesichts des Verhältnismäßigkeitsprinzips kein Interesse an der Benachrichtigung gibt, und dass dies gesetzlich klar geregelt werden sollte (a. a. O. 522).

[498] *K-MRK-Beschluss* (Fn. 472), 17.

[499] *K-VerfGE* 30-1, 596, 606.

für andere Straftaten als die o. g. schweren Straftaten verlangt wird oder ④ das Auskunftsverlangen nicht mit einem Erlaubnisschein erfolgt."[500] *(Übersetzung vom Autor)*

Um den Missbrauch der Funkzellenabfrage zu begrenzen, machte das K-VerfG dem Gesetzgeber die Vorschläge, ihre Anwendung auf schwere Straftaten oder Straftaten mittels der TK zu beschränken, zu den Eingriffsvoraussetzungen eine Subsidiaritätsklausel – vorbehaltlich der schweren Straftaten – hinzuzufügen oder eine pauschale Erlaubnis zu verbieten. Es liegt im Ermessen des Gesetzgebers, einen dieser Vorschläge zu wählen, um die Eingriffsvoraussetzungen der Funkzellenabfrage strenger auszugestalten. Er hat gesetzlich festgelegt, dass die Funkzellenabfrage – ebenso wie die Erhebung der Standortdaten in Echtzeit – subsidiär zulässig ist, ausgenommen bei schweren Straftaten des § 5 Abs. 1 K-KGSG oder denen mittels der TK.

cc) Zusammenfassung und Zwischenfazit

Die Eingriffsintensität der Erhebung von Verkehrsdaten wird in Südkorea – im Vergleich zu Europa und Deutschland – i. d. R. nicht hoch bewertet. Sie wird u. a. nicht nur von Ermittlungsbehörde, sondern auch von Gerichten und *K-VerfG* immer noch als schwächer angesehen als solche der TKÜ. Selbst bei der Echtzeit-Lokalisierung und der Funkzellenabfrage, die in der Literatur in den letzten 10 Jahren wegen der intensiven Grundrechtseingriffe heftig umstritten waren, hat das *K-VerfG* nicht unbedingt verlangt, ihren Anwendungsbereich auf schwere Straftaten zu beschränken, und der Gesetzgeber hat nur eine Subsidiaritätsklausel zu den Eingriffsvoraussetzungen hinzugefügt. Insbesondere durch die Gesetzesänderung Ende 2019 hat er einerseits eindeutig beabsichtigt, dass die Erhebung und Verwendung der Verkehrsdaten – als verdeckte Ermittlungsmaßnahme – unter einem vergleichbaren Kontrollniveau wie allgemeine Beschlagnahme und Durchsuchung möglich sein sollte, andererseits hat er ausdrücklich abgelehnt, dass die Echtzeit-Lokalisierung und die Funkzellenabfrage bei den in § 5 Abs. 1 K-KGSG genannten schweren Straftaten lediglich subsidiär zulässig sind.

Aus alledem geht hervor, dass die wirksame Strafverfolgung mindestens, soweit es die Erhebung und Verwendung der Verkehrsdaten betrifft, in Südkorea von größerer Bedeutung ist als der Grundrechtsschutz. Aber es ist zweifelhaft, ob dies angemessen ist und ob es auch in Zukunft so sein sollte. Dies liegt daran, dass mit der Entwicklung der IuK-Technologie ein Eingriff in das Persönlichkeitsrecht heute nur durch die Verwertung der Verkehrsdaten ausreichend möglich ist und außerdem genaue Standortdaten auf der Basis der GPS-Technologie ebenso sensibel sind wie TK-Inhalte.[501] Diese Daten ermöglichen nicht nur die Überwachung, Verfolgung

[500] *K-VerfGE* 30-1, 596, 607.

[501] Im Beschluss zur Funkzellenabfrage erklärt auch das *K-Verf* die Bedeutung von Verkehrsdaten wie folgt (*K-VerfGE* 30-1, 596, 607): „*Die Verkehrsdaten, die i. R. d. Kommunikation mittels Mobiltelefonen zwangsläufig aufgetreten, sind zwar keine Inhaltsdaten, aber sie können eine vergleichbare Rolle wie die Inhaltsdaten spielen, indem sie es ermöglichen, verschiedene*

oder Verhaftung des Verdächtigen, sondern auch teilweise die Untersuchung des Sachverhalts.[502] Daher sollte die Ermächtigung zur Erhebung und Verwendung von Verkehrsdaten auf ein Niveau verstärkt werden, das der TKÜ entspricht.[503]

3. Bestandsdatenauskunft: § 83 K-TKGG (= § 54 K-TKGG a. F.)

(1) Niemand darf die personenbezogenen Daten von Nutzern, die bei TK-Anbieter in Verwahrung sind, verletzen oder offenbaren (§ 83 Abs. 1, 2 K-TKGG). Ersucht die Ermittlungsbehörde den Anbieter zur Strafverfolgung oder Strafvollstreckung[504] darum, Name, Registrierungsnummer des Bewohners, Anschrift, Rufnummer, Kennung und das Datum von Vertragsschluss oder -kündigung von Nutzern bereitzustellen (im Folgenden „Bestandsdatenauskunft"), so „kann" er diesem Ersuchen „nachkommen" (Abs. 3). Die Ermittlungsbehörde muss dieses Auskunftsverlangen in schriftlicher Form unter Angabe von Gründen für das Verlangen, der Relevanz bezüglich der Nutzer und dem Umfang der erforderlichen Daten stellen. In dringenden Fällen kann es auf andere Weise als schriftlich gestellt werden, aber die Behörde muss sofort danach dem Anbieter unverzüglich ein Formular des Ersuchens übergeben, nachdem die Dringlichkeit nicht mehr vorhanden ist (Abs. 4). Wenn der Anbieter die Bestandsdaten gemäß dem Verfahren bereitstellt hat, muss er diese Tatsache schriftlich dokumentieren und das Dokument sicher verwahren (Abs. 5). Außerdem muss er diesen Status zweimal jährlich dem Minister für WTIK berichten, und dieser kann die Wahrhaftigkeit der berichteten Inhalte und die Verwaltung der Unterlagen gemäß Abs. 5 überprüfen (Abs. 6). Darüber hinaus muss er auch den Leiter der Behörde für Gerichtsverwaltung und den Leiter der Hauptverwaltung, zu der jede Ermittlungsbehörde gehört, über den Status informieren (Abs. 7). Schließlich muss der Dienstanbieter eine Sonderorganisation einrichten und betreiben, die für die Angelegenheiten der Kommunikationsgeheimnisse der Nutzer zuständig ist, und die Details über ihre Funktion und Struktur sind in der DVO festgelegt (Abs. 8).

(neue) Informationen über den von den Daten Betroffenen durch Kombination mit Analyse mit anderen Informationen abzuleiten … Die Daten sind sensible Informationen, die stark zu schützen sind, und sie gehören zusammen mit den TK-Inhaltsdaten zum wesentlichen Element der Freiheit der Kommunikation, sodass die Auskunft über Verkehrsdaten zum Zwecke der Funkzellenabfrage unter strengen Anforderungen ausnahmsweise zulässig sein sollte." (Übersetzung vom Autor). Dennoch räumt das Gericht in diesem Beschluss aus Gründen des gesetzgeberischen Gestaltungsspielraums das Ergebnis ein, das solcher starken Schutzbedürftigkeit entgegensteht. Der Gesetzgeber fügte den Eingriffsvoraussetzungen lediglich eine Subsidiaritätsklausel hinzu.

[502] In jüngster Zeit werden die Standortdaten auch bei der Verfolgung von infizierten Personen für Zwecke der Quarantäne erheblich verwendet; § 15 Abs. 1 Nr. 3 StandODSG und § 76b Abs. 2 Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten (Kurztitel: Infektionsschutzgesetz).

[503] Zust. *Hojung Lee*, JPL, 17-1, 2019, 35, 56 f.

[504] Nach dem Absatz dürfen Gerichte für die Entscheidung und Geheimdienste für die Gefahrenabwehr die Erteilung der Bestandsdaten verlangen.

Laut Statistik steigt die Anzahl der Auskunftserteilung nach § 83 K-TKGG jährlich erheblich: 113.422 Fälle im Jahr 2001; 127.787 Fälle im Jahr 2002; 189.192 Fälle im Jahr 2003; 279.929 Fälle im Jahr 2004; 342.771 Fälle im Jahr 2005; 323.566 Fälle im Jahr 2006, 426.408 Fälle im Jahr 2007, 474.568 Fälle im Jahr 2008, 561.467 Fälle im Jahr 2009, 591.467 Fälle im Jahr 2010, 651.185 Fälle im Jahr 2011, 820.800 Fälle im Jahr 2012, 944.927 Fälle im Jahr 2013, 1.001.013 Fälle im Jahr 2014, 1.124.874 Fälle im Jahr 2015, 1.109.614 Fälle im Jahr 2016, 989.751 Fälle im Jahr 2017, 974.481 Fälle im Jahr 2018, 1.003.399 Fälle im Jahr 2019.[505] Und jedes Verlangen enthält i. d. R. mehrere Telefonnummern und Internet-Kennungen, deren Anzahl beträgt 9.574.659 im Jahr 2013, 12.967.456 im Jahr 2014, 10.577.079 im Jahr 2015, 8.272.504 im Jahr 2016, 6.304.985 im Jahr 2017, 6.141.107 im Jahr 2018 und 6.028.268 im Jahr 2019.[506]

Bezüglich der Bestandsdatenauskunft nach § 83 K-TKGG ist es fragwürdig, was die Formulierung „kann der Anbieter diesem Ersuchen nachkommen" in Abs. 3 bedeutet, und ob für dieses Ersuchen eine Einschaltung des Richters erforderlich ist. Diesbezüglich wurden insb. die Entscheidungen, die im Jahr 2012 von *K-VerfG* und *Obergericht Seoul* nacheinander getroffen wurden, zum Anhaltspunkt von Kontroversen. Dabei handelt es sich im Wesentlichen um die Intensität des Eingriffs der Bestandsdatenauskunft und die Abwägung zwischen dem Grundrechtsschutz und der effektiven Strafverfolgung.

(2) Nach dem Beschluss des *K-VerfG* vom 23. August 2012 hat der Beschwerdeführer geltend gemacht, dass § 54 K-TKGG a. F. (= § 83 K-TKGG), der vorsieht, dass der Ermittlungsbehörde die Bestandsdaten ohne Einschaltung eines Gerichts zur Verfügung gestellt werden können, verfassungswidrig sei. Im Beschluss lehnte die Mehrheit der Richter die Beschwerde jedoch als unzulässig ab:

> „Die Vorschrift … räumt dem Dienstanbieter nur die Befugnis ein, die Bestandsdaten der Nutzer auf Verlangen der Ermittlungsbehörde bereitzustellen, und auferlegt ihm keine Verpflichtung. Daher kann er dem Verlangen nicht nachkommen, wobei keine Sanktionen verhängt werden. Daher fällt die Erfassung der Bestandsdaten in freie Ermittlung, bei der kein Zwang besteht, und so sie ist keine Ausübung hoheitlicher Gewalt, die Gegenstand einer Verfassungsbeschwerde sein kann. Schließlich ist die vorliegende Beschwerde unzulässig."[507] *(Übersetzung vom Autor)*

---

[505] Ministerium für WTIK, <https://www.msit.go.kr/web/msipContents/contents.do?mId=MTAxOA==>, Abruf: 31. 12. 2020, ausgezogen aus den Statusdaten der ersten und zweiten Hälfte jedes Jahres; *Yangsub Kwon*, korLR, Band 59, 2015, 397, 401.

[506] Clinical Legal Education Center (CLEC) in der Universität Korea School of Law, Korea Internet Transparency Report 2020, 10. Die Telefonnummern oder Kennungen, die etwa 16,5 % der Gesamtbevölkerung Südkoreas entsprechen, werden jährlich an die Ermittlungsstelle weitergeleitet (a. a. O. 11). Der Grund dafür, dass mehrere Bestandsdaten von einem Dokument angefordert werden, liegt darin, dass diese Maßnahme hauptsächlich dazu dient, den Verdächtigen zu Beginn einer Ermittlung zu identifizieren (*Yangsub Kwon*, korLR, Band 59, 2015, 397, 408).

[507] *K-VerfGE* vom 23. 8. 2012 – 2010 HunMa 439 (24-2, 641, 646 f.). Eine Minderheitsmeinung (drei Richter) dagegen erklärt jedoch wie folgt (a. a. O. 648 f.): „*Nur in Anbetracht der*

Andererseits hat ein Bürger mittlerweile in einem anderen Fall gegen seinen TK-Anbieter Schadenersatzklage erhoben, weil seine Bestandsdaten der Ermittlungsbehörde gemäß § 54 K-TKGG a. F. ohne angemessene Prüfung mechanisch erteilt wurden. Hierbei entschied das *Obergericht Seoul* am 18. Oktober 2012 wie folgt:

> „Diese Vorschrift bestätigt nur die allgemeine Verpflichtung des Dienstanbieters zur Unterstützung bei der Ermittlung, und er ist nicht verpflichtet, dem Auskunftsverlangen von Ermittlungsbehörden nachzukommen. Der Anbieter muss in der Lage sein, die personenbezogenen Daten von Nutzern wirksam zu schützen, indem er das Verlangen in Einzelfällen angemessen prüft, und er ist weiterhin verpflichtet, ausreichende Maßnahmen zu solchem Schutz zu ergreifen, etwa indem er detaillierte Richtlinien darüber erstellt, ob und in welchem Umfang personenbezogene Daten bereitgestellt werden sollen, wobei das Gewicht der Tatvorwürfe, die Schwere und Dringlichkeit des Falls usw. durch die Abwägung zwischen konkurrierenden Rechtsgütern umfassend berücksichtigt werden sollten. In vorliegendem Fall verstößt die Handlung des Anbieters, der Ermittlungsbehörde die Bestandsdaten des Nutzers zur Verfügung zu stellen, jedoch gegen diese Verpflichtung und verursacht Schäden durch einen rechtswidrigen Eingriff in das Recht auf informationelle Selbstbestimmung, sodass er verpflichtet ist, ein Schmerzensgeld für seelische Schäden des Nutzers zu zahlen.“[508] *(Übersetzung vom Autor)*

Nach den beiden Entscheidungen wurden infrage gestellt, ob die Erhebung der Bestandsdaten durch die Ermittlungsbehörde eine Zwangsmaßnahme ist, und ob sie mit dem Richtervorbehalt in Verbindung gebracht werden sollte. Insb. die Entscheidung des K-VerfG wurde von der Öffentlichkeit stark kritisiert, weil es seine Aufgabe zum Schutz der Grundrechte vernachlässigt hatte. Kurz darauf wurde ein Gesetzesvorschlag, diese Datenerhebung mit dem Richtervorbehalt und der nachträglichen Benachrichtigung des von Daten Betroffenen zu verknüpfen, von den Abgeordneten vorgelegt.[509] Im Jahr 2014 beschloss auch die K-MRK, dass die Bestandsdatenauskunft gemäß § 83 K-TKGG zwar tatsächlich eine Zwangsmaßnahme darstellt, aber in der Praxis ohne richterliche Kontrolle von der Ermittlungsbehörde übermäßig verlangt wird und sie daher durch Gesetzesänderung dem Richtervor-

Regulierungsform dieser Vorschrift … so scheint es, dass die Auskunft über Bestandsdaten vom Diensteanbieter entschieden wird. Aber … wenn eine Ermittlungsbehörde aufgrund dieser Vorschrift die Bestandsdatenauskunft von einem Dienstanbieter verlangt, hat er keinen Grund, diese auf eigene Gefahr abzulehnen. Somit schreibt die Vorschrift vor, dass die Bestandsdaten grundsätzlich bereitgestellt werden. Daher sollte davon ausgegangen werden, dass die Bereitstellung der Bestandsdaten nicht individuell vom Dienstanbieter beurteilt wird, sondern tatsächlich auf Verlangen (der Behörde) aufgrund der Vorschrift erfolgt. In dieser Struktur wird die Auslegung, dass das Auskunftsverlangen von der Seite des Dienstanbieters nicht zwingend ist, sodass es … keine Ausübung hoheitlicher Gewalt ist, … dazu führen, dass die Natur der Beschränkung der Grundrechte vernachlässigt wird. Das heißt, die Erhebung von Bestandsdaten in diesem Fall liegt im Wesentlichen in der Beschränkung der Grundrechte für den von Daten Betroffenen, und daher muss anhand von ihm beurteilt werden, ob eine öffentliche Gewalt ausgeübt wurde. … Sie ist ein Ermittlungsakt und gehört zu einem hoheitlichen Realakt.“ Dafür ist *Gyeo-Cheol Lim*, PLR, 57-4, 2016, 197, 208 f.

[508] *Obergericht Seoul-Entscheidung* vom 18. 10. 2012 – 2011 Na 19012.

[509] Info-System über Gesetzentwürfe, <http://likms.assembly.go.kr/bill/BillSearchLawResult.do>, Abruf: 31. 12. 2020.

behalt unterliegen und der Betroffene nachträglich benachrichtigt werden sollte.[510] Im Schrifttum stehen aber die Meinungen im Widerspruch. Die vorherrschende Ansicht ist, dass die Bestandsdaten i. d. R. dazu dienen, zu Beginn der Ermittlung den Verdächtigen zu bestimmen, sodass das Auskunftsverlangen durch die gerichtliche Prüfung eine rasche frühe Untersuchung behindert.[511] Sie schlägt somit andere Möglichkeiten vor, um die übermäßigen Auskunftserteilungen in der Praxis zu begrenzen: etwa die Schaffung der sog. „Richtlinien zur Bestandsdatenauskunft", die Verfahren, Kriterien und Umfang etc. enthalten und bei der Auskunft über Bestandsdaten und der Auskunftserteilung von der Ermittlungsbehörde und dem Anbieter eingehalten werden müssen,[512] oder die Kontrolle durch den zuständigen LOStA.[513] Andererseits argumentiert die h. M., dass auch für diese Auskunftserteilung eine Benachrichtigung erforderlich ist.[514] Inzwischen hat der K-OGH am 30. März 2016 in der Revisionsinstanz gegen die o. g. Entscheidung vom Obergericht Seoul wie folgt entschieden und das angefochtene Urteil aufgehoben:

> „Um zu sagen, dass die Bereitstellung … von Bestandsdaten durch den TK-Dienstanbieter illegal ist, sollte … davon ausgegangen werden, dass er verpflichtet ist, die Bereitstellung unter Berücksichtigung der konkreten Umstände des Einzelfalls praktisch zu prüfen. Eine solche Verpflichtung kann jedoch aus folgenden Gründen i. d. R. nicht bestehen: § 54 Abs. 3, 4 K-TKGG a. F. sieht … nicht vor, dass der Anbieter … tatsächlich prüfen kann. Dies gilt auch dann, wenn eine Sonderorganisation nach § 54 Abs. 8 K-TKGG a. F. in Betracht gezogen wird. In der Realität ist es schwierig, von dem Anbieter, der keine Justizbehörde darstellt, … eine praktische Prüfung der konkreten Umstände des Einzelfalls wie die Abwägung oder die Schwere und Dringlichkeit des Falls zu verlangen oder zu erwarten … Die Auferlegung einer solchen tatsächlichen Prüfungspflicht steht nicht im Einklang mit der gesetzgeberischen Absicht von § 54 K-TKGG a. F. … Grundsätzlich sollte die Kontrolle gegen den Amtsmissbrauch der Ermittlungsbehörde direkt bei ihr erfolgen. Bei der Ertei-

---

[510] *K-MRK-Beschluss* (Fn. 472), 4 – 6. Hier schlug die *K-MRK* vor, die Bestandsdaten in die Verkehrsdaten von § 2 Nr. 11 K-KGSG einzubeziehen (auch *Yangsub Kwon*, korLR, Band 59, 2015, 397, 408 f.). Dies scheint auf der herrschenden Ansicht Südkoreas zu basieren, dass die Bestandsdaten – nicht nur durch das Recht auf informationelle Selbstbestimmung, sondern auch – durch den Schutz des Kommunikationsgeheimnisses geschützt werden (vgl. Kapitel 2, C. II. 2.).

[511] *Jusung Yoo*, KCR, 24-3, 2013, 85, 92 – 97 und 101 f.; *Chan-Keol Park*/*Dong-Wook Kang*, JLP, 14-1, 2014, 9, 25 f.; auch die Stellungnahme des Justizministeriums und der Polizei, die im *K-MRK-Beschluss* (Fn. 472) angegeben wird: 13 f.; a. A. *Kyung-Sin Park*, IHLR, 13-2, 2010, 265, 293 f.: Durch die Streichung von § 83 K-TKGGG sollten die allgemeinen Vorschriften von Beschlagnahme und Durchsuchung der K-StPO angewendet werden; zust. *Jina Cha*, KLAJ, 67-2, 2018, 366, 390 [Fn. 51]. Natürlich kann die Ermittlungsbehörde auch jetzt noch unabhängig von § 83 K-TKGG die Daten durch einfache Beschlagnahme und Durchsuchung erhalten (*Jusung Yoo*, a. a. O. 97).

[512] *Jusung Yoo*, KCR, 24-3, 2013, 85, 100; *Chan-Keol Park*/*Dong-Wook Kang*, JLP, 14-1, 2014, 9, 36 f.; *Yangsub Kwon*, korLR, Band 59, 2015, 397, 409 f.

[513] *Won-Sang Lee*, TPCP, 7-1, 2015, 70, 89.

[514] *Jusung Yoo*, KCR, 24-3, 2013, 85, 105; *Chan-Keol Park*/*Dong-Wook Kang*, JLP, 14-1, 2014, 9, 36; *Won-Sang Lee*, TPCP, 7-1, 2015, 70, 86; *Gyeo-Cheol Lim*, PLR, 57-4, 2016, 197, 210.

lung einer Auskunft über Bestandsdaten durch die Ermittlungsbehörde dem Anbieter eine tatsächliche Prüfungspflicht und eine Verantwortung für die Erteilung aufzuerlegen, ist nichts anderes als die Übertragung der vom Staat oder der Ermittlungsbehörde zu tragenden Verantwortung auf die Privatperson. Wenn er die in der Vorschrift festgelegten formalen Anforderungen geprüft und der Ermittlungsbehörde die Bestandsdaten des Nutzers mitgeteilt hat, kann daher nicht ausgegangen werden, dass die Grundrechte des Nutzers verletzt wurden, es sei denn, es liegen besondere Umstände vor, z. B. im Fall, dass es offensichtlich ist, dass die Ermittlungsbehörde das Recht auf Auskunftsverlangen missbraucht, sodass die Interessen des von Daten Betroffenen oder Dritter unberechtigt verletzt werden."[515] *(Übersetzung vom Autor)*

(3) Es ist praktisch unmöglich, dass der Dienstanbieter als Privatperson ein Auskunftsverlangen einer Ermittlungsbehörde ablehnt, es sei denn, es gibt einen formalen Fehler oder einen eindeutigen Amtsmissbrauch. Daher ist es nicht angebracht, ihn für die Bereitstellung von Bestandsdaten verantwortlich zu machen. Damit diese Verantwortung ihm auferlegt werden soll, muss ihm gleichzeitig das Recht auf Verweigerung oder Einspruch gegen das Auskunftsverlangen gewährleistet werden.[516] Daher ist die Stellungnahme des K-OGH angemessen.[517] Auf der anderen Seite wird das informationelle Selbstbestimmungsrecht des Betroffenen durch die Erhebung von Bestandsdaten eingegriffen, aber diese muss mit Blick auf ihre geringe Eingriffsintensität nicht unbedingt mit dem Richtervorbehalt in Verbindung gebracht werden. Außerdem ist es angesichts der hohen Annahmerate bei der Erhebung von Verkehrsdaten (siehe Fn. 474), die bereits mit dem Richtervorbehalt verbunden ist, sehr wahrscheinlich, dass die richterliche Prüfung zur Auskunft über Bestandsdaten formell erfolgt.[518] Aus alledem wird empfohlen, dass solche Daten auf der Grundlage der „Richtlinien zur Auskunft über Bestandsdaten und ihrer Verwendung" (als provisorische Bezeichnung) zu verlangen und zu verwenden sind, die gemeinsam von verwandten Organisationen wie dem Ministerium für Justiz, für Verwaltung und Inneres und für WTIK und dem Dienstanbieterverband erstellt werden.[519] Der Anbieter führt nur formale und verfahrensmäßige Prüfungen durch, und das ist ausreichend. Schließlich müssen nicht alle von Daten Betroffenen über die Auskunftserteilung informiert werden, zumindest sind jedoch die Verfahrensbeteiligten wie der Verdächtigte zu benachrichtigen, und die restlichen Daten sind zu löschen bzw. zu vernichten, dies ist aktenkundig zu machen; diese Verpflichtung sollte gesetzlich festgelegt werden.[520]

---

[515] *K-OGHE* vom 10. 3. 2016 – 2012 Da 105482.

[516] *Gyeo-Cheol Lim*, PLR, 57-4, 2016, 197, 217.

[517] Zust. *Jusung Yoo*, KCR, 24-3, 2013, 85, 99 f.; *Gyeo-Cheol Lim*, PLR, 57-4, 2016, 197, 216.

[518] Vgl. *Jusung Yoo*, KCR, 24-3, 2013, 85, 103: Formeller Richtervorbehalt.

[519] Zust. *Jusung Yoo*, KCR, 24-3, 2013, 85, 100 und 105; *Yangsub Kwon*, korLR, Band 59, 2015, 397, 410.

[520] Im gleichen Sinne *Gyeo-Cheol Lim*, PLR, 57-4, 2016, 197, 219.

4. Das Abhören von nichtöffentlichen Gesprächen: § 14 K-KGSG

(1) K-KGSG sieht für das Abhören des Gesprächs lediglich vor, dass „niemand nichtöffentliche Gespräche zwischen anderen Personen aufzeichnen oder mit Hilfe der technischen Mittel abhören darf" (§ 14 Abs. 1; auch § 3 Abs. 1), und umfassend gelten entsprechend für das Abhören die Ermächtigungsnormen zur TKÜ wie Eingriffsvoraussetzungen und Durchführungsverfahren ausgenommen die Regelungen bezüglich des Dienstanbieters (§ 14 Abs. 2 i. V. m. §§ 4 – 8, § 9 Abs. 1 S. 1, Abs. 3, § 9a, § 11 Abs. 1, 3 und 4 sowie § 12 K-KGSG). Der Inhalt des Gesprächs, der durch illegales Abhören erhalten wurde, darf nicht als Beweismittel in Gerichts- oder Disziplinarverfahren verwendet werden (§ 4 K-KGSG). Das Abhören des Gesprächs darf nur für die in § 5 Abs. 1 K-KGSG genannten Straftaten durch richterliche Erlaubnis durchgeführt werden und es muss für jeden Betroffenen im Einzelnen beantragt und erlaubt werden (§ 6 Abs. 1 – 3, 5 K-KGSG). In der Antragsschrift und dem Erlaubnisschein sind Art, Zweck, Gegenstände, Umfang und Zeitraum und Durchführungsort und -methode des Abhörens des Gesprächs anzugeben (§ 6 Abs. 4, 6 K-KGSG). Seine Anordnung und Verlängerung darf zwei Monate nicht überschreiten (§ 6 Abs. 7 K-KGSG) und die gesamte Verlängerungsfrist ein oder drei Jahre nicht überschreiten (§ 6 Abs. 8 K-KGSG). In dringenden Fällen kann auch das Abhören des Gesprächs nach § 8 K-KGSG gestattet sein. Diese Maßnahme wird i. d. R. direkt von der Ermittlungsbehörde durchgeführt (§ 9 Abs. 1 S. 1 K-KGSG). Die Behörde muss den Betroffenen, gegen den sich die Maßnahme richtet, über die Durchführung, Durchführungsbehörde und den -zeitraum etc. schriftlich benachrichtigen (§ 9a Abs. 1 – 2 K-KGSG), dies kann in bestimmten Fällen zurückgestellt werden (§ 9a Abs. 4 – 6 K-KGSG). Für dieses Abhören gelten freilich auch § 11 K-KGSG über das Verbot der Veröffentlichung und Offenbarung von Informationen bezüglich der Erlaubnis, Durchführung oder Benachrichtigung der Maßnahme und § 12 K-KGSG über die Beschränkung der Verwertung erfasster Daten.

Heute scheint die Ermittlungsbehörde jedoch in der Untersuchungspraxis kaum das Abhören des Gesprächs nach § 14 K-KGSG einzusetzen. Seit der Schaffung dieses Gesetzes wurde in den Rspr. bisher kein Fall gefunden, in dem die Ermittlungsbehörde selbst Äußerungen oder Gespräche anderer Personen – innerhalb oder außerhalb von Wohnraum – heimlich aufgezeichnet hat. Alle Entscheidungen über das Abhören des Gesprächs beziehen sich auf die Beweisfähigkeit der von Privatpersonen aufgezeichneten (Telefon-)Gespräche, was natürlich nicht auf dem K-KGSG beruht.

(2) Was von § 3 Abs. 1 und § 14 Abs. 1 K-KGSG geregelt wird, sind nicht „Worte" von Menschen, sondern „Gespräche", die von zwei oder mehr Personen geführt werden. Dies unterscheidet sich entscheidend von der Regelung in Deutschland, wo die Äußerungen der Menschen selbst aufgrund des Persönlichkeitsrechts geschützt werden. Nach dem Wortlaut der o. g. Vorschriften ist verboten ein Abhören von „nichtöffentlichen Gesprächen zwischen anderen Personen". Im

Allgemeinen wird die Bedeutung von „nichtöffentlich“ danach beurteilt, ob die Teilnehmer oder Hörer des Gesprächs eingeschränkt sind und wo es stattfindet,[521] und „Gespräche“ bedeuten ein Kommunikationsverhalten, das mit natürlicher Stimme ohne Medium an einem räumlich nahen Ort geführt wird.[522] Es ist jedoch umstritten, was „zwischen anderen Personen“ bedeutet. Diesbezüglich stellt sich u. a. die Frage, ob der Gesprächspartner, wenn er den Gesprächsinhalt selbst oder unter Mitwirkung eines Dritten aufgezeichnet hat, vom Begriff der „anderen Personen“ ausgeschlossen oder darin einbezogen wird, d. h. ob diese Aufzeichnung gegen § 3 Abs. 1 K-KGSG verstößt und daher sie nach § 4 K-KGSG nicht als Beweismittel verwendet werden darf.[523] In der Literatur sind die Meinungen zwar widersprüchlich, aber der K-OGH unterscheidet hierbei kontinuierlich zwischen der Aufzeichnung des (Telefon-)Gesprächs durch einen Partner und derjenigen durch eine dritte Person mit Zustimmung eines Partners. Nach seiner Rspr. gehört der Partner im ersteren Fall begrifflich nicht zu „anderen Personen“, sodass kein Verstoß gegen § 3 Abs. 1 K-KGSG vorliegt und somit die Aufzeichnung als Beweismittel verwendet werden darf,[524] während ein solcher Verstoß im letzteren Fall aufgrund des Sinns und Zwecks des K-KGSG – ohne weitere Begründung – vorliegt.[525] In der Literatur wird diese Stellungnahme teilweise kritisiert; durch die Intervention eines Dritten wird nämlich das (Telefon-)Gespräch nicht mehr nichtöffentlich geführt, daher gilt § 3 Abs. 1 K-KGSG nicht mehr.[526]

Da die Äußerungen von Menschen durch die Aufzeichnung und Speicherung tatsächlich dauerhaft erhalten werden, sollte aber hinsichtlich der Intensität des Eingriffs in die Privatsphäre vom einfachen Abhören und der mündlichen Übermittlung der Äußerungen unterschieden werden. Zum wirksamen Schutz des Persönlichkeitsrechts sollte das Gesetz dahingehend überarbeitet werden, dass die menschlichen Äußerungen selbst geschützt werden.[527] Der Grund, warum der K-OGH entschieden hat, dass Aufzeichnungen, die durch eine dritte Person mit

---

[521] Nichtöffentlichkeit ist von Heimlichkeit zu unterscheiden (*Hyung-Joon Kim*, JCL, Nr. 24, 2005, 213, 231).

[522] *Hyung-Joon Kim*, JCL, Nr. 24, 2005, 213, 230 f.; *Joo-Won Rhee*, K-StPO, 383; zust. *K-OGHE* vom 15. 3. 2017 – 2016 Do 19843: Daher gehört der Ton, der von Dingen ausgeht und keine menschliche Stimme ist, nicht zum Begriff des Gesprächs, und außerdem gehören einfache Schreie oder Seufzer, die menschliche Stimme sind, nicht dazu, es sei denn, er dient der Kommunikation.

[523] In Südkorea wird auf der gleichen Ebene auch die Fallkonstellation behandelt, dass ein Partner des Telefongesprächs selbst oder unter Mitwirkung Dritter seinen Inhalt aufzeichnet (vgl. oben 1. a) aa) (3)).

[524] *K-OGHE* vom 28. 3. 1997 – 97 Do 240; *ders.* vom 9. 3. 1999 – 98 Do 3169; *ders.* vom 9. 10. 2001 – 2001 Do 3106; *ders.* vom 23. 10. 2008 – 2008 Do 1237; dies gilt auch für Gespräche zwischen drei Personen, *ders.* vom 28. 3. 1997 – 96 Do 2417; *ders.* vom 12. 10. 2006 – 2006 Do 4981; *ders.* vom 16. 5. 2014 – 2013 Do 16404.

[525] *K-OGHE* vom 8. 10. 2002 – 2002 Do 123.

[526] *Hyung-Joon Kim*, JCL, Nr. 24, 2005, 213, 221 und 231 f.

[527] Im gleichen Sinne, *Kuk Cho*, Ausschlussprinzip, 320 f.

Zustimmung eines (Telefon-)Gesprächspartners gemacht wurden, als Beweismittel unzulässig sind, liegt darin, dass der Gerichtshof i. R. d. aktuellen Gesetzestextes die Äußerungen selbst so weit wie möglich schützen will.[528]

5. Einsatz eines eigenständigen GPS-Trackers

Wie bereits erwähnt, sind die Standortdaten in Echtzeit keine Inhaltsdaten, aber sie werden als empfindlicher und wichtiger als andere Verkehrsdaten in Südkorea angesehen (vgl. oben 2. c) aa)). Solche Daten können jedoch nicht nur über Mobiltelefone, die bereits mit GPS-Technologie ausgestattet sind, sondern auch über einen eigenständigen GPS-Tracker erhoben werden. Im letzteren Fall ist das Gerät nicht mit dem Dienst des TK-Dienstanbieters verbunden und wird so verwendet, dass die Ermittlungsbehörde es an einem zu überwachenden und zu verfolgenden Objekt befestigt und seinen Standort von ihm erhält. Daher kann nach einer Ansicht der Literatur der Einsatz eines eigenständigen GPS-Trackers nur unter den gleichen Eingriffsvoraussetzungen und Kontrollverfahren wie bei TKÜ erlaubt werden.[529] Dies ist angesichts der Bedeutung von Standortdaten in Echtzeit sinnvoll. Diese Ansicht argumentiert jedoch, dass die Ermächtigungsnorm in K-KGSG festgelegt werden sollte, da diese Maßnahme auch eine Ermittlungsmethode im Zusammenhang mit IuK-Technologie ist. Dies entspricht nicht dem Titel und dem legislativen Zweck des Gesetzes „Schutz der Kommunikationsgeheimnisse". Freilich bedarf es einer Ermächtigungsnorm im Lichte der Normenklarheit. Angesichts der weiteren Entwicklung der Methode zur heimlichen Datenerhebung ist auch in Südkorea eine Vorschrift erforderlich, die dieselbe Rolle spielt wie § 100h Abs. 1 S. 2 StPO.[530]

III. Zusammenfassung und Zwischenfazit

Die heimlichen Ermittlungsmaßnahmen, die von Ermittlungsbehörden zur Beweissicherung in Südkorea eingesetzt oder verwendet werden, unterscheiden sich nicht wesentlich von denen in Deutschland. Die Ermächtigungsgrundlagen für diese Maßnahmen sind jedoch weder so detailliert noch normenklar ausgestaltet wie in Deutschland, je nach ihrer Eingriffsintensität und der Art und Weise ihrer Durchführung; insb. betrifft dies die Überwachung innerhalb oder außerhalb von Wohn-

[528] Diese Ansicht des *K-OGH* beruht darauf, dass der aufzeichnende Dritter seitens des Gegenübers des zustimmenden Gesprächspartners ein echter Dritter ist (*Hyung-Joon Kim*, JCL, Nr. 24, 2005, 213, 231).

[529] *Bong-Su Kim*, CNLR, 32-3, 2012, 271, 290 ff.; *Daeho Choi*, KNULJ, Band 62, 2018, 213, 244 f. Beide Autoren fordern die gleichen Anforderungen wie bei TKÜ auch für die Erhebung von GPS-Standortdaten (in Echtzeit) mittels Mobiltelefonen (siehe Fn. 491).

[530] Des Weiteren ist es erforderlich, einen unabhängigen Abschnitt innerhalb der K-StPO oder ein Sondergesetz zu schaffen, in dem Ermächtigungsgrundlagen zur Sicherstellung, Verwendung oder Verwahrung personenbezogener Daten abgesehen von allgemeiner Beschlagnahme und Durchsuchung umfassend festlegt werden.

raum, die Online-Durchsuchung, die Echtzeit-Lokalisierung und ein Einsatz technischer Mittel. In der Literatur wird i. d. R. gefordert, dass die Ermächtigungen für jede Maßnahme klarer und strenger ausgestaltet werden als jetzt, um den Missbrauch von Ermittlungsbefugnissen zu verhindern und die Grundrechte wirksam zu schützen. Ermittlungsbehörden und Geheimdienste lehnen dies jedoch stark ab. Sie ergreifen in der Praxis ggf. Maßnahmen, die in Grundrechte schwer eingreifen, – ohne gerichtliche Einschaltung – selbstständig, weil es keine eindeutige Ermächtigung dafür gibt; z. B. die Online-Durchsuchung oder den Einsatz des GPS-Trackers. Gerichte erlauben auch oft auf Verlangen der StA eine neue Art von starken Maßnahmen auf der Grundlage bestehender Vorschriften: z. B. die Erhebung der Standortdaten in Echtzeit. Schließlich ist das *K-VerfG* u. a. bei der Prüfung der Verfassungswidrigkeit bestimmter Ermittlungsmaßnahmen oder der Ermächtigungsnormen nicht streng. Natürlich unterscheiden sich die Kriterien und die Gewichte der Prüfung der rechtsstaatlichen Abwägung bezüglich der heimlichen Ermittlungsmaßnahmen, die einen schwerwiegenden Grundrechtseingriff bewirken, von Land zu Land, was sich im Gesetz durch die Gesetzgebung widerspiegelt. Dennoch hat die K-KGSG insgesamt viele Mängel. Insb. die Mängel beim Verfahren der nachträglichen Benachrichtigung des Betroffenen, das Fehlen eines effektiven Rechtsschutzes und das Fehlen der ergänzenden Ermächtigung zum Einsatz neuer technischer Mittel stehen im Widerspruch zu den Grundsätzen der Normenklarheit und Verhältnismäßigkeit und dem Recht auf Anrufung der Gerichte, auch unter Berücksichtigung der besonderen Umstände Koreas im Zusammenhang mit der Staatssicherheit.

Kapitel 4

Anwendungsbereich und Verfahrensgarantien allgemeiner Vorschriften der Beschlagnahme und Durchsuchung

A. Vorrede

Für den Zwang zur Sicherstellung von Beweismitteln im Ermittlungsverfahren bestehen in der StPO §§ 94 ff., 102 ff. StPO als allgemeine Rechtsgrundlage und §§ 99 ff. StPO für die jeweilige Maßnahme (vgl. Kapitel 3, B.). Aus der Auslegung jeder Vorschrift wird jedoch ihr Anwendungsbereich in einigen Fällen nicht klar abgeleitet. Insbesondere neigen die Ermittlungsbehörden dazu, gestützt auf die allgemeinen Vorschriften neue Arten von Maßnahmen oder andere, die von §§ 99 ff. StPO nicht eindeutig erfasst werden, auszuführen. Denn die meisten Ermächtigungen der §§ 99 ff. StPO unterliegen qualifizierten Eingriffsvoraussetzungen und Verfahrensgarantien, die über dieselben der allgemeinen Vorschriften, ausschließlich den Grundrechtseingriff mittlerer Qualität zu legitimieren,[1] hinausgehen. Die Art und Weise der Durchsuchung und Beschlagnahme zu klären, die durch §§ 94 ff., 102 ff. StPO (nicht) abgedeckt werden kann, ist daher einerseits mit Blick auf das

[1] Vgl. *Brodowski/Eisenmenger*, ZD 3/2014, 119, 122. Bezüglich Datenzugriff steht das Recht auf informationelle Selbstbestimmung im Mittelpunkt. Heute kann aber insb. bei umfangreichem Zugriff auf Datenbestände oder Daten das Computer-Grundrecht betroffen sein. Es ist unklar, ob dieses Grundrecht, die Vertraulichkeit und Integrität informationstechnischer Systeme zu schützen, „ausschließlich durch heimliche Zugriffe" zu verletzen ist. Dies gilt auch dann, wenn die Entscheidung des *BVerfG* berücksichtigt wird (vgl. *BVerfGE* 120, 274, 313 ff. [Rn. 201 – 206]). Nach ihrer Beschreibung schützt das Computer-Grundrecht in erster Linie das Interesse des Nutzers, dass die vom (geschützten) System erzeugten, verarbeiteten und gespeicherten Daten „vertraulich bleiben", und die (technische) Integrität des Systems (a. a. O. 314 [Rn. 204]). Insbesondere „vor einem heimlichen Zugriff", durch den die auf dem System vorhandenen Daten ganz oder zu wesentlichen Teilen ausgespäht werden können, schützt es die Daten (a. a. O. 314 [Rn. 205]). Der Hauptgrund, warum das Gericht – neben dem informationellen Selbstbestimmungsrecht – das Grundrecht neu geschaffen hat, besteht jedoch darin, Einzelpersonen vor dem Zugang zum System zu schützen, das personenbezogene Daten in einem Umfang und in einer Vielfalt enthalten kann, dass ein Zugriff darauf es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten (vgl. a. a. O. 314 [Rn. 203]). Heute sind diese Eingriffe nicht unbedingt an einen geheimen Zugang gebunden. Auch angesichts der Tatsache, dass die Unverletzlichkeit der Wohnung nicht nur durch offene Maßnahmen, sondern auch durch heimliche tangiert werden kann (a. a. O. 309 f. [Rn. 192 – 193]), gilt dies. Diese Diskussion bezieht sich auf die Durchsicht der gesamten Datenbestände gemäß § 110 StPO.

Gebot der Normenbestimmtheit und -klarheit nicht nur für die Bürger, sondern auch für die Ermittlungsbehörden und Gerichte wichtig, und es dient andererseits in Hinsicht auf den Grundsatz der Verhältnismäßigkeit der Überprüfung der Rechtmäßigkeit der Ermittlungsmaßnahmen.

Die Beschlagnahme und Durchsuchung im Strafverfahren stellt – zusammen mit der präventiven Datenerhebung zur Abwehr von Gefahren – einen typischen staatlichen Eingriff in personenbezogene Daten dar. Sie ist nach dem Grundsatz der Zweckbindung und -bestimmung nur zum Ermittlungszweck, nämlich zum Zweck der Aufklärung für die Strafverfolgung im konkreten Anlassfall, zulässig, und sie kann nach dem Grundsatz der Verhältnismäßigkeit nur in angemessenen Grenzen gerechtfertigt werden. So sind für den Begriff der Durchsuchung und Beschlagnahme der Zweck und die Verfahrensrelevanz entscheidend[2], und *sie* wird traditionell als Ermittlungsmaßnahme verstanden, um Gegenstände zu sichern, die unmittelbar oder mittelbar für die Tat oder die Umstände ihrer Begehung Beweis erbringen, d. h. potenzielle Beweisbedeutung haben.[3]

Nach diesem Verständnis stellt sich zuerst die Frage, ob §§ 94 ff., 102 ff. StPO in der modernen Informationsgesellschaft immer noch dem Gebot der Normenbestimmtheit und -klarheit gerecht werden. In erster Linie stellt sich die Frage um die Beschlagfähigkeit elektronischer Daten, die auch mit Beschlagnahmemethoden zu tun hat (vgl. unten B. I.). Es ist dann umstritten, ob nach den Vorschriften nur eine offene Maßnahme zulässig ist (vgl. unten B. II.). Dabei handelt es sich um die Rechtfertigung einer neuen Art von (heimlichen) Maßnahmen. Schließlich ist streitig, ob die – offene – Erfassung der Daten, die auf dem Server des Dienstanbieters gespeichert sind, auf dieser Regelung beruhen kann (vgl. unten B. III.). Dieses Problem ist wirklich erheblich, da heutzutage fast alle personenbezogenen Daten durch informationstechnische Systeme erzeugt, verarbeitet und weitergegeben und am Ende beim Anbieter umfassend gespeichert werden. Zum anderen stellt sich die Frage, ob §§ 94 ff., 102 ff. StPO unter dem Gesichtspunkt der Verhältnismäßigkeit, insb. der Abwägung, auch beim Zugriff auf den gesamten Datenbestand des Betroffenen so ausgestaltet sind, dass sie seine Persönlichkeit ausreichend schützen (vgl. unten C. I.). Dies ist darauf zurückzuführen, dass die Durchsuchung und Beschlagnahme nach den Vorschriften heutzutage auch mit der nur einmaligen

[2] Vgl. *BVerfGE* 113, 29, 51 [Rn. 104]; 124, 43, 61 [Rn. 64 a. E.]: „*Die Ermittlungsmethoden der Strafprozessordnung sind zwar im Hinblick auf die Datenerhebung und den Datenumfang weit gefasst. Der den Datenzugriff begrenzende Verwendungszweck ist aber unter Beachtung des Normzusammenhangs, in welchen die §§ 94 ff. StPO eingebettet sind (vgl. § 152 Abs. 2, § 155 Abs. 1, § 160, § 170, § 244 Abs. 2, § 264 StPO), hinreichend präzise vorgegeben. Die jeweiligen Eingriffsgrundlagen stehen unter einer strengen Begrenzung auf den Ermittlungszweck. Strafprozessuale Ermittlungsmaßnahmen sind nur zulässig, soweit dies zur Vorbereitung der anstehenden Entscheidungen im Hinblick auf die in Frage stehende Straftat nötig ist. Auf die Ermittlung anderer Lebenssachverhalte und Verhältnisse erstrecken sich die Eingriffsermächtigungen nicht.*“

[3] *Park*, § 2 Rn. 31 und 50 und § 3 Rn. 446 und 454 ff.: dazu M-G/*Schmitt*, StPO, § 94 Rn. 5 f.

Durchführung zur umfassenden Erfassung von personenbezogenen Daten und dadurch zur Erstellung von Persönlichkeitsprofilen führen kann. Wurden personenbezogene Daten von den Ermittlungsbehörden bereits umfassend erfasst und eingesehen, so kann die daraus resultierende Persönlichkeitsbeeinträchtigung wesentlich nicht mehr rückgängig gemacht werden, daher ist hier eine vorherige Kontrolle durch die Richter und die Sicherung ihrer Wirksamkeit wichtig (vgl. unten C. II.) und dabei ist die Verwendung des § 110 StPO von entscheidender Bedeutung (vgl. unten C. III.). Eine einfache Durchsuchung und Beschlagnahme veranlasst – ebenso wie die heimliche Ermittlungsmaßnahme – zwar stets schwere Grundrechtseingriffe, aber die allgemeinen Vorschriften enthalten – anders als §§ 99 ff. StPO – keine qualifizierten Verfahrensgarantien, um die Eingriffsintensität der Datensammlung auszugleichen. Dazu kommt, dass die Strafverfolgungsbehörden in der Praxis häufig durchgängig versuchen, sich auf eine ausnahmsweise eingreifende Eilkompetenz zu berufen oder das Verfahren der Durchsicht gemäß § 110 StPO zu vermeiden. Vor diesem Hintergrund wird zum wirksamen Grundrechtsschutz im Verfahren der Durchsuchung und Beschlagnahme die Verstärkung der Stellung des Beschuldigten verlangt (vgl. unten C. IV.).

B. Abgrenzung nach dem Gebot der Normenbestimmtheit und -klarheit

I. Dürfen elektronische Daten Gegenstände der Beschlagnahme und Durchsuchung sein? – Beschlagnahmefähige Gegenstände

1. Fragestellung und Meinungsstreit

(1) Derzeit gibt es keine Einwände dagegen, dass informationstechnische Systeme als körperliche Gegenstände beschlagnahmefähig sind[4] und Durchsuchungsobjekte darstellen.[5] Zu den Gegenständen i. S. d. § 94 Abs. 1 StPO und zu den Sachen i. S. d. § 102 StPO gehören so nicht nur externe Speichermedien von Disketten, CDs, DVDs, USB-Sticks etc., sondern auch EDV-Anlagen wie PCs oder Smartphones des Einzelnen und Server von TK-Dienstanbietern oder Unternehmen.[6] Daneben können die technischen Hilfsmittel, mit deren Hilfe sichergestellte Daten sichtbar und lesbar

[4] *BVerfGE* 113, 29, 50; 124, 43, 60 f.; *Greven*, KK-StPO, § 94 Rn. 4; *Herrmann*/*Soine*, NJW 2011, 2922; *Kemper*, NStZ 2005, 538, 540; *Klesczewski*, ZStW 123 (2011), 737, 746; *Park*, § 4 Rn. 800; *Roxin*/*Schünemann*, § 34 Rn. 4; *Wohlers*/*Greco*, SK-StPO, § 94 Rn. 24; *Zimmermann*, JA 5/2014, 321, 322.

[5] *Bruns*, KK-StPO, § 102 Rn. 11; *Herrmann*/*Soine*, NJW 2011, 2922, 2924; *Klesczewski*, ZStW 123 (2011), 737, 746; M-G/*Schmitt*, StPO, § 102 Rn. 10a und § 103 Rn. 3; *Park*, § 4 Rn. 800; *Roxin*/*Schünemann*, § 35 Rn. 2; *Wohlers*/*Jäger*, SK-StPO, § 102 Rn. 15.

[6] In vielen Fällen ist es i. R. d. Durchsuchung und Beschlagnahme elektronischer Daten praktisch ziemlich schwierig, an Ort und Stelle aus solchen Systemen nur diejenigen Teile, die eine Speicherfunktion haben, physikalisch zu trennen.

gemacht werden, wie z. B. die vom Beschuldigten verwendete spezielle Software oder Computerprogramme sowie die Hardware, auf der solche Daten gefertigt wurden, bei Bedarf auch zusammen gesichert und verwendet werden.[7] Außerdem ist es klar, dass die (Computer-)Ausdrucke als körperliche Gegenstände beschlagnahmefähig sind.[8] Es ist jedoch umstritten, ob elektronische Daten selbst unter dem Aspekt der Normenklarheit Beschlagnahmefähigkeit haben. Bei dieser Kontroverse geht es teilweise darum, wie die Verfahrensvorschriften über die Durchsuchung von §§ 105 – 110 StPO auf eine Reihe von Prozessen zur Durchsuchung und Beschlagnahme von Daten anzuwenden sind und ferner, wann die Durchsuchung zu beenden ist.

(2) Nach einer Ansicht können nur physische Datenträger, aber keine Daten nach § 94 StPO beschlagnahmt bzw. sichergestellt werden.[9] Elektronische Daten können als solche nicht beschlagnahmt werden, weil sie keine körperlichen Gegenstände[10] oder nicht verkörpert[11] sind. Dass nur Daten auf einen Datenträger der Strafverfolgungsbehörden kopiert oder übertragen werden, ist allerdings auch nach dieser Ansicht möglich und gestattet, weil dies nach dem Verhältnismäßigkeitsgrundsatz weniger belastend ist.[12] Das heißt, diese „Kopie" oder „Übertragung" der Daten wird begrifflich aus Sicht des Strafprozessrechts vom § 94 StPO nicht erfasst und stellt eine ganz anders geartete Maßnahme dar.[13] Insb. vertreten *Wohlers*/*Greco* die

[7] *Greven*, KK-StPO, § 94 Rn. 4; *Kemper*, NStZ 2005, 538, 540 [Fn. 30]; M-G/*Schmitt*, StPO, § 94 Rn. 4; *Park*, § 4 Rn. 800 und 812; dazu *LG Trier* NJW 2004, 869: im Fall, dass die von einem der Beschuldigten verwendete Software nur serverunterstützt funktioniert.

[8] M-G/*Schmitt*, StPO, § 94 Rn. 4.

[9] *Kemper*, NStZ 2005, 538, 540 f.; *Klesczewski*, ZStW 123 (2011), 737, 747; *Roxin*/*Schünemann*, § 34 Rn. 4; *Wicker*, MMR 2013, 765, 766; *Wohlers*/*Greco*, SK-StPO, § 94 Rn. 26.

[10] *Klesczewski*, ZStW 123 (2011), 737, 747: nur körperliche Gegenstände; *Roxin*/*Schünemann*, § 34 Rn. 4; *Wohlers*/*Greco*, SK-StPO, § 94 Rn. 26. Der *BGH* hat in der Vergangenheit bei der Beurteilung der Rechtsgrundlage zur Beschlagnahme und Durchsuchung „der in den Mailboxen gespeicherten Daten" ausgeführt, dass die unmittelbare Anwendung der §§ 94 ff., 102 ff. StPO schon deshalb ausscheidet, weil es nicht um die Sicherstellung körperlicher Gegenstände oder um ein körperliches Eindringen in Wohnungen oder andere Räume geht (NJW 1997, 1934, 1935).

[11] *Kemper*, NStZ 2005, 538, 540 und dazu 541: „*Wenn der Gesetzgeber wirklich davon ausgeht, dass auch die auf einem Datenträger ‚verkörperten' Daten sichergestellt und beschlagnahmt werden können, dann kann und muss er dies auch eindeutig im Gesetz zum Ausdruck bringen, insbesondere wenn es sich um derartig fundamentale Fragen der Rechtsordnung handelt.*"

[12] *Greven*, KK-StPO, § 94 Rn. 4 und 13; *Kemper*, NStZ 2005, 538, 540; *Roxin*/*Schünemann*, § 34 Rn. 4; *Wohlers*/*Greco*, SK-StPO, § 94 Rn. 26.

[13] *Klesczewski*, ZStW 123 (2011), 737, 747. Vgl. *Kemper*, NStZ 2005, 538, 541 f.: Die Vornahme des Kopierens ist zu dokumentieren und sollte also die Zulässigkeit der Anfertigung einer „Kopie" bei der Durchsuchung und Beschlagnahme durch ein Tätigwerden des Gesetzgebers gelöst werden.

Auffassung, dass der § 110 Abs. 3 StPO, der durch das TKÜG vom 2008 geschaffen wurde, ein solches Vorgehen verdeutlicht.[14]

Die Vorschrift kann jedoch auch als Grundlage für die Gegenmeinung dienen. Das heißt, sie könnte die Grundlage dafür sein, dass der Gesetzgeber die Beschlagnahmefähigkeit elektronischer Daten ausdrücklich anerkannt hat. Die Möglichkeit der Beschlagnahme durch die Sicherstellung von Daten auf behördeneigenen Datenträgern begründet auch, dass die Daten als Gegenstände i. S. d. § 94 StPO beschlagnahmt werden können.[15] Dieser Auffassung ist aber nicht zuzustimmen. Nach klassischer Auslegung ist unter der – formlosen – amtlichen Inverwahrnahme (Hs. 1) oder der Sicherstellung in anderer Weise (Hs. 2) gemäß § 94 Abs. 1 StPO zu verstehen, dass die Sache der amtlichen Obhut untersteht (z. B. durch die Überführung der Sache in den Besitz der Behörde oder einer beauftragten Stelle oder Person und durch bestimmte an den Gewahrsamsinhaber gerichtete Verbote),[16] und weiter ist unter der – förmlichen – Beschlagnahme gemäß Abs. 2 zu verstehen, dass die Sache der tatsächlichen Verfügungsgewalt des Betroffenen entzogen und staatlicher Herrschaft unterworfen wird.[17] Da auch nach der Ablichtung elektronischer Daten die Möglichkeit des Zugriffs des Betroffenen auf sie nicht ausgeschlossen ist, kann somit infrage gestellt werden, ob die einfache Kopie oder Übertragung unter den Begriff der Beschlagnahme fällt. Jedoch zielt die Beschlagnahme nach § 94 StPO auf die Beweissicherung zur Erforschung und Aufklärung von Straftaten ab, nicht auf die Wegnahme des Verfügungsrechts.[18] Da der § 94 StPO für alle Gegenstände gilt, die als Beweismittel für die Untersuchung von Bedeutung sein können,[19] sind alle Arten von Sachen zu beschlagnahmen, zu denen auch die in Form von Dateien gespeicherten, unkörperlichen Daten gehören.[20]

Darüber hinaus können die Gründe hierfür aus verschiedenen Blickwinkeln dargelegt werden. Aus historischem und legislativem Gesichtspunkt war der § 94 StPO in erster Linie ursprünglich bei Schaffung der Norm ausschließlich von kör-

---

[14] Vgl. *Wohlers*/*Greco*, SK-StPO, § 94 Rn. 26: „*Der Kopiervorgang auf einen anderen Datenträger schafft vielmehr physikalisch einen neuen Gegenstand als Verkörperung der elektronischen Daten im Herrschaftsbereich der Strafverfolgungsbehörde.*"

[15] *Hofmann*, NStZ 2005, 121, 123; *Park*, § 4 Rn. 799.

[16] M-G/*Schmitt*, StPO, § 94 Rn. 14 ff.; *Park*, § 3 Rn. 432; *Wohlers*/*Greco*, SK-StPO, § 94 Rn. 10.

[17] *Park*, § 3 Rn. 433 und 436; *Wohlers*/*Greco*, SK-StPO, § 94 Rn. 11.

[18] Vgl. *Sieber*, 69. DJT 2012, C 114: „*Im Zuge einer Anpassung der StPO an die neuen Herausforderungen der IT sollte (jedoch) das für körperliche und sichtbare Gegenstände entwickelte ‚Wegnahmekonzept' der Beschlagnahme durch ein differenzierteres Konzept für die Beweisverwertung und die Konfiskation immaterieller Daten ergänzt werden.*"

[19] *BVerfGE* 113, 29, 51 [Rn. 102]; 124, 43, 61 [Rn. 63].

[20] *BVerfGE* 113, 29, 50 [Rn. 100]; *Bär*, EDV-Beweissicherung, Rn. 407; *Graulich*, wistra 8/2009, 299; *Meininghaus*, Der Zugriff auf E-Mails, 2007, 203 f.; M-G/*Schmitt*, StPO, § 94 Rn. 4 und 16a; *Park*, § 4 Rn. 799; *Singelstein*, NStZ 2012, 593, 596 f. und 602; *Zimmermann*, JA 5/2014, 321, 322.

perlichen Gegenständen ausgegangen.[21] In Anbetracht der zwischenzeitlichen Änderungen in der Entwicklung der IT, der Ergänzung der §§ 98a ff. StPO durch das OrgKG im Jahr 1992 und der Gesetzesmaterialien[22] zur Neufassung des § 110 Abs. 1 StPO durch das 1. Justizmodernisierungsgesetz vom 24. August 2004 ist es jedoch nunmehr nachvollziehbar zu verstehen, dass auch unkörperliche Gegenstände, insb. elektronische Daten als nichtkörperliche Informationen, begrifflich von § 94 StPO erfasst werden.[23] Dass die Daten nicht ergreifbar und ihr Inhalt nur unter Inanspruchnahme weiterer Hilfsmittel wahrnehmbar ist, ist anerkanntermaßen irrelevant wie etwa bei klassischen Tonbandaufnahmen.[24] Auch unter rechtssystematischem Gesichtspunkt spricht die StPO für die Beschlagnahmefähigkeit elektronischer Daten. Das *BVerfG* hat in der Überprüfung über die Verfassungsbeschwerde gegen den Beschlagnahmebeschluss von Kopien aller auf den Festplatten von Computern gespeicherten Daten dies ausdrücklich erklärt: „*Der Wortsinn (des § 94 StPO) gestattet es, als ‚Gegenstand' des Zugriffs auch nichtkörperliche Gegenstände zu verstehen. Der Wortlaut wird durch die Annahme, auch unkörperliche Gegenstände seien von § 94 StPO erfasst, … nicht überschritten.*"[25] Schließlich ergibt sich auch aus der teleologischen Interpretation, dass Daten oder Dateien nicht nur durch die Formulierung „der Sicherstellung durch (amtliche) Inverwahrungnahme oder auf andere Weise" des § 94 Abs. 1 StPO zu erfassen sind (sog. „formlose Sicherstellung"),[26] sondern auch in „Papieren" i. S. d. § 110 StPO enthalten sind (vgl. unten C. III. 2. a) aa)).[27] Das Strafverfahrensrecht ist – anders als das materielle Strafrecht – flexibel in praktischer und pragmatischer Hinsicht auszulegen. Aus alledem folgt, dass in der modernen Informationsgesellschaft, in der Informationen als Beweismittel meist in digitaler Form vorhanden sind, elektronische Daten selbst als Gegenstände der Beschlagnahme und Durchsuchung sichergestellt werden können.[28]

---

[21] *BVerfGE* 113, 29, 50 [Rn. 99]; *Meininghaus*, Der Zugriff auf E-Mails, 2007, 200.

[22] BT-Drs. 15/1508, S. 24: „*Der geltende § 110 Abs. 1 StPO … wird insbesondere angesichts der Entwicklung der modernen Bürotechnik praktischen Bedürfnissen nicht mehr gerecht, zumal der Begriff ‚Papiere' alle Arten von Unterlagen, auch elektronische, umfasst.*"

[23] *BVerfGE* 113, 29, 50 f.; *Park*, § 4 Rn. 790.

[24] Vgl. auch *Wohlers*/*Greco*, SK-StPO, § 94 Rn. 24.

[25] *BVerfGE* 113, 29, 50 [Rn. 100].

[26] M-G/*Schmitt*, StPO, § 94 Rn. 12 und § 95 Rn. 1; *Park*, § 3 Rn. 432. Die gesetzliche Terminologie ist zwar nicht ganz eindeutig, jedoch ist „Sicherstellung" als Oberbegriff gegenüber „förmliche Beschlagnahme" einerseits und „sonstige formlose Herstellung der staatlichen Gewalt" andererseits zu verstehen (M-G/*Schmitt*, StPO, § 94 Rn. 11; *Park*, § 3 Rn. 429 f.).

[27] Vgl. *Szesny*, WiJ 2012, 228, 231: Beweismittel ist der Inhalt der Dateien, nicht der gesamte Datenträger.

[28] In technischer Hinsicht ist das Original elektronischer Daten etwa mithilfe des Hashwerts von der Kopie zu unterscheiden. Weiterhin ist nach Erhebung der Daten zur Verhinderung der Fälschung und Manipulation und zur Auffindung versteckter oder gelöschter Dateien die Erstellung einer Eins-zu-eins-Kopie in der Praxis erlaubt und oft erforderlich.

Daher besteht kein Problem darin, dass die Daten durch die Spiegelung auf Speichermedien der Ermittlungsbehörde gesichert werden.[29]

2. Zwischenfazit

Aus alledem lässt sich herleiten, dass nicht nur körperliche Datenträger, sondern auch unkörperliche Daten unter „Gegenständen" i. S. d. § 94 StPO und „Sachen" i. S. d. § 102 StPO subsumiert werden. Dies widerspricht nicht dem Grundsatz der Normenklarheit. Heute sind elektronische Daten kein neues Phänomen mehr[30] und für die Bürger ist hinreichend erkennbar, dass durch §§ 94 ff. StPO neben Datenträgern auch die hierauf gespeicherten Daten sicherzustellen und zu beschlagnahmen sind.[31] Eine solche Auslegung, dass bei der Durchsuchung, die als Vorstufe der Beschlagnahme anzusehen ist,[32] lediglich die verfahrensrelevanten Daten gesucht und hierauf nur diese als Gegenstände der Beschlagnahme sichergestellt werden, ist nicht mehr fremd.

II. Sind eine „heimliche" Beschlagnahme und Durchsuchung aufgrund der §§ 94 ff., 102 ff. StPO zulässig?

1. Fragestellung

Diesbezüglich haben das *BVerfG* und der *BGH* bereits in ihren Entscheidungen klargestellt, dass durch §§ 94 ff., 102 ff. StPO nur eine offene Durchsuchung und Beschlagnahm gedeckt werden darf, jedoch nicht eine heimliche.[33] Im Licht des Rechts auf freie Gestaltung des Ermittlungsverfahrens kann man aber dies infrage stellen. Dies steht auch i. V. m. der Frage, ob §§ 105 ff. StPO zwingende Vorschriften oder bloße Ordnungsvorschriften sind. Für ihre Beurteilung ist einerseits die Auslegung der §§ 94, 98, 105 – 110 i. V. m. §§ 33, 35 StPO und andererseits der Abgleich mit §§ 99 ff. StPO erforderlich.

[29] *Park*, § 4 Rn. 799; *Zimmermann*, JA 5/2014, 321, 322.

[30] Vgl. *Kudlich*, StV 2102, 560, 561 [Fn. 16].

[31] Vgl. *BVerfGE* 113, 29, 51 [Rn. 102].

[32] *Park*, § 1 Rn. 14.

[33] *BVerfGE* 115, 166, 194 ff. [Rn. 104 ff.]; 124, 43, 62 ff. [Rn. 69 – 77]; *BGHSt* 51, 211, 212 – 216 [Rn. 5 – 13].

2. Meinungsstreit

a) Eine Mindermeinung: Zulässigkeit heimlicher Durchsuchung

Nach einer Meinung darf eine heimliche Durchsuchungsanordnung aufgrund der §§ 102, 103 StPO erlassen und durchgeführt werden. Denn die strafprozessuale Durchsuchung setzt weder ein offenes Handeln noch eine körperliche Anwesenheit von Ermittlungsbeamten am Durchsuchungsort voraus, und daher ist Offenheit kein konstitutives Merkmal des Durchsuchungsbegriffs.[34] Als Konsequenz hieraus sind die §§ 105 ff. StPO, die die Art und Weise der Durchführung der Durchsuchung regeln, bloße Ordnungsvorschriften und aus deren Verletzung können keine Rechtsfolgen hergeleitet werden.[35]

b) Herrschende Meinung: Unzulässigkeit heimlicher Durchsuchung

Die vorstehende Ansicht widerspricht jedoch der Justizförmigkeit des Strafverfahrens, die sich aus dem Grundsatz der Rechtsstaatlichkeit ergibt (vgl. Kapitel 2, A. II. 2. b)). Zuerst ist die Beschlagnahme und Durchsuchung nach §§ 94, 102, 103 StPO mit dem Richtervorbehalt und der Bekanntmachung/Benachrichtigung verbunden (vgl. unten aa)), die Durchführung der Durchsuchung muss in Befolgung des Verfahrens nach §§ 105 Abs. 2, 106 ff. StPO erfolgen (vgl. unten bb)). Daher darf diese Beschlagnahme und Durchsuchung heimlich weder angeordnet noch durchgeführt werden. Dass die Regelungen, die dem Grundrechtsschutz des Betroffenen dienen, als bloße Ordnungsvorschrift und nicht als zwingendes Recht angesehen werden und hierauf die Ermittlungsbehörden willkürlich über sie verfügen können, steht dem justizförmigen Strafverfahren entgegen. Zudem reichen verfahrensrechtliche Sicherungen der allgemeinen Vorschriften auch nicht aus, um das Eingriffsgewicht verdeckter Maßnahmen auszugleichen (vgl. unten cc)).

aa) Einfacher Richtervorbehalt

Die allgemeine Durchsuchung- und Beschlagnahmeanordnung, die mit einfachem Richtervorbehalt verbunden ist (§§ 98 Abs. 1, 105 Abs. 1 StPO), muss stets vor ihrer Ausführung dem Betroffenen bekanntgemacht werden (vgl. §§ 33 Abs. 3, 35 Abs. 2 StPO). Da die Heimlichkeit der Maßnahme von der Kenntnisnahme des Betroffenen zum Zeitpunkt ihrer Durchführung abhängt, ist der Betroffene über diese Durchsuchung und Beschlagnahme bis spätestens unmittelbar vor Beginn ihrer Durchführung zu unterrichten (Notwendigkeit überraschender Maßnahmen). Dabei ist die Benachrichtigung – anders als bei verdeckten Ermittlungsmaßnahmen (vgl. § 101 Abs. 5 StPO) – wegen Gefährdung des Untersuchungszwecks nicht zurückzustellen (vgl. Kapitel 3, A. II. 3.). So muss die richterliche Anordnung der

[34] *Hofmann*, NStZ 2005, 121, 123.

[35] *Hofmann*, NStZ 2005, 121, 124.

Durchsuchung und Beschlagnahme nach den allgemeinen Vorschriften i. d. R. mit Ausschluss von rechtlichem Gehör (§ 33 Abs. 3 – 4 StPO) in der Form eines Beschlusses, der schriftlich abgefasst und begründet wird, erlassen werden[36] und dieser muss mindestens an Ort und Stelle dem Betroffenen vorgelegt werden.

bb) Das Durchführungsverfahren der Durchsuchung gemäß §§ 102 ff. StPO

Das Bild einer regulären Durchsuchung nach §§ 102 ff. StPO wird dadurch geprägt, dass Ermittlungsbeamte am Ort körperlich anwesend sind, die Ermittlungen offenlegen und die Regelung nach §§ 105 Abs. 2, 106, 107 S. 1, 109 StPO einhalten.[37]

(1) § 105 Abs. 2 StPO sieht sog. „Durchsuchungszeugen" vor. Dies bezweckt, die ordnungsgemäße Durchführung der Durchsuchung und deren Beweisbarkeit zu gewährleisten.[38] Die Zuziehung der Zeugen muss nach dem Wort der Vorschrift möglich sein, jedoch wird sie unmöglich sein, wenn der damit verbundene Zeitverlust den Erfolg der Durchsuchung gefährden würde.[39] Nach h. M. trifft der die Durchsuchung leitende Beamte die Entscheidung über die Möglichkeit dieser Hinzuziehung nach pflichtgemäßem Ermessen,[40] aber die Konstellation ist mit dem Vorliegen der Gefahr im Verzug i. S. d. Abs. 1 vergleichbar (vgl. unten C. II. 2.).[41] Somit handelt es sich dabei um einen unbestimmten, aber überprüfbaren Rechtsbegriff und er ist objektiv zu beurteilen.[42] Diese Zeugenhinzuziehung schützt einerseits den Betroffenen vor Übergriffen der durchsuchenden Beamten, andererseits auch die Beamten vor unberechtigten Vorwürfen des Betroffenen wegen der Art und Weise der Durchsuchung.[43]

(2) § 106 Abs. 1 StPO sieht vor, dass der Inhaber der zu durchsuchenden Räume oder Gegenstände (S. 1) und bei dessen Abwesenheit, wenn möglich, sein Vertreter

[36] M-G/*Schmitt*, StPO, § 98 Rn. 8.

[37] Vgl. *BGHSt* 51, 211, 212 f. [Rn. 5].

[38] *BGH* NJW 1963, 1461; *Park*, § 2 Rn. 172.

[39] *BGH* NStZ 1986, 84, 85; M-G/*Schmitt*, StPO, § 105 Rn. 11; *Park*, § 2 Rn. 174; *Wohlers/Jäger*, SK-StPO, § 105 Rn. 56.

[40] *Bruns*, KK-StPO, § 105 Rn. 14; M-G/*Schmitt*, StPO, § 105 Rn. 11; *Park*, § 2 Rn. 175; *Wohlers/Jäger*, SK-StPO, § 105 Rn. 57; vgl. *BGHSt* 51, 211, 213 [Rn. 6]: Die Fassungen der § 105 Abs. 2 S. 1 und § 106 Abs. 1 S. 2 StPO („… sind/ist … zuzuziehen") postulieren Pflichten der Ermittlungsorgane.

[41] *Park*, § 2 Rn. 175; *Wohlers/Jäger*, SK-StPO, § 105 Rn. 57.

[42] *Park*, § 2 Rn. 175; *Wohlers/Jäger*, SK-StPO, § 105 Rn. 57.

[43] *BGH* NJW 1963, 1461; *Bruns*, KK-StPO, § 105 Rn. 14; M-G/*Schmitt*, StPO, § 105 Rn. 12; *Park*, § 2 Rn. 177; *Wohlers/Jäger*, SK-StPO, § 105 Rn. 53. Daher dürfen zwar der Betroffene oder die Beamten jeweils auf ihre Einhaltung verzichten, zum endgültigen Absehen von der Zuziehung müssen sie übereinstimmend darauf verzichten (*Roxin/Schünemann*, § 35 Rn. 10). Bei Anliegen des Betroffenen, von der Zuziehung von Zeugen abzusehen, um Aufsehen zu vermeiden, bleibt demzufolge die Entscheidung dem Ermessen des zuständigen Beamten überlassen (*Bruns*, a. a. O.; *Park*, a. a. O.; a. A. M-G/*Schmitt*, a. a. O.).

oder ein erwachsener Angehöriger, Hausgenosse oder Nachbar (S. 2) der Durchsuchung beiwohnen darf.

Der Begriff des Inhabers i. S. d. S. 1 richtet sich nicht nach Eigentumsverhältnissen, sondern nach den tatsächlichen Umständen, also dem Hausrecht bzw. den Gewahrsamsverhältnissen.[44] Bei der Durchsuchung nach § 102 StPO wird der Beschuldigte i. d. R. der Inhaber sein. Besteht die Gefahr, dass seine Anwesenheit die Durchsuchung nicht unerheblich erschwert oder hindert, z. B. Verdunklungsgefahr, so kann aber eine Anordnung zur Störungsbeseitigung aufgrund von unmittelbarem Zwang oder § 164 StPO getroffen werden.[45] Allerdings hat der inhaftierte Beschuldigte keinen Anspruch auf Anwesenheit,[46] jedoch kann er einen anderen, z. B. einen Rechtsanwalt mit der Wahrnehmung seiner Rechte beauftragen (vgl. Anwesenheit nach S. 2).[47] In diesem Fall kann er in sachlicher Weise die Rechtmäßigkeit des Vorgehens der Beamten prüfen und die Rechte des Beschuldigten wahrnehmen, aber dies ist keine Störung i. S. d. § 164 StPO.[48] Bei Durchsuchungen nach § 103 StPO können zum anderen alle Personen, die nicht verdächtig sind, z. B. Eltern, Geschwister, Freunde, Sozien und TK-Dienstanbieter oder nicht tatverdächtige Unternehmen, als Inhaber angeführt werden. In diesem Fall ist der Beschuldigte kein Inhaber i. S. d. S. 1 und daher hat kein Anwesenheitsrecht; Gleiches gilt für seinen Verteidiger.[49] Sie können aber hier – wie bei Durchsuchungen nach § 102 StPO – dann der Durchsuchung faktisch beiwohnen, wenn der Inhaber der zu durchsuchenden Räume über sein Hausrecht ihnen dieses gestattet.[50] Bei der Durchsuchung bei Dienstanbietern oder Unternehmen stellen insofern die Personen in leitender Stellung, wie z. B. Geschäftsführer, örtlicher Betriebsleiter, Vorstand, den Inhaber

---

[44] *Ciolek-Krepold*, Rn. 125; *Park*, § 2 Rn. 167; *Wohlers/Jäger*, SK-StPO, § 106 Rn. 4. Vgl. bei mehreren Inhabern ist jeder anwesenheitsberechtigt (M-G/*Schmitt*, StPO, § 106 Rn. 2; *Park*, a. a. O.; *Wohlers/Jäger*, a. a. O. Rn. 5).

[45] *Wohlers/Jäger*, SK-StPO, § 106 Rn. 18; vgl. zur Differenzierung der Rechtsgrundlagen a. a. O. Rn. 19.

[46] M-G/*Schmitt*, StPO, § 106 Rn. 2; *Wohlers/Jäger*, SK-StPO, § 106 Rn. 9. Weder der Strafgefangene noch der Untersuchungsgefangene ist Inhaber seines Haftraumes, daher kann er nicht beanspruchen, bei der Durchsuchung des Haftraumes anwesend zu sein, und weiter auch sein Verteidiger nicht (*OLG Stuttgart*, NStZ 1984, 574; *Bruns*, KK-StPO, § 106 Rn. 1; M-G/*Schmitt*, StPO, § 106 Rn. 3; *Park*, § 2 Rn. 167; *Wohlers/Jäger*, SK-StPO, § 106 Rn. 6).

[47] M-G/*Schmitt*, StPO, § 106 Rn. 2. Nach h. M. hat der Verteidiger grundsätzlich kein eigenes strafprozessuales Anwesenheitsrecht bei einer Durchsuchung (M-G/*Schmitt*, a. a. O. Rn. 3; *Park*, § 2 Rn. 196 f.; *Wohlers/Jäger*, SK-StPO, § 106 Rn. 10), er kann jedoch bei der Durchsuchung nach § 102 StPO meistens aufgrund des Hausrechts des Beschuldigten einen Zugang zu den durchsuchten Räumlichkeiten haben (*Park*, § 2 Rn. 196; *Wohlers/Jäger*, a. a. O.).

[48] *Park*, § 2 Rn. 196; *Wohlers/Jäger*, SK-StPO, § 106 Rn. 10.

[49] *Bruns*, KK-StPO, § 106 Rn. 3; M-G/*Schmitt*, StPO, § 106 Rn. 3; *Park*, § 2 Rn. 169; *Wohlers/Jäger*, SK-StPO, § 106 Rn. 11.

[50] *Park*, § 2 Rn. 169 und 196 f.; *Wohlers/Jäger*, SK-StPO, § 106 Rn. 11; auch *Peters*, NZWiSt 2017, 465, 472 am Anfang.

i. S. d. S. 1 dar, nicht den Vertreter i. S. d. S. 2.[51] Andererseits ist der Durchsuchungsbeamte nicht verpflichtet, vor oder zu Beginn der Durchsuchung auf Erscheinen des Inhabers – egal, ob er der Beschuldigte ist oder nicht – zu warten oder ihn herbeiholen zu lassen.[52] Wenn dadurch keine erhebliche Verzögerung eintritt, sollte er das aber tun.[53] Allerdings braucht dabei eine Bitte des von der Durchsuchung Betroffenen (insb. des Beschuldigten) um seine Anwesenheit deswegen nicht unbedingt aktiv berücksichtigt zu werden, weil die Nichtbeachtung des Anwesenheitsrechts nach S. 1 durch die Zuziehung Dritter des S. 2 ergänzt werden kann.

Bei Abwesenheit des Inhabers ist, wenn möglich, nach S. 2 ein Vertreter etc.[54] in der gesetzlichen Reihenfolge hinzuzuziehen.[55] Zum Vertreter gehört ein vertretungsberechtigter Hausverwalter oder ein bevollmächtigter Anwalt, wie etwa der Verteidiger des Beschuldigten oder der Rechtsbeistand des nichtverdächtigen Betroffenen.[56] Auch hier besteht für den Durchsuchungsbeamten keine Verpflichtung, bis zum Eintreffen des Verteidigers oder des Rechtsbeistands zu warten.[57] Dabei ist aber der Begriff „wenn möglich" des § 106 Abs. 1 S. 2 StPO – wie bei § 105 Abs. 2 StPO – ein objektiv überprüfbarer Rechtsbegriff. Auch hier hat der Durchsuchungsbeamte dem Vertreter etc., insb. dem Verteidiger des Beschuldigten, die Möglichkeit zur Beiwohnung einzuräumen, soweit dadurch der Untersuchungszweck nicht gefährdet werden könnte; z. B. wenn keine Verdunkelungsgefahren bestehen und ein baldiges Erscheinen des Verteidigers angekündigt wird.[58] Diese Hinzuziehung des Vertreters etc. soll die Interessen des Inhabers i. S. d. S. 1 vertreten, daher entfällt die Verpflichtung zur Zuziehung nach Abs. 2, wenn der Inhaber auf sein Anwesenheitsrecht verzichtet hat.[59]

Problematisch ist nun i. R. d. Auslegung und Anwendung des § 106 Abs. 1 StPO vor allem ein Anwesenheitsrecht des von der Durchsuchung Betroffenen und seines Verteidigers bei der Durchsicht von Daten in behördlichen Räumen gemäß § 110 StPO. Dabei handelt es sich auch um die Erhaltung der Offenheit der Durchsuchung nach §§ 102, 103 StPO (vgl. unten IV. 2.).

---

[51] *Ciolek-Krepold*, Rn. 125; *Wohlers/Jäger*, SK-StPO, § 106 Rn. 4.

[52] *Bruns*, KK-StPO, § 106 Rn. 1; M-G/*Schmitt*, StPO, § 106 Rn. 2; *Park*, § 2 Rn. 168.

[53] M-G/*Schmitt*, StPO, § 106 Rn. 2. Dabei beginnt die Durchsuchung wegen der verspäteten Anwesenheit nicht von vornherein (a. a. O.).

[54] Sie sind auch eine Art von Durchsuchungszeugen (*Bruns*, KK-StPO, § 106 Rn. 2).

[55] *Bruns*, KK-StPO, § 106 Rn. 2; M-G/*Schmitt*, StPO, § 106 Rn. 4; *Wohlers/Jäger*, SK-StPO, § 106 Rn. 13. Wegen des Unterschieds der Funktion kann diese Zuziehung nicht durch die von Durchsuchungszeugen nach § 105 Abs. 2 StPO ersetzt werden (*Wohlers/Jäger*, a. a. O.).

[56] *Park*, § 2 Rn. 160; dazu *Bruns*, KK-StPO, § 106 Rn. 2; M-G/*Schmitt*, StPO, § 106 Rn. 4; *Wohlers/Jäger*, SK-StPO, § 106 Rn. 15.

[57] *Park*, § 2 Rn. 160 und 198; dazu *Wohlers/Jäger*, SK-StPO, § 106 Rn. 10.

[58] *Park*, § 2 Rn. 198. In der Praxis hängt die Gewährung der Möglichkeit häufig von der Deliktsart ab und sie wirkt sich häufig positiv auf das Klima zwischen allen Beteiligten aus (a. a. O.).

[59] *Park*, § 2 Rn. 168; *Wohlers/Jäger*, SK-StPO, § 106 Rn. 13.

(3) § 106 Abs. 2 StPO sieht vor, dass bei der Durchsuchung nach § 103 Abs. 1 StPO der Zweck der Durchsuchung dem Inhaber oder der in dessen Abwesenheit zugezogenen Person nach § 106 Abs. 1 StPO „vor" deren Beginn bekanntzumachen ist, soweit sie nicht unter den Voraussetzungen des § 103 Abs. 2 oder § 104 Abs. 2 StPO stattfindet. Dann sieht § 107 S. 1 StPO vor, dass der Grund der Durchsuchung dem von der Durchsuchung Betroffenen „nach" deren Beendigung auf Verlangen schriftlich mitzuteilen ist. Die Inhalte des Wortlauts in beiden Vorschriften würden jedoch den vom *BVerfG* aufgestellten Anforderungen nicht gerecht werden. Sie sind daher insb. im Hinblick auf die Messbarkeit und Kontrollierbarkeit des Grundrechtseingriffs durch den Betroffenen und das Gericht verfassungskonform auszulegen.[60]

Der § 106 Abs. 2 S. 1 StPO gilt zuerst nicht nur für die Durchsuchung des § 103 Abs. 1 StPO, sondern auch für solche des § 102 StPO, es sei denn, dass die Bekanntgabe den Durchsuchungszweck gefährden würde.[61] Außerdem ist der § 107 S. 1 StPO dahingehend auszulegen, dass er nur für Ausnahmefälle gilt, in denen der Betroffene wegen der Gefährdung des Untersuchungszwecks vor Beginn der Durchsuchung über deren „Zweck", aber über deren „Gründe" nicht vollständig oder nur teilweise informiert wird.[62] Nach §§ 34, 35 Abs. 2, 36 Abs. 2 S. 1 StPO ist ein richterlicher schriftlicher Durchsuchungsbeschluss zwar grundsätzlich über die StA – zumindest kurz vor deren Beginn[63] – durch die Aushändigung einer in den Gründen vollständigen Ausfertigung oder zumindest deren Kopie[64] dem anwesenden, von der Durchsuchung Betroffenen vorzuzeigen oder bekannt zu machen, jedoch kann die Bekanntmachung der Gründe ausnahmsweise dann zurückgestellt werden, wenn durch sie der Untersuchungszweck gefährdet wäre.[65] Außer in solchem Ausnahmefall ist es verfassungsrechtlich bedenklich, dass nur eine Durchsuchungsanordnung, nämlich die Beschlussformel des Ermittlungsrichters ohne

[60] *Park*, § 2 Rn. 164 und 170; *Wohlers/Jäger*, SK-StPO, § 106 Rn. 25. Andererseits sind die Vorschriften insb. in nichtrichterlichen Durchsuchungsanordnungen von Bedeutung, weil der richterliche Durchsuchungsbeschluss bereits aufgrund der § 35 f. StPO bekanntgemacht wird (*Park*, § 2 Rn. 210).

[61] *Bruns*, KK-StPO, § 106 Rn. 4; M-G/*Schmitt*, StPO, § 106 Rn. 5; *Park*, § 2 Rn. 164 und 170; *Wohlers/Jäger*, SK-StPO, § 106 Rn. 25.

[62] *Bruns*, KK-StPO, § 107 Rn. 3: Trotz des Gesetzeswortlauts („nach deren Beendigung") sollte der Betroffene möglichst schon zu Beginn der Durchsuchung, wenigstens mündlich, über den Grund der Durchsuchung informiert werden.

[63] *Park*, § 2 Rn. 164.

[64] *Wohlers/Jäger*, SK-StPO, § 106 Rn. 26; *Park*, § 2 Rn. 211 und 164: Sie ist dem Betroffenen bei der Durchsuchung auszuhändigen und dies ist ggf. auch mit einer Kopie oder in Form eines Telefax möglich.

[65] *BGH* NStZ 2003, 273, 274 [Tz. 4.]; *Wohlers/Jäger*, SK-StPO, § 107 Rn. 6; *Bruns*, KK-StPO, § 107 Rn. 3: Auch in diesem Fall ist der Durchsuchungszweck und die rechtliche Einordnung der Tat anzugeben; auch *Park*, § 2 Rn. 211; a. A. M-G/*Schmitt*, StPO, § 107 Rn. 2: Bei der (schriftlichen) Durchsuchungsbescheinigung i. S. d. S. 1 genügt seine abstrakte Angabe (etwa Ergreifung oder Auffinden von Beweisgegenständen) „unabhängig davon, dass der Untersuchungszweck gefährdet wäre".

Gründe, dem Betroffenen ausgehändigt wird. Weil die eingehenden Gründe der Durchsuchung sobald wie möglich mitzuteilen sind, wenn die Gefährdung beseitigt wird, ist diese Mitteilung nach Beendigung der Durchsuchung möglichst unverzüglich an Ort und Stelle zu machen.[66] Dadurch können unnötige Rechtsmittel nicht nur vermieden werden,[67] sondern auch die Rechtmäßigkeit des Grundrechtseingriffs und dessen Durchführung kann nachträglich messbar und kontrollierbar sein (vgl. unten C. II. 1. c)).[68] Andererseits sollte in den Fällen der Durchsuchung gemäß § 103 Abs. 1 StPO aus Verhältnismäßigkeitsgesichtspunkten dem von der Durchsuchung Betroffenen und insb. den unverdächtigen TK-Dienstanbietern oder Unternehmen, die Möglichkeit gewährt werden, sie durch die freiwillige Herausgabe der Gegenstände abzuwenden. Dafür ist ihnen zu Beginn der Durchsuchung mitzuteilen, aus welchem Grund nach welchen Gegenständen gesucht wird.[69]

(4) Die in Verwahrung oder in Beschlag genommenen Gegenstände sind genau zu verzeichnen und zur Verhütung von Verwechslungen durch amtliche Siegel oder in sonst geeigneter Weise kenntlich zu machen (§ 109 StPO). Das Sicherstellungsverzeichnis ist durch die Behörde, die die Durchsuchung durchgeführt hat, im Regelfall die StA (vgl. § 36 Abs. 2 StPO),[70] dem Betroffenen auf Verlangen auszuhändigen, falls aber nichts Verdächtiges gefunden wird, ist ihm eine Bescheinigung hierüber (sog. „Negativattest oder -bescheinigung") zu geben (§ 107 S. 2 StPO).[71] Die Vorschriften enthalten nicht, wann das Beschlagnahmeverzeichnis oder das Negativattest zu erstellen und zu erteilen ist, jedoch sind diese – wie die Mitteilung des Durchsuchungsbeschlusses nach § 107 S. 1 StPO – wenn möglich an Ort und Stelle anzufertigen und auszustellen.[72] Wenn dies jedoch unmöglich ist, insb. etwa bei der Sicherstellung einer großen Menge von Unterlagen in Aktenschränken oder Daten in Datenbeständen,[73] sollte es sofort nach der vorläufigen Sicherstellung und der Durchsicht nach § 110 StPO (vgl. unten C. III. 3.) erfolgen.[74]

---

[66] *Park*, § 2 Rn. 212; *Wohlers/Jäger*, SK-StPO, § 106 Rn. 26 und § 107 Rn. 5 und 6 a. E.

[67] *Park*, § 2 Rn. 211; *Wohlers/Jäger*, SK-StPO, § 107 Rn. 6; dazu *BGH* NStZ 2003, 273, 274 [Tz. 4.].

[68] Kann der von der Durchsuchung Betroffene keine schriftliche Mitteilung verlangen, etwa weil weder er noch sein Vertreter etc. anwesend war oder er gar keine Kenntnis erlangt hat, so sind ihm die erforderlichen Mitteilungen von Amts wegen zu machen, um die Möglichkeit effektiven Rechtsschutzes zu gewährleisten (*Park*, § 2 Rn. 215; *Wohlers/Jäger*, SK-StPO, § 106 Rn. 25 und § 107 Rn. 3).

[69] *Park*, § 2 Rn. 163.

[70] *Bruns*, KK-StPO, § 107 Rn. 4.

[71] In der Praxis werden vorgefertigte Verzeichnisse (Vordrucke), die mit laufender Nummer, Kurzbeschreibung der Gegenstände etc. von Hand ausgefüllt werden können; sie sind aber nicht bundeseinheitlich vorgegeben (vgl. *Kemper*, wistra 3/2008, 96 [Fn. 9]).

[72] *OLG* Stuttgart StV 1993, 235; *Bruns*, KK-StPO, § 107 Rn. 4; *Wohlers/Jäger*, SK-StPO, § 107 Rn. 8.

[73] *Kemper*, wistra 3/2008, 96. 97 f.: sog. „Großverfahren". Bei diesen Verfahren neigen die Ermittlungsbeamten dazu, lieber zu viel als zu wenig Unterlagen mitzunehmen, aber dies ist aus deren Sicht verständlich (a. a. O. [Fn. 29]).

Bei Anfertigung des Beschlagnahmeverzeichnisses ist am wichtigsten, die Gegenstände in geeigneter Weise kenntlich zu machen, nämlich eine eindeutige Identifizierbarkeit bzw. Unterscheidbarkeit der Gegenstände.[75] Beweismittel sind grundsätzlich vor Ort in der vorgefundenen Form zu beschlagnahmen und so, wie sie sind, zu verzeichnen. Allerdings berücksichtigen die Vorschriften ursprünglich eine geringe Anzahl von zu beschlagnahmenden Tatwaffen wie etwa Messer, aber sie gelten heute im Allgemeinen auch für umfangreiche Unterlagen und Daten (vgl. Originalunterlagen oder Kopien) in Wirtschafts- und Steuerstrafverfahren.[76] Denn ein detailliertes Verzeichnis trägt zu der Verfahrensbeschleunigung und dem Grundrechtsschutz bei, indem es allen Verfahrensbeteiligten, nämlich sowohl dem Beschuldigten und seinem Verteidiger als auch den Ermittlungsbehörden und dem Gericht, erleichtert, verfahrensrelevante Beweise zu erkennen.[77] Dabei können die Papiere auch auf eine Weise kenntlich gemacht werden, indem die Beschriftung des Ordners mit einer „Sammelbezeichnung" angegeben wird (z. B. ordnerweise), sofern alles dadurch identifizierbar ist.[78] Dabei sollten wichtige Beweisgegenstände wie Notariatsurkunden, Verträge etc. jedoch einzeln aufgeführt werden, damit sie leicht im Verzeichnis gefunden werden können.[79] Im Beschlagnahmeverzeichnis sind zudem zur Kenntlichmachung der Auffindungsort und die Beamten, die an der Durchsuchung teilgenommen haben – auch das Aktenzeichen des Verfahren und eine

[74] Vgl. *BGH* NStZ 2003, 670; *Bruns*, KK-StPO, § 107 Rn. 4 f.; abw. *Wohlers*/*Jäger*, SK-StPO, § 107 Rn. 8, so schnell wie möglich; vgl. *Kemper*, wistra 3/2008, 96, 97 und [Fn. 18]: Dabei können aus rechtsstaatlichen Gründen keine zu langen Fristen gelten und der Zeitraum lässt sich wohl an dem zivilrechtlichen Begriff „ohne schuldhaftes Zögern" festmachen. Nach h. M. gilt § 107 S. 2 StPO für vorläufige Beschlagnahme nach § 108 StPO und vorläufige Sicherstellung zum Zweck der Durchsicht nach § 110 StPO entsprechend (M-G/*Schmitt*, StPO, § 107 Rn. 3; *Graulich*, wistra 8/2009, 209, 302; auch *Wohlers*/*Jäger*, a. a. O.). Denn auch bei diesen Fällen kann der Betroffene durch entsprechende Anwendung des § 98 Abs. 2 S. 2 StPO jederzeit die richterliche Entscheidung beantragen (*Graulich*, a. a. O.).

[75] *Bruns*, KK-StPO, § 107 Rn. 4; *Kemper*, wistra 3/2008, 96, 96 f.; M-G/*Schmitt*, StPO, § 107 Rn. 3; *Park*, § 2 Rn. 213; *Wohlers*/*Jäger*, SK-StPO, § 107 Rn. 7 und § 109 Rn. 2.

[76] *Kemper*, wistra 3/2008, 96; auch *Bruns*, KK-StPO, § 107 Rn. 4.

[77] *Kemper*, wistra 3/2008, 96, 97 und 99. Außerdem sollte dies rechtsstaatlich begrüßt werden und ist auch ein Merkmal professioneller Ermittlungsarbeit (*Kemper*, a. a. O. 99). Vor diesem Hintergrund sollte in dieses Verzeichnis eine Belehrung über Antragsrecht nach § 98 Abs. 2 S. 2 StPO aufgenommen werden (M-G/*Schmitt*, StPO, § 98 Rn. 11; *Wohlers*/*Jäger*, SK-StPO, § 109 Rn. 2).

[78] *Ciolek-Krepold*, Rn. 156; *Kemper*, wistra 3/2008, 96, 98; *Park*, § 2 Rn. 213; *Wohlers*/*Jäger*, SK-StPO, § 107 Rn. 7 und § 109 Rn. 2. So sind die Angaben wie z. B. „ein Ordner mit Schriftverkehr/Ausgangsrechnungen vom 1. Januar 2006 bis 30. September 2006" gestattet, hingegen sind Bezeichnungen wie z. B. „ein Regal mit diversen Ordnern", „3 Ordner mit Schriftwechsel" oder „ein Karton mit Schriftverkehr" nicht erlaubt (*Park*, a. a. O.; *Wohlers*/*Jäger*, a. a. O.). Sofern die Verwendung dieser Bezeichnungen unmöglich und unzumutbar ist, kann aber eine Bezeichnung wie z. B. „eine Kiste lose Unterlagen" zulässig sein (*Kemper*, a. a. O.).

[79] *Kemper*, wistra 3/2008, 96, 97.

laufende Nummer[80] – aufzuführen.[81] Bei der Suche nach Gebäuden mit mehreren Räumen oder der Suche nach Räumen, die von verschiedenen Personen genutzt werden, ist eindeutig festzustellen, aus welchem Raum ein Beweismittel stammt und welcher Person es zugeordnet wird; etwa durch die Anfertigung eines separaten Verzeichnisses für jeden Raum oder durch die Sortierung nach Räumen in das Gesamtverzeichnis.[82] Dies kann bei Überprüfung der Rechtsmäßigkeit der Art und Weise der Durchführung der Maßnahme teilweise zum Nachweis für die Umstände des Durchsuchungsverfahrens beitragen.[83]

Vor allem bei Beschlagnahme der EDV-A selbst oder des ganzen oder eines größeren Teils der darauf gespeicherten Daten genügt es, dass die gesicherten Daten mit einer Sammelbezeichnung kenntlich gemacht werden.[84] Insofern sollte aus dem Verzeichnis zudem nicht nur die wesentliche Struktur der gesicherten Daten oder Dateien erkennbar sein, sondern auch, ob sie nach § 110 Abs. 3 StPO von räumlich getrennten Speichermedien oder von lokalen Rechnern erfasst wurden und ob der gesamte Datenbestand oder nur einzelne Dateien gesichert wurden.[85] Wurden die Dateien nur teilweise gesichert, kann die Bezeichnung des Directorys oder des Ordners entsprechend gekennzeichnet werden.

(5) *Verfahrensverstöße und ihre Rechtsfolge:* Nach h. M. in der Literatur und der Entscheidung des *BGH* aus dem Jahr 2007 sind §§ 105 Abs. 2, 106 Abs. 1 – 2, 107 S. 1 StPO als wesentliche Förmlichkeiten, die dem Grundrechtsschutz der von einer Durchsuchung Betroffenen dienen, zwingendes Recht und keine bloße Ordnungsvorschrift, die zur beliebigen Disposition der Ermittlungsrichter und der Ermittlungsorgane stehen, daher hängt die Rechtmäßigkeit der Durchsuchung von ihrer Beachtung ab.[86] Als Konsequenz hieraus hat bei einem Verstoß gegen diese Vor-

[80] *Kemper*, wistra 3/2008, 96, 97.

[81] *Ciolek-Krepold*, Rn. 154 und 156; *Park*, § 2 Rn. 213 f.; *Wohlers/Jäger*, SK-StPO, § 109 Rn. 2.

[82] Vgl. *Kemper*, wistra 3/2008, 96, 98.

[83] Freilich kommt dem Verzeichnis keine Beweiskraft für und gegen jedermann zu (*Bruns*, KK-StPO, § 109 Rn. 2; *Wohlers/Jäger*, SK-StPO, § 109 Rn. 1).

[84] *Kemper*, wistra 3/2008, 96, 99. Obwohl Tausende oder Zehntausende Dateien zu verzeichnen sind, kann eine solche Liste nicht schlicht überblickt werden und alle Bezeichnungen können auch nicht einfach verstanden werden (a. a. O.).

[85] Vgl. *Kemper*, wistra 3/2008, 96, 99.

[86] *BGHSt* 51, 211, 213 ff. [Rn. 6 – 8]; *Bruns*, KK-StPO, § 105 Rn. 14; M-G/*Schmitt*, StPO, § 105 Rn. 10, § 106 Rn. 1 und § 107 Rn. 1; *Park*, § 2 Rn. 171 und 176; *Wohlers/Jäger*, SK-StPO, § 105 Rn. 58 und § 106 Rn. 27; *Zimmermann*, JA 5/2014, 321, 323; a. A. *Hofmann*, NStZ 2005, 121, 124. Dem Richter ist es verboten, zur verdeckten Durchsuchung die Anordnung nach § 102 StPO zu erlassen, den Ermittlungsbehörden ist es untersagt, eine richterliche Durchsuchungsanordnung nach § 102 StPO bewusst heimlich durchzuführen (*BGHSt* a. a. O. [Rn. 9]; *Hamm*, NJW 2007, 930, 932). Durch diese Entscheidung des *BGH* kann seine frühere Rechtsprechung, wobei er ausgeführt hat, dass eine Beeinträchtigung des Anwesenheitsrechts nach § 106 Abs. 1 S. 1 StPO bei der Durchsuchung nichts an der Rechtmäßigkeit der Durchsuchung als solcher geändert hätte (NStZ 1983, 375, 376), nicht mehr aufrechterhalten werden. § 109 StPO ist hingegen eine reine Ordnungsvorschrift, deswegen hat ihre Verletzung nicht nur

schriften der Betroffene das Recht zur Notwehr gemäß § 32 StGB und zum Widerstand gemäß § 113 StGB.[87] Jedoch lässt der *BGH* die Frage offen, ob die Missachtung der Vorschriften – über die Unrechtmäßigkeit hinaus – ein Verwertungsverbot der gewonnenen Erkenntnisse zur Folge hat.[88] Insofern zitierte er die Entscheidung des *BVerfG* nur als Referenz,[89] nach der ein Beweisverwertungsverbot zumindest „bei schwerwiegenden, bewussten oder willkürlichen Verfahrensverstößen" als Folge einer fehlerhaften Durchsuchung und Beschlagnahme geboten ist.[90] Die h. M. im Schrifttum ist auch nicht anders.[91] Daher ist die Wirksamkeit der zwingenden Vorschriften auf diese Grenze beschränkt.[92]

Es ist jedoch zweifelhaft, ob diese Ansicht überzeugend ist. Insbesondere die Verstöße gegen §§ 106 und 107 S. 1 StPO müssen strenger behandelt werden als in der allgemeinen Stellungnahme des *BVerfG* zum Verwertungsverbot. Denn das Verfahren nach den Vorschriften ist heute u. a. bei der umfassenden Datenerfassung ein wichtiges Mittel, um den Persönlichkeitsschutz des Betroffenen zu gewährleisten, d. h., um zu verhindern, dass er zu bloßem Objekt des Verfahrens wird. Daher ist es schwer, der Ansicht zuzustimmen, dass ein Verstoß gegen diese Vorschriften „keinesfalls" ein Verwertungsverbot nach sich ziehen soll.[93] Dazu hat u. a. die „Einhaltung des § 106 StPO" ganz eng mit der Sicherung der „Offenheit" der Durchsuchung gemäß §§ 102, 103 StPO zu tun.

cc) Rechtssystematischer Vergleich zu §§ 99 ff. StPO

Dass §§ 94 ff., 102 ff. StPO nur die offene Durchsuchung und Beschlagnahme rechtfertigen, lässt sich auch durch den Vergleich zwischen den Eingriffsvoraussetzungen und Verfahrensgarantien der Vorschriften und denjenigen der §§ 100a ff. StPO erklären. Die Durchsuchung nach §§ 102 ff. StPO ist deswegen mit geringeren

---

auf die Rechtswirksamkeit einer Beschlagnahme keinen Einfluss, sondern begründet auch kein Verwertungsverbot (*Bruns*, KK-StPO, § 109 Rn. 1; *Kemper*, wistra 3/2008, 96, 97; M-G/*Schmitt*, StPO, § 109 Rn. 2; *Wohlers/Jäger*, SK-StPO, § 109 Rn. 4).

[87] M-G/*Schmitt*, StPO, § 105 Rn. 11; *Park*, § 2 Rn. 176; *Wohlers/Jäger*, SK-StPO, § 105 Rn. 58.

[88] *Park*, § 2 Rn. 171.

[89] Vgl. *BVerfGE* 113, 29, 61 [Rn. 135].

[90] Vgl. *BGHSt* 51, 211, 214 [Rn. 8].

[91] *Amelung*, NJW 1991, 2533, 2538 [Tz. 4.]; *Bruns*, KK-StPO, § 105 Rn. 21, § 106 Rn. 6 und § 107 Rn. 5; M-G/*Schmitt*, StPO, § 105 Rn. 11 und 18 f.; vgl. *Park*, § 2 Rn. 415–419; *Wohlers/Jäger*, SK-StPO, § 105 Rn. 80, § 106 Rn. 28 und § 107 Rn. 10; *Roxin/Schünemann*, § 35 Rn. 9: keinesfalls Verwertungsverbot; a. A. *Krekeler*, NStZ 1993, 263, 268: „*Werden aber Regelungen verletzt, …, muß eine solche Verletzung die Unverwertbarkeit der rechtswidrig erlangten Beweismittel zur Folge haben.*"

[92] Vgl. *Park*, § 2 Rn. 171. Insoweit ändert sich nichts an der alten Stellungnahme des *BGH*, § 106 Abs. 1 StPO als Ordnungsvorschrift einzuordnen (siehe Fn. 86).

[93] *Roxin/Schünemann*, § 35 Rn. 9; *Wohlers/Jäger*, SK-StPO, § 105 Rn. 80, § 106 Rn. 28 und § 107 Rn. 10.

Eingriffsschwellen und Verfahrenskontrollen verbunden als die Maßnahmen nach §§ 100a ff. StPO, weil sie offen durchgeführt wird (vgl. §§ 105 ff. StPO). Diesbezüglich hat der *BGH* in seiner Entscheidung vom 2007 zutreffend ausgeführt:

> „Auch systematische Erwägungen sprechen dafür, die Durchsuchung i. S. d. § 102 StPO nur als eine offen auszuführende Maßnahme zu erlauben. Die besonders grundrechtsintensiven Ermittlungsmaßnahmen mit technischen Mitteln (wie etwa die Überwachung der TK, die Wohnraumüberwachung und der Einsatz technischer Mittel), die ohne Wissen des Betroffenen erfolgen können, sind in §§ 100a bis 100i StPO geregelt. Für sie bestehen gerade auch wegen ihrer Heimlichkeit hohe formelle (vgl. § 100b Abs. 2, Abs. 6 S. 2, § 100c Abs. 5 S. 4, § 100d Abs. 1 – 4 StPO) und materielle Anforderungen an die Anordnung und die Durchführung. … Vergleichbar hohe Eingriffsschranken für die Anordnung einer Durchsuchung beim Verdächtigen gem. § 102 StPO bestehen nicht.“[94]

3. Zwischenfazit

Aus der Auslegung der §§ 102 ff. StPO und dem rechtssystematischen Vergleich mit §§ 100a ff. StPO geht hervor, dass heimliche (Zwangs)Maßnahmen aufgrund der allgemeinen Vorschriften nicht zulässig sind. *Sieber* hat richtigerweise darauf verwiesen, dass das offene Vorgehen gegenüber dem Betroffenen, nämlich die Offenheit, ein Wesensmerkmal der Beschlagnahme und Durchsuchung nach §§ 94 ff., 102 ff. StPO sein muss und im Bereich der – heimliche Maßnahmen erleichternden – Informationstechnik ein klares Abgrenzungskriterium zu §§ 100a ff. StPO bilden: Bedarf an Abgrenzung zwischen § 100a und §§ 94, 99 StPO durch den Gesetzestext.[95]

III. Rechtfertigen §§ 94 ff., 102 ff. StPO eine offene Sicherstellung der „beim Server des ISP gespeicherten“ Daten?

1. Vorrede

Es ist unzweifelhaft, dass es möglich und zulässig ist, aufgrund der allgemeinen Vorschriften der Beschlagnahme und Durchsuchung auf private informationstechnische Systeme und darauf gespeicherte Daten offen zuzugreifen.[96] Heutzutage sind alle Arten von Daten jedoch zumeist auch bei TK-Dienstanbietern oder Unterneh-

[94] *BGHSt* 51, 211, 215 f. [Rn. 11 – 13].

[95] *Sieber*, 69. DJT 2012, C 111 f., insb. [Tz. (a)]: „*der Gesetzgeber sollte in § 94 StPO klarstellen, dass die Vorschriften der Beschlagnahme … nur einzelne und offene Sicherstellungen von Daten erlauben*“.

[96] BT-Drs. 18/12785, S. 54; *Brodowski*, JR 2009, 402, 411 [Tz. VII. 2. a)]; M-G/*Schmitt*, StPO, § 94 Rn. 16a; *Sieber*, 69. DJT 2012, C 112 [Tz. (c)]; *Singelnstein*, NStZ 2012, 593, 597 f., 602; *Wohlers*/*Greco*, SK-StPO, § 94 Rn. 24 ff.; *Zimmermann*, JA 5/2014, 321, 322 f. m. w. N. Erfolgt die Durchsuchung verdeckt, geht es um Online-Durchsuchung nach § 100b StPO (*Brodowski*, a. a. O.; *Sieber*, a. a. O.).

men umfassend gespeichert. Ein heimlicher Zugriff auf diese „außerhalb des Herrschaftsbereichs des Betroffenen" liegenden Daten wird durch §§ 100a ff. StPO oder künftige Gesetze gerechtfertigt (vgl. Kapitel 3, C.). Aber wenn ein solcher Zugriff „offen, also in Kenntnis des Betroffenen", gemacht wird, auf welcher Vorschrift kann er beruhen?[97] Nach h. M. in der Literatur werden die Daten im Herrschaftsbereich der Anbieter nach schutzfunktionaler Theorie (vgl. Kapitel 2, B. IV. 2.) durch Art. 10 Abs. 1 GG geschützt und ein Eingriff in den Schutzbereich – unabhängig von seiner Offenheit oder Heimlichkeit – ist nur aufgrund der §§ 100a und g StPO zulässig. Dagegen hat das *BVerfG* in der Entscheidung (2 BvR 902/06) vom 19. Juni 2009 erklärt, dass „offene" Eingriffe in das Fernmeldegeheimnis durch §§ 94 ff., 102 ff. StPO verfassungsrechtlich zu rechtfertigen sind.[98] Aber auch danach ist diese Frage immer noch umstritten. Das liegt daran, dass die Auffassung des Gerichts dem schematischen Denken zwischen Grundrechten und Ermächtigungen, das im Strafprozessrecht herkömmlich allgemein angenommen ist, widerspricht. Diese Debatte bezieht sich zum einen im Hinblick auf den Schutzbereich des Grundrechts auf die Frage, ob ein etwaiger Eingriff in Art. 10 Abs. 1 GG – nicht nur durch §§ 100a ff. StPO der Sondervorschriften, sondern – auch durch §§ 94 ff., 102 ff. StPO der allgemeinen Vorschriften gerechtfertigt werden kann, und zum anderen im Hinblick auf die Verhältnismäßigkeit (i. e. S.) auf die Frage, mit welchen Verfahrenssicherungen ein – besonders – schwerer Eingriff aufgrund der allgemeinen Vorschriften verbunden sein muss.

2. Bestimmung der Ermächtigung

a) Herkömmliche schematische Einstellung und eine Wende des Denkens durch das BVerfG

Bis vor der o. g. Entscheidung des *2. BVerfG-Senats* von 2009 war in Literatur und Rspr. die Meinung überwiegend, dass die Eingriffsnormen dem Schutzbereich der Grundrechte entsprechen sollen. Demnach sollten Eingriffe in das Fernmeldegeheimnis nach § 100a StPO, solche in das Brief- und Postgeheimnis nach § 99 StPO und solche in das allgemeine Persönlichkeitsrecht nach §§ 94 ff. StPO erfolgen.[99] Hiervon ausgehend ist der Beschluss des *BGH* (1 StR 76/09) logisch zu verstehen, der noch kurz vor der Entscheidung des *BVerfG* erging;[100] da er im Beschluss bezüglich der – heimlichen – Sicherstellung von beim Provider gespeicherten E-Mails einen

[97] Hierbei steht die Erweiterung der Maßnahme nach § 110 Abs. 3 StPO, der eine offene Durchsuchung „gegenüber dem Betroffenen" vor Ort voraussetzt, nicht infrage.

[98] *BVerfGE* 124, 43, 58 ff. [Rn. 52 ff.].

[99] Vgl. *BGHSt* 31, 304, 306; 34, 39, 50: „*Die §§ 100a ff. StPO regeln die materiellen und formellen Voraussetzungen des durch Art. 10 Abs. 2 S. 1 GG zugelassenen Eingriffs in das Fernmeldegeheimnis*"; *Brodowski*, JR 2009, 402, 406; *Roxin/Schünemann*, § 36 Rn. 6; *Wohlers/Greco*, SK-StPO, § 94 Rn. 27.

[100] *BGHSt* NJW 2009, 1828.

Eingriff in das Fernmeldegeheimnis verneint hat, kam § 100a StPO als Ermächtigungsgrundlage von vornherein nicht in Betracht, stattdessen galt § 99 StPO dafür – *faute de mieux* – „entsprechend".[101]

Der *2. Senat* hat jedoch die Verknüpfung des Schutzbereichs der betroffenen Grundrechte und der Ermächtigungsgrundlage ausdrücklich abgelehnt, indem er entschied, dass serverbasiert gespeicherte E-Mail-Nachrichten vom Art. 10 GG gewährleistet werden und eine offene Erhebung der Daten durch §§ 94, 98 StPO gerechtfertigt werden kann:[102]

> „§ 94 StPO kann ohne Verfassungsverstoß als Ermächtigung auch zu Eingriffen in Art. 10 Abs. 1 GG verstanden werden. Aus der systematischen Stellung von § 94 StPO und § 99, § 100a und § 100g StPO ist nicht der Schluss auf ein gesetzgeberisches Regelungskonzept zu ziehen, wonach nur aufgrund von § 99, § 100a und § 100g StPO in Art. 10 GG eingegriffen werden könnte. … im 8. Abschnitt des Ersten Buches der Strafprozessordnung … Diese Aneinanderreihung unterschiedlicher Maßnahmen legt nicht den Schluss nahe, der Gesetzgeber habe Eingriffe in Art. 10 GG nur aufgrund von § 99, § 100a und § 100g StPO zulassen wollen. Auch die Gesetzesmaterialien enthalten keinen hinreichenden Anhaltspunkt dafür … Nach Wortlaut, Systematik und Zweck handelt es sich bei den §§ 94 ff. StPO um Vorschriften über unterschiedliche strafprozessuale Maßnahmen, deren Anwendungsbereich nicht durchgehend jeweils in spezifischer Weise auf die Reichweite spezieller Grundrechte abgestimmt sind."[103]

Während die Rechtsgrundlage für die Eingriffe in der vorangegangenen schematischen Einstellung nach dem betroffenen Grundrecht bestimmt worden war, sieht das *BVerfG* insofern das maßgebliche Kriterium in der Differenzierung zwischen offenen und heimlichen Eingriffen.[104] Es ist daher der Ansicht, dass die besondere Eingriffsintensität der TKÜ und die hohen Schwellen der § 100a StPO in der Heimlichkeit des Eingriffs vorrangig begründet sind, nicht in einer einfachen Be-

---

[101] *Kasiske*, StraFo 6/2010, 228, 230.

[102] *BVerfGE* 124, 43, Tenor; vgl. *Brunst*, CR 2009, 584, 591; „einen eigenen Weg"; *Kasiske*, StraFo 6/2010, 228, 230: Die „Kehrtwendung" des *BVerfG*. Hier handelt es sich um E-Mails, die nach Beendigung des Übermittlungsvorgangs auf dem Mailserver des Providers gespeichert sind und die nicht heimlich, sondern offen (mit Kenntnis des Betroffenen) und punktuell und durch den Ermittlungszweck beschränkt erhoben wurden (vgl. a. a. O. 63 [Rn. 69] und 65 [Rn. 75]). Nach dem Sachverhalt der Entscheidung erfolgte die Beschaffung der beim Anbieter gespeicherten E-Mails von den Ermittlungspersonen mit Wissen des Betroffenen nach einer Wohnungsdurchsuchung und daher hat das *BVerfG* auch sein Urteil unter der Voraussetzung begründet, dass die Beschlagnahme und Durchsuchung offen durchgeführt wurde. Auch im Schrifttum wird festgestellt, dass die im Urteil behandelte Maßnahme eine „offene Beschlagnahme und Durchsuchung" darstellt (*Brodowski*, JR 10/2009, 402, 403; *Kasiske*, StraFo 6/2010 228, 229; *Roxin/Schünemann,* § 36 Rn. 6; *Wohlers/Greco*, SK-StPO, § 94 Rn. 27; *Zimmermann*, JA 5/2014, 321, 325 m. w. N.; abw. *Klesczewski*, ZStW 123 (2011), 737, 749: „*Schließlich vermag auch die Kennzeichnung der E-Mail-Beschlagnahme als offene Ermittlungsmaßnahme nicht zu überzeugen. … Das verkennt der E-Mail-Beschluss des 2. Senats.*").

[103] *BVerfGE* 124, 43, 58 f. [Rn. 57].

[104] *Kasiske*, StraFo 6/2010, 228, 231; *Singelnstein*, NStZ 2012, 593, 596.

troffenheit gemäß Art. 10 Abs. 1 GG[105] Dies wird auch durch den Vergleich mit seinen früheren Rspr. bestätigt, die in der Entscheidung zur Überprüfung der Verhältnismäßigkeit i. e. S. heranzogen werden: Die „offene Sicherstellung und Beschlagnahme von auf dem Mailserver gespeicherten E-Mails" ist weniger eingriffsintensiv im Vergleich zu „heimlichen Eingriffen in die laufenden Kommunikationsinhalte" (*BVerfGE* 100, 313, 394) und „heimlichen Zugriffen auf die vom Provider verdachtslos vorgehaltenen Verkehrsdaten" (*BVerfGE* 107, 299, 318 ff.; vgl. 125, 260, 318 ff.) und daher ist insofern die Maßnahme aufgrund der Bedeutung der Straftaten nicht zu beschränken und zu ihrer Anordnung genügt der Anfangsverdacht.[106] Kurzum hat das *BVerfG* klargestellt, dass die Bestimmung der Ermächtigungsnorm in erster Linie von Offenheit oder Heimlichkeit der Maßnahme abhängt.[107]

b) Kritik an der Entscheidung des BVerfG

Die Inhalte der obigen Entscheidung des *BVerfG* werden in Literatur vielfach kritisiert.[108] Der Kern der Kritiken trifft, dass der „Zugriff auf serverbasiert gespeicherte Telekommunikationsinhalte" i. d. R. eingriffsintensiver ist als eine – heimliche – TKÜ, er daher schlichtweg nicht auf den §§ 94 ff., 102 ff. StPO beruhen kann, auch wenn er offen erfolgt. Daneben wird dies auch damit begründet, dass in diesem Fall kein Unterschied zwischen offener oder verdeckter Maßnahme in der materiellen Wirkung des Eingriffs besteht,[109] und dass ein Persönlichkeitsprofil weitaus eher aus einem solchen umfangreichen Nachrichtenbestand erstellt werden kann, als aus einer nur wenige Stunden oder Tage andauernden Überwachung.[110]

---

[105] *Kasiske*, StraFo 6/2010, 228, 231; *Singelnstein*, NStZ 2012, 593, 596; dazu *Zimmermann*, JA 5/2014, 321, 325: „*Denn anstatt anhand der Art des betroffenen Grundrechts auf die ‚passende' Ermächtigungsgrundlage zu schließen, bestimmt das BVerfG vornehmlich die Eingriffsintensität zum Auswahlkriterium der ‚richtigen' Ermächtigungsgrundlage.*"

[106] *BVerfGE* 124, 43, 62 f. [Rn. 69].

[107] Vgl. *BVerfGE* 124, 43, 65 f. [Rn. 76]. Daraus geht auch hervor, dass die Heimlichkeit der Maßnahme entscheidender ist als die Art der zu erhebenden Daten. Der Zugriff auf Inhaltsdaten wird nämlich im Allgemeinen als schwerwiegender angesehen als solcher auf Verkehrsdaten.

[108] Vgl. *Brodowski*, JR 2009, 402, 406 f.; *Gercke*, GA 2012, 474, 486 f.; *Klesczewski*, ZStW 123 (2011), 737, 747; *Kudlich*, GA 2011, 193, 203; *Meinicke*, StV 2012, 462, 463; *Neuhöfer*, JR 2015, 21, 23 ff.; *Roxin/Schünemann,* § 36 Rn. 6; *Wohlers/Greco*, SK-StPO, § 94 Rn. 27; a. A. *Singelnstein*, NStZ 2012, 593, 596.

[109] *Neuhöfer*, JR 2015, 21, 25; dazu *Roxin/Schünemann*, § 36 Rn. 6: „*Es leuchtet auch nicht ein, dass für einen einheitlichen Kommunikationsvorgang unterschiedliche Eingriffsvoraussetzungen gelten sollen, je nachdem, in welcher Phase des Vorgangs der Eingriff erfolgt. Richtigerweise müssten immer §§ 100a, b einschlägig sein, unabhängig davon, ob der Zugriff offen oder verdeckt erfolgt*"; auch *Kasiske*, StraFo 6/2010, 228, 231 a. E.

[110] *Brodowski*, JR 2009, 402, 406; auch *Kudlich*, GA 2011, 193, 203 [Fn. 57]: der drohende Wertungswiderspruch. Es dürfte auch verständige Bürger überraschen, dass solche Zugriffe auf beim Anbieter lagernde Nachrichteninhalte durch die allgemeinen Vorschriften, die nicht mit spezifischen Schutzstandards versehen, erlaubt sind (*Brodowski*, a. a. O.).

Nach dieser Kritik bilden die §§ 94 ff., 102 ff. StPO u. a. in Hinsicht auf die Verhältnismäßigkeit i. e. S. keine ausreichende gesetzliche Grundlage für die offene Sicherstellung der beim Anbieter gespeicherten Daten und dafür sind Eingriffsvoraussetzungen und gesetzliche Vorkehrungen zur TKÜ erforderlich.[111] Vor allem argumentiert *Neuhöfer*, dass die Auffassung des *BVerfG* von 2009 im Widerspruch zu seiner früheren steht, und dass unter rechtssystematischem Gesichtspunkt, in teleologischer Erwägung und in verfassungskonformer Auslegung der bestehende schematische Ansatz über die Bestimmung der Ermächtigungsnormen vertretbar ist.[112] Diese Kritik ist aber nicht überzeugend und kann im Gegenteil kritisiert werden.

c) Gegenargumente

Zunächst hat das *BVerfG* in der Entscheidung vom 27. Juli 2005 (1 BvR 668/04) ausgelegt, dass §§ 100a, b, g, h und i StPO a. F. eine abschließende Regelung darstellen, bezüglich der TKÜ zu Zwecken der Strafverfolgung die konkurrierende Gesetzgebungskompetenz der Länder auszuschließen.[113] Daraus lässt sich jedoch zwangsläufig nicht folgern, dass §§ 94 ff. StPO keine Ermächtigungsgrundlage für den Eingriff in das Telekommunikationsgeheimnis sein können. Seit der Entscheidung des Gerichts vom 2. März 2006 (2 BvR 2099/04)[114] ist der Herrschaftsbereich i. R. d. Bestimmung des Schutzbereichs des Fernmeldegeheimnisses nach Art. 10 Abs. 1 GG von entscheidender Bedeutung (schutzfunktionale Theorie; vgl. Kapitel 2, B. IV. 2.) und angesichts der angemessenen Ausweitung dieses Schutzbereichs nach der Entwicklung der IT wäre die Kritik von *Neuhöfer*, dass der Beschluss des *Zweiten Senats* von 2009 dem Urteil des *Ersten Senats* von 2010 widerspricht,[115] ungültig.[116] Zum anderen wurde die Quellen-TKÜ im August 2017 in die StPO eindeutig eingeführt (vgl. § 100a Abs. 1 S. 2 – 3 StPO). Zwar ist sie eine Art der TKÜ

[111] Vgl. *Klesczewski*, ZStW 123 (2011), 737, 749 f. Insofern macht er geltend, dass zur Sicherstellung von E-Mail-Dateien die Eingriffsvoraussetzungen der §§ 100a, b StPO (a. F.) mit §§ 94 ff., 102 ff. StPO zu kombinieren sind. Dies steht aber dem Beschluss des *BGH* entgegen, dass es unzulässig ist, einzelne Elemente von Eingriffsermächtigungen zu kombinieren (*BGHSt* 51, 211, 219 [Rn. 22]).

[112] *Neuhöfer*, JR 2015, 21, 24 ff. Hierbei kann die teleologische Erwägung (a. a. O. 24 [Tz. bb)]) nicht länger aufrechterhalten werden, da sie die heutige Situation, in der TK-Daten umfassend hinterlassen werden, überhaupt nicht berücksichtigt.

[113] Vgl. *BVerfGE* 113, 348, 372 f. [Rn. 105 – 108]: „*Der Bundesgesetzgeber hat mit der Regelung der TKÜ in der Strafprozessordnung eine abschließende Regelung getroffen. … Der Bundesgesetzgeber hat die Überwachung der TK zu Zwecken der Strafverfolgung in den §§ 100a, 100b, 100g, 100h und 100i StPO nach Umfang, Zuständigkeit und Zweck sowie hinsichtlich der für die jeweilige Maßnahme erforderlichen Voraussetzungen umfassend geregelt. … Der Verzicht des Bundesgesetzgebers darauf, die TKÜ im Vorfeldbereich noch weiter auszudehnen, ist eine bewusste Entscheidung.*“

[114] *BVerfGE* 115, 166, 183 ff.

[115] Vgl. *Neuhöfer*, JR 2015, 21, 24 [Tz. aa) 1. Absatz].

[116] Auch *Brodowski*, JR 2009, 402, 407 [Tz. IV. 1.].

nach § 100a StPO, aber sie richtet sich an die nach Abschluss des Übertragungsvorgangs im Herrschaftsbereich des Empfängers gespeicherten Kommunikationsdaten, die aber nicht durch das Fernmeldegeheimnis, sondern durch das allgemeine Persönlichkeitsrecht geschützt werden. So rechtfertigt § 100a StPO mit der Neuregelung neben Eingriffen in Art. 10 Abs. 1 GG – ergänzend – auch Eingriffe in Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG.[117]

Außerdem kritisiert *Neuhöfer*, dass die Auffassung des *Zweiten Senats* auf Wertungswidersprüchen basiert, indem er unter rechtssystematischem Gesichtspunkt die strengen Eingriffsvoraussetzungen der §§ 100a, g StPO mit den einfachen der §§ 94 ff. StPO vergleicht.[118] Freilich ist sein Hinweis zutreffend, dass ein Zugriff auf den gesamten Datenbestand i. d. R. eingriffsintensiver ist als ein solcher auf Daten im laufenden Kommunikationsvorgang und ein Eingriff in Inhaltsdaten schwerwiegender ist als ein solcher in Verkehrsdaten. Die qualifizierten Eingriffsvoraussetzungen und Verfahrensgarantien der §§ 100a, g StPO folgen aber aus der Heimlichkeit der Maßnahme. Daher ist dieser Vergleich selbst unangemessen. Die problematischen Wertungswidersprüche sollten durch andere Garantien als die künstliche Analogie der §§ 100a, g StPO ausgeglichen werden. Dass die Ermittlungsbehörde aufgrund der §§ 94 ff. i. V. m. §§ 33, 35 StPO – mit Wissen des Betroffenen durch die Benachrichtigung – unmittelbar aus dem ISP die serverbasiert gespeicherten Daten erhalten können, steht vielmehr aus rechtssystematischer Sicht im Einklang damit, dass sie bei offenen Durchsuchungen nach allgemeinen Vorschriften aufgrund des § 110 Abs. 3 StPO auf solche Daten zugreifen kann.[119]

Daneben argumentiert *Neuhöfer*, dass die Auffassung des *Zweiten Senats* gegen eine verfassungskonforme Auslegung des Anwendungsbereichs der §§ 94 ff. StPO spricht: unter Hinweis auf die Prinzipien der Normenklarheit und -bestimmtheit, die Abwägung sowie die organisatorischen und verfahrensrechtlichen Sicherungen.[120] Der Kern der Kritik besteht darin: Da der Zugriff auf serverbasiert gespeicherte Nachrichteninhalte eines sozialen Netzwerks oder einer E-Mail mit Blick auf die Qualität und die Vielzahl der erlangten Informationen so hohe Eingriffsintensität hat, dass er weitreichende Rückschlüsse auf die Persönlichkeit und eine Bildung von Persönlichkeitsprofilen ermöglichen kann, sind die bestehenden §§ 94 ff. StPO angesichts der Verhältnismäßigkeit i. e. S. nicht mit hinreichenden bzw. adäquaten verfahrensrechtlichen Sicherungen versehen. Darauf, ob die Zugriffsmaßnahme für

[117] BT-Drs. 18/12785, S. 48 ff.: insb. Computer-Grundrecht; *Niedernhuber*, JA 3/2018, 169, 171; *Singelnstein/Derin*, NJW 2017, 2646, 2648.

[118] Vgl. *Neuhöfer*, JR 2015, 21, 24 [Tz. aa) 2. Absatz].

[119] *Kasiske*, StraFo 6/2010, 228, 233 a. E. Bei Durchsuchung beim Betroffenen kann die Ermittlungsbehörde nach § 110 Abs. 3 StPO unter gewissen Voraussetzungen über seine Speichermedien, die im Zug der Durchsuchung aufgefunden werden, auf Daten zugreifen, die sich außerhalb seines Herrschaftsbereichs befinden, d. h. die auf dem räumlich getrennten Server des Anbieters etwa zu E-Mail-Dienst, sozialen Netzwerken oder Cloud-Computing gespeichert sind (vgl. *Singelnstein*, NStZ 2012, 593, 598).

[120] Vgl. *Neuhöfer*, JR 2015, 21, 24–26 [Tz. cc)]; auch *Brodowski*, JR 2009, 402, 406 f.

den Betroffenen offen oder verdeckt erfolgt, kommt es insoweit nicht entscheidend an, da dies beim Zugriff auf außerhalb des Herrschaftsbereichs des Betroffenen liegende und dauerhaft gespeicherte Daten irrelevant ist. In jedem Fall kommt es zum umfassenden staatlichen Zugriff.

Dieser Kritik ist zwar zum Teil als gerechtfertigt zuzustimmen, jedoch zum Teil nicht. Eine Durchsuchung und Beschlagnahme, die einen vertiefenden Eingriff in persönlichen Bereich auslösen, sind zwar nach dem Grundsatz der Verhältnismäßigkeit zu beschränken, doch bei den in Rede stehenden Fällen ist es ausreichend, dass die Beschränkungen nicht gesetzgeberisch geregelt werden, sondern dass ihnen im Einzelfall in vielfältiger Weise Rechnung getragen wird. Denn unter den heutigen informationstechnischen Gegebenheiten soll die offene Erhebung bei Dienstanbietern gespeicherter Nachrichteninhalte im Hinblick auf wirksame Strafverfolgung in der Praxis auch unter den einfachen Voraussetzungen der allgemeinen Vorschriften möglich sein.[121] Es ist daher nicht erforderlich, eine solche Maßnahme auf begrenzte schwerwiegende Straftaten zu beschränken.[122] Obwohl sie umfangreiche und sensible Daten betrifft, ist es dabei ausreichend, dass die Beschränkung auf nur verfahrensrelevante Daten und den Ausschluss der dem Kernbereich privater Lebensgestaltung zuzuordnenden Daten beim Erlass des Beschlusses der Beschlagnahme und Durchsuchung und bei der Ausführung der Maßnahme im Einzelfall durch konkrete und abgestufte Vorkehrungen nach dem Verhältnismäßigkeitsgrundsatz sichergestellt wird.[123]

3. Zwischenfazit

Heute gehört in der Ermittlung der Zugriff auf bei TK-Dienstanbietern gespeicherte Daten zur Beweissicherung neben dem Zugriff auf Geräte und Speichermedien des Einzelnen zu den typischsten und gebräuchlichsten Arten. Er ist keine besondere Art der Maßnahme mehr. Wenn ein solcher Angriff offen statt heimlich durchgeführt wird, trotzdem bei anderen als schweren Straftaten nicht zulässig ist, so kann dies in kriminalistischer Hinsicht zu einem schwerwiegenden Ermittlungsfehler führen.[124] Wird der Polizei deren Eilkompetenz – wie in § 100e Abs. 1 StPO –

[121] Zust. *Dalby*, CR 2013, 361, 368 [Tz. aa)]; M-G/*Schmitt*, StPO, § 94 Rn. 16b.

[122] Vgl. *BVerfGE* 124, 43, 62–66 [Rn. 69–76]; dazu *Kasiske*, StraFo 6/2010, 228, 231 ff.

[123] Vgl. *BVerfGE* 124, 43, 66 ff.; *Singelnstein*, NStZ 2012, 593, 597: durch die strafprozessualen und verfassungsrechtlichen Grenzen; krit. *Brodowski*, JR 2009, 402, 406: „*(…) leidet die vom BVerfG als Korrektiv vorgesehene Einzelfallprüfung der Verhältnismäßigkeit unter deren Unvorhersehbarkeit – auch angesichts derer diffuser Kriterien – …*“

[124] *BVerfGE* 124, 43, 62–66 [Rn. 69–76, insb. 71 und 74]; vgl. auch für die im Herrschaftsbereich des Beschuldigten vorhandenen Daten *BVerfGE* 115, 166, 191 ff. [Rn. 96–103]; abw. *Kasiske*, StraFo 6/2010, 228, 231: „*So lässt sich ein kriminalpolitisches Bedürfnis für den Zugriff auf den E-Mail-Verkehr zwar kaum bestreiten, weil … die E-Mail-Nutzung daher in praktisch alle Lebensbereiche vorgedrungen ist. Doch dieser hohe Verbreitungsgrad rechtfertigt es nicht, den Zugriff bei allen Arten von Straftaten zu gestatten. Denn selbst für … Telefon hat der Gesetzgeber eine Beschränkung auf die Verfolgung schwerer Straftaten vorgesehen.*“

genommen und tritt eine staatsanwaltliche Eilanordnung außer Kraft, wenn sie nicht binnen drei Werktagen von dem Gericht bestätigt wird, so können wirksame Ermittlungstätigkeiten ebenfalls übermäßig eingeschränkt sein.[125] Zum anderen kann heutzutage die Durchsuchung und Beschlagnahme, selbst wenn diese offen durchgeführt wird, immer zu einem Zugang zu Daten führen, die so umfangreich sind, dass die Erstellung von Persönlichkeitsprofilen möglich ist. Dies unterscheidet nicht zwischen der direkten Erfassung von Daten des Betroffenen (vgl. §§ 94 und 102 StPO) und der indirekten Übermittlung durch den TK-Dienstanbieter (vgl. §§ 95 und 103 StPO). Aus diesem Grund werden verfahrensrechtliche Sicherungen dafür im Hinblick auf die Verhältnismäßigkeit zu Recht verlangt (vgl. eingehend unten C.).

C. Verfahrensrechtliche Kontrolle nach dem Verhältnismäßigkeitsgrundsatz

I. Bilden die §§ 94 ff., 102 ff. StPO eine ausreichende gesetzliche Grundlage für die „offene, aber umfassende Sicherstellung" der Daten?

1. Fragestellung

Die §§ 94 ff., 102 ff. StPO sind allgemeine Ermächtigungsnormen zur Beschlagnahme und Durchsuchung, so können die Ermittlungsbehörden damit auf verschiedene atypische Tatsachen reagieren. Die Vorschriften sehen – anders als §§ 99 ff. StPO – nur die Gegenstände und den Zweck der Durchsuchung und Beschlagnahme vor und enthalten keine Einschränkungen in Bezug auf Art, Umfang oder Dauer der Durchführung. Unter den heutigen technischen und sozialen Bedingungen kann aber auch eine einfache Beschlagnahme und Durchsuchung aufgrund dieser allgemeinen Vorschriften jederzeit zur umfangreichen Erfassung personenbezogener Daten und zu einem schwerwiegenden Eingriff in Persönlichkeitssphäre führen.[126] Diese Kritik muss beachtet werden. Denn derzeit ermöglichen solche Datenerfassungen intensive Eingriffe, die weit über das ursprünglich damit zu erreichende Maß, nämlich den Grundrechtseingriff mittlerer Qualität, hinausge-

---

Die Überwachung des Telefons nach § 100a StPO stellt aber eine heimliche Maßnahme des „laufenden Kommunikationsvorgangs" dar. Vergleichbar damit ist verdeckte Beschaffung beim Dienstanbieter „gespeicherter E-Mails" (vgl. Kapitel 3, C.).

[125] Dazu auch *Kasiske*, StraFo 6/2010, 228, 233.

[126] Vgl. *BVerfGE* 113, 29, 60 [Rn. 132]: „*Die Sicherstellung des (bei der Wohnungsdurchsuchung aufgefunden) Datenträgers ermöglicht grundsätzlich, alle darauf enthaltenen Informationen zur Kenntnis zu nehmen. Schon wegen des Umfangs der Informationen kann es in erheblichem Umfang zu Zufallsfunden i. S. d. § 108 StPO kommen.*"

hen.[127] Aus diesem Grund stellt sich eine Frage, ob die §§ 94 ff., 102 ff. StPO aus der Sicht des Verhältnismäßigkeitsgrundsatzes den verfassungsrechtlichen Anforderungen genügen, um solche erhöhte Eingriffsintensität zu rechtfertigen, wobei insb. umstritten ist, ob „zusätzliche verfahrensrechtliche Sicherungen" erforderlich sind.

2. Stellungnahme des *BVerfG*

Diesbezüglich hat das *BVerfG* in den späten 2000er-Jahren durch seine drei beachtenswerten Entscheidungen klargestellt, dass die §§ 94 ff., §§ 102 ff. StPO auch für den – offenen – Zugriff auf umfangreiche gespeicherte Datenbestände verhältnismäßig i. e. S. ausgestaltet sind. Nach seiner Rechtsprechung von 2005 (2 BvR 1027/02) sind zunächst bei Sicherstellung und Beschlagnahme der Datenträger und der darauf vorhandenen Daten aufgrund der §§ 94 ff. StPO keine über die Voraussetzungen dieser Vorschriften hinausgehenden speziellen Eingriffsbeschränkungen erforderlich.[128] Hier hat das Gericht ausgeführt, dass es ausreicht, dass einer besonderen Eingriffsintensität, die sich aus Vielfalt und Umfang erhobener Daten ergibt, nach dem Verhältnismäßigkeitsgrundsatz im jeweiligen Einzelfall in vielfältiger Weise Rechnung getragen wird, diesbezüglich schlug es nur ein abgestuftes Vorgehen, nämlich eine stufige Verfahrensweise, vor, um die überschießende Gewinnung für das Verfahren bedeutungsloser Informationen i. R. d. Vertretbaren zu vermeiden.[129] Bald darauf hat es im Jahr 2006 in der Verfassungsbeschwerde über die Rechtswidrigkeit der Beschlagnahme von PC und Mobiltelefons nach §§ 94 ff., 102 ff. StPO (2 BvR 2099/04)[130] und im Jahr 2009 in der Verfassungsbeschwerde über die Sicherstellung und Beschlagnahme von auf dem Mailserver des Providers gespeicherten E-Mails, die nach den Vorschriften angeordnet wurde (2 BvR 902/06),[131] den Inhalt der Entscheidung vom 2005 jeweils in demselben Sinne herangezogen und zusätzlich dazu nur Schranken nach dem Grundsatz der Verhältnismäßigkeit im konkreten Fall dargestellt.[132] Auch hier hat das *BVerfG* hinsichtlich des

[127] *Singelnstein*, NStZ 2012, 593, 602; dazu *Neuhöfer*, JR 2015, 21, 25: bezüglich des Zugriffs auf serverbasiert gespeicherte Nachrichteninhalte in sozialen Netzwerken.

[128] Vgl. *BVerfGE* 113, 29, 52 ff. [Rn. 106 ff.].

[129] *BVerfGE* 113, 29, 55 ff. [Rn. 113 – 120]; Wiederholung desselben Inhalts 124, 43, 67 ff. [Rn. 82 ff.].

[130] *BVerfGE* 115, 166, 198 f. [Rn. 119 – 121].

[131] *BVerfGE* 124, 43, 62 – 66 [Rn. 69 – 76] und 66 – 70 [Rn. 78 – 90].

[132] *BVerfGE* 115, 166, 198 f. [Rn. 119 – 121] und 124, 43, 67 [Rn. 79 – 81]: „*Im Einzelfall können die Geringfügigkeit der zu ermittelnden Straftat, eine geringe Beweisbedeutung der zu beschlagnahmenden E-Mails/Verbindungsdaten sowie die Vagheit des Auffindeverdachts der Maßnahme entgegenstehen. Dem Schutz des Fernmeldegeheimnisses/des Rechts auf informationelle Selbstbestimmung muss bereits in der Durchsuchungsanordnung … durch Vorgaben zur Beschränkung des Beweismaterials auf den tatsächlich erforderlichen Umfang Rechnung getragen werden, etwa durch die zeitliche Eingrenzung oder die Beschränkung auf bestimmte Kommunikationsinhalte. Bei dem Vollzug von Durchsuchung und Beschlagnahme – insbesondere beim Zugriff auf umfangreiche elektronisch gespeicherte Datenbestände – … ist vor*

Zugriffs auf umfassend gespeicherte Datenbestände noch keine weiteren verfahrensrechtlichen Sicherungen verlangt.[133] Insofern hat das Gericht u. a. ausgeführt, dass es von Verfassungs wegen nicht stets geboten ist, dass die Prüfung der Verfahrenserheblichkeit sämtlicher sichergestellter Daten durch die Durchsicht gemäß § 110 StPO stattfindet und dabei der von Daten Betroffene und sein Verteidiger an der Durchsicht teilnehmen, sondern dies eher im jeweiligen Einzelfall von der Ermittlungsbehörde zu beurteilen ist.[134]

3. Teilweise Kritik

Im Rahmen der Beweissicherung für die Strafverfolgung muss die überschießende Gewinnung der für das Verfahren bedeutungslosen Daten im Blick auf Zweckbindung und Verhältnismäßigkeit nach Möglichkeit vermieden werden und so wird die Beschlagnahme sämtlicher gespeicherter Daten oder des gesamten Datenbestands regelmäßig zur Aufklärung von Sachverhalten nicht erforderlich sein.[135] Doch es ist schließlich erlaubt, die gesamten Daten bzw. Datenbestände zu beschlagnahmen, wenn Zuordnung und Trennung nur verfahrensrelevanter Daten nicht möglich ist.[136] In der Praxis machen Unsichtbarkeit und eine große Masse elektronischer Daten dieses Vorgehen vielfach zwangsläufig. Mit Blick auf seine besondere Eingriffsintensität in diesem Fall erscheint aber die Stellungnahme des *BVerfG* nicht angemessen, die in der geltenden StPO vorgesehenen verfahrensrechtlichen Garantien für ausreichend zu halten. Derzeit ist nämlich in diesem Fall kein zuverlässiges Verfahren für die Trennung und Auswahl verfahrensrelevanter Informationen gewährleistet. Die Auslegung und Anwendung von §§ 94 ff., 102 ff. StPO in

---

allem darauf zu achten, dass die Gewinnung überschießender, für das Verfahren bedeutungsloser Daten nach Möglichkeit vermieden wird. Die Beschlagnahme sämtlicher (auf einer Computerfestplatte) gespeicherter Daten und damit des gesamten E-Mail-Verkehrs (oder der gesamten Datenverarbeitungsanlage) wird regelmäßig nicht erforderlich sein."

[133] Vgl. *BVerfGE* 113, 29, 57 ff. [Rn. 122 – 135]; auch 124, 43, 70 ff. [Rn. 91 – 102]: Diesbezüglich enthält die StPO schon ausreichende Verfahrensregelungen, die dazu dienen, Grundrechtseingriffen vorzubeugen oder diese zu minimieren, etwa §§ 35, 98 Abs. 2 S. 5, § 110 und §§ 483, 489, 491 StPO sowie auch ein verfassungsrechtliches Verwertungsverbot und eine Kennzeichnungspflicht.

[134] Vgl. *BVerfGE* 113, 29, 58 [Rn. 127]; 124, 43, 72 [Rn. 96] und 77 [Rn. 112]: Allein aus dem Umstand, dass er Nichtverdächtiger ist, wird das Teilnahmerecht verfassungsunmittelbar nicht abgeleitet.

[135] Vgl. *BVerfGE* 124, 43, 67 [Rn. 81]; *BGH* NJW 2010, 1297, 1298 [Rn. 15]: die Beschlagnahme des gesamten auf dem Mailserver des Providers gespeicherten E-Mail-Bestands.

[136] Vgl. *BVerfGE* 113, 29, 57 [Rn. 120] und 124, 43, 69 [Rn. 89]: „*Ist den Strafverfolgungsbehörden im Verfahren der Durchsicht unter zumutbaren Bedingungen eine materielle Zuordnung der verfahrenserheblichen Daten/E-Mails einerseits oder eine Löschung oder Rückgabe der verfahrensunerheblichen Daten/E-Mails an den Berechtigten/Nutzer andererseits nicht möglich, steht der Grundsatz der Verhältnismäßigkeit jedenfalls unter dem Gesichtspunkt der Erforderlichkeit der Maßnahme einer Beschlagnahme des gesamten Datenbestands nicht entgegen.*"

der Praxis wird der neuen erhöhten Gefährlichkeit nach den Vorschriften nicht gerecht[137] und somit besteht insoweit eine große Kluft zwischen Normen und Rechtswirklichkeit. Dies gilt erst recht insb. angesichts des Leerlaufs des Richtervorbehalts und des Funktionsverlustes des § 110 StPO in der Praxis. Diesbezüglich wird im Schrifttum einerseits hauptsächlich kritisiert, dass Richter ihren Kontrollpflichten nicht in vollem Umfang nachkommen und ihre Kontrollbefugnisse durch die Ermittlungsbehörden übermäßig ausgeschlossen werden, und anderseits, dass die StA und ihre Ermittlungspersonen im Zuge der Durchführung der Durchsuchung und Beschlagnahme die Verfahrensvorschriften und den Inhalt in richterlichem Beschluss nicht vollständig einhalten.[138] Obwohl der Durchsuchung und Beschlagnahme im Strafverfahren stets eine erhebliche Bedeutung zukommt, lassen nicht nur die Ermittlungsbehörden als Vollzugsorgan, sondern auch die Gerichte als Kontrollinstanz bei der Anwendung der betroffenen Vorschriften weitgehend Großzügigkeit walten.[139] Hier bestehen erhebliche verfassungsrechtliche Bedenken. Trotz der Fülle, Vielfalt und Kompliziertheit der Durchsuchung und Beschlagnahme in der Praxis kann dies zur Uneinheitlichkeit der Rechtsprechung und zur Verletzung der Rechtssicherheit[140] und weiter u. a. zu einer übermäßigen Verletzung der Grundrechte führen. Dies ist eine Besorgnis, die nicht mehr übersehbar und tatsächlich spürbar ist.

Insoweit ist u. a. ein Ausgleich der Eingriffsintensität durch die Durchsicht gemäß § 110 StPO (vgl. unten III.) und die Gewährleistung des Anwesenheitsrechts des Betroffenen und seines Rechtsanwalts (vgl. unten IV.) zu berücksichtigen.[141] Vorher ist es geboten, dass der Richtervorbehalt, der zwar in der Praxis vielfach abgewertet wird, aber auf den – unter dem System des Akkusationsprinzips – besonderer Wert gelegt wird, so streng wie möglich eingehalten wird (vgl. unten II.).

---

[137] *Burhoff*, StraFo 4/2005, 140.

[138] *Park*, § 2 Rn. 56, 96, 142, 246 f. und 316 sowie § 3 Rn. 486 und 487; *Burhoff*, StraFo 4/2005, 140, 140 ff. [Tz. C. & D.]; *Dauster*, StraFo 6/1999, 186, 187; *Schünemann*, ZStW 114 (2002), 1, 20 m. w. N.

[139] *Park*, § 1 Rn. 1 f.

[140] Vgl. *Park*, § 1 Rn. 3.

[141] Vgl. *BVerfGE* 124, 43, 68 f. [Rn. 87 f.] und 72 [Rn. 96]. *Sieber* behauptet richtigerweise, dass die in der Entscheidung des *BVerfG* erwähnten erkennbaren Ansätze für Begrenzungen und Schutzmechanismen intensiviert und normiert werden müssen (*Sieber*, 69. DJT 2012, C 111; dazu *Kemper*, wistra 5/2006, 171, 175: pauschale Reformbedürftigkeit der Regelung der §§ 94 ff. StPO; auch *Hiéramente*, wistra 11/2016, 432: keine eindeutigen Regelungen für die Durchsuchungen im EDV-Bereich).

4. Exkurs: Erhebung der Zugangssicherungscodes und Herausgabe unverschlüsselter Daten in offenen Ermittlungen

a) Einleitung

Die Zugangssicherungscodes sind i. d. R. in zwei Typen zu unterteilen: einen zum Schutz eines Zugriffs auf Endgeräte und einen anderen zum Schutz eines Zugriffs auf räumlich getrennte Speicher (vgl. § 100j Abs. 1 S. 2 StPO). Zuerst haben bei den „Codes zum Zugriff auf Endgeräte" die Hersteller der Geräte (z. B. Smartphones oder PCs) oder deren Betriebssysteme (z. B. *Apple iOS*, *Google Android*, *Microsoft Window Mobile* etc.) zumeist nur ein technisches Hilfsmittel bzw. Programm zur Entschlüsselung, nicht das Passwort selbst.[142] Hierbei handelt es sich daher meistens nicht um die Erfassung der Codes selbst von den Anbietern, sondern um die Mitwirkung der Anbieter zur Entschlüsselung der Codes. Bei den „Codes zum Zugriff auf Online-Server"[143] haben zum anderen die Anbieter oder Unternehmen als Verwalter der Server zumindest Zugang zu den – durch die Codes geschützten – gespeicherten (Inhalts-)Daten.[144] Insoweit ist eine „direkte" Durchsuchung der Server durch die Ermittlungsbehörden unmöglich oder sie kann faktisch nur sehr eingeschränkt durchgeführt werden. Denn sie wird zum einen in vielen Fällen zum Zugriff auf Geschäftsgeheimnisse oder personenbezogene Daten von unverdächtigen Dritten führen, zum anderen ist es technisch nahezu unmöglich, dass die Ermittlungsbehörden online oder offline Zugang zu den Servern der – insb. großen multinationalen – Anbieter oder Unternehmen erhalten.

Damit die Ermittlungsbehörden bei „offenen Ermittlungen" nach §§ 94 ff., 102 ff. StPO zum Zweck der Sicherstellung der Daten, die auf im Zuge der Durchsuchung aufgefundenen Geräten oder externen Speichermedien gespeichert, aber zugangsgesichert sind, Kennungen und Passwörter mithilfe der Anbieter oder Unternehmen erfahren, ist grundsätzlich eine gerichtliche Anordnung erforderlich, aber – ausnahmsweise – bei Gefahr im Verzug kann die Anordnung auch durch die StA oder ihre Ermittlungspersonen getroffen werden (§ 100j Abs. 3 S. 1, 2 i. V. m. §§ 98 Abs. 1, 105 Abs. 1 StPO). Über die Beauskunftung ist die betroffene Person als der von Sicherheitsdaten Betroffene zu benachrichtigen, soweit und sobald hierdurch der Zweck der Auskunft nicht vereitelt wird (§ 100j Abs. 4 S. 1, 2 StPO). Jedoch ist diese Vorschrift i. R. d. offenen Ermittlungen nach der §§ 94 ff., 102 ff. StPO beschränkend

---

[142] Allerdings können sie von vornherein nicht vorliegen. Außerdem können bei vielfacher Eingabe falscher Passwörter ggf. die Geräte in den ursprünglichen Zustand, wie sie ab Werk voreingestellt sind, zurückversetzt werden und damit alle dort vorhandenen Daten gelöscht werden.

[143] Damit sind gemeint Benutzername und Passwort eines Benutzerkontos. In letzter Zeit sind diese Daten aus Sicherheitsgründen regelmäßig nur dem Betroffen bekannt und auch für sich selbst geschützt.

[144] Vgl. *BVerfGE* 124, 43, 55 [Rn. 46]: In diesem Fall bleiben die Anbieter und auch die Ermittlungsbehörden in der Lage, auf die Daten zuzugreifen, jedoch hat der Betroffene keine technische Möglichkeit, die Weitergabe der Daten durch die Anbieter zu verhindern.

dahin auszulegen, dass die Benachrichtigung spätestens „zum Zeitpunkt der Durchsuchung“ erfolgen muss, um den Charakter der offenen Maßnahme nicht zu verlieren (vgl. Kapitel 3, A. II.). Erfolgt daher die Benachrichtigung erst nach der Erhebung der – zugangsgesicherten – Daten oder unterbleibt sie endgültig nicht, so ist dies ein heimlicher Zugriff. Aus alledem bleibt nur der Zugriff nach § 110 Abs. 3 StPO letztendlich als Vorgehensweise, um „die serverbasiert gespeicherten Daten“ „mittels der Zugangscodes“ „offen“ zu durchsuchen und zu beschlagnahmen (vgl. dazu eingehend unten III. 2. a) cc)).

b) Beauskunftung von Zugangssicherungscodes und Anordnung von Ordnungs- und Zwangsmitteln

Wenn die Endgeräte wie PCs, Smartphones etc., die nach §§ 94, 102, 103 StPO rechtmäßig sichergestellt bzw. beschlagnahmt wurden, verschlüsselt sind und Zugangssicherungscodes nicht freiwillig herausgegeben wurden,[145] aber die Ermittlungsbehörde sie nicht selbstständig entschlüsseln konnte (vgl. unmittelbarer Zwang), dann können die Codes schließlich nach § 100j Abs. 1 S. 2, Abs. 3 S. 1 StPO durch richterliche Anordnung von Anbietern oder Unternehmen eine Mitwirkung – auf technischer Seite – verlangt werden (vgl. Abs. 5 S. 1). In diesem Fall befinden sich die Geräte schon in behördlichem Gewahrsam und daher ist die Gefahr im Verzug nicht anzunehmen (vgl. § 100j Abs. 3 S. 2 StPO). Hierbei kann ein Richter beim Ausbleiben der Mitwirkung auf Antrag der StA den Anbietern oder Unternehmen die in § 70 StPO bestimmten Ordnungs- und Zwangsmittel anordnen (vgl. § 100j Abs. 5 S. 2 i. V. m. § 95 Abs. 2 StPO).[146] Dennoch erfolgt eine solche Mitwirkung praktisch ggf. – insb. bei großen internationalen Unternehmen – nicht

[145] Nach h. M. gilt § 95 StPO nicht für den Beschuldigten, so geht er keine Verpflichtung ein, den Ermittlungsbehörden seine Sicherheitsdaten herauszugeben (vgl. Nemo-tenetur-Grundsatz, *Greven*, KK-StPO, § 95 Rn. 2; M-G/*Schmitt*, StPO, § 95 Rn. 5; *Sieber*, 69. DJT 2012, C 122 am Anfang; *Wohlers*/*Greco*, SK-StPO, § 95 Rn. 12; *Zimmermann*, JA 5/2014, 321, 322; vgl. abw. *Bäumerlich*, NJW 2017, 2718, 2720 [Tz. 1.]: gemäß § 136a StPO; vgl. *BVerfG* NJW 2005, 1640, 1641 a. E.: Der Angeklagte ist nicht dazu verpflichtet, zu seiner Strafverfolgung durch aktives Handeln beizutragen, und unterliegt im Strafverfahren keiner Darlegungs- und Beweislast).

[146] *Greven*, KK-StPO, § 95 Rn. 4 und *Bruns*, KK-StPO, § 100j Rn. 8; *Wohlers*/*Greco*, SK-StPO, § 95 Rn. 31 und *Greco*, SK-StPO, § 100j Rn. 20; M-G/*Schmitt*, StPO, § 95 Rn. 9 und § 100j Rn. 7. Die Zwangsmittel nach § 95 Abs. 2 StPO, nämlich ein Zwangsgeld und ersatzweise eine Ordnungshaft oder eine Beugehaft (bis zu 6 Monaten), bleiben nach einhelliger Meinung wegen ihrer Eingriffsintensität, die gegenüber der Beschlagnahme ähnlich (Zwangsgeld) oder stärker (Ordnungshaft) ist, ausschließlich dem Richter, nicht den Ermittlungsbehörden vorbehalten (*LG Gera* NStZ 2001, 276; *LG Halle* NStZ 2001, 276, 277; *LG Koblenz* wistra 9/2002, 359, 360; *Bittmann*, wistra 9/1990, 325, 335; *Greven*, KK-StPO, § 95 Rn. 4; *Klinger*, wistra 1/1991, 17, 19; *Kurth*, NStZ 1983, 327, 328; M-G/*Schmitt*, StPO, § 95 Rn. 9; *Park*, § 3 Rn. 642; *Roxin*/*Schünemann*, § 34 Rn. 9; *Wohlers*/*Greco*, SK-StPO, § 95 Rn. 32).

schnell und bereitwillig.[147] Um diese Probleme in der Praxis ohne Störung zu lösen, wäre es hilfreich, wenn es detaillierte Leitlinien für die Zusammenarbeit zwischen Ermittlungsbehörden und Unternehmen auf Bundes- oder Länderebene gäbe. Dabei verstößt es gegen den Verhältnismäßigkeitsgrundsatz und den Richtervorbehalt, dass die Ermittlungsbehörden ein entschlüsseltes Endgerät ohne jegliche Kontrolle vollständig auslesen können (vgl. unten IV.).

Die Erfassung der Zugangscodes ist zum anderen auch dann problematisch, wenn die Ermittlungsbehörden durch die Erweiterung der Durchsuchung nach § 110 Abs. 3 StPO auf externe Speichermedien zugreifen. Zunächst begründet § 110 Abs. 3 StPO – i. V. m. § 103 StPO – keine Verpflichtung für die Dienstanbieter oder Unternehmen, den Ermittlungsbehörden die Zugangsdaten selbst herauszugeben.[148] Dafür ist nach § 100j Abs. 1 S. 2 und Abs. 3 StPO grundsätzlich eine gesonderte richterliche Anordnung erforderlich und nur bei Gefahr im Verzug können die Ermittlungsbehörden dies anordnen. Hier sollte – anders als im obigen Fall – die Möglichkeit einer sofortigen Änderung der Passwörter und einer Löschung von Inhalten durch den Betroffenen in Betracht gezogen werden. Wenn der Ermittler die Daten auf dem Server vor Ort umgehend nicht sichern konnte, werden nämlich die von der Durchsuchung betroffenen Personen oder Teilnehmer, die diesen Zugriffsversuch bereits kennen, sie löschen oder übertragen oder die Passwörter ändern. Zu einer wirksamen Strafverfolgung sollte dies vermieden werden. Aus diesem Grund und auch in Betracht, dass die Besorgnis des Verlustes der Beweismittel eine Voraussetzung für diese Ausweitung der Durchsuchung ist (vgl. § 110 Abs. 3 S. 1 Hs. 2 StPO), ist die Gefahr im Verzug als Voraussetzung für Eilkompetenz i. d. R. anzunehmen, falls der Ermittlungsrichter vor Ort nicht sofort telefonisch oder per E-Mail erreicht wird.[149] Auch hier sind – wie im obigen Fall – die Ordnungs- und Zwangsmittel des § 70 StPO anzuordnen, wenn die Anbieter oder Unternehmen ihre Mitwirkungspflicht nicht nachkommen. Schließlich ist es nicht zulässig, mit erhaltenen Zugangscodes die externen Speichermedien mehrmalig abzufragen oder wiederholt darauf zuzugreifen; denn dies stellt in der Tat eine ständige – verdeckte – Überwachung des Datenverkehrs dar und kann unter die Formulierung, dass „der Verlust der gesuchten Daten zu besorgen ist", nicht subsumiert werden.[150]

---

[147] Erst recht lehnen sie das Ersuchen um Mitwirkung ab: z. B. für *Apple*, Spiegel, Apple widersetzt sich FBI-Forderung, <https://www.spiegel.de/netzwelt/gadgets/apple-fbi-will-hilfe-beim-iphone-knacken-konzern-wehrt-sich-a-1077769.html>, Abruf: 31. 10. 2020.

[148] *Park*, § 4 Rn. 817 a. E.; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 10.

[149] Dazu *Brodowski/Eisenmenger*, ZD 3/2014, 119, 124 [Tz. c)].

[150] Zust. *Brodowski/Eisenmenger*, ZD 3/2014, 119, 124 f.: eine Umgehung der Hürden des § 100a StPO; M-G/*Schmitt*, StPO, § 110 Rn. 6 f.; *Zerbes/El-Ghazi*, NStZ 2015, 425, 432.

c) Herausgabe unverschlüsselter Daten

(1) Daneben fragt es sich, ob die Ermittlungsbehörde „aufgrund richterlicher Anordnung“[151] die Anbieter oder Unternehmen auffordern oder zwingen kann, die von ihnen verwahrten, aber zugangsgesicherten Daten von Kunden bzw. Arbeitnehmern gedruckt im „Klartext“ herauszugeben (vgl. § 95 i. V. m. § 98 Abs. 1 StPO).[152] Laut *Sieber* sei diesbezüglich eine Gesetzesänderung dafür erforderlich, weil es sich bei § 95 Abs. 1 StPO nach seinem Wortlaut nur um die „Herausgabe bereits im Gewahrsam befindlicher beweglicher Sachen“ handele und die „Produktion zum Zwecke einer Herausgabe der zugangsgeschützten Daten (*production und decryption order*)“ von der Vorschrift nicht erfasst werde.[153] Es ist jedoch zweifelhaft, dass die Vorlage und Auslieferung des Gegenstandes nach § 95 Abs. 1 StPO so eng auszulegen ist. Derzeit ist hinreichend auszulegen, dass die Verpflichtung zur Entschlüsselung und Datenherausgabe nach §§ 95, 98 Abs. 1, 103, 105 Abs. 1 und § 100j Abs. 1 S. 2 StPO zulässig ist.

In der Auslegung des Wortlauts gilt § 95 Abs. 1 StPO nur für bewegliche Sachen, die vorgelegt oder ausgeliefert werden können,[154] und dazu gehören EDV-Daten und deren Ausdrucke. Er hat meistens in den Fällen praktische Bedeutung, in denen es zwar feststeht, dass sich ein Beweismittel im Gewahrsam einer Person befindet, aber es bei einer Durchsuchung nicht gefunden werden konnte oder der Ort des Ge-

[151] Nach der früher überwiegend vertretenen Ansicht ist für ein „Herausgabeverlangen“ nach § 95 Abs. 1 StPO unter Androhung der Ordnungs- oder Zwangsmittel des § 70 StPO grundsätzlich nur der Richter zuständig, und erst bei Gefahr im Verzug, also im Eilfall, die StA (*LG Bonn* NStZ 1983, 327; *LG Stuttgart* NJW 1992, 2646, 2647; *LG Düsseldorf* wistra 5/1993, 199, 200; *Greven*, KK-StPO, § 95 Rn. 3; *Roxin*/*Schünemann*, § 34 Rn. 9). Hingegen ist nach der heutzutage als herrschend angesehenen Gegenmeinung auch die StA (und auch die Polizei) neben dem Richter – ungeachtet des Vorliegens der Gefahr im Verzug – zum „Herausgabeverlangen“ nach § 95 Abs. 1 StPO befugt (*LG Gera* und *LG Halle* NStZ 2001, 276, 277: die StA; *LG Koblenz* wistra 9/2002, 359: die StA; *Bittmann*, wistra 9/1990, 325, 334: die StA; *Klinger*, wistra 1/1991, 17: die StA; *Kurth*, NStZ 1983, 327: die StA; M-G/*Schmitt*, StPO, § 95 Rn. 2: die StA und die Polizei; *Wohlers*/*Greco*, SK-StPO, § 95 Rn. 3 f. und 25: die StA und die Polizei. Mit Blick auf die Eingriffsintensität des Herausgabeverlangens sind seine Ermächtigungsnormen §§ 161, 163 StPO und daher ist auch die Polizei richtigerweise dazu befugt). Nach Wortlaut, Systematik und Zweck der §§ 94, 95, 98 StPO und aus Verhältnismäßigkeitsgesichtspunkten verdient die Gegenmeinung Zustimmung. Unabhängig von dieser Debatte dürfen aber die zugangsgeschützten Daten nur auf das Verlangen der Ermittlungsbehörde nicht herausgeben, weil die Verwendung der Zugangscodes nach § 100j Abs. 3 S. 1 StPO grundsätzlich dem Richtervorbehalt unterliegt.

[152] Bei fehlender Beschlagnahmeanordnung lehnen Kreditinstitute eine freiwillige Herausgabe von Unterlagen aus haftungsrechtlichen Gründen regelmäßig ab (*Kemper*, wistra 5/2006, 171, 173 a. E.).

[153] *Sieber*, 69. DJT 2012, C 121 f. und dazu C. 115: Dass sich die Vorlage eines Gegenstandes im Gewahrsam einer Person nach § 95 Abs. 1 StPO nach § 110 Abs. 3 StPO auf anderweitig gespeicherte Daten erstreckt, ist mit dem Gesetzesvorbehalt für strafprozessuale Eingriffe nicht vereinbar; auch M-G/*Schmitt*, StPO, § 95 Rn. 3a.

[154] *Greven*, KK-StPO, § 94 Rn. 1.

wahrsams nicht zu ermitteln war.[155] Die Durchsuchung und Beschlagnahme von EDV-Anlagen ist i. d. R. der Fall, daher betrifft der Anwendungsbereich des § 95 StPO heutzutage zumeist die Erhebung der Kunden- oder Arbeitsnehmerdaten von Anbietern oder Unternehmen, die – nicht beschuldigte (vgl. siehe Fn. 145) – Gewahrsamsinhaber darstellen (z. B. E-Mail oder Dateien, die auf ihren Mail- oder Cloud-Servern gespeichert sind, oder Bank- oder Kontounterlagen[156]). Insbesondere bezüglich Computerdaten und Bestandsdaten entspricht das Herausgabeverlangen nach Abs. 1 dem Art. 18 Abs. 1 Ziff. a und b CKÜ.[157] Ein solches Herausgabeverlangen kann in vielen Fällen nicht nur ein sehr effektiver und einfacher Weg zur Erlangung gesuchter Daten sein,[158] sondern dient auch dazu, dass die Durchsuchung und Beschlagnahme bei Anbietern oder Unternehmen als Dritte nach dem Grundsatz der Verhältnismäßigkeit sorgfältig durchgeführt wird (insb. um den Zugriff auf verfahrensirrelevante Geschäftsgeheimnisse, Finanzdaten, Kundendaten oder und andere sensible Daten und die Einsicht darin zu umgehen). Das heißt, dass § 95 StPO bei Maßnahmen zum Zweck der Beweiserhebung gegenüber den Anbietern und Unternehmen, die heutzutage riesige Mengen an personenbezogenen Daten in ihrem Gewahrsam haben, im Hinblick auf die Effizienz der Ermittlungen und den Schutz der Grundrechte sinnvoller ist als die Beschlagnahme nach § 94 Abs. 2 StPO.[159] Freilich liegt es im Ermessen der Ermittlungsbehörden, ob sie im Einzelfall mittels der Zugangscodes den Server persönlich durchsuchen (vgl. § 110 Abs. 3 StPO) oder die Herausgabe der Daten im Klartext von Anbietern verlangen (vgl. § 95 StPO).

(2) *Quick-Freezing-Verfahren:* In der geltenden StPO ist es fraglich, ob die umgehende Sicherung gespeicherter Daten nach Art. 16 CKÜ (sog. „Quick-Freezing-Verfahren") möglich ist. Nach dem Abs. 2 der Vorschrift besteht das Verfahren aus zwei Phasen: Die Ermittlungsbehörden können im Wege einer Anordnung den Gewahrsamsinhaber der Speichermedien verpflichten, bestimmte Daten unter Sicherung ihrer Integrität vorzuhalten (1. Sicherungsstufe), und hierauf muss er – nach richterlicher Anordnung – an die Behörden die Daten herausgeben (2. Herausgabestufe). Da alle Datenarten nicht nur beweisrelevant sein, sondern auch verloren gehen und manipuliert werden können, handelt es sich dabei naturgemäß nur um alle Daten einschließlich Verkehrsdaten, die zum Zeitpunkt der Anordnung noch vorhanden sind (vgl. Art. 16 Abs. 1 CKÜ).[160] Der Kern dieses Verfahrens liegt in der

[155] *Kurth*, NStZ 1983, 327; M-G/*Schmitt*, StPO, § 95 Rn. 1; *Park*, § 3 Rn. 437; *Roxin/Schünemann*, § 34 Rn. 10; *Wohlers/Greco*, SK-StPO, § 95 Rn. 3.

[156] *Bittmann*, wistra 9/1990, 325; *Greven*, KK-StPO, § 95 Rn. 2; *Klinger*, wistra 1/1991, 17; *Kurth*, NStZ 1983, 327; *Park*, § 3 Rn. 437; *Wohlers/Greco*, SK-StPO, § 95 Rn. 5; vgl. *LG Koblenz* wistra 9/2002, 359, 360: „*besonders bei Fällen …, in denen spezifische, in umfangreichen Datenbanken gespeicherte und dem Außenstehenden nicht leicht zugängliche Informationen den Gegenstand der Herausgabe bilden*".

[157] *Sieber*, 69. DJT 2012, C 114 f.

[158] Vgl. *Sieber*, 69. DJT 2012, C 114 a. E.

[159] Vgl. *Sieber*, 69. DJT 2012, C 121 f.

[160] *Sieber*, 69. DJT 2012, C 123. Daher ist die Maßnahme keine Alternative zur VDS für die präventive Speicherung von Verkehrsdaten, sondern sie kann diese nur ergänzen (a. a. O.).

Sicherungsstufe, in der die umgehende Sicherung der Daten im Eilfall, etwa bei Gefahr im Verzug, ohne Tätigwerden der Gerichte von den Ermittlungsbehörden, insb. der StA, angeordnet werden kann.[161] Hierbei werden alle gesicherten Daten weder automatisch an die Ermittlungsbehörden übermittelt noch von diesen beschlagnahmt. Die endgültige Herausgabe, nämlich Beschlagnahme, muss eine gerichtliche Anordnung voraussetzen. In dieser Hinsicht kann dieses Verfahren als ausgeglichenes Mittel zum Datenzugriff und Grundrechtsschutz angesehen werden.

Im deutschen Recht ist aber das Verfahren nicht in expliziter Form vorgesehen.[162] Vor allem ist es fragwürdig, ob in der Auslegung des geltenden Rechts die umgehende Sicherung der Daten als erste Stufe zu erzwingen ist.[163] Dass die Ermittlungsbehörden den Gewahrsamsinhaber der Daten in solche Sicherungspflicht nehmen, darf sich erst vor dem Hintergrund der Entscheidung zur Vorratsdatenspeicherung von 2010 und der Strenge ihrer Ermächtigungsnorm (§§ 100g, 101a, 101b StPO) einfach auf die Ermittlungsgeneralklauseln der §§ 161, 163 StPO stützen. Da es sich außerdem bei §§ 94, 95 StPO um die endgültige Beschaffung der Daten handelt und die vorläufige Sicherstellung nach § 110 StPO unter die Durchsuchung – i. V. m. dem Richtervorbehalt – fällt (vgl. unten III. 3.), können diese Vorschriften keine Ermächtigungsnorm der Maßnahme darstellen. In geltendem Recht ist schließlich die Anordnung der Sicherung – durch die StA – nicht zulässig. Dafür bedarf es einer neuen Rechtsgrundlage (vgl. Gesetzesvorbehalt).[164] Dabei ist Rechnung zu tragen, dass diese Vorhaltung im Einzelfall erst zu dem Zeitpunkt anzuordnen ist, zu dem ein konkreter Anlass wegen eines bestimmten Tatverdachts besteht.[165]

II. Richtervorbehalt

1. Grundsatz – richterliche Anordnung

a) Sinn und Zweck

Für die Beschlagnahme und Durchsuchung, die in das Grundrecht schwerwiegend eingreifende Zwangsmaßnahme darstellen und daher die strikte Beachtung der Verhältnismäßigkeit erfordern, gilt grundsätzlich – nicht nur Gesetzesvorbehalt,

[161] Vgl. *Sieber*, 69. DJT 2012, C 123 und 124 f.

[162] *Sieber*, 69. DJT 2012, C 123. Laut *Sieber* kann es mit einzelnen Vorschriften i. V. m. den jeweiligen Gefahr-im-Verzug-Regelungen (z. B. §§ 94, 95, 100g StPO) nur begrenzt erfüllt werden (a. a. O.).

[163] Die Herausgabe der zweiten Stufe kann nach §§ 94 oder 95 i. V. m. § 98 StPO angeordnet werden.

[164] *Sieber*, 69. DJT 2012, C 124 f. Bei der konkreten gesetzlichen Ausgestaltung ist daneben nach dem Grundsatz der Verhältnismäßigkeit zumindest der gegenständliche, zeitliche und räumliche Umfang der zu sichernden Daten normenklar zu regeln (a. a. O. C 125).

[165] Vgl. *BVerfGE* 125, 260, 318 [Rn. 208].

sondern auch – Richtervorbehalt (vgl. Art. 13 Abs. 2 GG; auch Art. 10 Abs. 2 GG; vgl. für die Freiheitsentziehung Art. 104 Abs. 2 GG).[166] Er ist zum Rechtsschutz des Betroffenen eine Vorkehrung, um die Vorabprüfung darüber zu gewährleisten, ob materielle Voraussetzungen für die Durchsuchung und Beschlagnahme bestehen, und er zielt auf eine vorbeugende Kontrolle der Maßnahme durch eine unabhängige und neutrale Instanz ab;[167] eine gerichtliche Vorabkontrolle exekutiver Maßnahmen. Diese dient insgesamt der verstärkten Sicherung des Grundrechts durch eine angemessene Begrenzung des Eingriffs gegenüber den Ermittlungsbehörden[168] und soll u. a. dafür sorgen, dass die Interessen des Betroffenen angemessen, d. h. im Einzelfall am besten und sichersten berücksichtigt werden.[169] So muss der Richter dafür eigenverantwortlich prüfen, ob die verfassungsrechtlichen und gesetzlichen Voraussetzungen der Durchsuchung und Beschlagnahme genau beachtet werden.[170] Dazu muss er den Beschluss der Durchsuchung und Beschlagnahme gehaltvoll begründen[171] und selbst verfassen.[172] Er ist daneben verpflichtet, durch eine geeignete Formulierung i. R. d. Möglichen und Zumutbaren sicherzustellen, dass der Eingriff

---

[166] *BVerfGE* 20, 162 186 f.; 42, 212, 219 f.; 103, 142, 151 [Rn. 27]; 139, 245, 265 [Rn. 57]; NJW 2002, 1333 [Tz. a)]; 2009, 2516 [Rn. 21]; 2015, 1585, 1586 [Rn. 23 f.]; *OLG Koblenz* NStZ 2007, 285, 286 [Rn. 3]; vgl. für heimliche Maßnahmen 125, 260, 338 [Rn. 249] und 141, 220, 275 f. [Rn. 118].

[167] *BVerfGE* 103, 142, 151 [Rn. 28]; 125, 260, 337 [Rn. 248]; 139, 245, 265 [Rn. 57]; NJW 2009, 2516 [Rn. 21]; 2015, 1585, 1586 [Rn. 24]; *Park*, § 2 Rn. 69; *Wohlers/Jäger*, SK-StPO, § 105 Rn. 16.

[168] *BVerfGE* 103, 142, 152 [Rn. 29 a. E.]; dazu *Park*, § 2 Rn. 69 und 471; *Wohlers/Jäger*, SK-StPO, § 105 Rn. 16. Zentraler Ausgangspunkt für das Verständnis des Richtervorbehalts ist der Grundsatz der Gewaltenteilung und der Gedanke effektiven Grundrechtsschutzes (*BVerfGE* 139, 245, 265 f. [Rn. 58 f.]).

[169] *BVerfGE* 103, 142, 151 [Rn. 28]; 139, 245, 266 [Rn. 60]; NJW 2009, 2516 [Rn. 21]; NJW 2015, 1585, 1586 [Rn. 24]; vgl. 139, 245, 279 [Rn. 93]: der Richtervorbehalt dient der Sicherstellung der Interessenabwägung.

[170] *BVerfGE* 96, 44, 51 [Rn. 24]; 103, 142, 151 [Rn. 29 am Anfang]; 125, 260, 338 [Rn. 249]; NJW 2009, 2516, 2516 f. [Rn. 21]; insb. 139, 245, 277 [Rn. 87]. Die Prüfungskompetenz des Ermittlungsrichters beschränkt sich auf die rechtliche Kontrolle darüber, ob die gesetzlichen Voraussetzungen für die Maßnahme vorliegen und der (verfassungsrechtliche) Verhältnismäßigkeitsgrundsatz gewahrt ist; dabei handelt es sich um die gesetzliche Zulässigkeit, nämlich die Rechtmäßigkeit der beantragten Handlung (§ 162 Abs. 2; *Park*, § 2 Rn. 70; *Wohlers/Jäger*, SK-StPO, § 105 Rn. 14; vgl. *BVerfGE* 120, 274, 331 [Rn. 258]). Die Prüfung auf die (bloße) Zweckmäßigkeit ist hingegen nicht dem Richter, sondern der StA als Herrin des Vorverfahrens vorbehaltlich (*Ciolek-Krepold*, Rn. 53 a. E.; M-G/*Schmitt*, StPO, § 162 Rn. 14 f.; *Park*, § 2 Rn. 70; *Schünemann*, ZStW 114 (2002), 1, 40; *Wohlers/Jäger*, a. a. O.). Die Ermittlungsstrategie bzw. das -konzept steht der StA zu. Daher darf der Ermittlungsrichter grundsätzlich eine von der StA nicht beantragte Ermittlungsmaßnahme nicht anordnen (Ausnahme: § 165 StPO; M-G/*Schmitt*, a. a. O. Rn. 5) und ist weiter nicht berechtigt, eine beantragte Maßnahme durch eine andere von ihm für besser gehaltene zu ersetzen. Insoweit ist der Ermittlungsrichter in tatsächlicher Hinsicht an den Antrag der StA gebunden (vgl. Grundsatz des *ne ultra petita*).

[171] *BVerfGE* 125, 260, 338 [Rn. 249].

[172] *Schünemann*, ZStW 114 (2002), 1, 37.

und dessen Durchführung messbar und kontrollierbar bleiben.[173] Durch den Richtervorbehalt sind die Unzulänglichkeiten eines nachträglichen Rechtsschutzes möglichst weitgehend auszugleichen.[174]

Aus diesem Grund ist bei Durchsuchung und Beschlagnahme die richterliche Intervention und Prüfung keine bloße Formsache.[175] Alle staatlichen Organe sind verpflichtet, dafür Sorge zu tragen, dass der Richtervorbehalt als Grundrechtssicherung praktisch wirksam wird.[176] Wie das *BVerfG* bereits in der Entscheidung von 2001 erklärt hat, sind dafür die Ermittlungsbehörden verpflichtet, vollständige Informationen auf ihrer Seite über den Sachstand den Ermittlungsrichtern zu erbringen,[177] hierauf ist jeder Ermittlungsrichter verpflichtet, sich die notwendige Zeit für die Prüfung eines Antrags der Durchsuchung und Beschlagnahme zu nehmen und sich Kenntnis von der Sache sowie das erforderliche Fachwissen zu verschaffen. Insbesondere den für die Organisation der Gerichte und für die Rechtsstellung der dort tätigen Ermittlungsrichter zuständigen Organen der Länder und des Bundes ist die Pflicht aufgelegt, die Voraussetzungen für eine richterliche, tatsächlich wirksame präventive Kontrolle zu schaffen; etwa eine entsprechende Geschäftsverteilung, ausreichende personelle und sächliche Ausstattung des Gerichts (z. B. ein nächtlicher Bereitschaftsdienst[178]) sowie Aus- und Fortbildungsmöglichkeiten.[179] Erst dadurch kann das Gericht in eigener Verantwortung sorgfältig prüfen, ob die beantragte Durchsuchung oder Beschlagnahme den Eingriffsvoraussetzungen einschließlich der Beschränkungen nach dem Grundsatz der Verhältnismäßigkeit entspricht.[180]

---

[173] *BVerfGE* 20, 162, 224; 42, 212, 220; 96, 44, 51; 103, 142, 151 [Rn. 29]; NJW 2009, 2516, 2517 [Rn. 22]; 2015, 1585, 1586 [Rn. 25]; *Roxin*, StV 1997, 654; *Wohlers*/*Jäger*, SK-StPO, § 105 Rn. 16.

[174] *Wohlers*/*Jäger*, SK-StPO, § 98 Rn. 6; dazu *Park*, § 3 Rn. 471: „*dass … ein nachträglicher Rechtsschutz die bereits eingetretenen Grundrechtsbeeinträchtigungen in aller Regel nicht oder nur unvollständig beseitigen könnte*"; vgl. *BVerfGE* 139, 245, 266 [Rn. 59]: eine teilweise Kompensation struktureller Rechtsschutzdefizite.

[175] Vgl. *BVerfGE* 57, 346, 355; 139, 245, 266 [Rn. 61]; NJW 2009, 2516, 2517 [Rn. 21]; *Burhoff*, StraFo 4/2005, 140, 143 a. E.; *Wohlers*/*Jäger*, SK-StPO, § 105 Rn. 17.

[176] *BVerfGE* 103, 142, Tenor 2 und 156 [Rn. 41]; 139, 245, 267 [Rn. 62].

[177] Vgl. *Wohlers*/*Jäger*, SK-StPO, § 105 Rn. 15; dazu *Griesbaum*, KK-StPO, § 162 Rn. 19a: Vorlegung des die Ermittlungsergebnisse vollständig wiedergebenden Aktenmaterials.

[178] Vgl. *BVerfGE* 103, 142, 156 [Rn. 41]; 139, 245, 267 f. [Rn. 64]; NJW 2004, 1442.

[179] *BVerfGE* 103, 142, 152 f. [Rn. 30]: Sie können nicht allein durch den jeweils zuständigen Richter erfüllt werden; 139, 245, 267 f. [Rn. 62 – 65] und 280 [Rn. 98]: Geschäftsordnungs- und Vertretungsregelungen, die eine rechtzeitige Entscheidung über den Durchsuchungsantrag regelmäßig gewährleisten; vgl. für heimliche Überwachungsmaßnahmen 125, 260, 338 [Rn. 249]; 141, 220, 275 f. [Rn. 118].

[180] *BVerfGE* 57, 346, 355; 103, 142, 151 [Rn. 29]; NJW 2009, 2516, 2516 f. [Rn. 21]; 2015, 1585, 1586 [Rn. 24]; vgl. 96, 44, 51 [Rn. 24]: „*Der Richter darf die Durchsuchung nur anordnen, wenn er sich … überzeugt hat, daß die Maßnahme verhältnismäßig ist.*"

b) Form

Für die richterliche Durchsuchungs- und Beschlagnahmeanordnung wird anders als im Fall des Haftbefehls (vgl. § 114 Abs. 1 StPO) im Gesetz keine bestimmte Form vorgesehen. Nach h. M. und Rspr. sollte sie grundsätzlich stets schriftlich abgefasst und erlassen werden, doch sie darf in Eilfällen zur Vollstreckung (vgl. § 36 Abs. 2 S. 2 StPO) – ausnahmsweise – wenn möglich durch Telefax oder E-Mail[181] oder, wenn nicht möglich, auch (fern)mündlich getroffen werden.[182] Der nicht schriftlich fixierte Beschluss kann die Voraussetzungen und Grenzen der Maßnahmen nicht klar darlegen und wird auch später kaum angemessen messbar und kontrollierbar bleiben, wodurch die Möglichkeit eines wirksamen Rechtsschutzes (vgl. Art. 19 Abs. 4 GG) erheblich eingeschränkt wird.[183] Mit Blick auf den Sinn und Zweck des Richtervorbehalts muss somit ein behördlicher Antrag auf Erlass einer Anordnung der Durchsuchung und Beschlagnahme grundsätzlich schriftlich gestellt werden und auch eine richterliche Anordnung muss grundsätzlich mit einem schriftlichen Beschluss i. V. m. ausreichender Begründung ergehen.[184] In Eilfällen, in denen der Untersuchungszweck durch die mit der schriftlichen Abfassung des Antrags und des Beschusses der Anordnung verbundene Verzögerung gefährdet werden könnte, kann aber die Ermittlungsbehörde und der Ermittlungsrichter (fern)mündlich die Durchsuchung und Beschlagnahme beantragen und anordnen („Eilrichter"), wobei dies wegen der Gefahr des Leerlaufs der Kontroll- und Begrenzungsfunktion des Richtervorbehalts[185] stets eindeutig der schriftlichen Anordnung nachstehen muss.[186] Die nicht schriftliche Anordnung eines Richters kann in Ausnahmefällen nur nach

[181] Vgl. *LG Mühlhausen* wistra 5/2007, 195.

[182] *BVerfGE* 20, 162, 223 [Rn. 146]: „*Die Rechtsstaatlichkeit gebietet zunächst, dass ein Durchsuchungsbefehl grundsätzlich schriftlich abzusetzen ist*" und 227 [Rn. 155]: aufgrund des § 107 Abs. 1 Hs. 1 StPO; 103, 142, 154 [Rn. 34]: die – i. d. R. schriftliche – richterliche Durchsuchungsanordnung; 139, 245, 270 [Rn. 71]: eine richterliche Eilentscheidung; für den Ausnahmecharakter der (fern)mündlichen Durchsuchungsanordnung, BeckRS 2007, 25604; *BGH* 2005, 1060, 1061 [Tz. d)]; *LG Mühlhausen* wistra 5/2007, 195, 196: aus § 34 StPO; *Bruns*, KK-StPO, § 105 Rn. 3; *Burhoff*, StraFo 4/2005, 140, 142: „*Zwar sollte und wird der Ermittlungsrichter i. d. R. schriftlich entscheiden*"; M-G/*Schmitt*, StPO, § 98 Rn. 8, § 105 Rn. 3; *Park*, § 2 Rn. 64, § 3 Rn. 468; *Wohlers*, SK-StPO, § 105 Rn. 31.

[183] *Park*, § 2 Rn. 64: auch *LG Mühlhausen* wistra 5/2007, 195, 196.

[184] *BVerfGE* 20, 162, 227 [Rn. 156]: Der schriftliche Durchsuchungsbeschluss sollte die Regel sein; *LG Mühlhausen* wistra 5/2007, 195; *Park*, § 2 Rn. 64; *Wohlers*/*Jäger*, SK-StPO, § 98 Rn. 14, § 105 Rn. 29.

[185] Vgl. *Wohlers*/*Jäger*, SK-StPO, § 98 Rn. 14, § 105 Rn. 29.

[186] Zust. *Park*, § 2 Rn. 64 und 91; *Wohlers*/*Jäger*, SK-StPO, § 98 Rn. 14; vgl. *BGH* NJW 2005, 1060, 1061 [Tz. d)]: Ein fernmündlicher Antrag auf die Durchsuchung und eine fernmündliche Gestattung der Durchsuchung genügen in Eilfällen den formellen Anforderungen an einen richterlichen Durchsuchungsbeschluss i. S. des § 105 Abs. 1 StPO und die (fern)mündliche Einholung richterlicher Anordnung ist mit einem effektiven Rechtsschutz konformer als die Wahrnehmung der Eilkompetenz durch die Ermittlungsbehörde (diese wird allenfalls mündlich getroffen; vgl. unten 2. d)).

einer sehr sorgfältigen Prüfung zugelassen werden,[187] und daher ist sie zur Gewährleistung nachträglicher Überprüfbarkeit schriftlich zu fixieren, zu begründen und zu den Ermittlungsakten zu nehmen (Dokumentations- und Begründungspflichten).[188] Danach hat der die Anordnungen erlassende Ermittlungsrichter sofort oder mindestens innerhalb von 1 – 2 Tagen einen schriftlichen regulären Beschluss zu erstellen und ihn der Ermittlungsbehörde zu übermitteln, und er ist zu den Ermittlungsakten zu bringen. Die Auferlegung dieser strikten Dokumentations- und Begründungspflicht für die richterlichen Anordnungen in nicht schriftlicher Form entspricht semantisch dem Urteil über „Gefahr im Verzug" für die nichtrichterliche Durchsuchungsanordnung des *BVerfG* vom 20. Februar 2001 (vgl. unten 2. b) und d)). Trotz alledem sollten die richterlichen „Beschlagnahme"-Anordnungen dann in (fern)mündlicher Form i. d. R. unzulässig sein, soweit „Papiere" einschließlich der EDV-Anlagen durch die Durchsicht nach § 110 StPO, insb. vorläufige Sicherstellung, zu beschlagnahmen sind (vgl. unten III. 1. c)).

c) Richterlicher Beschluss

Der Sinn und Zweck des Richtervorbehalts wird nur dann erreicht, wenn der Richter die Voraussetzungen der Durchsuchung- und Beschlagnahmeanordnung und sorgfältig prüft und in konkreten Fall nach umfassender Abwägung den Rahmen, die Grenzen und das Ziel der Maßnahme definiert.[189] Der Schutz der Privatsphäre des Betroffenen darf nicht allein dem Ermessen der mit der Durchführung der Anordnung beauftragten Beamten überlassen bleiben.[190] Aus diesem Grund ist der gerichtliche Durchsuchungs- und Beschlagnahmebeschluss keine Formsache,[191] und er erfüllt eine rechtstaatliche Begrenzungsfunktion, so wird es von dem Richter verlangt, der Abfassung des Beschlusses besondere Aufmerksamkeit zu schenken.[192] Diesbezüglich stellt sich die Frage, inwieweit eine Beschreibung der Gegenstände der Durchsuchung und Beschlagnahme erforderlich ist (vgl. unten aa) und bb)), und

[187] Vgl. *BVerfGE* 139, 245, 271 [Rn. 71]; *BGH* NJW 2005, 1060, 1061 [Tz. d)].

[188] *BVerfGE* 139, 245, 271 [Rn. 71]: Insofern bestehen keine verfassungsrechtlichen Bedenken; auch BeckRS 2007, 25604; *BGH* NJW 2005, 1060; *LG Tübingen* NStZ 2008, 589, 591 [Rn. 9]: Dokumentierung von Dringlichkeitsgründen; M-G/*Schmitt*, StPO, § 98 Rn. 8 und dazu § 105 Rn. 3: Dokumentierung von Eilbedürftigkeit; *Park*, § 2 Rn. 67 und § 3 Rn. 468; *Roxin*/*Schünemann*, § 35 Rn. 8. Diese nicht schriftlichen Durchsuchungs- und Beschlagnahmeanordnungen müssen etwa (hand-)schriftlich, auf einem Tonträger oder durch automatische Speicherung auf E-Mail-Server fixiert werden (*Park*, § 2 Rn. 66). Dabei ist die Dokumentation auch durch einen von der Polizei erstellten Vermerk möglich, jedoch führt auch diese unzureichende Dokumentation nicht zu einem Beweisverwertungsverbot (*BGH* NJW 2005, 1060: bei der telefonischen richterlichen Durchsuchungsanordnung).

[189] *BVerfGE* 103, 142, 151; *Burhoff*, StraFo 4/2005, 140, 143 f.; *Wohlers*/*Jäger*, SK-StPO, § 105 Rn. 17.

[190] *BVerfGE* 42, 212, 220 [Rn. 29]; NJW 2009, 2516, 2517 [Rn. 22]; vgl. 20, 162, 224 [Rn. 147].

[191] Vgl. *Michalke*, StraFo 3/2014, 89, 89 [Tz. a)].

[192] *BVerfGE* 20, 162, 227 [Rn. 156].

ob in den Beschluss daneben auch die Angaben über die Verhältnismäßigkeit der Maßnahmen und die Art und Weise ihrer Durchführung aufgenommen werden sowie in welchem Umfang sie ausgeführt werden sollten (vgl. unten cc)). Zudem wird auch geprüft, ob die in der Praxis häufig erlassenen Durchsuchungsanordnungen i. V. m. einer Beschlagnahmeanordnung rechtmäßig sind (vgl. unten dd)).

aa) Durchsuchungsobjekt

Durchsuchungsobjekte sind nach h. M. ungeachtet des Wortlauts der §§ 102, 103 StPO eine Wohnung und andere Räume des Verdächtigen und des Unverdächtigen sowie ihre Person und die ihnen gehörenden Sachen.[193] Sie müssen in den Durchsuchungsbeschluss so detailliert beschrieben werden, dass er seine Begrenzungsfunktion wirksam entfalten kann.[194] Das heißt, sie müssen so weit konkretisiert werden, dass weder bei dem Betroffenen noch bei dem die Durchsuchung vollziehenden Beamten Zweifel über die zu suchenden – und zu beschlagnahmenden – Gegenstände entstehen können.[195] Dabei müssen die „anderen Räume" – neben der Wohnung – genau bezeichnet werden.[196] Hingegen ist dies bei den „Sachen" nicht der Fall. Häufig wird nämlich eine genaue Bezeichnung des Beweismaterials, auf das die Durchsuchung gerichtet ist, nicht möglich sein[197] und zum Zeitpunkt des Erlasses des Beschlusses wird es zumeist schwierig sein, die Sachen konkret zu beschreiben.[198] Trotzdem müssen im Durchsuchungsbeschluss die Art und der vorgestellte Inhalt der zu suchenden Beweismittel so genau bezeichnet werden, wie es nach Lage der Dinge geschehen kann.[199] Sie sind zumindest „nach Art und Inhalt" näher zu spezifizieren (eine gattungsmäßige Bestimmung).[200] Dabei sind die Sachen ggf. in Form bei-

---

[193] *Bruns*, KK-StPO, § 102 Rn. 7 und § 103 Rn. 3; M-G/*Schmitt*, StPO, § 102 Rn. 7 ff. und § 103 Rn. 3; *Park*, § 2 Rn. 78 und 117 f.; *Wohlers*/*Jäger*, SK-StPO, § 103 Rn. 7.

[194] *Park*, § 2 Rn. 78; vgl. *BVerfG* BeckRS 2004, 22487 und NStZ-RR 2005, 203, 204: eine angemessene rechtsstaatliche Begrenzung der Durchsuchung.

[195] *BGH* NStZ 2002, 215, 216 [Rn. 3]; auch *Burhoff*, StraFo 4/2005, 140, 144 f.

[196] M-G/*Schmitt*, StPO, § 105 Rn. 5; vgl. *BVerfG* NJW 1992, 551: „*Ein Durchsuchungsbeschluß, der … und die neben der Wohnung zu durchsuchenden ‚anderen Räume' nicht bezeichnet, genügt nicht den verfassungsrechtlichen Anforderungen aus Art. 13 Abs. 1 und Art. 2 Abs. 1 und dem Rechtsstaatsprinzip des GG.*" Zum anderen ist bei der Durchsuchung zum Unternehmensserver diese örtliche Eingrenzung häufig unmöglich oder unnötig, weil dabei der gesamte Server potentielles Durchsuchungsgebiet ist (*Hiéramente*, wistra 11/2016, 432, 435).

[197] *BVerfGE* 42, 212, 221 [Rn. 32].

[198] *Park*, § 2 Rn. 79. Die Datenträger und die informationstechnischen Systeme, die bei der Durchsuchung der Wohnung oder der Person aufgefunden werden, gehören als die Sachen i. S. d. § 102 StPO zu den Durchsuchungsobjekten, auch wenn sie im Beschluss nicht ersichtlich angegeben werden (vgl. *BVerfGE* 113, 29, 60 [Rn. 132]).

[199] *BVerfGE* 20, 162, 224 [Rn. 148]; BeckRS 2004, 22487; NStZ-RR 2005, 203, 204; *Burhoff*, StraFo 4/2005, 140, 144; vgl. *Wohlers*/*Jäger*, SK-StPO, § 105 Rn. 20: möglichst konkret.

[200] *BVerfG* NJW 2003, 2669; *BGH* NStZ 2002, 215, 216 [Rn. 3]; *Burhoff*, StraFo 4/2005, 140, 145; M-G/*Schmitt*, StPO, § 105 Rn. 5; *Wohlers*/*Jäger*, SK-StPO, § 105 Rn. 21; abw.

spielhafter Angaben oder durch die Verwendung von Oberbegriffen zu beschreiben.[201] Auch in diesen Fällen muss allerdings mindestens die Vornahme einer Einzelfallprüfung erkennbar und daher eine angemessene Begrenzung der Durchsuchung auch möglich sein. In dieser Hinsicht ist eine umfassende Bezeichnung wie „sämtliche Gegenstände, die den Tatvorwurf betreffen", „Schriftstücke und sonstige Gegenstände, die als Beweismittel von Bedeutung sein könnten" oder „sämtliche ihm gehörende Sachen (Unterlagen)" oder eine Aufzählung aller denkbaren Unterlagen nicht ausreichend.[202] Bei der Bestimmung der zu durchsuchenden Sachen ist die Verwendung von Ausdrücken wie sämtlich, all, pauschal, komplett, sonstig, insbesondere etc., die den Durchsuchungsbeamten keine Mindestgrenzen für den Umfang der Durchsuchung setzen, nicht zulässig.

Im Rahmen der Durchsuchung von informationstechnischen Systemen und darauf gespeicherten Daten ist die Art und Weise ihrer Durchführung (vgl. unten cc)), insb. vorläufige Sicherstellung nach § 110 StPO zur Trennung von Daten nach Verfahrensrelevanz, von Bedeutung (vgl. unten III.).

bb) Zu beschlagnahmende Gegenstände

Nur beweiserhebliche Informationen dürfen beschlagnahmt werden (potenzielle Beweisbedeutung).[203] Im richterlichen Beschlagnahmebeschluss sind – wie bei der Durchsuchung – die zu beschlagnahmende Gegenstände so genau zu bezeichnen, dass keine Zweifel über ihren Umfang weder für den Betroffen noch für den die Anordnung vollziehenden Beamten entstehen.[204] Der Grad der dabei geforderten

Hiéramente, wistra 11/2016, 432, 433: Weil die Möglichkeiten einer gattungsmäßigen Eingrenzung bei der Durchsuchung nach § 103 StPO Risiken der Sicherstellung sämtlicher Daten bergen, ist dabei zwangs1äufig ein Mehr an Präzision vorzuweisen. Etwa Koffer, Taschen oder auch ein Pkw, die in zu durchsuchenden Wohnungen oder Räumen vorhanden sind, können im richterlichen Durchsuchungsbeschluss mit dem Zusatz „sowie der ihm gehörenden Sachen" umfasst werden (*Wohlers/Jäger*, a. a. O. Rn. 23a).

[201] M-G/*Schmitt*, StPO, § 105 Rn. 5; *Wohlers/Jäger*, SK-StPO, § 105 Rn. 21.

[202] *Burhoff*, StraFo 4/2005, 140, 145; *Park*, § 2 Rn. 79; *Wohlers/Jäger*, SK-StPO, § 105 Rn. 22. Dies gilt auch dann, wenn die gesuchten Gegenstände durch die Verwendung des Wortes „insbesondere" eingegrenzt sind (*LG Berlin*, NStZ 2004, 571, 573 [Rn. 12 f.]).

[203] Nach h. M. müssen im richterlichen Beschlagnahmebeschluss auch die Umstände, Anlass/Gründe zur Annahme dieser Bedeutung angegeben werden (*OLG Düsseldorf* StV 1983, 407; *LG Bielefeld* StraFo 3/2013, 114; *Park*, § 3 Rn. 483; *Roxin/Schünemann*, § 34 Rn. 12; *Wohlers/Greco*, SK-StPO, § 98 Rn. 20). Es braucht aber – zum Zeitpunkt der Anordnung bzw. Durchführung der Beschlagnahme – noch nicht festzustehen, für welche Beweisführung ein Gegenstand im Einzelnen in Betracht kommt (*LG Bielefeld*, a. a. O.; M-G/*Schmitt*, StPO, § 94 Rn. 6; *Park*, a. a. O.). Laut *Park* werden aber in der Praxis diese Umstände – die von den Ermittlungsbehörden vielleicht für eindeutig gehalten werden – in dem Beschlagnahmebeschluss keinesfalls ausgeführt (*Park*, a. a. O.).

[204] *BVerfG* NJW 1992, 551, 552; *OLG Koblenz* NStZ 2007, 285, 286 [Rn. 3]; *LG Bonn* StraFo 2/1998, 53; *LG Chemnitz* wistra 4/1999 154; *LG Koblenz* StV 2001, 501, 502; *LG Hildesheim* StraFo 3/2007, 114, 115; *LG Essen* wistra 2/2010 78, 79 f.; *Kemper*, wistra 5/2006, 171, 172; *Park*, § 3 Rn. 481; *Wohlers/Greco*, SK-StPO, § 98 Rn. 18. Andernfalls würde die

Konkretisierung ist strenger als bei den Durchsuchungsobjekten, die zumindest ihrer Gattung nach bestimmt werden müssen. Eine Beschlagnahmeanordnung muss sich auf konkrete und zweifelsfrei individualisierbare Einzelgegenstände beziehen.[205] Genügt die Beschlagnahmeanordnung des AG nicht der Voraussetzung dieser Genauigkeit, so ist sie rechtsstaatlichen Grundsätzen zuwider und daher unwirksam.[206] Demzufolge hat sie lediglich die Bedeutung einer Richtlinie für die Durchsuchung, wenn sie i. V. m. einem Durchsuchungsbeschluss erlassen wird (vgl. unten dd)). Dies gilt insb. für die pauschale Beschlagnahmeanordnung derart, dass die/alle bei einer Durchsuchung gefundenen Gegenstände als Beweismittel beschlagnahmt werden sollen (sog. „allgemeine Beschlagnahmeanordnung“).[207] In diesem Fall wird eine Trennung durch die inhaltliche Überprüfung gefordert. Daher ist eine umfangreiche Erfassung durch die Verwendung von Oberbegriffen oder eine beispielhafte Aufzählung aller in Betracht kommenden Unterlagen nicht zur Konkretisierung der Beschlagnahmeanordnung geeignet.[208] Bei der Beschlagnahme erheblicher Mengen an Unterlagen und Dateien – insb. in Wirtschafts- und Steuerstrafverfahren – dürfen aber die Anforderungen zur konkreten Bezeichnung der zu beschlagnahmenden Gegenstände freilich nicht so streng gehen, dass die praktische Handhabbarkeit von Beschlagnahmen tatsächlich ausgehebelt wird.[209] So ist es praktisch nicht möglich, jede einzelne Unterlage oder Datei im Beschluss konkret zu benennen, und eine gewisse Unbestimmtheit ist in Kauf zu nehmen.[210] Bei der Konkretisierung zu beschlagnahmender Schriftstücke oder Dateien handelt es sich im Ergebnis darum, einen gerechten Ausgleich zwischen Praktikabilitätserfordernissen in der Praxis und der rechtsstaatlichen Begrenzungsfunktion zum Datenschutz zu schaffen, und hierbei bedarf es einzelfallbezogener Erwägungen.

Entscheidung, welche Gegenstände unter die richterliche Beschlagnahmeordnung fallen, nicht dem Richter obliegen, sondern den Strafverfolgungsbehörden (*BVerfG* a. a. O.; BeckRS 2004, 20407; *OLG Koblenz* a. a. O. [Rn. 4]; *Kemper*, a. a. O.).

[205] *LG Hildesheim* StraFo 3/2007, 114, 115; vgl. *BVerfG* NJW 2003, 2669, 2670.

[206] *BVerfG* NJW 1992, 551, 552; *Park*, § 3 Rn. 481; *Roxin*/*Schünemann*, § 34 Rn. 12; *Wohlers*/*Greco*, SK-StPO, § 98 Rn. 18. Daher ist dieser Beschlagnahmebeschluss aufzuheben (*BVerfG* a. a. O.).

[207] *BVerfG* NJW 1992, 551, 552; *Kemper*, wistra 5/2006, 171, 172; M-G/*Schmitt*, StPO, § 98 Rn. 9; *Park*, § 3 Rn. 481; *Roxin*/*Schünemann*, § 34 Rn. 12; *Wohlers*/*Greco*, SK-StPO, § 98 Rn. 18. Hier kann die Begrenzungsfunktion des Beschlagnahmebeschlusses nicht wirksam entfaltet werden (*Park*, a. a. O.).

[208] *LG Bonn* StraFo 2/1998, 53; *LG Oldenburg* StV 1994, 178, 179: beispielhafte Aufzählung von denkbaren Geschäftsunterlagen; *Park*, § 3 Rn. 481. Dies gilt auch für den Zusatz von „insbesondere …“; denn er räumt unter Rückgriff auf die bloße Beispielhaftigkeit der genannten Gegenstände den Ermittlungsbehörden einen unzulässigen Ermessensspielraum ein und höhlt somit die Begrenzungsfunktion des Beschlagnahmebeschlusses aus (*LG Chemnitz* wistra 4/1999 154, 154 f.; *Park*, a. a. O.; *Wohlers*/*Greco*, SK-StPO, § 98 Rn. 19).

[209] *Park*, § 3 Rn. 481.

[210] *Kemper*, wistra 5/2006, 171, 172 f.; M-G/*Schmitt*, StPO, § 98 Rn. 9; *Park*, § 3 Rn. 481.

cc) Verhältnismäßigkeit der Maßnahmen sowie Art und Weise ihrer Durchführung

Nach der Literatur ist die Angabe der Verhältnismäßigkeit der Maßnahmen in der Begründung des richterlichen Beschlusses der Durchsuchung und Beschlagnahme praktisch schwerlich anzutreffen,[211] und dies wird erst recht nur als frommer Wunsch verstanden.[212] Dies widerspricht jedoch eindeutig der Stellungnahme des *BVerfG* und verstößt gegen die Rechtsstaatlichkeit.[213] Die Durchsuchung und Beschlagnahme als Eingriffe in die grundrechtlich geschützte Lebenssphäre müssen verhältnismäßig sein[214] und dies ist nicht nur bei der Durchführung der Maßnahmen, sondern auch beim Erlass ihres Beschlusses zu beachten.[215] Dies kann nur dadurch gewährleistet werden, dass bei Erlass des Beschlusses dem Ermittlungsrichter eine Verpflichtung zur entsprechenden Ausführung der Verhältnismäßigkeit der Maßnahmen in der Begründung auferlegt wird (Begründungszwang):[216] insb. wenn die Verhältnismäßigkeit nicht klar ist oder wenn grundrechtlich besonders geschützte Bereiche eingegriffen werden.[217] Im Einzelfall ist die Verhältnismäßigkeit wenigstens dann mit konkreten Anhaltspunkten zu begründen, wenn Redaktionsräume durchsucht[218] oder sämtliche Daten einer EDV-Anlage gesichert werden müssen.[219] Diesbezüglich hat das *BVerfG (1. Kammer des Ersten Senats)* im Jahr 2010 bei der Entscheidung über die Verfassungsbeschwerde gegen die Durchsuchungsanordnung der Geschäftsräume eines Rundfunksenders wie folgt ausgeführt:

> „Auch sind umfangreiche Ausführungen zur Verhältnismäßigkeit weder im Durchsuchungsbeschluss noch in der Beschwerdeentscheidung grundsätzlich und stets von Verfassungs wegen geboten. Aus grundrechtlicher Sicht ist es aber nicht mehr hinnehmbar, dass dem angegriffenen Durchsuchungsbeschluss keinerlei Erwägungen zur Verhältnismäßig-

[211] *Ciolek-Krepold*, Rn. 53; *Park*, § 2 Rn. 84, § 3 Rn. 487; *Wohlers/Jäger*, SK-StPO, § 105 Rn. 24.

[212] *Park*, § 3 Rn. 487.

[213] Zust. *Park*, § 2 Rn. 84 und § 3 Rn. 487: bedenklich; *Wohlers/Jäger*, SK-StPO, § 105 Rn. 24.

[214] *BVerfGE* 113, 29, 53; 115, 166, 197; 124, 43, 66 [Rn. 78]; *BGH* NJW 2010, 1297, 1298 [Rn. 15].

[215] *Park*, § 2 Rn. 84; *Wohlers/Jäger*, SK-StPO, § 105 Rn. 24; insb. *BVerfGE* 115, 166, 198 [Rn. 120 f.] und 124, 43, 67 [Rn. 80 f.].

[216] *Park*, § 2 Rn. 84; *Ciolek-Krepold*, Rn. 72. Dass die richterliche Durchsuchungs- und Beschlagnahmeanordnung dem Verhältnismäßigkeitsgrundsatz hinreichend Rechnung trägt, muss aus den Angaben in der Begründung des Beschlusses abgeleitet werden können (*Park*, a. a. O.; *Wohlers/Jäger*, SK-StPO, § 105 Rn. 24). Nach der Entscheidung des *BGH* genügen allgemeine formelhafte Wendungen wie das „bisherige Ermittlungsergebnis" zur Begründung gerichtlicher Entscheidungen grundsätzlich nicht (NStZ-RR 2009, 142, 143).

[217] *Wohlers/Jäger*, SK-StPO, § 98 Rn. 20, § 105 Rn. 24; vgl. *Roxin*, StV 1997, 654: in Anlehnung an § 114 Abs. 3 StPO.

[218] Vgl. *BVerfG* NJW 2005, 965.

[219] *Kemper*, wistra 3/2008, 96, 99 [Fn. 43]: Dabei sind Anführungen wie, „dass der Verdacht auf versteckte oder gelöschte Dateien besteht" oder „dass der Nutzer des Gerätes ein EDV-Spezialist ist" erforderlich.

keit der Maßnahme zu entnehmen sind, obgleich sich Ausführungen hierzu einerseits wegen der ersichtlich geringen Schwere der in Rede stehenden Tat und andererseits wegen der mit einer Durchsuchung der Räume einer Rundfunkanstalt regelmäßig einhergehenden Beeinträchtigungen der Rundfunkfreiheit geradezu aufdrängten."[220]

Sind die Art und Weise der Durchführung der Beschlagnahme und Durchsuchung im richterlichen Beschluss anzugeben? Heutzutage ist dies insb. i. R. d. Maßnahmen zu EDV-Anlagen umstritten. Da das Ermittlungsverfahren von StA zu führen oder zu leiten ist (vgl. §§ 152, 160 StPO) und auch die Art und der Umfang der Durchsuchung und Beschlagnahme vorab nicht vollständig zu planen sind,[221] kann allerdings ihre Ausgestaltung nicht umfänglich mit dem Gericht bestimmt werden. Mit Blick auf den Sinn und Zweck des Richtervorbehalts, die Grundrechte durch vorbeugende Kontrolle zu schützen, hat aber der Richter i. d. R. die wesentlichen Entscheidungen hinsichtlich des Grundrechtseingriffs selbst zu treffen und daher ist es nicht angebracht, dass im richterlichen Beschluss die Art und Weise der Durchsuchung und Beschlagnahme der EDV-Anlage völlig beiseitegelassen werden.[222] Wie er vor allem im Beschluss anordnen kann, hinsichtlich der Verhältnismäßigkeit dem Betroffenen die Möglichkeit zu bieten, die Beschlagnahme von Originalschriftstücken durch eine Herausgabe von Fotokopien abzuwenden,[223] ist es auch hierbei anzugeben, dass die Beschlagnahme durch die Erstellung von Kopien erfolgen muss, es sei denn, die Sicherung des Originals ist erforderlich oder die Herstellung der Kopien wird behindert. Außerdem hat der Richter – insb. in Wirtschafts- und Steuerstrafsachen – zu einer inhaltlichen Prüfung zur Trennung verfahrensrelevanter von unerheblichen Daten grundsätzlich im Beschluss eine vorläufige Sicherstellung und die Durchsicht nach § 110 StPO anzuordnen und zugleich eine Suchbegriffsliste zu erstellen, um die zu durchsehenden und zu beschlagnahmenden Dateien herauszufiltern (vgl. dazu eingehend unten III. 2. a) bb)). Nach der Rspr. des *BVerfG* wird jedoch dem Richter keine Pflicht auferlegt, im Beschluss Angaben zu einer solchen Art und Weise zu machen.[224]

dd) Durchsuchungsanordnung i. V. m. einer Beschlagnahmeanordnung

In der Praxis wird die Beschlagnahme zumeist mit der Durchsuchung angeordnet, indem die Beschlagnahmeanordnung mit dem Durchsuchungsbeschluss verbunden wird (sog. „Kombi-Beschluss").[225] Nach den Rspr. und h. M. ist dies zulässig.[226] In

[220] *BVerfG* NJW 2011, 1859, 1862 [Rn. 26]; auch 2011, 1863, 1866 [Rn. 36].

[221] Vgl. *Hiéramente*, wistra 11/2016, 432, 436.

[222] Vgl. *Hiéramente*, wistra 11/2016, 432, 436 f.: Bei einer Unternehmensdurchsuchung nach § 103 StPO sind keine verfahrenstechnischen Gründe ersichtlich, warum sich der Richter in die Art und Weise der (IT-)Durchsuchung nicht einschaltet.

[223] *Park*, § 3 Rn. 487; *Wohlers/Jäger*, SK-StPO, § 98 Rn. 20; vgl. *Ciolek-Krepold*, Rn. 73.

[224] Vgl. *BVerfGE* 113, 29, 55 ff. [Rn. 113 – 120]; 124, 43, 67 ff. [Rn. 80 – 89].

[225] *Graulich*, wistra 8/2009, 299; dazu *Ciolek-Krepold*, Rn. 238: „Koppelung von Durchsuchungs- und Beschlagnahmebeschluss"; *Dauster*, StraFo 6/1999, 188, 188: „antizipierte

der Praxis beantragt zunächst die StA beim Richter den Erlass einer Durchsuchungsanordnung mit der Beschlagnahme der Gegenstände, die zum Zeitpunkt der Durchsuchung voraussichtlich aufgefunden werden, und dann erlässt er dementsprechend den Durchsuchungs- und Beschlagnahmebeschluss in einem und demselben Schriftstück. Auch in diesem Fall sind beide Anordnungen isoliert und bloß in dem einheitlichen Beschluss zusammengefasst.[227] Soweit in dem Beschluss die Voraussetzungen für die beiden Maßnahmen, insb. die Reichweite und Grenzen der Durchsuchung und die Bezeichnung der zu beschlagnahmenden Gegenständen jeweils angemessen angegeben sind, unterliegt diese Vorgehensweise keinen rechtlichen Bedenken.[228] Diesbezüglich ist jedoch meist die Bezeichnung der zu beschlagnahmenden Gegenständen problematisch, die näher zu konkretisieren sind, als die Durchsuchungsobjekte.[229] Auf ein und demselben Schriftstück gilt die Beschlagnahmeanordnung nur dann, wenn die in Beschlag zu nehmenden Gegenstände im Einzelnen so genau bezeichnet werden können und im Beschluss so bezeichnet werden, dass kein Zweifel darüber besteht, ob sie von der Anordnung erfasst sind oder nicht.[230] Eine vorab mit dem Durchsuchungsbeschluss verbundene Anordnung der „Beschlagnahme" wird für unwirksam gehalten, soweit dabei noch keine genaue Konkretisierung der erfassten Gegenstände, sondern nur eine gattungsmäßige Um-

---

Beschlagnahmeanordnung"; *Kemper*, wistra 5/2006, 171, 172: „einheitlicher Durchsuchungs- und Beschlagnahmebeschluss." Dies gilt insb. bei Durchsuchungsbeschlüssen beim Verdächtigen nach § 102 StPO (*Kemper*, a. a. O. [Tz. 2.]). Nach der Meinung von *Kemper* gilt die Anforderung des *BVerfG*, dass im Beschluss der Durchsuchung und Beschlagnahme die gesuchten Beweismittel immer so konkret wie möglich zu bezeichnen sind (vgl. *BVerfGE* 42, 212, 200), nicht für die Beschlagnahme der EDV-Anlage – insb. in Wirtschafts- und Steuerstrafsachen – (a. a. O. 172 f.) und daher führt hierbei der Verzicht auf die Anordnung der Beschlagnahme (der Erlass ausschließlich des isolierten Durchsuchungsbeschlusses) in den meisten Fällen zu unnötigen Problemen, die im Zweifel zulasten einer effektiven Bekämpfung von Straftaten gehen (a. a. O. 173 und 175). Daher ist bei Durchsuchung sowohl nach § 102 als auch nach § 103 StPO (z. B. bei der Bank des Beschuldigten) die Ausfertigung isolierter Durchsuchungsbeschlüsse i. d. R. nicht erforderlich. Dies scheint auf seiner Ansicht zu beruhen, dass die „Mitnahme zur Durchsicht" als nicht in der StPO vorgesehene Maßnahme nicht zulässig und eine Art der „vorgelagerten Beschlagnahme" für eine wirkungsvolle Arbeit der Ermittlungsbehörden ist (*Kemper*, a. a. O. 174 [Fn. 30]; auch wistra 8/2010, 295, 298). Dies steht jedoch in Widerspruch zum Verhältnismäßigkeitsgrundsatz, weil es in der Praxis praktisch immer zu einer Beschlagnahme der gesamten Daten führen würde.

[226] *BVerfG* NJW 1992, 551, 552; NJW 2003, 2669, 2670; BeckRS 2009, 36277; *BGH* NJW 2000, 84, 85; *OLG Koblenz* NStZ 2007, 285; *LG Bonn* StraFo 2/1998, 53; *LG Hildesheim* StraFo 3/2007, 114, 115; *LG Bielefeld* wistra 3/2008, 117, 119; *LG Essen* wistra 2/2010 78, 79 f.; *Dauster*, StraFo 6/1999, 188, 188; *Greven*, KK-StPO, § 98 Rn. 2; *Kemper*, wistra 5/2006, 171, 172; *Park*, § 3 Rn. 469, 488.

[227] *Park*, § 3 Rn. 488; vgl. *Kemper*, wistra 5/2006, 171, 172 am Anfang.

[228] Vgl. *Park*, § 3 Rn. 488.

[229] Vgl. *Park*, § 3 Rn. 488 a. E.; a. A. *Kemper*, wistra 8/2010, 295, 298.

[230] *BVerfG* NJW 1992, 551, 552; *LG Hildesheim* StraFo 3/2007, 114, 115; *LG Essen* wistra 2/2010 78, 80.

schreibung erfolgt,[231] und sie hat lediglich die Bedeutung einer Richtlinie für die Durchsuchung.[232] In diesem Fall könne nach den Rspr. und h. M. der von der Durchsuchung Betroffene gegen diese Sicherstellung, nämlich Beschlagnahme, nach § 98 Abs. 2 S. 2 StPO – entsprechend – die richterliche Bestätigung beantragen,[233] weil die Gegenstände ohne richterliche Anordnung i. S. d. § 98 Abs. 2 S. 1 StPO beschlagnahmt worden sei.[234]

Bei der Sicherstellung von „Papieren bzw. Dateien" in diesem Fall muss aber die „Beschlagnahme" für noch nicht angeordnet gehalten werden. Hier ist die Verbringung der Gegenstände aus dem Gewahrsam des Betroffenen in die Obhut der staatlichen Gewalt aufgrund des einheitlichen Beschlusses, dessen Beschlagnahmeanordnung nicht gültig ist, als „vorläufige Sicherstellung gemäß § 110 StPO" anzusehen. Denn die zu beschlagnahmenden Papiere müssen potenzielle Beweisbedeutung haben, aber, soweit dies vor Ort aus verschiedenen Gründen nicht festzustellen ist, ist die Mitnahme zur Durchsicht nach § 110 StPO stets erforderlich.[235] Die Beschlagnahme, die in der Praxis häufig – zur Umgehung der Anwendung des § 110 StPO – auf Grundlage dieser fehlenden Beschlagnahmeanordnung vorgenommen wird, verstößt daher gegen den Verhältnismäßigkeitsgrundsatz und gegen den Sinn und Zweck der Vorschrift. So stellt eine derartige Verbringung die vorläufige Sicherstellung nach § 110 StPO dar, aber keine Beschlagnahme nach § 94 StPO. Unter dieser Prämisse ist eine richterliche Bestätigung dann entsprechend

[231] *BVerfG* NJW 1992, 551, 552; NStZ 2002, 212, 213 [Rn. 6]; *OLG Koblenz* NStZ 2007, 285, 286 [Rn. 6]; *LG Hildesheim* StraFo 3/2007, 114, 115; *LG Bielefeld* wistra 3/2008, 117, 119; *Graulich*, wistra 8/2009, 299, 300; M-G/*Schmitt*, StPO, § 98 Rn. 9 und 19; *Park*, § 3 Rn. 481. Dabei ersetzt die Durchsuchungsanordnung die entkräftete richterliche Beschlagnahmeanordnung nicht (*Bruns*, KK-StPO, § 105 Rn. 3). In den jüngsten Rspr., bei denen es sich um den Erlass von kombinierten Beschlüssen handelt, wurden die darin enthaltenen Beschlagnahmeanordnungen für nicht wirksam erklärt (*Graulich*, a. a. O.).

[232] *BVerfG* NStZ 2002, 212, 213 [Rn. 6]; NJW 2003, 2669, 2670; BeckRS 2009, 36277; *OLG Koblenz* NStZ 2007, 285, 286 [Rn. 6]; *LG Essen* wistra 2/2010 78, 80; *Graulich*, wistra 8/2009, 299, 300; M-G/*Schmitt*, StPO, § 98 Rn. 9; *Park*, § 3 Rn. 481; *Wohlers*/*Greco*, SK-StPO, § 98 Rn. 19.

[233] *BVerfG* NJW 1992, 551, 552; *BGH-Ermi-Ri* CR 1999, 292; *OLG Koblenz* NStZ 2007, 285, 286 [Rn. 6 f.]; *LG Mühlhausen* wistra 5/2007, 195, 197; *LG Essen* wistra 2/2010 78, 80; *Park*, § 3 Rn. 482; M-G/*Schmitt*, StPO, § 98 Rn. 19; *Wohlers*/*Greco*, SK-StPO, § 98 Rn. 19.

[234] *Park*, § 3 Rn. 482. Die vorgefundenen Beweismittel müssten von den Durchsuchungsbeamten i. d. R. wegen Gefahr im Verzug beschlagnahmt werden (a. a. O.). Insofern hat *Dauster* aber Zweifel daran, dass der Richter in der Praxis diese Beschlagnahmeanordnungen erlässt, um es zu ermöglichen, dass die Polizei vor Ort im Vorgriff auf etwaigen Widerspruch aufgefundene Papiere sofort beschlagnahmt, und dies wäre weder mit § 110 StPO noch mit § 98 Abs. 1 S. 1 StPO zu vereinbaren (StraFo 6/1999, 188, 188 f.: polizeiliche „venia legendi" aufgrund richterlicher Beschlagnahmeanordnung). Diese Verweisung gilt auch noch heute.

[235] Dazu *Graulich*, wistra 8/2009, 299, 300 [Tz. 3.]: Die „vorsorgliche" Beschlagnahme zum Zwecke der Durchsuchung ist unzulässig; a. A. *Kemper*, wistra 8/2010, 295, 298: Da die Mitnahme zur Durchsicht von Papieren durch § 110 StPO nicht zu rechtfertigen ist und eine Art der vorgelagerten Beschlagnahme darstellt, ist es hinzunehmen, dass im Einzelfall unbestimmte Beschlagnahmebeschlüsse erlassen werden.

nach § 98 Abs. 2 S. 1 StPO zu beantragen, wenn die Durchsicht (bzw. Durchsuchung) für längere Zeit fortgesetzt werden sollte, und weiter ist eine Beschlagnahmeanordnung dann nach § 98 Abs. 1 StPO zu beantragen, wenn die vorläufig sichergestellten Papiere nach der Durchsicht beschlagnahmt werden müssen (vgl. ausführlich unten III. 3.).[236]

2. Ausnahmsweise Ausschluss – nichtrichterliche Anordnung

a) Eilkompetenz

Von Polizei und StA kann im Hinblick auf ihre Aufgabe (§§ 160 Abs. 1, 163 Abs. 1 StPO) anders als vom Richter keine strikte Neutralität erwartet werden und sie genießen daher keine Unabhängigkeit[237] und können nur nach einer gerichtlichen Anordnung eine Maßnahme durchführen (Regelzuständigkeit); dies ist eine durch das GG angestrebte Grundkonzeption. Das GG erlaubt jedoch bei Gefahr im Verzug „ausnahmsweise" den Ausschluss richterlicher Einschaltung, weil der Richtervorbehalt die Erreichung des öffentlichen Interesses der Strafverfolgung verhindern kann (Art. 13 Abs. 2 GG).[238] Der Zweck der Eilkompetenz besteht in der Ermöglichung eines schnellen und situationsgerechten Handelns durch die Ermittlungsbehörden.[239] In dieser Hinsicht könnte sie als Mittel verstanden werden, um ein Gleichgewicht zwischen dem Grundrechtsschutz und einer wirksamen Strafverfolgung nach dem Grundsatz der Verhältnismäßigkeit zu erreichen.[240]

In der Vergangenheit war die richterliche Anordnung in der Praxis eher eine Ausnahme.[241] Das *BVerfG* hat jedoch in seiner Entscheidung vom 20. Februar 2001[242] u. a. hervorgehoben, dass die Eilkompetenz auch in der Praxis stets der Ausnahmefall sein müsse.[243] Daraus ergeben sich mehrere Gebote. Staatliche Organe sind zunächst verfassungsrechtlich verpflichtet, dafür Sorge zu tragen, dass der Richtervorbehalt als Grundsatz tatsächlich in der Praxis gültig ist (vgl. oben 1. a)). Die Eilkompetenz der Ermittlungsbehörden ist gegenüber dem Richtervorbehalt

---

[236] Zust. *Graulich*, wistra 8/2009, 299, 300 [Tz. 2.5].

[237] *BVerfGE* 103, 142, 154 [Rn. 34].

[238] *BVerfGE* 103, 142, 155 [Rn. 37 f.]; 139, 245, 270 [Rn. 70].

[239] *BVerfGE* 139, 245, 268 [Rn. 68].

[240] Vgl. *BVerfGE* 103, 142, 154 [Rn. 36]; 139, 245, 268 [Rn. 68].

[241] *Burhoff*, StraFo 4/2005, 140, 141; *Park*, § 2 Rn. 96; *Wohlers/Greco*, SK-StPO, § 98 Rn. 33. Im Schrifttum wurde diese faktische Umkehrung des Regel-Ausnahme-Verhältnisses immer wieder vehement kritisiert, da sie allzu bedenklich ist (*Park*, § 2 Rn. 96; dazu *Krehl*, NStZ 2003, 461: eine Praxis, die offenbar allzu großzügig auf die Einholung einer richterlichen Entscheidung verzichtet hat). Im Rechtsstaat bestimmt das Recht die Praxis und nicht die Praxis das Recht (*BVerfGE* 139, 245, 280 [Rn. 98]).

[242] *BVerfGE* 103, 142 = NJW 2001, 1121.

[243] *Wohlers/Greco*, SK-StPO, § 98 Rn. 33; vgl. *BVerfGE* 103, 142, 153 [Rn. 32 f.]; dazu 139, 245, 269 [Rn. 69]: das Verhältnis liegt an Wortlaut und Systematik des Art. 13 Abs. 2 GG.

nachrangig[244] und dies sollte auch praktisch der Fall sein, sodass die Behörden verpflichtet sind, sich regelmäßig um eine Anordnung des zuständigen Richters zu bemühen.[245] Dann muss der Begriff der Gefahr im Verzug eng interpretiert werden (unten b))[246] und die Eilzuständigkeit ist vorzugsweise der StA zuzuweisen (unten c)). Schließlich muss die Inanspruchnahme der Eilkompetenz einer unbeschränkten gerichtlichen Nachprüfung unterliegen können (unten d)).[247]

b) Voraussetzung – „Gefahr im Verzug"

(1) Dieses Merkmal ist nicht nur wegen des Ausnahmecharakters der nichtrichterlichen Anordnung, sondern auch wegen der grundrechtssichernden Schutzfunktion des Richtervorbehalts eng auszulegen.[248] Die StA und ihre Ermittlungspersonen müssen eine richterliche Anordnung der Durchsuchung und Beschlagnahme veranlassen, sobald sich die Erforderlichkeit der Maßnahme abzeichnet und noch genügend Zeit vorhanden ist.[249] In Ausnahmesituationen, wenn die „zeitliche Verzögerung" wegen eines Versuchs der vorherigen Einholung der richterlichen Anordnung den Erfolg der Maßnahme gefährden würde, sind indes Gefahr im Verzug und darauf beruhende Eilkompetenz anzunehmen, um einen Beweismittelverlust zu verhindern.[250] Die Einschätzung, ob die Voraussetzungen für die Annahme von Gefahr im Verzug im konkreten Fall vorliegen, obliegt zunächst der StA – ggf. auch ihrer Ermittlungsperson – und diese hat sie selbst zu prüfen.[251] Für die Frage, ob dieses Merkmal gegeben ist oder die Ermittlungsbehörden eine richterliche Entscheidung rechtzeitig erreichen können, ist die objektive Prognose von Bedeutung, die zum Zeitpunkt, zu dem die Behörden die Durchsuchung oder Beschlagnahme für erforderlich hielten, die nach dem Stand der Ermittlungen bekannten Tatsachen zugrunde legt,[252] wobei auch darin einzubeziehen ist, dass richterliche Anordnung allein aufgrund mündlich übermittelter Informationen mündlich getroffen werden

---

[244] *BVerfGE* 139, 245, 264 [Rn. 55].

[245] *BVerfGE* 139, 245, 270 [Rn. 70]. Diese Pflicht begrenzt allerdings teilweise ihren Spielraum, das Ermittlungsverfahren nach kriminalistischen und taktischen Erwägungen frei zu gestalten (*BVerfGE* 103, 142, 155 [Rn. 40]; *BGHSt* 51, 285, 292 f. [Rn. 25]).

[246] *BVerfGE* 103, 142, Tenor 1 und 153 [Rn. 33]; 139, 245, 269 [Rn. 69].

[247] *BVerfGE* 103, 142, Tenor 3 und 159 f. [Rn. 53]; 139, 245, 272 f. [Rn. 74 – 76].

[248] *BVerfGE* 103, 142, 153 [Rn. 33]; 139, 245, 269 [Rn. 69]; *BGHSt* 51, 285, 292 [Rn. 25]; *Wohlers*/*Greco*, SK-StPO, § 98 Rn. 33 und § 105 Rn. 39. Freilich darf bei der Bestimmung von „Gefahr im Verzug" der Zweck der Eilkompetenz nicht außer Betracht bleiben (*BVerfGE* a. a. O. 154 [Rn. 35]).

[249] *BVerfG* NStZ 2011, 289, 292.

[250] *BVerfGE* 51, 97, 111 [Rn. 40]; 103, 142, 154 [Rn. 35]; *BGHSt* 51, 285, 288 [Rn. 17]; M-G/*Schmitt*, StPO, § 98 Rn. 6, § 105 Rn. 2; *Park*, § 2 Rn. 91.

[251] *BVerfGE* 139, 245, 269 f. [Rn. 70] und 273 [Rn. 78].

[252] *BGHSt* 51, 285, 289 [Rn. 17]; *Wohlers*/*Greco*, SK-StPO, § 98 Rn. 35, § 105 Rn. 40; *Park*, § 2 Rn. 92.

kann.[253] Die mündliche Einholung richterlicher Anordnung geht stets der Wahrnehmung der Eilkompetenz durch die Ermittlungsbehörde vor (vgl. oben 1. b)). Zur Annahme der Gefahr im Verzug ist somit die Möglichkeit einer (fern)mündlichen richterlichen Anordnung zwingend zu prüfen.[254] In dieser Hinsicht handelt es sich bei Gefahr im Verzug um einen auf eine Prognose abzielende unbestimmten Rechtsbegriff und sie muss sich auf eine nachweisbare konkrete Tatsachenbasis stützen; sie muss also mit Tatsachen bezogen auf den Einzelfall begründet werden.[255] Daher untersteht dieser Begriff einer uneingeschränkten richterlichen Nachprüfung (vgl. unten d)).[256]

Bei „umfassender Beschlagnahme" sämtlicher Dateien oder gesamter Datenträger darf anderseits die Gefahr im Verzug i. S. d. § 98 Abs. 1 S. 1 nicht angenommen werden, obwohl eine „Durchsuchung" wegen Gefahr im Verzug schon durch die Ermittlungsbehörde angeordnet wurde.[257] In diesem Fall ist der Verlust von Beweismitteln nämlich durch die vorläufige Sicherstellung nach § 110 StPO ausreichend zu verhindern (vgl. unten III. 1. c)). Darüber hinaus kann bei Durchsuchung bei Nichtverdächtigen nach § 103 StPO wie etwa Firma, Bank oder TK-Dienstanbieter des Beschuldigten – anders als bei Durchsuchung beim Verdächtigen nach § 102 StPO – in aller Regel die Gefahr im Verzug ausgeschlossen werden.[258] Dies würde freilich nicht gelten, wenn der Beschuldigte stets Zugang zu Datenbeständen Dritter haben und weiter die darauf gespeicherten Daten löschen kann oder wenn diese Dritte später zum Beschuldigten führen können. Wenn die Gefahr eines Beweismittelverlusts etwa durch die Anwendung des § 110 StPO oder die Verwah-

[253] *BVerfGE* 139, 245, 270 f. [Rn. 71].

[254] *BGH* NJW 2005, 1060, 1061; *Park*, § 2 Rn. 64 und 91.

[255] M-G/*Schmitt*, StPO, § 98 Rn. 7; *Park*, § 2 Rn. 92; *Wohlers*/*Greco*, SK-StPO, § 98 Rn. 35, § 105 Rn. 34; auch *Rabe von Kühlewein*, NStZ 2011, 289, 292: ein objektiver Begriff der Erforderlichkeit bezüglich der konkreten Situation; vgl. *BVerfGE* 103, 142, 157 [Rn. 46 f.]. So sind reine Spekulationen, hypothetische Erwägungen oder lediglich auf kriminalistische Alltagserfahrung gestützte, fallunabhängige Vermutungen als Grundlage einer Annahme der Gefahr im Verzug nicht hinreichend und dies gilt auch für die bloßen Möglichkeiten eines Beweismittelverlusts (*BVerfGE* 103, 142, 155 f. [Rn. 39 – 41], 160 [Rn. 54]; 139, 245, 270 [Rn. 70]; *BGHSt* 51, 285, 293 [Rn. 25]; *Park*, a. a. O.).

[256] *BVerfGE* 103, 142, 157 [Rn. 45]; 139, 245, 272 [Rn. 74]; *Wohlers*/*Greco*, SK-StPO, § 98 Rn. 35, § 105 Rn. 39; *Park*, § 2 Rn. 103. Die (endgültige) Konkretisierung des Begriffs „Gefahr im Verzug" ist daher von Verfassungs wegen grundsätzlich Sache der Gerichte und die Spielräume bei seiner Auslegung und Anwendung werden den nichtrichterlichen Organen nicht eröffnet (*BVerfGE* a. a. O. [Rn. 45 f.]).

[257] A. A. *Kemper*, wistra 5/2006, 171, 172: Liegen die Voraussetzungen von Gefahr im Verzug für die Durchsuchung vor, dann werden regelmäßig auch solche für die Beschlagnahme vorliegen.

[258] Vgl. auch *Kemper*, wistra 5/2006, 171, 172. In dieser Hinsicht liegt im Fall der VDS, bei der es sich um die Erhebung der auf dem Server des Providers bereits gespeicherten Verkehrsdaten handelt (vgl. § 100g Abs. 2 StPO), die Eilzuständigkeit wegen Gefahr im Verzug nicht vor (vgl. § 101a Abs. 1 S. 2 StPO).

rungspflicht Dritter nicht begründet wird, soll die Gefahr im Verzug bei der „Beschlagnahme“ in der Auslegung nicht angenommen werden können.

(2) Gefahr im Verzug darf aber nicht durch die Strafverfolgungsbehörden selbst herbeigeführt werden. Daher dürfen diese nicht so lange mit dem Antrag an den Ermittlungsrichter zuwarten, bis die Gefahr eines Beweismittelverlusts tatsächlich eingetreten ist, und damit die von Verfassungs wegen vorgesehene Regelzuständigkeit des Richters unterlaufen.[259] In diesen Fällen wird die Eilzuständigkeit der Ermittlungsbehörden ausgeschlossen. Zur Annahme der Eilkompetenz bedarf es eines Versuchs einer ernsthaften, zumindest telefonischen Kontaktaufnahme mit dem Gericht.[260] Bei der irrtümlichen Annahme von Gefahr im Verzug überschreiten andererseits grundsätzlich die Ermittlungsbehörden ihre Zuständigkeit und die von ihnen angeordnete Durchsuchung und Beschlagnahme ist rechtswidrig.[261] Nach den Rspr. und h. M. ist diese (Eil-)Anordnung aber nicht unwirksam und die dabei aufgefunden und beschlagnahmten Beweismittel sind verwertbar, es sei denn, dass die Gefahr im Verzug willkürlich angenommen wurde oder ein besonders schwerwiegender Fehler vorliegt.[262] Nach der Rspr. ist ein Verwertungsverbot auch dann zu entscheiden, wenn die Eilkompetenz missbraucht wurde, indem der Richtvorbehalt nicht beachtet wurde, beispielsweise durch hypothetische Ersatzeingriffe und willkürliche oder bewusste Missachtung der Verfahrensvorschriften.[263]

Bei Zwangsmaßnahmen ist die Beachtung des Richtervorbehalts indes für die Durchsetzung grundrechtssichernder Schutzfunktionen entscheidend. Somit sind die materiellen Voraussetzungen von Gefahr im Verzug stets allein streng anzunehmen und der Irrtum über sie ist mit Verstößen gegen sonstige die Art und Weise der Durchsuchung regelnde Vorschriften nicht gleichzusetzen.[264] Dabei ist nun auch die bedenkliche Umkehrung in der Praxis des Regel-Ausnahme-Verhältnisses zwischen

---

[259] *BVerfGE* 103, 142, 155 [Rn. 40]; 139, 245, 270 [Rn. 70]; *BGHSt* 51, 285, 288 f.; M-G/*Schmitt*, StPO, § 98 Rn. 6 und § 105 Rn. 2; *Park*, § 2 Rn. 92.

[260] M-G/*Schmitt*, StPO, § 105 Rn. 2; dazu *BVerfGE* 139, 245, 276 [Rn. 85]: Ohne ihn wird die Gefahr im Verzug von der Behörde selbst herbeigeführt.

[261] *Park*, § 2 Rn. 104; *Wohlers*/*Greco*, § 98 Rn. 36.

[262] *BVerfG* NJW 2009, 3225 [Rn. 16]; *BGHSt* 51, 285, 291 f. [Rn. 24]; *OLG Jena* NJW 2001, 1290, 1293 m. w. N.; *Bruns*, KK-StPO, § 105 Rn. 22; *Greven*, KK-StPO, § 98 Rn. 14; *Krehl*, NStZ 2003, 461, 463 f.; M-G/*Schmitt*, StPO, § 98 Rn. 7, § 105 Rn. 16 a. E.; *Roxin*/*Schünemann*, § 35 Rn. 9; *Wohlers*/*Greco*, § 98 Rn. 63, § 105 Rn. 79; dazu *Park*, § 2 Rn. 410 ff.

[263] Vgl. *Roxin*/*Schünemann*, § 24 Rn. 26. Insoweit *BGHSt* 51, 285, 291 [Rn. 22]: „*Gefahr im Verzug lag hier zwar nicht vor. Die Verletzung des Richtervorbehalts hat aber aus objektiver Sicht geringeres Gewicht als wenn, wie etwa im Falle des § 100b I StPO, der Polizei die Anordnung von Eingriffen der betreffenden Art schlechthin untersagt ist. Zudem kommt bei der hier gebotenen objektiven Sicht dem Umstand Bedeutung zu, dass ein richterlicher Durchsuchungsbeschluss höchstwahrscheinlich zu erlangen gewesen wäre.*“

[264] Vgl. *Amelung*, NJW 1991, 2533, 2536 f.: Nehmen die Ermittlungsbehörden jedoch auf eigenen Entschluss eine Durchsuchung vor, obgleich die materiellen Voraussetzungen dafür fehlen, so kommt ein Verwertungsverbot in Betracht; abw. *BGHSt* 51, 285, 293 [Rn. 25].

dem Richtervorbehalt und der Eilkompetenz in Rechnung zu ziehen.[265] So sollte auch die Annahme von Gefahr im Verzug aufgrund grober Fahrlässigkeit zum Verwertungsverbot führen können, außer wenn die Ermittlung Bagatellkriminalität betrifft.[266]

c) Eilzuständigkeit

Die Annahme von Gefahr im Verzug begründet für die Strafverfolgungsbehörden eine Eilzuständigkeit, und die StA oder ihre Ermittlungspersonen sind berechtigt, die Durchsuchung und Beschlagnahme anzuordnen.[267] Hierbei kommt nach h. M. und der Rspr. des *BVerfG* der StA als Herrin des Ermittlungsverfahrens vorrangige Kompetenz zu, die Anordnungsbefugnis der Ermittlungspersonen ist dagegen nachrangig und subsidiär.[268] So müssen diese vor der Wahrnehmung der eigenen Eilkompetenz versuchen, (fern)mündlichen Kontakt mit der zuständigen StA aufzunehmen, und sind nur dann zuständig, wenn sie nicht erreichbar ist.[269] Wenn die Ermittlungspersonen wegen Gefahr im Verzug eine Eilanordnung anregen, aber der Staatsanwalt dies verweigert, dürfen sie daher nicht selbst die Durchsuchung oder Beschlagnahme anordnen.[270] Wird die StA nicht erreicht, aber ist der Ermittlungsrichter erreichbar, dann können sie allerdings unmittelbar mit dem Gericht in Kontakt treten (§§ 163 Abs. 2 S. 2, 165 StPO).[271] Dies steht mit der Stellung der StA im Ermittlungsverfahren nicht in Widerspruch.

Die Eilkompetenz der Ermittlungsbehörden endet damit, dass ein Antrag auf Erlass einer Durchsuchungs- und Beschlagnahmeanordnung gestellt wird und sich der zuständige Ermittlungsrichter mit der Sache befasst, und mit der dadurch eröffneten Möglichkeit einer Sachprüfung.[272] Sie kann aber neu begründet werden, wenn, nachdem der Richter sich mit der Sache befasst hat, die Umstände eintreten oder bekannt werden, die sich nicht aus dem Prozess der Prüfung und Entscheidung

---

[265] Vgl. *Park*, § 2 Rn. 411: Die strenge Einschränkung des Verwertungsverbots fördert eher die Haltung der Ermittlungsbehörden, die Gefahr im Verzug großzügig – häufig zu großzügig – zu bejahen.

[266] Dazu *Park*, § 2 Rn. 411 f.: Die vorsätzlich fehlerhafte Bejahung von Gefahr im Verzug ist *de facto* zumeist nicht leicht zu beweisen.

[267] Hinsichtlich einer Durchsuchung, die rechtmäßig angeordnet wurde und noch läuft, besteht für sie keine Pflicht, eine richterliche Genehmigung zu erwirken (*BGH* NStZ 2017, 713 [Tz. 1.]; BeckRS 2018, 17706 [Rn. 25]; M-G/*Schmitt*, StPO, § 105 Rn. 2 a. E.).

[268] *BVerfG* NJW 2007, 1345, 1346 [Rn. 17]; NJW 2008, 3053, 3054 [Rn. 10]; *Greven*, KK-StPO, § 98 Rn. 11; M-G/*Schmitt*, StPO, § 98 Rn. 6; *Park*, § 2 Rn. 95 und § 3 Rn. 491.

[269] *Greven*, KK-StPO, § 98 Rn. 11; M-G/*Schmitt*, StPO, § 98 Rn. 6; *Park*, § 2 Rn. 95.

[270] *Park*, § 2 Rn. 95 a. E.

[271] M-G/*Schmitt*, StPO, § 98 Rn. 6. Die Vorschriften sind Ausnahme- bzw. Spezialregelungen des § 162 StPO (a. a. O. § 162 Rn. 5 und § 163 Rn. 26).

[272] *BVerfGE* 139, 245, 273 [Rn. 78].

ergeben, und hierdurch die Gefahr eines Beweismittelverlusts eigenständig begründet wird (überholende Kausalität).[273]

d) Justiziabilität – Dokumentations- und Begründungspflichten

Die ermittlungsbehördliche Durchsuchungs- und Beschlagnahmeanordnung bei Gefahr im Verzug bedarf keiner besonderen Form und kann angesichts der Eilbedürftigkeit nicht nur mündlich oder telefonisch getroffen werden, sondern in bestimmten Situationen auch sogar durch konkludentes Handeln ergehen.[274] Dies beinhaltet aber keinen Ausschluss der Justiziabilität von gesetzlichen Voraussetzungen der Durchsuchung und Beschlagnahme und von Auslegung und Anwendung des Begriffs Gefahr im Verzug. Art. 19 Abs. 4 GG gewährleistet einen möglichst lückenlosen und wirksamen gerichtlichen Schutz gegen die Verletzung der Rechtssphäre des Einzelnen durch öffentliche Gewalt.[275] Aus dieser verfassungsrechtlichen Gewährleistung ergibt sich grundsätzlich die Pflicht der Gerichte, die Anordnung in rechtlicher und tatsächlicher Hinsicht vollständig zu überprüfen,[276] und weiter obliegen den Strafverfolgungsbehörden Dokumentations- und Begründungspflichten, die die Erfüllung der gerichtlichen Pflicht möglich machen.[277] Nur eine vollständige Begründung ermöglicht dem Gericht die effektive Kontrolle der Anordnung.[278] So hat der eine Durchsuchung und Beschlagnahme mündlich oder telefonisch anordnende Beamte, möglichst der – vorrangig verantwortliche – Staatsanwalt,[279] die Voraussetzungen der Anordnung und die auf das Vorliegen von Gefahr im Verzug hindeutenden Erkenntnisse sowie die Darlegung der durchgeführten Kontaktversuche mit dem zuständigen Richter vor oder unmittelbar nach der Durchführung der Maßnahme[280] in den Akten zu dokumentieren.[281] Wird das Vorliegen von Gefahr im

[273] *BVerfGE* 139, 245, 279 f. [Rn. 95 f.].

[274] *OLG Jena* NJW 2001, 1290, 1292 f.; *Greven*, KK-StPO, § 98 Rn. 13; M-G/*Schmitt*, StPO, § 98 Rn. 8, § 105 Rn. 3; *Wohlers*/*Greco*, SK-StPO, § 98 Rn. 37; *Wohlers*/*Jäger*, SK-StPO, § 105 Rn. 42.

[275] *BVerfGE* 69, 1, 48; 101, 106, 122 f.; 103, 142, 156 [Rn. 42].

[276] *BVerfGE* 103, 142, 156.

[277] *BVerfGE* 103, 142, 159 f. [Rn. 53 – 55]; 139, 245, 272 [Rn. 75]; NJW 2007, 1345, 1346 [Rn. 17]; 2008, 3053, 3054 [Rn. 10].

[278] Daneben ermöglicht die Dokumentation i. V. m. der vollständigen Begründung einerseits dem Betroffenen eine sachgerechte Verteidigung seines Grundrechts und andererseits dem anordnenden Beamten eine Bestätigung der Rechtmäßigkeit seines Handelns (*BVerfGE* 103, 142, 160 f. [Rn. 54 f.]).

[279] *BVerfGE* 139, 245, 272 [Rn. 75].

[280] Vgl. *BVerfGE* 103, 142, 160 [Rn. 54]: „*Eine verspätete Dokumentation des zeitlichen Ablaufs birgt die Gefahr von Ungenauigkeiten oder gar Umgehungen mit der Folge, dass eine Behauptung der Strafverfolgungsbehörden … nicht mehr nachzuprüfen ist.*“

[281] *BVerfGE* 103, 142, 160 [Rn. 54]: der Tatverdacht, die gesuchten Beweismittel und die Umstände, die die Gefahr des Beweismittelverlusts begründen sowie insb. die Beschreibung des Versuchs des Beamten, den Ermittlungsrichter zu erreichen; 139, 245, 272 [Rn. 75] und 276 [Rn. 85]; *Wohlers*/*Greco*, SK-StPO, § 98 Rn. 37 und § 105 Rn. 41 f.; abw. M-G/*Schmitt*, StPO,

Verzug abgewiesen, hebt der Richter die Eilanordnung auf; hierbei muss die nicht (vollständig) vollzogene Durchsuchung abgebrochen oder bei der (bereits) vollzogenen muss eine Rechtswidrigkeit festgestellt werden.[282]

e) Gerichtliche nachträgliche Kontrolle: § 98 Abs. 2 StPO

Bei nichtrichterlicher Beschlagnahme soll der Beamte, der die Anordnung getroffen hat, binnen drei Tagen, insofern nicht bereits ein Antrag nach S. 2 gestellt ist, die gerichtliche Bestätigung beantragen, wenn bei der Beschlagnahme weder der davon Betroffene noch ein erwachsener Angehöriger anwesend war oder wenn der Betroffene und ein erwachsener Angehöriger gegen die Beschlagnahme ausdrücklichen Widerspruch erhoben haben (§ 98 Abs. 2 S. 1 StPO). Dabei kann der Betroffene jederzeit die gerichtliche Entscheidung beantragen (S. 2). Der Betroffene ist über seine Rechte zu belehren (S. 5). Enthalten soll die Belehrung gemäß S. 5 den Hinweis, dass der Betroffene nach S. 2 jederzeit, nämlich sowohl während als auch nach der Beschlagnahme eine gerichtliche Entscheidung beantragen kann, und die Information, bei welchem AG er diesen Antrag stellen kann (vgl. S. 3 und 4).[283] Sie obliegt der die Maßnahme durchführenden Behörde[284] und sie sollte in schriftlicher Form erteilt und in das Beschlagnahmeverzeichnis nach § 107 S. 2 und § 109 StPO aufgenommen werden.[285]

Als Umschreibung einer Antragspflicht wird § 98 Abs. 2 S. 1 StPO zumeist angesehen und der Ermittlungsbeamte ist daher verpflichtet, binnen 3 Tagen richterliche Bestätigung zu beantragen.[286] Insbesondere im Fall, dass er sich über die Rechtslage wie etwa das Vorliegen einer Eilkompetenz oder eines Beschlagnahmeverbots und die Zulässigkeit und den Umfang der Beschlagnahme im Klaren ist, wird dies empfohlen.[287] Der Antrag nach S. 2 ist eine Beschwerde gegen die „ohne

§ 98 Rn. 8, § 105 Rn. 3: eine Dokumentation der Anordnungsvoraussetzungen bei Beschlagnahme wird i. d. R. nicht erforderlich sein.

[282] M-G/*Schmitt*, StPO, § 105 Rn. 16.

[283] *Park*, § 3 Rn. 514; vgl. BT-Drs. 7/551, S. 65. Dabei genügt es, dass der Betroffene darüber belehrt wird, dass er nach S. 4 eine Beschwerde beim AG einreichen kann, in dessen Bezirk die Beschlagnahme stattgefunden hat (M-G/*Schmitt*, StPO, § 98 Rn. 11; *Park*, a. a. O.).

[284] *Greven*, KK-StPO, § 98 Rn. 18; M-G/*Schmitt*, StPO, § 98 Rn. 11; *Park*, § 3 Rn. 515.

[285] M-G/*Schmitt*, StPO, § 98 Rn. 11; *Park*, § 3 Rn. 515.

[286] M-G/*Schmitt*, StPO, § 98 Rn. 13; *Park*, § 3 Rn. 498. Hier soll eine Ermittlungsperson dem Gericht den Antrag i. d. R. über die StA zuleiten, weil ein Richter ohnehin gemäß § 33 Abs. 2 StPO nach der Anhörung der StA entscheiden muss (*Greven*, KK-StPO, § 98 Rn. 16; M-G/*Schmitt*, StPO, § 98 Rn. 13 und 17; *Park*, § 3 Rn. 504. Auch der Betroffene muss nach § 33 Abs. 3 StPO i. d. R. angehört werden, doch dies kann ausgeschlossen werden (§ 33 Abs. 4 S. 1 StPO).

[287] *Park*, § 3 Rn. 503. Auch im Fall einer freiwilligen Herausgabe kann er diesen Antrag stellen (*BGH* NJW 1956, 1805, 1806; *Greven*, KK-StPO, § 98 Rn. 16; *Park*, a. a. O.).

gerichtliche Anordnung“ erlassene „Beschlagnahme“ der Ermittlungsbehörde.[288] Nach h. M. und Rspr. gilt aber die Vorschrift aufgrund des Art. 19 Abs. 4 GG sowohl für die Durchsuchung (inklusive der Mitnahme zur Durchsicht gemäß § 110 StPO)[289] als auch für sonstige Zwangsmaßnahmen, die nichtrichterlich angeordnet wurden, u. a. dann entsprechend, wenn Beschwerde gegen die „Art und Weise des Vollzugs“ der erledigten Maßnahmen eingelegt wird.[290] Der § 98 Abs. 2 S. 2 StPO ist somit i. R. d. Zwangsmaßnahmen im Ermittlungsverfahren dann weitgehend analog anwendbar, wenn es keine Vorschrift für den beschwerdeähnlichen Rechtsbehelf wie §§ 110 Abs. 3 S. 2, 161a Abs. 3, 163a Abs. 3 StPO gibt und die Ermittlungsbehörde, insb. StA, die Maßnahmen oder die Art und Weise ihres Vollzugs anordnen kann.[291] Aus diesem Grund spielt der § 98 Abs. 2 S. 2 StPO nunmehr im Vorverfahren als Rechtsgrundlage zur richterlichen Überprüfung der Rechtmäßigkeit der nichtrichterlichen Zwangsmaßnahmen und der Art und Weise ihres Vollzugs eine Rolle und er dient also einem effektiven Grundrechtsschutz.

Betroffener i. S. d. S. 1 und 2 ist jeder, dessen Rechtsposition durch die Beschlagnahme berührt ist, insb. in dessen Gewahrsam eingegriffen wird oder dessen Rechte an dem Gegenstand berührt werden.[292] Der Beschuldigte kann daher kein Betroffener sein,[293] dazu werden aber z. B. Kontoinhaber, Briefversender und -empfänger, Geschäftsinhaber, Geheimnisgeschützte etc. als solcher, deren Rechtsposition durch die Beschlagnahme der Daten berührt ist, üblicherweise gehören.[294] Die Frist von 3 Tagen beginnt erst mit dem Ende der Durchführung der Beschlag-

[288] *Greven*, KK-StPO, § 98 Rn. 18; *Park*, § 2 Rn. 322 und § 3 Rn. 505. Dabei ist unerheblich, ob die Gegenstände freiwillig herausgegeben wurden (vgl. *BVerfG* NJW 2007, 3343 [Tz. a)]; *Greven*, a. a. O.; *Park*, a. a. O.; *Wohlers*/*Greco*, SK-StPO, § 98 Rn. 47). Denn auch im Fall einer freiwilligen Herausgabe besteht die Möglichkeit des von der Maßnahme Betroffenen, nachträglich eine richterliche Entscheidung herbeizuführen (*BVerfG* a. a. O.). So wird der Widerruf einer freiwilligen Herausgabe i. d. R. als Antrag i. S. d. S. 2 ausgelegt (*Greven*, a. a. O.; *Park*, a. a. O.; *Wohlers*/*Greco*, a. a. O.).

[289] *Bruns*, KK-StPO, § 105 Rn. 15 f.; M-G/*Schmitt*, StPO, § 105 Rn. 2b a. E. und Rn. 16; *Wohlers*/*Greco*, SK-StPO, § 105 Rn. 73; vgl. *BVerfGE* 139, 245, 271 [Rn. 73]; NJW 2002, 1333 [Tz. b)]. Dabei gilt S. 1 hingegen nicht entsprechend. Indes kann dieser Satz entsprechend gelten, solange die Durchsuchung noch nicht abgeschlossen ist, nämlich bei Durchsicht aufgrund vorläufiger Sicherstellung nach § 110 StPO (vgl. unten III. 3. d)).

[290] Vgl. *BGHSt* 44, 171, 174: Anordnung einer erledigten vorläufigen Festnahme; 44, 265, 270 ff.: für die Überprüfung der Art und Weise des Vollzugs einer nichtrichterlich angeordneten abgeschlossenen Durchsuchung; 45, 183, 186 f.: für dieselbe einer richterlich angeordneten abgeschlossenen Durchsuchung; M-G/*Schmitt*, StPO, § 98 Rn. 23; *Roxin*/*Schünemann*, § 29 Rn. 14.

[291] *Roxin*/*Schünemann*, § 29 Rn. 15. Für die in § 101 Abs. 1 StPO genannten verdeckten Ermittlungsmaßnahmen gilt aber Abs. 7 S. 2 – 4 als Sonderregelung (vgl. Kapitel 3, A. III. 3. c)).

[292] *Greven*, KK-StPO, § 98 Rn. 18; M-G/*Schmitt*, StPO, § 98 Rn. 15 und 20; *Park*, § 3 Rn. 502; *Wohlers*/*Greco*, SK-StPO, § 98 Rn. 48.

[293] *Greven*, KK-StPO, § 98 Rn. 18; *Wohlers*/*Greco*, SK-StPO, § 98 Rn. 48.

[294] *Greven*, KK-StPO, § 98 Rn. 18; M-G/*Schmitt*, StPO, § 98 Rn. 20; *Park*, § 3 Rn. 502; *Wohlers*/*Greco*, SK-StPO, § 98 Rn. 48.

nahme und gilt nicht für den Antrag des Betroffenen auf die gerichtliche Entscheidung nach S. 2.[295] Bei richterlicher Entscheidung nach S. 1 und 2 handelt es sich nicht darum, ob eine nichtrichterliche Anordnung zu Recht ergangen ist, sondern darum, ob die Beschlagnahme im Zeitpunkt der Entscheidung gerechtfertigt ist, d. h. ob die Voraussetzungen der Beschlagnahme noch vorliegen.[296] Die nichtrichterliche Anordnung wird für das weitere Verfahren durch die gerichtliche Entscheidung ersetzt, sodass diese dem Betroffenen und den Prozessbeteiligten bekanntzumachen ist.[297]

3. Exkurs – Aushöhlung des Richtervorbehalts in der Praxis

a) Kritik an der Praxis

Der Richtervorbehalt hat Verfassungsrang und dient dem Grundrechtsschutz gegen schwerwiegende Eingriffsmaßnahmen im Ermittlungsverfahren. Seine Funktion ist nur durch eine einzelfallbezogene und sorgfältige Prüfung zu erfüllen. Doch scheint es, dass der Richtervorbehalt in der Praxis – insb. hinsichtlich der umfangreichen Erfassung personenbezogener Daten – nicht ausreichend eingehalten wird. Diesbezüglich wird neben dem Inhalt des richterlichen Beschlusses, dem Kombi-Beschluss (vgl. oben 1. c)) sowie dem Missbrauch der Eilkompetenz (vgl. oben 2. a)) eine Geschäftspraxis erwähnt, dass die gerichtliche Überprüfung der Durchsuchungen und Beschlagnahmen nur oberflächlich durchgeführt wird. Der staatsanwaltliche Antrag wird in Beschlussform vorformuliert, die der Richter nur zu unterschreiben braucht, und die richterliche Anordnung ergeht – oft ohne sorgfältige Prüfung – auf der Grundlage dieses Beschlusses.[298] Aus diesem Grund wird der

[295] M-G/*Schmitt*, StPO, § 98 Rn. 14; *Park*, § 3 Rn. 507. Nach h. M. macht das Versäumen der Frist die Beschlagnahme nicht unwirksam (*Greven*, KK-StPO, § 98 Rn. 16; M-G/*Schmitt*, a. a. O.; *Park*, § 3 Rn. 508; *Wohlers*/*Greco*, SK-StPO, § 98 Rn. 43).

[296] *Greven*, KK-StPO, § 98 Rn. 20; M-G/*Schmitt*, StPO, § 98 Rn. 17. Daneben ist zu prüfen, ob Gefahr im Verzug vorlag und ob somit die Eilkompetenz der Ermittlungsbehörden gegeben war (*Greven*, a. a. O.; M-G/*Schmitt*, a. a. O.). Nach der Literatur hätte die gerichtliche Überprüfung der Rechtmäßigkeit aber erfahrungsgemäß i. d. R. kaum Erfolgsaussicht, sondern dadurch wird nur bescheinigt, dass die Maßnahme der Durchsuchung und Beschlagnahme rechtmäßig angeordnet und durchgeführt wurde (vgl. *Park*, § 1 Rn. 8).

[297] M-G/*Schmitt*, StPO, § 98 Rn. 17. Die richterliche Bestätigung nach S. 1 und die richterliche Ablehnung des Antrags nach S. 2 kann mit der Beschwerde gemäß § 304 StPO angefochten werden (M-G/*Schmitt*, a. a. O. Rn. 31; *Park*, § 2 Rn. 315, 321 und 324 sowie § 3 Rn. 675; vgl. für den Fall der gerichtlichen Entscheidung gemäß § 98 Abs. 2 S. 2 StPO, *BVerfGE* 139, 245, 271 [Rn. 73]; NJW 2002, 1333 [Tz. b)]; 2003, 2303, 2304 [Tz. b)]).

[298] *Burhoff*, StraFo 4/2005, 140; *Ciolek-Krepold*, Rn. 53 f.; *Park*, § 2 Rn. 56; *Schünemann*, ZStW 114 (2002), 1, 20; insb. *Stadler*, ZRP 2013, 179: „*Vollständig von der StA vorformulierte ermittlungsrichterliche Beschlüsse, die vom Gericht dann auch noch gänzlich unverändert erlassen werden, stellen also keine Seltenheit dar, sondern entsprechen gängiger Praxis an vielen Gerichten*"; als Rechtsprechung bezüglich des letzten Zitats, *AG Würzburg* Urt. v. 26. 9. 2012 – 103 Cs 701 Js 19849/11, BeckRS 2013, 13651: „*…, dass es jedenfalls in Würzburg seit Jahrzehnten gängige Praxis ist, dass die StA, wenn sie Beschlüsse beim Ermittlungsrichter*

Ermittlungsrichter kritisiert, indem er vielfach nur als ein „Teil der Exekutive“[299] oder eine Art „Urkundsbeamter der StA“[300] bezeichnet wird.[301] Eine solche Praxis höhlt jedoch höchstwahrscheinlich die verfassungsrechtliche und gesetzliche gewollte Überprüfung durch den Richter aus[302] und sie ist auch nach den Vorgaben des *BVerfG* zum Richtervorbehalt bedenklich:

> „Es ist seine(richterliche) Aufgabe und Pflicht, sich eigenverantwortlich ein Urteil zu bilden und nicht etwa nur die Anträge der StA nach einer pauschalen Überprüfung gegenzuzeichnen. Zur richterlichen Einzelentscheidung gehören eine sorgfältige Prüfung der Eingriffsvoraussetzungen und eine umfassende Abwägung zur Feststellung der Angemessenheit des Eingriffs im konkreten Fall. Schematisch vorgenommene Anordnungen vertragen sich mit dieser Aufgabe nicht.“[303]

Letztens führt zum Leerlauf des Richtervorbehalts auch die strenge Rspr. des Gerichts, in denen ein Beweisverwertungsverbot auch bei seiner Verletzung, wie etwa der Ausübung der Eilkompetenz ohne Gefahr im Verzug, nur beschränkt,

---

beantragt, dem Antrag einen vollständig ausformulierten Beschluss (mit Kopf des Amtsgerichts Würzburg) beifügt, welcher in aller Regel unverändert (aber nicht ungeprüft) vom Ermittlungsrichter unterzeichnet wird – wenn nicht der Erlass grundsätzlich abgelehnt wird.“

[299] *Paeffgen*, FS Roxin 2001, 1299, 1308.

[300] *Schünemann*, ZStW 114 (2002), 1, 20.

[301] *Roxin/Schünemann*, § 29 Rn. 25; vgl. *Park*, § 1 Rn. 6: In zahlreichen Fällen – von besonderen Einzelfällen abgesehen – ist der Richtervorbehalt praktisch bedeutungslos. Obwohl das *BVerfG* und eine Reihe von Literatur anstreben, (theoretisch) etwa durch Unterbindung der Eilkompetenz einen lückenlosen gerichtlichen Rechtsschutz im Ermittlungsverfahren zu gewährleisten, droht der Richtervorbehalt praktisch weitgehend leerzulaufen (*Schünemann*, ZStW 114 (2002), 1, 20).

[302] *Ciolek-Krepold*, Rn. 53 a. E. Wird nun der Beschluss der Durchsuchung und Beschlagnahme durch die StA vorformuliert und ohne weitere Prüfung durch den Richter unterschrieben, so liegt die richterliche Verhältnismäßigkeitsprüfung und ein effektiver Grundrechtsschutz in weiter Ferne (a. a. O. Rn. 54 a. E.).

[303] *BVerfG* NStZ-RR 2004, 143; vgl. NJW 2009, 2516, 2517 f. [Rn. 29]: „*(Allerdings,) Allein die Übernahme des Antrags der StA durch den Ermittlungsrichter lässt noch nicht auf das Fehlen einer eigenverantwortlichen Prüfung des Sachverhalts schließen. Auch müssen sich die Beschlussgründe grundsätzlich nicht zu jedem denkbaren Gesichtspunkt des Tatverdachts verhalten. Aus verfassungsrechtlicher Sicht nicht hinnehmbar ist es aber, wenn sich im Einzelfall auf Grund besonderer Umstände die Notwendigkeit der Erörterung eines offensichtlichen Problems aufdrängen musste und gleichwohl eine Prüfung vollständig unterbleibt.*“ Nach der obigen Entscheidung des *AG Würzburg* (siehe Fn. 298) ist jedoch die vollständige und unveränderte Übernahme des Beschlussvorschlags der StA durch den Ermittlungsrichter nicht nur unerlässlich, sondern daraus wird auch kein Schluss auf ein Fehlen richterlicher Überprüfung gezogen: „*Die hohe Anzahl der zu beurteilenden Anträge – häufig in Verbindung mit umfangreichem Akteninhalt – verlangen diese Vorgehensweise. Eine Abänderung/Ergänzung des Entwurfs, wenn er in der Sache – im Ergebnis richtig ist, … unterbleibt i. d. R. aufgrund dieser hohen Arbeitsbelastung. Da der unterzeichnete Beschluss wortgleich ist mit dem von der StA formulierten Entwurf, ist unter diesem Gesichtspunkt aus dem Beschluss nicht ersichtlich, dass der Richter selbst die Voraussetzungen überprüft hat. Allerdings trägt der Beschluss seine Unterschrift und im Beschluss ist dargelegt, dass der Richter die Durchsuchung bei einem Rechtsanwalt für verhältnismäßig … hält. Insofern spricht der Wortlaut unzweifelhaft und eindeutig für eine Prüfung durch den Richter.*“

nämlich bei willkürlicher oder bewusster Missachtung der Zuständigkeitsgrenzen angenommen wird.[304] Diese Auflockerung der richterlichen Kontrolle durch die Gerichte selbst läuft der jüngsten Tendenz, die eine Intensivierung der richterlichen Kontrolle bei schwerwiegenden Grundrechtseingriffen anstrebt, zuwider.[305]

b) Strukturelle und organisatorische Grenzen

Im Schrifttum werden zum Grund der Aushöhlung des Richtervorbehalts in der Praxis zumeist Probleme aus struktureller und organisatorischer Sicht angeführt. Zunächst können in der Verfahrensstruktur des Akkusationsprinzips die StA oder die Polizei personenbezogene Daten unmittelbar und aktiv erfassen und Straftaten erforschen (§§ 161 Abs. 1, 163 Abs. 1 StPO), während der Ermittlungsrichter aufgrund des Antrags der StA nur die von ihr erbrachten Informationen passiv zur Kenntnis nehmen kann (§ 162 Abs. 1 StPO). Der kontrollierende Richter besitzt daher wesentlich nicht das gleiche Informationsniveau wie der kontrollierte Staatsanwalt.[306] Danach spielt in organisatorischer Hinsicht eine große Differenz zwischen der Zahl der Staatsanwälte und der Ermittlungsrichter eine entscheidende Rolle.[307] Die Richter sind seit Langem mit ihren zahlreich zu treffenden Entscheidungen überlastet.[308] Gleichwohl wird der Richtervorbehalt bei gesetzlichen Regelungen zu neuen Maßnahmen stets als notwendiger Kontrollapparat in Ermächtigungsnormen eingefügt, sodass die Anzahl von Anordnungen, die richterlich zu erteilen oder zu überprüfen sind, fortwährend zunimmt.[309] In den letzten zwanzig Jahren nutzen das *BVerfG* und der Gesetzgeber ihn als rechtliches und politisches Mittel erschöpfend aus, um neue Eingriffsermächtigungen zu rechtfertigen.[310] Aus diesem Grund wird der Richtervorbehalt in letzter Zeit als „ein rechtsstaatliches Feigenblatt bzw. Placebo“ bezeichnet,[311] doch dies ist sicherlich überspitzt.[312] Immerhin leiden die Er-

[304] *Roxin/Schünemann*, § 24 Rn. 51 und vgl. § 35 Rn. 9.

[305] Vgl. *Roxin/Schünemann*, § 36 Rn. 15.

[306] Vgl. *Schünemann*, ZStW 114 (2002), 1, 36; auch *Stadler*, ZRP 2013, 179, 180: ein erhebliches Informationsdefizit des Ermittlungsrichters gegenüber StA und Polizei; vgl. *Roxin/Schünemann*, § 29 Rn. 25: geringe Effizienz der ermittlungsrichterlichen Kontrolle.

[307] Vgl. *Schünemann*, ZStW 114 (2002), 1, 36 [Fn. 113]: Beim *AG München* und *LG München I* stehen acht Ermittlungsrichtern 148 Staatsanwälte gegenüber.

[308] Vgl. *Schünemann*, ZStW 114 (2002), 1, 20.

[309] *Stadler*, ZRP 2013, 179.

[310] Vgl. *Roxin/Schünemann*, § 29 Rn. 25: „*Gesetzgeber und BVerfG nach wie vor das zentrale Scharnier zum Schutz der bürgerlichen Freiheit allein im Richtervorbehalt erblicken.*“

[311] *Lilie*, ZStW 111 (1999) 807, 814; *Hiéramente*, wistra 11/2016, 432, 437 am Anfang; dazu fasst *Stadler* angemessen dies zusammen (ZRP 2013, 179, 180): „*Der einfache Richter … wird zum Werkzeug einer Legislative, die allzu häufig die verfassungsrechtlichen Vorgaben nicht mehr beachtet. Während der Richtervorbehalt in der politischen Diskussion nahezu als Allheilmittel zur Aufrechterhaltung rechtsstaatlicher Zustände gepriesen wird, belegt die Praxis, dass er mehr und mehr zum Placebo verkommt, der keine rechtsstaatlich relevante Wirkung mehr erzielt, sondern vorwiegend dem (politischen) Zweck dient, neue Eingriffsbefugnisse rechtsstaatlich zu legitimieren.*“

mittlungsrichter derzeit unter chronischer Arbeitsüberlastung, so kann es von ihnen nicht erwartet werden, alle Akten vollständig und mit der gleichen Gründlichkeit wie die Staatsanwälte zur Kenntnis zu nehmen und auszuwerten; vielmehr können sie i. d. R. nur eine Art summarischer Prüfung durchführen oder sich auf die Angabe des beantragenden Staatsanwalts verlassen.[313] Aus Rücksicht auf diese strukturellen und organisatorischen Grenzen sowie die fast überall vorhandene Eilkompetenz der StA oder sogar der Polizei ist es im Grunde ansatzweise unabweisbar, dass der Richtervorbehalt die rechtsstaatliche Kontrolle der gewaltigen Macht der Ermittlungsorgane nicht ausreichend wahrnehmen kann, und daher darf seine freiheitsschützende Funktion heutzutage nicht zu hoch eingeschätzt werden.[314]

Trotz alledem ist das Ermittlungsverfahren im Grunde identisch mit dem alten Inquisitionsprozess, daher ist die Kontrolle durch eine unabhängige und neutrale Instanz zur Verfahrensbalance noch von Bedeutung[315] und der Sinn und Zweck des Richtervorbehalts, durch eine angemessene Abgrenzung der kriminalistischen Eingriffsmaßnahmen Grundrechte zu schützen, darf nicht aufgegeben werden. Sowohl theoretisch als auch praktisch ist die gerichtliche Kontrolle objektiver und zuverlässiger als die verwaltungsinterne Kontrolle. Mittel zum Grundrechtsschutz, um die strukturellen und organisatorischen Grenzen des Richtervorbehalts zu ergänzen, sollten in Betracht gezogen werden.

c) Eine Alternative zur Lösung

Wie lautet die Lösung für die Aushöhlung des Richtervorbehalts und des Ferneren für den unverhältnismäßigen Eingriff in Grundrechte im Ermittlungsverfahren? Zuerst ist auf struktureller Ebene die Vermehrung der Zahl der Ermittlungsrichter erforderlich.[316] Dabei handelt es sich um eine Haushaltsfrage, aber ebenso wie bei der Einrichtung eines Nachtdienstes sind der Bund und die Länder von Verfassungs wegen verpflichtet, die Wirksamkeit des Richtervorbehalts zu gewährleisten. Andererseits, obwohl das Ungleichgewicht zwischen der StA und dem Ermittlungsrichter bezüglich der Informationen strukturell unvermeidbar ist, sollte sich dieser bemühen, den Zweck und die Funktion des Richtervorbehalts zu verwirklichen, indem er eine Begründung für seine Entscheidung selbst formuliert. Dafür sollte er bei der Anfertigung des Durchsuchung- oder Beschlagnahmebeschlusses im Einzelfall, insb. im Fall, dass mit einer umfassenden Datenerfassung zu rechnen ist, den Ermittler drängen, ausreichende Aktenmaterialien vorzulegen, und weiter die Art und Weise der Durchsuchung und den Umfang der Beschlagnahme angemessen

[312] Zust. *Schünemann*, ZStW 114 (2002), 1, 36.

[313] *Park*, § 1 Rn. 6; *Schünemann*, ZStW 114 (2002), 1, 36.

[314] Vgl. *Roxin*/*Schünemann*, § 29 Rn. 25.

[315] *Roxin*/*Schünemann*, § 69 Rn. 4 f.

[316] Zust. *Park*, § 1 Rn. 7; auch *Stadler*, ZRP 2013, 179: Problematisch ist, fortwährend neue gesetzliche Richtervorbehalte zu schaffen, ohne die personelle Ausstattung der Gerichte zu verbessern.

angeben, zumindest nicht so vage, dass sie von der Untersuchungsbehörde willkürlich erweitert werden. Hierbei wird u. a. eine ausreichende Ausnutzung des § 110 StPO verlangt (vgl. unten III.).

Als Letztes wird die Stärkung der Stellung der Betroffenen und der Rechte der Verteidigung im Ermittlungsverfahren, u. a. im Zuge der Durchsuchung und Beschlagnahme als Lösung außerhalb des gerichtlichen Bereichs verlangt.[317] Derzeit scheint dies am effektivsten zu sein. Denn im Einzelfall zu überwachen, ob Ermittlungsbeamte die Vorschriften der StPO und die Grenzen eines richterlichen Beschlusses verletzen, und dem entgegenzuwirken, kann nur vom Betroffenen und seinen Verteidigern effektiv erfolgen. Personenbezogene Daten sind u. a. unter modernen informationstechnischen Gegebenheiten häufig unerlässlich in großen Mengen oder umfangreich durchzusehen und sicherzustellen, wobei die Nützlichkeit des Richtervorbehalts ersichtlich beschränkt ist und es unmöglich ist, im Einzelfall nur mit ihm ein prozessuales Gleichgewicht ausreichend zu erreichen. Im gesamten Strafverfahren ist die Bedeutung der Ermittlungsverfahren noch größer und der Ausgang der Hauptverhandlung ist ggf. durch die Ermittlungsergebnisse bereits bestimmt.[318] Mit Blick auf das Ermittlungsverfahren, das so wichtig wird wie die Hauptverhandlung, die Stellung des Beschuldigten, die in diesem Verfahren der Strafverfolgungsbehörde wesentlich unterlegen ist, und die Aushöhlung des Richtervorbehalts bedarf es im Ergebnis neben diesem einer institutionellen Einrichtung, die zur Überwachung gewaltiger Ermittlungsmacht bzw. zur Kontrolle der Richtigkeit der Ermittlungen die Intervention des Beschuldigten und seines Verteidigers im Ermittlungsverfahren gesetzlich gewährleistet. Diesbezüglich weist *Roxin/Schünemann* zutreffend darauf hin, dass *de lege ferenda* zur Beibehaltung prozessualer *checks and balances* durch eine Stärkung der Verteidigungsfunktion, z. B. die Gewährung umfassender Akteneinsicht an den Verteidiger nach schwerwiegendem Datenzugriff und die Schaffung einer sog. Not- oder Proto-Verteidigung, dem Funktionswandel des Ermittlungsverfahrens begegnet werden muss (vgl. unten IV.).[319]

III. Durchsicht von Papieren: § 110 StPO

1. Allgemeines

a) Sinn und Zweck des § 110 StPO

Die im Ermittlungsverfahren aufgefundenen Papiere enthalten zumeist nicht nur die Daten, die zur Aufklärung von Straftaten zu beschlagnahmen sind, sondern auch die Daten, die für das Verfahren irrelevant sind oder deren Zugriff oder Erfassung

[317] Auch *Park*, § 1 Rn. 9.

[318] *Roxin/Schünemann*, § 39 Rn. 1.

[319] *Roxin/Schünemann*, § 29 Rn. 26 und auch § 19 Rn. 66 f.

rechtlich verboten ist. Bei praktischer Durchsuchung und Beschlagnahme – insb. in Wirtschafts- und Steuerstrafsachen – ist die Menge der aufgefundenen und sicherzustellenden Papiere i. d. R. so erheblich und ihr Inhalt eventuell so kompliziert, dass eine Entscheidung, ob sie beweiserheblich sind und in welchem Umfang sie zu beschlagnahmen sind, direkt an Ort und Stelle weder möglich noch zweckmäßig ist.[320] Dies gilt umso mehr, weil in der modernen Informationsgesellschaft die Papiere zumeist in Form unsichtbarer elektronischer Daten bzw. Dateien bestehen. Der Umfang der Beschlagnahme muss nach dem Verhältnismäßigkeitsgrundsatz durch die vorhergehende Durchsuchung[321] inhaltlich begrenzt werden. Daher sollten die Papiere im Zug der Durchsuchung und Beschlagnahme stets besonders behandelt werden und dies wird durch § 110 StPO in Rechnung gestellt.[322] Die Durchsicht nach dieser Vorschrift legt es darauf an, dass im Rahmen des technisch Möglichen und Vertretbaren lediglich diejenigen Informationen, die verfahrensrelevant und verwertbar sind, dauerhaft und tief greifend beeinträchtigt und sonstige vom Verfahren ausgeschlossen werden (die Feststellung der potenziellen Beweiserheblichkeit und -verwertbarkeit der Daten).[323] Dadurch können die verfassungsrechtlich oder gesetzlich mit Beweisverwertungsverboten verknüpften Informationen, insb. die kernbereichsrelevanten,[324] die nach § 97 Abs. 1 StPO beschlagnahmefreien[325] oder die verfahrensirrelevanten Informationen der öffentlichen Hand frühzeitig entzogen

[320] Vgl. *Graulich*, wistra 8/2009, 299, 300.

[321] Vgl. *Park*, § 1 Rn. 14.

[322] Dazu *Park*, § 2 Rn. 228: eine spezielle Regelung.

[323] Vgl. *BVerfGE* 113, 29, 56 [Rn. 118]; 124, 43, 69 [Rn. 88]; NJW 2002, 1410, 1411; 2014, 3085, 3088 [Rn. 44]; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 1. Freilich wird die Entscheidungsbefugnis darüber grundsätzlich der StA eingeräumt (NJW 2002, 1410, 1411; *Wohlers/Jäger*, a. a. O. Rn. 23).

[324] Vgl. *BVerfGE* 80, 367, 373 ff.; *BGH* NJW 1994, 1970: Nicht zulässig ist die Beschlagnahme und Verwertung von Tagebüchern, die zum absolut geschützten Kernbereich gehören.

[325] Nach höchstgerichtlichen Entscheidungen dürfen Unterlagen, die ein Beschuldigter erkennbar zu seiner Verteidigung in dem gegen ihn laufenden Strafverfahren angefertigt hat, aber sich in seinem Gewahrsam befanden, – wie Mitteilungen, Aufzeichnungen und Gegenstände nach § 97 Abs. 1 StPO – weder beschlagnahmt noch gegen seinen Widerspruch verwertet werden (*BVerfG* NJW 2002, 1410; *BGHSt* NJW 1998, 309; *Peters*, NZWiSt 2017, 465, 468 [Tz. bb)]; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 21). So darf E-Mail-Verkehr des Beschuldigten mit seinem Verteidiger nicht durchgesehen werden (vgl. *Szesny*, WiJ 2012, 228, 230 [Tz. 2.]). Ist es aber nicht sofort feststellbar, ob die bei einer Durchsuchung des Notebooks aufgefundenen Aufzeichnungen zur Verteidigungsunterlage gehören, so können sie gemäß § 110 StPO vorläufig sichergestellt und durchgesehen werden (*BVerfG* a. a. O.; *Peters* a. a. O.). In dieser Hinsicht dient die Vorschrift neben verfassungsrechtlichem Persönlichkeitsschutz auch der Durchsetzung der Beschlagnahmeverbote des § 97 StPO (*Knauer/Wolf*, NJW 2004, 2932, 2937; *Park*, § 2 Rn. 230; *Wohlers/Jäger*, a. a. O. Rn. 5). Nach einer anderen Meinung ist hingegen bei Durchsuchung – anders als Beschlagnahme – die Einschränkung aufgrund der Rücksichtnahme auf sog. „menschliche oder betriebliche Tabuzonen" nicht vertretbar; denn die Vorschriften über die Durchsuchung (§§ 102 ff. StPO) kennen eine solche Rücksichtnahme nicht und hierbei sind die staatlichen Aufklärungsinteressen vorrangig (*Dauster*, StraFo 6/1999, 186).

werden.[326] So bezweckt die Durchsicht gemäß § 110 StPO die Vermeidung einer verbotenen oder unnötigen Datenerhebung und der hiermit verbundenen Missbrauchsgefahren und damit eine Verminderung der Eingriffsintensität.[327] Gegen die Ermittlungsbehörden, die im Ermittlungsverfahren eine strukturelle Machtstellung innehaben, dient diese Vorschrift dem Schutz der Persönlichkeitssphäre des von der Durchsuchung Betroffenen, und sie funktioniert als Gegengewicht im Spannungsverhältnis zwischen der wirksamen Strafverfolgung und dem Grundrechtsschutz.[328] In dieser Hinsicht prägt sie im Verfahren der Durchsuchung und Beschlagnahme den Verhältnismäßigkeitsgrundsatz[329] und stellt keine Eingriffs-, sondern eine Schutzbestimmung dar.[330] Heutzutage hat der § 110 StPO daher eine sehr wichtige Bedeutung erlangt, da er bei Durchsuchung und Beschlagnahme von Datenträgern und von hierauf gespeicherten Daten zum Datenschutz zwingend berücksichtigt werden sollte, es sei denn, ihr Umfang ist offensichtlich oder ihr Inhalt ist leicht identifizierbar.[331] Schließlich kann er keine (bloße) Ordnungsvorschrift sein[332] und sollte in der Praxis ausreichend angewendet und ausgewertet werden. In der StPO gibt es jedoch keinen Inhalt, den Verlauf der Durchsicht zu regeln.

b) Charakter der „Durchsicht" gemäß § 110 StPO

Das Sichtungsverfahren gemäß § 110 StPO bewegt sich zwischen Durchsuchung und Beschlagnahme und ist der Durchsuchung zugeordnet.[333] Es ist der endgültigen

[326] Zust. *Brodowski/Eisenmenger*, ZD 3/2014, 119, 120; *Szesny*, WiJ 2012, 228, 230 [Tz. 2.]; auch *OLG Koblenz* NStZ 2007, 285, 286 [Rn. 5]: Erst eine solche Durchsicht kann Klarheit bringen, welche von den gesamten, einen begrenzten Zeitraum betreffenden Unterlagen das gesuchte Beweismittel oder die Daten des Beschlagnahmeverbots darstellen.

[327] *BVerfGE* 113, 29, 58 [Rn. 126]; 124, 43, 72 [Rn. 96]; dazu *Szesny*, WiJ 2012, 228, 229: Aus Sicht der Strafverfolgungsbehörden dient sie der Verschlankung des Beweisumfangs und der Verfahrenseffizienz.

[328] *Dauster*, StraFo 6/1999, 186.

[329] Dies ist abzuleiten aus *BVerfGE* 113, 29, 56 f. & 124, 43, 68 f.; dazu *Brodowski/Eisenmenger*, ZD 3/2014, 119, 120: als Korrektiv im Lichte der Verhältnismäßigkeit; *Peters*, NZWiSt 2017, 465, 469.

[330] *Bär*, CR 1999, 292, 294.

[331] Zust. *Ciolek-Krepold*, Rn. 145; *Park*, § 2 Rn. 233; vgl. *Brodowski/Eisenmenger*, ZD 3/2014, 119: Cloud-Computing.

[332] Zust. *Dauster*, StraFo 6/1999, 186, 189 [Tz. III.].

[333] *BVerfGE* 124, 43, 75 f. [Rn. 107]; NJW 2003, 2669, 2670; *BGH* StV 1988, 90; NStZ 2003, 670, 671 [Rn. 2]; *OLG Jena* NJW 2001, 1290, 1293; *Brodowski/Eisenmenger*, ZD 3/2014, 119, 120; *Bruns*, KK-StPO, § 105 Rn. 20; M-G/*Schmitt*, StPO, § 110 Rn. 2; *Michalke*, StraFo 3/2014, 89, 91; *Szesny*, WiJ 2012, 228, 230 [Tz. 1.]; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 2; vgl. dazu *Dauster*, StraFo 6/1999, 186. 188: Dies ist zudem abzuleiten nicht nur aus der systematischen Stellung des § 110 StPO, sondern auch daraus, dass es mit der Aufgabenerfüllung der Kriminalpolizei kollidiert, dass die Einschränkung ihrer Erkennungsmöglichkeit auch nach der abgeschlossenen Durchsuchung fortwirkt; a. A. *Peters*, NZWiSt 2017, 465, 466 a. E. und 469 [Tz. 4.]: Die Durchsicht muss weder als Teil der Durchsuchung noch als Teil der Beschlagnahme, sondern als dazwischenliegende selbstständige Ermittlungsmaßnahme von

Entscheidung über den Umfang der Beschlagnahme vorgelagert, um die Beweiseignung und Beschlagnahmefähigkeit der aufgefundenen Papiere zu überprüfen.[334] Insofern dauert während der Durchsicht von Papieren die Durchsuchung daher noch an und die Beschlagnahme wird noch nicht durchgeführt.[335] Die Rechtmäßigkeit dieser Durchsicht ist daher nicht anhand der Vorschriften der Beschlagnahme (§§ 94, 98 StPO), sondern anhand derjenigen der Durchsuchung (§§ 102 ff. StPO) zu beurteilen.[336] Demzufolge hat der Inhaber der Papiere oder dessen Vertreter nach § 106 Abs. 1 StPO einen Anspruch auf Anwesenheit bei der Durchsicht (vgl. dazu eingehend unten IV. 2) und das Verzeichnis sichergestellter Papiere (§ 109 StPO) muss nach § 107 StPO durch die Ermittlungsbehörde angefertigt und dem Betroffenen gegeben werden. Das sollte einen Hinweis darauf enthalten, dass die Papiere vorläufig sichergestellt werden und an welchen Ort der Dienststelle sie verbracht werden.[337] Zufallsfunde im Zuge dieser Durchsicht können freilich auch nach § 108 StPO „vorläufig beschlagnahmt" werden (vgl. unten 4.).[338] Die Verfahrensrechtliche Schutzwirkung des § 110 StPO entfällt zum Zeitpunkt, wo eine Durchsuchung beendet wird, d. h., dass eine Beschlagnahmeanordnung getroffen ist.[339] Die Sichtung nach der Beschlagnahme stellt keine Durchsicht i. S. d. § 110 StPO mehr dar, sondern die Auswertung der beschlagnahmten Unterlagen (vgl. unten 5.).

c) Bedarf an Verwendung, aber die Umgehung in der Praxis

Bei „umfassender" Durchsuchung von Papieren, insb. Datenbeständen oder Daten, ist nach dem Verhältnismäßigkeitsprinzip die Durchsicht und eine vorläufige Sicherstellung gemäß § 110 StPO erforderlich. Daher hat der Ermittlungsrichter in diesem Fall, soweit keine anderen speziellen Gründe vorliegen, grundsätzlich anzuordnen, dass eine solche Vorgehensweise vor endgültiger Beschlagnahme unternommen wird, und die Strafverfolgungsbehörde hat dementsprechend die Durchsuchung und Beschlagnahme durchzuführen. Dabei kann die Gefahr im Verzug

---

eigener rechtsverletzender Qualität angesehen werden. Es ist insofern zu empfehlen, Bezeichnungen wie „sichergestellt", „mit Beschlag belegt" oder „vorläufige Sicherstellung", nicht „beschlagnahmt", zu verwenden (*OLG Jena*, a. a. O.).

[334] *BVerfGE* 113, 29, 56 [Rn. 118]; 124, 43, 68 f. [Rn. 88] und 75 [Rn. 106]; NJW 2003, 2669, 2670; *Peters*, NZWiSt 2017, 465, 466; *Szesny*, WiJ 2012, 228, 230 [Tz. 1.].

[335] Bei der Durchsicht handelt es sich nicht um einen Eingriff in Art. 13 GG, sondern eher um einen Eingriff in die Persönlichkeitssphäre, insb. das Recht auf informationelle Selbstbestimmung (*Hiéramente*, wistra 11/2016, 432, 438 am Anfang; *Park*, § 2 Rn. 229; *Peters*, NZWiSt 2017, 465, 466). Darüber hinaus ist bei der Sicherstellung des gesamten Datenbestandes oder sämtlicher darauf befindlicher Daten dem Computer-Grundrecht Rechnung zu tragen (siehe Fn. 1).

[336] *BGH* NStZ 2003, 670, 671 [Rn. 2].

[337] *Graulich*, wistra 8/2009, 299, 302 [Tz. 4.5].

[338] *Graulich*, wistra 8/2009, 299, 301 [Tz. 4.1.2]; auch *Mildeberger/Riveiro*, StraFo 2004, 43, 44 [Tz. b)].

[339] Vgl. *Dauster*, StraFo 6/1999, 186, 188 f.

i. S. d. § 98 Abs. 1 S. 1 StPO auch dann nicht vorliegen, wenn dieselbe i. S. d. § 105 Abs. 1 S. 1 StPO schon angenommen wurde, es sie denn, dass gesamte Datenbestände oder sämtliche Daten ersichtlich zu beschlagnahmen sind; die Unterlagen sind nämlich vorläufig sicherzustellen (vgl. unten 3.).[340] So ist die Eilkompetenz der Ermittlungsbehörde für die „Beschlagnahme" insofern von vornherein zu verneinen. Aus einstweilen sichergestellten Papieren oder Datenträgern sind nur die potentiell beweiserheblichen Daten/Dateien erst nach der Durchsicht durch richterliche Anordnung zu beschlagnahmen.[341] Wenn die Durchsuchungsbeamten ohne diesen Vorgang direkt vor Ort sämtliche aufgefunden Unterlagen beschlagnahmen, ist dies unverhältnismäßig und bedenklich. In diesem Sinne unterbindet § 110 StPO bei „Beschlagnahme von Papieren" die Ausübung der Eilkompetenz wegen Gefahr im Verzug und verhilft dem Richtervorbehalt zur Durchsetzung.[342]

In der Praxis wird aber die Wirksamkeit des § 110 StPO zum einen durch die Missachtung der Vorschrift selbst (vgl. oben II. 1. c) dd) und 2.) und zum anderen durch die Umgehung der Beschränkung der Durchsichtsbefugnis erheblich beeinträchtigt (vgl. unten 2. b) cc)). Doch dies läuft dem Sinn und Zweck des § 110 StPO zuwider. Allerdings kann die Beachtung dieser Vorschrift in der Durchsuchungspraxis, die sich nur an der Effektivität der Aufklärung von Straftaten orientiert, wegen der Umständlichkeit wie Zeit- und Reibungsverlust hinderlich sein.[343] Gleichwohl ist diese Diskrepanz verfassungsrechtlich im Lichte der Rechtsstaatlichkeit oder der Justizförmigkeit des Strafverfahrens einerseits und verfahrensrechtlich im Interesse des Richtervorbehalts oder des Rechtsschutzes des Einzelnen andererseits aufzuheben.[344]

[340] *LG Berlin* NStZ 2004, 571, 573 [Rn. 23]; *Bruns*, KK-StPO, § 110 Rn. 4; *Park*, § 2 Rn. 248 und 261 a. E.; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 6 und 27; *Hiéramente*, wistra 11/2016, 432, 432 f.: bei einer Unternehmensdurchsuchung nach § 103 StPO; abw. *Kemper*, wistra 5/2006 171, 172 [Tz. 2.]: Wenn bereits die Durchsuchung unter den Voraussetzungen von Gefahr in Verzug erfolgen durfte, dann wird regelmäßig auch die Beschlagnahme der vorgefundenen Beweismittel aufgrund der Gefahr in Verzug erfolgen.

[341] *LG Berlin* NStZ 2004, 571, 573 [Rn. 23]: Zum Schluss ist eine Beschlagnahmeanordnung der zum Zweck der Durchsicht vorläufig sichergestellten Papiere stets dem Richter vorbehalten.

[342] Vgl. *Wohlers/Jäger*, SK-StPO, § 110 Rn. 6.

[343] *Dauster*, StraFo 6/1999, 186, 189.

[344] Zust. *Dauster*, StraFo 6/1999, 186, 188 f.

2. Tatbestände

a) Durchsicht von Papieren

aa) Papiere

Im Lichte des Sinns und Zweck des § 110 StPO ist der Begriff der Papiere weit auszulegen.[345] Dazu gehört alles private und geschäftliche Schriftgut, was wegen seines Gedankeninhalts Bedeutung hat, unabhängig davon, auf welchen Informationsträgern es festgehalten ist.[346] Als Papiere i. S. d. Vorschrift nicht nur die Informationsträger in Papierform, sondern auch diejenigen, bei denen ein anderes Material oder System verwendet wird, anzusehen.[347] Umfasst werden somit vom Anwendungsbereich § 110 StPO beispielsweise nicht nur analoge Medien oder Gedankenträger wie Ton- und Bildträger, sondern heutzutage auch alle Arten von digitalen Datenträgern (z. B. Magnetbänder, CDs, DVDs, USBs oder Festplatten) und EDV-Anlagen (z. B. PCs, Notebooks oder Smartphones) sowie die darauf gespeicherten EDV-Daten (einschließlich der auf dem Server der Anbieter vorhandenen E-Mails[348]).[349] Gleiches gilt außerdem nicht nur für die Software (Betriebssysteme, Programme etc.) und Hardware, die zur Lesbarkeit der Daten erforderlich ist,[350] sondern auch für die lesbaren Aufzeichnungen von Daten.[351]

bb) Durchsicht

Die Durchsicht von Papieren i. S. d. § 110 StPO bedeutet einen Einblick in ihren Inhalt, nämlich eine Kenntnisnahme ihres Inhalts.[352] Sie stellt ein Mittel zur inhaltlichen Überprüfung dar, ob die aufgefundenen Papiere zur (endgültigen) Beschlagnahme beim Richter zu beantragen oder zurückzugeben/zu löschen sind.[353]

---

[345] *BGH-Ermi-Ri* CR 1999, 292, 293; M-G/*Schmitt*, StPO, § 110 Rn. 1; *Park*, § 2 Rn. 232.

[346] *BGH* NStZ 2003, 670, 671 [Rn. 6]; *Bruns*, KK-StPO, § 110 Rn. 2; M-G/*Schmitt*, StPO, § 110 Rn. 1; *Park*, § 2 Rn. 232 f.; *Peters*, NZWiSt 2017, 465, 467.

[347] *Dauster*, StraFo 6/1999, 186; M-G/*Schmitt*, StPO, § 110 Rn. 1; *Wohlers*/*Jäger*, SK-StPO, § 110 Rn. 8.

[348] Vgl. *BVerfGE* 124, 43, 68 f. [Rn. 87 f.]; NJW 2014, 3085, 3088 [Rn. 44]: die vorläufige Sicherstellung größerer Teile oder gar des gesamten E-Mail-Bestands; *BGH* NJW 2010, 1297, 1298 [Rn. 19]; *Meininghaus*, Der Zugriff auf E-Mails, 2007, 197 ff.

[349] *BVerfGE* 113, 29, 50 f. [Rn. 100 f.]; NJW 2002, 1410: die Daten auf dem Notebook; *BGH* NStZ 2003, 670, 671 [Rn. 6]; *BGH-Ermi-Ri* CR 1999, 292, 293; *Bruns*, KK-StPO, § 110 Rn. 2; M-G/*Schmitt*, StPO, § 110 Rn. 1; *Park*, § 4 Rn. 233, 812; *Peters*, NZWiSt 2017, 465, 467; *Szesny*, WiJ 2012, 228.

[350] *LG Trier* NJW 2004, 869; *Bruns*, KK-StPO, § 110 Rn. 2; *Park*, § 2 Rn. 812.

[351] *BVerfG* NJW 2002, 1410; *BGH-Ermi-Ri* CR 1999, 292, 293.

[352] *Graulich*, wistra 8/2009, 299, 300; *Park*, § 2 Rn. 234; *Wohlers*/*Jäger*, SK-StPO, § 110 Rn. 12 und 20.

[353] M-G/*Schmitt*, StPO, § 110 Rn. 2; *Park*, § 2 Rn. 234 und 248; *Wicker*, MMR 2013, 765, 767; vgl. *Wohlers*/*Jäger*, SK-StPO, § 110 Rn. 20.

Dadurch sind beschlagnahmefreie bzw. -verbotene und verfahrensirrelevante Informationen aus dem Strafverfahren möglichst frühzeitig auszuschließen. In seltenen Fällen, falls die bei der Durchsuchung aufgefunden Papiere nur solche Informationen enthalten, ist die Durchsicht höchstmöglich zurückzuhalten.[354] Nach dem Grundsatz der Zweckbindung (vgl. Kapitel 2, A. III. 1. b)) beschränkt sich diese Durchsicht auf die Prüfung, ob die gefundenen Papiere von der Durchsuchungsanordnung erfasst sind und als Beweismittel in Betracht kommen. Die Durchsicht zum anderen Zweck ist daher nicht zulässig und rechtswidrig. Unzulässig ist somit die gezielte oder willentliche Durchsicht von Papieren bei einer Durchsuchung zum Zweck des Auffindens und der Beschlagnahme von Waffen, Sprengstoffen oder Betäubungsmitteln etc. oder diejenige von Unterlagen, die außerhalb des in richterlichem Beschluss angegebenen Zeitraums liegen.[355] Wenn während der Durchsicht Unterlagen, die auf die Verübung einer anderen Straftat hindeuten, zufällig gefunden werden, sind sie nach § 108 StPO einstweilen zu beschlagnahmen (vgl. unten 4.).

Bei der Durchsicht sind je nach den Umständen des Einzelfalls unterschiedliche, miteinander kombinierbare Möglichkeiten der materiellen Datenzuordnung und -trennung in Betracht zu ziehen.[356] Im Rahmen der materiellen/inhaltlichen Datenzuordnung durch die Durchsicht im EDV-Bereich ist u. a. die Auswertung der Struktur eines Datenbestands von Bedeutung.[357] Dabei kann eine Zuordnung der Daten nach Verfahrensrelevanz beispielsweise themen-, zeit- oder personenbezogen oder auch durch Anwendung automatisierter Suchfunktionen mit geeigneten Suchbegriffen oder speziellen Suchprogrammen erfolgen.[358] In der Praxis sollen diesbezüglich regelmäßig fast immer zwei Listen erstellt werden: die „Liste der gesuchten konkretisierten Beweismittel" (was wird gesucht?) und die „Liste der Suchbegriffe bzw. Schlagwörter" (wie wird gesucht?).[359] Bei der Ersteren handelt es sich um die zu beschlagnahmenden Gegenstände, während die Letztere die Mittel

[354] M-G/*Schmitt*, StPO, § 110 Rn. 2; vgl. *BVerfGE* 124, 43, 67: „*Wird festgestellt, dass sich auf dem Mailserver überhaupt keine verfahrenserheblichen E-Mails befinden können, wäre eine Sicherstellung schon ungeeignet.*"

[355] Vgl. M-G/*Schmitt*, StPO, § 110 Rn. 1; *Park*, § 2 Rn. 235 f.

[356] *BVerfGE* 113, 29, 55 [Rn. 114 ff.]; 124, 43, 67 f. [Rn. 88 ff.]; M-G/*Schmitt*, StPO, § 94 Rn. 19a. Ist diese Zuordnung und Trennung jedoch den Strafverfolgungsbehörden unter zumutbaren Bedingungen nicht möglich, so ist unter dem Gesichtspunkt der Erforderlichkeit – ausnahmsweise – die „Beschlagnahme" des gesamten Datenbestands oder sämtlicher Daten möglich (*BVerfGE* 113, 29, 57 [Rn. 120]; 124, 43, 69 [Rn. 89]; M-G/*Schmitt*, a. a. O.), und dies ist ggf. auch dann mit dem Verhältnismäßigkeitsgrundsatz vereinbar, wenn konkrete Anhaltspunkte dafür vorliegen, dass sie für das Verfahren potentiell beweiserheblich sind (*BGH* NJW 2010, 1297, 1298 [Rn. 16]; M-G/*Schmitt*, a. a. O.).

[357] Vgl. *Hiéramente*, wistra 11/2016, 432, 435 [Tz. b)]: Hier ist der gesamte Datenspeicher potentielles Durchsuchungsgebiet.

[358] *BVerfGE* 113, 29, 55 f. [Rn. 116]; 124, 43, 68 [Rn. 86]. Bei Durchsuchung der E-Mails ist eine Zuordnung anhand bestimmter Übermittlungszeiträume oder Sender- und Empfängerangaben in Betracht zu ziehen (a. a. O.; *BGH* NJW 2010, 1297, 1298 [Rn. 19]); *Peters*, NZWiSt 2017, 465, 469 am Anfang).

[359] *Hiéramente*, wistra 11/2016, 432, 435.

zum Heraussuchen solcher Daten, nämlich ein Instrument zur Durchsuchung, darstellt. Den Suchbegriffen wird die Funktion beigemessen, die immense Datenmasse auf potentiell beweisrelevante Daten einzuschränken.[360] Je nach den Umständen des Einzelfalls hat die StA die Durchsuchung und Beschlagnahme anhand der Listen zu beantragen, die auf der Grundlage der bis dahin festgestellten Tatsachen erstellt wurden,[361] und der Ermittlungsrichter hat nach Feststellung der Angemessenheit der Liste einen Durchsuchungsbeschluss zu erlassen. Er kann – ggf. in Absprache mit der StA – die Suchbegriffe teilweise löschen oder ändern. Hierbei ist es umstritten, inwieweit die Datenzuordnung über die Suchbegriffe konkret erlaubt/geboten ist. Dabei handelt es sich um die Gefahr der Offenlegung der Intimsphäre des Einzelnen oder der Betriebs- und Geschäftsgeheimnisse oder Personaldaten der Unternehmen im Zuge der Suche. Zwar wird in der Praxis behauptet, dass eine zu komplett oder ausführlich erstellte Liste von Suchbegriffen zu weit geht, jedoch müssen sie auf jeden Fall zumindest inhaltlich mit der Verfahrensrelevanz oder der potenziellen Beweiserheblichkeit in Zusammenhang stehen; in diesem Fall kann die Suche nach der Liste keine gezielte Suche nach Zufallsfunden darstellen.[362]

cc) Erweiterung der Durchsicht um externe Speichermedien: Abs. 3

(1) Die Durchsicht eines Endgerätes wie PC oder Smartphone des von der Durchsuchung Betroffenen darf auch auf hiervon räumlich getrennte Speichermedien, z. B. Datenträger/Server im Intra- oder Internet,[363] erstreckt werden (§ 110 Abs. 3 S. 1 StPO). Die Vorschrift entspricht Art. 19 Abs. 2 CKÜ und wurde durch das TKÜG, das am 01. Januar 2008 in Kraft trat, in die StPO eingeführt. Dies trägt dem Umstand Rechnung, dass beweiserhebliche Daten bei der Durchsuchung elektronischer Datenträger vielfach bei einem vom Ort räumlich getrennten, externen Anbieter ausgelagert sind, und der Besorgnis darüber, dass die Suche nach den Daten eine erhebliche Zeitverzögerung und damit einen Beweismittelverlust verursacht.[364] Bei der Durchsicht nach § 110 StPO handelt es sich nicht um eine heimliche Durchsuchung.[365] Sie setzt eine offene Durchsuchung durch die Endgeräte des Be-

[360] *Hiéramente*, wistra 11/2016, 432, 435 [Tz. (1)]: Schlagwortliste kann eine Benennung „bestimmter Gegenstände" (i. S. d. § 103 StPO) nicht ersetzen. Außerdem können durch einen Suchlauf mittels geeigneter Schlagwörter der Umfang und die Dauer der Durchsuchung erheblich reduziert werden (a. a. O. 436).

[361] Zust. *Peters*, NZWiSt 2017, 465, 472 [Tz. IV. a. E.]: die Vorlage von Suchwortkatalogen im Zuge der Beantragung der Anordnung.

[362] *Wohlers/Jäger*, SK-StPO, § 110 Rn. 21.

[363] Vgl. *Brodowski/Eisenmenger*, ZD 3/2014, 119, 120 f.: Netzwerklaufwerke und technisches Äquivalent zur lokalen Speicherung.

[364] M-G/*Schmitt*, StPO, § 110 Rn. 6.

[365] Vgl. BT-Drs. 16/6979, S. 45: Charakter der Maßnahme als Teil einer „offenen" Durchsuchung; *Brodowski*, JR 2009, 402, 408; *Brodowski/Eisenmenger*, ZD 3/2014, 119, 122 [Tz. a)]; *Michalke*, StraFo 3/2014, 89, 92; *Wicker*, MMR 2013, 765, 766; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 10. Im Schrifttum wird die Durchsuchung durch diesen Zugriff teilweise als

troffenen voraus und darf die heimliche Online-Durchsuchung oder die Quellen-TKÜ nicht legitimieren.[366] So muss sie unter der Regelung nach §§ 105 – 109 i. V. m. §§ 33 Abs. 3 – 4, 35 StPO stattfinden.[367]

(2) Die „räumlich getrennten Speichermedien" und das „(lokale) Speichermedium" i. S. d. S. 1 bedeuten informationstechnische Systeme; so sind sie in einem weiten Sinne zu verstehen.[368] Da heute in fast allen Arten der Kommunikationen wie z. B. E-Mail-Dienste, soziale Netzwerke, Internet-Foren oder Cloud-Computing sowohl TK-Daten als auch sonstige allgemeine Daten auf dem Online-Speicherplatz gespeichert sind, steht ein enges Verständnis der Speichermedien der Gesetzesbegründung entgegen.[369] Zum anderen können die externen Speichermedien auch unter die „dem von Durchsuchung Betroffenen gehörenden Sachen" i. S. d. § 102 StPO fallen (vgl. oben II. 1. c) aa)), weil er faktisch auf die Sache und deren Inhalt zugreifen kann. Dass auch Dienstanbieter darauf zugreifen können, ist hierbei nicht entscheidend, weil es hier nicht auf eine Zuordnung nach zivilrechtlichen Eigentumsgrundsätzen, sondern auf einen strafrechtlichen Gewahrsam, also die tatsächliche Sachherrschaft, ankommt.[370]

Die Vorschrift unterliegt den bestimmten Voraussetzungen: Der externe Speicherplatz muss vom durchsuchten Gerät aus zugänglich sein (S. 1 Hs. 1), und ohne Erstreckung der Durchsicht muss der „Verlust beweisrelevanter Daten besorgt" werden (Hs. 2).[371] Dies ist insb. der Fall, wenn noch vor einer körperlichen Sicherstellung des externen Speichermediums – mit erheblicher Verzögerung – die

„kleine Online-Durchsuchung" bezeichnet (*Brodowski/Eisenmenger*, a. a. O.; *Gaede*, StV 2009, 96, 101; *Michalke*, a. a. O. 91; *Zimmermann*, JA 5/2014, 321, 322 [Fn. 23]). Bevor die Ermächtigungsgrundlage zur (heimlichen) Online-Durchsuchung (§ 100b StPO) im Jahre 2017 begründet wurde, hat sie allerdings begrifflich stets eine Heimlichkeit nicht vorausgesetzt. Jedoch ist die Verwendung solcher Ausdrücke nach der Gesetzgebung nicht mehr angebracht, um Verwechslungen mit der neuen Maßnahme zu vermeiden. Zum anderen verwendet *Sieber* für die Quellen-TKÜ den Begriff „kleine Online-Durchsuchung" (*Sieber*, 69. DJT 2012, C 105).

[366] M-G/*Schmitt*, StPO, § 110 Rn. 6; *Wohlers/Jäger*, SK-StPO, § 102 Rn. 15; insb. BT-Drs. 16/6979, S. 45: „*Klarzustellen ist, dass auch mit der modifizierten Fassung des § 110 Abs. 3 StPO keine verdeckte Onlinedurchsuchung erlaubt wird, wie sie derzeit im politischen Raum diskutiert wird. Insbesondere ermächtigt § 110 Abs. 3 StPO nicht dazu, das durchsuchte Speichermedium oder die externen Speichermedien derart zu manipulieren, dass auf diesen Medien oder Systemen heimlich eine Software aufgebracht wird, die eine Überwachung dieser Medien zulässt.*"

[367] Vgl. *Brodowski/Eisenmenger*, ZD 3/2014, 119, 125 [Tz. 5.].

[368] Vgl. BT-Drs. 16/5846, S. 27: Computersysteme; auch *Schlegel*, HRRS 2008, 23, 27.

[369] A. A. *Brodowski/Eisenmenger*, ZD 3/2014, 119, 122: In teleologischer Auslegung ist die sachliche Reichweite des § 110 Abs. 3 StPO auf diejenigen Dienste zu beschränken, deren alleiniger oder zumindest überwiegender Zweck es ist, eine lokale Datenspeicherung zu ersetzen bzw. zu ergänzen.

[370] *Wicker*, MMR 2013, 765, 766 f.; *Wohlers/Jäger*, SK-StPO, § 102 Rn. 15a f.; auch *Peters*, NZWiSt 2017, 465, 467: physischer Zugriff.

[371] M-G/*Schmitt*, StPO, § 110 Rn. 6; *Park*, § 2 Rn. 817; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 9.

Löschung, die Veränderung und die Unterdrückung solcher Daten zu erwarten ist.[372] Können die zugegriffenen Daten für die Untersuchung von Bedeutung sein, so dürfen sie zumeist auf einem Datenträger der Strafverfolgungsbehörden gesichert werden (S. 2 Hs. 1).[373] Da dabei die Inhaber des externen Speichermediums wie Anbieter oder Unternehmen nicht der von der Durchsuchung Betroffene, sondern Dritte sind, gilt zu ihrem Rechtsschutz § 98 Abs. 2 StPO entsprechend (Hs. 2).[374] Hierbei soll daher der eine Durchsicht durchführende Beamte unter den Voraussetzungen des § 98 Abs. 2 S. 1 StPO binnen drei Tagen die gerichtliche Bestätigung – hinsichtlich der Sicherung der auf dem externen Speichermedium gesicherten Daten – beantragen.[375] Das dafür zuständige Gericht hat dabei gemäß § 33 Abs. 2 und 3 StPO vor der Bestätigung dem Betroffenen, nämlich dem Inhaber des externen Speichermediums, rechtliches Gehör zu gewähren, wodurch er die Maßnahme zur Kenntnis nehmen und seine rechtlichen Interessen wahrnehmen kann.[376] Dies ist auch durch eine Belehrung nach § 98 Abs. 2 S. 5 StPO und einen Antrag auf gerichtliche Entscheidung nach S. 2 möglich.[377] Im Ergebnis verliert diese Maßnahme nach alledem auch ihm als Dritten gegenüber nicht den Charakter einer offenen Durchsuchung.[378]

(3) Andererseits wird die Frage gestellt, ob die Maßnahme nach Abs. 3 in die völkerrechtliche Souveränität des Drittstaats eingreift und unter welchen Bedingungen sie gerechtfertigt werden kann, wenn sich die externen Speichermedien der Vorschrift, nämlich die Server von Anbietern oder Unternehmen, im Ausland befinden. Dabei handelt es sich grundlegend um die Voraussetzungen für die Zulässigkeit grenzüberschreitender Online-Ermittlungsmaßnahmen in Cyberspace. Zwar greifen Hoheitsmaßnahmen im Ausland ohne Ermächtigung grundsätzlich in die völkerrechtliche Souveränität des betroffenen Staates ein.[379] Doch könnte ein solcher Zugriff auf bei einem Server im Ausland befindliche, aber öffentlich zugängliche

[372] BT-Drs. 16/6979, S. 44; M-G/*Schmitt*, StPO, § 110 Rn. 6; *Park*, § 2 Rn. 817; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 9. Nach einer Meinung wird jedoch eingewendet, dass diese Voraussetzung aber keine wirkliche Einschränkung wäre (*Brodowski/Eisenmenger*, ZD 3/2014, 119, 124). Der Wortlaut sei nämlich gleicherweise auszulegen wie „bei Gefahr im Verzug" i. S. d. § 100e Abs. 1 S. 2 StPO. Demzufolge sei diese Klausel im Fall der Besorgnis über den Beweismittelverlust, die die Ermittlungsbehörden selbst herbeiführen, nicht anzuwenden (vgl. oben II. 2. b. (2)).

[373] BT-Drs. 16/6979, S. 44 a. E.; M-G/*Schmitt*, StPO, § 110 Rn. 7; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 9.

[374] BT-Drs. 16/6979, S. 45; *Park*, § 4 Rn. 820; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 9.

[375] BT-Drs. 16/6979, S. 45; M-G/*Schmitt*, StPO, § 110 Rn. 8.

[376] BT-Drs. 16/6979, S. 45; M-G/*Schmitt*, StPO, § 110 Rn. 8; *Park*, § 4 Rn. 820; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 9.

[377] Vgl. M-G/*Schmitt*, StPO, § 110 Rn. 11; *Park*, § 4 Rn. 820.

[378] M-G/*Schmitt*, StPO, § 110 Rn. 8; *Obenhaus*, NJW 2010, 651, 653 [Tz. 2.]; abw. *Zimmermann*, JA 5/2014, 321, 322: Die Maßnahme stellt aus Sicht des Providers eine heimliche Maßnahme dar, aber ihre Zulässigkeit bei offener Ermittlung ist die gesetzgeberische Wertung in § 110 Abs. 3 StPO.

[379] *Kasiske*, StraFo 6/2010, 228, 234; *Sieber*, 69. DJT 2012, C 143 f.

Daten ungeachtet des Speicherorts für die Vertragsstaaten nach Art. 32 lit. a CKÜ und für Nicht-Vertragsstaaten völkergewohnheitsrechtlich begründet werden.[380] Dagegen ist für einen solchen Zugriff auf nichtöffentlich zugängliche Daten nach lit. b – zumindest für die Vertragsstaaten – die rechtmäßige und freiwillige Zustimmung der berechtigten Person erforderlich.[381] Sonst ist er grundsätzlich nicht zulässig und ein förmliches Rechtshilfeersuchen erforderlich (Art. 31 Abs. 1 CKÜ).[382]

Demzufolge bedarf es nach einigen Ansichten zum Zugriff nach Abs. 3 grundsätzlich eines Rechtshilfeersuchens an die Staaten, in denen die Server vorhanden sind, und wenn dies nicht befolgt werde, verletze er die fremdstaatliche Souveränität und die Rechtshilfeabkommen und schließlich sei dies völkerrechtswidrig und könne i. d. R. zu einem Beweisverwertungsverbot führen.[383] Insbesondere laut *Sieber* gehört auch eine vom Inland in das Ausland hineinreichende Maßnahme über das Internet zum Souveränitätseingriff, weil es völkerrechtlich unerheblich sei, dass sich der Beamte nicht physisch auf fremdem Territorium befinde.[384] Diese Verletzung könne ausnahmsweise nur im Fall der Beachtung der erforderlichen Sorgfalt ausgeschlossen werden, eine solche Online-Ermittlung gehöre jedoch in aller Regel nicht zu dieser Ausnahme; denn die Strafverfolgungsbehörden müssten im Vorfeld der Maßnahme den genauen Serverstandort in Rechnung stellen.[385] In diesem Fall muss die Einsichtnahme daher unterbleiben, wenn zum Zeitpunkt der Maßnahme unklar ist, ob der externe Datenspeicher im Inland oder im Ausland besteht,[386] und nur eine vorläufige Sicherung i. V. m. einem Rechtshilfeersuchen kann in Betracht kommen.[387] Dieses Problem bleibe nun noch ausstehend und es fehlt bisher an entsprechenden völkerrechtlichen Verträgen oder Gewohnheitsrechten.[388]

---

[380] *Bruns*, KK-StPO, § 110 Rn. 8a; M-G/*Schmitt*, StPO, § 110 Rn. 7a; insb. *Sieber*, 69. DJT 2012, C 144 f.: Angesichts der heute selbstverständlichen weltweiten Nutzung des Internets, der häufig fehlenden Kenntnis der Nutzer über den Speicherort abgerufener Daten sowie der geringen Eingriffsintensität einer Abfrage öffentlicher Daten im globalen Cyberspace.

[381] Vgl. *Brodowski/Eisenmenger*, ZD 3/2014, 119, 123; krit. *Sieber*, 69. DJT 2012, C 145 f.: Unter den Vertragsstaaten besteht indes keine Einigkeit über Auslegung und Grenzen der Vorschrift, nämlich keine einheitliche Rechtsauffassung, und vor allem ist das Individuum nicht über die staatliche Souveränität dispositionsbefugt.

[382] *Bruns*, KK-StPO, § 110 Rn. 8a; *Gaede*, StV 2009, 101 f.; M-G/*Schmitt*, StPO, § 110 Rn. 7a; *Obenhaus*, NJW 2010, 651, 654.

[383] *Bär*, EDV-Beweissicherung, Rn. 375; *Park*, § 4 Rn. 801; *Sieber*, 69. DJT 2012, C 148: als Völkerrechtsverstoß über Art. 25 GG; *Zimmermann*, JA 5/2014, 321, 322 f.; auch *Kudlich*, GA 2011, 193, 208: *„§ 110 Abs. 3 StPO sich allein auf im Inland extern gespeicherte Daten bezieht."*

[384] *Sieber*, 69. DJT 2012, C 144.

[385] *Sieber*, 69. DJT 2012, C 147.

[386] *Park*, § 4 Rn. 819.

[387] *Zimmermann*, JA 5/2014, 321, 323 am Anfang.

[388] *Sieber*, 69. DJT 2012, C 149.

Diesen Meinungen ist aber angesichts der gegenwärtigen Dringlichkeit der Ermittlungen nicht zuzustimmen. Bei einer Durchsicht externer Speichermedien gemäß § 110 Abs. 3 StPO ist es zumeist – vor Ort umgehend – nicht feststellbar, unter welcher Souveränität sich die Server, auf denen die gesuchten Daten gespeichert sind, überhaupt befinden.[389] Heutzutage können Server überall auf der Welt aufgestellt werden und ihre Betreiber wie Anbieter oder Unternehmen können etwa aus geschäftlichen Gründen den Speicherort jederzeit sofort an einen anderen verlegen.[390] Außerdem sind die Daten in aller Regel au Sicherheitsgründen auf unterschiedliche Staaten verteilt gespeichert. Aus Sicht der Strafverfolgungsbehörden ist somit es unklar, an welche Staaten sich ein förmliches Rechtshilfeersuchen richten sollte.[391] Dies ist eine unüberwindbare praktische Schwierigkeit.[392] Aus diesen Gründen löst die bloße Möglichkeit, dass die Daten sich irgendwo im Ausland befinden, bei den Ermittlungsbehörden keine Rechtshilfeverpflichtung aus[393] und die fehlende Berücksichtigung beinhaltet auch keine willkürliche Missachtung der ausländischen Souveränität.[394] Greifen deutsche Ermittlungsbeamte über das Gerät und den Account des von der Durchsuchung Betroffenen im Inland auf ein externes Speichermedium zu für die von ihm genutzten TK-Dienste wie E-Mail, soziale Netzwerke oder Cloud-Computing etc. (vgl. hierbei zur Erhebung von Zugangscodes unten (4)), so ist dies daher regelmäßig eine rechtmäßige Ermittlungshandlung im Inland, die von § 110 Abs. 3 StPO erfasst werden kann, und verletzt keine Souveränität fremder Staaten, solange keine Willkür vorliegt. Demzufolge führt dies auch nicht zu einem Beweisverwertungsverbot.[395] Hierbei ist jedoch ein Beweisverwertungsverbot etwa dann anzunehmen, wenn die Sicherstellung bzw. Verwertung der Daten gegen den ausdrücklichen Widerspruch des Staates erfolgt, in dessen Sou-

[389] *Wohlers/Jäger*, SK-StPO, § 102 Rn. 15a; dazu *Kasiske*, StraFo 6/2010, 228, 234: „*Vorerst ungelöst bleibt das Problem, wie die Strafverfolgungsbehörden im Einzelfall ermitteln sollen, in welchem Land sich der Server mit den begehrten Daten befindet.*"

[390] *Kasiske*, StraFo 6/2010, 228, 234; *Obenhaus*, NJW 2010, 651, 653.

[391] M-G/*Schmitt*, StPO, § 110 Rn. 7b; auch *Wicker*, MMR 2013, 765, 768 [Tz. IV.].

[392] *Wohlers/Jäger*, SK-StPO, § 102 Rn. 15a; dazu *Kudlich*, GA 2011, 193, 208: rein praktische Probleme.

[393] Zust. M-G/Schmitt, StPO, § 110 Rn. 7b; vgl. T-CY Guidance Note # 3, Transborder access to data (Art. 32) vom 3. Dez. 2014, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726a, Abruf: 31. 12. 2020, 6 [Tz. 3.2]; auch T-CY Ad-hoc Sub-group on Jurisdiction and Transborder Access to Data vom 6. Dez. 2012, What are the options?, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8, Abruf: 31. 12. 2020, 29 [Rn. 138].

[394] Zust. *Wohlers/Jäger*, SK-StPO, § 102 Rn. 15a, § 110 Rn. 30a; dazu *Wicker*, MMR 2013, 765, 768 f.: „*Beim Zugriff … liegt mangels Kenntnis über den Speicherort keine willkürliche Überschreitung der eigenen Hoheitsmacht vor. … Soweit also ein Zugriff beim Cloud-Nutzer möglich ist, ist der Ort der Daten nicht von Bedeutung.*"

[395] Zust. *Brodowski/Eisenmenger*, ZD 3/2014, 119, 123; M-G/*Schmitt*, StPO, § 110 Rn. 7c; *Wicker*, MMR 2013, 765, 768 f.; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 30a.

veränität eingegriffen wurde,[396] oder wenn die deutschen Ermittlungsbehörden sich bewusst über völkerrechtlich verbürgerte Individualrechte hinwegsetzen.[397]

Falls ein Versuch, auf die Daten über das Endgerät und den Account des Betroffenen zuzugreifen, den Ermittlungsbehörden misslungen ist, können diese auch aufgrund des § 103 StPO direkt von inländischen Mutter- oder Tochterunternehmen die Daten gewinnen, wobei es sich nicht um eine Souveränitätsverletzung bzw. ein Rechtshilfeersuchen handelt.[398] Denn es ist Sache der Dienstanbieter bzw. Unternehmen, zu entscheiden, in welchem Staat die Kunden- oder Geschäftsdaten gespeichert werden und ob sie an einen anderen Speicherort verschoben werden, und darüber hinaus sind die transnational tätigen Anbieter bzw. Unternehmen auch verpflichtet, bei rechtmäßiger Anordnung der Durchsuchung und Beschlagnahme in bestimmtem Territorium mitzuwirken und auf Erfordern den Ermittlungsbehörden die Daten vorzulegen und herauszugeben (vgl. § 95 Abs. 1 StPO für freiwillige Herausgabe, §§ 94, 95 Abs. 2 und 98 Abs. 1 StPO für Beschlagnahme oder erzwungene Herausgabe i. V. m. dem Richtervorbehalt).

(4) Insoweit stellt sich die Frage, wie die Ermittlungsbehörden dem Fall entgegenwirken müssen, wenn externe Speichermedien durch eine „Zugangsberechtigung", nämlich „Nutzerkennung" und „Passwort" zum Zugang (sog. „Einloggen bzw. Log-in"), geschützt sind und diese von dem von der Durchsuchung Betroffenen nicht freiwillig herausgegeben werden.[399] Zunächst ist der Beschuldigte gestützt auf das Verbot des Zwangs zur Selbstbelastung verpflichtet, diese Sicherungsdaten auf Verlangen den Behörden freiwillig herauszugeben (vgl. Absehen von Anwendung des § 95 Abs. 1 StPO).[400] Hingegen kann der Durchsuchungsbeamte mittels – zufällig – vorgefundener Zugangscodes (insb. durch Lesezeichen im Webbrowser und auf dem Rechner installierte Programme, die Zugangsdaten zu Webdiensten zu speichern)[401] oder auch durch die Entschlüsselung mit eigenen technischen Mitteln

[396] *BGHSt* 34, 334, 344; *Bruns*, KK-StPO, § 110 Rn. 8a; M-G/*Schmitt*, StPO, § 110 Rn. 7c; *Sieber*, 69. DJT 2012, C 148; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 30a.

[397] *Bruns*, KK-StPO, § 110 Rn. 8a; M-G/*Schmitt*, StPO, § 110 Rn. 7c; *Sieber*, 69. DJT 2012, C 148; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 30a.

[398] A. A. *Sieber*, 69. DJT 2012, C 147 f.: Auch bei Datenbeschaffung über Mutter- und Tochterunternehmen gelten die oben dargestellten Grundsätze.

[399] Dabei ist eine Umgehung oder eine Überwindung des Zugangscodes auf dem nicht dafür vorgesehenen Weg nicht gestattet, weil sie einen verdeckten Zugriff darstellt, der auf der Grundlage des § 110 Abs. 3 StPO nicht zu rechtfertigen ist (zust. *Brodowski/Eisenmenger*, ZD 3/2014, 119, 123).

[400] *Bruns*, KK-StPO, § 95 Rn. 2; M-G/*Schmitt*, StPO, § 95 Rn. 5; *Obenhaus*, NJW 2010, 651, 652 a. E.; *Park*, § 4 Rn. 817; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 10 und § 95 Rn. 12 und 20; *Zimmermann*, JA 5/2014, 321, 322; abw. *Bäumerlich*, NJW 2017, 2718, 2720 [Tz. 1.]: gemäß § 136a StPO.

[401] *Brodowski/Eisenmenger*, ZD 3/2014, 119, 123; *Klein*, NJW 2009, 2996, 2998 a. E.; M-G/*Schmitt*, StPO, § 110 Rn. 6; *Obenhaus*, NJW 2010, 651, 652; *Zerbes/El-Ghazi*, NStZ 2015, 425, 429 f.; *Zimmermann*, JA 5/2014, 321, 322; vgl. auch *Bäumerlich*, NJW 2017, 2718, 2720 [Tz. 1.]: als Annex zu der erfolgten Sicherstellung gemäß § 94 StPO.

(sog. „Knacken" von Passwörtern)[402] darauf zugreifen. Insb. die letztere Vorgehensweise ist als unmittelbarer Zwang durch § 110 Abs. 3 StPO – i. V. m. §§ 102, 103 StPO – gedeckt.[403] Wie bei der Durchsetzung der Durchsuchung die Vorgehensweise üblich ist, dass die Ermittler vor Ort die verschlossenen Türen oder Schlösser von Gebäuden, Wohnungen, Aktenschränken, Belegablagen oder Behältnissen gewaltsam öffnen und Beweismaterialien suchen, ist ein vergleichbarer Zwang auch beim Zugriff auf einen externen Speicher nach Abs. 3 einzusetzen.[404] Dies geschieht nur im Cyberspace innerhalb des Gerätes des Betroffenen und vor allem zumindest mit Wissen des Betroffenen und seines Vertreters, insb. am Ort vor ihnen (vgl. § 106 Abs. 1 StPO). Wenn daneben Kennungen bzw. Passwörter als solche von den Anbietern oder Unternehmen den Ermittlungsbehörden – mit oder ohne Wissen des Betroffenen – übermittelt werden, sollten die Voraussetzungen und das Verfahren des § 100j Abs. 1 S. 2, Abs. 3 und 4 StPO in Rechnung gezogen werden.

b) Befugnisse zur Durchsicht

aa) Zur Durchsicht befugte Beamte: Abs. 1

Aus der Auslegung nach dem Wortlaut des § 110 StPO sind für die Durchsicht der bei Durchsuchung aufgefundenen Papiere die StA und auf deren Anordnung ihre Ermittlungspersonen (§ 152 GVG) – einschließlich des Richters[405] – grundsätzlich zuständig.[406] Zwar wird die Durchsichtsbefugnis der Ermittlungspersonen von der

[402] M-G/*Schmitt*, StPO, § 110 Rn. 6; *Obenhaus*, NJW 2010, 651, 653; *Peters*, NZWiSt 2017, 465, 467; *Zerbes/El-Ghazi*, NStZ 2015, 425, 429 f.; *Zimmermann*, JA 5/2014, 321, 322; a. A. *Brodowski/Eisenmenger*, ZD 3/2014, 119, 123: Ein sog. „brute-force"-Angriff zum Erraten der Zugangsdaten ist auf der Grundlage des § 110 Abs. 3 StPO nicht gestattet.

[403] Zust. *Obenhaus*, NJW 2010, 651, 653; *Peters*, NZWiSt 2017, 465, 467; a. A. *Brodowski/Eisenmenger*, ZD 3/2014, 119, 123.

[404] Zust. *Obenhaus*, NJW 2010, 651, 653: Das Knacken macht den Zugriff nicht zu einem heimlichen; vgl. M-G/*Schmitt*, StPO, § 105 Rn. 13; a. A. *Brodowski/Eisenmenger*, ZD 3/2014, 119, 123.

[405] *Bruns*, KK-StPO, § 110 Rn. 1; M-G/*Schmitt*, StPO, § 110 Rn. 3; *Mildeberger/Riveiro*, StraFo 2004, 43, 44; *Park*, § 2 Rn. 240; *Wohlers/Jäger*, SK-StPO § 110 Rn. 12; weitergehend *OLG Jena* NJW 2001, 1290, 1293: Ist Anklage erhoben und die Durchsuchung vom Gericht vorgenommen worden, ist nur der Richter zur Durchsicht gemäß § 110 StPO befugt.

[406] In Zoll- und Steuerstrafverfahren gilt insofern ausnahmsweise § 404 S. 2 AO als Sonderregelung. Nach dem Wortlaut dieser Vorschrift steht die Durchsicht der Papiere in solchem Strafverfahren den Finanzämtern, also den Steuerfahndungsstellen oder den Zollfahndungsämtern, zu, nicht den einzelnen Fahndungsbeamten (§ 404 S. 2 Hs. 1 AO: „Die in Satz 1 bezeichneten Stellen"). Diese Befugnis wird zur Durchsicht von den Stellen deren einzelnen Fahndungsbeamten übertragen (*Park*, § 2 Rn. 241). Diese Beamten sind Ermittlungspersonen der StA, haben jedoch ohne ihre Anordnung die eigenverantwortliche Durchsichtsbefugnis i. S. d. § 110 Abs. 1 StPO (§ 404 S. 2 Hs. 1 und 2 AO).

StA beauftragt, sie führen aber – anders als Unterstützungskräfte – wie der Staatsanwalt eigenverantwortlich die Durchsicht durch.[407]

Im Hinblick auf den Zweck des § 110 StPO des Persönlichkeitsschutzes durch die Beschränkung der Befugnis zur Durchsicht haben die StA und ihre Ermittlungspersonen die Durchsicht der Papiere persönlich zu vorzunehmen und die Übertragung der Befugnis auf andere Personen ist unzulässig.[408] Jedoch kann sich der zur Durchsicht befugte Beamte, insb. der Staatsanwalt, der Hilfe anderer Personen (Sachverständiger) bedienen, die in den jeweiligen Gebieten ausgebildet sind und eine überlegene Sachkompetenz haben, falls sich dies zum Verständnis des Inhalts der Papiere als erforderlich erweist: z. B. eine Durchsicht verschiedener Arten von EDV-Anlagen und Dateien durch Informatiker, eine Durchsicht fremdsprachiger Papieren durch Dolmetscher oder eine Durchsicht der Buchführung und Bilanzen durch Wirtschaftsexperten (insb. die bei den Schwerpunktstaatsanwaltschaften tätigen Wirtschaftsreferenten[409]).[410] Dies kann ggf. für die Ermittlung notwendig und entscheidend sein. Heutzutage ist eine „IT-Durchsuchung" insb. im Bereich des Wirtschaftsstrafrechts nicht mehr wegzudenken und kann ohne EDV-Experten kaum auskommen.[411] Inzwischen ist ihr Einsatz bei der Durchsuchung Standard.[412] Sie verfügen durch fachliche Ausbildung über eine überlegene Sachkompetenz in ihrem Bereich gegenüber der StA. Dabei verbleibt aber die Leitung der Durchsicht noch bei der StA, so können diese Unterstützungskräfte nicht eigenverantwortlich tätig werden.[413] Daher darf die Entscheidung über die Durchsicht oder die Auswahl der zu beschlagnahmenden Dateien nicht ihnen allein überlassen werden.[414] Die Hinzuziehung dieser Unterstützungskräfte bei der Durchsicht ist nur dann möglich, sofern dies sachlich geboten ist, und die Anordnung bzw. die Anweisung der StA an sie ist

[407] Vgl. *Graulich*, wistra 8/2009, 299, 301; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 14. Der Kreis der befugten Ermittlungspersonen wird durch Rechtsverordnung der jeweiligen Landesregierung festgelegt (*Wohlers/Jäger*, a. a. O.).

[408] *Park*, § 2 Rn. 242; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 13.

[409] Die Wirtschaftsreferenten, die für Wirtschaftsstrafsachen als „Angehörige der StA" insb. in die Schwerpunktstaatsanwaltschaften gemäß § 143 Abs. 4 GVG eingegliedert sind, zählen i. d. R. nicht zu „Ermittlungspersonen der StA" i. S. d. § 110 Abs. 1 StPO, sondern zu „anderen Beamten" i. S. d. Abs. 2 (*Park*, § 2 Rn. 245). Dies kann je nach Land verschieden sein (*Wohlers/Jäger*, SK-StPO, § 110 Rn. 14).

[410] *Bruns*, KK-StPO, § 110 Rn. 4; *Ciolek-Krepold*, Rn. 148; M-G/*Schmitt*, StPO, § 110 Rn. 2 f.; *Park*, § 2 Rn. 243 ff.; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 13: Diese Personen müssen grundsätzlich unparteiisch und neutral sein.

[411] *Hiéramente*, wistra 11/2016, 432.

[412] *Hiéramente*, wistra 11/2016, 432, 439 f. [Tz. IV.]; *Szesny*, WiJ 2012, 228, 229 am Anfang.

[413] *Park*, § 2 Rn. 243; auch *Bruns*, KK-StPO, § 110 Rn. 4; *Mildeberger/Riveiro*, StraFo 2004, 43, 45.

[414] M-G/*Schmitt*, StPO, § 110 Rn. 3.

aktenkundig zu machen, um die Umgehung der gesetzlichen Beschränkung zu verhindern.[415]

bb) Andere zur Durchsicht nicht befugte Beamte: Abs. 2

Andere zur Durchsicht nicht befugte Beamte dürfen die Papiere durchsehen, wenn der Inhaber die Durchsicht genehmigt (S. 1). Bei der Durchsicht elektronischer Daten ist der Gewahrsamsinhaber von Daten derjenige, der physischen Zugriff auf das entsprechende Speichermedium hat.[416] Diese Genehmigung/Einwilligung kann beschränkt, also nur für bestimmte Papiere oder bestimmte Beamte erteilt und widerrufen werden[417] und darüber ist aber u. a. der Inhaber vor der Abgabe zu belehren.[418] Auch wenn er abwesend ist, ist sein Vertreter etc., der nach § 106 Abs. 1 S. 2 StPO der Durchsuchung beiwohnen darf, nicht zu der Genehmigung befugt;[419] es sei denn, dass eine Vertretungsmacht gesondert erteilt ist; z. B. Vertreter bei einer juristischen Person.[420]

Ohne ein entsprechendes Einverständnis haben diese anderen Beamten die für die Durchsicht für geboten erachteten Papiere in einem amtlich versiegelten Umschlag in Anwesenheit ihres Inhabers an die StA abzuliefern (S. 2). Dafür sind zuerst solche Papiere auszuwählen und auszusondern. Welche konkreten Handlungen können dazu gehören? Dabei handelt es sich um die Abgrenzung zwischen zulässigen und unzulässigen Sichtungen, aber jedenfalls sollte hier die Sichtung zur Auswahl und Aussonderung auch für die einfachen Beamten zumindest i. R. d. Zumutbaren möglich sein. Dies kann die Verletzung von Grundrechten minimieren. Nach h. M. ist eine (inhaltliche) „Grobsichtung", die ein oberflächliches Lesen des Inhalts der Papiere darstellt, unzulässig, weil sie ohnehin Kenntnisnahme des Inhalts ermöglicht.[421] Hingegen ist die Sichtung der Papiere nach äußeren Merkmalen erlaubt: z. B. Beschriftungen der Aktenschränke oder -ordner, Briefköpfe, Betreffangaben im Schreiben, Absender- und Empfängerangaben oder Namen der Dateien.[422] So ist bezüglich der Durchsuchung der EDV-Daten für die zur Durchsicht nicht befugten

[415] *Park*, § 2 Rn. 243 f.

[416] Vgl. *Peters*, NZWiSt 2017, 465, 467.

[417] *Bruns*, KK-StPO, § 110 Rn. 5; M-G/*Schmitt*, StPO, § 110 Rn. 4; *Park*, § 2 Rn. 240.

[418] *Park*, § 2 Rn. 240.

[419] M-G/*Schmitt*, StPO, § 110 Rn. 4.

[420] Vgl. *Bruns*, KK-StPO, § 110 Rn. 5.

[421] *Dauster*, StraFo 6/1999, 186, 187 [Fn. 12]; M-G/*Schmitt*, StPO, § 110 Rn. 4; *Park*, § 2 Rn. 240; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 17; abw. *Bruns*, KK-StPO, § 110 Rn. 7: insb. bei elektronischen Daten einschließlich der E-Mail.

[422] *Dauster*, StraFo 6/1999, 186, 187; M-G/*Schmitt*, StPO, § 110 Rn. 4; *Mildeberger/Riveiro*, StraFo 2004, 43, 44: eine Grobsichtung nach äußeren Kriterien; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 17. Diese Sichtung verfährt nach einem ersten Augenschein und dem optischen Eindruck (*Dauster*, a. a. O.).

Beamten die Auswahl nach einer Dateiübersicht (*directory listing*)[423] und bei E-Mails die Auswahl und Auflistung der Verzeichnisse nach Datum, Betreff, Absender oder Empfänger zulässig.[424]

Der Begriff des „Umschlags" des S. 2 ist – ebenfalls wie „Papiere" (vgl. oben a) aa)) – nach dem Normzweck weit auszulegen. So können alle Behältnisse, in denen die Papiere verwahrt und verschlossen oder versiegelt werden können, als Umschlag betrachtet werden; z. B. Briefumschlag, Paket, Datenträger im EDV-Bereich.[425] Werden die Papiere in Gegenwart des Inhabers oder, bei seiner Abwesenheit, seines Vertreters etc. nach § 106 Abs. 1 S. 2 StPO[426] mit dem Amtssiegel in einem Umschlag und mindestens so verpackt, dass sie der Kenntnisnahme durch Dritte entzogen sind, dann erfolgt die Versiegelung auf geeignete Weise.[427] Ist eine derartige Versiegelung aber nicht möglich, sind vergleichbare Vorkehrungen zu treffen.[428] Im Zuge dieser Versiegelung ist nach dem nunmehr (durch das 1. JuMoG vom 2004[429]) aufgehobenen § 110 Abs. 3 Hs. 1 StPO a. F. dem Inhaber der Papiere oder dessen Vertreter etc. das Beidrücken seines Siegels gestattet.[430]

cc) Umgehung der Beschränkung der Durchsichtsbefugnis in der Praxis

Die Beschränkung des Durchsichtsrechts nach § 110 Abs. 1 und 2 StPO dient dem Persönlichkeitsschutz und dem Datenschutz, indem die Kenntnisnahme des Intimbereichs des Einzelnen oder von wirtschaftlichen Vertraulichkeiten des Unternehmens nur den wenigsten Personen vorbehalten bleibt. Doch reichen die aktuellen Bedingungen nicht aus, um die Beschränkung in der Praxis reibungslos umzusetzen:

---

[423] Vgl. *Wohlers/Jäger*, SK-StPO, § 110 Rn. 17; auch *Park*, § 4 Rn. 813.

[424] Vgl. *Bruns*, KK-StPO, § 110 Rn. 7; *Park*, § 4 Rn. 813.

[425] Vgl. *Park*, § 2 Rn. 250 f.; auch M-G/*Schmitt*, StPO, § 110 Rn. 5.

[426] *Bruns*, KK-StPO, § 110 Rn. 6; M-G/*Schmitt*, § 110 Rn. 5; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 19.

[427] Vgl. *Wohlers/Jäger*, SK-StPO, § 110 Rn. 18: Die Datenträger sind in geeignete Behältnisse einzulegen.

[428] *Bruns*, KK-StPO, § 110 Rn. 5; *Park*, § 2 Rn. 251. Andererseits dürfte bei der Mitnahme der EDV-Anlagen die Sicherung mittels eines Passwortes beim Verbleib der Anlagen beim Inhaber wegen der Manipulationsmöglichkeiten nicht ausreichend sein, vielmehr ist hier die Erstellung einer vollständigen Kopie der Datenträger (z. B. Eins-zu-eins-Kopie) erforderlich (*Wohlers/Jäger*, SK-StPO, § 110 Rn. 18).

[429] Vgl. BT-Drs. 15/3482, S. 21: Da dieser Beidrückung in der Praxis keine Bedeutung zukommt, ist die ausdrückliche Regelung dieser Möglichkeit entbehrlich.

[430] Zust. M-G/*Schmitt*, StPO, § 110 Rn. 5; dazu *Park*, § 2 Rn. 252: Diese Regelung soll noch gelten, um einem etwaigen Wunsch des Inhabers zu entsprechen, Manipulationsrisiken zu vermeiden; abw. *Wohlers/Jäger*, SK-StPO, § 110 Rn. 19: Aber es ist zweifelhaft. Andererseits gilt Abs. 2 S. 2 nicht für die Mitnahme durch die zur Durchsicht Befugten, indessen ist eine Versiegelung wegen der Gefahr der Manipulation empfehlenswert (*Park*, a. a. O.; *Wohlers/Jäger*, a. a. O. Rn. 16).

insb. der Mangel an Staatsanwälten[431] und die Durchführung der Durchsuchung tatsächlich unter eigener Verantwortung der Polizei.[432] In den meisten Strafsachen wird diese Durchsicht in der Tat ohne konkrete Hinweise des Staatsanwaltes, d. h. mit Fehlen oder Unklarheit der Anordnung i. S. d. § 110 Abs. 1 StPO, – ggf. auch von unbefugten Beamten – durchgeführt.[433] Hierbei wird der Inhaber der Papiere u. a. einem faktischen Zwang ausgesetzt, die exzessive Mitnahme der Papiere in Kauf nehmen oder unbefugten Beamten die Durchsicht genehmigen zu müssen.[434] Zumeist ist es für die Beamten unmöglich oder sehr schwierig festzustellen, ob die aufgefundenen Papiere nur mit einer Grobsichtung bzw. einer Sichtung des Äußeren weiter durchgesehen werden müssen. Daher wollen die zur Durchsicht befugten Beamten in der Praxis gesamte oder größere Teile der Papiere sicherstellen, um den Vorwurf zu vermeiden, wesentliche Beweismittel übersehen oder unberücksichtigt gelassen zu haben.[435] Außerdem hat der Betroffene den Unbefugten die Durchsicht in dem von ihnen bestimmten Umfang (vielfach durchaus über eine Grobsichtung hinaus) zu gestatten, um die Mitnahme des gesamten Datenbestandes zu verhindern.[436] Nach alledem entfernt sich die Rechtswirklichkeit von dem Vorstellungsbild des § 110 StPO, das den Datenschutz durch Einschränkung der Durchsichtsbefugnis darstellt, und auch der Justizförmigkeit des Strafprozesses. Derzeit kommt dem § 110 StPO ein funktional größeres Gewicht seitens der Beschränkung der übermäßigen Sicherstellung und Beschlagnahme personenbezogener Daten nach dem Grundsatz der Verhältnismäßigkeit[437] zu, als seitens des Schutzes der Persönlichkeitssphäre durch die Beschränkung der Durchsichtskompetenz.[438]

[431] Mit Stand vom 11. Dezember 2017 sind in Deutschland 115 Bundesanwälte und 5.387 Landesanwälte tätig (<https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Personal/Personal_node.html)>; Abruf: 31. 12. 2020). Vor der Novellierung durch das 1. JuMoG hat das *OLG Jena* wie folgt aufgeführt (NJW 2001, 1290, 1292): „*Vielfach sind, wie vorliegend, Hilfskräfte zur Durchsuchung herangezogen worden, denen die Durchsicht i. S. d. § 110 StPO gerade nicht gestattet ist.*"

[432] *Dauster*, StraFo 6/1999, 186, 187. Dies deutet sich auch in § 3 (persönliche Ermittlungen des Staatsanwalts) Abs. 1 S. 1 RiStBV an: Der Staatsanwalt soll in bedeutsamen oder in rechtlich oder tatsächlich schwierigen Fällen den Sachverhalt vom ersten Zugriff an selbst aufklären, namentlich den Tatort selbst besichtigen, die Beschuldigten und die wichtigsten Zeugen selbst vernehmen.

[433] Vgl. *Park*, § 2 Rn. 247 und 262.

[434] Vgl. *Dauster*, StraFo 6/1999, 186, 187; M-G/*Schmitt*, StPO, § 110 Rn. 4; *Park*, § 4 Rn. 813.

[435] Vgl. *Dauster*, StraFo 6/1999, 186, 187.

[436] *Park*, § 4 Rn. 813 und dazu § 2 Rn. 262: „*Nach Sätzen wie: ‚Wenn Sie die Genehmigung nicht erteilen, nehmen wir hier alles mit, und es kann sehr lange dauern, bis Sie irgendetwas davon zurückbekommen' verweigern die wenigsten Betroffenen die Durchsicht auch durch dazu eigentlich nicht befugte Personen*"; vgl. *Dauster*, StraFo 6/1999, 186, 187 f.: Die Verweigerung der Genehmigung durch Inhaber kann etwa zur Unterbrechung seines wirtschaftlichen Fortkommens oder zu einer Entblößung von Daten der Intimsphäre oder Geschäftsgeheimnissen führen.

[437] Vgl. *Wohlers/Jäger*, SK-StPO, § 110 Rn. 6.

[438] Vgl. *Park*, § 2 Rn. 262: Sie bleibt nicht mehr übrig.

3. Vorläufige Sicherstellung

a) Begriff und Funktion

Ist die Trennung der potenziell beweiserheblichen Informationen von den übrigen direkt am Durchsuchungsort durch die Durchsicht möglich, und werden die getrennten Papiere weiter beschlagnahmt, so ist die Durchsuchung damit beendet.[439] Heute gibt es jedoch nicht viele solche Fälle. Vielmehr sind die gefundenen Papiere normalerweise so zahlreich und komplex, dass die Erforderlichkeit der Beschlagnahme nicht direkt vor Ort beurteilt werden kann, weshalb die Beamte zur Durchsicht das Ganze oder große Teile davon – meist in ihre Diensträume – (vorläufig) mitnehmen. Bei der Durchsuchung von EDV-Anlagen – insb. in Wirtschafts- und Steuerstrafsachen – ist dies von erheblicher Bedeutung.[440] Diese „Mitnahme/Verbringung zum Zweck der Durchsicht des § 110 StPO" heißt vorläufige Sicherstellung[441] und dazu gehören bei der Durchsuchung der EDV-Daten sowohl die Mitnahme von informationstechnischen Systemen oder Datenträgern als auch das Kopieren (nämlich Speicherung) von Dateien oder Datensätzen auf Datenträger der Ermittlungsbehörde.[442] Die vorläufige Sicherstellung stellt noch keine Beschlagnahme, sondern eine „Fortsetzung der Durchsuchung an Amtsstelle" dar.[443]

In der StPO wird der Begriff der vorläufigen Sicherstellung nicht erwähnt, zudem fehlt eine solche ausdrückliche Regelung dafür, wie die Maßnahme zu qualifizieren ist.[444] Nach h. M. ist das Verfahren der Durchsicht auf der Grundlage der vorläufigen Sicherstellung nicht nur „auf Grund des § 110 StPO"[445] anerkannt,[446] sondern auch

---

[439] *OLG Bremen* wistra 1999, 74, 76 [Tz. a)]; *Park*, § 2 Rn. 248 und 261.

[440] Vgl. *Hiéramente*, wistra 11/2016, 432, 437; *Kemper*, wistra 8/2010, 295, 297 f.; *Peters*, NZWiSt 2017, 465, 466.

[441] Vgl. *Graulich*, wistra 8/2009, 299, 301: In den letzten Rspr. wird das Verbringen der bei einer Durchsuchung aufgefundenen Papiere zum Zwecke der Durchsicht an Amtsstelle in aller Regel als vorläufige Sicherstellung qualifiziert. Daran wird ein öffentlich-rechtliches Verwahrungsverhältnis i. S. d. §§ 688 ff. BGB begründet (*Glock*, NStZ 2019, 248, 249).

[442] *BVerfG* NJW 2002, 1410, 1411; *BGH* NStZ 2003, 670; *BGH-Ermi-Ri* CR 1999, 292, 293; *Bruns*, KK-StPO, § 110 Rn. 4; M-G/*Schmitt*, StPO, § 110 Rn. 2a; *Park*, § 4 Rn. 812; *Szesny*, WiJ 2012, 228, 229 und 230 [Tz. 1.]: als „Minus" in Form einer Spiegelung von Daten; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 16; vgl. *Peters*, NZWiSt 2017, 465, 466: So wird dabei eine Gefahr begründet, dass sie mit der auf Freiwilligkeit des Betroffenen beruhenden Sicherstellung gemäß § 94 Abs. 1 StPO zu verwechseln ist. Deswegen empfiehlt *Peters* die Etablierung einer neuen Begrifflichkeit: „vorläufige Entziehung (zur Durchsicht)" (a. a. O. 472 [Tz. IV.]).

[443] *Hiéramente*, wistra 11/2016, 432, 438; *Kemper*, wistra 8/2010, 295, 297; M-G/*Schmitt*, StPO, § 110 Rn. 10; *Park*, § 2 Rn. 249; a. A. *Kemper*, wistra 5/2006, 171, 174: Die StPO lässt diese Mitnahme nur im Rahmen einer Beschlagnahme nach § 94 Abs. 2 StPO zu; a. A. *Peters*, NZWiSt 2017, 465, 466: selbstständige Ermittlungsmaßnahme.

[444] *Hiéramente*, wistra 11/2016, 432, 437; *Peters*, NZWiSt 2017, 465, 465 f.; *Szesny*, WiJ 2012, 228, 230 [Tz. 1.]; dazu *Graulich*, wistra 8/2009, 299, 301: Sie wird auch von der Rspr. nicht ausdrücklich benannt.

[445] *BVerfGE* 113, 29, 56; 124, 43, 68; NJW 2014, 3085, 3088 [Rn. 45]; *BGH* NJW 1995, 3397; 2010, 1297, 1298 [Rn. 19]; *OLG Jena* NJW 2001, 1290, 1293 f.; *LG Frankfurt* wistra 3/

zur Wahrung des „Grundsatzes der Verhältnismäßigkeit“ bei Eingriffen in die Grundrechte geboten.[447] Dieses Vorgehen nimmt Rücksicht sowohl auf die Interessen der Betroffenen als auch auf den Ermittlungszweck.[448] Zuerst ist die Beeinträchtigung der Integrität der Räume dadurch gering zu halten, dass ein längerer Aufenthalt der Ermittlungsbeamten am Ort vermieden wird.[449] Insbesondere im Fall der EDV-Daten ist durch die vorläufige Sicherstellung durch das Kopieren ein intensiverer Eingriff wie etwa die Nichtnutzbarkeit der EDV-Anlagen oder die langdauernde umfangreiche Inverwahrnahme der Daten zu vermeiden.[450] Dabei ist es auch erforderlich, dass womöglich durch eine erste Filterung – durch eine zur Durchsicht befugte Person – vor Ort die Masse der mitzunehmenden Papiere frühzeitig reduziert wird.[451] Die technische Möglichkeit zur Mitnahme des gesamten Datenträgers befreit

---

1997, 117; *LG Köln* StV 2002, 413 usw.; *Bruns*, KK-StPO, § 110 Rn. 9; *Glock*, NStZ 2019, 248, 248 f.; *Hiéramente*, wistra 11/2016, 432, 439; M-G/*Schmitt*, StPO, § 110 Rn. 10; *Peters*, NZWiSt 2017, 465, 466; *Szesny*, WiJ 2012, 228, 229 f.; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 16 [Fn. 79]; abw. *Park*, § 2 Rn. 249 [Fn. 669]: § 110 Abs. 2 S. 2 StPO; abw. *Graulich*, wistra 8/2009, 299, 301: aufgrund einer analogen Anwendung des § 94 Abs. 1 StPO (der formlosen Sicherstellung). Die letztere Ansicht wird aber beanstandet, weil ein solches Verständnis dem Stadium der Durchsicht entgegensteht, die der endgültigen Entscheidung über den Umfang der Beschlagnahme vorgelagert ist.

[446] Krit. *Kemper*, wistra 5/2006, 171, 174: Sie stellt eine in der StPO nicht vorgesehene Sicherstellung von Beweismitteln (sog. die „Hintertüre“) dar; *ders.*, wistra 8/2010, 295, 297: Weder in der StPO noch in einem anderen Gesetz gibt es eine klare Rechtsgrundlage für die Mitnahme zur Durchsicht und diese Maßnahme ist – nicht die Durchsuchung, sondern – ein „neues strafprozessuales Eingriffsrecht“ bzw. eine Art der „vorgelagerten Beschlagnahme“ (a. A. *Graulich*, wistra 8/2009, 299, 301 [Tz. 4.3]: eine vorsorgliche Beschlagnahme ist unzulässig). Die Ansicht von *Kemper* geht im Grunde darauf zurück, dass bei der Durchsuchung und Beschlagnahme der EDV-Daten die Konkretisierung und Bezeichnung der gesuchten Beweismittel nur beschränkt möglich ist und daher ein ausreichend konkreter Beschlagnahmebeschluss erst nach Beendigung der Durchsicht ergehen kann (vgl. wistra 5/2006, 171, 173). Er unterzieht zum Schluss die h. M. einer Kritik, dass sie eine Grauzone schafft, welche in dem Strafprozessrecht wenig wünschenswert ist (wistra 8/2010, 295, 298), und behauptet, dass §§ 94 ff. StPO heute mit Blick auf die Unmenge der durchzusehenden Papiere – insb. in Steuer- und Wirtschaftsstrafverfahren – insgesamt überarbeitet werden sollten (wistra 5/2006, 171, 175).

[447] *BVerfGE* 113, 29, 55 ff.; 124, 43, 67 ff.; NJW 2014, 3085, 3088 [Rn. 44 f.]; *BGH* NJW 1995, 3397, 3397 f.; 2010, 1297, 1298 [Rn. 19]; *BGH-Ermi-Ri* CR 1999, 292, 293; *LG Hildesheim* StraFo 3/2007 114, 115; *Hiéramente*, wistra 11/2016, 432, 439; M-G/*Schmitt*, StPO, § 110 Rn. 2a und 10; *Park*, § 2 Rn. 249; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 16.

[448] *BVerfGE* 124, 43, 76 [Rn. 108]; vgl. *Hiéramente*, wistra 11/2016, 432, 437 a. E.: Das erfolgt primär im Interesse des Betroffenen.

[449] *BVerfGE* 124, 43, 76 [Rn. 108]; *Hiéramente*, wistra 11/2016, 432, 437 [Tz. III.]; *Park*, § 2 Rn. 249.

[450] *Szesny*, WiJ 2012, 228, 230 [Tz. 1.]. Dabei muss dem Betroffenen i. d. R. das Recht eingeräumt werden, zumindest auf eigene Kosten Kopien selbst anzufertigen (*Park*, § 2 Rn. 260).

[451] *Hiéramente*, wistra 11/2016, 432, 437; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 16; auch *Brodowski/Eisenmenger*, ZD 3/2014, 119, 124 am Anfang: durch etwa sog. Live-Analyse bzw. selektive Sicherung.

nämlich dem Ermittler nicht von einer Vorsortierung vor Ort (*ultima ratio*).[452] Zum anderen haben auch die Durchsuchungsbeamten von dieser Vorgehensweise einen Vorteil. So dient sie nicht nur der Vereinfachung der Ermittlungstätigkeit,[453] sondern reduziert auch die Gefahr, dass der Antrag auf richterliche Beschlagnahme abgelehnt wird.[454]

b) Die Fälle, in denen einer vorläufigen Sicherstellung Rechnung zu tragen ist

Nach den Entscheidungen des *BVerfG* kann die Mitnahme der Papiere zur Durchsicht gemäß § 110 StPO nur dann erwogen werden, wenn eine sorgfältige Sichtung und eine unverzügliche Zuordnung nach der Verfahrensrelevanz am Durchsuchungsort nicht erlaubt werden.[455] Daher ist die vorläufige Sicherstellung zur Durchsicht entbehrlich, wenn die nicht beschlagnahmefreien und verfahrensrelevanten Papiere vor Ort sofort ausgewählt und ausgesondert und endgültig beschlagnahmt werden können.[456] Heute ist dies jedoch selten und bei IT-Durchsuchungen ist die vorläufige Sicherstellung tatsächlich fast immer erforderlich. Sie kann nicht nur aus einer großen Menge Papiere und einer Kompliziertheit ihrer Inhalte, sondern auch aus technischer Erfassbarkeit von Datenbestand, Betriebssystem oder Software folgen. Im letzten Fall wird es zuweilen wegen der Intransparenz der elektronischen Datenverarbeitung, wie undurchsichtiger/unübersichtlicher Strukturen der Datenablage, uneinheitlicher Dateinamen (vermeintlich harmlose Dateien von ihrer Bezeichnung her), uneindeutiger Zugriffsbefugnisse etc., oder zuweilen zur Sichtbarmachung und Wiederherstellung verschleierter, vermischter, verschlüsselter oder gelöschter Daten[457] (subsidiär) zu Recht gefordert, „gesamte" Datenbestände oder „sämtliche" darauf befindliche Daten zu sichern oder eine Eins-

[452] Vgl. *Szesny*, WiJ 2012, 228, 230 f. [Tz. 2.]: die Begrenzung des „vorläufig sicherzustellenden" Materials. Angesichts der Sichtbarmachung verschleierter, verschlüsselter oder gelöschter Daten oder der Intransparenz der Datenträger kann aber solche Vorsortierung nicht stets zu streng sein (vgl. unten b)).

[453] *Hiéramente*, wistra 11/2016, 432, 437 und 439.

[454] Vgl. *BGH* NJW 1995, 3397, 3397 f.: Wird die Beschlagnahme der Papiere ohne ausreichende inhaltliche Durchsicht beantragt, so kann dieser Antrag wegen Fehlens potentieller Beweisbedeutung oder wegen unverhältnismäßigen Eingriffs abgelehnt werden.

[455] Vgl. *BVerfGE* 113, 29, 56 [Rn. 117]; 124, 43, 68 [Rn. 87]; NJW 2014, 3085, 3088 [Rn. 44]; *Peters*, NZWiSt 2017, 465, 467; *Szesny*, WiJ 2012, 228, 231; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 16.

[456] *Graulich*, wistra 8/2009, 299; *Park*, § 2 Rn. 229; *Szesny*, WiJ 2012, 228, 230 [Tz. 2.]; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 1.

[457] Insoweit ist allein die „Beschlagnahme" erwähnt, *BVerfGE* 113, 29, 56 f. [Rn. 119]; auch M-G/*Schmitt*, StPO, § 94 Rn. 18a: Auch die Beschlagnahme kann vorgenommen werden. Zwar ist diese Vorgehensweise natürlich in begründeten Einzelfällen als Methode der Beschlagnahme möglich (*Kemper*, wistra 3/2008, 96, 99), doch sie muss möglichst zuvor als Methode der vorläufigen Sicherstellung zur Durchsicht nach § 110 StPO erfolgen (vgl. *Brodowski/Eisenmenger*, ZD 3/2014, 119, 124).

zu-eins-Kopie eines solchen Datenträgers anzufertigen;[458] insb. bei Wirtschafts- und Steuerdelikten oder schweren Straftaten. Zudem ist diese Maßnahme zu begründen wegen des Versagens der Entschlüsselung und der Unmöglichkeit der Ablichtung[459] oder zur Umgehung der Hektik des Ortes einer Durchsuchung, um die Entscheidung über die Beschlagnahme oder Rückgabe der Daten in aller Ruhe zu treffen.[460] Allerdings kann eine solche Sicherstellung scheinbar dem Sinn und Zweck des § 110 StPO entgegenstehen, aber sie ist in der Praxis häufig unvermeidlich und sogar eventuell zweckmäßig.[461] Damit taucht aber das Problem auf, dass die Begrenzung des richterlichen Durchsuchungsbeschlusses praktisch bedeutungslos wird,[462] und es bedarf verfahrensrechtlicher Vorkehrungen, um einen massiven Grundrechtseingriff aus dieser umfangreichen Datenerfassung auszugleichen.

c) Begrenzung der Fortdauer der Durchsicht

Die vorläufig sichergestellten und in die Behördenräume mitgenommenen Papiere müssen von den befugten Personen zügig durchgesehen werden,[463] damit in angemessener Zeit zu einem Ergebnis des Beschlagnahmeantrags oder der Herausgabe bzw. Löschung gelangt wird.[464] Dabei wird unter dem Gesichtspunkt der Verhältnismäßigkeit i. R. d. vorläufigen Sicherstellung die „Zulässigkeit der Fortsetzung der Durchsicht", nämlich die „zeitliche Grenze der Durchsicht", oft infrage gestellt. Hierfür liegt noch keine höchstgerichtliche Rechtsprechung vor.[465] Dauert

[458] *Hiéramente*, wistra 11/2016, 432, 439 [Tz. IV.]: eine Komplettspiegelung; *Peters*, NZWiSt 2017, 465, 466; *Szesny*, WiJ 2012, 228, 229: auch *Kemper*, wistra 3/2008, 96, 99. In den meisten Fällen in der Praxis wird diese Herangehensweise verfolgt (*Brodowski*/*Eisenmenger*, ZD 3/2014, 119, 123 a. E.).

[459] Vgl. *Bäumerlich*, NJW 2017, 2718, 2719 [Tz. III.].

[460] *Bär*, CR 1999, 292, 294; vgl. *Brodowski*/*Eisenmenger*, ZD 3/2014, 119, 123 f.: Sie hat den Vorteil, dass die Auswertung der Daten in aller Ruhe und unter Laborbedingungen erfolgen kann.

[461] A. A. *Szesny*, WiJ 2012, 228, 229 und 231: Dies ist mit Blick auf Wortlaut, Sinn und Zweck des § 110 StPO sowie das Computer-Grundrecht erheblich bedenklich und daher in einer Vielzahl der Fälle nicht zulässig. Er macht außerdem geltend, dass bereits vor einer vorläufigen Sicherstellung vor Ort durch die Durchsicht eine Abwägung der Erforderlichkeit der Mitnahme stattzufinden hat (a. a. O. 231). Dies ist jedoch in vielen Fällen – insb. in wirtschaftlichen und steuerlichen Strafsachen – für die Ermittlungsbehörden eine übermäßige Forderung.

[462] *Peters*, NZWiSt 2017, 465, 467 [Tz. b)].

[463] *BGH* NStZ 2003, 670, 671 [Tz. c)]; *Graulich*, wistra 8/2009, 299, 301; *Hiéramente*, wistra 11/2016, 432, 437; *Wohlers*/*Jäger*, SK-StPO, § 110 Rn. 24.

[464] *LG Mühlhausen* StV 2003, 433, 434 [Rn. 35] = StraFo 2003, 237, 238; *LG Hildesheim* StraFo 3/2007, 114, 115; *Kemper*, wistra 8/2010, 295, 298; *Szesny*, WiJ 2012, 228, 232. Hier herrscht bis zur Beschlagnahme oder Freigabe ein ungeklärter Rechtszustand (*Kemper*, a. a. O.).

[465] In Deutschland sind die fachgerichtlichen Entscheidungen über die Angemessenheit der Zeitspanne der Durchsicht aufgrund der vorläufigen Sicherstellung derzeit nicht nur uneinheitlich, sondern sie scheint auch überhaupt großzügig behandelt zu werden; vgl. für die Fälle, dass die Fortdauer als hinnehmbar angesehen wird, *LG Frankfurt* wistra 1997, 117: 1 1/4 Jahre; *LG Hildesheim* StraFo 3/2007, 114: 3 1/2 Monate; hingegen für die Fälle, dass sie als zu lang

die Durchsicht unzumutbar lange an, so darf dies zuerst nach dem Übermaßverbot nicht gestattet werden[466] und es auch verstößt gegen das Beschleunigungsgebot (Art. 6 Abs. 1 EMRK).[467] Hierbei versteht es sich von selbst, dass die Zeitdauer dessen, was angemessen ist, wesentlich von der Menge des zu überprüfenden Materials und der Schwierigkeit seines Inhalts abhängt.[468] Die Durchsicht i. S. d. § 110 StPO, die keine (nähere) Auswertung der beschlagnahmten Papiere darstellt (vgl. unten 5), beschränkt sich aber nach verfassungsrechtlicher Zweckbindung auf die Überprüfung, ob sie als Beweismittel in Betracht kommen, und nur die dafür erforderliche Frist ist zulässig.[469] Dafür sind i. d. R. einige Tage oder Wochen ausreichend und diese Zeitdauer sollte ausnahmsweise auch in wirtschaftlichen und steuerlichen Strafsachen, bei denen etwa eine große Anzahl von Unternehmen oder Großunternehmen beteiligt sind und eine große Menge von Dokumenten überprüft werden muss, maximal 8 Wochen (2 Monate) betragen.[470] Eine darüber hinausgehende Dauer ist i. d. R. eine übermäßige Beeinträchtigung für den Betroffenen. In einigen Rspr. wurde schon darauf hingewiesen, dass eine Verzögerung der (Durch-)

angesehen wird, *LG Köln* StV 2002, 413: 7 Monate; *LG Dresden* NStZ 2003, 567: 3 Monate; *LG Mühlhausen* StV 2003, 433, 434: 2 3/4 Jahre; *LG Limburg* StraFo 2006, 198: 8 Monate. Zum anderen hat das *BVerfG (3. K)* in seiner Entscheidung von 2002 zu Recht ausgeführt, dass der Grundsatz zur zeitlichen Geltung von Durchsuchungsbeschlüssen im Beschluss vom 27. Mai 1997 (vgl. *BVerfGE* 96, 44, 54: maximal 6 Monate) auf die Phase der Durchsicht von Unterlagen nach § 110 StPO nicht anzuwenden ist (*BVerfG* NJW 2002, 1410, 1411 [Tz. a)]). Der Beschluss von 1997 richtet sich auf die Gültigkeitsdauer richterlicher Durchsuchungsanordnung und dabei handelt es sich um den Beginn der Durchsuchung, nicht um deren Fortführung oder Beendigung (vgl. *Szesny*, WiJ 2012, 228, 232). Das heißt, er bezieht sich auf die Frage, ob bei richterlicher Durchsuchungsanordnung, die ohnehin schon relativ alt war und noch nicht vollzogen wurde, der präventive Grundrechtsschutz noch gültig ist. Die *3. Kammer* hat dagegen beurteilt, ob die vorläufige Sicherstellung und die Fortdauer der Durchsicht nach § 110 StPO im Einzelfall im Lichte des Verhältnismäßigkeitsgrundsatzes rechtmäßig und erforderlich sind. Hier besteht nur eine Beschränkung des Eigentumsgrundrechts aufgrund der Fortdauer des Sachenzugs, aber keine Gefahr, dass der Richtervorbehalt mit der Zeit leerläuft (*BVerfG* NJW 2002, 1410, 1411 [Tz. a)]; *Park*, § 2 Rn. 133). Dauert die Durchsicht der Papiere nach § 110 StPO länger als sechs Monate, so wird dies allerdings i. d. R. rechtswidrig sein, weil dies unverhältnismäßig ist, nicht weil die richterliche Durchsuchungsanordnung als Eingriffsermächtigung entfällt (vgl. *Mildeberger*/*Riveiro*, StraFo 2004, 43, 46).

[466] *Park*, § 2 Rn. 260.

[467] *Szesny*, WiJ 2012, 228, 232.

[468] *LG Frankfurt* wistra 1997, 117, 118; *LG Mühlhausen* StV 2003, 433, 434 [Rn. 36]; *Graulich*, wistra 8/2009, 299, 301 f.; *Peters*, NZWiSt 2017, 465, 469; *Szesny*, WiJ 2012, 228, 232; *Wohlers*/*Jäger*, SK-StPO, § 110 Rn. 24.

[469] Diese Durchsicht stellt eine grobe Auswertung dar und dabei bedarf es keiner tiefergehenden Auswertung der Unterlagen (*Glock*, NStZ 2019, 248, 249; *Cordes*/*Pannenborg*, NJW 2019, 2973, 2977).

[470] Abw. *Ciolek-Krepold*, Rn. 152: eine Zeitspanne von maximal vier Wochen; anders *Park*, § 2 Rn. 260: ein kurzer Zeitraum von wenigen Tagen oder – in Ausnahmefällen – wenigen Wochen.

Sichtung auf die unzureichende Personalausstattung der Ermittlungsbehörden[471] und einen hohen Geschäftsandrang sowie eine damit einhergehende Arbeitsüberlastung[472] zurückzuführen ist. Allerdings ist dies nicht der einzige Grund für Verzögerungen und dazu kommt ein erheblicher Umfang des zu überprüfenden Materials. Doch kann ein solch lang andauernder Engpass staatlicher Organe, der zulasten des Einzelnen gehen kann, hinsichtlich des Grundsatzes des Rechtsstaates und der Verhältnismäßigkeit nicht bestehen bleiben.[473] Zum effektiven Grundrechtsschutz ist eine Verstärkung der Arbeitskräfte auf struktureller und organisatorischer Ebene erforderlich. Insoweit kann andererseits die Anwesenheit des Betroffenen, seiner Mitarbeiter oder seiner Verteidiger bei der Durchsicht zu einer schnellen Auswahl und Aussonderung verfahrens(ir)relevanter Daten dienen (vgl. unten IV.). Derzeit fehlt es aber jedenfalls an rechtlichen Anreizen für diese beschleunigte Bearbeitung.[474]

d) Antrag auf gerichtliche Bestätigung bzw. Entscheidung

Die vorläufige Sicherstellung der Papiere und ihre Durchsicht nach § 110 StPO fallen unter die Durchsuchung als Vorstufe der Beschlagnahme. Daher ist die Durchsuchung während der Fortsetzung der Durchsicht noch nicht beendet. Die Mitnahme und die amtliche Verwahrung der Papiere zur Durchsicht begründet aber eine der Beschlagnahme vergleichbare Beschwerde, keine solche aufgrund der Durchsuchung.[475] Aus diesem Grund muss die StA entsprechend dem § 98 Abs. 2 S. 1 StPO die gerichtliche Bestätigung der „vorläufigen Sicherstellung zur Durchsicht" beantragen, nicht aber eine solche der Beschlagnahme, wenn die Durchsicht der bei der Durchsuchung sichergestellten Materialien wegen ihres Umfangs noch nicht beendet ist und sie – insb. länger als im richterlichen Beschluss festgelegten Zeitraum oder als 8 Wochen (vgl. oben c)) – fortgesetzt werden sollte.[476] Außerdem kann der von Durchsuchung Betroffene zur Prüfung der Rechtfertigung dieser

[471] Vgl. *LG Mühlhausen* StV 2003, 433, 434 = StraFo 2003, 237, 238. Hier habe der Staatsanwalt mit der Begründung Einwand erhoben, dass wegen der unzureichenden Personalausstattung mehr als 12 Monate ohne Sichtung verstrichen seien, aber dies wurde nicht angenommen.

[472] Vgl. insb. *LG Limburg* StraFo 2006, 198; auch *LG Köln* StV 2002, 413.

[473] *LG Köln* StV 2002, 413; *LG Limburg* StraFo 2006, 198.

[474] *Brodowski/Eisenmenger*, ZD 3/2014, 119, 120; dazu *Peters*, NZWiSt 2017, 465, 472 [Tz. IV.]: Anforderung gesetzlicher Verankerung einer zeitlichen Höchstdauer.

[475] *BGH-Ermi-Ri* CR 1999, 292, 293; auch *BVerfG* NJW 2003, 2669, 2670; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 2: die Mitnahme gemäß § 110 StPO und die Beschlagnahme gemäß § 94 Abs. 2 StPO macht aus Sicht des Betroffenen keinen Unterschied.

[476] Vgl. *BGH* NStZ 2003, 670, 671 [Tz. 1.]. Nach dem Sachverhalt der Entscheidung hat der *BGA* gegen das Begehren der Freigabe der sichergestellten Materialien (persönlicher Unterlagen, elektronischer Datenträger, eines PC etc.) gemäß §§ 94 Abs. 1, 2, 98 Abs. 2, 169 Abs. 1 StPO „richterliche Bestätigung der Beschlagnahme" beantragt und der *BGH-Ermi-Ri* hat dementsprechend den Antrag bestätigt.

vorläufigen Sicherstellung und der Beachtung der Grenzen nach dem Grundsatz der Verhältnismäßigkeit entsprechend dem § 98 Abs. 2 S. 2 StPO einen Antrag auf richterliche Entscheidung stellen;[477] etwa wenn ein zur Durchsicht nicht befugter Beamter die Papiere ohne Genehmigung ihres Inhabers durchgesehen oder ohne Versiegelung mitgebracht hat, wenn ein befugter Beamter die Durchsicht unverhältnismäßig durchgeführt hat und wenn die Ermittlungsbehörden gegen das Verfahren nach § 110 StPO oder die darauf bezügliche Anordnung des Richters verstoßen haben.[478] Zu dieser nachträglichen Prüfung sind die Erwägungen für die vorläufige Sicherstellung (vgl. oben b)) nach Möglichkeit auf dem richterlichen Beschluss anzugeben und bei Gefahr im Verzug sind sie durch die Ermittlungsbehörden schriftlich abzufassen und zu den Akten zu bringen (Dokumentation und Begründung).[479] Bei der Prüfung der Rechtmäßigkeit der Mitnahme und Durchsicht der Papiere sowie ihrer Fortsetzung hat der Richter nach dem Prinzip der Verhältnismäßigkeit etwa den Vorgang der Sicherstellung bzw. der Herausgabe der Papiere, die zu ihrer Durchsicht bereits abgelaufene Dauer, den Grad des Grundrechtseingriffs und das Gewicht der Tatvorwürfe in Rechnung zu ziehen.[480]

4. Zufallsfunde: § 108 StPO

(1) Bei der Durchsicht eines gesamten Datenbestandes oder sämtlicher darauf gespeicherten Daten ist die Regelung der einstweiligen Beschlagnahme nach § 108 Abs. 1 S. 1 StPO von großer Bedeutung. Die Vorschrift sieht vor, dass solche Gegenstände, die zwar anlässlich der Durchsuchung zufällig gefunden wurden, aber nicht den Ausgangstatvorwurf betreffen und auf Verübung anderer Straftaten hin-

[477] *BVerfG* NJW 2002, 1410, 1411; NJW 2003, 2669, 2671; *BGH* StV 1988, 90; NStZ 2003, 670, 671; *BGH-Ermi-Ri* CR 1999, 292, 293 und 294 (mit Anmerkung von *Bär:* Rechtsschutzmöglichkeit nach Art. 19 Abs. 4 GG); *Bruns*, KK-StPO, § 110 Rn. 9; *Graulich*, wistra 8/2009, 299, 301 [Tz. 4.4]; M-G/*Schmitt*, StPO, § 110 Rn. 10; *Mildeberger/Riveiro*, StraFo 2004, 43, 45; *Park*, § 2 Rn. 258; *Szesny*, WiJ 2012, 228, 235. Daher steht der Antrag des Betroffenen auf Herausgabe im Regelfall dem Antrag der Ermittlungsbehörden auf richterliche Bestätigung der vorläufigen Sicherstellung gegenüber (*Graulich*, a. a. O.). Andererseits ist nunmehr durch die Entscheidung des *BVerfG* von 1997, dass Beschwerden gegen bereits abgeschlossene Durchsuchungen zum Rechtsschutz noch zulässig sind (*BVerfGE* 96, 27), die Störung der sog. „prozessualen Überholung" aufgehoben (*Park*, a. a. O.).

[478] Vgl. *Graulich*, wistra 8/2009, 299, 301 a. E.: die Überprüfung der unvertretbaren Entscheidung, in welchem Umfang die Durchsicht des vorläufig sichergestellten Materials notwendig, wie sie im Einzelnen zu gestalten und wann sie zu beenden ist.

[479] Vgl. *Szesny*, WiJ 2012, 228, 231 am Anfang.

[480] *BVerfG* NJW 2002, 1410, 1411 [Tz. b)]; vgl. *BGH* StV 1988, 90: „*Die weitere Durchsicht des sichergestellten Materials ist unverhältnismäßig, wenn der Betroffene das dringend zur Fortführung seines Betriebes benötigt und bei der weiteren Durchsicht erhebliche Nachteile entstehen, auf der anderen Seite aber nur ein vager Verdacht vorliegt, das gesuchte Beweismittel befinde sich unter den mitgenommenen Gegenständen.*"

deuten (sog. „Zufallsfunde"), einstweilen in Beschlag zu nehmen sind.[481] Infolge der Vorschrift brauchen die durchsuchenden Beamten einerseits bei Zufallsfunden nicht die Augen verschließen, andererseits wird die Eingrenzungsfunktion der richterlichen Durchsuchungsanordnung nicht unterlaufen.[482] Das heißt, durch die einstweilige Beschlagnahme von Zufallsfunden wird den Ermittlungsbehörden die Gelegenheit zur Prüfung des (Anfangs-)Verdachts bezüglich eines weiteren Ermittlungsverfahrens gegeben und die Eingrenzungsfunktion des bestehenden Durchsuchungsbeschlusses nicht ausgehöhlt.[483] Daher ist eine systematisch/planmäßig „gezielte Suche" nach Zufallsfunden, die in der Durchsuchungsanordnung nicht genannt sind, unzulässig,[484] was ggf. zu einem Beweisverwertungsverbot führen kann.

(2) Das Merkmal des „Hindeutens" in § 108 Abs. 1 S. 1 StPO wird erfüllt, wenn sich aus einem Fund selbst oder den Umständen seines Auffindens Anhaltspunkte für eine andere Straftat als Anlasstat ergeben,[485] und nach h. M. ist ausreichend dafür ein ungewisser Verdacht der Tat (kein Anfangsverdacht) und die naheliegende Möglichkeit, dass der Fund zu ihrem Beweis geeignet ist.[486] Zufallsfunde sind „bei Gelegenheit einer Durchsuchung" aufzufinden. Daher ist der § 108 StPO dann nicht mehr anwendbar, wenn die im Durchsuchungsbeschluss aufgeführten Gegenstände bereits gefunden sind oder wenn der Betroffene sie alle freiwillig herausgegeben hat; dabei wurde die Durchsuchung schon beendet und außerdem ist eine weitere Suche nach anderen Beweismitteln angesichts der Eingrenzungsfunktion des Durchsuchungsbeschlusses und des Verbots der gezielten Suche unzulässig.[487] Nach § 108 Abs. 1 S. 3 StPO gilt der S. 1 nicht bei Gebäudedurchsuchungen nach 103 Abs. 1 S. 2

---

[481] *Hauschild*, MüKo-StPO, § 108 Rn. 1; M-G/*Schmitt*, StPO, § 108 Rn. 1; *Park*, § 2 Rn. 216; *Roxin/Schünemann*, § 35 Rn. 11.

[482] *Park*, § 2 Rn. 217; vgl. *LG Kiel* StV 2017, 22, 23; *LG Berlin* NStZ 2004, 571, 573 [Rn. 17 und 20].

[483] *Hauschild*, MüKo-StPO, § 108 Rn. 1 f.

[484] *Cordes/Pannenborg*, NJW 2019, 2973, 2974; *Hauschild*, MüKo-StPO, § 108 Rn. 1, 7 und 12; M-G/*Schmitt*, StPO, § 108 Rn. 1; *Park*, § 2 Rn. 217; *Roxin/Schünemann*, § 35 Rn. 12; auch *LG Berlin* NStZ 2004, 571, 573 [Rn. 19]. Zum anderen, für Zufallsfunde, die von der Durchsuchungsanordnung nicht umfasst werden, aber im Zusammenhang mit dem Ausgangstatvorwurf stehen (sog. „tatbezogene Zufallsfunde"), gibt es nun keine gesetzliche Regelung (*LG Berlin* a. a. O. [Rn. 18]; *LG Kiel* StV 2017, 22, 23). Nach den Rspr. von *LG Berlin* und *Kiel* soll ihre Sicherstellung bzw. Beschlagnahme nur zulässig sein, wenn ihre Beweisbedeutung in Bezug auf den Ausgangstatvorwurf „offensichtlich" ist (*LG Kiel* a. a. O.; dazu *LG Berlin* a. a. O. [Rn. 20]: Beim Zufallsfund, der seine Beweisbedeutung gleichsam auf der Stirn trägt). Angesichts der Eingrenzungsfunktion ist die bloße Möglichkeit einer Beweisbedeutung insoweit unzureichend (*LG Kiel* a. a. O.).

[485] *Cordes/Pannenborg*, NJW 2019, 2973, 2973 f.; *Hauschild*, MüKo-StPO, § 108 Rn. 6; M-G/*Schmitt*, StPO, § 108 Rn. 2; *Park*, § 2 Rn. 216.

[486] *Bruns*, KK-StPO, § 108 Rn. 2; *Cordes/Pannenborg*, NJW 2019, 2973; *Hauschild*, MüKo-StPO, § 108 Rn. 6; M-G/*Schmitt*, StPO, § 108 Rn. 2; abw. *Park*, § 2 Rn. 216 a. E.: Reine Vermutungen oder ein ungewisser Verdacht genügen nicht.

[487] *Park*, § 2 Rn. 217 und 223.

StPO, weil diese nur der Ergreifung eines Beschuldigten dienen.[488] Daher dürfen anlässlich dieser Durchsuchung aufgefundene Zufallsfunde nicht einstweiligen beschlagnahmt werden. Doch sie können ggf. nach §§ 94, 98 StPO – insb. bei Gefahr im Verzug durch die StA oder Polizeibeamte – beschlagnahmt werden.[489]

Zuständig für die einstweilige Beschlagnahme ist jeder Richter, Staatsanwalt oder Polizeibeamte, die die Durchsuchung vornehmen.[490] So gilt hierfür keine Zuständigkeitsregelung des § 98 Abs. 1 S. 1 StPO[491] und unter § 108 Abs. 1 S. 1 ist eine Erweiterung des Beschlagnahmerechts zu verstehen, nicht jedoch eine Ausdehnung des Durchsuchungsrechts.[492] Bei der vorläufigen Sicherstellung und Durchsicht von Papieren nach § 110 StPO bleibt jedoch die Befugnis zur einstweiligen Beschlagnahme i. d. R. der StA oder auf deren Anordnung ihren Ermittlungspersonen, die die Durchsuchung vornehmen, vorbehalten. Im Fall der einstweiligen Beschlagnahme nach § 108 Abs. 1 S. 1 StPO wird Gefahr im Verzug gesetzlich vermutet.[493]

Die StA ist über die einstweilige Beschlagnahme von Zufallsfunden zu unterrichten (§ 108 Abs. 1 S. 2 StPO).[494] Sie hat anschließend in angemessener Frist[495] zu prüfen, ob ein neues Ermittlungsverfahren eingeleitet werden soll und bei Verfahrenseinleitung ob die einstweilig in Beschlag genommenen Gegenstände freizugeben, oder – nach §§ 94, 98 StPO – endgültig zu beschlagnahmen sind. Im ersteren Fall muss die einstweilige Beschlagnahme aufgehoben werden, im letzteren Fall trifft der für das neue Verfahren zuständige Richter die Entscheidung über die endgültige Beschlagnahme, weil Gefahr im Verzug nicht mehr besteht.[496] Gegen die vorläufige Beschlagnahme kann der Betroffene analog § 98 Abs. 2 S. 2 StPO je-

[488] *Cordes*/*Pannenborg*, NJW 2019, 2973, 2974; *Hauschild*, MüKo-StPO, § 108 Rn. 10; M-G/*Schmitt*, StPO, § 108 Rn. 5.

[489] *Cordes*/*Pannenborg*, NJW 2019, 2973, 2974; *Hauschild*, MüKo-StPO, § 108 Rn. 10; M-G/*Schmitt*, StPO, § 108 Rn. 5. Dabei ist allerdings ein neues Ermittlungsverfahren einzuleiten (*Cordes*/*Pannenborg*, a. a. O.; *Park*, § 2 Rn. 226).

[490] *Cordes*/*Pannenborg*, NJW 2019, 2973, 2975; *Hauschild*, MüKo-StPO, § 108 Rn. 5; M-G/*Schmitt*, StPO, § 108 Rn. 6.

[491] *Cordes*/*Pannenborg*, NJW 2019, 2973, 2975.

[492] *Cordes*/*Pannenborg*, NJW 2019, 2973, 2977; *Hauschild*, MüKo-StPO, § 108 Rn. 7; *Park*, § 2 Rn. 217; *Roxin*/*Schünemann*, § 35 Rn. 12.

[493] *BGHSt* 19, 374, 376; *Cordes*/*Pannenborg*, NJW 2019, 2973, 2975; M-G/*Schmitt*, StPO, § 108 Rn. 6; a. A. *Bruns*, KK-StPO, § 108 Rn. 3.

[494] Dabei sind die in Beschlag genommenen Gegenstände nach § 109 StPO zu verzeichnen und kenntlich zu machen (*Roxin*/*Schünemann*, § 35 Rn. 11).

[495] Angesichts der § 98 Abs. 2 S. 1 StPO scheint i. d. R. die Frist von drei Tagen sachgerecht zu sein, doch bei Ungewissheit des Anfangsverdachts sollte sie ab dem Zeitpunkt der Einleitung des neuen Ermittlungsverfahrens zu laufen beginnen (*Cordes*/*Pannenborg*, NJW 2019, 2973, 2975).

[496] *Bruns*, KK-StPO, § 108 Rn. 5; *Cordes*/*Pannenborg*, NJW 2019, 2973, 2975; *Hauschild*, MüKo-StPO, § 108 Rn. 15; M-G/*Schmitt*, StPO, § 108 Rn. 7.

derzeit gerichtliche Entscheidung beantragen und zuständig dafür ist das Gericht, das für das neue Ermittlungsverfahren zuständig ist.[497]

(3) § 108 Abs. 2 und 3 StPO regelt ein Verwertungsverbot von Zufallsfunden nach Abs. 1 S. 1. Zufallsfunde aus einem Strafverfahren gegen einen Arzt dürfen nach Abs. 2 nicht als Beweismittel in einem Strafverfahren gegen eine Patientin wegen einer Straftat nach § 218 StGB verwertet werden, was dem Schutz des Vertrauensverhältnisses zwischen Arzt und Patientin dient.[498] Auch Zufallsfunde, auf die sich das Zeugnisverweigerungsrecht von Medienmitarbeitern i. S. d. § 53 Abs. 1 S. 1 Nr. 5 StPO erstreckt, dürfen nach Abs. 3 i. d. R. zu Beweiszwecken nicht verwertet werden, doch ihre Verwertung ist ausnahmsweise zulässig, wenn sie eine Straftat betreffen, die im Höchstmaß mit mindestens fünf Jahren Freiheitsstrafe bedroht ist und bei der es sich nicht um eine Straftat nach § 353b StGB handelt. Dies dient zur Stärkung des Informantenschutzes und der Pressefreiheit.[499]

Ansonsten zieht jeder Verstoß gegen § 108 StPO nicht ohne Weiteres ein strafprozessuales Verwertungsverbot von (Zufalls-)Funden nach sich.[500] Nach ständigen Rspr. des *BVerfG* ist ein Beweisverwertungsverbot zumindest bei schwerwiegenden, bewussten oder willkürlichen Verfahrensverstößen geboten, bei denen die grundrechtlichen Sicherungen planmäßig oder systematisch außer Acht gelassen worden sind,[501] und auch dabei muss das Interesse des Betroffenen das Strafverfolgungsinteresse des Staates überwiegen.[502] Zuerst wird in den Fällen, in denen der Kernbereich privater Lebensgestaltung berührt ist, ein absolutes Beweisverwertungsverbot unmittelbar aus den Grundrechten angenommen. Ob ein Sachverhalt zu diesem Kernbereich zuzuordnen ist, kann jedoch nur unter Berücksichtigung der Besonderheiten des einzelnen Falls bewertet werden (vgl. Kapitel 2, B. II. 2.). Außerdem führt nach h. M. auch die (einstweilige) Beschlagnahme von Gegenständen, die einem Beschlagnahmeverbot nach § 97 unterliegen, – ausnahmslos – zum Ver-

[497] *Bruns*, KK-StPO, § 108 Rn. 9; *Cordes*/*Pannenborg*, NJW 2019, 2973, 2975; *Hauschild*, MüKo-StPO, § 108 Rn. 16.

[498] *Cordes*/*Pannenborg*, NJW 2019, 2973, 2974 f.; *Hauschild*, MüKo-StPO, § 108 Rn. 13; M-G/*Schmitt*, StPO, § 108 Rn. 9; *Roxin*/*Schünemann*, § 35 Rn. 12.

[499] BT-Drs. 16/6979, S. 44; *Cordes*/*Pannenborg*, NJW 2019, 2973, 2975; *Hauschild*, MüKo-StPO, § 108 Rn. 14; M-G/*Schmitt*, StPO, § 108 Rn. 10; *Roxin*/*Schünemann*, § 35 Rn. 12.

[500] *BVerfG* NJW 2009, 3225, 3226 [Rn. 18]; *Hauschild*, MüKo-StPO, § 108 Rn. 12; vgl. auch aus einem Verstoß gegen § 108 Abs. 1 S. 3 StPO, *Park*, § 2 Rn. 126.

[501] *BVerfGE* 113, 29, 61 [Rn. 135]: Hierbei handelte es sich um Verfahrensverstöße bezüglich der Beschlagnahme von Datenträgern in einer Anwaltskanzlei und der auf das Verfahrensrelevante beschränkten Kenntnisnahme der darauf vorhandenen Daten; NJW 2009, 3225, 3226 [Rn. 17]; 2011, 2417, 2419 [Rn. 45]; *Cordes*/*Pannenborg*, NJW 2019, 2973, 2976 [Tz. 3.]; *Hauschild*, MüKo-StPO, § 108 Rn. 12; M-G/*Schmitt*, StPO, Einl. Rn. 55; *Roxin*/*Schünemann*, § 35 Rn. 11.

[502] *BVerfG* NJW 2009, 3225, 3225 f. [Rn. 17]; 2011, 2417, 2419 [Rn. 44]; *Cordes*/*Pannenborg*, NJW 2019, 2973, 2976; *Hauschild*, MüKo-StPO, § 108 Rn. 12.

wertungsverbot.[503] Haben die durchsuchenden Beamten hingegen verfahrensirrelevante Daten, insb. Beweismittel für eine andere Straftat, unter dem Vorwand des § 108 Abs. 1 S. 1 StPO einstweilig beschlagnahmt (bei einem Verstoß gegen das Verbot der systematisch/planmäßig gezielten Suche),[504] dann fallen die Meinungen zum Verwertungsverbot für derart gefundene Gegenstände auseinander. Nach h. M. und Rspr. folgt dies der Abwägung im Einzelfall.[505] In der Praxis ist es jedoch fast unmöglich, dass der Betroffene eine bewusste oder absichtliche Ausdehnung der Durchsuchung durch Ermittlungsbehörden wirksam überwacht, und außerdem ist dies faktisch schwerlich nachzuweisen. Dies unterläuft schließlich die Begrenzungsfunktion des richterlichen Durchsuchungsbeschlusses. Wenn das Verwertungsverbot bei gezielter Suche nur schwerlich anzunehmen ist, wird dies *de facto* dazu, dass der Eingrenzungsfunktion in der Praxis Rechnung getragen wird.[506] In dieser Hinsicht ist bei Durchsicht vorläufig sichergestellter elektronischer Daten ihre Auswertung und Verwendung ohne Schlagwörter aufgrund richterlicher Anordnung unzulässig, es sei denn, es gibt einen besonderen Grund.[507] Zudem sollte der Betroffene mit seinem Verteidiger bei der Durchsuchung und insb. der Durchsicht der vorläufig sichergestellten Daten anwesend sein und dadurch die durchsuchenden Beamten überwachen können;[508] vgl. unten IV. 2.

5. Beendigung der Durchsicht

Werden die zu beschlagnahmenden Papiere durch die Durchsicht nach § 110 StPO ausgewählt und ausgesondert und sind sie weiter trennbar, so muss die StA die Durchsicht zu Ende bringen und sogleich bei dem Ermittlungsrichter die Be-

---

[503] *Hauschild*, MüKo-StPO, § 108 Rn. 12; dazu *Greven*, KK-StPO, § 97 Rn. 9; *Park*, § 3 Rn. 683; *Wohlers*/*Greco*, SK-StPO, § 97 Rn. 95; abw. M-G/*Schmitt*, StPO, § 97 Rn. 46a und 50: Bei Angehörigen nach § 52 Abs. 1 StPO wird ein Verwertungsverbot bejaht, bei Berufsgeheimnisträgern nach § 53 StPO wird hingegen das nur bei Unverhältnismäßigkeit bejaht.

[504] Eine Durchsuchung darf kein bloßer Vorwand sein, um systematisch nach Gegenständen zu suchen, auf die die Durchsuchungsanordnung nicht abzielt (*Hauschild*, MüKo-StPO, § 108 Rn. 12; M-G/*Schmitt*, StPO, § 98 Rn. 1).

[505] *BVerfGE* 113, 29, 61 [Rn. 135]; NJW 2009, 3225 [Rn. 16]; 2011, 2417, 2418 f. [Rn. 44]; *Bruns*, KK-StPO, § 108 Rn. 1; M-G/*Schmitt*, StPO, Einl. Rn. 55; *Hauschild*, MüKo-StPO, § 108 Rn. 12. In dem auf dem Prinzip der materiellen Wahrheit basierenden deutschen Prozessmodell ist das Beweisverwertungsverbot nicht so selbstverständlich (*Roxin*/*Schünemann*, § 24 Rn. 13), aus der StPO ist auch kein grundsätzliches Beschlagnahmeverbot bzw. kein allgemeines Beweisverwertungsverbot für Fälle fehlerhafter Durchsuchungen abzuleiten (*BVerfG* NJW 2011, 2417, 2419 [Rn. 45]; *Park*, § 2 Rn. 377).

[506] Zust. *Cordes*/*Pannenborg*, NJW 2019, 2973, 2975 f.; *Park*, § 2 Rn. 420; vgl. *Krekeler*, NStZ 1993, 263, 267 [Tz. b)]. Die Verwertung der hier erlangten Beweismittel stellt einen Verstoß gegen den Grundsatz des fairen Verfahrens und eine Beeinträchtigung des Anspruchs des Betroffenen auf Einhaltung der Verfahrensvorschriften dar (*Cordes*/*Pannenborg*, a. a. O.; *Krekeler*, a. a. O.; *Park*, a. a. O.).

[507] *Cordes*/*Pannenborg*, NJW 2019, 2973, 2977 [Tz. 6.].

[508] *Park*, § 2 Rn. 217.

schlagnahme der möglichst genau bezeichneten Papiere beantragen und die sonstigen an den Betroffenen wieder herausgeben oder löschen.[509] Die Durchsicht wird auch dann beendet, wenn das Gesamte der Daten oder der Datenbestände oder größere Teile davon wegen der inhaltlichen oder technischen Unmöglichkeit der Auswahl, Aussonderung und Trennung zu beschlagnahmen sind. Wurde der Originaldatenbestand vorläufig sichergestellt, so sind die zu beschlagnahmenden Daten auf Datenträger der Ermittlungsbehörden zu kopieren und die Übrigen zu löschen sowie das Original an den Inhaber zurückzugeben. Hierbei bedeutet die „Rückgabe", dass der ursprüngliche Gewahrsamsinhaber die Originaldaten zurückerhält und zugleich die Behörden keine Zugriffsmöglichkeit auf die – verfahrensirrelevanten – Daten mehr haben.[510] Andererseits ist wie schon erwähnt die Eilzuständigkeit für die Anordnung der „Beschlagnahme" der StA von vornherein ausgeschlossen und diese ist stets dem Richter vorbehalten (vgl. oben 1. c)).

Nach – endgültiger – Beschlagnahme gilt § 110 StPO nicht mehr, und daher gibt es auch keine Beschränkung der Durchsichtsbefugnis. Die Verwendung der beschlagnahmten Papiere stellt eine „Auswertung der Beweismittel" dar und diese ist von der Durchsicht der Papiere gemäß § 110 StPO zu unterscheiden.[511] Während die Durchsicht als Durchsuchung auf die Entscheidung über den Antrag zur Beschlagnahme oder Rückgabe bzw. Löschung abzielt, ist die Auswertung der Papiere nach der Beschlagnahme auf ihre Verwendung oder Bewahrung zur Aufklärung von Straftaten ausgerichtet. Nach außen hin sind die beiden Fälle insofern identisch, als die Papiere von den Ermittlungsbehörden sichergestellt und durchgesehen werden, aber der „Zweck jeder Maßnahme" ist unterschiedlich. Daher ist aufgrund der §§ 94, 98 StPO eine „vorsorgliche Beschlagnahme" zum Zweck der Durchsicht i. S. d. § 110 StPO nicht gestattet[512] und die zeitliche Grenze nach dem Verhältnismäßigkeitsgrundsatz ist anders zu beurteilen. Die Dauer der Auswertung der beschlagnahmten Papiere bestimmt sich nach den Umständen des Einzelfalls und daher liegt keine feste Zeitgrenze vor.[513] Sie wird indes meist länger als die Zeitspanne der Durchsicht nach § 110 StPO (vgl. oben 3. c)) sein, weil die Auswertung die Verwendung potenziell beweiserheblicher Materialien betrifft. Zum anderen beruht der Sachentzug der Papiere, der nach dem Abschluss der Durchsicht fortdauert, nicht mehr auf der Durchsuchungs-, sondern auf einer neuen Beschlagnahmeanordnung. Daher kann

[509] *BGH* NJW 1995, 3397; *Graulich*, wistra 8/2009, 299, 302; *Mildeberger/Riveiro*, StraFo 2004, 43, 44, 46; *Szesny*, WiJ 2012, 228, 233; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 27; auch *BVerfG* NJW 2002, 1410, 1410 f.: Bei Dateien in einem Computer wird deren Löschung auf den Datenträgern gefordert.

[510] *Szesny*, WiJ 2012, 228, 233: Ansonst kann dies zu illegaler Vorratsdatenspeicherung führen.

[511] *OLG Bremen* wistra 1999, 74, 76; *Ciolek-Krepold*, Rn. 145; *Glock*, NStZ 2019, 248, 249 am Anfang; *Mildeberger/Riveiro*, StraFo 2004, 43, 44 [Tz. 1.] und 46; *Park*, § 2 Rn. 229, 246 und 261; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 27.

[512] *Graulich*, wistra 8/2009, 299, 300; *Park*, § 2 Rn. 248.

[513] M-G/*Schmitt*, StPO, § 94 Rn. 18 a. E. und Rn. 18a a. E.

der Betroffene gegen die (richterliche) Beschlagnahmeanordnung Beschwerde einlegen, soweit er sich gegen solchen Eingriff wehren möchte (§§ 304 ff. StPO).[514]

6. Zusammenfassung und Zwischenfazit

(1) Die Durchsicht nach § 110 StPO, die im Zuge der Durchsuchung der Auswahl und Aussonderung nur von potenziell beweiserheblichen Daten dient, ist heutzutage u. a. bei IT-Durchsuchungen für den von der Maßnahme Betroffenen bezüglich des Grundrechtsschutzes und aufseiten der Ermittlungsbehörden zur Verfahrenseffizienz von erheblicher Bedeutung. Die inhaltliche Einschränkung des Umfangs der Beschlagnahme durch diese Vorgehensweise kommt somit sowohl dem Betroffenen als auch den Ermittlungsbehörden zugute. Die Vorschrift ist keineswegs eine inhaltlose (Ordnungs-)Formel. Es scheint aber, dass in der täglichen Durchsuchungspraxis § 110 StPO weder ausreichend noch sinnvoll genutzt, sondern hintangesetzt wird, und dass sowohl die Ermittlungsbehörden als auch die Gerichte keinen besonders großen Wert auf die Vorschrift legen.[515] Jedoch besteht bei IT-Durchsuchung einer umfangreichen Datenbank die Eilzuständigkeit für die „Beschlagnahmeanordnung" i. d. R. nicht von vornherein, hierbei ist die Mitnahme in die Behördenräume der bei der Durchsuchung aufgefunden Papiere oder EDV-Anlagen nicht als Beschlagnahme, auch wenn die Ermittlungsbehörden sie förmlich so bezeichnet, sondern als die vorläufige Sicherstellung nach § 110 StPO anzusehen. Dies gilt auch dann, wenn die Gültigkeit der Beschlagnahmeanordnung im Kombi-Beschluss abgelehnt wird. Das *LG Berlin* wies diesbezüglich zu Recht darauf hin:

> „Für die … mitgenommenen Gegenstände – (zusammen mit Mobiltelefon) Notizzettel und -blöcke, PC-Tower, CD-ROMs und Disketten sowie einen USB-Speicherstick – …. Bei der insoweit durch die durchsuchenden Polizeibeamten erfolgten ‚Beschlagnahme' handelt es sich folglich in Wirklichkeit nicht um eine Beschlagnahme i. S. v. §§ 94 Abs. 2, 98 StPO, sondern lediglich um die Mitnahme zum Zweck einer Durchsicht gemäß § 110 StPO, die der Auswahl möglicherweise zu beschlagnahmender Aufzeichnungen dient."[516]

Nach der Mitnahme und Durchsicht hat die StA somit zur Beschlagnahme nach § 98 Abs. 1 S. 1 StPO eine allgemeine „gerichtliche Anordnung" zu beantragen, nicht die – ausnahmsweise – gerichtliche „Bestätigung" i. S. d. § 98 Abs. 2 S. 1 StPO.[517] Zum anderen, da dabei auch irrtümlich keine Gefahr im Verzug für die Beschlagnahme anzunehmen ist, liegt in der (umfassenden) Beschlagnahme von Daten auf Grundlage der Eilkompetenz und der darauf beruhenden Durchsicht (nämlich Auswertung der beschlagnahmten Beweismittel) ein schwerwiegender, willkürlicher oder – mindestens – bewusster Verstoß unmittelbar gegen den Rich-

[514] *BGH* NJW 1995, 3397; *Graulich*, wistra 8/2009, 299, 302; *Mildeberger/Riveiro*, StraFo 2004, 43, 46.

[515] Vgl. *Park*, § 2 Rn. 246 f.

[516] *LG Berlin* NStZ 2004, 571, 573 [Rn. 23].

[517] *LG Berlin* NStZ 2004, 571, 573 f. [Rn. 24 f.].

tervorbehalt und mittelbar gegen § 110 StPO vor. So können die erlangten Informationen ausreichend zu einem Verwertungsverbot führen.[518]

(2) Da sonstige Regelungen als die Beschränkung der Durchsichtskompetenz in der § 110 StPO nicht vorliegen, unterliegt es zunächst der Entscheidung der StA, in welchem Umfang und wie die Mitnahme und Durchsicht der Papiere im Verlauf der Durchführung der Durchsuchung im Einzelfall zu gestalten ist und wann sie zu beenden ist. Die StA stellt als Herrin des Ermittlungsverfahrens die zur Durchsicht original befugte Person nach § 110 Abs. 1 StPO dar und hat einen eigenverantwortlichen Ermessenspielraum in der Gestaltung.[519] In Ansehung dessen, dass der Persönlichkeits- und Datenschutz heute im Zuge der Durchsicht der EDV-Daten von großer Bedeutung ist, müssen aber hierbei die verfahrensrechtlichen Vorkehrungen zum Schutz der Grundrechte des Betroffenen nach dem Verhältnismäßigkeitsgrundsatz gestaltet werden. Dies ist nicht schlechthin nur in das Ermessen der StA und ihrer Ermittlungspersonen zu stellen. Dies gilt umso mehr u. a. vor dem Hintergrund, dass in der Praxis die Daten vielfach „umfassend" mitgenommen werden (vgl. unten IV.).

IV. Verfahrensbalance i. R. d. Beschlagnahme und Durchsuchung von Papieren

1. Vorrede

Bei der Durchsuchung und Beschlagnahme im EDV-Bereich ist in vielen Fällen ein umfassender Zugriff auf Daten zwar unvermeidlich, aber hier ist der Umfang der Beschlagnahme durch die vorläufige Sicherstellung und die Durchsicht nach § 110 StPO unbedingt inhaltlich angemessen zu beschränken. In der Praxis wird indes diese Verfahrensweise vielfach unter Außerachtlassung des § 110 StPO schlichtweg vernachlässigt, oder die Einhaltung der inhaltlichen Beschränkung liegt in der Tat in der Hand der Ermittlungsbehörden.[520] In diesem Fall wirft sich eine neue Frage auf. Die Beschlagnahme nach § 94 StPO oder die vorläufige Sicherstellung und Durchsicht nach § 110 StPO zählen rechtssystematisch zu „offenen Ermittlungsmaßnahmen", doch sie können dann faktisch zu einer „heimlichen Maßnahme" führen, wenn sie sich auf den gesamten Datenbestand oder sämtliche darauf ge-

[518] Zust. *Park*, § 2 Rn. 425: bei einem bewussten, willkürlichen Verstoß; vgl. M-G/*Schmitt*, StPO, § 110 Rn. 10: bei schwerwiegenden Verstößen gegen § 110 Abs. 1 oder 2 StPO; *Wohlers*/*Jäger*, SK-StPO, § 110 Rn. 30: bei schwerwiegenden, bewussten oder willkürlichen Verstößen; vgl. aber *Dauster*, StraFo 6/1999, 186, 188.

[519] *BGH* NJW 1995, 3397; NStZ 2003, 670, 671; *Bruns*, KK-StPO, § 110 Rn. 1; *Graulich*, wistra 8/2009, 299, 301; *Peters*, NZWiSt 2017, 465, 467 am Anfang.

[520] Vgl. *Peters*, NZWiSt 2017, 465, 468 f.: Die Einhaltung ist vielfach schwierig.

speicherte Daten richten.[521] Dabei ist freilich den von der Durchsuchung Betroffenen das „ob" der Durchsicht erkennbar, es ist aber noch nicht klar, welche Daten oder Dateien inhaltlich betroffen sind.[522] Daher können sie dabei anders als bei allgemeinen offenen Ermittlungen – unter Hinzuziehung anwaltlichen Beistandes – einer Durchführung der Maßnahme nicht entgegentreten, der es an den gesetzlichen Voraussetzungen fehlt, oder die über die Grenzen richterlicher Anordnung hinaus geht. Dazu kommt, dass dabei die unzulässige gezielte Suche nach Zufallsfunden ohne Kontrolle und Begrenzung möglich wird.[523] Schließlich kann dies tatsächlich zu einer heimlichen Online-Durchsuchung (vgl. § 100b StPO) führen, die derzeit nur unter besonders strengen Anforderungen zulässig ist. Dies steht aber dem Charakter der Durchsuchung nach §§ 102 ff. StPO ersichtlich entgegen, die eine „Offenheit" der Maßnahme voraussetzt.

Vor diesem Hintergrund sind nach dem Grundsatz der Verhältnismäßigkeit verfahrensrechtliche Schutzvorkehrungen erforderlich, um die Schwere des Eingriffs beim umfassenden Datenzugriff gemäß § 110 StPO auszugleichen.[524] Der Grundrechtsschutz durch eine nachträgliche Intervention des Richters reicht dabei wegen seiner geringen Erfolgsaussicht[525] nicht aus. Dies gilt auch angesichts der Tatsache, dass die Ermittlungsbehörden stets – tendenziell – versuchen, Daten so umfassend wie möglich sicherzustellen. Daher bedarf es u. a. eines Mittels, um direkt am Ort der Durchsuchung/Durchsicht ihr Verhalten angemessen zu überwachen. Der beste Weg dafür ist das Anwesenheitsrecht des Betroffenen und seines Verteidigers bei der Durchsicht der – mitgenommenen – Papiere. Damit kann der Betroffene einen übermäßigen Eingriff in seine Privat- bzw. Geschäftssphäre und ein Missbrauchspotenzial sensibler Informationen zumindest in einem gewissen Maße wirksam verhindern.[526] Insoweit ist es problematisch, ob das bereits *de lege lata* anerkannt werden kann oder *de lege ferenda* verankert werden sollte, und dies betrifft sowohl die Anwendung des § 106 Abs. 1 StPO auf die Durchsicht nach § 110 StPO als auch den Grundsatz der Verhältnismäßigkeit.

[521] Zust. *Peters*, NZWiSt 2017, 465, 469; *Szesny*, WiJ 2012, 228, 231: zu einer nahezu vollständigen Durchsuchung im Geheimen; vgl. *Knauer/Wolf*, NJW 2004, 2932, 2938: die Durchsicht im Dunklen.

[522] *Peters*, NZWiSt 2017, 465, 469 [Tz. 4.].

[523] Vgl. *Szesny*, WiJ 2012, 228, 231.

[524] Zust. *Peters*, NZWiSt 2017, 465, 469 f.: Mit Blick auf die massive Eingriffsqualität der Durchsicht gemäß § 110 StPO, die sich aus der Digitalisierung sämtlicher Lebensbereiche ergibt, weist die StPO massive Regelungslücken auf.

[525] Vgl. *Park*, § 1 Rn. 8.

[526] *Peters*, NZWiSt 2017, 465, 471; *Hamm*, StV 2010, 418, 420: der Verteidiger als Garant für die Einhaltung des Verfahrensrechts.

2. Anwesenheitsrecht des Betroffenen und seines Verteidigers

a) Meinungsstreit und Stellungnahme des BVerfG

Die Vorgängerregelung des § 110 Abs. 3 Hs. 2 StPO[527] enthielt die Bestimmung, dass „der Inhaber der Papiere oder dessen Vertreter", wenn möglich, zur Teilnahme an der Entsiegelung und Durchsicht der Papiere aufzufordern ist. Dieser Satz wurde zwar durch das 1. JuMoG vom 24. August 2004 „ohne nähere Begründung und ersatzlos" gestrichen,[528] aber die Bedeutung bzw. Wirkung dieser Überarbeitung ist umstritten. Dabei handelt es sich um die Frage, ob das Anwesenheitsrecht des von der Durchsuchung Betroffenen oder des von den Daten Betroffenen (insb. des Beschuldigten) und seines Verteidigers „vor der Beschlagnahme" der Papiere/Daten „bei deren Durchsicht" eingeräumt wird. Zuerst liegt eine tragende Begründung für die Ansicht, das Recht zu verweigern, in der Abschaffung im Jahr 2004 selbst,[529] es gibt keine anderen besonderen Gründe.[530] Die Gegenmeinung hingegen bezieht sich einerseits auf strafverfahrensrechtlicher Ebene auf den systematischen Gesichtspunkt, dass die Durchsicht noch zur Durchsuchung gehört,[531] und andererseits auf verfassungsrechtlicher Ebene auf den Grundsatz der Verhältnismäßigkeit.[532] Insoweit hat das *BVerfG* entschieden, dass die Anwesenheit des – nicht beschuldigten – Inhabers der sichergestellten Daten und seines Verteidigers zwar im Einzelfall zur Wahrung der Verhältnismäßigkeit (Abwägung) geboten sein kann, doch nicht immer:

> „Zur Wahrung der Verhältnismäßigkeit kann es im Einzelfall von Verfassungs wegen geboten sein, den Inhaber der sichergestellten E-Mails in die Prüfung der Verfahrenserheblichkeit einzubeziehen. … Konkrete, nachvollziehbare und überprüfbare Angaben vor allem Nichtverdächtiger zur Datenstruktur und zur Relevanz der jeweiligen Daten können deren materielle Zuordnung vereinfachen und den Umfang der sicherzustellenden Daten reduzieren. Von Verfassungs wegen ist es allerdings nicht geboten, in jedem Fall eine Teilnahme an der Sichtung sichergestellter E-Mails vorzusehen. Ob eine Teilnahme bei der Durchsicht

---

[527] § 110 Abs. 3 StPO in der bis zum 31. 8. 2004 geltenden Fassung.

[528] *BVerfGE* 113, 29, 58 [Rn. 127]; 124, 43, 72 [Rn. 96]; *Hiéramente*, wistra 11/2016, 432, 438; *Park*, § 2 Rn. 253; *Szesny*, WiJ 2012, 228, 232 [Tz. 2.]. Da dieser gesetzgeberische Akt ursprünglich auf den Wegfall der Möglichkeit der Beidrückung eines eigenen Siegels nach Abs. 3 Hs. 1 a. F. abgezielt hat, wird im Schrifttum teilweise die Streichung des Satzes 2 auch als „Redaktionsversehen" angesehen (*Knauer*/*Wolf*, NJW 2004, 2932, 2937; *Peters*, NZWiSt 2017, 465, 471 [Tz. 2.]; a. A. *Wohlers*/*Jäger*, SK-StPO, § 110 Rn. 25: Dies ist aber unsicher).

[529] Vgl. M-G/*Schmitt*, StPO, § 110 Rn. 5.

[530] Vgl. *Hiéramente*, wistra 11/2016, 432, 438; *Peters*, NZWiSt 2017, 465, 471 [Tz. 2.].

[531] *Hiéramente*, wistra 11/2016, 432, 438 f.; *Knauer*/*Wolf*, NJW 2004, 2932, 2937 f.: *Peters*, NZWiSt 2017, 465, 470 [Tz. a)]; *Szesny*, WiJ 2012, 228, 232 [Tz. 2.]; *Wohlers*/*Jäger*, SK-StPO, § 110 Rn. 25.

[532] *Hiéramente*, wistra 11/2016, 432, 438 f.; *Peters*, NZWiSt 2017, 465, 470 f. [Tz. b)]; *Szesny*, WiJ 2012, 228, 232 [Tz. 2.]; *Wohlers*/*Jäger*, SK-StPO, § 110 Rn. 25.

geboten ist, ist im jeweiligen Einzelfall unter Berücksichtigung einer wirksamen Strafverfolgung einerseits und der Intensität des Datenzugriffs andererseits zu beurteilen."[533]

Das *BVerfG* hat hierbei auf das „Anwesenheitsrecht des Inhabers der Papiere/Daten" nach der gestrichenen Vorgängerregelung (§ 110 Abs. 3 StPO a. F.) hingewiesen. In diesem Fall könnte die Vorschrift aber gelten, weil die Daten (E-Mails) bereits beschlagnahmt sind, daher hat das Gericht für die Teilnahme ihres Inhabers an der Prüfung der Verfahrenserheblichkeit nur grundsätzliche Vorgabe, nämlich Verhältnismäßigkeit/Abwägung, dargelegt. Angesichts dieser Umstände hat sich es in die Frage noch nicht vertieft, ob ein reines Anwesenheitsrecht des Betroffenen bei der Durchsicht (nach einer vorläufigen Sicherstellung) nach § 110 StPO gewährt werden kann,[534] und es ist noch unklar, ob es das Recht anerkennt.

b) Begründung für das Anwesenheitsrecht

Daran hat sich trotz des Wegfalls des § 110 Abs. 3 StPO a. F. nichts geändert und das Anwesenheitsrecht „des von Durchsuchung Betroffenen (Inhaber der Papiere/Daten)" bzw. „des von Daten Betroffenen (Daten-Eigentümer)" und „seines Verteidigers" können aufgrund des Verhältnismäßigkeitsgrundsatzes und von einigen Vorschriften der StPO noch eingeräumt werden. Sie sind daher berechtigt, der Durchsicht der – mitgenommen – Papiere/Daten beizuwohnen, und davon davor in Kenntnis zu setzen.

(1) Nach dem Grundsatz der Verhältnismäßigkeit muss die überschießende Gewinnung von verfahrensirrelevanten Informationen zum Grundrechtsschutz i. R. d. Vertretbaren vermieden werden,[535] doch dies kann – insb. in Wirtschafts- und Steuerstrafsachen – nur dann zumindest in einem gewissen Maße verwirklicht werden, wenn die Anwesenheit des Betroffenen und seines Verteidigers bei der inhaltlichen Durchsicht nach § 110 StPO gewährleistet wird. Dies gilt u. a. für die Sicherstellung und die Sichtung umfangreicher Daten.[536] Je weiter und undifferenzierter der Umfang der durchzusehenden Daten ist, desto schwerer wiegt das Interesse des von der Daten Betroffenen an Anwesenheit bei der Durchsicht.[537] Können sie in diesem Fall bei der Durchsicht in behördlichen Räumen nicht anwesend sein, dann bedeutet dies unter Verhältnismäßigkeitsgesichtspunkten einen „bedeutenden

[533] *BVerfGE* 124, 43, 72 [Rn. 96]; vgl. 113, 29, 58 f. [Rn. 127]. Nach dem Sachverhalt der ersteren Entscheidung wurden etwa 2.500 E-Mails, die auf dem Server eines Dienstanbieters gespeichert worden waren, aufgrund der Beschlagnahmeanordnung nach §§ 94, 98 StPO – nicht aufgrund der vorläufigen Sicherstellung nach § 110 StPO – durch ihn auf einen Datenträger kopiert und den Ermittlungsbehörden übergeben (a. a. O. 47 f. [Rn. 23]), aber allein daraus, dass er Nichtverdächtiger ist, folgt kein verfassungsunmittelbares Teilnahmerecht an der Durchsicht der sichergestellten E-Mails (a. a. O. 77 [Rn. 112]).

[534] Zust. *Hiéramente*, wistra 11/2016, 432, 438.

[535] *BVerfGE* 113, 29, 55 [Rn. 114]; 124, 43, 68 [Rn. 84].

[536] *Peters*, NZWiSt 2017, 465, 471 [Tz. b)].

[537] *Szesny*, WiJ 2012, 228, 232 a. E.

Verfahrensrechtsverlust".[538] Diese verfassungsrechtliche Begründung ist sinnvoll, wenn der von der Durchsuchung Betroffene den – einfachen – Gewahrsamsinhaber der Daten darstellt, der nicht der Beschuldigte ist (vgl. § 103 StPO), insb. wenn die Daten auf dem Server des Dienstanbieters vorhanden sind.

Zum anderen fällt die vorläufige Sicherstellung und Durchsicht der Daten nach § 110 StPO unter die Durchsuchung, somit gilt hierfür auch die Anwesenheit des Inhabers und seines Vertreters i. S. d. § 106 Abs. 1 StPO.[539] Diese Vorschrift kennzeichnet u. a. die Offenheit der Durchsuchung nach §§ 102, 103 StPO, indem sie das Recht des Inhabers der Durchsuchungsgegenstände gewährleistet, der Durchsuchung beizuwohnen. Das heißt, ein solches Anwesenheitsrecht ist mit dem offenen Charakter der Maßnahme verbunden, dem Betroffenen die Möglichkeit zu geben, – ggf. mit anwaltlichem Beistand – den staatlichen Eingriff zu kontrollieren, und es gewährleistet dadurch den Schutz des Einzelnen.[540] All dies ist in Ordnung bei der Durchsuchung der Beschuldigten nach § 102 StPO.[541] Bei der Durchsuchung anderer Personen nach § 103 StPO, insb. bei der „Durchsuchung der serverbasiert gespeicherten Daten", gibt es hingegen ein Problem mit dem Schutz des von der Daten Betroffenen. Denn in diesem Fall hat er, auch wenn er der Beschuldigte ist, kein eigenes Anwesenheitsrecht bei der Durchsicht, weil er keinen Inhaber des Speichermediums oder der Daten darstellt.[542] Dabei kann er – und auch sein Verteidiger – allerdings unter Einverständnis des Gewahrsamsinhabers an der Durchsicht teilnehmen (vgl. oben B. II. 2. b)) bb) (2)). Es ist aber erheblich zweifelhaft, ob das in der Praxis – außer etwa von Familie, Freunden und Arbeitgebern – auch von Dienstleistern unbefangen und frei erteilt wird. Hierbei könnte jedoch ein eigenes Anwesenheitsrecht dem von der Daten Betroffenen, der kein Gewahrsamsinhaber der Daten ist, unter Verhältnismäßigkeitsgesichtspunkt zukommen (vgl. obiger Absatz).

(2) Der Betroffene ist zumeist juristischer Laie, und so kann sein Anwesenheitsrecht nur mithilfe eines Verteidigers/Anwalts wirksam gewährleistet werden. Auch wenn er bei der Durchsicht anwesend ist, ist es überhaupt für ihn sehr schwer, dass er allein, ohne Verteidiger, beurteilt, welche Unterlagen für ihn möglicherweise nachteilig sind[543] oder so früh wie möglich zurückgegeben oder gelöscht werden

[538] Vgl. *Hiéramente*, wistra 11/2016, 432, 439.

[539] *Bruns*, KK-StPO, § 106 Rn. 1; *Michalke*, StraFo 3/2014, 89, 91. Dabei ist ein Verteidiger oder Anwalt des Betroffenen, nicht sein Nachbar oder Hausgenosse, als Vertreter primär bei der Durchsicht hinzuzuziehen (*Knauer/Wolf*, NJW 2004, 2932, 2938).

[540] *BVerfGE* 115, 166, 194 f. [Rn. 106]; *BGHSt* 51, 211, 215 [Rn. 10]; *Hiéramente*, wistra 11/2016, 432, 438 a. E.; *Peters*, NZWiSt 2017, 465, 470 [Tz. a)] und dazu [Tz. b)]: Ein Anwesenheitsrecht ist der effektivste Weg, um den Charakter als offene Ermittlungsmaßnahme der Durchsicht zu gewährleisten.

[541] Hier stellt er als Gewahrsamsinhaber der Datenträger oder der darauf gespeicherten Daten den originären Inhaber des Anwesenheitsrechts dar (vgl. *Peters*, NZWiSt 2017, 465, 471 [Tz. 3.]).

[542] *Peters*, NZWiSt 2017, 465, 471 f. [Tz. 3.].

[543] *Park*, § 2 Rn. 254.

sollten. Daher sollte der Verteidiger des von den Papieren/Daten Betroffenen im Regelfall bei der Durchsicht anwesend sein können, es sei denn, es ist gegen den Willen des Betroffenen.[544] Diesbezüglich stellt sich die Frage, ob dem Verteidiger ein eigenes Anwesenheitsrecht zukommen kann. Wenn der von Daten Betroffene der Beschuldigte ist, gleichviel, ob er der Inhaber ist, so kann das Recht seinem Verteidiger unter Hinweis auf § 163a Abs. 3 S. 2 i. V. m. § 168c Abs. 1 StPO verliehen werden. Denn wenn der Verteidiger des Beschuldigten bei dessen Vernehmung stets ein Anwesenheitsrecht hat, so muss dies auch für die Durchsicht von den Beschuldigten möglicherweise belastenden Papieren gelten.[545]

Eine solche Anwesenheit des Verteidigers kann zum anderen die Grenzen seines Akteneinsichtsrechtes nach § 147 StPO ergänzen. Nach § 147 Abs. 1 und 2 StPO ist er im Ermittlungsverfahren befugt, die Akten, die dem Gericht vorliegen oder diesem im Falle der Erhebung der Anklage vorzulegen wären, und amtlich verwahrte Beweisstücke dann einzusehen, soweit dies den Untersuchungszweck nicht gefährden kann[546] und zu den letzteren Beweisstücken gehören die Daten, die nach §§ 94 ff. StPO beschlagnahmt oder in anderer Weise sichergestellt sind.[547] Die Teilnahme des Verteidigers an der Durchsicht nach § 110 StPO gibt ihm die Gelegenheit, Genaueres über den gegenüber dem Beschuldigten erhobenen Vorwurf und das ihn belastende Material kennenzulernen, und dies trägt zur Sicherung prozessualer Rechte des Beschuldigten bei.[548] In diesem Sinne ist die Anwesenheit des Verteidigers ein taktisches Mittel, sich frühzeitig in das Ermittlungsverfahren einzuschalten und entsprechend die Interessen des Betroffenen zu vertreten.[549]

3. Zwischenfazit

(1) Weil die Durchsichtsbefugnis nach § 110 StPO bereits bis auf die Ermittlungspersonen der StA erweitert ist, ist ein Problem bezüglich der Personalsituation in der Praxis durch die Einschränkung der Durchsichtsbefugnis in gewissem Maße verringert (vgl. oben III. 2. b)). Die Regelvorstellung des § 110 StPO, die Verhältnismäßigkeit bei Beschlagnahme und Durchsuchung zu erreichen, ist jedoch noch nicht ausreichend verwirklicht. Dafür ist es vor allem sinnvoll, beim Zugriff auf umfangreiche Daten im Ermittlungsverfahren – neben der Gewährleistung des

[544] Vgl. *OLG Jena* NJW 2001, 1290, 1294 [Tz. dd)]: Denn den berechtigten Interessen des Inhabers des Schriftguts daran, dass sich die Kenntnisnahme von dessen Inhalt auf den in § 110 StPO vorgesehenen Personenkreis beschränkt, kommt große Bedeutung zu.

[545] *Knauer*/*Wolf*, NJW 2004, 2932, 2938; *Park*, § 2 Rn. 254: arg. *a maiore ad minus.*

[546] M-G/*Schmitt*, StPO, § 147 Rn. 10 & 25; *Willnow*, KK-StPO, § 147 Rn. 15.

[547] M-G/*Schmitt*, StPO, § 147 Rn. 19; *Peters*, NZWiSt 2017, 465, 470 [Tz. a)]; vgl. *OLG Jena* NJW 2001, 1290, 1294: Der Befugnis zur Akteneinsicht nach § 147 Abs. 1 StPO unterliegen *de lege lata* die i. R. d. Durchsuchung vorläufig sichergestellten Papiere erst, wenn die Durchsicht gem. § 110 Abs. 1 StPO erfolgt und eine Beschlagnahmeanordnung ergangen ist.

[548] *Park*, § 2 Rn. 255.

[549] *Mildeberger*/*Riveiro*, StraFo 2004, 43, 46 [Tz. 6.].

Verfahrens nach § 110 StPO – dem Betroffenen und seinem Verteidiger grundsätzlich die Möglichkeit zu geben, bei der Durchsicht anwesend zu sein. Dies trägt eindeutig zur Vermeidung übermäßiger Datenzugriffe im Wege der Durchsicht und zur Angemessenheit inhaltlicher Aussonderung und Trennung verfahrens(ir)relevanter Daten bei. Freilich besteht hierbei die Gefahr eines erheblichen Zeitaufwands, der zu einer Verzögerung des gesamten Ermittlungsverfahrens führt.[550] Dennoch kann dies i. d. R. nicht als Gefährdung des Untersuchungszwecks angesehen werden, es sei denn, dass dies eine Störung i. S. d. § 164 StPO ist und eine Verdunkelungsgefahr vorliegt. Vielmehr sind durch eine solche Anwesenheit und einen gewissenhaften Dialog zwischen den Ermittlungsbehörden und dem rechtlichen Beistand ggf. die Behörden hinsichtlich der Durchsicht der Papiere zu entlasten und auch eine Verfahrensverzögerung ist zu vermeiden.[551] Außerdem ist es ggf. für alle Parteien praktisch, eine sinnvolle Lösung zu finden.[552] Andererseits können die Behörden auch mit diesem transparenten Vorgehen etwaigen Vorwürfen begegnen, dass die Durchsicht in unrechtmäßiger Weise durchgeführt wurde.[553]

(2) Wenn die Teilnahme des Betroffenen und seines Verteidigers an der Durchsicht nach § 110 StPO von einer Abwägung abhängt, wird die Zuständigkeit dafür i. d. R. der StA oder ggf. ihren Ermittlern zugeordnet. Aber hierbei kann das Anwesenheitsrecht tatsächlich ausgehöhlt werden. Denn die Ermittlungsbehörden werden tendenziell seine Anwesenheit ausschließen und zudem wird der nachträgliche Einwand gegen ihre Entscheidung wahrscheinlich unwirksam sein. Vor diesem Hintergrund wird die Anwesenheit, die in der Praxis oft erfolgt, irrtümlicherweise als ein „kulantes Entgegenkommen der Strafverfolgungsbehörden" angesehen, nicht als rechtstaatliche Garantie.[554] Somit ist die Zurückhaltung des *BVerfG* bezüglich des Anwesenheitsrechts unvertretbar. Das kann nicht mehr fakultativ sein und dafür ist eine ausdrückliche gesetzliche Regelung erforderlich.[555]

Der von der Durchsuchung oder Daten Betroffene hat im Regelfall das Anwesenheitsrecht.[556] Das ist jedoch angesichts der effektiven Strafverfolgung dann –

[550] *Mildeberger/Riveiro*, StraFo 2004, 43, 46 [Tz. 6.].

[551] *Peters*, NZWiSt 2017, 465, 471 [Tz. b)]; Erhöhung der Effizienz der Durchsicht; *Szesny*, WiJ 2012, 228, 232: erhebliche Beschleunigung der Aussonderung verfahrensirrelevanter Dateien und schnellere Identifikation relevanter Beweismittel; *Wohlers/Jäger*, SK-StPO, § 110 Rn. 25: Begrenzung des Eingriffsumfangs auf das erforderliche Maß durch Hinweise; vgl. auch *BVerfGE* 113, 29, 59 [Rn. 127]: „*Auch der Generalbundesanwalt vertritt dementsprechend in seiner Stellungnahme die Auffassung, dass konkrete Angaben der nichtverdächtigen Sozien, welche Daten nur ihnen zuzuordnen seien, die Entscheidung über den Umfang der Sicherstellung und Beschlagnahme hätten beeinflussen können. Der Deutsche Steuerberaterverband betont, dass dem Berufsgeheimnisträger zur Begrenzung des Zugriffs die Gelegenheit zu geben sei, die Relevanz der Daten darzulegen.*"

[552] *Hiéramente*, wistra 11/2016, 432, 439.

[553] Zust. *Park*, § 2 Rn. 253.

[554] Vgl. *Peters*, NZWiSt 2017, 465, 472 [Tz. 4.].

[555] Zust. *Peters*, NZWiSt 2017, 465, 472 [Tz. 4. und IV.].

[556] Natürlich kann er sein Recht ausdrücklich oder stillschweigend aufgeben.

ausnahmsweise – auszuschließen, soweit seine Anwesenheit den „Untersuchungszweck gefährden“ kann, beispielsweise wenn weitere überraschende Zwangsmaßnahmen aufgrund einer Ermittlungsstrategie oder geplanter Ermittlungen wahrscheinlich erwartet werden,[557] oder wenn eine übermäßige zeitliche Verzögerung auftreten kann[558] (vgl. analog § 147 Abs. 2 S. 1 StPO). Doch nur eine vage und bloße Möglichkeit der Gefährdung wird dieser Beschränkung nicht gerecht,[559] sondern es bedarf einer durch konkrete Anhaltspunkte belegten Gefahr.[560] Bei der Gefährdung des Untersuchungszwecks, das Anwesenheitsrecht auszuschließen, handelt es sich daher – wie bei der Gefahr im Verzug – um einen gerichtlich nachprüfbaren unbestimmten Rechtsbegriff, der einer vollständigen gerichtlichen Kontrolle in tatsächlicher und rechtlicher Hinsicht unterliegen sollte. Hierbei obliegt der StA die Beweislast für konkrete Tatsachen. Daher darf sie die Anwesenheit des Betroffenen und seines Verteidigers nur wegen einer damit verbundenen vagen Besorgnis oder üblichen Zeitverzögerung ohne konkrete Begründung nicht verweigern. Demzufolge kann der Betroffene insofern entsprechend § 98 Abs. 2 S. 2 StPO eine gerichtliche Entscheidung über die Rechtmäßigkeit der Entscheidung der StA beantragen, und andererseits kann der Richter am AG den Beschlagnahmeantrag der StA wegen des Fehlens einer Gewährleistung des Verfahrensrechts zurückweisen.

D. Anwendungsbereich und Verfahrenskontrolle der allgemeinen Vorschriften der Beschlagnahme und Durchsuchung in der K-StPO

I. Übersicht

Der Begriff und die materiellen Voraussetzungen der Beschlagnahme und Durchsuchung sowie der Sinn und Zweck des Richtervorbehalts werden in Südkorea genauso verstanden wie in Deutschland. Die Einzelheiten und die Auslegung der allgemeinen Vorschriften der Beschlagnahmen und Durchsuchung, §§ 106 ff. i. V. m. §§ 215 ff. K-StPO, unterscheiden sich jedoch teilweise von denen der StPO. In diesem Abschnitt werden zunächst die allgemeinen Voraussetzungen und Verfahren für die Beschlagnahme und Durchsuchung nach den Vorschriften erläutert (vgl.

[557] M-G/*Schmitt*, StPO, § 147 Rn. 25; *Wohlers*, SK-StPO, § 147 Rn. 96; auch *Willnow*, KK-StPO, § 147 Rn. 15: Eine solche Gefährdung liegt vor, wenn zu befürchten ist, dass weiter sicherzustellende Beweismittel durch die Akteneinsicht weggeschafft werden (dazu *Wohlers*, a. a. O.).

[558] Bloße zeitliche Verzögerung, die mit der Einsicht verbunden ist, begründet keine Gefährdung des Untersuchungszweckes (*Wohlers*, SK-StPO, § 147 Rn. 96).

[559] *LG Regensburg*, StV 2004, 369; M-G/*Schmitt*, StPO, § 147 Rn. 25; *Wohlers*, SK-StPO, § 147 Rn. 97.

[560] *LG Regensburg*, StV 2004, 369; *Wohlers*, SK-StPO, § 147 Rn. 97; a. A. M-G/*Schmitt*, StPO, § 147 Rn. 25: Bei alledem wird eine konkrete Gefahr nicht vorausgesetzt.

unten II.) Daran anschließend werden die Diskussionen in Südkorea dargelegt, die mit den Streitpunkten in obigen Abschnitten B. und C. verglichen werden können. Zuerst ist es wegen der unklaren Bestimmung von K-StPO umstritten, ob elektronische Daten beschlagnahmt und durchsucht werden dürfen (vgl. unten III. 1.). Danach wird infrage gestellt, ob die Auslegung, dass die §§ 106 ff. i. V. m. § 219 K-StPO – zusammen mit § 9b K-KGSG – auch heimliche Maßnahmen rechtfertigen, gültig ist (vgl. unten III. 2.). In Südkorea werden derzeit die Daten, die auf einem Server gespeichert sind, der für TK-Dienste wie E-Mail-Verkehr, Messenger-Nachrichten, SNS-Nachrichten, Cloud-Computing usw. bereitgestellt wird, nach den allgemeinen Vorschriften ohne Wissen des von Daten Betroffenen beschlagnahmt und durchsucht, und der § 9b K-KGSG sieht die nachträgliche Benachrichtigung des Betroffenen in diesem Fall vor. Es ist zu prüfen, ob eine solche Auslegung und Anwendung angemessen ist. Darüber hinaus erließ der *K-OGH* im Jahr 2017 ein umstrittenes Urteil bezüglich der Zulässigkeit von Netzwerkdurchsuchung, insb. grenzüberschreitender Durchsuchung (vgl. unten III. 3.). In K-StPO gibt es nun keine Bestimmungen wie § 110 Abs. 3 StPO und Südkorea ist noch kein Mitgliedstaat des CKÜ. Schließlich stellt sich die Frage, mit welchen verfahrensrechtlichen Mitteln bei der umfassenden Beschlagnahme und Durchsuchung elektronischer Daten ihr Umfang verhältnismäßig beschränkt und wirksam kontrolliert werden kann. Um nur verfahrensrelevante Daten auszuwählen und endgültig zu beschlagnahmen und um verfahrensirrelevante Daten zu löschen oder zu vernichten, nimmt die Ermittlungsbehörde in der Praxis i. d. R. EDV-Anlagen oder Datenträger in ihre Diensträume mit oder sie kopiert oder übertragt sämtliche darauf gespeicherten Daten auf ihren Datenträger (sog. „Kopieren und Mitnehmen sämtlicher Daten“).[561] Hier wird infrage gestellt, unter welchen Voraussetzungen eine solche Beschlagnahme- und Durchsuchungsmethode zulässig ist und inwieweit der Beschuldigte oder sein Verteidiger am Durchführungsprozess teilnehmen kann (vgl. unten III. 4.).

Andererseits wurde das Prinzip des Ausschlusses illegal erlangter Beweise durch die K-StPO-Reform 2007 in das koreanische Strafverfahren eingeführt, und der *K-OGH* legte in seiner Entscheidung vom November 2007 die Kriterien für das Verwertungsverbot im Einzelfall fest (vgl. Kapitel 2, C. III.). Infolgedessen hat die Einhaltung des Verfahrens durch die Ermittlungsbehörde in der Praxis der Beschlagnahme und Durchsuchung einen großen Einfluss auf die Beweisverwertung und ist praktisch wichtig geworden.

[561] Dies entspricht der vorläufigen Sicherstellung nach § 110 Abs. 1, 2 StPO (vgl. oben C. III. 3.). In der Praxis wird das Speichermedium selbst selten mitgenommen, und zumeist werden nur Daten durch Kopieren gesichert (*Sungsoo Ahn*, KoK-StPO, § 106, 564).

II. Beschlagnahme und Durchsuchung im Ermittlungsverfahren: §§ 106 ff. i. V. m. §§ 215 ff. K-StPO

1. Vorbemerkung

§§ 215 – 220 K-StPO sind die Ermächtigungsgrundlage für die Beschlagnahme und Durchsuchung zur Beweissicherung im Ermittlungsverfahren, aber aufgrund der einzigartigen Systemstruktur der K-StPO gelten §§ 106 ff. K-StPO, die vonseiten des Gerichts vorgesehen sind, durch § 219 K-StPO umfassend dafür (vgl. siehe Kapitel 1, Fn. 33).

§ 215 K-StPO sieht allgemeine Voraussetzungen für die Beschlagnahme und Durchsuchung vor: Die Ermittlungsbehörde darf bei Vorliegen des Tatverdachts aufgrund des richterlichen schriftlichen Anordnungsbeschlusses nur Gegenstände beschlagnahmen und durchsuchen, die für die Untersuchung erforderlich sind und die mit dem Fall in Verbindung stehen können. §§ 216 – 218 K-StPO regeln eine Beschlagnahme und Durchsuchung ohne richterliche Anordnung. Dies setzt das aktuelle Vorliegen einer vorläufigen Festnahme oder Verhaftung oder der Tatbegehung, weggeworfene oder verlorene Sachen oder freiwillige Vorlegung voraus (vgl. unten 3. d)). Darin unterscheidet sich die Eilkompetenz der K-StPO von derjenigen der StPO. § 218a K-StPO regelt (Quasi-)Rückgabe der beschlagnahmten Gegenstände im Ermittlungsverfahren (vgl. unten 3. e)). § 220 K-StPO sieht vor, dass § 123 Abs. 2 K-StPO (Anwesenheit von Durchsuchungszeugen) und § 125 K-StPO (Beschränkung der Durchsuchung von Räumen zur Nachtzeit) nicht bei der Beschlagnahme und Durchsuchung ohne richterliche Anordnung nach § 216 K-StPO gelten.

2. Voraussetzungen und Gegenstände: §§ 106 – 112 und 215 K-StPO

(1) Die Ermittlungsbehörde darf zur Ermittlung bei Bedarf aufgrund des richterlichen schriftlichen Beschlusses die zu beschlagnahmenden oder einzuziehenden Gegenstände beschlagnahmen, die mit dem Fall in Zusammenhang stehen können (§ 106 Abs. 1 i. V. m. §§ 215, 219 K-StPO), und Körper, Sachen, Wohnräume und sonstige Orte des Verdächtigen oder anderer Personen durchsuchen (§ 109 i. V. m. §§ 215, 219 K-StPO).[562] Aus diesen Vorschriften werden die materiellen Anforderungen der Beschlagnahme und Durchsuchung abgeleitet, d. h. Anfangsverdacht, Verhältnismäßigkeit, Erforderlichkeit und Relevanz.[563] Die Relevanz bedeutet insb. Wahrscheinlichkeit, dass die Gegenstände als Beweismittel von Bedeutung sein

[562] Die Durchsuchung bei Nichtverdächtigen ist jedoch nur dann zulässig, wenn Tatsachen vorliegen, aus denen zu schließen ist, dass sich die zu beschlagnahmenden Gegenstände dort befinden (§ 109 Abs. 2 K-StPO).

[563] Vgl. *Lee/Cho*, K-StPO, § 20 Rn. 2 ff. Unter der Relevanz versteht man, dass das verfassungsrechtliche Verhältnismäßigkeitsprinzip in der Beschlagnahme und Durchsuchung umgesetzt ist (*Gi-du Oh*, Juris, Nr. 28, 2014, 199, 201 und 206 f.), und daher wird sie ohne ausdrückliche Vorschrift anerkannt (*K-OGHE* vom 26. 5. 2011 – 2009 Mo 1190; *Joo-Won Rhee*, K-StPO, 146).

können,[564] und bei der Beschlagnahme und Durchsuchung von (elektronischen) Daten dient sie dazu, die Maßnahme nur auf Daten zu beschränken, die für den Fall und den Beschuldigten relevant sein können.[565] *K-OGH* versteht ihren Begriff wie folgt:

> „Wenn Beweise, die nicht für den die richterliche Anordnung verursachten Tatverdacht relevant sind, beschlagnahmt werden, können sie grundsätzlich nicht als Beweismittel zur Verurteilung verwendet werden. … Die Straftaten, die für den Verdacht in einem Anordnungsbeschluss der Beschlagnahme und Durchsuchung relevant sind, sind Straftaten, die objektiv mit den dort angegebenen Tatsachen und persönlich zwischen dem von (Ermittlungs-)Maßnahme Betroffenen und dem Beschuldigten zusammenhängen. Objektiver Zusammenhang ist zunächst natürlich für die im Beschluss angegebenen Tatsachen selbst anzunehmen, und außerdem nicht nur für den Tatverdacht anzunehmen, dessen grundlegende Tatsachen mit ihnen identisch sind, sondern auch dann, wenn sie in unmittelbaren Zusammenhang mit ihnen stehen, und auch dann, wenn sie als Indizien verwendet werden können, um das Motiv und Geschehen, die Mittel und Methoden, die Zeit und den Ort der Tat zu beweisen. Dieser Zusammenhang wird nur dann anerkannt, wenn eine konkrete und individuelle Beziehung besteht, indem der Inhalt der im Beschluss angegebenen Tatsachen sowie das Ziel und Geschehen der Untersuchung etc. pauschal in Rechnung gestellt werden, aber nicht nur deshalb, weil es sich um eine gleiche oder ähnliche Art des Verdachts handelt. Und persönlicher Zusammenhang wird dann anerkannt, wenn eine bestimmte Beziehung zwischen dem von der Maßnahme Betroffenen, der im Beschluss genannt ist, und dem Beschuldigten besteht, wie z. B. Mittäterschaft, mittelbare Täterschaft, Anstiftung etc.“[566] *(Übersetzung vom Autor)*

Zu beschlagnahmen sind nur die Gegenstände, die mit dem Tatverdacht, der der Beschlagnahme und Durchsuchung zugrunde liegt und im richterlichen Anordnungsbeschluss angegeben ist, „im Zusammenhang“ stehen, nämlich „verfahrensrelevante“ Daten (Beweise). Andere Gegenstände, nämliche „verfahrensirrelevante“ Daten, sind durch einen zügigen weiteren Beschluss zu beschlagnahmen, wenn sie auf die Verübung einer anderen Straftat hindeuten, und ansonsten ist diese Beschlagnahme rechtswidrig und die beschlagnahmten Daten dürfen nach dem Ausschlussprinzip nicht als Beweismittel verwendet werden.[567] Die Beschränkung des Umfangs der Beschlagnahme und Durchsuchung durch den Zusammenhang bzw. die Relevanz verhindert eine Untersuchung, die in gleicher Weise wie Rasterfahndung durchgeführt wird, und u. a. der persönliche Zusammenhang trägt zur Verwirkli-

---

[564] *Lee/Cho*, K-StPO, § 20 Rn. 5.

[565] *Seungsoo Chun*, CRCL, Nr. 49, 2015, 37, 42; vgl. *K-OGHE (Plenum)* vom 16. 7. 2015 – 2011 Mo 1839: „*Bei der Beschlagnahme und Durchsuchung elektronischer Daten sind verfahrensrechtliche Vorkehrungen von Bedeutung, um Suchen, Kopieren und Drucken ohne Rücksicht auf die Relevanz für den Verdacht zu verhindern.*“ (Übersetzung vom Autor).

[566] *K-OGHE* vom 5. 12. 2017 – 2017 Do 13458; *ders.* vom 17. 10. 2019 – 2019 Do 6775; vgl. *ders.* vom 25. 1. 2017 – 2016 Do 13489.

[567] *K-OGHE* vom 26. 5. 2011 – 2009 Mo 1190; *ders. (Plenum)* vom 16. 7. 2015 – 2011 Mo 1839; *ders.* vom 10. 3. 2016 – 2013 Do 11233 m. w. N.; *Joo-Won Rhee*, K-StPO, 146.

chung des Schuldprinzips bei.[568] Aber der *K-OGH* versteht diesen Zusammenhang durch dessen objektiven Aspekt sehr breit. Daher können fast alle Daten, die bei der Beschlagnahme oder Durchsuchung sowohl beim Beschuldigten als auch beim Tatbeteiligten gefunden wurden, i. d. R. zu den Indizien gehören.[569] Jedenfalls ergibt sich jedoch aus der obigen Entscheidung klar, dass ein „anderer Verdacht bezüglich des Tatbeteiligten" in keinem Zusammenhang mit der Untersuchung steht, wenn er keine objektive Beziehung zu den Tatsachen hat.[570] Die Relevanz bzw. der Zusammenhang hat viel mit den Zufallsfunden zu tun, und es geht insb. um die Beschlagnahme und Durchsuchung elektronischer Daten (vgl. unten III. 4.).

(2) Grundsätzlich sind die Gegenstände der Beschlagnahme Sachen (§ 106 Abs. 1 i. V. m. § 219 K-StPO). Wenn es sich jedoch um Festplatten von Computern oder andere Datenträger handelt, muss die Beschlagnahme in einer Weise durchgeführt werden, dass die dort gespeicherten Daten „in einem bestimmten Umfang gedruckt oder kopiert" werden, aber wenn dies nicht möglich ist oder es wesentlich erschwert wäre, das Ziel der Beschlagnahme zu erreichen, sind die Datenträger selbst zu beschlagnahmen (§ 106 Abs. 3 i. V. m. § 219 K-StPO). Erhält eine Ermittlungsbehörde nach § 106 Abs. 3 K-StPO von unverdächtigen Dritten die zu beschlagnahmenden Daten, so hat sie den von Daten Betroffenen i. S. d. § 2 Nr. 3 K-DSG unverzüglich zu informieren (§ 106 Abs. 4 i. V. m. § 219 K-StPO).[571] Postsendungen oder TK i. S. d. § 2 Nr. 3 K-KGSG, die die Post oder der TK-Dienstanbieter innehat oder in Verwahrung nimmt, können aufgrund des richterlichen Anordnungsbeschlusses beschlagnahmt werden (§ 107 Abs. 1 i. V. m. § 219 K-StPO), und dies muss den Absendern oder Empfängern mitgeteilt werden (§ 107 Abs. 3 S. 1 i. V. m. § 219 K-StPO), es sei denn, es gibt eine Gefahr, dass die Untersuchung gestört wird (§ 107 Abs. 3 S. 2).

Aus diesen Vorschriften ergibt sich die Beschlagnahmefähigkeit elektronischer Daten selbst nicht klar, und daher ist dies in der Literatur umstritten (vgl. unten III. 1.). Außerdem ist es problematisch, ob §§ 106 ff. i. V. m. § 219 K-StPO als allgemeine Vorschriften eine heimliche Maßnahme rechtfertigen können. Dies ist darauf zurückzuführen, dass § 107 Abs. 3 S. 2 und § 122 S. 2 K-StPO schlechthin vorsehen, dass die Benachrichtigung des Betroffenen im Falle einer Gefahr für einer

[568] *Gi-du Oh*, Juris, Nr. 28, 2014, 199, 206 – 210. Daher argumentiert Richter *Gi-du Oh*, dass dieser persönliche Zusammenhang zuerst beurteilt werden muss, und wenn er abgelehnt wird, muss der objektive Zusammenhang nicht mehr geprüft werden (a. a. O. 212; a. A. *Seungsoo Chun*, CRCL, Nr. 49, 2015, 37, 43).

[569] Zust. *Wankyu Lee*, CRCL, Nr. 48, 2015, 90, 133 f.; vgl. *Joo-Won Rhee*, K-StPO, 155: Ob die Relevanz auch für den bestärkenden/entlastenden Hilfsbeweis und die zur Strafzumessung dienenden Tatsachen anerkannt wird, wird nicht genau aus Rspr. abgeleitet. Andererseits sagt Richter *Gi-du Oh*, dass der persönliche Zusammenhang grundsätzlich dem Beschuldigten und nur ausnahmsweise dem Tatbeteiligten anzuerkennen ist (*Gi-du Oh*, Juris, Nr. 28, 2014, 199, 203 f.).

[570] *Joo-Won Rhee*, K-StPO, 155.

[571] Vgl. § 2 K-DSG [Begriffsbestimmungen] 3. „Der von Daten Betroffene" ist eine Person, die an den verarbeiteten Daten erkannt werden kann.

Störung der Untersuchung oder in dringenden Fällen unterbleiben kann (vgl. unten III. 2.).

(3) Andererseits kann das Gericht die Vorlage der zu beschlagnahmenden Gegenstände dem Eigentümer, Besitzer oder Gewahrsamsinhaber anordnen (§ 106 Abs. 2 K-StPO). Nach § 219 K-StPO gilt diese Vorschrift entsprechend für Ermittlungsverfahren, doch nach h. M. der Literatur wird die Befugnis zur Vorlageanordnung der Ermittlungsbehörde nicht eingeräumt (vgl. § 95 Abs. 1 StPO).[572] Gegenstände, die der Eigentümer etc. freiwillig vorgelegt hat, und verlorene oder weggeworfene Gegenstände können ohne einen richterlichen Beschluss beschlagnahmt werden (§ 108 K-StPO); in § 218 K-StPO befindet sich dieselbe Regelung für die Ermittlungsbehörde. Orte, die als militärische Geheimnisse geschützt sind, und Gegenstände, die zu amtlichen Geheimnissen gehören, können beschlagnahmt oder durchsucht werden, es sei denn, sie beeinträchtigen die überwiegenden Interessen des Staates (§§ 110, 111 i. V. m. § 219 K-StPO). Gegenstände, die Berufsgeheimnisträgern wie Rechtsanwälten, Steuerberatern, Ärzten, Apothekern etc. in dieser Eigenschaft anvertraut worden sind oder von ihnen in Verwahrung genommen sind und zum Geheimnis anderer gehören, dürfen nicht beschlagnahmt werden, wenn die Geheimnisträger dies ablehnen, aber dies gilt nicht für den Fall, wenn die Zustimmung der anderen Person oder ein überwiegendes öffentliches Interesse vorliegt (§ 112 i. V. m. § 219 K-StPO).

3. Verfahren

a) Antrag und Erlass der Anordnung in schriftlicher Form

Die Anordnung der Beschlagnahme- und Durchsuchung wird vom Richter auf Antrag des Staatsanwalts schriftlich erlassen, wobei die Polizei sie nur über den Staatsanwalt beantragen und erhalten kann (§ 215 K-StPO). Der Antrag muss schriftlich gestellt werden mit folgenden Angaben: Name des Beschuldigten (falls unklar, Angelegenheiten, die ihn identifizieren können, wie Eindruck oder Körpergröße), Registrierungsnummer des Bewohners, Beruf, Anschrift, Name der Straftat und eine Zusammenfassung der Tatsachen, die zu beschlagnahmenden Gegenstände, die zu durchsuchenden Orte, Körper oder Sachen und die Gründe für die Beschlagnahme und Durchsuchung sowie Zweck und Gründe, falls diese vor Sonnenaufgang oder nach Sonnenuntergang erforderlich ist, und ggf. Erstellungsperiode der TK bei der Beschlagnahme und Durchsuchung der TK nach § 2 Nr. 3 K-KGSG (§ 107 DVO der K-StPO). Dabei muss der Staatsanwalt auch die Materialien vorlegen, die das Vorliegen des Verdachts, die Erforderlichkeit der Beschlagnahme oder Durchsuchung und den Zusammenhang mit dem Fall vorweisen (§ 108 Abs. 1 DVO der K-StPO). In der K-StPO und ihrer DVO gibt es keine Einschränkungen

[572] *Sungsoo Ahn*, KoK-StPO, § 106, 562; *Joo-Won Rhee*, K-StPO, 144. In § 106 Abs. 2 K-StPO gibt es andererseits keine Rechtsgrundlage für die Festsetzung von Ordnungs- und Zwangsmitteln wie § 70 i. V. m. § 95 Abs. 2 StPO (*Sungsoo Ahn*, a. a. O.).

hinsichtlich des Zeitpunkts des Antrags auf die Anordnung. Der *K-OGH* entschied jedoch, dass im Fall, dass die Beschlagnahme und Durchsuchung nach Erhebung der öffentlichen Klage durch eine Anordnung eines anderen Gerichts als des mit der Sache befassten Gerichts erfolgte, die hier erlangten Beweise nicht als Beweismittel für eine Verurteilung dienen dürfen, weil dies nicht dem legitimen Verfahren folgt.[573]

Im gerichtlichen Beschlagnahme- und Durchsuchungsbeschluss müssen Name des Beschuldigten, Name der Straftat, die zu beschlagnahmenden Gegenstände, die zu durchsuchenden Orte, Körper oder Sachen, Ausstellungsdatum, Gültigkeitsdauer und Angaben, in denen nach Ablauf der Dauer die Vollstreckung der Maßnahme nicht eingeleitet werden darf und der Beschluss zurückgegeben werden muss, und Gründe für die Beschlagnahme und Durchsuchung[574] angegeben werden, und dort muss der Vorsitzende oder ein beauftragter Richter unterschreiben; und ggf. auch „Erstellungsperiode der TK“[575] bei der Beschlagnahme und Durchsuchung der TK nach § 2 Nr. 3 K-KGSG (§ 114 Abs. 1 i. V. m. § 219 K-StPO, § 58 DVO der K-StPO). Der Kern des Richtervorbehalts für die Beschlagnahme und Durchsuchung liegt nicht nur in einer Kontrolle der Ermittlungsbehörde durch eine unabhängige und neutrale Instanz, sondern auch im „Verbot einer Generalermächtigung“.[576] Daher müssen der Betroffene bzw. die Orte, an den sich die Beschlagnahme und Durchsuchung richtet, unbedingt und die Gegenstände – auch wenn es abstrakt ist – in gewissem Maß bestimmt werden.[577] Darüber hinaus müssen die Wortlaute im Beschluss, die zu beschlagnahmenden Gegenstände zu bestimmen, streng ausgelegt werden und sie dürfen nicht zulasten des von Maßnahme Betroffenen extensiv oder

[573] *K-OGHE* vom 28. 4. 2011 – 2009 Do 10412: In Anbetracht der Verfahrensstruktur der geltenden K-StPO, die auf den Grundsatz des rechtsstaatlichen Verfahrens, das Recht auf Anrufung der Gerichte, den Schwerpunkt der Hauptverhandlung, das gegnerische System und das Unmittelbarkeitsprinzip ausgerichtet ist, und des Systems, Wortlauts und Inhalts der einschlägigen Vorschriften ist die Beschlagnahme und Durchsuchung gemäß § 215 K-StPO nach Erhebung der öffentlichen Klage nicht gestattet. Im Strafverfahren nach der K-StPO muss die Beweissicherung nach Erhebung der öffentlichen Klage vor dem ersten Termin zur Hauptverhandlung aufgrund des Beweissicherungsverfahrens nach § 184 K-StPO und danach auf Anordnung des mit der Sache befassten Gerichts erfolgen (*Son*/*Kim*, Durchsuchungs- und Beschlagnahmeverfahren, 31).

[574] Die Gründe für die Beschlagnahme und Durchsuchung bedeutet ihre Erforderlichkeit, die Beziehung zum Fall, die Wahrscheinlichkeit der Existenz der zu beschlagnahmenden Gegenstände etc. (*Son*/*Kim*, Durchsuchungs- und Beschlagnahmeverfahren, 30).

[575] Dieser Wortlaut wurde durch die K-StPO-Änderung 2011 eingefügt. Zuvor war in 80 – 90 % der richterlichen Anordnungsbeschlüsse zur Beschlagnahme und Durchsuchung von E-Mails diese Erstellungsperiode nicht enthalten, sodass in einigen Fällen die gesamten E-Mails für 10 oder 7 Jahre beschlagnahmt wurden (*Kuk Cho*, KJC, 22-1, 2010, 99, 118 f.).

[576] *Joo-Won Rhee*, K-StPO, 144; *Lee*/*Cho*, K-StPO, § 20 Rn. 13.

[577] *Son*/*Kim*, Durchsuchungs- und Beschlagnahmeverfahren, 29; *Joo-Won Rhee*, K-StPO, 150 f. Dass die Gegenstände der Beschlagnahme oder Durchsuchung im Beschluss hilfsweise angegeben werden, ist nicht gestattet (*Lee*/*Cho*, K-StPO, § 20 Rn. 13 [Fn. 2]). Der Inhalt, der im richterlichen Beschluss anzugeben ist, ist ähnlich wie in Deutschland (vgl. oben C. II. 1. c)).

analog ausgelegt werden.[578] Die Gültigkeitsdauer des Beschlagnahme- und Durchsuchungsbeschlusses beträgt 7 Tage, sofern ein Richter nichts anderes bestimmt (§ 178 DVO der K-StPO). Wird die Beschlagnahme und Durchsuchung innerhalb dieser Frist durchgeführt oder beendet, ist der Beschluss nicht mehr gültig. Da dieselben Orte oder Sachen nicht mit demselben Beschluss mehrmals durchsucht werden können, muss ein neuer Beschluss vom Gericht eingeholt werden, wenn dies erforderlich ist.[579] Er tritt außer Kraft, wenn seine Durchführung beendet wird, auch wenn er unvollständig ist, es sei denn, er wird vorübergehend ausgesetzt.[580]

b) Durchführung der Anordnung

(1) Der Anordnungsbeschluss zu Beschlagnahme und Durchsuchung wird unter Sachleitung der StA von ihren Ermittlern oder Polizeibeamten durchgeführt (§ 115 Abs. 1 i. V. m. § 219 K-StPO), und er muss „dem von Maßnahmen Betroffenen" unbedingt vorgezeigt werden (§ 118 i. V. m. § 219 K-StPO).[581] Dies verhindert eine ohne Beschluss durchgeführte Beschlagnahme und Durchsuchung, sodass diese nur für die im Beschluss aufgeführten Orte, Körper oder Sachen vollstreckt werden kann, und außerdem gewährleistet er dem Betroffenen die praktische Möglichkeit, eine Beschwerde über die Art und Weise der Durchführung zu richten.[582] Daher muss die Ermittlungsbehörde vor der Durchführung der Maßnahme im Voraus den Beschluss vorlegen, und selbst in dringenden Fällen darf sie die Maßnahme nicht ohne seine Mitführung vollstrecken.[583] Aber da dies eine Situation voraussetzt, in der das Vorzeigen des Beschlusses realistisch möglich ist, ist die Beschlagnahme oder Durchsuchung ohne dieses Vorzeigen etwa dann nicht illegal, wenn der von der Maßnahme Betroffene nicht vor Ort ist oder dort nicht gefunden werden kann.[584] Der von der Maßnahme Betroffene, dem der Beschluss vorzulegen ist, ist „die Person, die

[578] *K-OGHE* vom 12. 3. 2009 – 2008 Do 763. Der Auffindung unerwarteter Beweismittel oder eines neuen Tatverdachts muss durch eine neue richterliche Anordnung dafür begegnet werden (vgl. unten III. 4. b)), anderenfalls besteht die Gefahr, dass jede Anordnung zur Generalanordnung wird, die eine umfassende Beschlagnahme und Durchsuchung ermöglicht (*Joo-Won Rhee*, K-StPO, 160).

[579] *K-OGHE* vom 1. 12. 1999 – 99 Mo 161; *Lee*/*Cho*, K-StPO, § 20 Rn. 13.

[580] *Joo-Won Rhee*, K-StPO, 161.

[581] Hierbei muss das Original grundsätzlich vorgezeigt werden (*Lee*/*Cho*, K-StPO, § 20 Rn. 15). Wenn bei Beschlagnahme von E-Mails die Ermittlungsbehörde nur eine Kopie des Anordnungsbeschlusses per Fax gesendet und sein Original nicht vor Ort vorgezeigt und auch das Beschlagnahmeverzeichnis nicht erstellt und ausgehändigt hat, so haben die beschlagnahmten E-Mails als illegal erlangte Beweise keine Beweisfähigkeit (*K-OGHE* vom 7. 9. 2017 – 2015 Do 10648). Was die Vorzeigung des Beschlusses betrifft, ist diese Auslegung jedoch zu streng und belastet die Ermittlungsbehörden übermäßig. Insb. gibt es in § 118 K-StPO nicht das Wort „Original". In der Praxis ist es vielmehr i. d. R. angebracht, eine Abschrift vor Ort oder per E-Mail auszuhändigen.

[582] *K-OGHE* vom 21. 9. 2017 – 2015 Do 12400.

[583] *Joo-Won Rhee*, K-StPO, 152.

[584] *K-OGHE (Plenum)* vom 22. 1. 2015 – 2014 Do 10978.

die Orte oder Sachen der Durchsuchung besitzt, innehabt oder verwahrt“,[585] und dazu gehört der Betroffene von auf dem Server Dritter vorhandenen Daten nicht.[586] Daher, wenn die Ermittlungsbehörde die Computer oder Datenträger und die darauf gespeicherten Daten in dem Wohn- oder Büroraum des von der Maßnahme Betroffenen durchsucht und beschlagnahmt, wird ihm der Beschluss i. d. R. vorgezeigt. Aber wenn sie E-Mails oder Messenger-Nachrichten, die auf dem Server des TK-Dienstanbieters gespeichert sind, von diesem erhält, wird er nur diesem vorgezeigt, nicht dem von Daten Betroffenen. Der Anordnungsbeschluss muss so vorgezeigt werden, dass alle darin angegebenen Inhalte wohl zu verstehen sind, und es ist illegal, dass er so präsentiert wird, dass nur seine Deckseite und der Tatverdacht vorgezeigt werden und der Rest nicht bestätigt werden kann.[587]

(2) Während der Durchführung der Beschlagnahme- und Durchsuchungsanordnung kann die Ermittlungsbehörde anderen Personen den Zutritt untersagen, eine bereits existierende Person vertreiben oder sie bewachen lassen (§ 119 i. V. m. § 219 K-StPO).[588] Bei der Durchführung kann sie notwendige Maßnahmen ergreifen, wie das Öffnen des Schlosses etc. (§ 120 i. V. m. § 219 K-StPO). Dieses wird hier als Beispiel verstanden, und die Ermittlungsbehörde kann erforderliche und angemessene Maßnahmen in einem Mindestmaß ergreifen, um den Zweck der Beschlagnahme und Durchsuchung zu erreichen.[589] Diesbezüglich ist umstritten, ob Netzwerkdurchsuchung und weiter grenzüberschreitende Durchsuchung nach § 120 K-StPO erlaubt werden können, weil es in K-StPO derzeit keine Vorschrift wie § 110 Abs. 3 StPO gibt (vgl. unten III. 3.).

An der Durchführung der Beschlagnahme und Durchsuchung können der „Beschuldigte und sein Verteidiger“ teilnehmen (§ 121 i. V. m. § 219 K-StPO). Dazu sind das Datum und der Ort der Durchführung ihnen im Voraus bekanntzumachen (§ 122 S. 1 i. V. m. § 219 K-StPO), aber dies gilt nicht in dringenden Fällen oder in dem Fall, dass sie die Absicht der Abwesenheit klar zum Ausdruck bringen (S. 2). Die Teilnahme nach dem § 121 K-StPO dient der Gewährleistung der Fairness des Verfahrens und dem Schutz der Interessen des Beschuldigten.[590] Der „dringende Fall“ gemäß § 122 S. 2 K-StPO bezieht sich auf einen Fall, in dem die vorherige Mitteilung die Vernichtung und Beschädigung der Beweismittel verursachen kann und somit das

[585] Da der Anordnungsbeschluss allen von der Maßnahme Betroffenen einzeln vorzulegen ist, muss er dem Verwalter des Ortes und dem Inhaber der Gegenstände jeweils vorgelegt werden (*K-OGHE* vom 12. 3. 2009 – 2008 Do 763; *ders.* vom 21. 9. 2017 – 2015 Do 12400).

[586] *K-VerfGE* 24-2, 467, 472.

[587] *K-OGHE* vom 21. 9. 2017 – 2015 Do 12400.

[588] Bei Unterbleiben der Durchführung kann die Ermittlungsbehörde, falls erforderlich, den Durchsuchungsort bis zu ihrer Beendigung schließen oder bewachen lassen (§ 127 i. V. m. § 219 K-StPO).

[589] *Joo-Won Rhee*, K-StPO, 153.

[590] *Lee/Cho*, K-StPO, § 20 Rn. 16; *Joo-Won Rhee*, K-StPO, 153; *Wankyu Lee*, CRCL, Nr. 48, 2015, 90, 106.

Erreichen des Zwecks der Beschlagnahme oder Durchsuchung gefährdet.[591] Bei der Beschlagnahme und Durchsuchung personenbezogener Daten stellt der von der Maßnahme Betroffene i. d. R. den Beschuldigten dar und daher ist er der Inhaber des Teilnahmerechts und der Adressat der Benachrichtigung nach §§ 121, 122 S. 1 K-StPO. Auch bei der Beschlagnahme und Durchsuchung der Daten, die auf Servern Dritter gespeichert sind, können der Beschuldigte, der i. d. R. zwar nicht der von der Maßnahme Betroffene, aber der von Daten Betroffene ist, und sein Verteidiger aufgrund der Vorschriften benachrichtigt werden und daran teilnehmen.[592] In diesem Fall erhält die Ermittlungsbehörde jedoch eine große Menge von Daten wie E-Mails, Messenger-Nachrichten etc. vom Diensteanbieter aufgrund des § 122 S. 2 K-StPO (in dringenden Fällen) ohne Benachrichtigung des Beschuldigten und danach sie beschlagnahmt die durch Suche und Durchsicht ausgewählten Daten. Diesbezüglich stellen sich im Schrifttum zwei Fragen: einerseits ob die Beschlagnahme und Durchsuchung, die in einer Weise durchgeführt wird, dass E-Mails etc. ohne Wissen des von Daten Betroffenen vom Dienstanbieter umfassend an die Ermittlungsbehörde weitergeleitet werden, aufgrund der allgemeinen Vorschriften, die weniger streng als §§ 5 ff. K-KGSG sind, gerechtfertigt werden kann, weil eine solche Durchführung in der Tat der TKÜ entspricht (vgl. unten III. 2.), andererseits inwieweit beim Kopieren und Mitnehmen sämtlicher Daten und ihrer Durchsicht das Teilnahmerecht des Beschuldigten und seines Verteidigers zulässig ist (vgl. unten III. 4.).

Die Durchführung der Beschlagnahme und Durchsuchung in öffentlichen Ämtern oder militärischen Luftfahrzeugen, Schiffen oder Zügen sind der vorgesetzten Dienststelle zur Teilnahme mitzuteilen (§ 123 Abs. 1 i. V. m. § 219 K-StPO). An der Durchführung in sonstigen Wohnräumen, Gebäuden, Luftfahrzeugen, Schiffen oder Zügen muss ihr Inhaber teilnehmen können, und ansonsten muss ein Gemeindebeamter einbezogen werden (§ 123 Abs. 2, 3 i. V. m. § 219 K-StPO). An der Durchsuchung des weiblichen Körpers muss eine erwachsenen Frau teilnehmen (§ 124 i. V. m. § 219 K-StPO). Wenn der Anordnungsbeschluss der Beschlagnahme und Durchsuchung nicht besagt, dass ihre Durchführung auch vor Sonnenaufgang oder nach Sonnenuntergang zulässig ist, ist es nicht gestattet, Wohnräumen etc. dafür zu betreten (§ 125 i. V. m. § 219 K-StPO). Diese Beschränkung gilt jedoch nicht für Orte, die zu sittenwidrigen Handlungen wie Glücksspiel dienen, oder Orte, die zur Nachtzeit öffentlich zugänglich sind, wie Gasthäuser und Restaurants (§ 126 i. V. m. § 219 K-StPO).

---

[591] *K-OGHE* vom 11. 10. 2012 – 2012 Do 7455; auch *K-VerfGE* 24-2, 467, 474.

[592] *Wankyu Lee*, CRCL, Nr. 48, 2015, 90, 107. Staatsanwalt *Wankyu Lee* macht jedoch geltend, dass es wegen der Heimlichkeit der Ermittlung rechtlich problematisch sei, dass § 121 K-StPO durch § 219 K-StPO entsprechend auf das Ermittlungsverfahren angewendet werde (a. a. O. 107 f.).

c) Verfahren nach der Durchführung

Nach Beendigung der Beschlagnahme und Durchsuchung ist ein Protokoll zu erstellen, in dem Art, äußere Merkmale und Menge der in Beschlag genommenen Gegenstände angegeben sind (§ 49 Abs. 1, 3 K-StPO). Dem von der Maßnahme Betroffenen wie Eigentümer, Besitzer oder Gewahrsamsinhaber etc. ist außerdem ein Beschlagnahmeverzeichnis (§ 129 i. V. m. § 219 K-StPO) und, falls die zu beschlagnahmenden oder einzuziehenden Gegenstände nicht gefunden werden, eine Bescheinigung hierüber (§ 128 i. V. m. § 219 K-StPO) auszuhändigen. Das Verzeichnis oder die Bescheinigung ist unabhängig vom Verlangen des Betroffenen vom Beamten, der die Beschlagnahme und Durchsuchung durchgeführt hat, aufzunehmen und auszuhändigen[593] und ist mit seiner Unterschrift und mit dem Datum zu versehen (§ 57 Abs. 1 K-StPO). Dies sind die grundlegendsten Materialien, um die (Quasi-) Rückgabe der beschlagnahmten Gegenstände zu beantragen oder eine Beschwerde über die Maßnahme einzulegen, und daher sind sie grundsätzlich sofort nach der Beschlagnahme vor Ort aufzunehmen und auszuhändigen.[594] Beim Kopieren und Mitnehmen sämtlicher Daten sollte dies nicht nur bei dieser Mitnahme, sondern auch nach der endgültigen Beschlagnahme der ausgewählten Daten erfolgen. Auch bei der Beschlagnahme und Durchsuchung elektronischer Daten muss das Beschlagnahmeverzeichnis mit den Einzelheiten der Dateien ausgehändigt werden, wobei dies in einem Ausdruck oder einer Kopie der Datei oder per E-Mail erfolgen kann.[595]

d) Beschlagnahme und Durchsuchung ohne richterliche Anordnung: §§ 216–218, 220 K-StPO

Beim Ermittlungsverfahren in Südkorea ist die Beschlagnahme und Durchsuchung ohne vorherige Anordnung des Richters nur in den folgenden fünf Fällen zulässig.[596]

---

[593] *Sungsoo Ahn*, KoK-StPO, § 128, 633 und § 129, 634.

[594] *K-OGHE* vom 12. 3. 2009 – 2008 Do 763: Daher ist es illegal, dass das Beschlagnahmeverzeichnis, das das Erstellungsdatum nicht enthält und dessen Inhalt teilweise nicht mit den Tatsachen übereinstimmt, fünf Monate nach dem Ende der Beschlagnahme und Durchsuchung ausgehändigt wurde.

[595] *K-OGHE* vom 8. 2. 2018 – 2017 Do 13263.

[596] In Südkorea ist der Ausschluss des Richtervorbehalts bei der Beschlagnahme und Durchsuchung sehr begrenzt. Diesbezüglich sieht K-Verf Folgendes: Festnahme und Verhaftung sowie Beschlagnahme und Durchsuchung sind nur gesetzlich zulässig (Art. 12 Abs. 1 K-Verf), und bei ihrer Durchführung muss der Anordnungsbeschluss, der nach dem legitimen Verfahren auf Antrag der StA durch Richter erlassen wird, außer im Fall der Festnahme im Eilfall oder auf frischer Tat vorgelegt werden (Art. 12 Abs. 3 K-Verf). Bei der Beschlagnahme und Durchsuchung von Wohnraum muss der Anordnungsbeschluss, der auf Antrag der StA durch Richter erlassen wird, vorgelegt werden (Art. 16 S. 2 K-Verf). Aus diesen Vorschriften ergibt sich, dass der Ausschluss vom Richtervorbehalt bei der Beschlagnahme und Durchsuchung grundsätzlich verboten ist und dass die ausnahmsweise Zulassung nur in dringenden Fällen nach §§ 216–217 K-StPO möglich ist (*Joo-Won Rhee*, K-StPO, 178). Außerdem ist es

(1) Erstens, wenn die Ermittlungsbehörde – aufgrund der Festnahme nach richterlicher Anordnung (§ 200a), der Festnahme im Eilfall (§ 200b), der Festnahme auf frischer Tat (§ 212) oder der Verhaftung nach richterlicher Anordnung (§ 201 K-StPO) – einen Verdächtigen vorläufig festnimmt oder verhaftet,[597] darf sie „ohne richterliche Anordnung (der Beschlagnahme und Durchsuchung)" Wohnräume, Gebäude, Luftfahrzeuge, Schiffe oder Züge von anderen durchsuchen, wenn dies notwendig ist, „um den Verdächtigen zu finden"; bei der Festnahme oder Verhaftung nach richterlicher Anordnung nach § 200a oder § 201 K-StPO ist dies jedoch auf „dringende Fälle" beschränkt, in denen es schwierig ist, einen Durchsuchungsbeschluss im Voraus auszustellen (§ 216 Abs. 1 Nr. 1 K-StPO). Die letzte Kautel wurde am 31. Dezember 2019 nach dem Beschluss des *K-VerfG*[598] eingefügt (Gesetz Nr. 16850). Doch der § 216 Abs. 1 Nr. 1 K-StPO wurde schon vorher nach h. M. der Literatur dahingehend ausgelegt, dass er nur dann anwendbar ist, wenn der Beschuldigte mit ziemlicher Sicherheit vor Ort ist (Wahrscheinlichkeit) und es dringende Umstände gibt, die es schwierig machen, einen Durchsuchungsanordnung im Voraus auszustellen (Dringlichkeit), weil er einen Ausschluss vom Richtervorbehalt darstellt, was nicht in der *K-Verf* festgelegt ist.[599] Da diese Eil-Durchsuchung nur dazu dienen kann, den Verdächtigen zu finden, ist die Durchsuchung nach der Vorschrift unzulässig, wenn er bereits festgenommen oder verhaftet wurde.[600] Für diese Durchsuchung ist keine nachträgliche Genehmigung des Richters erforderlich.[601]

Zweitens, wenn die Ermittlungsbehörde einen Verdächtigen vorläufig festnimmt oder verhaftet, darf sie „ohne richterliche Anordnung" „vor Ort" durchsuchen und beschlagnahmen (§ 216 Abs. 1 Nr. 2, Abs. 2 K-StPO). Nach h. M. ist diese Beschlagnahme und Durchsuchung nur als „dringliche Maßnahme" zulässig, um die Sicherheit des Ermittlers zu gewährleisten, der den Verdächtigen ergreift, oder um die Verschleierung oder Vernichtung von Beweismitteln vor Ort zu verhindern, und daher sollte sie in großer zeitlicher und örtlicher Nähe mit der Festnahme oder

---

auch in diesem Fall i. d. R. erforderlich, unverzüglich die nachträgliche Genehmigung des Richters einzuholen. Daher ist diese Ausnahme nicht der Ausschluss der richterlichen Prüfung selbst, sondern der Ausschluss der vorherigen Prüfung (*Joo-Won Rhee*, a. a. O.).

[597] Bezüglich der körperlichen Unversehrtheit im Ermittlungsverfahren schreibt die K-StPO die Verhaftung (§ 201 K-StPO) und die Festnahme vor, und diese ist in die Festnahme nach richterlicher Anordnung (§ 200a K-StPO) und die ohne richterliche Anordnung, nämlich die Festnahme im Eilfall (§ 200b K-StPO) und die Festnahme auf frischer Tat (§ 212 K-StPO), unterteilt. Die letzten beiden Arten beruhen im Wesentlichen auf Art. 12 Abs. 3 K-Verf (siehe Fn. 596).

[598] *K-VerfGE* vom 26. 4. 2018 – 2015 HunBa 370 etc. (30-1, 563, 572 – 574): Wenn die Durchsuchung ohne richterliche Anordnung gemäß § 216 K-StPO ohne dringende Umstände durchgeführt wird, ist dies nicht mit der Verfassung vereinbar.

[599] *Joo-Won Rhee*, K-StPO, 179.

[600] *Son*/*Kim*, Durchsuchungs- und Beschlagnahmeverfahren, 37; *Lee*/*Cho*, K-StPO, § 20 Rn. 22; *Joo-Won Rhee*, K-StPO, 179.

[601] *Joo-Won Rhee*, K-StPO, 180.

Verhaftung stattfinden.[602] Diese Anforderungen werden streng ausgelegt und eine darüberhinausgehende Beschlagnahme oder Durchsuchung ist nicht gestattet. Zur Anwendung der Vorschrift muss daher die Ergreifung des Verdächtigen zumindest bereits eingeleitet werden und er muss noch vor Ort sein.[603] Falls die Festnahme oder Verhaftung erfolglos war, kann die Beschlagnahme aber nicht aufgrund dieser Vorschrift, sondern nach Erhaltung des Orts nur durch eine gesonderte Anordnung oder nach § 216 Abs. 3 K-StPO erfolgen.[604] Sollten die ohne richterliche Anordnung sichergestellten Gegenstände weiter beschlagnahmt werden, so muss die Ermittlungsbehörde unverzüglich, d. h. innerhalb von 48 Stunden nach der Festnahme oder Verhaftung, eine richterliche Anordnung zur Beschlagnahme und Durchsuchung beantragen (§ 217 Abs. 2 K-StPO), sonst müssen die Gegenstände sofort zurückgegeben werden (Abs. 3). Die Gegenstände, die ohne die nachträgliche Genehmigung durch den Richter nicht zurückgegebenen werden, dürfen nicht als Beweismittel dienen.[605]

Drittens kann die Ermittlungsbehörde im „Notfall", wenn eine richterliche Anordnung während oder unmittelbar nach Begehung der Straftat „an ihrem Ort" nicht erhalten werden kann, „ohne die Anordnung" Wohnräume etc. durchsuchen und beschlagnahmen, wobei sie nachträglich unverzüglich eine richterliche Genehmigung einholen muss (§ 216 Abs. 3 K-StPO). Dies gilt für den Fall, in dem eine Beschlagnahme oder Durchsuchung dringend erforderlich ist, nachdem eine Festnahme auf frischer Tat gescheitert ist, und so werden der Versuch der Ergreifung und die Präsenz des Verdächtigen am Tatort nicht vorausgesetzt, anders als bei der dringenden Beschlagnahme und Durchsuchung am Ort der Festnahme oder Verhaftung nach § 216 Abs. 1 Nr. 2, Abs. 2 K-StPO.[606] Diese Beschlagnahme und Durchsuchung muss zeitlich und örtlich eng mit der „Tatbegehung" verbunden sein und ist nur im Notfall zulässig.[607] Wenn eine dieser Anforderungen nicht erfüllt ist, ist die Beschlagnahme oder Durchsuchung illegal, und dies kann auch mit der nachträglichen Genehmigung des Richters nicht geheilt werden.[608] Es ist aber ein Pro-

[602] *Lee/Cho*, K-StPO, § 20 Rn. 25 f.; *Joo-Won Rhee*, K-StPO, 180 f.: vgl. *K-OGHE* vom 22. 7. 2010 – 2009 Do 14376: Als die Polizei nach der Festnahme des Verdächtigen zu seiner Wohnung, die 20 Meter vom Ort entfernt ist, ging und sie durchsuchte und ein Messer und Papiere beschlagnahmte, wurden diese ohne richterliche Anordnung rechtswidrig beschlagnahmt, und somit dürfen sie nicht als Beweismittel dienen.

[603] *K-OGHE* vom 29. 11. 2017 – 2014 Do 16080; *Joo-Won Rhee*, K-StPO, 181; a. A. *Lee/Cho*, K-StPO, § 20 Rn. 26: Wenn der Verdächtige vor Ort war, ist es egal, ob die Ergreifung schon eingeleitet wurde.

[604] *Joo-Won Rhee*, K-StPO, 182; a. A. *Lee/Cho*, K-StPO, § 20 Rn. 26.

[605] *K-OGHE* vom 14. 5. 2009 – 2008 Do 10914: bei der Festnahme im Eilfall; *ders.* vom 24. 12. 2009 – 2009 Do 11401: bei der Festnahme auf frischer Tat.

[606] *Lee/Cho*, K-StPO, § 20 Rn. 30; *Joo-Won Rhee*, K-StPO, 183 f.

[607] *Joo-Won Rhee*, K-StPO, 184.

[608] *K-OGHE* vom 29. 11. 2017 – 2014 Do 16080.

blem, dass die zeitliche Begrenzung für den Antrag auf die Genehmigung nicht in der Vorschrift enthalten ist.[609]

Viertens darf die Ermittlungsbehörde innerhalb von 24 Stunden nach der „Festnahme im Eilfall" nach § 200b K-StPO „ohne richterliche Anordnung" die Gegenstände, die eine festgenommene Person besitzt, innehat oder verwahrt, beschlagnahmen und durchsuchen, wenn diese „dringend" beschlagnahmt werden müssen (§ 217 Abs. 1 K-StPO). Dies soll verhindern, dass Beweismittel verschleiert oder vernichtet werden, wenn die Tatsache der Festnahme den Tatbeteiligten bekannt gegeben wird, und dazu dienen, sie umgehend sicherzustellen.[610] Diese Beschlagnahme und Durchsuchung setzt eine rechtmäßige Festnahme im Eilfall voraus und ist nur in dem Mindestmaß zulässig, das für die Untersuchung der Straftat, die die Festnahme verursachte, erforderlich ist.[611] Sollten die sichergestellten Gegenstände weiter beschlagnahmt werden, so muss die Ermittlungsbehörde unverzüglich, d. h. innerhalb von 48 Stunden nach der Festnahme, eine richterliche Anordnung zur Beschlagnahme und Durchsuchung beantragen (§ 217 Abs. 2 K-StPO). Ohne die nachträgliche Genehmigung des Richters einzuholen, dürfen die nicht zurückgegebenen Gegenstände nicht als Beweismittel dienen.[612]

Schließlich kann die Ermittlungsbehörde die „verlorenen oder weggeworfenen Gegenstände" und die „freiwillig eingereichten Gegenstände" „ohne richterliche Anordnung" beschlagnahmen (§ 218 K-StPO). Dabei ist eine richterliche Anordnung oder Genehmigung nicht erforderlich,[613] aber dies gehört zur Beschlagnahme als Zwangsmaßnahme, weil die nach dieser Vorschrift gesicherten Gegenstände nicht willkürlich zurückgegeben werden dürfen.[614] Daher muss auch hier das Beschlagnahmeverzeichnis ausgehändigt (vgl. oben c)) und die eingereichten Gegenstände müssen aufgrund der einschlägigen Vorschriften (quasi) zurückgegeben werden (vgl. unten e)).[615] Das Recht zur Einreichung ist auf den Eigentümer, Besitzer oder Gewahrsamsinhaber beschränkt.[616] Da die Gefahr besteht, dass die Ermittlungsbehörde zur Umgehung des Richtervorbehalts anhand ihrer überlegenen Position tatsächlich den Betroffenen dazu zwingt, die Gegenstände freiwillig einzureichen, wird die Freiwilligkeit streng beurteilt und die Beweislast für ihr Vorliegen trägt die StA.[617] Selbst wenn nach einer rechtswidrigen Beschlagnahme eine Zustimmung zur freiwilligen Einreichung erfolgt, können die Gegenstände nicht als Beweismittel ver-

[609] Zust. *Lee/Cho*, K-StPO, § 20 Rn. 30; auch *Joo-Won Rhee*, K-StPO, 185: in 48 Stunden.
[610] *K-OGHE* vom 12. 9. 2017 – 2017 Do 10309.
[611] *K-OGHE* vom 10. 7. 2008 – 2008 Do 2245.
[612] *Lee/Cho*, K-StPO, § 20 Rn. 34.
[613] *K-OGHE* vom 18. 2. 2016 – 2015 Do 13726; *ders.* vom 14. 11. 2019 – 2019 Do 13290.
[614] *Lee/Cho*, K-StPO, § 20 Rn. 35; *Joo-Won Rhee*, K-StPO, 188.
[615] *Sungsoo Ahn*, KoK-StPO, § 129, 634; *Joo-Won Rhee*, K-StPO, 188.
[616] *K-OGHE* vom 28. 1. 2010 – 2009 Do 10092.
[617] *K-OGHE* vom 10. 3. 2016 – 2013 Do 11233; *Joo-Won Rhee*, K-StPO, 190 f.

wendet werden, es sei denn, es gibt besondere Umstände.[618] Dies gilt auch, wenn rechtswidrig beschlagnahmte Gegenstände zuerst an den Betroffenen zurückgegeben und dann freiwillig erneut eingereicht wurden, aber nicht, wenn ein vernünftiger Zweifel an der Freiwilligkeit durch den Nachweis der StA ausgeschlossen werden kann.[619]

(2) Die erste Ausnahme, die eine Durchsuchung von Wohnräumen etc. für die Auffindung des Verdächtigen darstellt, unterscheidet sich der Natur nach von den übrigen Ausnahmen. Die zweite bis vierte Ausnahme setzen eine Festnahme oder Verhaftung oder einen Ort, wo eine frische Tat begangen wurde und eine Dringlichkeit voraus, die bedeutet, dass keine Zeit bleibt, um eine richterliche Anordnung zu erhalten. In diesen Fällen muss die Ermittlungsbehörde unverzüglich, d. h. innerhalb von 48/24 Stunden nach der Vollstreckung, die nachträgliche Genehmigung des Richters einholen. Die Maßnahmen nach § 216 K-StPO unterliegen nicht der Nachtbeschränkung nach § 125 K-StPO (§ 220 K-StPO), sodass sie auch nachts zulässig sind. Diese Ausnahmen bedeuten vor allem nicht den Ausschluss einer richterlichen Überprüfung, da eine solche Beschlagnahme und Durchsuchung unverzüglich nach ihrer Durchführung beim Gericht zur Genehmigung beantragt werden muss. Darüber hinaus beschränkt sich sie natürlich auf Beweise im Zusammenhang mit dem Tatvorwurf der Festnahme und Verhaftung.[620] Wenn eine dieser Anforderungen verletzt wird, ist die Beschlagnahme oder Durchsuchung nach h. M. illegal, was i. d. R. zu einem Verwertungsverbot führt.

e) Verwahrung und (Quasi-)Rückgabe der beschlagnahmten Gegenstände

Die beschlagnahmten Gegenstände werden grundsätzlich an die Ermittlungsbehörde, die sie beschlagnahmt hat, transportiert und von ihr selbst verwahrt, und es müssen Maßnahmen ergriffen werden, um ihren Verlust oder ihre Beschädigung zu verhindern (§ 131 i. V. m. § 219 K-StPO). Wenn dieser Transport oder die Inverwahrnahme jedoch schwierig ist, können sie mit dem Einverständnis des Berechtigten wie Eigentümer etc. ihm anvertraut oder vernichtet werden (§ 130 i. V. m. § 219 K-StPO). In Fällen, in denen die einzuziehenden oder zurückzugebenden Gegenstände Vernichtung, Verlust, Beschädigung oder Abwertung unterliegen oder schwer aufzubewahren sind, kann die Ermittlungsbehörde den Preis für ihren Verkauf einbehalten (§ 132 i. V. m. § 219 K-StPO).

Die Ermittlungsbehörde muss die zur Verwendung als Beweismittel beschlagnahmten Gegenstände auf Verlangen dem Eigentümer, Besitzer oder Gewahrsamsinhaber oder einem Einreicher (quasi) zurückgeben, wenn die Beschlagnahme

[618] *K-OGHE* vom 22. 7. 2010 – 2009 Do 14376.

[619] *K-OGHE* vom 10. 3. 2016 – 2013 Do 11233.

[620] *Joo-Won Rhee*, K-StPO, 182, 184 und 186. Wenn andere Beweismittel aufgefunden werden, ist eine gesonderte Anordnung dafür erforderlich, es sei denn, sie werden freiwillig eingereicht (a. a. O. 182).

nicht fortgesetzt werden muss, wie im Fall, dass eine Kopie gesichert ist (§ 218a Abs. 1, 4 K-StPO). Dem Verlangen muss sie entsprechen, es sei denn, es gibt besondere Gründe, das abzulehnen.[621] Bei der Entscheidung über (Quasi-)Rückgabe hat die Ermittlungsbehörde das Opfer und den Beschuldigten oder seinen Verteidiger im Voraus zu benachrichtigen (§ 135 i. V. m. § 219 K-StPO) und ihnen Gelegenheit zu geben, sich dazu zu erklären. Wenn die Ermittlungsbehörde den Antrag des Betroffenen ablehnt, kann dieser eine Entscheidung über die (Quasi-)Rückgabe bei dem Gericht beantragen, in dessen Bezirk die Behörde ihren Sitz hat (§ 218a Abs. 2 K-StPO), und sie muss dieser Entscheidung nachkommen § 218a Abs. 3 K-StPO). Der § 218a K-StPO, der durch die Änderung 2011 geschaffen wurde, betrachtet Papiere und Datenträger im Lichte der Worte der „zur Verwendung als Beweismittel beschlagnahmten Gegenstände" und der „Kopie". Die Rückgabe bedeutet, dass die beschlagnahmten Gegenstände, wenn sie nicht weiter beschlagnahmt werden müssen, endgültig an den von der Maßnahme Betroffenen zurückgegeben werden,[622] und die Quasi-Rückgabe bedeutet, dass die Gegenstände vorläufig an ihn zurückgegeben werden, wenn ihre Beschlagnahme fortgesetzt werden und wirksam bleiben muss.[623] Die (Quasi-)Rückgabe muss erfolgen, es sei denn, sie ist unmöglich. Sie hat keinen Einfluss auf das materielle Rechtsverhältnis; daher wirkt der Verzicht auf das Eigentum oder das Recht auf (Quasi-)Rückgabe nicht auf die (Quasi-)Rückgabepflicht der Ermittlungsbehörde.[624]

f) Nachweis der Identität elektronischer Daten

Elektronische Daten oder Dateien können nur dann als Beweismittel dienen, wenn nachgewiesen wird, dass es sich um das Original handelt oder dass im Zuge des Kopierens keine Bearbeitung oder Manipulation stattgefunden hat.[625] Dies kann beurteilt werden, indem alle Umstände wie die Aussagen einer Person, die am Verfahren der Erstellung, Übertragung, Speicherung etc. von Kopien oder Drucken beteiligt ist, der Vergleich des Hashwerts des Originals und der Kopie, die Ergebnisse des Augenscheins und des Sachverständigengutachtens der Dateien etc. umfassend berücksichtigt werden.[626] Da diese Identität mit dem Original eine Voraussetzung für die Beweisfähigkeit ist, liegt die Beweislast für ihren Nachweis bei der StA.[627]

---

[621] *K-OGHE* vom 29. 9. 2017 – 2017 Mo 236.

[622] *Joo-Won Rhee*, K-StPO, 171. In der Hauptverhandlung werden die beschlagnahmten Gegenstände vom Gericht ohne Aufforderung des Betroffenen von Amts wegen zurückgegeben (§ 133 Abs. K-StPO).

[623] *Joo-Won Rhee*, K-StPO, 172.

[624] *K-OGHE (Plenum)* vom 16. 8. 1996 – 94 Mo 51.

[625] *Joo-Won Rhee*, K-StPO, 166.

[626] *K-OGHE* vom 26. 7. 2013 – 2013 Do 2511; *ders.* vom 28. 9. 2016 – 2014 Do 9903; *ders.* vom 8. 2. 2018 – 2017 Do 13263.

[627] *K-OGHE* vom 4. 9. 2001 – 2000 Do 1743; *ders.* vom 8. 2. 2018 – 2017 Do 13263.

4. Beschwerde gegen die Art und Weise der Durchführung: § 417 K-StPO

Der Beschluss des „Gerichts" kann angefochten werden, es sei denn, es gibt besondere Bestimmungen in diesem Gesetz (sog. „allgemeine Beschwerde", § 402 K-StPO). Anfechtbar sind auch bestimmte Beschlüsse des „vorsitzenden oder beauftragten Richters", den Ablehnungsantrag zurückzuweisen, eine Anordnung über Verhaftung, Freilassung gegen Kaution, Beschlagnahme oder Rückgabe beschlagnahmter Gegenstände zu treffen, eine Sachverständige in Gewahrsam zu halten oder eine Zahlung von Bußgeldern oder Entschädigungen für Zeugen, Gutachter und Dolmetscher anzuordnen (sog. „entsprechende Beschwerde von § 416 K-StPO"). Schließlich können die Maßnahmen der „Ermittlungsbehörde" über Verhaftung, Beschlagnahme, Rückgabe oder Anwesenheit des Verteidigers bei der Vernehmung nach § 243a K-StPO angefochten werden (sog. „entsprechende Beschwerde von § 417 K-StPO").

Nach ständigen Rspr. des *K-OGH* ist der § 402 K-StPO nur auf das mit der Sache befasste Gericht anwendbar und der Ermittlungsrichter stellt keinen vorsitzenden oder beauftragten Richter i. S. d. § 416 Abs. 1 K-StPO dar.[628] Daher kann unter der geltenden K-StPO die Anordnung des Ermittlungsrichters zur Festnahme, Verhaftung, Beschlagnahme oder Durchsuchung selbst nicht angefochten werden.[629] Wenn eine Maßnahme der Ermittlungsbehörde über die Durchführung richterlicher Beschlagnahmeanordnung oder die Rückgabe der beschlagnahmten Gegenstände gegen das Verfahren nach K-StPO verstößt, kann der von der Maßnahme Betroffene sie aufgrund der entsprechenden Beschwerde von § 417 K-StPO anfechten.[630] Wenn schließlich der Antrag auf Anordnung der Beschlagnahme oder Durchsuchung im Ermittlungsverfahren zurückgewiesen wird, kann die StA nur durch Hinzufügung zusätzlicher Materialien erneut einen Antrag stellen, und der Betroffenen kann erst nach Beendigung der Maßnahme entsprechende Beschwerde gegen die Rechtswidrigkeit ihrer Durchführung durch die Ermittlungsbehörde einlegen. Das heißt, im südkoreanischen Ermittlungsverfahren kann der Beschluss des Gerichts über die Maßnahme nicht angefochten werden und nur gegen die Rechtmäßigkeit der Art und Weise ihres Vollzugs kann Beschwerde geführt werden. Die entsprechende Beschwerde gemäß § 417 K-StPO kann beim Gericht erhoben werden, in dessen Bezirk die Maßnahme stattgefunden hat oder die StA ihren Sitz hat.[631]

Andererseits ist nach der Entscheidung des *K-OGH* die entsprechende Beschwerde unzulässig, wenn ihr Ziel bereits erreicht wurde oder ihr Interesse im Laufe der Zeit verloren gegangen ist.[632] Dies entspricht insb. der früheren Stellungnahme

[628] *K-OGHE* vom 12. 7. 1986 – 86 Mo 25; *ders.* vom 16. 6. 1997 – 97 Mo 1; *ders.* vom 29. 9. 1997 – 97 Mo 66; *ders.* vom 18. 12. 2006 – 2006 Mo 646 m. w. N.

[629] *Joo-Won Rhee*, K-StPO, 627.

[630] *K-OGHE* vom 29. 9. 1997 – 97 Mo 66.

[631] *Joo-Won Rhee*, K-StPO, 629.

[632] *K-OGHE* vom 15. 10. 2015 – 2013 Mo 1970.

des *BVerfG*, die eine Beschwerde gegen die Rechtswidrigkeit der „Durchsuchung" wegen prozessualer Überholung für unzulässig hielt (siehe Fn. 477).

III. Einzelne Streitpunkte

1. Dürfen elektronische Daten Gegenstände der Beschlagnahme und Durchsuchung sein?

Dieses Problem ist bereits seit dem Zeitpunkt umstritten, als elektronische Daten als Beweismittel wichtig wurden,[633] und dies gilt umso mehr in der aktuellen IT-Umgebung, in der Web-basierte TK-Dienste wie Webmail, Web-Foren und Cloud-Computing üblich sind. Dies liegt daran, dass es möglich ist und auch angefordert wird, durch Zugriff über das Netzwerk nur Daten zu durchsuchen und zu beschlagnahmen. Inzwischen wurde durch die K-StPO-Änderung 2011 der § 106 Abs. 3 K-StPO begründet, der die Art und Weise der Beschlagnahme und Durchsuchung elektronischer Daten regelt. Diese Vorschrift sieht vor, dass nur Daten, die als Beweismittel für die Untersuchung von Bedeutung sein können, ausgewählt und beschlagnahmt werden dürfen, aber wenn dies nicht möglich ist oder es sehr schwer ist, das Ziel der Beschlagnahme zu erreichen, die Datenträger selbst zu beschlagnahmen sind; also macht dies deutlich, dass die Ermittlungsbehörde nur Daten sichern kann.[634] Vor dieser Änderung hat der Gesetzgeber im Jahr 2009 auch den § 9b K-KGSG geschaffen, der Mitteilung über die (heimliche) Durchführung von Beschlagnahme und Durchsuchung der bereits gesendeten und empfangenen TK regelt. Diese Vorschriften legen die Beschlagnahmefähigkeit elektronischen Daten nicht klar fest, aber gehen davon aus, dass nur elektronische Daten beschafft werden können. Außerdem sind solche Daten heutzutage aufgrund der Entwicklung der Technologie nicht nur konzeptionell unabhängig von dem Datenträger, sondern verfahrensirrelevante Daten, die auf ihm zusammen gespeichert sind, dürfen nicht beschlagnahmt werden. Aus diesem Grund hält die h. M. elektronische Daten selbst für beschlagnahmefähig.[635] Der *K-OGH* erklärte in der Entscheidung vom 26. Mai 2011 kurz vor der Änderung 2011:

---

[633] Diesbezüglich gab es bis 2010 große Meinungsverschiedenheiten und keine eindeutig dominierende Meinung. Vor allem bestritt der *K-OGH* den Begriff des Vermögensgegenstandes elektronischer Daten bei der Prüfung, ob diese Gegenstände von Diebstahl sein könnten (vom 12. 7. 2002 – 2002 Do 745): „*Die Daten, die auf dem Computer gespeichert sind, selbst können weder als körperlichen Gegenstand noch als materielle Kraft angesehen werden, sodass sie kein Vermögensgegenstand sein können, und selbst wenn sie kopiert oder gedruckt werden, wird ihr Wert oder ihr Besitz und ihre Verfügbarkeit des Opfers nicht verringert. Daher kann nicht davon ausgegangen werden, dass eine solche Handlung ein Diebstahl darstellt.*" (Übersetzung vom Autor). Nach h. M. handelt es sich jedoch um eine Auslegung des materiell-strafrechtlichen Begriffs, sodass dies nicht auf das Verfahrensgesetz übertragen werden kann.

[634] *Lee/Cho*, K-StPO, § 20 Rn. 10.

[635] *Kuk Cho*, KJC, 22-1, 2010, 99, 104 f.; *Joo-Won Rhee*, ALR, Nr. 37, 2012, 151, 160; *Sookyeon Lee*, KJCL, 18-1, 2012, 1, 21 – 22; *Won-Sang Lee*, CRCL, Nr. 38, 2013, 174, 191 f.;

„Grundsätzlich muss die Beschlagnahme und Durchsuchung elektronischer Daten in der Weise erfolgen, dass nur der Teil, der mit dem Tatvorwurf, der dem Erlass des richterlichen Beschlusses zugrunde liegt, im Zusammenhang steht, ausgedruckt oder auf das Speichermedium der Ermittlungsbehörde kopiert wird. Die Beschlagnahme und Durchsuchung in der Weise, dass sämtliche Daten kopiert oder mitgenommen werden, kann … nur ausnahmsweise zugelassen werden."[636] *(Übersetzung vom Autor)*

In der Praxis werden elektronische Daten schon seit Langem i. d. R. so beschlagnahmt und durchsucht, dass nur sie ohne Speichermedium übertragen oder kopiert werden.[637] Daher stimmt die Bejahung ihrer Beschlagnahmefähigkeit mit der Rechtswirklichkeit überein (vgl. oben B. I.). Es ist angemessen, das Gesetz und seine Auslegung an die veränderte IT-Umgebung anzupassen.[638]

2. Rechtfertigen die allgemeinen Vorschriften eine „heimliche" Sicherstellung der „beim Server des ISP gespeicherten" Daten?

Nach höchstrichterlichen Entscheidungen und h. M. rechtfertigen §§ 106 ff. i. V. m. § 219 K-StPO – nicht nur die offene Beschlagnahme und Durchsuchung, sondern auch – die heimlichen Maßnahmen, die nicht vom K-KGSG abgedeckt werden. Auf dieser Grundlage kann die Ermittlungsbehörde u. a. ohne Wissen des Betroffenen seine Postsendungen oder E-Mail- oder Messenger-Nachrichten durchsuchen und beschlagnahmen, die von Posten oder TK-Dienstanbietern in Verwahrung genommen sind (vgl. §§ 106 Abs. 4, 107 Abs. 3 S. 1 K-StPO).[639] Die Bestimmung, die dies eindeutig bestätigt, ist § 9b K-KGSG:

„Wenn die Ermittlungsbehörde die bereits gesendete und empfangene TK beschlagnahmt oder durchsucht hat, muss sie innerhalb von 30 Tagen ab dem Datum des Beschlusses bezüglich der öffentlichen Klage – ausgenommen des Beschlusses zur Verfahrenseinstellung – den TK-Teilnehmer, an den sich die Ermittlung richtet, über ihre Durchführung benachrichtigen."

Heun-Jae Lee, DLR, 37-3, 2013, 129, 135 – 137; *In-Gon Lee*/*Chul-Ha Kang*, CRCL, Nr. 54, 2017, 322, 348 f.; *Son*/*Kim*, Durchsuchungs- und Beschlagnahmeverfahren, 40 f.; a. A. *Kil-Young Oh*, JML, 14-1, 2015, 33, 51 f.

[636] *K-OGHE* vom 26. 5. 2011 – 2009 Mo 1190; weiter *ders. (Plenum)* vom 16. 7. 2015 – 2011 Mo 1839.

[637] *Sungsoo Ahn*, KoK-StPO, § 106, 564.

[638] *Kuk Cho*, KJC, 22-1, 2010, 99, 104; *Joo-Won Rhee*, ALR, Nr. 37, 2012, 151, 160 f.; *Won-Sang Lee*, CRCL, Nr. 38, 2013, 174, 192; *Heun-Jae Lee*, DLR, 37-3, 2013, 129, 136 [Fn. 12]; *In-Gon Lee*/*Chul-Ha Kang*, CRCL, Nr. 54, 2017, 322; auch *Kil-Young Oh*, JML, 14-1, 2015, 33, 52 ff.

[639] Vgl. *K-VerfGE* 24-2, 467, 472: *„Da E-Mails i. d. R. auf dem Server des ISP gespeichert sind, werden bei ihrer Beschlagnahme und Durchsuchung … der ‚von der Maßnahme Betroffene' und der ‚Eigentümer von Daten, die tatsächliche Gegenstände darstellen' voneinander getrennt."* (Übersetzung vom Autor).

In diesem Fall erhält die Ermittlungsbehörde i. d. R. unter Mitwirkung des Dienstanbieters Daten im Zusammenhang mit dem Tatverdacht, wobei der richterliche Anordnungsbeschluss nicht den von Daten Betroffenen, an die sich die Maßnahme nicht unmittelbar richtete, nämlich den Absender oder Empfänger, vorgezeigt werden muss (§ 118 i. V. m. § 219 K-StPO; vgl. oben II. 3. b) (1)).[640] Darüber hinaus kann die Benachrichtigung über die Maßnahme wegen der Gefahr der Störung der Untersuchung unterbleiben (§ 107 Abs. 3 S. 2 K-StPO), und die Benachrichtigung über die Teilnahme des Beschuldigten und seines Verteidigers kann in dringenden Fällen ebenfalls ausgeschlossen werden (vgl. §§ 121, 122 K-StPO). Bei einer solchen heimlichen Durchführung werden schließlich die Verfahren, die die Offenheit der Maßnahme in den allgemeinen Vorschriften der Beschlagnahme und Durchsuchung kennzeichnen, fast immer ausgeschlossen. Das *K-VerfG* ist aber der Ansicht, dass dies keine Probleme beim Schutz der Grundrechte des von den Daten Betroffenen verursacht: Auch wenn die vorherige Benachrichtigung bei heimlicher Beschlagnahme und Durchsuchung von auf Servern gespeicherten E-Mails oder Messenger-Nachrichten aufgrund der §§ 107 Abs. 3 S. 2, 122 S. 2 K-StPO ausnahmsweise ausgenommen wird, kann der von den Daten Betroffene „mindestens" nach § 9b K-KGSG benachrichtigt werden, sodass der Schutz seiner Grundrechte nicht beeinträchtigt wird.[641]

Diese Interpretation ist jedoch nicht angebracht. Zunächst ist fraglich, ob die Notwendigkeit der geheimen Durchführung der Beschlagnahme und Durchsuchung zum Begriff der Gefahr der Störung der Untersuchung i. S. d. § 107 Abs. 3 S. 2 K-StPO gehört und in den dringenden Fällen i. S. d. § 122 S. 2 K-StPO enthalten ist. Wenn das Gericht nicht in diese Entscheidung eingreift, wird die Ermittlungsbehörde tendenziell nicht benachrichtigen. Außerdem dient der § 9b K-KGSG bei einer heimlichen Durchführung nur zum nachträglichen Rechtsschutz des von den Daten Betroffenen und ist keine Ermächtigungsnorm für die Rechtfertigung heimlicher Ermittlungsmaßnahmen. Daher ist es schwierig, der Entscheidung des *K-VerfG* zuzustimmen, dass die allgemeinen Vorschriften aufgrund der o. g. Vorschriften auch die heimliche Beschlagnahme und Durchsuchung rechtfertigen. Darüber hinaus wird dies in der Literatur unter dem Gesichtspunkt der Verhältnismäßigkeit kritisiert. Das heißt, es ist unter der heutigen IuK-Technologie nicht verhältnismäßig, dass heimliche Zugriffe auf die auf dem Server des Dienstanbieters gespeicherten Daten nach den allgemeinen Vorschriften mit milderen Eingriffsvoraussetzungen und Verfahrenssicherungen zugelassen werden als bei solchen auf Daten im laufenden Kommunikationsvorgang, nämlich der TKÜ; angesichts der Tatsache, dass personenbezogene Daten heute kumulativ unbegrenzt auf dem Server gespeichert sind, ist der erstere Eingriff schwerwiegender als der letztere.[642] Schließlich ist es erforderlich,

[640] *K-VerfGE* 24-2, 467, 472.

[641] *K-VerfGE* 24-2, 467, 472 f.

[642] *Kil-Young Oh*, JML, 14-1, 2015, 33, 34; *Seok-soon Im*, KCR, 27-2, 2016, 203, 221 – 224; *Hojung Lee*, JPL, 17-1, 2019, 35, 43; *Joongwook Park*, CRCL, Nr. 68, 2020, 97, 125 f. Aus dem gleichen Grund werden auch die ständigen Rspr. vom *K-OGH* kritisiert, dass die TKÜ nach K-

eine neue Ermächtigung für die heimliche Beschlagnahme und Durchsuchung zu schaffen, die zumindest mit der TKÜ entsprechenden Verfahrenskontrollen ausgestattet ist.

3. Ist Netzwerkdurchsuchung bzw. grenzüberschreitende Durchsuchung zulässig?

(1) Die Erweiterung der Durchsuchung/Durchsicht um externe Speichermedien, die in § 110 Abs. 3 StPO und Art. 19 Abs. 2 CKÜ vorgesehen ist, sog. „Netzwerkdurchsuchung", und auch die „grenzüberschreitende Durchsuchung", ist in Südkorea erst seit Kurzem problematisch. Diese Ermittlungsmethode wird in der Praxis zwar bereits durchgeführt, aber in der Literatur kaum behandelt, und es gibt auch keine Entscheidung, die sie betrifft. Inzwischen fällten im Juni und Juli 2017 diesbezüglich die *12.* und *8. Kammer* vom *Obergericht Seoul* jeweils widersprüchliche Urteile,[643] und im November desselben Jahres traf der *K-OGH* ein Revisionsurteil des ersteren.[644]

Der Sachverhalt der beiden Fälle ist fast ähnlich. Aufgrund richterlicher Anordnung hat die Ermittlungsbehörde die Wohnräume etc. eines Beschuldigten rechtmäßig beschlagnahmt und durchsucht und dabei eine große Anzahl von Taschen- oder Notizbüchern und auch Kopien elektronischer Daten in ihr Dienstbüro mitgenommen, um sie zu durchzusehen. Während ihrer Durchsicht hat sie Benutzername und Passwort des E-Mail-Kontos des Beschuldigten aufgefunden, das von einem ausländischen E-Mail-Dienstanbieter bereitgestellt wird,[645] und dann beim Gericht eine neue Anordnung beantragt, um damit auf das Konto zuzugreifen und die für den Tatverdacht relevanten Daten zu beschlagnahmen und zu durchsuchen. Der Richter erließ einen Anordnungsbeschluss zur Beschlagnahme und Durchsuchung, in dem Folgendes bestimmt angegeben ist: als ihre Gegenstände Kopien oder Drucke

KGSG die Gleichzeitigkeit bzw. Gegenwärtigkeit ihrer Durchführung voraussetzt (vgl. Kapitel 3, D. II. 1. a) aa)).

[643] *Obergericht Seoul-Entscheidung* vom 13. 6. 2017 – 2017 No 23 und *ders.* vom 5. 7. 2017 – 2017 No 146.

[644] *K-OGHE* vom 29. 11. 2017 – 2017 Do 9747. Darin ist die Begründung des Urteils der *8. Kammer* (2017 No 146) enthalten.

[645] In Südkorea ist es kein Problem, dass die Ermittlungsbehörde die Zugangsdaten auf eine solche Weise erhält. Nach teilweise in der Literatur vertretener Auffassung gehört das Verlangen nach Herausgabe von Benutzername und Passwort vom Verdächtigen zum Zwang zu selbstbelastenden Aussagen und die Ermittlungsbehörde kann sie nur durch die Belehrung des Aussageverweigerungsrechts erhalten. Die ohne solche Mitteilung erhaltenen Daten sind illegal erlangte Beweise und dürfen nicht als Beweismittel dienen (*Jongmo Yang*, jhlr, 15-3, 2014, 1, 19 – 21; *In-Gon Lee*/*Chul-Ha Kang*, CRCL, Nr. 54, 2017, 322, 339; vgl. oben C. III. 2. a) cc); dazu *K-OGHE* vom 20. 8. 2009 – 2008 Do 8213; *ders.* vom 10. 11. 2011 – 2010 Do 8294: Aufgrund der Aussagefreiheit, die sich aus dem Grundsatz des Verbots der Selbstbelastung ergibt (Art. 12 Abs. 1, 2 K-Verf und § 244b K-StPO), ist der Zwang zu selbstbelastenden Aussagen gegen den Beschuldigten verboten und die Aussagen, die ohne Bekanntgabe dieses Rechts erlangt wurden, werden nicht als Beweismittel zugelassen.

der E-Mails, die mit dem Verdacht auf einen Verstoß gegen das Staatssicherheitsgesetz im Zusammenhang stehen, in einem bestimmten Zeitraum gesendet oder empfangen wurden und danach auf dem Server gespeichert wurden, als ihr Durchführungsort der PC, der im Büro der Korea Internet & Security Agency (KISA) eingerichtet ist und für eine grenzüberschreitende Durchsuchung und Beschlagnahme bestimmt ist, und als ihre Durchführungsmethode ① der Zugriff auf den ausländischen Server, der im PC durch die Eingabe des Benutzernamens und Passworts in Anwesenheit institutioneller und privater forensischer Experten erfolgt, und dann ② das Ausdrucken und Kopieren nur der für dem Verdacht relevanten E-Mails aus den heruntergeladenen und angezeigten. Hierbei hat der Richter von Amts wegen eine Bedingung hinzugefügt: „Die Ermittlungsbehörde muss dem Beschuldigten Gelegenheit geben, an der Beschlagnahme und Durchsuchung teilzunehmen, aber dies gilt nicht bei dem Fall, wenn er sie aufgibt oder ablehnt." Infolgedessen hat die Ermittlungsbehörde dem Beschuldigten und seinem Verteidiger die Gelegenheit zur Teilnahme gegeben, indem sie ihnen Datum und Ort der Durchführung mitteilte, und dann hat sie nach Vorlage des Beschlusses bei KISA die Maßnahme nach der darin beschriebenen Methode durchgeführt.

(2) Im Urteil von 2017 No 23 hat die *12. Kammer* vom *Obergericht Seoul* entschieden, dass die Netzwerkdurchsuchung und die grenzüberschreitende Durchsuchung illegal sind, weil sie nicht auf §§ 106 Abs. 1, 2, 107 Abs. 1, 109 Abs. 2, 118 i. V. m. § 219 K-StPO beruhen können. Vor allem hat sie dies damit begründet, dass eine Rechtsgrundlage erforderlich ist, um die Durchsuchung und Beschlagnahme als Zwangsmaßnahme zum Server im Ausland auszudehnen, aber eine derartige Durchführung der Maßnahme nicht durch die o. g. Vorschriften gerechtfertigt werden kann, weil hierbei der von der Maßnahme Betroffene der Dienstanbieter ist. Sie erklärte auch, dass eine solche Durchführung die Anwendung von § 123 K-StPO vermeidet und dem Willen des Anbieters widerspricht und weiter nicht unter die „notwendige Maßnahme" i. S. v. § 120 K-StPO fallen kann. Hingegen hat der *K-OGH* im Urteil von 2017 Do 9747 entschieden, dass diese Durchführung auch unter der aktuellen K-StPO zulässig ist. In der Begründung setzt er Folgendes voraus: Bei der Beschlagnahme und Durchsuchung, die über Netzwerk vorgenommen wird, wird der Umfang der Durchführung nicht räumlich erweitert, der von den Daten Betroffene, nämlich der Beschuldigte, ist der von der Maßnahme Betroffene und die Handlungen von ① betrifft die Durchsuchung und solche von ② die Beschlagnahme. Daneben widersprechen die Handlungen von ① weder der Absicht des Anbieters noch ist sie rechtswidrig, weil er den Zugang ohne praktische Prüfung erlaubt, wenn eingegebenen Zugangsdaten (Benutzername und Passwort) mit den registrierten übereinstimmen.[646] Demzufolge wird diese Beschlagnahme und Durchsuchung am im richterlichen Beschluss angegebenen Ort, d. h. am bestimmten PC im Büro der

[646] *Jung-Min Lee*, KJCCL, 19-3, 2017, 117, 134; *Soonok Lee*, CALR, 20-1, 2018, 117, 136; a. A. *Dae-Won Kim*, TPCP, 11-1, 2019, 91, 105; *Jong-Jin Cha*, KJCCL, 21-2, 2019, 149, 165 f.

KISA, durchgeführt,[647] und dies gehört auch zu der notwendigen Maßnahme i. S. d. § 120 K-StPO.[648] Schließlich sagte der *K-OGH* vor allem, dass diese Auslegung zur Netzwerkdurchsuchung auch für die grenzüberschreitende Durchsuchung ohne Weiteres gilt.[649]

In Südkorea besteht das grundlegende Problem hinsichtlich der Zulässigkeit der Netzwerkdurchsuchung und der grenzüberschreitenden Durchsuchung darin, dass solche Ermittlungsmethoden zwar in der Praxis unbedingt erforderlich sind, die K-StPO jedoch keine klare Rechtsgrundlage dafür hat. Dies ist die größte Kritik am Urteil des *K-OGH*. Dennoch unterstützt eine repräsentative Ansicht der Literatur das Urteil aufgrund ihrer praktischen Notwendigkeit und des Grundsatzes der Verhältnismäßigkeit. Sie unterstreicht, dass die Ermittlungsbehörde insb. im Sachverhalt die Zugangsdaten rechtmäßig – nicht illegal, wie z. B. durch Hacking oder Vortäuschung – erhalten hat, dass sie für diese Art von Zugang eine richterliche Anordnung neu erlangt hat und dass sie dem Beschuldigten die Möglichkeit zur Teilnahme an der Durchsuchung gab.[650] Auf jeden Fall wird eine derartige Durchsuchung in Südkorea jetzt nach dem Urteil des *K-OGH* als zulässig angesehen, solange sie aufgrund der Anordnung des Gerichts an einem bestimmten Ort in Südkorea – wie z. B. einem bestimmten PC von KISA – durchgeführt wird. Natürlich wird im Schrifttum immer noch die Frage gestellt, ob der Zugang zu Servern in Übersee, der mit völkerrechtlicher Souveränität in Verbindung steht, nur durch diese Interpretation erfüllt werden kann. Zum Schluss sollte dies durch Gesetzgebung, Vertragsabschluss, Beitritt zum CKÜ etc. gelöst werden.[651]

4. Kopie und Mitnahme sämtlicher Daten, Teilnahmerecht und Zufallsfunde

a) Charakter der Kopie und Mitnahme sämtlicher Daten und Gewährleistung des Teilnahmerechts

Wie bereits erwähnt, muss die Beschlagnahme und Durchsuchung elektronischer Daten grundsätzlich so erfolgen, dass nur der für den Verdacht relevante Teil beschlagnahmt wird (vgl. § 106 Abs. 3 K-StPO), was in vielen Fällen in der Weise

[647] *Sookyeon Lee*, 34; *Soonok Lee*, CALR, 20-1, 2018, 117, 136 f.; a. A. *Jong-Jin Cha*, KJCCL, 21-2, 2019, 149, 168 f. In diesem Fall meint Prof. *Soonok Lee*, dass die Handlungen der Beschlagnahme und Durchsuchung im Inland, nicht im Ausland, durchgeführt werden, während Dr. *Cha* glaubt, dass sie sowohl im Inland als auch im Ausland durchgeführt werden.

[648] *Jung-Min Lee*, KJCCL, 19-3, 2017, 117, 134; *Soonok Lee*, CALR, 20-1, 2018, 117, 137 f.

[649] Zust. *Soonok Lee*, CALR, 20-1, 2018, 117, 137 und 139; abw. begrenzt in Fällen der Staatssicherheit, *Jung-Min Lee*, KJCCL, 19-3, 2017, 117, 138 ff.; a. A. *Won-Sang Lee*, JDF, 11-3, 2017, 29, 32 f.

[650] *Soonok Lee*, CALR, 20-1, 2018, 117, 139; teilweise auch *Sookyeon Lee*, 34.

[651] *Sookyeon Lee*, 36 f.; *Won-Sang Lee*, JDF, 11-3, 2017, 29, 36; *Jung-Min Lee*, KJCCL, 19-3, 2017, 117, 142; *Soonok Lee*, CALR, 20-1, 2018, 117, 139; *Dae-Won Kim*, TPCP, 11-1, 2019, 91, 116; *Jong-Jin Cha*, KJCCL, 21-2, 2019, 149, 170 f.

durchgeführt wird, dass sämtliche oder die meisten der gefundenen Daten von Ermittlern kopiert und mitgenommen und danach nur verfahrensrelevante Daten infolge der Suche und Durchsicht gedruckt und kopiert werden.[652] Nach dem Urteil des *K-OGH* ist diese Durchführungsmethode als Ausnahme nur auf Anordnung des Richters zulässig.[653]

Es ist umstritten, ob die Tätigkeit der Suche und Durchsicht nach dem Kopieren und Mitnehmen zur Durchsuchung oder zur Sichtung nach der Beschlagnahme gehört. Dabei handelt es sich um den Zeitpunkt des Abschlusses des Beschlagnahme- und Durchsuchungsverfahrens und die Zulässigkeit des Teilnahmerechts des Beschuldigten und seines Verteidigers nach § 121 K-StPO.[654] Diesbezüglich hat der *K-OGH* in seiner Entscheidung von 2011 (2009 Mo 1190) erstmals ausgeführt, dass eine Reihe von Handlungen zum Kopieren, Mitnehmen, Suchen und Durchsehen sämtlicher Daten insgesamt einer Beschlagnahme und Durchsuchung auf der Grundlage eines einzelnen Beschlusses entspricht und dass die endgültig zu beschlagnahmenden Daten je nach Relevanz zu begrenzen sind und schließlich dass hierfür dem Beschuldigten und seinem Verteidiger die Möglichkeit gegeben werden muss, an diesem gesamten Prozess teilzunehmen. Daran anschließend bestätigte er denselben Inhalt in der Entscheidung von 2015 (2011 Mo 1839) durch den Beschluss im *Plenum.*[655] Daher ist dies zu einem Verfahren geworden, das festgehalten werden muss, es sei denn, es wird durch eine neue Entscheidung im *Plenum* oder eine Gesetzgebung geändert.

> „Angesichts der Grundätze des rechtsstaatlichen Verfahrens, des Richtervorbehalts, der Verhältnismäßigkeit nach Art. 12 Abs. 1, 3 K-Verf und §§ 114, 215 K-StPO ist es selbstverständlich, dass die Gegenstände des Ausdruckens und Kopierens (aus den mitgenommenen Daten) auch auf den für den Verdacht relevanten Teil beschränkt werden müssen. Daher ist es illegal, Speichermedien oder Kopien, die in das Büro einer Ermittlungsbehörde verbracht wurden, ohne Rücksicht auf die Relevanz zu drucken oder zu kopieren, es sei denn, es gibt besondere Umstände."[656] *(Übersetzung vom Autor)*

> „Bei einer Reihe von Prozessen des Kopierens und Mitnehmens sämtlicher Daten müssen der Richtervorbehalt und das rechtsstaatliche Verfahren eingehalten werden, indem nach §§ 121 i. V. m. § 219 K-StPO dem von der Maßnahme Betroffenen oder seinem Verteidiger die Möglichkeit zur Teilnahme am Prozess gewährleistet wird und geeignete Maßnahmen

[652] *Wankyu Lee*, CRCL, Nr. 48, 2015, 90, 99 f.

[653] *K-OGHE* vom 26. 5. 2011 – 2009 Mo 1190 und *ders. (Plenum)* vom 16. 7. 2015 – 2011 Mo 1839: „*Die Beschlagnahme und Durchsuchung in der Weise, dass sämtliche Daten kopiert oder mitgenommen werden, kann nur dann gestattet sein, wenn eine solche Durchführungsweise im richterlichen Beschluss angegeben ist, und … in Ausnahmefällen, z. B. wenn eine lange Zeit aufgrund der Umstände des Durchführungsorts oder der großen Menge an Daten oder Fachkräfte für technische Maßnahmen erforderlich sind.*" (Übersetzung vom Autor).

[654] *Wankyu Lee*, CRCL, Nr. 48, 2015, 90, 103 f.

[655] *K-OGHE* vom 26. 5. 2011 – 2009 Mo 1190 und *ders. (Plenum)* vom 16. 7. 2015 – 2011 Mo 1839; zust. *Lee*/*Cho*, K-StPO, § 20 Rn. 10.

[656] *K-OGHE* vom 26. 5. 2011 – 2009 Mo 1190 und *ders. (Plenum)* vom 16. 7. 2015 – 2011 Mo 1839.

ergriffen werden, um ein willkürliches Kopieren verfahrensirrelevanter Daten zu verhindern.[657] Ansonsten ist die Beschlagnahme oder Durchsuchung illegal, es sei denn, der Betroffene brachte ausdrücklich seine Absicht zur Nichtteilnahme zum Ausdruck oder es gibt besondere Umstände, in denen sein Teilnahmerecht tatsächlich nicht verletzt wurde.[658] Dies gilt auch dann, wenn die Ermittlungsbehörde nur die verfahrensrelevanten Daten von Speichermedien oder Kopien ausgedruckt oder kopiert hat."[659] *(Übersetzung vom Autor)*

„Nachdem eine solche Reihe von Handlungen durchgeführt wurde und somit die Beschlagnahme und Durchsuchung schon abgeschlossen ist, stellt sich nur eine Frage, ob die Ergebnisse der Maßnahme von der Ermittlungsbehörde beibehalten oder verwertet werden, weil dabei die Aufhebung einer einzelnen Maßnahme in einem bestimmten Stadium sinnlos ist. Solange es keine besonderen Umstände gibt … muss das Beschwerdegericht daher nicht entscheiden, ob jede einzelne Handlung rechtswidrig und daher aufzuheben ist, sondern ob die Maßnahme der Beschlagnahme und Durchsuchung insgesamt aufzuheben ist; dabei ist es von Bedeutung, ob die einzelnen rechtswidrigen Handlungen, die im gesamten Prozess der Maßnahme aufgetreten sind, schwer genug sind, um die Beschlagnahme und Durchsuchung illegal zu machen. Hierbei sollte die Schwere der Rechtswidrigkeit beurteilt werden, indem der Sinn und Zweck der verletzten Verfahrensbestimmung, der Prozess und die Schwere der rechtswidrigen Handlung, die Schwere der verletzten Rechtsgüter etc. umfassend berücksichtigt werden."[660] *(Übersetzung vom Autor)*

Aus diesen Entscheidungen geht hervor, dass der *K-OGH* das Recht zur Teilnahme nach §§ 121, 122 K-StPO als wichtiges Mittel zum Grundrechtsschutz durch den Ausschluss verfahrensirrelevanter Daten betrachtet. Die Stellungnahme des *K-OGH* wird aus Sicht der Ermittlungsbehörde allgemein kritisiert, da sie die wirksame

---

[657] Nach dem Urteil von *K-OGH* gehört auch das Wiederherstellen gelöschter Dateien oder das Entschlüsseln verschlüsselter Dateien, das einen Vorbereitungsprozess für die Suche nach Daten darstellt, zur Beschlagnahme und Durchsuchung, sodass der Beschuldigte und sein Verteidiger auch die Möglichkeit haben, an diesem Prozess teilzunehmen (*K-OGHE* vom 15. 10. 2015 – 2013 Mo 1969; a. A. *Wankyu Lee*, CRCL, Nr. 48, 2015, 90, 121 f.). In dieser Entscheidung hat der *K-OGH* jedoch erklärt, dass der Entzug der Möglichkeit, an der Entschlüsselung und Dateikonvertierung teilzunehmen, nicht so illegal ist, dass die gesamte Beschlagnahme und Durchsuchung aufgehoben wird; der Grund dafür war, dass die Möglichkeit der Teilnahme an allen anderen Prozessen garantiert wurde, dass Original bereits vor der Handlung zurückgegeben wurde, dass die Teilnahme an diesem Prozess nicht im Richterbeschluss enthalten war und dass er nicht der Prozess der Suche nach verfahrensrelevanten Daten selbst ist.

[658] *K-OGHE* vom 26. 5. 2011 – 2009 Mo 1190: „*Nach §§ 120, 131 i. V. m. § 219 K-StPO ist … bei Kopieren und Mitnehmen sämtlicher Daten das Durchführungsverfahren nur dann rechtmäßig, wenn geeignete Maßnahmen getroffen werden, um Verzerrung, Beschädigung, Missbrauch, willkürliche Vervielfältigung oder Kopieren usw. von Daten während des gesamten Prozesses zu verhindern; z. B. die ständige Gewährleistung des Rechts auf Teilnahme des Beschuldigten und seines Verteidigers, das Verbot der Durchsicht und Vervielfältigung ohne diese Teilnahme, die Erstellung und Aushändigung des Verzeichnisses der kopierten Daten etc.*" (Übersetzung vom Autor).

[659] *K-OGHE (Plenum)* vom 16. 7. 2015 – 2011 Mo 1839; und weiter *ders.* vom 21. 9. 2017 – 2015 Do 12400.

[660] *K-OGHE (Plenum)* vom 16. 7. 2015 – 2011 Mo 1839; und weiter *ders.* vom 15. 10. 2015 – 2013 Mo 1969.

Strafverfolgung in der Praxis stört,[661] aber im Schrifttum wird sie weitgehend unterstützt.[662]

b) Zufallsfunde

Werden Daten, die zwar nicht für das Verfahren relevant sind, aber auf die Begehung anderer Straftaten hindeuten, bei der Durchsicht nach dem Kopieren und Mitnehmen sämtlicher Daten zufällig gefunden, darf die Ermittlungsbehörde sie nicht eigenständig – auch nicht vorläufig – beschlagnahmen (vgl. § 108 StPO). Das heißt, die willkürliche Beschlagnahme und Verwertung verfahrensirrelevanter Daten durch die Ermittlungsbehörde ist illegal und unzulässig (vgl. oben II. 2. (1)), es sei denn, dies entspricht den §§ 216–218, 220 K-StPO (vgl. oben II. 3. d)). Daher muss sie in diesem Fall zunächst die weitere Durchsicht einstellen und zügig eine richterliche Anordnung zur Beschlagnahme oder Durchsuchung der Daten bezüglich der anderen Vorwürfe beantragen und einholen,[663] andernfalls werden die zufällig gefundenen Daten rechtswidrig erlangt und dürfen nicht als Beweismittel dienen.[664] Da sich dieses Beschlagnahme- und Durchsuchungsverfahren vom ursprünglichen Verfahren unterscheidet, ist die Gewährleistung des Teilnahmerechts und die Aushändigung des Beschlagnahmeverzeichnisses gesondert erforderlich, sofern keine besonderen Umstände vorliegen.[665] Hier stellt sich die Frage, in welchen Fällen die Ermittlungsbehörde die gesonderte Anordnung zur Beschlagnahme der zufällig gefundenen Daten beantragen muss. Dabei handelt es sich darum, ob diese Daten verfahrensirrelevante Daten betreffen, die nicht durch den bereits ausgestellten Beschluss gesichert werden können.[666] Da die Relevanz nach der Rspr. des *K-OGH* weithin anerkannt wird, gibt es praktisch nur wenige Fälle, in denen die Ermitt-

[661] *Wankyu Lee*, CRCL, Nr. 48, 2015, 90, 104. Staatsanwalt *Wankyu Lee* kritisiert, dass in der Praxis dieses Teilnahmerecht nicht effektiv genug ist, um übermäßige Ermittlungen einzuschränken, sondern nur zu verwirrenden Situationen führt. Laut ihm wird in der Praxis normalerweise der Beschuldigte nach § 122 S. 2 K-StPO nicht über die Durchsicht der mitgenommenen Daten informiert oder er gibt freiwillig das Recht auf (a. a. O. 108 und 110 f.).

[662] *Lee/Cho*, K-StPO, § 20 Rn. 16; *Kil-Young Oh*, JML, 14-1, 2015, 33, 59 f. Prof. *Oh* argumentiert, dass der Beschuldigte und sein Verteidiger in der Lage sein müssen, gegen die Prüfung der Relevanz und die Verletzung des Geheimnisses des Privatlebens teilweise Einspruch zu erheben, um das Teilnahmerecht in der Praxis tatsächlich zu verwirklichen, und dass dies im Protokoll der Beschlagnahme und Durchsuchung angegeben werden muss (a. a. O. 61).

[663] *K-OGHE (Plenum)* vom 16. 7. 2015 – 2011 Mo 1839; *Kuk Cho*, KJC, 22-1, 2010, 99, 119; a. A. *Wankyu Lee*, CRCL, Nr. 48, 2015, 90, 146 ff.; *Seungsoo Chun*, CRCL, Nr. 49, 2015, 37, 64. Die letzten beiden Autoren sind als Staatsanwälte im Grunde der Meinung, dass das „Kopieren und Mitnehmen sämtlicher Daten" – im Gegensatz zur Stellungnahme des *K-OGH* – eine endgültige Beschlagnahme ist, keine vorläufige Maßnahme zur weiteren Durchsuchung (*Wankyu Lee*, a. a. O. 103 f.; *Seungsoo Chun*, a. a. O. 67).

[664] *K-OGHE* vom 16. 1. 2014 – 2013 Do 7101.

[665] *K-OGHE (Plenum)* vom 16. 7. 2015 – 2011 Mo 1839.

[666] *Wankyu Lee*, CRCL, Nr. 48, 2015, 90, 132 und 147.

lungsbehörde wegen der zufällig gefundenen Daten eine neue Anordnung beantragen muss.[667]

IV. Zusammenfassung und Zwischenfazit

In Südkorea wird bereits seit über 20 Jahren darüber diskutiert, wie elektronische Daten im Ermittlungsverfahren zu beschlagnahmen und zu durchsuchen sind. In den 2000er Jahren ging es hauptsächlich darum, wie bestehende Auslegungen, die körperliche Gegenstände voraussetzen, auf immaterielle Daten übertragen werden konnten. In den letzten Jahren wird jedoch der Verfahrenskontrolle und der Rechtmäßigkeit der Durchführung der Beschlagnahme und Durchsuchung mehr Aufmerksamkeit gewidmet, um übermäßige Eingriffe in Persönlichkeitssphäre bei umfassender Datenerhebung zu verhindern. Dies ist auf Datenfülle und Netzwerkbezogenheit aus technischer Sicht und die Einführung des Ausschlussprinzips aus rechtlicher Sicht zurückzuführen. Die individuelle Gesetzgebung, die sich an die Veränderungen in der Realität anpasst, ist jedoch langsam. Aus diesem Grund versucht der *K-OGH* oft, die Forderung nach dieser neuen Verfahrenskontrolle durch eine erweiterte Interpretation bestehender Vorschriften zu lösen.

In Südkorea gibt es vier große Kontroversen bezüglich der Beschlagnahme und Durchsuchung elektronischer Daten: Beschlagnahmefähigkeit der Daten, Rechtfertigung heimlicher Beschlagnahme und Durchsuchung aufgrund der allgemeinen Vorschriften, Zulässigkeit der Netzwerkdurchsuchung bzw. der grenzüberschreitenden Durchsuchung und Gewährleistung des Teilnahmerechts des Beschuldigten und seines Verteidigers. Erstens wird jüngst in der Literatur die Beschlagnahmefähigkeit elektronischer Daten kaum mehr beanstandet; insb. nach der K-StPO-Änderung 2011. Und in der Literatur wird ständig darauf hingewiesen, dass es angesichts des Grundrechtsschutzes problematisch ist, dass die auf dem Server des TK-Dienstanbieters gespeicherten Daten aufgrund der allgemeinen Vorschriften ohne Wissen des Betroffenen beschlagnahmt und durchsucht werden dürfen. Der *K-OGH* und das *K-VerfG* erkennen dies aber nicht an, und auch der Gesetzgeber unternimmt keine legislativen Versuche. Bei der Netzwerkdurchsuchung bzw. der grenzüberschreitenden Durchsuchung ist eine Lösung durch Gesetzgebung oder internationale Zusammenarbeit von grundlegender Bedeutung, was dem Strafrechtsverfahren eine starke Rechtfertigung geben wird.[668] Schließlich gibt das Recht auf Teilnahme dem Beschuldigten und seinem Verteidiger die Möglichkeit, die Einhaltung der Verfahren der Ermittlungsbehörde zu überwachen und ihren offensichtlichen illegalen Handlungen zügig zu begegnen. Dies kann u. a. dazu dienen, übermäßige Datenzugriffe in Ermittlungsverfahren zu beschränken. Insb. hinsichtlich der Beschlagnahme und Durchsuchung durch das Kopieren und Mitnehmen sämtlicher Daten verlangt der *K-*

[667] *Wankyu Lee*, CRCL, Nr. 48, 2015, 90, 152.

[668] Derzeit wird in Südkorea über den Beitritt zu CKÜ diskutiert: <http://news.kmib.co.kr/article/view.asp?arcid=0013647817&code=61111211&cp=nv> Abruf: 31. 12. 2020.

OGH, dass der Beschuldigte und sein Verteidiger die Möglichkeit erhalten, an der Suche und Durchsicht und an dem Drucken und Kopieren teilzunehmen. Darüber hinaus sagte er, dass die Verletzung des Teilnahmerechts i. d. R. die gesamte Beschlagnahme und Durchsuchung illegal mache und die hier erlangten Daten nicht als Beweismittel dienen dürfen. Das folgende Formular ist derzeit einem richterlichen Anordnungsbeschluss zur Beschlagnahme und Durchsuchung in Südkorea beigefügt, um die zu beschlagnahmenden Papiere und Daten und die Art und Weise der Durchsuchung zu beschränken.

<Anlage>

Beschränkung von zu beschlagnahmenden Gegenständen und Durchführungsmethoden

1. Beschlagnahme der Papiere

a) Wenn die Papiere eingezogen werden müssen, muss ihr Original beschlagnahmt werden.

b) Wenn die Papiere als Beweismittel dienen werden, muss ihre Kopie beschlagnahmt werden, die unter Hinzuziehung des von der Maßnahme Betroffenen oder des unverdächtigen Inhabers etc.[1)] erstellt wurde; ihr Original darf jedoch beschlagnahmt werden, wenn es unmöglich ist, eine Kopie zu erstellen oder eine Mitwirkung dazu zu fordern, oder wenn das Original selbst erforderlich ist, weil der Beweiswert in der Erscheinungsform, Materialqualität etc. der Papiere besteht.

c) Wenn die Beschlagnahme des Originals nicht fortgesetzt werden muss, muss es unverzüglich nach der Kopie zurückgegeben werden.

2. Beschlagnahme, Durchsuchung und Augenschein elektronischer Daten, die auf einem Speichermedium wie Festplatte gespeichert sind.

a) Durchsuchung und Augenschein elektronischer Daten
Wenn der Untersuchungszweck nur durch Durchsuchung und Augenschein erreicht werden kann, muss nur dies ohne Beschlagnahme durchgeführt werden.

b) Beschlagnahme elektronischer Daten

(1) Grundsatz: Nach Durchsuchung und Augenschein am Ort, wo ein Speichermedium ist, dürfen nur die für den Verdacht relevanten Daten beschlagnahmt werden, indem sie in einem bestimmten Umfang gedruckt oder auf einen von der Ermittlungsbehörde geführten Datenträger kopiert werden.

(2) Fälle, in denen das Speichermedium selbst oder nur die Kopie der darin vorhandenen Daten durch Eins-zu-eins-Kopie oder Imaging der Festplatte etc. mitgenommen werden darf.

(a) Fälle, in denen nur die Kopie der im Speichermedium vorhandenen Daten mitgenommen werden darf.

Nur in Fällen, in denen die grundsätzliche Methode von (1) unmöglich ist oder es wesentlich erschwert wäre, den Zweck der Beschlagnahme zu erreichen,[2)] dürfen Kopien aller Dateien im Speichermedium durch Eins-zu-eins-Kopie oder Imaging der Festplatte etc. nach außen gebracht werden.

(b) Fälle, in denen das Speichermedium selbst mitgenommen werden darf.

1) Nur in Fällen, in denen die Methode von (a) unmöglich ist oder wesentlich erschwert wäre,[3)] kann das Speichermedium selbst unter Hinzuziehung des von der Maßnahme Betroffenen oder des unverdächtigen Inhabers etc. versiegelt und an einen externen Ort gebracht werden.

2) Wenn das Speichermedium selbst gemäß 1) mitgenommen wurde, muss es unter Gewährleistung des Teilnahmerechts des von der Maßnahme

Betroffenen oder des unverdächtigen Inhabers etc. geöffnet und kopiert werden, und danach unverzüglich zurückgegeben werden; dies darf 10 Tage ab dem Datum der Mitnahme nicht überschreiten, es sei denn, es gibt besondere Umstände.

(c) In Fällen von (a) und (b) müssen nur die für den Verdacht relevanten Daten gedruckt oder kopiert werden, und wenn die Daten wiederhergestellt oder analysiert werden müssen, sollte dies in einer Weise erfolgen, dass Zuverlässigkeit und Sachkompetenz garantiert werden.

(3) Vorsichtsmaßnahme

(a) Nachdem die für den Verdacht relevanten Daten gemäß (1) und (2) gesucht und kopiert oder gedruckt wurden, muss dem von der Maßnahme Betroffenen oder dem unverdächtigen Inhaber etc. ① ein Verzeichnis der beschlagnahmten Daten ausgehändigt werden und müssen ② andere Daten gelöscht, vernichtet oder zurückgegeben werden, und dies mitgeteilt werden. Die Mitteilung kann ersetzt werden, indem der Inhalt der Löschung oder Vernichtung im Verzeichnis angegeben wird.

(b) Die Versiegelung und Öffnung können durch eine physische Methode oder eine Passworteinstellung, an der sich die Ermittlungsbehörde und der von der Maßnahme Betroffene oder der unverdächtige Inhaber etc. gemeinsam beteiligen, erfolgen. Bei Erstellung einer Kopie müssen Maßnahmen ergriffen werden, um die Identität mit dem Original zu überprüfen, wie z. B. die Bestätigung des Hashwerts oder das Aufnehmen des Vorgangs der Beschlagnahme und Durchsuchung.

(c) Das Teilnahmerecht muss während des gesamten Prozesses der Beschlagnahme und Durchsuchung (einschließlich der Erhaltung von Kopien, der Suche nach Daten und ihres Kopierens oder Druckens) dem von der Maßnahme Betroffenen oder dem unverdächtigen Inhaber etc. gewährleistet werden. Wenn dieser die Teilnahme verweigert, sollte die Beschlagnahme und Durchsuchung in einer Weise erfolgen, dass Zuverlässigkeit und Sachkompetenz garantiert werden.

[1)] der von der Maßnahme Betroffene – der Beschuldigte und sein Verteidiger, der Eigentümer sowie der Besitzer; der unverdächtigen Inhaber etc. – der Inhaber etc. i. S. d. § 123 K-StPO

[2)] ① wenn der von der Maßnahme Betroffene oder der unverdächtige Inhaber etc. dabei nicht mitwirkt oder seine Mitwirkung nicht erwartet werden kann, ② wenn ein Indiz festgestellt wird, dass die Daten, die wahrscheinlich mit dem Verdacht zusammenhängen, gelöscht oder vernichtet wurden, ③ wenn die Durchführung durch Drucken oder Kopieren die Geschäftstätigkeiten oder die Ruhe der Privatsphäre des Betroffenen etc. beeinträchtigt und ④ in anderen ähnlichen Fällen.

[3)] ① wenn die Durchführung von Eins-zu-eins-Kopie oder Imaging der Festplatte am Ort physisch oder technisch unmöglich oder äußerst schwierig ist, ② wenn eine solche Durchführung die Geschäftstätigkeiten oder die Ruhe der Privatsphäre des Betroffenen etc. erheblich beeinträchtigt und ③ in anderen ähnlichen Fällen.

Kapitel 5

Schlussbemerkung

In der modernen digitalen Gesellschaft bestehen personenbezogene Daten in elektronischer Form, und in der TK werden sowohl ihre Inhaltsdaten als auch ihre Verkehrsdaten automatisch erstellt und auf den informationstechnischen Systemen kumulativ und unbegrenzt angesammelt und konzentriert. Sie sollten einerseits grundrechtlich geschützt werden, andererseits auch strafrechtlich verwendet werden können. In der heutigen IT-Umgebung birgt die Beweissicherung durch die Ermittlungsbehörde – insb. mit technischen Mitteln – jedoch immer die Gefahr in sich, dass sie zu einer umfassenden Erfassung personenbezogener Daten und zu einer Erstellung von Persönlichkeits- und Bewegungsprofilen führt. Dies steht im Widerspruch zu einer verfassungsrechtlichen Forderung nach Persönlichkeitsschutz durch Datenschutz. Die Beweissicherung im Ermittlungsverfahren ist auch i. R. d. Rechtsstaatsprinzips zulässig, und ihre Ermächtigungsnormen, nämlich Eingriffsvoraussetzungen und verfahrensrechtliche Vorkehrungen, müssen nach den Grundsätzen der Normenklarheit und Verhältnismäßigkeit sorgfältig ausgestaltet werden. Im Rechtsstaat sollten die Erfassung personenbezogener Daten zum Zwecke der Strafverfolgung und deren Kontrolle zum Zwecke des Grundrechtsschutzes aufgrund der Interessenabwägung ausbalanciert werden, und dieser Ausgleich sollte zur Anpassung der Veränderungen in der Realität kontinuierlich aktualisiert werden. Der Gesetzgeber hat neue Ermittlungsmaßnahmen zu legalisieren, wenn diese für die Verwirklichung der funktionstüchtigen Strafrechtspflege erforderlich ist, dabei zugleich aber auch sicherzustellen, dass maßgebliche Grundrechte effektiv durch die verfahrensrechtliche Sicherungen geschützt werden, die die Eingriffsintensität der Maßnahmen ausgleichen können, und weiter die Wirksamkeit der vorgesehenen Schutzmechanismen fortwährend zu überprüfen. Diese Aktualisierung geht von der Bemessung bzw. Festlegung der Eingriffsintensität der zuzulassenden Maßnahme aus, und insoweit ist für die Ermächtigungsnormen zur Beweissicherung im Ermittlungsverfahren heute die Entwicklung der IuK-Technologie von entscheidender Bedeutung, die die Heimlichkeit der Maßnahme und die umfassende Datenerhebung ermöglicht. Zum anderen handelt es sich beim Grundrechtsschutz hinsichtlich der Rechtsstaatlichkeit um die volle Wahrung der Justizförmigkeit, und dazu ist in erster Linie das Eingreifen des Gerichtes ins Vorverfahren von Bedeutung, aber auch die Teilnahme des Beschuldigten und seines Verteidigers ist eindeutig erforderlich, auch wenn sie begrenzt ist.

Der deutsche Gesetzgeber reagiert in den letzten 20 Jahren durch ständige Revisionen der StPO auf Fortschritte der IT. Auf diese Entwicklung hat u. a. das *BVerfG*

durch seine Entscheidungen einen großen Einfluss. Es unterteilt heimliche Ermittlungsmaßnahmen mit technischen Mitteln, um personenbezogene Daten zu erheben, je nach Art und Weise ihrer Durchführung und verlangen, dass Eingriffsvoraussetzungen und verfahrensrechtliche Vorkehrungen jeder Ermächtigungsnorm im Verhältnis zu ihrer Eingriffsintensität individuell auszugestalten sind. Demzufolge sind die verdeckten Maßnahmen nach §§ 99 ff. StPO i. d. R. mit strengeren Eingriffsschwellen und Vorkehrungen verbunden als bei der allgemeinen Beschlagnahme und Durchsuchung nach §§ 94 ff., 102 ff. StPO. Natürlich macht jede eigenständige Ermächtigung die Tätigkeit der Ermittlungsbehörde teilweise umständlich, aber dies trägt zur Ausübung der Ermittlungsrechte nach Verhältnismäßigkeit bei, was in der Praxis leicht übersehen wird. Dies gilt umso mehr, als unter heutigen technischen Gegebenheiten technische Ausspähungsmethoden stets zu einem unverhältnismäßigen Eingriff in die Grundrechte führen können. Vor diesem Hintergrund ist die Legitimierung der Online-Durchsuchung für Strafverfolgungszwecke aus dem Jahr 2017 fragwürdig, einerseits da sie eine Rundum- od. Totalüberwachung leicht ermöglicht, andererseits da andere bestehende Maßnahmen wie TKÜ, akustische Wohnraumüberwachung etc. angesichts des technischen Niveaus bereits sowohl eine umfassende Datenerfassung als auch eine beträchtliche Persönlichkeitsverletzung ermöglichen. Die Einführung dieser Maßnahmen in das Ermittlungsverfahren lässt die Grenze zwischen der Strafverfolgung und der präventivpolizeilichen Aufgabe verschwimmen und stellt den liberalen Rechtsstaat vor ernste Gefahren (vgl. *Roxin/Schünemann*, § 2 Rn. 8).

Andererseits ist ein übermäßiger Eingriff in die Persönlichkeit durch umfassende Datenerfassung auch bei der einfachen Beschlagnahme und Durchsuchung nach den allgemeinen Vorschriften ein zentrales Thema. Dies liegt daran, dass die Ermittlungsbehörde mit nur einem Zugriff auf den PC oder das Smartphone des Einzelnen so viele Daten erhält, dass sie ein Persönlichkeitsprofil erstellen kann. Diese Maßnahme ist, auch wenn sie öffentlich durchgeführt wird, de facto dieselbe wie die TKÜ und ggf. die Online-Durchsuchung. Das heißt, die Ermittlungsbehörde kann durch die einfache Beschlagnahme und Durchsuchung, die aufgrund der allgemeinen Vorschriften, die nur einen mittelmäßigen Grundrechtseingriff rechtfertigen, angeordnet wurde, mit hoher Wahrscheinlichkeit auf Daten zugreifen, die zu den kernbereichsrelevanten, beschlagnahmefreien oder verfahrensirrelevanten Informationen gehören, aber es ist fraglich, ob die verfahrensrechtlichen Vorkehrungen diesbezüglich verhältnismäßig ausgestaltet sind. Natürlich hat das *BVerfG* in seinen Entscheidungen wiederholt erklärt, dass dies kein Problem sei. In der Praxis wird jedoch die Kontrollfunktion des Richtervorbehalts nicht voll verwirklicht und auch die Beschränkung des Umfangs der Beschlagnahme durch die Anwendung von § 110 StPO wird häufig umgangen. Angesichts der Nutzung informationstechnischer Systeme durch die Bürger müssen die Handlungen der Behörde, die auf die Systeme zugreifen, um die dort gespeicherten Daten umfassend zu sichern, praktisch auf angemessener Ebene kontrolliert werden können. Insofern werden neben gerichtlicher Kontrolle auch institutionelle und rechtliche Vorkehrungen gefordert, die die

Möglichkeit des Eingreifens des Beschuldigten und seines Verteidigers in die Beschlagnahme und Beschlagnahme gewährleisten, um eindeutig rechtswidrige Handlungen der Ermittlungsbehörde zu verhindern und den untergeordneten Status des Beschuldigten zu stärken, auch wenn dies nur in begrenzten Fällen zulässig ist.

Die Ermächtigungsgrundlagen zur Beweissicherung im Vorverfahren sind auch in Südkorea in die allgemeinen Vorschriften zur Beschlagnahme und Durchsuchung sowie die Vorschriften für heimliche Ermittlungsmaßnahmen wie TKÜ, Verkehrsdatenerhebung, Gesprächsüberwachung etc. unterteilt. Letztere werden vom K-KGSG als Sondergesetz geregelt. Das Gesetz hat jedoch mehrere Mängel bezüglich der Normenklarheit und Verhältnismäßigkeit. Vor allem sind Beschwerdemöglichkeiten über die Rechtswidrigkeit der Durchführung jeder Maßnahme sehr begrenzt. Eine Benachrichtigung des von der Maßnahme Betroffenen kann nicht nur i. d. R. erst nach dem Beschluss bezüglich der öffentlichen Klage erfolgen, sondern auch die Prüfung ihrer Rechtswidrigkeit kann nur indirekt durch den Ausschluss von illegal erlangten Beweisen in der Hauptverhandlung erfolgen. Das ist eine wichtige legislative Lücke hinsichtlich des effektiven Rechtsschutzes. Auf der anderen Seite sollte die Einführung allgemeiner Ermächtigungsvorschriften zu heimlichen Ermittlungsmaßnahmen, die vom K-KGSG nicht gedeckt werden, aber durch Datenerfassung oder Verhaltensbeobachtung mittels technischer Mittel nicht geringfügig in die Grundrechte des Betroffenen eingreifen, wie z. B. der Einsatz eines (eigenständigen) GPS-Trackers oder von Drohnen, in Betracht gezogen werden. Da das K-KGSG nur eine begrenzte Art der verdeckten Ermittlungen rechtfertigt, werden andere Maßnahmen oft nach Ermessen der Ermittlungsbehörde ohne Intervention des Richters getroffen, oder sie können ggf. nur auf den allgemeinen Vorschriften der Beschlagnahme und Durchsuchung beruhen. Dies widerspricht dem rechtsstaatlichen Grundsatz der Verhältnismäßigkeit. Derzeit schreitet die gesetzgeberische Verbesserung verdeckter Ermittlungsmaßnahmen in Südkorea nur langsam voran, was größtenteils auf den Widerstand des Justizministeriums, der Ermittlungsbehörden und der Geheimdienste zurückzuführen ist. Freilich kann dies angesichts der Konfrontation zwischen Süd- und Nordkorea im Bereich der Staatssicherheit teilweise berechtigt sein, aber nicht in anderen Bereichen. Vor allem ist die Verfahrenskontrolle bei den heimlichen Ermittlungsmaßnahmen insgesamt zu locker.

Andererseits ist klar, dass auch bei der Beschlagnahme und Durchsuchung elektronischer Daten nur verfahrensrelevante Daten beschlagnahmt werden müssen. In dieser Hinsicht tragen die Einführung des Ausschlussprinzips von 2007 und die relativ strengen Entscheidungen vom *K-OGH* dazu derzeit erheblich zur Kontrolle von Verfahrensverstößen und zur Beschränkung der umfassenden Datenerhebung im Zuge der Ermittlungen bei. Insbesondere nach der ständigen Rspr. des *K-OGH* kann auch eine Durchführungsmethode der Beschlagnahme und Durchsuchung, die nicht klar im Gesetz festgelegt ist, durch die Anordnung eines Richters gerechtfertigt werden, und weiter können die Verstöße gegen den Inhalt des Anordnungsbeschlusses zu einem Ausschluss der Beweisfähigkeit führen. Daher ist die Einhaltung der Vorschriften der K-StPO und des richterlichen Anordnungsbeschlusses bei der

Beschlagnahme und Durchsuchung in Südkorea von erheblicher Bedeutung. Diesbezüglich ist jüngst in der Literatur und Rspr. am umstrittensten, ob die Netzwerkdurchsuchung, insb. die grenzüberschreitende Durchsuchung, zulässig ist und inwieweit die Teilnahme an der Durchsicht zur Beschlagnahme verfahrensrelevanter Daten zulässig ist. Im ersteren Fall entschied der *K-OGH*, dass eine solche Art der Durchsuchung aufgrund von § 120 K-StPO und eines richterlichen Anordnungsbeschlusses zulässig sein kann, und im letzteren Fall betont er, dass das Recht auf Teilnahme am gesamten Prozess der Beschlagnahme und Durchsuchung dem Beschuldigten und seinem Verteidiger gewährleistet wird.

Seit der Befestigung des liberal-rechtstaatlichen Strafverfahrens sind Eingriffe in die Grundrechte in Ermittlungsverfahren und ihre Einschränkungen in allen Ländern ein sensibles Thema und stehen im Zentrum der Diskussion des Strafverfahrensrechts. Angesichts der Entwicklung der IuK-Technologie zeigt sich, wie wichtig der Persönlichkeitsschutz durch den Datenschutz ist, und es stellen sich weiterhin die Fragen, unter welchen Eingriffsschwellen bzw. -voraussetzungen die in die Grundrechte – intensiv – eingreifenden Maßnahmen anzuordnen sind und welcher Verfahrenskontrolle sie unterliegen sollten. Der konkrete Inhalt jeder Ermächtigungsgrundlage hängt freilich im Wesentlichen von den politischen Entscheidungen jeder Gemeinschaft ab. Sie muss jedoch in rechtsstaatlicher Hinsicht normenklar und verhältnismäßig ausgestaltet und als solche weiter ausgelegt und angewendet werden. Um mit der Entwicklung der Informationstechnologie Schritt zu halten, müssen einerseits neue Untersuchungsmethoden bzw. Interpretationen gerechtfertigt werden, andererseits müssen auch Verfahrenskontrollen zur Verhinderung übermäßiger Persönlichkeitsverletzung gewährleistet werden.

Literaturverzeichnis

I. Deutschland

1. Kommentare & Monografien

Amelung, Knut, Rechtsschutz gegen strafprozessuale Grundrechtseingriffe, Duncker & Humblot, Berlin 1976. (Zitiert: *Amelung*, Rechtsschutz, S. …)

Bär, Wolfgang, Handbuch zur EDV-Beweissicherung im Strafverfahren, Richard Boorberg, 2007. (Zitiert: *Bär*, EDV-Beweissicherung, Rn. …)

Ciolek-Krepold, Katja, Durchsuchung und Beschlagnahme in Wirtschaftsstrafsachen, NJW-Schriftenreihe Band 68, C. H. Beck, München 2000. (Zitiert: *Ciolek-Krepold*, Rn. …)

Epping/Hillgruber (Hrsg.), Beck'scher OK GG, 25/. Edition, 01. 06. 2015/30/. Edition, 01. 03. 2015/32/. Edition, 01. 03. 2017. (Zitiert: *Bearbeiter*, in: Epping/Hillgruber, BeckOK GG, Art. … Rn. …)

Hannich, Rolf (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung mit GVG, EGGVG und EMRK, 8. Auflage, C. H. Beck, München 2019. (Zitiert: *Bearbeiter*, KK-StPO, § … Rn. …)

Isensee, Josef/*Kirchhof*, Paul (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, Band II Verfassungsstaat, 3. Auflage, C. F. Müller, Heidelberg 2004. (Zitiert: *Bearbeiter*, in: Isensee/Kirchhof, HStR II, § … Rn. …)

Knauer/Kudlich/Schneider (Hrsg.), Münchener Kommentar zur Strafprozessordnung, 1. Auflage, 2014. (Zitiert: *Bearbeiter*, MüKo-StPO, § … Rn. …)

Maunz/Dürig (Hrsg.), Grundgesetz-Kommentar, 77. EL, Juli 2016/74. EL, Mai 2015. (Zitiert: *Bearbeiter*, in: Maunz/Dürig, GG-K, Art. … Rn. …)

Meininghaus, Florian, Der Zugriff auf E-Mails im strafrechtlichen Ermittlungsverfahren, Kovač, Hamburg 2007. (Zitiert: *Meininghaus*, Der Zugriff auf E-Mails, S. …)

Meyer-Goßner, Lutz/*Schmitt*, Bertram, Strafprozessordnung mit GVG, Nebengesetze und ergänzende Bestimmungen, Kommentar, 60. bis 62. Auflage, C. H. Beck, München 2017 bis 2019. (Zitiert: M-G/*Schmitt*, StPO, § … Rn. …)

Park, Tido, Durchsuchung und Beschlagnahme, 3. Auflage, C. H. Beck, München 2015. (Zitiert: *Park*, § … Rn. …)

Roxin, Claus/*Schünemann*, Bernd, Strafverfahrensrecht, 29. Auflage, C. H. Beck, München 2017. (Zitiert: *Roxin*/*Schünemann*, § … Rn. …)

Rzepka, Dorothea, Zur Fairness im Deutschen Strafverfahren, Vittorio Klostermann, Frankfurt a. M., 2000.

Schmidt-Bleibtreu/Hofmann/Henneke (Hrsg.), Kommentar zum Grundgesetz, 13. Auflage, 2014. (Zitiert: *Bearbeiter*, in: Schmidt-Bleibtreu/Hofmann/Henneke, K zum GG, Art. … Rn. …)

Sieber, Ulrich, Straftaten und Strafverfolgung im Internet, Gutachten C zum 69. Deutschen Juristentag, C. H. Beck, München 2012. (Zitiert: *Sieber*, 69. DJT 2012, C …)

Sodan, Helge (Hrsg.), Grundgesetz, C. H. Beck, München 2009. (Zitiert: *Sodan*, GG, Art. … Rn. …)

Vogelgesang, Klaus, Grundrecht auf informationelle Selbstbestimmung?, Nomos, Baden-Baden 1987.

Volk, Klaus/*Engländer*, Armin, Grundkurs StPO, 9. Auflage, C. H. Beck, München 2018. (Zitiert: *Volk*/*Engländer*, § … Rn. …)

Wolter, Jürgen (Hrsg.), SK-StPO, 5. Auflage, Carl Heymanns, Köln 2016. (Zitiert: *Bearbeiter*, SK-StPO, § … Rn. …)

2. Aufsätze

Amelung, Knut, Grundfragen der Verwertungsverbote bei beweissichernden Haussuchungen im Strafverfahren, NJW 1991, S. 2533.

Bär, Wolfgang, BGH-Ermittlungsrichter: Sicherstellung von Datenträgern mit Anmerkung, CR 1999, S. 292.

Bär, Wolfgang, Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen Gesetzliche Neuregelungen zum 1. 1. 2008, MMR, 2008, S. 215.

Bär, Wolfgang, Beschlagnahme von E-Mails beim Provider – BGH, Beschluss vom 31. 3. 2009 – 1 StR 76/09 mit Anmerkung, NStZ 2009, S. 397.

Bär, Wolfgang, Die Neuregelung des § 100j StPO zur Bestandsdatenauskunft – Auswirkungen auf die Praxis der Strafverfolgung, MMR 2013, S. 700.

Bäumerlich, Maik, Verschlüsselte Smartphones als Herausforderung für die Strafverfolgung – Neue Technologie, alte Befugnisse, NJW 2017, S. 2718.

Beukelmann, Stephan, Online-Durchsuchung und Quellen-TKÜ, NJW-Spezial 2017, S. 440.

Bittmann, Folker, Das Beiziehen von Kontounterlagen im staatsanwaltschaftlichen Ermittlungsverfahren, wistra 9/1990, S. 325.

Blechschmitt, Lisa, Strafverfolgung im digitalen Zeitalter – Auswirkungen des stetigen Datenaustauschs auf das strafrechtliche Ermittlungsverfahren, MMR 2018, S. 361.

Brodowski, Dominik, Strafprozessualer Zugriff auf E-Mail-Kommunikation – zugleich Besprechung zu BVerfG, Beschl. vom 16. 6. 2009 – 2 BvR 902/06 sowie zu BGH, Beschl. vom 31. 3. 2009 – 1 StR 76/09 –, JR 10/2009, S. 402.

Brodowski, Dominik/*Eisenmenger*, Florian, Zugriff auf Cloud-Speicher und Internetdienste durch Ermittlungsbehörden – Sachliche und zeitliche Reichweiter der „kleinen Online-Durchsuchung" nach § 110 Abs. 3 StPO, ZD 3/2014, S. 119.

Brunst, Phillip W., *BVerfG:* Sicherstellung und Beschlagnahme von Mails auf dem Mailserver mit Anmerkung, CR 9/2009, S. 584.

Burhoff, Detlef, Durchsuchung und Beschlagnahme – Bestandsaufnahme zur obergerichtlichen Rechtsprechung, StraFo 4/2005, S. 140.

Cordes, Malte/*Pannenborg*, Eerke: Strafprozessuale und verfassungsrechtliche Grenzen im Umgang mit Zufallsfunden, NJW 2019, S. 2973.

Cornelius, Kai, Cloud-Computing für Berufsgeheimnisträger, StV 2016, S. 380.

Dalby, Jakob, Das neue Auskunftsverfahren nach § 113 TKG – Zeitdruck macht Gesetze – Eine Beurteilung der Änderung des manuellen Auskunftsverfahrens und der Neuschaffung des § 100j StPO, CR 6/2013, 361.

Dauster, Manfred, Betroffenheit in der Vertraulichkeitssphäre, polizeiliche „venia legendi" aufgrund richterlicher Beschlagnahmeanordnung und die Restriktionen des § 110 StPO, StraFo Juni 1999, S. 186.

Freiling, Felix/*Safferling*, Christoph/*Rückert*, Christian, Quellen-TKÜ und Online-Durchsuchung als neue Maßnahmen für die Strafverfolgung: Rechtliche und technische Herausforderungen, JR 2018, S. 9.

Gercke, Marco, Die Entwicklung des Internetstrafrechts 2015/2016, ZUM 2016, S. 825.

Glock, Stefan, Unterlagen, deren richterliche Beschlagnahme noch nicht angeordnet oder bestätigt wurde, dürfen seitens der Ermittlungsbehörden nicht verwendet werden, NStZ 2019, S. 248.

Graulich, Volker, Die Sicherstellung von während einer Durchsuchung aufgefunden Gegenständen – Beispiel Steuerstrafverfahren, wistra 8/2009, S. 299.

Gurlit, Elke, Verfassungsrechtliche Rahmenbedingungen des Datenschutzes, NJW 2010, S. 1035.

Hamm, Rainer, Der Einsatz heimlicher Ermittlungsmethoden und der Anspruch auf ein faires Verfahren, StV 2001, S. 81.

Hamm, Rainer, Unzulässigkeit einer „verdeckten Online-Durchsuchung" – BGH, Beschluss vom 31. 1. 2007 – StB 18/06 mit Anmerkung, NJW 2007, S. 930.

Hamm, Rainer, Der Verteidiger als Garant der Einhaltung von strafprozessualen Verfahrensregeln?, StV 2010, S. 418.

Hassemer, Winfried, Die „Funktionstüchtigkeit der Strafrechtspflege" – ein neuer Rechtsbegriff?, StV 1982, S. 275.

Heckmann, Dirk, Persönlichkeitsschutz im Internet – Anonymität der IT-Nutzung und permanente Datenverknüpfung als Herausforderungen für Ehrschutz und Profilschutz, NJW 2012, S. 2631.

Heinlich, Jens, Die Durchsuchung in Wirtschaftsstrafverfahren, wistra 6/2017, 219.

Herrmann, Klaus/*Soiné*, Michael, Durchsuchung persönlicher Datenspeicher und Grundrechtsschutz, NJW 2011, S. 2922.

Hiéramente, Mayeul, Durchsuchung und „Durchsicht" der Unternehmens-IT – Betrachtungen zu §§ 103, 110 StPO, wistra 11/2016, S. 432.

Hofmann, Manfred, Die Online-Durchsuchung – staatliches „Hacken" oder zulässige Ermittlungsmaßnahme?, NStZ 2005, S. 121.

Kasiske, Peter, Neues zur Beschlagnahme von E-Mails beim Provider – Besprechung von BGH 1 StR 76/09 und BVerfG 2 BvR 902/06, StraFo 6/2010, S. 228.

Kemper, Martin, Die Beschlagnahmefähigkeit von Daten und E-Mails, NStZ 2005, S. 538.

Kemper, Martin, Die Beschlagnahme von Beweisgegenständen bei fehlender Beschlagnahmeanordnung, wistra 5/2006, S. 171.

Kemper, Martin, Die Beschlagnahmeverzeichnis nach § 109 stopp in Wirtschafts- und Steuerstrafverfahren, wistra 3/2008, S. 96.

Kemper, Martin, Die „Mitnahme zur Durchsicht" – Ein vom Gesetz nicht vorgesehenes Instrument zur Sicherstellung von Beweismitteln?, wistra 8/2010, S. 295.

Klein, Oliver, Offen und (deshalb) einfach – Zur Sicherstellung und Beschlagnahme von E-Mails beim Provider, NJW 2009, S. 2996.

Klesczewski, Diethelm, Straftataufklärung im Internet – Technische Möglichkeiten und rechtliche Grenzen von strafprozessualen Ermittlungseingriffen im Internet, ZStW 123 (2011), S. 737.

Klinger, Peter M., Die Zuständigkeit der Staatsanwaltschaft für Maßnahmen nach § 95 StPO, wistra 1/1991, S. 17.

Knauer, Christoph/*Wolf*, Christian, Zivilprozessuale und strafprozessuale Änderungen durch das Erste JuMoG – Teil 2: Änderungen der StPO, NJW 2004, S. 2932.

Krekeler, Wilhelm, Beweisverwertungsverbot bei fehlerhaften Durchsuchungen, NStZ 1993, S. 263.

Kudlich, Hans, Der heimliche Zugriff auf Daten in einer Mailbox: ein Fall der Überwachung des Fernmeldeverkehrs? – BGH, NJW 1997, 1934, JuS 1998, S. 209.

Kudlich, Hans, Strafverfolgung im Internet: Bestandsaufnahme und aktuelle Probleme – Zur 34. Strafrechtslehrertagung 2011 in Leipzig, GA 2011, S. 193.

Kudlich, Hans, Straftaten und Strafverfolgung im Internet – Zum strafrechtlichen Gutachten für den 69. DJT 2012 –, StV 2012, S. 560.

Kutscha, Martin, Rechtsschutzdefizite bei Grundrechtseingriffen von Sicherheitsbehörden, NVwZ 2003, S. 1296.

Kutscha, Martin, Mehr Schutz von Computerdaten durch ein neues Grundrecht?, NJW 2008, S. 1042.

Kutscha, Martin, Überwachungsmaßnahmen von Sicherheitsbehörden im Fokus der Grundrechte, LKV 2008, S. 481.

Landau, Herbert, Die Pflicht des Staates zum Erhalt einer funktionstüchtigen Strafrechtspflege, NStZ, 2007, S. 121.

Löffelmann, Markus, Der Rechtsschutz gegen Ermittlungsmaßnahmen, StV 2009, S. 379.

Meinicke, Dirk, Beschlagnahme eines Nutzerkontos bei Facebook, StV 2012, S. 462.

Michalke, Reinhart, Durchsuchung und Beschlagnahme – Verfassungsrecht im Alltag, StraFo 3/2014, S. 89.

Mildeberger, Tobias/*Riveiro*, Karen A., Zur Durchsicht von Papieren gem. § 110 StPO, StraFo Februar 2004, S. 43.

Moldenhauer, Gerwin/*Wenske*, Marc, Aktuelle Entwicklungen der Rechtsprechung zur Gefahr in Verzug, JA 3/2017, S. 206.

Neuhöfer, Daniel, AG Reutlingen: Beschlagnahme von Facebook-Daten mit Anmerkung, ZD 4/2014, S. 178.

Neuhöfer, Daniel, Soziale Netzwerke: Private Nachrichteninhalte im Strafverfahren – Der strafprozessuale Zugriff auf Inhalte privater Nachrichten bei Facebook & Co., JR 2015, S. 21.

Niedernhuber, Tanja, Die StPO-Reform 2017 – wichtige Änderungen im Überblick, JA 3/2018, S. 169.

Obenhaus, Nils, Cloud Computing als neue Herausforderung für Strafverfolgungsbehörden und Rechtsanwaltschaft, NJW 2010, S. 651.

Paeffgen, Hans-Ullrich, Überlegungen zu einer Reform des Rechts der Überwachung der Telekommunikation, in: Festschrift für Claus Roxin zum 70. Geburtstag am 15. Mai 2001, S. 1299.

Papier, Hans-Jürgen, Rechtsstaatlichkeit und Grundrechtsschutz in der digitalen Gesellschaft, NJW 2017, S. 3025.

Peters, Kristina, Anwesenheitsrechte bei der Durchsicht gemäß § 110 StPO: Bekämpfung der Risiken und Nebenwirkungen einer übermächtigen Ermittlungsmaßnahme, NZWiSt 2017, 465.

Rieß, Peter, Die „Straftat von erheblicher Bedeutung" als Eingriffsvoraussetzung – Versuch einer Inhaltsbestimmung, GA 2004, S. 623.

Roggan, Fredrik, Die „Technikoffenheit" von strafprozessualen Ermittlungsbefugnissen und ihre Grenzen – Die Problematik der Auslegung von Gesetzen über ihren Wortlaut oder Wortsinn hinaus, NJW 2015, S. 1995.

Roggan, Fredrik, Die strafprozessuale Quellen-TKÜ und Online-Durchsuchung: Elektronische Überwachungsmaßnahmen mit Risiken für Beschuldigte und die Allgemeinheit, StV 2017, S. 821.

Roxin, Claus, Zur richterlichen Kontrolle von Durchsuchungen und Beschlagnahmen, StV 1997, S. 654.

Schertz, Christian, Der Schutz des Individuums in der modernen Mediengesellschaft, NJW 2013, S. 721.

Schlegel, Stephan, „Beschlagnahme" von E-Mail-Verkehr beim Provider – Zugleich Besprechung zu BVerfG 2 BvR 902/06 vom 29. 6. 2006, HRRS 2/2007, S. 44.

Schlegel, Stephan, „Online-Durchsuchung light" – Die Änderung des § 110 StPO durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung, HRRS Januar 2008, S. 23.

Schünemann, Bernd, Wohin treibt der deutsche Strafprozess?, ZStW 114 (2002), S. 1.

Simitis, Spiros, Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung, NJW 1984, S. 398.

Singelnstein, Tobias, Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co, NStZ 2012, S. 593.

Singelnstein, Tobias/*Derin*, Benjamin, Das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens – Was aus der StPO-Reform geworden ist, NJW 2017, S. 2646.

Soiné, Michael, Personale verdeckte Ermittlungen in sozialen Netzwerken zur Strafverfolgung, NStZ 2014, S. 248.

Soiné, Michael, Die strafprozessuale Online-Durchsuchung, NStZ 2018, S. 497.

Sommermeyer, Jörg, Neuralgische Aspekte der Betroffenenrechte und ihres Rechtsschutzes bei strafprozessualen Hausdurchsuchungen, NStZ 1991, S. 257.

Stadler, Thomas, Der Richtervorbehalt – ein stumpfes Schwert oder ein rechtsstaatlich gebotenes Instrument?, ZRP 2013, S. 179.

Szesny, André-M., Durchsicht von Daten gem. § 110 StPO, WiJ 2012, S. 228.

Vogel, Joachim, Informationstechnologische Herausforderungen an das Strafprozessrecht, ZIS 2012, S. 480.

Vogelgesang, Klaus, Verfassungsregelungen zum Datenschutz, CR 1995, S. 554.

Wicker, Magda, Durchsuchung in der Cloud Nutzung von Cloud-Speichern und der strafprozessuale Zugriff deutscher Ermittlungsbehörden, MMR 2013, S. 765.

Zerbes, Ingeborg/*El-Ghazi*, Mohamad, Zugriff auf Computer: Von der gegenständlichen zur virtuellen Durchsuchung, NStZ 2015, S. 425.

Zimmermann, Till, Der strafprozessuale Zugriff auf E-Mails, JA 5/2014, S. 321.

II. Südkorea

1. Kommentare & Monografien

Cho, Kuk, Das Prinzip des Ausschlusses von illegal erlangten Beweisen, 2. Auflage, Pakyoungsa, Seoul 2017. (Zitiert: *Kuk Cho*, Ausschlussprinzip, S. …) [조국, 위법수집증거배제법칙, 전면개정판, 박영사, 2017]

Kim, Hee-Ok/*Park*, Il-Hwan (Hrsg.), Kommentar K-StPO (I)/(II), 5. Auflage, Korean Association of Justice and Administration, Seoul 2017. (Zitiert: *Bearbeiter*, KoK-StPO (I)/(II), § … S. …) [김희옥/박일환(편집대표), 주석형사소송법(I)/(II), 제5판, 한국사법행정학회, 2017]

Lee, Jae-Sang, Neue Strafprozessordnung, 2. Auflage, Pakyoungsa, Seoul 2008. (Zitiert: *Jae-Sang Lee*, K-StPO, S. …) [이재상, 신형사소송법, 제2판, 박영사, 2008]

Lee, Jae-Sang/*Cho*, Kyun-Seok, Strafprozessordnung, 12. Auflage, Pakyoungsa, Seoul 2019. (Zitiert: *Lee*/*Cho*, K-StPO, § … Rn. …) [이재상/조균석, 형사소송법, 제12판, 박영사, 2019]

Lee, Sookyeon, Handhabung und Beweisfähigkeit digitaler Daten in Strafverfahren, Dissertation, Korea Uni., 2010. (Zitiert: *Sookyeon Lee*, Digitale Daten, S. …) [이숙연, 형사절차에서의디지털증거의취급과증거능력, 박사학위논문, 고려대학교, 2010]

Park, Sang-Gi/*Tak*, Hee-Sung, Freiwilligkeit und Beweisfähigkeit von Geständnissen, Korean Institute of Criminology, Seoul 1997. (Zitiert: *Park*/*Tak*, Beweisfähigkeit von Geständnissen, S. …) [박상기/탁희성, 자백의임의성과증거능력에관한연구, 형사정책연구원연구총서, 1997]

Rhee, Joo-Won, Strafprozessordnung, 2. Auflage, Pakyoungsa, Seoul 2020. (Zitiert: *Joo-Won Rhee*, K-StPO, S. …) [이주원, 형사소송법, 제2판, 박영사, 2020]

Son, Ji-Young/*Kim*, Joo-Seok, Forschungen zur Verbesserung der Durchsuchungs- und Beschlagnahmeverfahren, Judicial Policy Research Institute, 2016. (Zitiert: *Son/Kim*, Durchsuchungs- und Beschlagnahmeverfahren, S. …) [손지영/김주석, 압수수색절차의개선방안에관한연구, 대법원사법정책연구원, 2016]

Sung, Nak-In, Verfassungsrecht, 20. Auflage, Bobmunsa, Seoul 2020. (Zitiert: *Nak-In Sung*, K-Verfassungsrecht, S. …) [성낙인, 헌법학, 제20판, 법문사, 2020]

2. Aufsätze

Cha, Jina, Effektive Vorgehen gegen Cyberkriminalität und grundrechtlicher Schutz des Fernmeldegeheimnisses, Public Law Journal (PLJ), Band 14, Nr. 1, 2013, S. 39. [차진아, 사이버범죄에대한실효적대응과헌법상통신의비밀보장, 「공법학연구」, 제14권제1호, 2013, 39쪽]

Cha, Jina, Betrachtung über die Verfassungsmäßigkeit von § 13 Abs. 1 und Abs. 2 etc. K-KGSG, Korean Lawyers Association Journal (KLAJ), Band 66, Nr. 4, 2017, S. 237. [차진아, 통신비밀보호법 제13조 제1항 및 제2항 등의 합헌성 여부에 대한 검토, 「법조」, 제66권 제4호, 2017, 237쪽]

Cha, Jina, Probleme der Erhebung von Verkehrsdaten zu Ermittlungszwecken und Richtung der Änderung des K-KGSG, Korean Lawyers Association Journal (KLAJ), Band 67, Nr. 2, 2018, S. 366. [차진아, 범죄수사를위한통신사실확인자료제공요청의문제점과개선방안, 「법조」, 제67권 제2호, 2018, 366쪽]

Cha, Jong-Jin, Zulässigkeit des Zugriffs auf räumlich getrennte E-Mail-Server, Korean Journal of Comparative Criminal Law (KJCCL), Band 21, Nr. 2, 2019, S. 149. [차종진, 이메일원격지압수수색의적법성에관한소고, 「비교형사법연구」, 제21권제2호, 2019, 149쪽]

Cha, Young-Seok, Fakultative Ermittlungen und Zwangsmaßnahmen, Die Welt von Staatsexamen, 1988/2, S. 14. [차용석, 임의수사와강제수사, 「고시계」, 1988/2, 14쪽]

Cho, Gi-Yeong, Richtung der Reformen des K-KGSG i.R.d. jüngsten hauptsächlichen Streitpunkte, Journal of Criminal Law (JCL), Band 26, Nr. 4, 2014, S. 105. [조기영, 최근주요쟁점과관련한통신비밀보호법개정방향, 「형사법연구」, 제26권제4호, 2014, 105쪽]

Cho, Kuk, Bedeutungen, Grenzen und Streitpunkte des überarbeiteten K-KGSG, Korean Criminological Review (KCR), Band 15, Nr. 4, 2004, S. 103. [조국, 개정통비법의의의, 한계및쟁점, 「형사정책연구」, 제15권제4호, 2004, 103쪽]

Cho, Kuk, Erforderlichkeit, Grundlage und Kriterien diskretionären Ausschlusses von illegal erlangten Beweisen, Seoul Law Journal (SLJ), Band 45, Nr. 2, 2004, S. 43. [조국, 재량적위법수집증거배제의필요성, 근거및기준, 서울대학교「법학」, 제45권제2호, 2004, 43쪽]

Cho, Kuk, Rechtsstatus und Ausdehnung des verankerten Ausschlussprinzips, Juris, Nr. 3, 2008, S. 198. [조국, 위법수집증거배제법칙재론, 「사법」, 제3호, 2008, 198쪽]

Cho, Kuk, Exegetische Auseinandersetzungen mit der Durchsuchung und Beschlagnahme von Computerdaten, Korean Journal of Criminology (KJC), Band 22, Nr. 1, 2010, S. 99. [조국, 컴퓨터전자기록에대한대물적강제처분의해석론적쟁점, 「형사정책」, 제22권제1호, 2010, 99쪽]

Choi, Daeho, Legitimation der Positionsverfolgung durch GPS zum Ermittlungszweck, Kyungpook National Uni. Law Journal (KNULJ), Band 62, 2018, S. 213. [최대호, 수사목적GPS 위치추적의적법성, 경북대학교「법학논고」, 제62집, 2018, 213쪽]

Chun, Seungsoo, Die praktischen Probleme bezüglich der Relevanz im Prozess der Durchsuchung und Beschlagnahme, Contemporary Review of Criminal Law (CRCL), Nr. 49, 2015, S. 37. [전승수, 압수수색상관련성의실무상문제점, 「형사법의신동향」, 제49호, 2015, 37쪽]

Chung, Jin-Yeon, Bearbeitung des Gesetzentwurfs des Strafprozesses, Soongsil Law Review (SLR), Band 18, 2007, S. 73. [정진연, 형사소송관련법률개정안에대한제검토, 숭실대학교「법학논총」, 제18집, 2007, 73쪽]

Chung, Soung-Jin, Vorermittlung als Strafverfahren, Kookmin Law Review (KLR), Nr. 9, 1997, S. 93. [정성진, 형사절차로서의내사, 국민대학교「법학논총」, 제9호, 1997, 93쪽]

Ha, Tae-Hoon, Bemerkung über den Gesetzentwurf zur Änderung der K-StPO von The Korean Criminal Law Association, Journal of Criminal Law (JCL), Band 23, Nr. 1, 2011, S. 3. [하태훈, 한국형사법학회형사소송법개정안에대한논평-수사일반과강제처분부분-,「형사법연구」, 제23권 제1호, 2011, 3쪽]

Han, Soo-Woong, Verfassungsrechtliches Persönlichkeitsrecht, Constitutional Law Review (CLR), Band 13, 2002, S. 623. [한수웅, 헌법상의 인격권, 「헌법논총」, 제13집, 2002, 623쪽]

Han, Young-Soo, Bildung systematischer Theorie über den Ausschluss oder die Verwertung von illegal erlangten Beweisen, Journal of Criminal Law (JCL), Band 11, 1999, S. 401. [한영수, 위법수집증거(물)의배제 또는 사용에 관한 체계적인 이론의 형성, 「형사법연구」, 제11권, 1999, 401쪽]

Heo, Hwang, Eine Untersuchung über die Online-Durchsuchung gem. §100b StPO und Quelle-TKÜ gem. § 100a StPO, Contemporary Review of Criminal Law (CRCL), Nr. 58, 2018, S. 94. [허황, 최근개정된독일형사소송법제100조b의온라인수색과제100조a의소스통신감청에관한연구, 「형사법의신동향」, 제58호, 2018, 94쪽]

Hwang, Mungyu, Möglichkeiten und Grenzen polizeilicher und staatsanwaltschaftlicher Tätigkeit im Ermittlungsverfahren nach der Neufassung des § 196 K-StPO, Korean Criminological Review (KCR), Band 22, Nr. 3, 2011, S. 217. [황문규, 개정형사소송법상경찰의 수사개시권및검사의수사지휘권의내용과한계, 「형사정책연구」, 제22권제3호, 2011, 217쪽]

Hwang, Sung-Gi, Verfassungsrechtliche Probleme des bestehenden Rechtswesens zum Geheimnisschutz der Kommunikation, Journal of Media Law, Ethics and Policy (JML), Band 14, Nr. 1, 2015, S. 1. [황성기, 현행통신비밀보호법제의헌법적문제점, 「언론과법」, 제14권 제1호, 2015, 1쪽]

Im, Seok-Soon, Inhaltliche sowie strukturelle Probleme der Regelungen der Durchsetzungsmitteilung im K-KGSG und deren Verbesserung, Korean Criminological Review (KCR), Band 27, Nr. 2, 2016, S. 203. [임석순, 통신비밀보호법상집행통지규정의내용적구조적문제점과개선방안, 「형사정책연구」, 제27권 제2호, 2016, 203쪽]

Jeon, Sang-Hyeon, Verfassungsrechtliche Grundlage und Schutzbereich des Rechts auf informationelle Selbstbestimmung, The Justice, Nr. 169, 2018, S. 5. [전상현, 개인정보자기결정권의헌법상근거와보호영역, 「저스티스」, 제169호, 2018, 5쪽]

Jeong, Oung-Seok, Bewertung der überarbeiteten K-StPO und zukünftige Aufgaben, The Justice, Nr. 101, 2007, S. 205. [정웅석, 개정형사소송법의평가와향후과제, 「저스티스」, 제101호, 2007, 205쪽]

Jung, Aeryung, Das Verhältnis zwischen dem Schutz des Privatlebens und dem Schutz personenbezogener Daten, Public Law Journal (PLJ), Band 17, Nr. 3, 2016, S. 51. [정애령, 사생활보호와 개인정보보호의 관계에 관한 연구, 「공법학연구」, 제17권 제3호, 2016, 51쪽]

Kang, Taesoo, Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses, Kyung Hee Law Journal (KHLJ), Band 45, Nr. 4, 2010, S. 287. [강태수, 통신의 비밀보장에 관한 연구, 「경희법학」, 제45권 제4호, 2010, 287쪽]

Kim, Bong-Su, Kritische Bemerkungen über ‚diskretionäres' Ausschlussprinzip, Korean Journal of Comparative Criminal Law (KJCCL), Band 11, Nr. 2, 2009, S. 189. [김봉수, '재량적' 위법수집증거배제(론)에 대한 비판적 고찰, 「비교형사법연구」, 제11권 제2호, 2009, 189쪽]

Kim, Bong-Su, Die Untersuchung zum Schutz von Standortdaten in der Strafjustiz, ChonNam Law Review (CNLR), Band 32, Nr. 3, 2012, S. 271. [김봉수, 위치정보의 보호를 위한 형법적 고찰, 전남대학교 「법학논총」, 제32집 제3호, 2012, 271쪽]

Kim, Dae-Won, Das Gesetzlichkeitsprinzip der Zwangsmaßnahme und eine grenzüberschreitende Durchsuchung und Beschlagnahme, Theories and Practices of Criminal Procedure (TPCP), Band 11, Nr. 1, 2019, S. 91. [김대원, 강제처분법정주의와 역외원격지 서버에 대한 압수·수색, 「형사소송이론과 실무」, 제11권 제1호, 2019, 91쪽]

Kim, Hyung-Joon, Probleme und Verbesserungsvorschläge des bestehenden K-KGSG, Journal of Criminal Law (JCL), Nr. 24, 2005, S. 213. [김형준, 현행 통신비밀보호법의 문제점과 개선방안, 「형사법연구」, 제24호, 2005, 213쪽]

Kim, Il-Hwan, Die Untersuchung über den Schutzbereich des Geheimnisschutzes der Kommunikation im Verfassungsrecht und Änderungsbedürftigkeit des K-KGSG, Korean Journal of Criminology (KJC), Band 16, Nr. 1, 2004, S. 25. [김일환, 통신비밀의 헌법상 보호와 관련법제도에 관한 고찰, 「형사정책」, 제16권 제1호, 2004, 25쪽]

Kim, Seoung-Cheon, Stellungnahme zum Entwurf zur Neuregelung des K-KGSG, Öffentliche Anhörung zur teilweisen Überarbeitung des K-KGSG, 21. April 2009, Rechtsausschuss des Parlaments, S. 7. [김성천, 통신비밀보호법개정법률안에 대한 의견, 「통신비밀보호법 일부개정법률안에 관한 공청회」, 2009.4.21., 국회법제사법위원회, 7쪽]

Kim, Sung-Ryong, Die gegenwärtige Diskussionslage in Deutschland über den Einsatz von verdeckten Ermittlern, V-Personen und Informanten, Korean Journal of Comparative Criminal Law (KJCCL), Band 7, Nr. 2, 2005, S. 275. [김성룡, 신분위장수사 경찰및 비밀정보원 활용과 그 형사법적 문제점에 관한 독일의 논의 현황, 「비교형사법연구」, 제7권 제2호, 2005, 275쪽]

Kong, Jinseong, Verfassungsrechtliche Grenzen i.R.d. Schutzes des Geheimnisses des Gesprächs nach dem K-KGSG, ChonNam Law Review (CNLR), Band 38, Nr. 4, 2018, S. 67. [공진성, 통신비밀보호법상 대화의 비밀보호의 헌법적 한계, 전남대학교 「법학논총」, 제38권 제4호, 2018, 67쪽]

Kwon, Geonbo, Verfassungsrechtliche Grundlage und Aufgaben für den Schutz personenbezogener Daten, The Justice, Nr. 144, 2014, S. 7. [권건보, 개인정보보호의 헌법적 기초와 과제, 「저스티스」, 제144호, 2014, 7쪽]

Kwon, Geonbo, Die Untersuchung über den Schutzbereich des Rechts auf informationelle Selbstbestimmung, Public Law Journal (PLJ), Band 18, Nr. 3, 2017, S. 199. [권건보, 개인정보 자기결정권의 보호범위에 대한 분석, 「공법학연구」, 제18권 제3호, 2017, 199쪽]

Kwon, Yangsub, Die Zulässigkeit von Packet Inspection im Internet, Korean Law Review (korLR), Band 39, 2010, S. 177. [권양섭, 인터넷패킷감청의허용가능성에관한고찰, 한국법학회「법학연구」, 제39집, 2010, 177쪽]

Kwon, Yangsub, Probleme hinsichtlich der Bestandsdatenauskunft zum Ermittlungszweck und deren Verbesserungsvorschläge, Korean Law Review (korLR), Band 59, 2015, S. 397. [권양섭, 범죄수사에있어서통신자료제공제도의문제점과개선방안, 한국법학회「법학연구」, 제59집, 2015, 397쪽]

Lee, Heun-Jae, Hauptstreitpunkte hinsichtlich der Durchsuchung und Beschlagnahme digitaler Daten, Dankook Law Review (DLR), Band 37, Nr. 3, 2013, S. 129. [이흔재, 디지털증거의압수수색에관한쟁점별해석과통제방안, 단국대학교「법학논총」, 제37권제3호, 2013, 129쪽]

Lee, Heun-Jae, Fahndung mittels der Standortdaten eines Mobiltelefons und Benachrichtigung in Deutschland, Korean Lawyers Association Journal, Band 68, Nr. 4, 2019, S. 497. [이흔재, 독일의휴대전화위치정보추적수사와당사자에대한통보제도, 「법조」, 제68권제4호, 2019, 497쪽]

Lee, Hojung, Probleme der Erhebung von Verkehrsdaten und Richtung der Verbesserung, Journal of Police & Law (JPL), Band 17, Nr. 1, 2019, S. 35. [이호중, 통신사실확인자료제공제도의문제점과개선방향, 「경찰법연구」, 제17권 제1호, 2019, 35쪽]

Lee, In-Gon/*Kang*, Chul-Ha, Probleme der Durchsuchung und Beschlagnahme elektronischer Daten in Cloud-Computing-Umgebung und Richtung zu deren Verbesserung, Contemporary Review of Criminal Law (CRCL), Nr. 54, 2017, S. 322. [이인곤/강철하, 클라우드컴퓨팅환경에서전자정보압수수색의문제점과개선방향, 「형사법의신동향」, 제54호, 2017, 322쪽]

Lee, Jung-Min, Ein grenzüberschreitender Zugriff auf die E-Mail-Server im Ausland mittels des legal erlangten Zugangssicherungscodes, Korean Journal of Comparative Criminal Law (KJCCL), Band 19, Nr. 3, 2017, S. 117. [이정민, 외국계이메일계정에대한압수·수색의정당성, 「비교형사법연구」, 제19권 제3호, 2017, 117쪽]

Lee, Sang-Kyung, Verfassungsrechtliche Kontrolle der Standortverfolgung informationstechnischer Systeme zur Verfolgung, Journal of Constitutional Justice (LCJ), Band 6, Nr. 1, 2019, S. 77. [이상경, 정보통신기기의위치추적에대한헌법적통제에관한소고, 「헌법재판연구」, 제6권 제1호, 2019, 77쪽]

Lee, Sookyeon, Durchsuchung und Beschlagnahme, Grundrechte und Richtervorbehalt i. R. v. elektronischen Daten, Korean Journal of Constitutional Law (KJCL), Band 18, Nr. 1, 2012, S. 1. [이숙연, 전자정보에대한압수수색과기본권, 그리고영장주의에관하여, 「헌법학연구」, 제18권 제1호, 2012, 1쪽]

Lee, Soonok, Grenzüberschreitende Durchsuchung und Beschlagnahme der auf dem externen Speichermedium vorhandenen digitalen Daten, ChungAng Law Review (CALR), Band 20, Nr. 1, 2018, S. 117. [이순옥, 디지털증거의역외압수수색, 「중앙법학」, 제20집 제1호, 2018, 117쪽]

Lee, Wankyu, Überlegung über das Prinzip des Ausschlusses von illegal erlangten Beweisen in Gesetzentwurf zur Änderung der K-StPO vom Präsidialausschuss zur Förderung der Justizreform, Korean Journal of Comparative Criminal Law (KJCCL), Band 8, Nr. 1, 2006, S. 595. [이완규, 사개추위안의위법수집증거배제원칙에대한검토, 「비교형사법연구」, 제8권 제1호, 2006, 595쪽]

Lee, Wankyu, Unterschied zwischen Vorermittlung und Ermittlung unter geltendem Recht und Praxis, Theories and Practices of Crimonal Procedure, Band 7, Nr. 1, 2015, S. 33. [이완규, 현행법상 내사와 수사의 구별과 실무 상황, 「형사소송 이론과 실무」, 제7권 제1호, 2015, 33쪽]

Lee, Wankyu, Die Teilnahme des Betroffenen am Prozess der Durchsuchung und Beschlagnahme, und die Beschlagnahme der verfahrensirrelevanten Beweise, Contemporary Review of Criminal Law (CRCL), Nr. 48, 2015, S. 90. [이완규, 디지털증거압수절차상 피압수자 참여방식과 관련성 범위 밖의 별건 증거압수방법, 「형사법의 신동향」, 제48호, 2015, 90쪽]

Lee, Won-Sang, Die Untersuchung über Standortdaten in der Strafjustiz, Korean Criminological Review (KCR), Band 23, Nr. 2, 2012, S. 109. [이원상, 형사사법에있어개인위치정보에대한 고찰, 「형사정책연구」, 제23권 제2호, 2012, 109쪽]

Lee, Won-Sang, Sicherstellung digitaler Beweise in Cloud-Computing-Umgebung, Contemporary Review of Criminal Law (CRCL), Nr. 38, 2013, S. 174. [이원상, 클라우드컴퓨팅환경에서의디지털증거확보를 위한 소고, 「형사법의 신동향」, 제38호, 2013, 174쪽]

Lee, Won-Sang, Untersuchung zur Verwertung der Bestandsdaten im Ermittlungsverfahren, Theories and Practices of Criminal Procedure (TPCP), Band 7, Nr. 1, 2015, S. 70. [이원상, 수사절차에서 통신자료 활용에 따른 쟁점 고찰, 「형사소송 이론과 실무」, 제7권 제1호, 2015, 70쪽]

Lee, Won-Sang, Die Grenzen des geltenden Gesetzes zur Erhebung digitaler Daten, Journal of Digital Forensics (JDF), Band 11 Nr. 3, 2017, S. 29. [이원상, 현행디지털증거수집관련법률의 한계, 「디지털포렌식연구」, 제11권 제3호, 2017, 29쪽]

Lim, Gyeo-Cheol, Einige Problematiken zur Kontrolle bei Vergabe der Bestandsdaten durch TK-Diensteanbieter, Pusan Law Review (PLR), Band 57, Nr. 4, 2016, S. 197. [임규철, 전기통신사업자의 수사기관으로의 통신자료 제공에 대한 비판적 연구, 부산대학교 「법학연구」, 제57권 제4호, 2016, 197쪽]

Min, Mankee, Rechtsvergleichende Untersuchung zur Zulässigkeit von illegal erlangten Beweismitteln, SungKyunKwan Law Review (SKKLR), Band 24, Nr. 2, 2012, S. 339. [민만기, 수집절차에 위법이 있는 압수물의 증거능력에 관한 비교법적 고찰, 「성균관법학」, 제24권 제2호, 2012, 339쪽]

Min, Mankee, Die Rechtsnatur von Packet Inspection im Internet und ihre Zulässigkeit, Contemporary Review of Criminal Law (CRCL), Nr. 53, 2016, S. 214. [민만기, 인터넷패킷감청의 법적 성격 및 허용가능성 검토, 「형사법의 신동향」, 제53호, 2016, 214쪽]

Min, Youngsung/*Park*, Hee-Young, Zulässigkeit der Echtzeit-Verfolgung mit den Standortdaten eines Mobiltelefons und Richtung ihres Gesetzesvorschlags, Korean Criminological Review (KCR), Band 28, Nr. 4, 2017, S. 203. [민영성/박희영, 통신비밀보호법상 휴대전화 위치정보의 실시간 추적 허용과 입법방향, 「형사정책연구」, 제28권 제4호, 2017, 203쪽]

Moon, Byoung-Hyo, Kritik an dem Entwurf zur Neuregelung des K-KGSG, Public Land Law Review (PLLR), Band 45, 2009, S. 503. [문병효, 통비법개정안에 대한 비판적 고찰, 「토지공법연구」, 제45집, 2009, 503쪽]

Moon, Jaewan, Verfassungsrechtliche Beleuchtung der Rechtssysteme für den Schutz personenbezogener Daten, World Constitutional Law Review (WCLR), Band 19, Nr. 2, 2013,

S. 271. [문재완, 개인정보 보호법제의 헌법적 고찰, 「세계헌법연구」, 제19권 제2호, 2013, 271쪽]

Oh, Gi-Du, Durchsuchung und Beschlagnahme von subjektiv verfahrensrelevanten Daten, Juris, Nr. 28, 2014, S. 199. [오기두, 주관적관련성있는전자정보만의수색검증, 압수, 「사법」, 제28호, 2014, 199쪽]

Oh, Kil-Young, Kritik an dem Entwurf zur Neuregelung des K-KGSG, Democratic Legal Studies (DLS), Nr. 34, 2007, S. 357. [오길영, 통신비밀보호법개정안에대한비판, 「민주법학」, 제34호, 2007, 357쪽]

Oh, Kil-Young, Eine Überwachung im Internet und Deep Packet Inspection, Democratic Legal Studies (DLS), Nr. 41, 2009, S. 391. [오길영, 인터넷 감청과 DPI, 「민주법학」, 제41호, 2009, 391쪽]

Oh, Kil-Young, Probleme des bestehenden K-KGSG und Richtung zu deren Verbesserung, Journal of Media Law, Ethics and Policy (JML), Band 14, Nr. 1, 2015, S. 33. [오길영, 현행통비법의문제점과개선방향, 「언론과법」, 제14권 제1호, 2015, 33쪽]

Oh, Kyung-Sik, Unterschied zwischen Vorermittlung und Ermittlung, Contemporary Review of Criminal Law (CRCL), Nr. 34, 2012, S. 48. [오경식, 내사와수사의구별기준에대한고찰, 「형사법의신동향」, 제34호, 2012, 48쪽]

Park, Chan-Keol, Probleme der Bestandsdatenauskunft nach K-TKGG und deren Verbesserung, Journal of Law and Politics research (JLP), Band 14, Nr. 1, 2014, S. 9. [박찬걸/강동욱, 전기통신사업법상 통신자료 제공제도의 문제점과 개선방안, 「법과정책연구」, 제14권 제1호, 2014, 9쪽]

Park, Chan-Keol/*Kang*, Dong-Wook, Rechtspolitische Überlegung über die Durchführung der Maßnahmen zur Beschränkung des Kommunikationsverkehrs, Jeju Law & Policy Review (JLPR), Band 20, Nr. 1, 2014, S. 315. [박찬걸/강동욱, 통신제한조치의집행에관한법정책적고찰, 제주대학교「법과정책」, 제20권 제1호, 2014, 315쪽]

Park, Hee-Young, Die Technik von Deep Packet Inspection und eine strafrechtliche Verantwortlichkeit der Dienstanbieter, Internet and Information Security (IIS), Band 2, Nr. 1, 2011, S. 105. [박희영, DPI 기술의운영과 ISP의형사책임, 「Internet and Information Security」, 제2권 제1호, 2011, 105쪽]

Park, Hee-Young, Zulässigkeit und Grenzen der Online-Durchsuchung zum präventiven Zweck und zur Strafverfolgung, WonKwang Law Review (WKLR), Band 28, Nr. 3, 2012, S. 153. [박희영, 예방및수사목적의온라인비밀수색의허용과한계, 「원광법학」, 제28권 제3호, 2012, 153쪽]

Park, Hee-Young, Zulässigkeit ‚Stiller SMS' zur Erhebung der Standortdaten eines Mobiltelefons und ihre legislativen Leitlinien, Pusan Law Review (PLR), Band 61, Nr. 2, 2020, S. 137. [박희영, 휴대전화 위치정보수집을 위한 '비밀 SMS 수사'(Stille SMS)의허용과입법방향, 부산대학교「법학연구」, 제61권 제2호, 2020, 137쪽]

Park, Hee-Young/*Lee*, Sang-Hak, Zulässigkeit und Grenzen der Begleitmaßnahmen der Quellen-TKÜ und Online-Durchsuchung, Korean Criminological Review (KCR), Band 30, Nr. 2, 2019, S. 113. [박희영/이상학, 암호통신감청및온라인수색에서부수처분의허용과한계, 「형사정책연구」, 제30권 제2호, 2019, 113쪽]

Park, Joongwook, Probleme und Verbesserungsweg der Benachrichtigungsregelungen im K-KGSG, Contemporary Review of Criminal Law (CRCL), Nr. 68, 2020, S. 97. [박중욱, 통신비밀보호법 통지규정의 문제점과 개선방향, 「형사법의 신동향」, 제68호, 2020, 97쪽]

Park, Kyung-Sin, Probleme bezügliche der Durchsuchung und Beschlagnahme von E-Mails und legislative Lösungen, InHa Law Review, Band 13, Nr. 2, 2010, S. 265. [박경신, E-메일 압수수색의 제문제와 관련법률 개정안들에 대한 평가, 인하대학교 「법학연구」, 제13집 제2호, 2010, 265쪽]

Rhee, Joo-Won, Verbesserung der Durchsuchung und Beschlagnahme digitaler Beweise, Anam Law Review (ALR), Nr. 37, 2012, S. 151. [이주원, 디지털증거에 대한 압수수색 제도의 개선, 「안암법학」, 제37호, 2012, 151쪽]

Roh, Myung-Sun, Gedanken über das Prinzip des Ausschlusses von illegal erlangten Beweisen in der K-StPO, ChonBuk Law Review (CBLR), Band 37, 2012, S. 91. [노명선, 한국형사소송법상 위법수집증거배제법칙에 관한 소고, 전북대학교 「법학연구」, 제37호, 2012, 91쪽]

Shin, Dong-Woon, Die Institution der Voruntersuchung während der Kolonialherrschaft des japanischen Imperialismus, Seoul Law Journal (SLJ), Band 27, Nr. 1, 1986, S. 149. [신동운, 일제하 예심제도에 관하여, 서울대학교 「법학」, 제27권 제1호, 1986, 149쪽]

Shin, Sang-Hyun, Der Rechtsschutz des Beschuldigten gegen Zwangsmaßnahmen im Ermittlungsverfahren, HUFS Law Journal (HUFSLJ), Band 43, Nr. 3, 2019, S. 93. [신상현, 수사절차에서 준항고를 통한 피의자의 법적보호, 「외법논집」, 제43권 제3호, 2019, 93쪽]

Shin, Yang-Kyun, Das Prinzip des Ausschlusses von illegal erlangten Beweisen in der K-StPO, Journal of Criminal Law (JCL), Band 26, Nr. 2, 2014, S. 447. [신양균, 우리나라 형사소송법상 위법수집증거배제법칙, 「형사법연구」, 제26권 제2호, 2014, 447쪽]

Shin, Yang-Kyun/*Cho*, Gi-Yeong, Der Begriff und der zulässige Umfang der Vorermittlungen, Journal of Criminal Law (JCL), Band 23, Nr. 3, 2011, S. 181. [신양균/조기영, 내사의 개념과 허용범위, 「형사법연구」, 제23권 제3호, 2011, 181쪽]

Sim, Huigi, Aktueller Status der TKÜ durch Ermittlungsbehörden und Geheimdienste sowie Richtung zur Reform des K-KGSG, Korean Criminological Review (KCR), Band 10, Nr. 3, 1999, S. 5. [심희기, 수사·정보기관의 감청도청의 실태와 통신비밀보호법의 개정방향, 「형사정책연구」, 제10권 제3호, 1999, 5쪽]

Suh, Bo-Hack, Die Doktrin vom giftigen Baum und deren Ausnahme sowie die Zulässigkeit von durch eine Privatperson illegal erlangten Beweisen, Korean Criminological Review (KCR), Band 20, Nr. 3, 2009, S. 31. [서보학, 위법수집증거의 쟁점: 독수독과 의원칙과 예외, 사인이 위법수집한 증거의 증거능력, 「형사정책연구」, 제20권 제3호, 2009, 31쪽]

Yang, Jongmo, Durchsuchung und Beschlagnahme elektronischer Daten in Cloud-Computing-Umgebung, Journal of hongik law review (jhlr), Band 15, Nr. 3, 2014, S. 1. [양종모, 클라우드 컴퓨팅 환경에서의 전자적 증거압수수색에 대한 고찰, 「홍익법학」, 제15권 제3호, 2014, 1쪽]

Yoo, Jusung, Bestandsdatenauskunft der Ermittlungsbehörde und Richtervorbehalt, Korean Criminological Review (KCR), Band 24, Nr. 3, 2013, S. 85. [유주성, 수사기관의 통신자료 제공요청과 영장주의의 적용, 「형사정책연구」, 제24권 제3호, 2013, 85쪽]

Stichwortverzeichnis