

**Schriften zum Prozessrecht**

---

**Band 290**

**Die Auswirkungen des Völkerrechts  
auf die grenzüberschreitende Ermittlung  
digitaler Beweise nach der StPO**

**Von**

**Esther-Nicola Vehling**



**Duncker & Humblot · Berlin**

ESTHER-NICOLA VEHLING

Die Auswirkungen des Völkerrechts  
auf die grenzüberschreitende Ermittlung  
digitaler Beweise nach der StPO

Schriften zum Prozessrecht

Band 290

# Die Auswirkungen des Völkerrechts auf die grenzüberschreitende Ermittlung digitaler Beweise nach der StPO

Von

Esther-Nicola Vehling



Duncker & Humblot · Berlin

Der Fachbereich Rechtswissenschaft der Universität Hamburg  
hat diese Arbeit im Jahre 2022 als Dissertation angenommen.

Bibliografische Information der Deutschen Nationalbibliothek

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

Alle Rechte vorbehalten  
© 2023 Duncker & Humblot GmbH, Berlin  
Satz: L101 Mediengestaltung, Fürstenwalde  
Druck: CPI books GmbH, Leck  
Printed in Germany

ISSN 0582-0219  
ISBN 978-3-428-18814-7 (Print)  
ISBN 978-3-428-58814-5 (E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier  
entsprechend ISO 9706 ☺

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

*Meinen Eltern*



## Vorwort

Die vorliegende Arbeit wurde im Sommersemester 2022 von der Juristischen Fakultät der Universität Hamburg als Dissertation angenommen. Für die Drucklegung wurde das Manuskript überarbeitet und auf den Stand von November 2022 gebracht.

Die Arbeit ist mit ihrem Beginn im Herbst 2019 nicht nur während Zeiten der Pandemie entstanden, sondern auch zu einer Zeit, in der sich sowohl der Gesetzgeber als auch die Gerichte immer wieder mit Fragen der digitalen Beweiserhebung auseinandergesetzt haben. Durch den teilweise eingeschränkten Zugang zu Literatur, durch die Aktualität des Themas und die fortwährende Anpassung der Gesetzeslage gestaltete sich das Erstellen der Dissertation als besonders herausfordernd, aber auch als besonders spannend. Insgesamt empfand ich die Zeit der Dissertationserstellung als lehrreiche, interessante und vor allem bereichernde Zeit.

An erster Stelle gebührt mein besonderer Dank meinem Doktorvater Herrn Professor Dr. Milan Kuhli. Er unterstützte mich nicht nur bei der Wahl des Themas, sondern stand während des Verfassens der Dissertation stets als Diskussionspartner zur Verfügung. Durch seine konstruktiven Anmerkungen, wertvollen Hinweise und sein ermunterndes Lob hatte ich stets das Gefühl gut betreut und auf dem richtigen Weg zu sein. Mein Dank gilt auch Herrn Professor Dr. Kai Cornelius für die Erstellung des Zweitgutachtens und seine wertvollen abschließenden Hinweise.

In privater Hinsicht gilt mein herzlicher und unermesslicher Dank meinen Eltern, Karl-Heinz Vehling und Doris Knops-Vehling, die es mir durch ihre fortwährende Unterstützung ermöglicht haben, meiner Freude am Lernen und am wissenschaftlichen Arbeiten nachzugehen. Darüber hinaus möchte ich mich bei meinen Schwestern bedanken, die mich stets in all meinen Vorhaben bestärkt haben. Nicht zuletzt gebührt mein Dank meinen Freunden, die immer wieder dafür gesorgt haben, dass es mir während des Verfassens der Doktorarbeit nie an hinreichend Motivation, Disziplin und notwendiger Erholung fehlte und somit wesentlich zum Gelingen dieser Arbeit beigetragen haben. Ganz besonderer Dank gilt in dieser Hinsicht meinem besten Freund Jacob, der mir von den Anfängen der Dissertation bis zu ihrer Verteidigung in jedweder Hinsicht wie kein anderer zur Seite stand.

Berlin, im Februar 2023

*Esther-Nicola Vehling*



# Inhaltsverzeichnis

<b>Einleitung</b>	17
<i>Kapitel 1</i>	
<b>Technische Grundlagen der unkörperlichen Telekommunikation und des Internets</b>	<b>20</b>
A. Technische Grundlagen der Telefonie .....	20
I. Festnetz .....	20
II. Mobilfunknetz .....	22
B. Technische Grundlagen des Internets .....	24
I. Architektur des Internets .....	25
II. Das TCP/IP-Referenzmodell .....	26
1. Die Anwendungsschicht .....	29
2. Die Transportschicht .....	29
3. Die Internetschicht .....	30
4. Die Netzwerkschicht .....	31
5. Die physikalische Schicht .....	31
III. Internetanwendungen .....	32
1. Das World Wide Web (www) .....	32
2. Cloudcomputing .....	33
3. E-Mails .....	36
4. WhatsApp .....	37
5. Soziale Netzwerke .....	37
6. VoIP .....	38
<i>Kapitel 2</i>	
<b>Ermächtigungsgrundlagen für den Zugriff auf nicht-gegenständliche Beweise im deutschen Strafverfahren</b>	<b>39</b>
A. Verdeckte Ermittlungsmaßnahmen .....	40
I. Die zentrale Bedeutung des Telekommunikationsbegriffs für die Bestimmung der repressiven Zugriffsmöglichkeiten auf ermittlungsrelevante Daten .....	41
II. Der Telekommunikationsbegriff der StPO .....	42
1. Die Legaldefinition des Telekommunikationsgesetzes (TKG) .....	42

2. Formell-technischer Telekommunikationsbegriff .....	43
3. Genuin strafverfahrensrechtlicher Telekommunikationsbegriff der Literatur .....	44
4. Stellungnahme .....	46
III. Die Ermächtigungsgrundlagen im Einzelnen .....	53
1. § 100a Abs. 1 S. 1 StPO: „Herkömmliche“ Telekommunikationsüberwachung .....	53
a) E-Mails .....	55
aa) E-Mails in der Ruhendphase auf dem Server des E-Mail-Anbieters .....	55
bb) Endgespeicherte, auf dem Server des E-Mail-Anbieters belassene E-Mails .....	57
b) Der Telekommunikationsanbieter als der nach § 100a Abs. 4 StPO zur Mithilfe an der Telekommunikationsüberwachung Verpflichtete .....	61
aa) Literatur .....	62
bb) Rechtsprechung .....	64
(1) EuGH Urteil vom 13.06.2019: Google LLC/Bundesrepublik Deutschland .....	64
(2) LG München I, Beschluss vom 4.12.2019 – 9 Qs 15/19 .....	65
cc) Abschaffung des Problems durch das TKModG in Umsetzung des Europäischen Elektronischen Kommunikationskodexes .....	66
c) Verschlüsselte Telekommunikationsformen (internetbasierte Telefon- und Messengerdienste) .....	67
2. § 4 Abs. 2 S. 1 TKÜV: Auslandskopfüberwachung .....	68
3. § 100a Abs. 1 S. 2 und 3 StPO: Quellen-Telekommunikationsüberwachung .....	70
a) Zugriff auf laufende Kommunikation, § 100a Abs. 1 S. 2 StPO .....	71
b) Zugriff auf Inhalte bereits abgeschlossener Kommunikation, § 100a Abs. 1 S. 3 StPO .....	72
4. § 100b StPO: Online-Durchsuchung .....	73
a) Das informationstechnische System i.S.d. § 100b StPO .....	74
b) Die Nutzung von Webcam und Mikrofon zur Raumüberwachung unter § 100b StPO .....	76
c) Herausgabeverlangen von Inhaltsdaten an Dienstanbieter als Minus von der Online-Durchsuchung erfasst? .....	79
5. § 100i StPO: Technische Ermittlungsmaßnahmen bei Mobilfunkendgeräten .....	80
6. Datenabfrage bei Dienstanbietern .....	81
a) Grundmodell der behördlichen Datenabfrage bei privaten Dienstanbietern .....	81
b) § 100g StPO: Erhebung von Verkehrsdaten .....	82

aa) Erhebung von nach §§ 9, 12 TTDSG, § 2a Abs. 1 BDBOSG gespeicherten Verkehrsdaten .....	83
bb) Erhebung von nach § 176 TKG (§ 113b TKG a.F.) gespeicherten Verkehrsdaten .....	84
cc) Funkzellenabfrage .....	86
dd) Sicherungsanordnung (Quick-Freeze), § 100g Abs. 5 StPO-E	87
c) §§ 161 Abs. 1, 163 Abs. 1 StPO, § 173 TKG (§ 112 TKG a.F.): Auskunftsersuchen bei der Bundesnetzagentur über Telekommunikationsbestandsdaten im automatisierten Verfahren .....	87
d) § 100j StPO: Auskunftsverlangen beim Dienstanbieter über Bestandsdaten im manuellen Verfahren .....	89
aa) Entwicklung der manuellen Bestandsdatenauskunft in den Jahren 2020–2022 .....	89
bb) Regelungsgehalt des § 100j StPO .....	91
e) § 100k StPO: Abfrage von Nutzungsdaten bei Telemedienanbietern .....	92
<b>B. Offene Ermittlungsmaßnahmen .....</b>	<b>93</b>
I. § 94 StPO: Sicherstellung und Beschlagnahme von Gegenständen zu Beweiszwecken .....	93
1. Der Wortlaut des § 94 StPO .....	94
2. Zulässigkeit einer Beschlagnahme von Daten unter verfassungsrechtlichen Gesichtspunkten .....	95
II. § 95 StPO: Pflicht zur Herausgabe beweisrelevanter Gegenstände .....	101
III. § 110 Abs. 3 StPO: Durchsicht von Papieren und elektronischen Speichermedien .....	101
IV. Die Ermittlungsgeneralklausel, §§ 161 Abs. 1, 163 Abs. 1 StPO .....	103
1. Zugriff auf öffentlich zugängliche Daten im Internet (OSINT-Recherchen) .....	103
2. Ermittlungen durch informelle Kooperation mit Dateninhabern .....	105

### *Kapitel 3*

#### **Völkerrechtliche Implikationen eines Zugriffs auf digitale Beweismittel** 106

<b>A. Territorialität als Kernelement des Völkerrechts .....</b>	<b>107</b>
I. Territoriale Souveränität als Zuweisungs- und Abgrenzungskriterium von Staatsmacht .....	107
II. Grenzüberschreitende Hoheitsbefugnisse und Beschränkung der Rechtsdurchsetzungsmacht ( <i>jurisdiction to enforce</i> ) auf das Hoheitsgebiet .....	109
III. Territoriale Hoheitsansprüche im Telefonnetz .....	112
IV. Territoriale Hoheitsansprüche im Cyberspace .....	112
1. Cyberspace als Raum sui generis unter dem Ausschluss hoheitlicher Rechte .....	113

2. Cyberspace als Staatengemeinschaftsraum frei von territorialer Hoheitsgewalt .....	114
3. Cyberspace als Objekt territorialer Hoheitsgewalt .....	116
4. Stellungnahme .....	117
<b>B. Beweisermittlung unter Verstoß gegen das Völkerrecht .....</b>	<b>120</b>
I. Extraterritorialität ohne physische Penetration eines fremden Staatsgebietes: Eingriff in eine fremde Gebietshoheit durch datenbezogene Ermittlungsmaßnahmen? .....	122
1. Extraterritorialität bei einer Überwachung leitungsgebundener Telekommunikation in Echtzeit .....	123
a) Ansichten in der Literatur und in der Rechtsprechung .....	124
b) Eigene Ansicht .....	126
aa) Die Überwachung des Anschlusses .....	127
bb) Das Ausleiten der Daten .....	128
cc) Ergebnis .....	128
2. Extraterritorialität beim Zugriff auf in fremdem Hoheitsgebiet gespeicherte Daten .....	129
a) Zugriff auf Daten, die lokal auf dem Gerät eines Nutzers gespeichert sind .....	129
b) Zugriff auf Daten, die „im Netz“, d.h. serverbasiert gespeichert sind .....	132
aa) Direkter Zugriff durch die Ermittlungsbehörden selbst .....	132
(1) Der Speicherort der Daten als Anknüpfungspunkt für territoriale Hoheitsbefugnisse .....	133
(2) Der Aufenthaltsort der handelnden Ermittlungsperson als Anknüpfungspunkt für territoriale Hoheitsbefugnisse .....	134
(3) Der Beschuldigte .....	134
(4) Ort, von welchem die Daten bestimmungsgemäß abgerufen werden sollen als Anknüpfungspunkt für territoriale Hoheitsbefugnisse .....	135
(5) Zuordnung zu einem Hoheitsgebiet durch Abwägung der staatlichen Interessen an der Geltendmachung ihrer territorialen Hoheitsansprüche .....	135
(6) Rechtsauffassung der Staaten (opinio juris) .....	136
(7) Stellungnahme und Ergebnis .....	138
bb) Zugriff auf die Daten unter Zuhilfenahme der Serviceprovider .....	139
(1) Anfrage an Dienstanbieter territorial oder extraterritorial	140
(a) Zuordnung des Dienstanbieters zu der territorialen Hoheitsmacht eines Staates .....	140
(b) An ausländische Serviceprovider gerichtete Herausgabeanordnung als Ausübung extraterritorialer Hoheitsmacht .....	143

(2) Umfang der Herausgabeverpflichtung – auch Daten im Ausland? .....	146
(3) Informelle Anfrage beim Serviceprovider .....	149
3. Extraterritorialität beim Zugriff auf im Internet öffentlich zugängliche Daten .....	153
II. Extraterritoriale Datenermittlung als völkerrechtliches Delikt .....	154
1. Kein Verstoß gegen das Interventionsverbot .....	155
a) Domaine réservé .....	156
b) Zwangselement .....	157
2. Völkerrechtsbruch durch Verstoß gegen das Gebot der Achtung der Souveränität .....	159
a) Souveränität als unverbindliches Prinzip des Völkerrechts .....	159
b) Souveränität und deren Achtung als rechtlich verbindliche Norm .....	160
c) Stellungnahme und Ergebnis .....	160
d) Verstoß gegen das Gebot der Achtung der Souveränität bei Datenermittlungen, insbesondere im Cyberspace .....	162
aa) Geltung des Gebots der Achtung fremder Souveränität .....	163
bb) Bruch des Gebots der Achtung fremder Souveränität .....	166
(1) Grundsatz .....	166
(2) Ausnahmen bei loss of location und „good faith“-Fällen .....	168
3. Bruch von Völkervertragsrecht durch Umgehung eines Rechtshilfevertrags .....	170
III. Zwischenergebnis Beweisermittlungsmaßnahmen unter Verstoß gegen das Völkerrecht .....	171
C. Völkerrechtliche Erlaubnistatbestände .....	171
I. Nach Gewohnheitsrecht anerkannte völkerrechtliche Erlaubnistatbestände der ILC .....	171
1. Zulässige Gegenmaßnahme/Repressalie (countermeasures) .....	172
2. Notlage (distress) und Notstand (necessity) .....	173
3. Einwilligung .....	173
a) Ad-hoc Einwilligung zum Datenzugriff durch ausländische Ermittlungsbehörden .....	173
b) Völkervertragliche Einwilligung .....	174
II. Völkervertragsrecht als Ausdruck der Einwilligung .....	174
1. Überblick über relevante Rechtshilfeübereinkommen .....	176
a) Allgemeine Rechtshilfeverträge .....	176
aa) Die Europäische Ermittlungsanordnung .....	176
bb) Andere allgemeine Rechtshilfeinstrumente in Europa .....	178
cc) Rechtshilfeabkommen zwischen Deutschland und den USA .....	179
b) Datenspezifische Rechtshilfeabkommen .....	180
aa) Cybercrime Convention des Europarats .....	180
bb) Zweites Zusatzprotokoll zur Cybercrime Convention .....	181

cc) Entwurf einer Europäischen Sicherungs- und Herausgabeabordnung .....	182
2. Einzelne Vorschriften der Rechtshilfe bei der Telekommunikationsüberwachung.....	184
a) Cybercrime Convention .....	184
b) Europäische Ermittlungsanordnung .....	184
c) EurRhÜbk und RhÜbk-EU .....	186
d) Rechtshilfeabkommen mit den USA .....	187
3. Einzelne Vorschriften der Rechtshilfeabkommen beim Zugriff auf in fremdem Hoheitsgebiet gespeicherte Daten .....	187
a) Cybercrime Convention .....	188
aa) Klassische Rechtshilferegelungen des Art. 31 CCC .....	188
bb) Unilaterale Handlungsbefugnis des Art. 32 CCC .....	188
b) Europäische Ermittlungsanordnung .....	189
aa) Allgemein: Erweiterung des räumlichen Anwendungsbereichs inländischer Ermittlungsmaßnahmen .....	189
bb) Problem des Befugnis-Shoppings .....	191
c) EurRhÜbk und RhÜbk-EU .....	192
d) Rechtshilfeabkommen mit den USA .....	192
e) Zweites Zusatzprotokoll zur Cybercrime Convention .....	193
aa) Art. 6 Zusatzprotokoll: Abfrage von Domain-Name-Registrierungsinformationen ( <i>Request for domain name registration information</i> ) .....	193
bb) Art. 7 Zusatzprotokoll: Preisgabe von Bestandsdaten ( <i>Disclosure of subscriber information</i> ) .....	193
cc) Art. 8 Zusatzprotokoll: Durchsetzung von Anordnungen ausländischer Strafverfolgungsbehörden zur beschleunigten Übermittlung von Bestands- und Verkehrsdaten ( <i>Giving effect to orders from another party for expedited production of subscriber information and traffic data</i> ) .....	194
dd) Art. 9 Zusatzprotokoll: Beschleunigte Preisgabe gespeicherter Computerdaten bei außerordentlicher Dringlichkeit ( <i>Expedited disclosure of stored computer data in an emergency</i> ) und Art. 10 Zusatzprotokoll: Rechtshilfe bei außerordentlicher Dringlichkeit ( <i>Emergency mutual assistance</i> ) .....	195
ee) Art. 12 Zusatzprotokoll: Einrichtung von gemeinschaftlichen Ermittlungsgruppen ( <i>joint investigation teams and joint investigations</i> ) .....	196
ff) Einfluss des Zusatzprotokolls auf die völkerrechtliche Zulässigkeit grenzüberschreitender Datenzugriffe .....	197
f) Entwurf einer europäischen Herausgabe- und Sicherungsanordnung .....	199

*Kapitel 4*

**Bedeutung der völkerrechtlichen Grundsätze für  
die nationalen Ermittlungsbefugnisse der Strafverfolgungsbehörden  
nach der StPO**

202

A. Verdeckte Ermittlungsmaßnahmen .....	202
I. § 100a Abs. 1 S. 1 StPO und § 4 Abs. 2 S. 1 TKÜV: Herkömmliche Telekommunikationsüberwachung und Auslandskopfüberwachung .....	202
1. Grundsatz .....	202
2. Rechtshilfe .....	203
II. § 100a Abs. 1 S. 2 und 3 StPO und § 100b StPO: Quellen-Telekommunikationsüberwachung, Online-Durchsuchung .....	204
1. Grundsatz .....	204
2. Rechtshilfeverfahren .....	205
III. § 100g, § 100j und § 100k StPO: Erhebung von Verkehrs-, Bestands- und Nutzungsdaten .....	206
1. Grundsatz .....	206
2. Rechtshilfeverfahren .....	206
IV. § 100i StPO: Technische Ermittlungen bei Mobilfunkendgeräten .....	207
1. Grundsatz .....	207
2. Rechtshilfe .....	208
B. Offene Ermittlungsmaßnahmen .....	208
I. § 94 StPO: Sicherstellung und Beschlagnahme .....	208
1. Grundsatz .....	208
2. Rechtshilfe .....	208
II. § 95 StPO: Herausgabepflicht beweisrelevanter Gegenstände .....	209
III. § 110 Abs. 3 StPO: Durchsicht von Papieren und elektronischen Speichermedien .....	209
1. Grundsatz .....	209
2. Rechtshilfe .....	210
IV. Die Ermittlungsgeneralklause, §§ 161 Abs. 1, 163 Abs. 1 StPO .....	210
C. Fazit zu den völkerrechtlichen Auswirkungen auf die deutschen Ermittlungsbefugnisse .....	211

*Kapitel 5*

**Die Verwertbarkeit völkerrechtswidrig erlangter Beweise**

212

A. Herrschende Meinung in Rechtsprechung und Literatur .....	212
B. Eigene Ansicht .....	213
I. Prämissen der herrschenden Meinung .....	213
II. Unselbstständige Beweisverwertungsverbote .....	214
1. Dogmatische Einordnung im deutschen Strafprozessrecht .....	214

2. Funktion und Begründung eines unselbstständigen Beweisverwertungsverbots .....	214
a) Funktion von Beweisverwertungsverboten .....	215
b) Begründung eines unselbstständigen Beweisverwertungsverbots .....	216
aa) Rechtskreistheorie und Schutzzwecklehre .....	216
bb) Abwägungslehre .....	217
cc) Informationsbeherrschungslehre .....	218
dd) Beweisverwertungsverbot bei Verletzung des Rechts auf ein faires Verfahren .....	219
ee) Stellungnahme und Ergebnis .....	221
(1) Entstehung des Beweisverwertungsverbots .....	221
(a) Recht auf faires Verfahren und Informationsbeherrschungsrecht maßgebend .....	221
(b) Unzulänglichkeit der Abwägungslehre, Rechtskreistheorie und Schutzzwecktheorie .....	224
(2) Berücksichtigungsfähigkeit hypothetischer Ermittlungsverläufe .....	225
(a) Grundsatz: Keine Berücksichtigungsfähigkeit .....	225
(b) Berücksichtigungsfähigkeit bei Vorliegen eines Erlaubnistanstumstandssirrums seitens der Behörden .....	226
3. Ergebnis zur Entstehung eines Beweisverwertungsverbots .....	228
III. Bedeutung der beweisrechtlichen Grundsätze für völkerrechtswidrig erlangte Beweismittel .....	228
1. Das Gebot der Achtung fremdstaatlicher Souveränität und Art. 25 GG als Beweiserhebungsverbot .....	228
2. Verwertungsverbot bei völkerrechtswidriger Beweiserlangung .....	229
a) Grundsatz .....	229
b) Besonderheiten bei der Verwertbarkeit bei völkerrechtswidrig ermittelter Beweise .....	231
aa) Vorliegen eines Rechtshilfevertrags .....	231
bb) Nachträgliche Zustimmung des Staates .....	232
cc) Good faith .....	233
dd) Unbestimmbarkeit des Aufenthaltsorts der Zielperson oder des Speicherorts (loss of location) .....	233
C. Zusammenfassung .....	234
<b>Fazit</b>	237
<b>Literaturverzeichnis</b> .....	240
<b>Stichwortverzeichnis</b> .....	262

## Einleitung

Die voranschreitende Globalisierung und Digitalisierung verändern nach wie vor die Gesellschaft. Nationale Grenzen werden durch die Bürger immer weniger wahrgenommen. Moderne Technik erlaubt es Personen, sich weltweit zu vernetzen und auch Dienstleistungen aus dem Ausland in Anspruch zu nehmen. Die Phänomene der Globalisierung und Digitalisierung bergen viele Vorteile für die Zivilgesellschaft. Die Strafverfolgungsbehörden stellen sie jedoch vor nicht zu unterschätzende Probleme: Strafverfolgungsbehörden sind als Teil der Staatsmacht in ihren Handlungen grundsätzlich auf das eigene Staatsgebiet beschränkt.<sup>1</sup> Die Strafprozessordnung, die den Behörden Befugnisse für bestimmte Ermittlungsmaßnahmen an die Hand gibt, ist insofern in ihrer Anwendung geografisch beschränkt und kann im Grundsatz nur Maßnahmen auf deutschem Hoheitsgebiet legitimieren.<sup>2</sup> Diese örtliche Beschränkung folgt aus dem völkerrechtlichen Souveränitätsprinzip, zu dessen Ausprägungen das Recht zur Selbstständigkeit und zur Selbstbestimmung auf dem eigenen Staatsgebiet zählen.<sup>3</sup> Das aus diesen Rechten folgende Gebot der Achtung der Souveränität anderer Staaten macht es erforderlich, die Erlaubnis eines betroffenen fremden Staates einzuholen, bevor hoheitliche Tätigkeiten auf dessen Staatsgebiet ausgeübt werden.<sup>4</sup> Ohne eine solche Erlaubnis bleibt der ermittelnde Staat nach den Grundsätzen des Völkerrechts darauf verwiesen, die behördliche Mithilfe des betroffenen Staates im Rechtshilfeverfahren zu ersuchen, um Ermittlungen auf dessen Staatsgebiet vorzunehmen oder vornehmen zu lassen.<sup>5</sup>

Während Ermittlungsbefugnisse sich also auf das eigene Staatsgebiet beschränken, weisen Ermittlungsverfahren aufgrund der Globalisierung und

---

<sup>1</sup> Frank P. Schuster, „Verwertbarkeit von Beweismitteln bei grenzüberschreitender Strafverfolgung“, ZIS 2016, S. 564, 564; Daskal, „Transnational Government Hacking“, Journal of National Security Law & Policy 2020, S. 677, 680; Bell, „Strafverfolgung und die Cloud: Strafprozessuale Ermächtigungsgrundlagen und deren völkerrechtliche Grenzen“, Duncker & Humblot 2019, S. 159.

<sup>2</sup> Marberth-Kubicki, „Computer- und Internetstrafrecht“, Beck 2005, S. 236.

<sup>3</sup> Epping, in: Epping/Heintschel von Heinegg (Hrsg.), Ipsen, Völkerrecht, 2018, § 7 Rn. 261.

<sup>4</sup> Tiedemann, „Die Auslandskopf-Überwachung nach der TKÜV 2005“, CR 2005, S. 858, 862.

<sup>5</sup> Seitz, „Transborder Search: A New Perspective in Law Enforcement?“, Yale Journal of Law and Technology 2005, S. 22, 27.

Digitalisierung immer mehr internationale Bezüge auf. Moderne Telekommunikations- und Informationstechnologie erlaubt es Tätern, sich international zu vernetzen. Insbesondere in den Bereichen des Terrorismus und der organisierten Kriminalität zeigt sich eine große Prävalenz an internationalen Tätergruppierungen: Kaum eine groß angelegte OK-Gruppierung ist heutzutage nicht international tätig. So wurden in Deutschland für das Jahr 2019 426 OK-Verfahren mit Auslandsbezug gemeldet, bei denen Verbindungen der Täternetzwerke in insgesamt 123 verschiedene Länder nachgewiesen werden konnten.<sup>6</sup> Aber auch außerhalb der internationalen organisierten Kriminalität kann schon die Nutzung des Internets per se Ermittlungsverfahren einen internationalen Einschlag geben.<sup>7</sup> Grund dafür ist die Architektur und technische Funktionsweise des Internets, wie sich exemplarisch anhand des Unternehmens „Google“ verdeutlichen lässt: Im Oktober 2018 waren bei *Google Mail* (Gmail) 1,5 Milliarden Nutzer registriert.<sup>8</sup> Unabhängig davon, ob die Nutzer den Webmail-Service (Abruf des E-Mail-Postfachs über den Browser) oder einen E-Mail Client (z.B. Gmail App auf dem Smartphone oder Tablet) nutzen, wird jede E-Mail, die über einen Gmail-Account gesendet oder empfangen wird, inklusive Anhang auf den Servern von Google gespeichert.<sup>9</sup> Google verfügt neben Rechenzentren in Nord-, Mittel- und Südamerika und in Asien auch über Server in Europa. Letztere befinden sich allerdings nicht in Deutschland, sondern in Irland, Finnland, Belgien und den Niederlanden.<sup>10</sup> Für das Strafverfahren bedeutet dies, dass die Strafverfolgungsbehörden nicht auf die bei Gmail vorgehaltenen E-Mails eines Verdächtigen zugreifen können – sofern er diese nicht lokal auf seinem Computer gespeichert hat – ohne auf Rechenzentren in anderen Jurisdiktionen zuzugreifen.

In Ermittlungsverfahren, denen die eben dargelegten internationalen Bezüge anhaften, ist es für die Ermittlung digitaler Beweise, anders als bei der Ermittlung gegenständlicher Beweise, nicht notwendig, dass die deutschen Ermittlungsbehörden physisch auf fremdem Staatsgebiet anwesend sind.

---

<sup>6</sup> Bundeskriminalamt, „Bundeslagebild Organisierte Kriminalität 2019“, 2019, S. 58; ähnliche Ergebnisse auch auf Landesebene, vgl: Ministerium des Innern Brandenburg, „Organisierte Kriminalität wird internationaler: Nr. 154/2005“, 25.08.2005, zuletzt geprüft am: 29.12.2019, wo 81 % der OK-Verfahren internationale Bezüge aufwiesen.

<sup>7</sup> M. Gercke, „Die Bekämpfung der Internetkriminalität als Herausforderung für die Strafverfolgungsbehörden“, MMR 2008, S. 291, 296.

<sup>8</sup> Vgl. Twitter-Post von Googlemail vom 26.10.2018, abrufbar unter: [https://twitter.com/gmail/status/1055806807174725633?ref\\_src=twsr%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1055806807174725633%7Ctwgr%5E%7Ctwcon%5Es1\\_c10&ref\\_url=https%3A%2F%2Fstadt-bremerhaven.de%2Fgmail-15-milliarden-active-nutzer%2F](https://twitter.com/gmail/status/1055806807174725633?ref_src=twsr%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1055806807174725633%7Ctwgr%5E%7Ctwcon%5Es1_c10&ref_url=https%3A%2F%2Fstadt-bremerhaven.de%2Fgmail-15-milliarden-active-nutzer%2F), zuletzt geprüft am: 30.05.2021.

<sup>9</sup> Spoenle, „Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?“, 2010, S. 5.

<sup>10</sup> <https://www.google.com/about/datacenters/inside/locations/index.html>.

Vielmehr können die Beweise mittels Fernzugriff erlangt werden und somit quasi auf das eigene Staatsgebiet „herübergezogen werden“.

Vor dem Hintergrund dieser Problematik drängt sich – aus deutscher Sicht – die folgende Überlegung auf: Dürfen die Ermittlungsbehörden aufgrund der Möglichkeit, bei den Ermittlungsmaßnahmen im eigenen Hoheitsgebiet zu verweilen, ihren Arm aus Deutschland heraus ins Ausland „ausstrecken“ und so auch sich im Ausland befindliche Anschlüsse überwachen und Daten von Servern in fremden Hoheitsgebieten abrufen? Oder müssen sie vielmehr auch bei ihren Ermittlungshandlungen bezüglich digitaler Beweise strikt auf das deutsche Staatsgebiet beschränkt bleiben und bei Auslandsbezügen stets um Rechtshilfe des betroffenen Staates ersuchen? Wenn Letzteres zutrifft, welche Konsequenzen hat es für die Beweisverwertung im Strafverfahren, wenn ein Zugriff auf digitale Daten unter Verstoß gegen völkerrechtliche Grundsätze erfolgt?

Die Untersuchung der Frage, wie das Völkerrecht die *deutschen* Ermittlungsbehörden bei der Ermittlung digitaler Beweise begrenzt, wird in der vorliegenden Arbeit in drei Schritten erfolgen, wobei internationale Ermittlungsbehörden wie die Europäische Staatsanwaltschaft, die zum 01. Juni 2021 ihre Arbeit aufnahm<sup>11</sup>, Inter- und Europol außen vor bleiben. In einem ersten Teil wird untersucht, welche nationalen Ermittlungsbefugnisse den Ermittlungsbehörden für einen Zugriff auf Daten nach der StPO zur Verfügung stehen, wobei andere Gesetze zur Strafverfolgung, wie das Zollfahndungsdienstgesetz, außen vor bleiben. Dabei wird auch auf die im Jahr 2021 eingeführten Erweiterungen der Verkehrs-, Nutzungs- und Bestandsdatenauskunft eingegangen werden. In einem zweiten Teil wird dargestellt, wie völkerrechtliche Grundsätze diese Ermittlungsmaßnahmen räumlich begrenzen. Dafür wird zunächst die Anwendbarkeit des Völkerrechts auf internationale Telefonnetze und das Internet erörtert, bevor geprüft wird, ob Ermittlungshandlungen, die ausschließlich von deutschem Territorium aus durchgeführt werden, überhaupt völkerrechtliche Relevanz zukommen kann. Nach der Feststellung, dass auch Zugriffe auf Daten, die aus dem Inland initiiert werden, gegen das Völkerrecht verstossen können, werden die einschlägigen Rechtshilfeinstrumente der Bundesrepublik Deutschland dargestellt. Im dritten und damit letzten Schritt wird untersucht, welche Konsequenzen die Völkerrechtswidrigkeit einer Beweiserhebung auf die Verwertbarkeit der Beweismittel im Verfahren gegen den Beschuldigten hat. Bearbeitungsstand der vorliegenden Arbeit ist der 30.10.2021. In Hinblick auf die Änderung der Rechtslage durch das Inkrafttreten des neuen TKG und des TTDSG und durch den Beschluss des Zweiten Zusatzprotokolls zur Cybercrime Convention wurde die Arbeit zur Drucklegung diesbezüglich auf den Stand November 2022 aktualisiert.

---

<sup>11</sup> <https://www.consilium.europa.eu/de/policies/eppo/#>, zuletzt geprüft am: 30.09.2020.