

# Inhaltsverzeichnis

<b>Einleitung</b>	17
-------------------	----

## *Kapitel 1*

<b>Technische Grundlagen der unkörperlichen Telekommunikation und des Internets</b>	20
---	----

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

## *Kapitel 2*

<b>Ermächtigungsgrundlagen für den Zugriff auf nicht-gegenständliche Beweise im deutschen Strafverfahren</b>	39
--	----

A. Verdeckte Ermittlungsmaßnahmen	40
I. Die zentrale Bedeutung des Telekommunikationsbegriffs für die Bestimmung der repressiven Zugriffsmöglichkeiten auf ermittlungsrele- vante 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“ Telekommunikationsüber- wachung .....	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/Bundesrepu- blik Deutschland .....	64
(2) LG München I, Beschluss vom 4.12.2019 – 9 Qs 15/19	65
cc) Abschaffung des Problems durch das TKModG in Umset- zung des Europäischen Elektronischen Kommunikations- kodexes .....	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-Telekommunikationsüber- wachung .....	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 Mobilfunkend- geräten .....	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.): Auskunftersuchen 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. Offene Ermittlungsmaßnahmen .....	93
I. § 94 StPO: Sicherstellung und Beschlagnahme von Gegenständen zu Beweis Zwecken .....	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

A. Territorialität als Kernelement des Völkerrechts .....	107
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 <i>sui generis</i> 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>
<b>I. Extraterritorialität ohne physische Penetration eines fremden Staatsgebietes: Eingriff in eine fremde Gebietshoheit durch datenbezogene Ermittlungsmaßnahmen? .....</b>	<b>122</b>
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 Herausgabeordnung 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) <i>Domaine réservé</i> .....	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 <i>loss of location</i> 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 ( <i>countermeasures</i> ) .....	172
2. Notlage ( <i>distress</i> ) und Notstand ( <i>necessity</i> ) .....	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 Herausgabeordnung .....	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 Rechtshilferegulungen 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-Telekommu- nikationsüberwachung, 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 Spei- chermedien .....	209
1. Grundsatz .....	209
2. Rechtshilfe .....	210
IV. Die Ermittlungsgeneralklausel, §§ 161 Abs. 1, 163 Abs. 1 StPO .....	210
C. Fazit zu den völkerrechtlichen Auswirkungen auf die deutschen Ermitt- lungsbefugnisse .....	211

*Kapitel 5*

**Die Verwertbarkeit völkerrechtswidrig erlangter Beweise** 212

A. Herrschende Meinung in Rechtsprechung und Literatur .....	212
B. Eigene Ansicht .....	213
I. Prämisse 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 Beweisverwertungsverböten .....	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 faïres Verfahren .....	219
ee) Stellungnahme und Ergebnis .....	221
(1) Entstehung des Beweisverwertungsverbots .....	221
(a) Recht auf faïres Verfahren und Informationsbeherr- schungsrecht maßgebend .....	221
(b) Unzulänglichkeït der Abwägungslehre, Rechtskreis- theorie und Schutzzwecktheorie .....	224
(2) Berücksichtigungsfähigkeit hypothetischer Ermittlungs- verläufe .....	225
(a) Grundsatz: Keine Berücksichtigungsfähigkeit .....	225
(b) Berücksichtigungsfähigkeit bei Vorliegen eines Erlaubnistatumsstandsirrtums seitens der Behörden .....	226
3. Ergebnis zur Entstehung eines Beweisverwertungsverbots .....	228
III. Bedeutung der beweisrechtlichen Grundsätze für völkerrrechtswidrig erlangte Beweismittel .....	228
1. Das Gebot der Achtung fremdstaatlicher Souveränität und Art. 25 GG als Beweiserhebungsverbot .....	228
2. Verwertungsverbot bei völkerrrechtswidriger Beweiserlangung .....	229
a) Grundsatz .....	229
b) Besonderheiten bei der Verwertbarkeit bei völkerrrechtswidrig 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