

Schriften zum Prozessrecht

Band 319

**Strafverfahrensrechtliche Fragen bei
Daten aus sog. »Anom-Chatforen«**

Von

Maximilian Mrokon



Duncker & Humblot · Berlin

MAXIMILIAN MROKON

Strafverfahrensrechtliche Fragen bei Daten
aus sog. »Anon-Chatforen«

Schriften zum Prozessrecht

Band 319

Strafverfahrensrechtliche Fragen bei Daten aus sog. »Anom-Chatforen«

Von

Maximilian Mrokon



Duncker & Humblot · Berlin

Die Rechtswissenschaftliche Fakultät der Eberhard Karls Universität Tübingen
hat diese Arbeit im Jahre 2024 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.

D21

Alle Rechte vorbehalten
© 2025 Duncker & Humblot GmbH, Berlin
Satz: 3w+p GmbH, Rimpau
Druck: CPI books GmbH, Leck
Printed in Germany

ISSN 0582-0219
ISBN 978-3-428-19588-6 (Print)
ISBN 978-3-428-59588-4 (E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ☺

Verlagsanschrift: Duncker & Humblot GmbH, Carl-Heinrich-Becker-Weg 9,
12165 Berlin, Germany | E-Mail: info@duncker-humblot.de
Internet: <https://www.duncker-humblot.de>

Meiner Familie

Vorwort

Die vorliegende Arbeit wurde im Wintersemester 2024/25 von der Juristischen Fakultät der Universität Tübingen als Dissertation angenommen. Literatur und Rechtsprechung konnten bis März 2025 berücksichtigt werden.

Besonderer Dank gilt meinem Doktorvater, Herrn Professor Dr. Jörg Eisele, für die hervorragende Betreuung dieses Vorhabens. Seine wertvollen Anregungen waren stets bereichernd. Auch hat er mir die notwendigen wissenschaftlichen Freiräume eingeräumt, um eigene Gedanken zu entwickeln.

Zudem gilt mein Dank auch Herrn Professor Dr. Dr. h.c. Bernd Heinrich, der nicht nur das Zweitgutachten erstellt und die Arbeit mit weiteren wertvollen Hinweisen versehen hat, sondern auch dafür, dass er es mir durch die Tätigkeit als akademischer Mitarbeiter an seinem Lehrstuhl überhaupt erst möglich gemacht hat, dieses Projekt in absehbarer Zeit fertigstellen zu können.

Auch danke ich allen Lehrstuhlkollegen und -kolleginnen, nicht nur für die konstruktive Zusammenarbeit, sondern auch die unzähligen angenehmen und stets bereichernden Gespräche und die gemeinsame Zeit. Ebenso danke ich meinen übrigen Freunden, mit denen ich mich stets kritisch über meine Thesen und Gedanken, aber auch über fachfremde Themen, austauschen konnte. So vor allem mit Jonathan Kapp in unzähligen gemeinsamen Mittagspausen.

Darüber hinaus danke ich auch meiner Partnerin, Dr. Laura Millak, die durch ihre Art und ihre Unterstützung maßgeblich zum Erfolg dieser Arbeit beigetragen hat.

Abschließend möchte ich auch meiner Familie danken, vor allem meinen Eltern Sabine Pfaff-Mrokon und Heinrich Mrokon, die mir das Studium der Rechtswissenschaften überhaupt erst ermöglichten und die mich während der anstrengendsten Phasen dieser Ausbildung immer unterstützten. Auch gebührt mein Dank meinen Brüdern Alexander, Konstantin und Frederik, durch die ich die Kunst des (gesitteten) Streitens erlernen konnte.

All diese Personen gaben dieser Arbeit nicht nur die richtigen Impulse, sondern auch dem Verfasser mehr.

Tübingen, im April 2025

Maximilian Mrokon

Inhaltsverzeichnis

1. Kapitel	15
A. Einführung	15
I. Einleitung	15
II. Gang der Untersuchung	16
B. Ziel der Untersuchung	17
 2. Kapitel	18
A. Tatsächliche und rechtliche Grundlagen	18
I. Tatsächlicher Sachverhalt und technische Grundlagen	19
1. Vorgeschichte und chronologischer Ablauf der „Anom“-Ermittlungen	19
a) Frühere Ermittlungen und Entwicklung der „Anom-App“	20
b) „Operation Trojan Shield“ und Inbetriebnahme der „Anom“-Geräte	22
c) Eintritt in die eigentliche Datensammlung	23
d) Weitergabe an deutsche Behörden	25
2. Funktionsweise der „Anom-App“	25
a) Grundlagen der Kryptographie	25
aa) Begriff und Relevanz der Kryptographie	26
bb) Gängige Methoden der Verschlüsselung	27
cc) Kryptografie als Herausforderung der Strafverfolgung	28
b) Qualifikation und Funktionsweise der „Anom-Chatforen“	29
c) Ausleiten der Daten durch das FBI	31
3. Abgrenzung zu einzelnen Ermittlungsmaßnahmen im Rahmen der „Operation Trojan Shield“	31
a) Allgemeines zu „EncroChat“	32
aa) Sachverhalt und Rechtsfragen zu „EncroChat“	32
(1) Sachverhalt	32
(2) Rechtsfragen	33
bb) Zwischenergebnis	35
b) Unterschiede und Gemeinsamkeiten der einzelnen Systeme	35
4. Organisierte Kriminalität in Deutschland	38
a) Definition der organisierten Kriminalität	39
b) Lage in Deutschland	40

c) Internationale Aspekte der Organisierten Kriminalität	43
d) Erfolg der „Operation Trojan Shield“	44
5. Zwischenergebnis	45
II. Rechtliche Grundlagen	48
1. Telekommunikationsüberwachung als Grundrechtseingriff nach innerstaatlichem Recht	48
a) Grundrechtlicher Schutz der Telekommunikation	48
aa) Betroffene Grundrechte	49
(1) Brief-, Post- und Fernmeldegeheimnis gemäß Art. 10 Abs. 1 GG ..	49
(2) Allg. Persönlichkeitsrecht gemäß Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG	52
(a) Recht auf informationelle Selbstbestimmung	53
(b) Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	54
(c) Abgrenzung zwischen den Grundrechten und zu Art. 10 GG ..	56
(3) Berufs- und Eigentumsfreiheit gemäß Art. 12 GG und Art. 14 GG ..	58
(4) Räumliche Geltung der Grundrechte	61
(5) Grundrechtliche Schutzpflichten	64
bb) Überwachungsmaßnahmen als Eingriffe in Grundrechte	66
(1) Der „klassische“ Eingriffsbegrieff	66
(2) Der „faktische“ und „mittelbare“ Eingriff	66
(3) Einwilligung in Grundrechtseingriff	69
(4) Zwischenergebnis	70
cc) Verfassungsrechtliche Rechtfertigung etwaiger Eingriffe	71
(1) Notwendigkeit einer Ermächtigungsgrundlage	71
(2) Verfassungsrechtliche Anforderungen an den Gesetzesvorbehalt ..	72
(a) Allgemeine Anforderungen	72
(b) Besonderheiten im Rahmen von Art. 10 Abs. 1 GG	75
(c) Besonderheiten im Rahmen von Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG	79
(d) Besonderheiten im Rahmen von Art. 12 GG	80
(e) Besonderheiten im Rahmen von Art. 14 GG	80
b) Darstellung ausgewählter Ermächtigungsgrundlagen	81
aa) Nachrichtendienstliche Ermächtigungsgrundlagen	81
bb) Präventive Ermächtigungsgrundlagen	83
(1) Grundlagen	83
(2) Anordnungsvoraussetzungen	84
(a) Wesentliche Anordnungsvoraussetzungen	84
(b) Weitere Voraussetzungen	85

cc) Repressive Ermächtigungsgrundlagen	85
(1) Telekommunikationsüberwachung gemäß § 100a Abs. 1	
Satz 1 StPO	86
(a) Grundlagen	86
(b) Anordnungsvoraussetzungen	89
(aa) Vorliegen von Telekommunikation	89
(bb) Tatverdacht im Sinne des § 100a Abs. 1 und 2 StPO	92
(α) Tatsachenbasis	92
(β) Verdacht	96
(γ) Katalogtat	100
(δ) Beurteilungsspielraum und Perspektive	102
(cc) Tat, die auch im Einzelfall schwer wiegt	103
(dd) Subsidiarität	104
(ee) Verhältnismäßigkeit der Anordnung	105
(c) Betroffene der Maßnahme	106
(d) Technische Durchführung der Überwachungsmaßnahme	108
(2) Quellen-Telekommunikationsüberwachung gemäß § 100a Abs. 1	
Satz 2 und 3 StPO	110
(a) Grundlagen	110
(b) Abgrenzung zwischen § 100a Abs. 1 Satz 1, 2 und 3 StPO	114
(c) Eingriffsvoraussetzungen	116
(d) Betroffene der Maßnahme	118
(e) Technische Durchführung	118
(aa) Ende-zu-Ende-Verschlüsselung	118
(bb) Technische Mittel	119
(cc) Anforderungen an technische Mittel gemäß § 100a	
Abs. 5 StPO	122
(3) Online-Durchsuchung gemäß § 100b Abs. 1 Satz 1 StPO	124
(a) Grundlagen	124
(b) Abgrenzung zu § 100a Abs. 1 StPO	126
(c) Anordnungsvoraussetzungen	126
(d) Betroffener der Maßnahme	127
(e) Technische Durchführung	127
(4) Verfahren und Kernbereichsschutz	128
(5) Stellungnahme	130
dd) Sonderfall der „antizipierten Strafverfolgung“	131
(1) Problemherkunft und Begriff	132
(2) Vor(feld)ermittlungen als Eingriff in Grundrechte	133
(3) Zulässigkeit von Vor(feld)ermittlungen	134
(4) Verwendung der Erkenntnisse aus Maßnahmen der „antizipierten	
Strafverfolgung“	136

c) Exkurs: Zuständigkeit und Kompetenzen amerikanischer Bundesbehörden am Beispiel des FBI	138
2. (Weiter-)Verwendung von Daten und Ermächtigungsgrundlage	141
a) Unterscheidung zwischen Verwendung und Verwertung	141
b) Grundrechtsrelevanz einer (Weiter-)Verwendung von Daten	142
c) Mögliche (strafprozessuale) Ermächtigungsgrundlagen	144
aa) § 261 StPO	144
bb) § 244 Abs. 2 StPO	145
cc) § 161 Abs. 1 StPO	147
dd) § 203 StPO	148
ee) §§ 100e Abs. 6, 161 Abs. 3 Satz 1 und 479 Abs. 2 Satz 1 StPO	149
ff) § 77 IRG i. V. m. innerstaatlicher Norm	151
gg) Ermächtigungsgrundlage für die Stellung von Rechtshilfeersuchen? ..	153
hh) Stellungnahme	154
3. Grundlagen der Beweisverbote	154
a) Allgemeines	155
aa) Zweck der Beweisverbote	155
bb) Beweiserhebungsverbote	156
cc) Beweisverwertungsverbote	157
(1) Selbstständige Beweisverwertungsverbote	157
(2) Unselbstständige Beweisverwertungsverbote	158
(a) „Rechtskreistheorie“	158
(b) „Abwägungslehre“	160
(c) „Widerspruchslösung“	161
(d) Weitere Ansätze	162
b) Nachweis eines Beweisverbots	163
4. Verwertbarkeit von im Ausland erhobenen Beweisen	164
a) Grundlagen der Rechtshilfe	164
aa) Begriffe der Rechtshilfe	165
bb) Relevante Rechtsquellen der Rechtshilfe	168
(1) Innerhalb der EU	168
(2) Gegenüber den Vereinigten Staaten	169
cc) Zeitlicher Ablauf bei Stellung eines Rechtshilfeersuchens durch inländische Hoheitsträger	170
b) Die Verwertbarkeit von im Ausland gewonnenen Beweisen	171
aa) Rechtsprechung des Bundesgerichtshofes	172
bb) Ansichten in der Literatur	179
cc) Vorzugswürdige Ansicht der Rechtsprechung	183
dd) Inhalt des <i>ordre public</i>	186
ee) Zwischenergebnis	197

B. Zwischenergebnis	200
3. Kapitel	203
A. Verwertbarkeit der erlangten Daten aus „Anom-Chatforen“	203
I. Einordnung in den Rahmen der repressiven Rechtshilfe?	203
II. Anwendbare Ermächtigungsgrundlage	205
1. Notwendigkeit einer zeitlichen Aufteilung	205
2. Grundrechtsrelevanz der einzelnen Akte	208
a) Modifikation und Verteilung der Endgeräte	208
b) „Beta-Test“ in Zusammenarbeit mit australischen Behörden	211
c) Datenerhebung in Kooperation mit EU-Mitgliedsstaat	211
d) Übermittlung an deutsche Behörden	211
e) Ermittlungs- und anschließendes Gerichtsverfahren	213
f) Zwischenergebnis	213
3. Korrespondierende Ermächtigungsgrundlagen	214
a) Qualifikation als Maßnahme nach § 100a StPO oder § 100b StPO?	214
b) Anzuwendende Ermächtigungsgrundlage	216
aa) Stellung des Rechtshilfeersuchens	218
bb) Ermittlungs-, Zwischen- und Hauptverfahren	218
cc) Urteil	219
4. Zwischenergebnis	220
III. Mögliche Beweis(verwertungs)verbote	220
1. Vorliegen von Beweis(verwertungs)verboten	221
a) Beweis(last)problematik	221
b) Verstöße ausländischer Behörden	225
aa) Fehlen des erforderlichen (Anfangs-)Verdachts	225
bb) Verstoß gegen Art. 8 Abs. 1 EMRK	229
cc) Verstoß gegen Art. 31 Abs. 1 RL EEA bzw. § 91g Abs. 6 IRG	236
dd) Verstoß gegen das völkerrechtliche Souveränitätsprinzip	240
ee) Befugnis-Shopping der amerikanischen Behörden	240
ff) Verstoß gegen § 136a StPO (analog)	242
gg) Rechtsstaatswidrige Tatprovokation	246
hh) Anlasslose Vorratsdatenspeicherung	248
ii) Zwischenergebnis	249
c) Verstöße inländischer Behörden	249
aa) Verstoß gegen Art. 6 Abs. 1 und 3 EMRK	249
bb) Verstoß gegen grundrechtliche Schutzpflichten	262
d) Selbstständige Beweisverwertungsverbote	264
2. Zwischenergebnis	266

B. Abschließende Betrachtung	266
I. Wiederholbarkeit der „Anom“-Ermittlungen	266
II. Weitere Ansätze zum Umgang mit verschlüsselter Kommunikation	267
1. Technische Ansätze	267
2. Tatsächliche Ansätze	268
3. Rechtliche Ansätze	269
a) Regulierung der kryptierten Telekommunikation	269
b) Möglichkeit der „Anom“-Ermittlungen am Maßstab der inländischen Rechtsordnung	270
aa) Erneute zeitliche Aufteilung	271
(1) Modifikation der Endgeräte und Einrichtung eines Servers	271
(2) Verteilung der Endgeräte durch die Vertrauensperson	271
(3) „Beta-Test“ der Endgeräte	275
(4) Eigentliche Datenerhebung	275
(5) Verwertung im anschließenden Verfahren	277
bb) Stellungnahme	277
4. Ausblick	277
Literaturverzeichnis	282
Sachwortverzeichnis	307

1. Kapitel

A. Einführung

I. Einleitung

Das 21. Jahrhundert zeichnet sich insbesondere durch eine zunehmende Digitalisierung aus. Dabei ist bemerkenswert, dass sämtliche Bereiche des modernen Lebens von dieser Entwicklung betroffen sind und sich dadurch bereits angepasst haben oder sich sukzessiv anpassen werden müssen. Insbesondere ist hiervon auch die Art und Weise der Telekommunikation betroffen. Diese spielt sich vermehrt in technischen Medien ab. So hat der herkömmliche Brief schon seit geraumer Zeit als Telekommunikationsmedium stark an Bedeutung verloren. Ein Kommunizieren in der heutigen digitalen Gesellschaft ohne den Rückgriff auf technische Endgeräte ist nahezu undenkbar geworden. Dies gilt dabei natürlich auch für das kriminelle Milieu.

Im Zuge dieser Entwicklung steht dabei vor allem auch der Schutz der durch die Telekommunikation übermittelten Daten im Vordergrund. Ein solches Interesse kann sowohl bei gewissen Personengruppen¹, als auch im kriminellen Bereich bestehen. Demgegenüber muss sich auch eine effektive Strafverfolgung eingehend mit den fortschreitenden technischen Neuerungen immer wieder befassen und kann neue Entwicklungen nicht ignorieren. Umso bedrohlicher, auch für den Bestand des Staates an sich, ist es, wenn die Strafverfolgungsbehörden aufgrund ihrer technischen Möglichkeiten nicht mehr effektiv in der Lage sind, potentiell Zugriff auf kriminelle digitale Inhalte zu nehmen.

Außer Frage steht dabei, dass aufgrund der grundrechtlichen Werteentscheidung keine „Strafverfolgung um jeden Preis“² stattfinden darf. Nichtsdestotrotz besteht ebenfalls auch ein staatliches Interesse an einer effektiven Strafverfolgung.

Dass es bei diesen widerstreitenden Interessen zwangsläufig zu Kollisionen kommt ist genauso vorhersehbar wie auch unbestreitbar. Und auch die in dieser Arbeit untersuchten „Anom-Chatforen“ sind wohl genau auf dem Ereignishorizont dieser widerstreitenden Interessen anzusiedeln. Denn so ist es nachvollziehbar, dass eine „Strafverfolgung um jeden Preis“ angenommen wird, wenn eine Ermittlungsbehörde scheinbar unentschlüsselbare Smartphones unter Mithilfe einer Vertrau-

¹ Vgl. hierzu die Personen und Personengruppen bei *Deusch/Eggendorfer*, K&R 2022, 404 (406 f.).

² Statt vieler nur *Gebhard/Michalke*, NJW 2022, 655 (659); BGHSt 51, 285 (290).

ensperson an Mitglieder von kriminellen Organisationen verteilt, um anschließend nahezu alle über diese Smartphones versendeten und empfangenen Nachrichten zu überwachen und auszuwerten.³ Gleichzeitig bestätigt der Ermittlungserfolg eines solchen Vorgehens in gewisser Weise die Annahme der Strafverfolgungsbehörden nachträglich.⁴ Der Ermittlungserfolg dürfte Kritiker der Maßnahme zwar nicht überzeugen. Jedoch zeigen die hier untersuchten „Anom-Chatforen“ auf, dass umstrittene Ermittlungsmethoden einen großen Erfolg versprechen können.

Aufgrund der bisherigen Auseinandersetzung mit dieser Thematik und der Kollision der widerstreitenden Interessen lohnt es sich auch in rechtlicher Hinsicht, die Auseinandersetzung mit diesem Thema zu suchen. Denn die Nutzung von verschlüsselten Messengerdiensten zu kriminellen Zwecken ist auch eine Thematik, die in ihrer Bedeutung weit über die hier untersuchten Ermittlungsgeschehnisse hinaus Bedeutung erlangt.

II. Gang der Untersuchung

Die Untersuchung wird dabei zunächst auf die tatsächlichen und rechtlichen Grundlagen eingehen die notwendig sind, um die Thematik vollumfänglich behandeln zu können.⁵ Dabei werden auch die innerstaatlichen rechtlichen Grundlagen der Telekommunikationsüberwachung einer kritischen Prüfung unterzogen und aufgezeigt, an welchen rechtlichen Gesichtspunkt auch die innerstaatliche Dogmatik Schwächen aufweist.⁶ Ebenso verfahren wird bei der Betrachtung des Rechtshilfrechts in Strafsachen.⁷

Nachdem die rechtlichen und tatsächlichen Grundlagen eingehend erläutert wurden, wird in einem dritten Kapitel ein eigener Ansatz zur Verwertbarkeit der Daten aus den „Anom-Chatforen“ dargestellt.⁸ Dieser bezieht alle der bisher geäußerten Gesichtspunkte der rechtlichen Auseinandersetzung mit ein und setzt sich mit diesen kritisch auseinander.⁹

Nachdem Stellung zur Frage der Verwertbarkeit der Daten bezogen wurde, wird in einem letzten Kapitel der Frage nachgegangen, welche Ansätze zu einem besseren Umgang mit verschlüsselten Messengerdiensten in Betracht kommen, wobei zwischen technischen, tatsächlichen und rechtlichen Ansätzen unterschieden werden

³ Siehe ausführlich zum Sachverhalt unter 2. Kapitel A.I. 1. sowie zur Funktionsweise der „Anom-Chatforen“ 2. Kapitel A.I. 1.

⁴ Siehe zum Erfolg der „Operation Trojan Shield“ unter 2. Kapitel A.I. 4. d).

⁵ 2. Kapitel A.

⁶ 2. Kapitel A.II. 1.b).

⁷ 2. Kapitel A.II. 4.

⁸ 3. Kapitel A.

⁹ 3. Kapitel A.

soll.¹⁰ Ausgehend von den bisherigen Ergebnissen wird zudem noch ein abschließender Ausblick gewagt.¹¹

B. Ziel der Untersuchung

Das Ziel der Untersuchung besteht dabei vor allem darin, die bisher zu der Problematik geäußerten Ansätze auf ihre Tragfähigkeit hin zu untersuchen und im Anschluss hieran einen eigenen Lösungsansatz zu entwickeln. Denn nach hier vertretener Ansicht wird die bisherige Debatte weitgehend von hypothetischen Erwägungen geprägt, die nicht bewiesen oder beweisbar sind. Zudem ist bezüglich der bisherigen Diskussion zu vermerken, dass es oftmals zu einer Vermengung der einzelnen und unabhängig voneinander zu behandelnden rechtlichen Gesichtspunkte kommt, sodass ein Anliegen dieser Arbeit ebenfalls darin zu sehen ist, diese Vermischung aufzulösen und ausführlich alle in Frage kommenden rechtlichen Erwägungen abzuhandeln. Dabei sollen die Ausführungen über die „Anom-Chatforen“ hinaus grundsätzliche Antworten auf die strafverfahrensrechtlichen Fragen geben, die sich bei ähnlichen Ermittlungsmaßnahmen stellen.

Mit der weitergehenden Betrachtung anderer Lösungsansätze zum besseren Umgang mit verschlüsselten Messengerdiensten soll zudem deutschen Behörden ein möglicher Denkanstoß gegeben werden, um die bisherigen Methoden im Umgang mit verschlüsselten Messengerdiensten zu überdenken und damit effizienter mit verschlüsselten Messengerdiensten im kriminellen Kontext umgehen zu können.

¹⁰ 3. Kapitel B.II.

¹¹ 3. Kapitel B.II.4.