

EuropaInstitut

AN DER UNIVERSITÄT ZÜRICH

Franziskus Jaklin

Verwertbarkeit von Daten aus ausländischer Überwachung von Messenger-Diensten

Eine Analyse der EncroChat-, SkyECC- und Anom-Überwachung

EIZ Publishing

Verwertbarkeit von Daten aus ausländischer Überwachung von Messenger-Diensten

Eine Analyse der EncroChat-, SkyECC- und Anom-Überwachung

Dissertation

der rechtswissenschaftlichen Fakultät
der Universität Zürich
zur Erlangung der Würde eines Doktors der Rechtswissenschaft

vorgelegt von

Franziskus Jaklin

genehmigt auf Antrag von
Prof. Dr. Felix Bommer
und
Prof. Dr. Marc Thommen

Die Rechtswissenschaftliche Fakultät der Universität Zürich gestattet hierdurch die Drucklegung der vorliegenden Dissertation, ohne damit zu den darin ausgesprochenen Anschauungen Stellung zu nehmen.

Zürich, den 30. September 2026

Der Dekan: Prof. Dr. Thomas Gächter

© 2026 – CC BY-NC-ND (Werk), CC BY (Text)

Verlag: EIZ Publishing (eizpublishing.ch), Bellerivestrasse 49, 8008 Zürich,
eizpublishing@europa-institut.ch
Autor: Franziskus Jaklin
ISBN:
978-3-03994-136-0 (Print – Softcover)
978-3-03994-137-7 (Print – Hardcover)
978-3-03994-138-4 (ePub)
DOI: https://doi.org/10.36862/60WK-4D9R
Version: 1.01 – 20261029

Die vorliegende Dissertation wurde von Franziskus Jaklin eingereicht und am 30. September 2026 von der Rechtswissenschaftlichen Fakultät der Universität Zürich auf Antrag von Herrn Prof. Dr. Felix Bommer (Erstgutachter) und Herrn Prof. Dr. Marc Thommen (Zweitgutachter) genehmigt.

Dieses Werk ist als gedrucktes Buch sowie als E-Book (open access) in verschiedenen Formaten verfügbar. Weitere Informationen finden Sie unter der URL: https://eizpublishing.ch/publikationen/verwertbarkeit-von-daten-aus-auslaendischer-ueberwachung-von-messenger-diensten/.

Vorwort

Die vorliegende Dissertation wurde im Herbstsemester 2026 von der Rechtswissenschaftlichen Fakultät der Universität Zürich angenommen.

Mein Dank gilt zunächst Prof. Felix Bommer für die kompetente Betreuung und das äusserst schnelle Erstellen des Erstgutachtens. Ebenso danke ich Prof. Marc Thommen für das gleichermassen zügig verfasste Zweitgutachten.

Ferner bedanke ich mich bei meinem früheren Arbeitgeber, der Strafrechtskanzlei taormina law AG, die mir durch ein flexibles Pensum und grosse Rücksichtnahme das rasche Verfassen meiner Dissertation ermöglicht hat.

Mein grösster Dank gilt jedoch meiner Familie, deren umfassende Unterstützung unerlässlich war.

Zürich, im Oktober 2026 Franziskus Jaklin

Inhaltsverzeichnis

Literaturverzeichnis XV

Materialienverzeichnis XXV

Abkürzungsverzeichnis XXVII

A. Ereignisdarstellung 1

I. EncroChat 1
1. Eckdaten 1
2. Funktionen 2
3. Untersuchungsbeginn und involvierte Staaten 3
4. Aufklärungszugriffe auf die Server 4
5. Genehmigungsbeschlüsse 5
6. Zugriff auf die Endgeräte 6
a) Aufspielen der Schadsoftware 6
b) Historical data collection 6
c) Forward facing collection 7
d) Ausmass der Überwachung 8
7. Zwischenstaatlicher Informationsaustausch und Datenübermittlung 8
8. Datenbearbeitung 9
9. Ermittlungserfolge 11
10. Prozessuales: Zielperson und Verfahrensart 11

II. SkyECC 12
1. Eckdaten 12
2. Funktionen und Verschlüsselung 13
3. Untersuchungsbeginn und involvierte Staaten 14
4. Französische Server-Überwachung 15
5. Provokation der Zugangsdaten und Kommunikationszugriff 16
6. Informationsaustausch und Datenübermittlung 17
7. Ermittlungserfolge 18

III. Anom 18
1. Phantom Secure und Anom 18
2. Angepriesene Funktionen 19
3. Geheime Überwachungsfunktionen 20
4. Testphase in Australien 21
5. Internationale Überwachung 21
6. Ausnahmen von der Überwachung 23
7. Informationsaustausch 23
8. Ermittlungserfolge 24
9. Prozessuales: Verfahrensart und Operationszweck 25

B. Gemeinsame Merkmale der Kryptophones und deren Überwachung 27
I. Kryptophones als «grey infrastructure» 27
II. Die Überwachungen als internationale Verbrechensbekämpfung 28
III. Verdachtsbegründung und Verurteilungsrate 29

C. Verwertbarkeitsrecht 33
I. Beweiserhebungsverbote (Art. 140 StPO) 33
II. Beweisverwertungsverbote (Art. 141 StPO) 33
1. Absolute Beweisverwertungsverbote 33
2. Relative Beweisverwertungsverbote 34
3. Verwertbarkeit bei Ordnungsvorschriftsverletzung 34
4. Folgebeweis 34
III. Verwertbarkeit präventiv erhobener Informationen 35

D. Lokalisierung von digitalen Beweisen 37
I. Lokalisierung anhand der Infrastruktur 37
II. Lokalisierung anhand des Zugriffsberechtigten 38
1. Das Zugriffsprinzip 38
2. Anwendungsbereich des Zugriffsprinzips 38
III. Lokalisierung anhand des Netzwerkes? 39
IV. Zusammenfassung 40
V. In casu: Lokalisierung der Massnahmen 41
1. EncroChat 41
2. SkyECC 41
3. Anom 41

E. Das Vertrauensprinzip 43
I. Die Bedeutung des Vertrauensprinzips 43
II. Das tatsachenbezogene Vertrauensprinzip 43
1. Funktion 43
2. Verfahrensmaximen im Rechtshilfe- und Strafverfahren 44
3. Teilnahmerechte bei ausländischer Sachverhaltserstellung 45
4. Keine Übertragung des tatsachenbezogenen Vertrauensprinzips in das Strafverfahren 45
III. Das rechtsbezogene Vertrauensprinzip 46
1. Vertrauensgrundlage als Voraussetzung 46
2. Beschränkte Tragweite des Vertrauensprinzips 47
3. Vertrauensprinzip und Beweiserhebungen in einem Drittstaat? 47
IV. Territorialitätsrechtliche Implikationen des Vertrauensprinzips? 48
V. Gültigkeit ausländischer Genehmigungen in der Schweiz? 49
VI. In casu: EncroChat, SkyECC, Anom und das Vertrauensprinzip 50
1. Ausländische Darstellungen als Arbeitshypothese 50
2. Vertrauen in EMRK-Konformität der Massnahmen? 50
3. EncroChat 51
4. SkyECC 51

5. Anom 51
a) Keine Anwendbarkeit des Vertrauensprinzips hinsichtlich des unbekannten Staates 51
b) Keine Anwendbarkeit des rechtsbezogenen Vertrauensprinzips hinsichtlich der USA 52
c) Folge: Fehlende Genehmigung und keine Rechtmässigkeitsvermutung 53

F. Beurteilung von Auslandsbeweisen 55
I. Unterteilung von Auslandsbeweisen 55
II. Beurteilung von «reinen» Auslandsbeweisen 55
1. Zweistufige Bewertung 55
2. Beurteilung des Verfahrensverstosses nach lex loci 56
3. Vorgehensweise bei Verfahrensverstoss nach lex loci 56
4. Vorgehen bei Rechtmässigkeit nach lex loci 57
a) Ordre public-Vorbehalt im Allgemeinen 57
b) Beweisausforschungsverbot als Ordre public? 57
c) Territorialitätsprinzip als Ordre public? 58
III. Beurteilung von «gemischten» Auslandsbeweisen 59
IV. EncroChat, SkyECC und Anom als «gemischte» Auslandsbeweise 60

G. Die Massnahmen im Lichte des Verdachtskriteriums 61
I. Der Tatverdacht als Abgrenzungskriterium 61
II. Das Verdachtserfordernis im Strafprozessrecht 61
1. Der Begriff des Tatverdachts 62
a) Dreigliedriger Begriff 62
b) Konkrete Tatsachen 62
c) Erfahrungssatz 62
d) Tatbestandsmässigkeit als Bezugspunkt 63
2. Die Abstufungen des Tatverdachts 63
a) Der Verdacht als dynamisches Kriterium 63
b) Anfangsverdacht 63
c) Hinreichender Tatverdacht 63
d) Dringender Tatverdacht 64
3. Zufallsfund und fishing expedition 64
4. Exkurs: Verwertbarkeitsfolgen des fehlenden Tatverdachts 64
III. In casu: Verdachtsbeurteilung 65
1. Verdacht auf kriminelle Organisation und Betäubungsmitteldelikte? 65
2. Vorliegende Tatsachen? 66
3. Schluss auf strafbares Verhalten? 66
a) Kein Rückschluss anhand der Sicherheitsarchitektur 66
b) Kein Rückschluss anhand der Vertriebsumstände 67
c) Kein Rückschluss anhand der Hersteller und Vertreiber 67
d) Kein Rückschluss anhand der angeblichen Nutzung 68
e) Zwischenfazit: Kein Tatverdacht 68
IV. Einordnung in das präventiv-polizeirechtliche Recht? 69
V. Exkurs: Zufallsfund? 69

H. Die Massnahmen als Massenüberwachungen 71
I. Begriff und Zulässigkeit der Massenüberwachung 71
1. Begriffskriterien der Massenüberwachung (bulk interception) 71
2. Zulässigkeit der Massenüberwachung nach EGMR 71
3. Massenüberwachung als geheimdienstliche Massnahme (Art. 38 f. NDG) 72
II. EncroChat, SkyECC, Anom als Massenüberwachung 73
1. Qualifizierung als Massenüberwachung 73
2. Folge: Strukturell geheimdienstähnliche Massnahmen 74

I. Die Massnahmen als Eingriff in das Fernmeldegeheimnis (Art. 13 Abs. 1 BV) 75
I. Das Fernmeldegeheimnis als Einordnungskriterium 75
II. Schutzbereich des Fernmeldegeheimnisses 76
1. Zeitlicher Geltungsbereich 76
a) Beginn des Übermittlungsvorganges 76
b) Abschluss des Übermittlungsvorganges 77
2. Sachlicher Geltungsbereich 77
a) Schutz der Vertraulichkeitserwartung 77
b) Geschützte Daten: Inhalts- und Randdaten 78
c) Akzessorische Beurteilung von Zugangsdaten 78
III. Die Geltung des Fernmeldegeheimnisses in casu 79
1. EncroChat 79
a) Historical data collection 79
b) Forward facing collection 79
2. SkyECC 80
a) Qualifizierung als Zugangsdaten 80
b) Vorfrageweise Beurteilung des Inhaltsdatenabgriffes 80
c) Akzessorische Beurteilung der Zugangsdaten 81
3. Anom 81

J. Fernmelderechtliche Massnahmenqualifikation 83
I. Fernmeldeüberwachung als Bundeskompetenz 83
II. Strafprozessuale Fernmeldeüberwachungen 83
1. Konventionelle Überwachung (Art. 269 StPO) 83
2. Besondere technische Geräte zur Überwachung des Fernmeldeverkehrs (Art. 269bis StPO) 84
3. Besondere Informatikprogramme zur Überwachung des Fernmeldeverkehrs (Art. 269ter StPO) 85
a) Art. 269ter StPO als gesetzliche Grundlage für die GovWare 85
b) Die Zieldaten der GovWare 85
c) Die GovWare als gerätspezifische Massnahme 86
4. Exkurs: Online-Recherche 86
a) Voraussetzungen der Online-Recherche 86
b) Erstes Abgrenzungskriterium: Kein Fernmeldegeheimnis 87
c) Zweites Abgrenzungskriterium: Offene Zwangsmassnahme 87
III. Ausserstrafprozessuale Fernmeldeüberwachungen 88
1. Fernmeldeüberwachung zwecks Personensuche (Art. 35 f. BÜPF) 88

2. Rechtshilfeweise Überwachung (Art. 18a f. IRSG) 88
3. Nachrichtendienstrechtliche Überwachung (Art. 26 NDG) 89
a) Ausgewählte Überwachungsmassnahmen nach Art. 26 NDG 89
b) Die Massnahmen nach Art. 26 NDG als zielgerichtete Massnahmen 89
IV. Strafprozessuale Würdigung 90
1. Vorgehenshinweis 90
2. EncroChat 90
a) Schadsoftware als GovWare 90
b) EncroChat-Überwachung als unbekannte Massnahme 91
3. SkyECC 91
a) Provokation der Zugangsdaten als IMSI-Catcher i.S.v. Art. 269bis StPO? 91
b) Provokation der Zugangsdaten als GovWare i.S.v. Art. 269ter StPO? 92
c) Provokation der Zugangsdaten als geheime Online-Recherche? 92
d) Provokation der Zugangsdaten als unbekannte Massnahme 93
4. Anom 93
V. Sicherheitsrechtliche Würdigung 94
1. Präventiv-polizeirechtliche Bewertung 94
2. Nachrichtendienstliche Bewertung (Art. 26 NDG) 94
3. Exkurs: Unverwertbarkeit von sicherheitsrechtlichen Informationen 95
VI. Kapitelzusammenfassung 95
VII. Die Massnahmen als hybride Überwachungsmassnahmen 96

K. Anforderungen an Fernmeldeüberwachungen 97
I. Verfassungsrechtliche Anforderungen 97
II. Anforderungen an eine strafprozessuale Fernmeldeüberwachung 98
1. Allgemeine Voraussetzungen für Zwangsmassnahmen 98
2. Strafprozessuale Voraussetzungen für die Fernmeldeüberwachung 98
III. Anforderungen an ausserstrafprozessuale Fernmeldeüberwachungen 99
IV. Kapitelzusammenfassung 100

L. Massnahmenbezogene Verwertbarkeitsbeurteilung 101
I. Verletzung des Legalitätsprinzips (Art. 36 BV) 101
II. Verletzung der Genehmigungspflicht (Art. 13 BV und Art. 277 StPO) 102
III. Verletzung des Täuschungsverbots (Art. 141 Abs. 1 StPO) 103
IV. Verwertbarkeitsbeurteilung in casu 104
1. Verletzung des Legalitätsprinzips / Territorialitätsrecht? 104
2. EncroChat 105
a) Verletzung des Legalitätsprinzips 105
b) Verletzung des Richtervorbehaltes 105
3. SkyECC 105
a) Verletzung des Legalitätsprinzips 105
b) Verletzung des Richtervorbehaltes 106
4. Anom 106
a) Verletzung des Legalitätsprinzips 106
b) Verletzung des Richtervorbehaltes 107
c) Verletzung des Täuschungsverbots 107
V. Verwertbarkeit bei transnationaler Kommunikation 108

M. Die Überwachungsmassnahmen und der nachträgliche Rechtsschutz 109
I. Die Rechtsweggarantie nach Art. 29a BV 109
II. Mitteilungspflicht 110
1. Mitteilung als verfahrensrechtliche Obliegenheit 110
a) Mitteilungspflicht und Mitteilungsmodalitäten gemäss StPO 110
b) Mitteilungspflicht bei ausserstrafprozessualen Fernmeldeüberwachungen 110
2. Aufschub und Unterlassung der Mitteilung 111
a) Ausnahmeregelung gemäss StPO 111
b) Verwertbarkeitsfolge 111
c) Ausnahmeregelung bei ausserstrafprozessualen Fernmeldeüberwachungen 112
III. Beschwerdegarantie 113
1. Verfassungsrechtliche Anforderungen an die Beschwerdeinstanz 113
2. Beschwerdemöglichkeit nach StPO 113
3. Beschwerdemöglichkeit bei ausserstrafprozessualer Fernmeldeüberwachung 113
4. Verletzungsfolgen 114
IV. In Casu (EncroChat, SkyECC und Anom) 115
1. Verletzung der Mitteilungspflicht 115
2. Unzulänglichkeit einer ausländischen Beschwerdeinstanz 115
3. Beeinträchtigung/Verunmöglichung des ausländischen Beschwerdewegs 116
a) EncroChat und SkyECC 116
b) Anom 117
4. Keine Überprüfung vor Schweizer Instanzen 117
V. Kapitelzusammenfassung 118

N. Akteneinsichtsrecht 119
I. Rechtliches Gehör nach Art. 29 Abs. 2 BV 119
II. Strafprozessuale Aktenführungspflicht (Art. 100 StPO) 119
1. Grundsatz der Aktenvollständigkeit 119
2. Aktenführung bei digitalen Beweisen 120
3. Ausnahmen vom Grundsatz der Aktenvollständigkeit 121
a) Schutz nicht staatlicher Geheimnisse 121
b) Schutz staatlicher Geheimnisse 121
c) Faktische Einschränkung des Akteneinsichtsrechts 122
4. Aktenführungs-, Untersuchungs- und Beschaffungspflicht 122
III. Strafprozessuales Einsichtsrecht (Art. 101 StPO) 123
1. Voraussetzungsloser Parteianspruch 123
2. Umfang 123
3. Exkurs: Primär-, Sekundär- und Tertiärdatensatz 123
IV. Einschränkung der Akteneinsicht (Art. 108 StPO) 125
1. Einschränkungsvoraussetzungen 125
2. Berücksichtigung ausländischer Interessen? 125
3. Einschränkung des Einsichtsrechts des Rechtsbeistands? 126

V. Verletzungsfolgen 127
1. Folgen der Verletzung der Aktenführungspflicht 127
2. Folgen der Verletzung des Akteneinsichtsrechts 127
VI. In Casu (EncroChat, SkyECC und Anom) 128
1. Verletzung der Beschaffungs- und Aktenführungspflichten 128
2. Verletzung des Akteneinsichtsrechts 129
3. Fazit 129

O. Faires Verfahren nach Art. 6 EMRK (Fair Trial) 131
I. Anwendungsbereich 131
II. Grundsatz der Verfahrensfairness 131
1. Der Fair Trial Grundsatz als Gesamtrecht 131
2. Die Rechtsweggarantie 132
3. Die Waffengleichheit 132
4. Das rechtliche Gehör 132
5. Einschränkungen und kompensatorische Massnahmen 133
6. Faire Handhabung von Beweismitteln 134
7. Verletzungsfolgen 134
III. In Casu: Gesamtwürdigung der Fairness (EncroChat, SkyECC, Anom) 135
1. Vorbemerkungen 135
2. Rechtswidriger Eingriff in den Korrespondenzschutz (Art. 8 EMRK) 135
3. Nicht überprüfbare Datenqualität (Art. 6 EMRK) 136
4. Fehlende kompensatorische Massnahmen (Art. 6 EMRK) 137
5. Fazit zur Gesamtwürdigung 137

P. Die Massnahmen im Lichte des Territorialitätsprinzips 139
I. Schutzweck des Territorialitätsprinzips 139
II. Territorialitätseingriff 139
1. Territorialitätsprinzip als Schutz der exklusiven Zuständigkeit 139
2. Eingriffsintensität von Datenverarbeitungsvorgängen 140
3. Bewusster Auslandsbezug? 142
III. Rechtfertigung von Territorialitätseingriffen 143
1. Information request gemäss Art. 32 lit. b CCC 143
2. Rechtfertigungsnorm von Art. 349b StGB? 144
3. Gewohnheitsrecht (insbes. Art. 32 lit. a CCC) 144
4. Einwilligung 145
a) Rechtsgründe der Einwilligung 145
b) Zuständigkeit 145
c) Zeitpunkt 146
d) Verwaltungsverfahren 146
e) Zusammenfassung 147
IV. Exkurs: «Hacking» als Eingriffsvoraussetzung? 147
V. Folgen der Territorialitätsverletzung 148
1. Absolute Unverwertbarkeit bei Verletzung fremder Territorialität 148
2. Kritik und Praxisänderung? 148
3. Ausweitung der Rechtsprechung 149
4. Berücksichtigung ausländischen Territorialitätsrechts 149

VI. EncroChat 150
VII. SkyECC 150
1. Uneinheitliche Bewertung 150
2. Territorialitätsverletzung 151
VIII. Anom 152
1. Uneinheitliche Bewertung 152
2. Territorialitätsverletzung 152
IX. Verwertbarkeit bei transnationaler Kommunikation 153

Q. Zusammenfassung 155

R. Fazit 161

Literaturverzeichnis

Die nachfolgend aufgeführten Werke werden, wo nicht anders angegeben, mit dem Nachnamen des Autors und der betreffenden Fundstelle zitiert:

ACKERMANN JÜRG-BEAT (Hrsg.), Kommentar Kriminelles Vermögen – Kriminelle Organisation: Einziehung, Kriminelle Organisation, Finanzierung des Terrorismus, Geldwäscherei, Band II, Zürich/Basel/Genf 2018 (zit. KommKV/KO II-BEARBEITER)

ACKERMANN JÜRG-BEAT, Tatverdacht und Cicero – in dubio contra suspicionem maleficii, in: Niggli Marcel Alexander/Hurtado Pozo José/Queloz Nicolas (Hrsg.), Festschrift für Franz Riklin, Zürich/Basel/Genf 2007, S. 319 ff.

ACKERMANN JÜRG-BEAT/VOGLER PATRICK, Nachrichtendienst und Strafprozess – zur Verwertbarkeit von Beweisen zwischen Systemen, in: Ackermann Jürg-Beat/Hilf Marianne Johanna (Hrsg.), TOP SECRET, Geheimnisschutz und Spionage, Zürich/Basel/Genf 2015, S. 161 ff.

ALBRECHT MARTIN ET AL., A Real-World Law Enforcement Hack: The case of EncroChat, Cryptology ePrint Archive Paper, 2026/1319 <https://eprint.iacr.org/2026/1319>

BANGERTER SIMON, Hausdurchsuchungen und Beschlagnahmen im Wettbewerbsrecht, unter vergleichender Berücksichtigung der StPO, Diss. Zürich, Zürich/Basel/Genf 2014 (Zürcher Studien zum Verfahrensrecht Band 176)

BÄR WOLFGANG, Transnationaler Zugriff auf Computerdaten, ZIS 2011, S. 53 ff., <https://www.zis-online.com/dat/artikel/2011_2_525.pdf>

BIAGGINI ELENA, Verwertbarkeit verdachtsbegründender Informationen aus Fernmeldeüberwachungen im Strafverfahren, Diss. Zürich, Zürich/Genf 2022 (Zürcher Studien zum Strafrecht Band 115)

BOFFEY DANIEL, Colombia's cartels target Europe with cocaine, corruption and torture, The Guardian online vom 11. April 2021 <https://www.theguardian.com/world/2021/apr/11/colombias-cartels-target-europe-with-cocaine-corruption-and-torture>

CAMPBELL DUNCAN, What does the police hack of messaging service EncroChat mean for criminal prosecution, fair trial, Videogespräch vom 26. März 2021 <https://www.youtube.com/watch?v=JogUfLFtVMU>

CAPUS NADJA, Strafrecht und Souveränität: Das Erfordernis der beidseitigen Strafbarkeit in der internationalen Rechtshilfe in Strafsachen, Bern 2010

COLLET PHILIPPE, L'acte coercitif en procédure pénale, Diss. Paris II Panthéon-Assas, Paris 2018 (Éditions Panthéon-Assas)

Cox Joseph, Encrypted Phone Network Says It's Shutting Down After Police Hack, vice vom 22. Juni 2020 <https://www.vice.com/en/article/encrochat-hacked-shutting-down-encrypted-phone/> (zit. Cox, Police Hack)

Cox Joseph, The Incredible True Story of the Largest Sting Operation Ever, Dark Wire, New York 2024 (zit. Cox, Dark Wire)

Cox Joseph, We Got the Phone the FBI Secretly Sold to Criminals, vice vom 8. Juli 2021 <https://www.vice.com/en/article/anom-phone-arcaneos-fbi-backdoor/> (zit. Cox, Phone)

Del Favero Elia, EncroChat: Europol liefert Schweiz Infos zum WhatsApp für Kriminelle, Nau.ch vom 2. April 2021 <https://www.nau.ch/news/digital/encrochat-europol-liefert-schweiz-infos-zum-whatsapp-fur-kriminelle-65897655>

Della Valle Nicoletta, Interview in: NZZ vom 17. April 2024, S. 8 f.

Demko Daniela, «Menschenrecht auf Verteidigung» und Fairness des Strafverfahrens auf nationaler, europäischer und internationaler Ebene, dargestellt anhand eines Strafrechtsvergleichs zum Konfrontationsrecht des Angeklagten gegenüber Belastungszeugen und unter Zugrundelegung von Erkenntnissen aus Philosophie und Psychologie, Habil. Zürich, Bern 2014

Desportes Frédéric/Lazerges-Cousquer Laurence, Traité de procédure pénale, 3. Aufl., Paris 2013

Dombrowski Nadine, Extraterritoriale Strafrechtsanwendung im Internet, Diss. Potsdam, Berlin 2014 (Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht Band 142)

Donatsch Andreas et al. (Hrsg.), Schulthess Kommentar, Kommentar zur Schweizerischen Strafprozessordnung StPO, Art. 1–195, 3. Aufl., Zürich/Basel/Genf 2020 (zit. SK StPO I-Bearbeiter)

Donatsch Andreas et al. (Hrsg.), Schulthess Kommentar, Kommentar zur Schweizerischen Strafprozessordnung StPO, Art. 196–457, 3. Aufl., Zürich/Basel/Genf 2020 (zit. SK StPO II-Bearbeiter)

Donatsch Andreas/Heimgartner Stefan/Simonek Madeleine, Internationale Rechtshilfe, unter Einbezug der Amtshilfe im Steuerrecht, 3. Aufl., Zürich/Genf 2024

Finder Joseph, Operation Trojan Shield: The Covert Sting That Unraveled the Underworld, lawyermonthly vom 9. November 2024 <https://www.lawyermonthly.com/2024/11/operation-trojan-shield-the-covert-sting-that-unraveled-the-underworld/>

Fiolka Gerhard, Das «Vertrauensprinzip» in der Rechtshilfe als organisierte Unverantwortung, in: Jositsch Daniel/Schwarzenegger Christian/Wohlers Wolfgang (Hrsg.), Festschrift für Andreas Donatsch, Zürich 2017, S. 605 ff.

Freiling Felix et al., Zur Einordnung der Verwertbarkeit von Beweisdaten aus EncroChat, SkyECC und Anom nach der Rechtsprechung des Bundesgerichtshofes, JR 2026, S. 430 ff.

Gall Moritz/Haskaya Elif, Die (Un)Verwertbarkeit der durch ausländische Behörden generierten Daten von verschlüsselten Kommunikationsdiensten wie Sky ECC, forumpoenale 2023, S. 301 ff.

Ginowski D.P., Der Fall EncroChat – A Real «True Crime» Story: Eine Analyse des «Kryptohandys der Gangster» mit Kommentaren von Cybersecurity-Experte Martin Frost und Rechtsanwältin Dr. jur. Arabella Pooth, Essen 2023

Gless Sabine, Heiligt der Zweck die Mittel 2.0? ZStrR 2026, S. 80 ff. (zit. Gless, ZStrR)

Gless Sabine, Rechtsprechung, Nr. 15 Obergerichts des Kantons Zürich, II. Strafkammer, Beschluss vom 15.8.2025 i. S. A. gegen B. Bürgschaftsgenossenschaft sowie Staatsanwaltschaft II des Kantons Zürich – SB240422, Urteilsbesprechung, forumpoenale 2026, S. 109 ff. (zit. Gless, forumpoenale)

Goodwin Bill, Ex-boxer fights US government over legality of Sky ECC cryptophone intercepts, ComputerWeekly.com vom 13. November 2024 <https://www.computerweekly.com/news/366615638/Ex-boxer-fights-US-government-over-legality-of-Sky-ECC-cryptophone-intercepts> (zit. Goodwin, Ex-boxer)

Goodwin Bill, Police crack world's largest cryptophone network as criminals swap EncroChat for Sky ECC, ComputerWeekly.com vom 10. März 2021 <https://www.computerweekly.com/news/252497565/Police-crack-worlds-largest-cryptophone-network-as-criminals-swap-EncroChat-for-Sky-NCC> (zit. Goodwin, Police)

Goodwin Bill, Police EncroChat cryptophone hacking implant did not work properly and frequently failed, ComputerWeekly.com vom 11. März 2022 <https://www.computerweekly.com/news/252514476/Police-EncroChat-cryptophone-hacking-implant-did-not-work-properly-and-frequently-failed> (zit. Goodwin, EncroChat)

Goodwin Bill, Police swoop on Sky ECC cryptophone distributors in Spain and Holland, ComputerWeekly.com vom 31. Januar 2025 <https://www.computerweekly.com/news/366618716/Police-swoop-on-Sky-ECC-cryptophone-distributors-in-Spain-and-Holland> (zit. Goodwin, SkyECC)

Graf Damian K. (Hrsg.), Onlinekommentar, Übereinkommen über die Cyberkriminalität (Cybercrime Convention), Version: 26. Oktober 2023 <https://onlinekommentar.ch/de/kommentare/ccc32> (zit. OK CCC-Bearbeiter)

Graf Damian K., Praxishandbuch zur Siegelung, StPO inklusive revidierter Bestimmungen VStrR – IRSG – MStP, Bern 2022 (zit. Graf, Praxishandbuch)

GRAF DAMIAN K., SkyECC, EncroChat, ANOM und der Rechtsstaat, Zum strafprozessualen Umgang mit ausländischen Kryptokommunikationsdaten in der Schweiz, Jusletter 3. November 2025 <https://jusletter.weblaw.ch/juslissues/2025/1260/skyecc_-encrochat_-a_310d2f4379.html> (zit. GRAF, Jusletter)

GRAF DAMIAN K., Strafprozessuale Verwertbarkeit von im Ausland erlangten Daten, Grenzen extraterritorialer Hoheitsakte sowie internationaler Rechtshilfe (unter Berücksichtigung überwachter Kryptokommunikation), AJP 2025, S. 523 ff. (zit. GRAF, Verwertbarkeit)

GRAF JÜRGEN (Hrsg.), Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, 52. Aufl., Stand 01. Juni 2024 <https://beck-online.beck.de/?vpath=bibdata%2Fkomm%2FBeckOKStPO_52%2Fcont%2FBECKOKSTPO%2ehtm> (zit. BeckOK D-StPO-BEARBEITER)

GRUBER JAN/HARGREAVES J. CHRISTOPHER/FREILING FELIX C., Contamination of digital evidence: Understanding an underexposed risk, FSI 2023, Artikel 44 <https://www.sciencedirect.com/science/article/pii/S2666281723000021>

HANSJAKOB THOMAS, Geheime Erhebung von Beweisen nach StPO, forumpoenale 2011, S. 299 ff. (zit. HANSJAKOB, forumpoenale)

HANSJAKOB THOMAS, Überwachungsrecht der Schweiz, Kommentar zu Art. 269 ff. StPO und zum BÜPF, Zürich/Basel/Genf 2017 (zit. HANSJAKOB, Überwachungsrecht)

HEIMGARTNER STEFAN, Strafprozessuale Beschlagnahme, Wesen, Arten und Wirkungen, Habil. Zürich, Zürich/Basel/Genf 2011

Heise online (o.V.), Organisierte Kriminalität: BGH lässt «Anom»-Chats als Beweise zu, heise online vom 9. Januar 2025 <https://www.heise.de/news/Organisierte-Kriminalitaet-BGH-laesst-Anom-Chats-als-Beweise-zu-10234711.html>

HINRICHS PER, Größter europäischer Fahndungserfolg – oder rechtlich fragwürdige Ermittlerpraktik?, WELT online vom 13. April 2021 <https://www.welt.de/politik/deutschland/article230103331/EncroChat-Zweifel-an-Rechtmaessigkeit-von-Auswertung.html>

HIZZIR HAMZA, Sky ECC: comment le décryptage de la messagerie secrète des trafiquants a mis à mal le crime organisé, TF1 INFO vom 4. März 2024 <https://www.tflinfo.fr/international/video-reportage-exclusif-sept-a-huit-sky-ecc-comment-le-decryptage-de-la-messagerie-secrete-des-trafiquants-de-drogue-a-mis-a-mal-le-crime-organise-2288196.html>

HÜRLIMANN CORNELIA, Die Eröffnung einer Strafuntersuchung im ordentlichen Verfahren gegen Erwachsene im Kanton Zürich, unter Berücksichtigung des Entwurfs zu einer Schweizerischen Strafprozessordnung, Diss. Zürich, Zürich/Basel/Genf 2006 (Zürcher Studien zum Verfahrensrecht Band 148)

HUSMANN MARKUS, Recht aus den Fugen, ein Beitrag zum Wesen der «Bewilligung nach Artikel 271 des Strafgesetzbuches», Diss. Freiburg i.Üe., Basel 2021 (Grundlegendes Recht Band 29) (zit. HUSMANN, Bewilligung)

Husmann Markus, Tragweite des Territorialitätsprinzips hinsichtlich der Verwendung von Aufzeichnungen, die von geheimen, in der Schweiz bewilligten technischen Überwachungsmassnahmen stammen, Entscheidbesprechung von BGer 1B_164/2019, AJP 2020, S. 364 ff. (zit. Husmann, Territorialitätsprinzip)

Jaklin Franziskus, Datenverarbeitungsvorgänge, Territorialitätsprinzip und SkyECC, Jusletter IT 19. Februar 2026 <https://www.jusletter-it.weblaw.ch/issues/2026/februar-2026/datenverarbeitungsvo_6b48abcbbc.html> (zit. Jaklin, Datenverarbeitungsvorgänge)

Jaklin Franziskus, Kryptophones und das Territorialitätsprinzip, eine Betrachtung anhand von Anom und SkyECC, AJP 2025, S. 1012 ff. (zit. Jaklin, Kryptophones)

Jeanneret Yvan/Kuhn André/Perrier Depeursinge Camille (Hrsg.), Commentaire Romand, Code de procédure pénale suisse, 2. Aufl., Basel 2019 (zit. CR StPO-Bearbeiter)

Jeker Konrad/Roos Eveline, Antennensuchlauf im Rahmen einer Rasterfahndung, forumpoenale 2012, S. 175 ff.

Jositsch Daniel/Schmid Niklaus, Handbuch des schweizerischen Strafprozessrechts, 4. Aufl., Zürich/St. Gallen 2023 (zit. Jositsch/Schmid)

Jositsch Daniel/Schmid Niklaus, Praxiskommentar, Schweizerische Strafprozessordnung, 4. Aufl., Zürich/St. Gallen 2023 (zit. PK StPO-Jositsch/Schmid)

Keller Helen/Hertig Randall Maya (Hrsg.), Basler Kommentar, Europäische Menschenrechtskonvention, Basel 2025 (zit. BSK EMRK-Bearbeiter)

Kiener Regina/Schindler Benjamin/Brunner Arthur, Polizeirecht, Rechtliche Grundlagen der polizeilichen Tätigkeit in der Schweiz, Bern 2026

Kipker Dennis-Kenji/Bruns Hauke, EncroChat and the "Chain of Custody" – Digitale Ermittlungen als Bewährungsprobe für ein Recht auf faires Verfahren, MMR 2022, S. 363 ff. <https://beck-online.beck.de/?vpath=bibdata%2fzeits%2fMMR%2f2022%2fcont%2fMMR%2e2022%2e363%2e1%2ehtm>

Klaubert David, Das Drittstaatsgeheimnis, FAZ Nr. 54 vom 5. März 2025, S. 3 (zit. Klaubert, Drittstaatsgeheimnis)

Klaubert David, «Heimlich», FAZ Nr. 226 vom 29. September 2025, S. 3 (zit. Klaubert, Heimlich)

Knauer Christof/Kudlich Hans/Schneider Hartmut (Hrsg.), Münchener Kommentar zur StPO, §§ 1-150, 2. Aufl., München 2023 (zit. MüKo D-StPO-Bearbeiter)

Knytel Dagna, Die Europäische Ermittlungsanordnung und ihre Umsetzung in die deutsche und französische Rechtsordnung, Diss. Freiburg i.Br./Straßburg, Berlin 2020 (Beiträge zum Internationalen und Europäischen Strafrecht Band 43)

Kochheim Dieter, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Aufl., München 2018

Kühne Stefan/Rütsche Serdar, GovWare-Einsatz – nur zur Fernmeldeüberwachung oder auch zur technischen Überwachung?, AJP 2019, S. 350 ff.

Lödden Christian/Makepeace Johannes, Same same but different: SkyECC oder wie europäische Strafverfolgungsbehörden eine Milliarde Nachrichten über 21 Monate lang abgefangen haben, HRRS 2023, S. 384 ff. <https://www.hrr-strafrecht.de/hrr/archiv/23-12/hrrs-12-23.pdf>

Ludwiczak Glassey Maria, Mesure suisse de surveillance secrète, résultats obtenus à l'étranger et projet de 3e Protocole additionnel à la CEEJ, ZStrR 2025, S. 271 ff.

Ludwiczak Glassey Maria/Moreillon Laurent (Hrsg.), Petit Commentaire, EIMP, Loi sur l'entraide pénale internationale, Basel 2024 (zit. PC IRSG-Bearbeiter)

Ludwiczak Glassey Maria/Staffler Lukas (Hrsg.), Onlinekommentar zum Bundesgesetz über internationale Rechtshilfe in Strafsachen, Version: 22. Mai 2025 (zit. OK IRSG-Bearbeiter) <https://onlinekommentar.ch/de/kommentare/irsg80a>

Martine Guillaume, Cour de cassation: the absence of a right of appeal in France does not pose a constitutional problem – Implications for SkyECC and EncroChat cases, Joint Defense Team, News vom 12. Juni 2025 <https://www.joint-defense-team.com/post/cour-de-cassation-the-absence-of-a-right-of-appeal-in-france-does-not-pose-a-constitutional-problem>

Meyer-Ladewig Jens/Nettesheim Martin/von Raumer Stefan (Hrsg.), Nomos Handkommentar, EMRK Europäische Menschenrechtskonvention, 5. Aufl., Baden-Baden 2023 (zit. NHK EMRK-Bearbeiter)

Miescher Martin, Die List in der Strafverfolgung, Diss. Bern, Bern 2008 (ASR 749)

Monnier Vincent, Affaire Sky ECC: comment les policiers ont infiltré le «WhatsApp des narcos», LeNouvelObs online vom 31. August 2023, aktualisiert am 4. September 2023 <https://www.nouvelobs.com/justice/20230831.OBS77577/affaire-sky-ecc-comment-les-policiers-ont-infiltre-le-whatsapp-des-narcos.html>

Moreillon Laurent (Hrsg.), Commentaire Romand, Entraide internationale en matière pénale, EIMP, TEJUS, LTEJUS, TEXUS, Basel 2004 (zit. CR IRSG-Bearbeiter)

Moreillon Laurent/Macaluso Alain/Queloz Nicolas (Hrsg.), Commentaire Romand, Code pénal II, Art. 111-392 CP, Art. 154 et 155 LIMF, 2. Aufl., Basel 2025 (zit. CR StGB II-Bearbeiter)

Mrokon Maximilian, Strafverfahrensrechtliche Fragen bei Daten aus sog. «Anom-Chatforen», Diss. Tübingen, Berlin 2025 (Schriften zum Prozessrecht Band 139)

Niggli Marcel Alexander/Heer Marianne/Wiprächtiger Hans (Hrsg.), Basler Kommentar, Schweizerische Strafprozessordnung, Jugendstrafprozessordnung, Art. 1-195 StPO, 3. Aufl., Basel 2023 (zit. BSK StPO I-Bearbeiter)

Niggli Marcel Alexander/Heer Marianne/Wiprächtiger Hans (Hrsg.), Basler Kommentar, Schweizerische Strafprozessordnung, Jugendstrafprozessordnung, Art. 196–457 StPO, Art. 1–54 JStPO, 3. Aufl., Basel 2023 (zit. BSK StPO II-Bearbeiter)

NIGGLI MARCEL ALEXANDER/HEIMGARTNER STEFAN (Hrsg.), Basler Kommentar, Internationales Strafrecht, IRSG, GWÜ, Basel 2015 (zit. BSK IRSG-BEARBEITER)

NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Hrsg.), Basler Kommentar, Strafrecht II, Art. 137–392 StGB Jugendstrafgesetz, 4. Aufl., Basel 2019 (zit. BSK StGB II-BEARBEITER)

OERLEMANS JAN-JAAP/ROYER SOFIE, The future of data-driven investigations in light of the Sky ECC operation, NJECL 2023, S. 434 ff.

OERLEMANS JAN-JAAP/VAN TOOR DAVE, Legal Aspects of the EncroChat Operation: A Human Rights Perspective, European Journal of Crime, Criminal Law and Criminal Justice 2022, S. 309 ff.

PIETH MARK/GETH CHRISTOPHER, Schweizerisches Strafprozessrecht, 4. Aufl., Basel 2023

PIOTET DENIS, Adages et brocards du droit privé, de leur origine à leur application actuelle en Suisse, Zürich/Genf 2024

POPP PETER, Grundzüge der internationalen Rechtshilfe in Strafsachen, Basel 2001

REISINGER JUSTUS, Ongoing Developments in international co-operation in the SkyECC investigation, Joint Defense Team, News vom 13. April 2025 <https://www.joint-defense-team.com/post/ongoing-developments-in-international-co-operation-in-the-skyecc-investigation>

RIEDI CLAUDIO, Auslandsbeweise und ihre Verwertung im schweizerischen Strafverfahren, Diss. Luzern, Zürich/Basel/Genf 2018 (Luzerner Beiträge zur Rechtswissenschaft Band 126)

RIEDO CHRISTOPH/FIOLKA GERHARD/NIGGLI MARCEL ALEXANDER, Strafprozessrecht sowie Rechtshilfe in Strafsachen, Basel 2011

RÜCKERT CHRISTIAN, Digitale Daten als Beweismittel im Strafverfahren, Habil. Erlangen-Nürnberg, Tübingen 2023 (Juspoenale Band 24)

RYSER DOMINIK, «Computer Forensics», eine neue Herausforderung für das Strafprozessrecht, in: Schwarzenegger Christian/Arter Oliver/Jörg Florian S. (Hrsg.), Internet-Recht und Strafrecht, 4. Tagungsband, Bern 2005, S. 553 ff.

SAGITTAE GEORGIOS, On the lawfulness of the EncroChat and Sky ECC-operations, NJECL 2023, S. 273 ff.

SAINTOURENS THOMAS/PIEL SIMON, Sky ECC, l'application prisée des trafiquants, mine d'or des enquêtes sur le crime organisé, Le Monde online vom 18. November 2022, aktualisiert am 1. April 2023 <https://www.lemonde.fr/societe/article/2022/11/18/sky-ecc-l-application-prisee-des-traficants-mine-d-or-des-enquetes-sur-le-crime-organise_6150398_3224.html>

SANDNER MARC-OLIVER, Operation «Emma» – Eine Europäische Erfolgsgeschichte? Eine Aufarbeitung der Infiltration des EncroChat-Netzwerks, Diss. Erlangen-Nürnberg, Berlin 2026 (Schriften zum Strafrecht Band 458)

Sarre Frank/Pruss Michael, Daten, Datenbanken und Datensicherheit, in: Auer-Reinsdorff Astrid/Conrad Isabell (Hrsg.), Handbuch IT- und Datenschutzrecht, 3. Aufl., München 2019, S. 114 ff.

Schär Caroline, Die Beschränkung von Teilnahmerechten und deren strafprozessualen Folgen, ZStrR 2019, S. 141 ff.

Simmler Monika, Gegenüberstellung des Schweizer Rechts und der E-Evidence-Gesetzgebung der EU – eine Auslegeordnung, forumpoenale 2025, S. 132 ff.

Sommer Ulrich, Anom oder: wie der Rechtsstaat Unrecht produzieren kann, HRRS 2024, S. 394 ff. <https://www.hrr-strafrecht.de/hrr/archiv/24-12/hrrs-12-24.pdf>

Stahl Sophia et al., Der Fall von Sky ECC: Wie eine der größten Polizeiaktionen Europas ablief, Der Standard online vom 22. Oktober 2024 <https://www.derstandard.at/story/3000000241679/der-fall-von-sky-ecc-wie-eine-der-groessten-polizeiaktionen-europas-ablief>

Stelzer-Wieckowska Marta, Die kleine Rechtshilfe in Strafsachen: grundrechtliche Stellung der betroffenen Person, Diss. Zürich, Zürich/Basel/Genf 2021 (Zürcher Studien zum Strafrecht 113)

Stoykova Radina, Encrochat: The hacker with a warrant and fair trials?, FSI 2023, Artikel 46 <https://www.sciencedirect.com/science/article/pii/S2666281723001142>

SZ (o.V.), Sind Urteile auf der Basis von EncroChat-Daten gültig, Süddeutsche Zeitung online vom 5. September 2023 <https://www.sueddeutsche.de/wirtschaft/justiz-sind-urteile-auf-basis-von-encrochat-daten-gueltig-dpa.urn-newsml-dpa-com-20090101-230905-99-79308>

Thomson Iain, Eurocops take down "secure" criminal chat system known as Matrix, The Register vom 4. Dezember 2024 <https://www.theregister.com/2024/12/04/eurocop_crack_matrix/>

Trechsel Stefan/Pieth Mark/Geth Christopher (Hrsg.), Praxiskommentar, Schweizerisches Strafgesetzbuch, 5. Aufl., Zürich/St. Gallen 2025 (zit. PK StGB-Bearbeiter)

Van de Pol Wim, Brits document laat zien hoe EncroChat werd gehackt, Crimesite vom 16. März 2021 <https://www.crimesite.nl/brits-document-laat-zien-hoe-encrochat-werd-gehackt/> (zit. Van de Pol, brits document)

Van de Pol Wim, DEA had mol in SkyECC, «Net een Netflix-serie», Crimesite vom 19. Oktober 2024 <https://www.crimesite.nl/dea-had-mol-in-sky-ecc-net-een-netflix-serie/> (zit. Van de Pol, DEA)

Van de Pol Wim, EncroChat: de reconstructie van de hack (UPDATE), Crimesite vom 10. Februar 2020 <https://www.crimesite.nl/encrochat-de-reconstructie-van-de-hack/> (zit. Van de Pol, reconstructie)

Van de Pol Wim, NFI kraakte ook fysieke telefoons van EncroChat, Crimesite vom 6. Oktober 2020 <https://www.crimesite.nl/nfi-kraakte-fysieke-telefoons-van-encrochat/> (zit. Van de Pol, NFI)

VAN DE POL WIM, Politie selecteert Encrodata voordat rechters die zien, Crimesite vom 20. Juli 2023 <https://www.crimesite.nl/politie-software-selecteert-encrodata-voordat-rechters-die-zien/> (zit. VAN DE POL, Encrodata)

VAN DE POL WIM, Rechtbanken hoorden lang niet alles over EncroChat-Hack (UPDATE), Crimesite vom 25. Mai 2021 <https://www.crimesite.nl/rechtbanken-hoorden-lang-niet-alles-over-encrochat-hack/> (zit. VAN DE POL, rechtbanken)

VAN DE POL WIM, Uitgelekt: geheim plan recherche over Sky ECC, Crimesite vom 3. Juni 2024 <https://www.crimesite.nl/uitgelekt-geheim-plan-recherche-over-sky-ecc/> (zit. VAN DE POL, geheim plan)

VILLIGER MARK E., Handbuch der Europäischen Menschenrechtskonvention (EMRK), 3. Aufl., Zürich/Basel/Genf 2020

VOGT FABIAN, So knackte die Polizei das «Whatsapp für Kriminelle», Blick vom 9. Juli 2020 <https://www.blick.ch/ausland/johnny-swales-und-encrochat-so-knackte-die-polizei-das-whatsapp-fuer-kriminelle-id15981574.html>

WALDER HANS ET AL., Kriminalistisches Denken, 11. Aufl., Heidelberg 2020

WALDMANN BERNHARD/BELSER EVA MARIA/EPINEY ASTRID (Hrsg.), Basler Kommentar, Bundesverfassung, 2. Aufl., Basel 2025 (zit. BSK BV-BEARBEITER)

WALDMANN BERNHARD/KRAUSKOPF PATRICK L. (Hrsg.), Praxiskommentar, Verwaltungsgesetz (VwVG), unter Einschluss des Reglements über die Kosten und Entschädigungen vor dem Bundesverwaltungsgericht (VGKE), 3. Aufl., Zürich/Genf 2023 (zit. PK VwVG-BEARBEITER)

WICKER MAGDA, Durchsuchung in der Cloud, Nutzung von Cloud-Speichern und der strafprozessuale Zugriff deutscher Ermittlungsbehörden, MMR 2013, S. 765 ff.

WIETLISBACH OLIVER, Warum Tausende Kriminelle das manipulierte Anom-Handy kauften und in die FBI-Falle tappten, watson vom 10. Juni 2021 <https://www.watson.ch/digital/international/816850392-wie-das-fbi-mit-manipulierten-handys-tausende-kriminelle-ueberlistete>

WILDHABER LUZIUS, Jurisdiktionsgrundsätze und Jurisdiktionsgrenzen im Völkerrecht, in: Schweizerische Vereinigung für internationales Recht (Hrsg.), Schweizerisches Jahrbuch für internationales Recht 1985, Zürich 1986, S. 99 ff.

WOHLERS WOLFGANG, Verwertbarkeit von Informationen aus im Ausland erfolgten Überwachungen sog. «Kryptohandys», Zugleich eine Besprechung von BGer, Urteil vom 11. Januar 2024, 7B_159/2022 und 7B_160/2022 (zur Publ. vorgesehen), forumpoenale 2024, S. 293 ff.

WOLTER JÜRGEN/DEITERS MARK (Hrsg.), Systematischer Kommentar zur Strafprozessordnung mit GVG und EMRK, Band II, §§ 94-136a StPO, 6. Aufl., Hürth 2023 (zit. SysK D-StPO-BEARBEITER)

ZHILLA FABIAN, Decrypting the Balkan underworld. A theoretical analysis of encrypted communication in organized crime, Jus & Justicia 2024 (Heft 18/1), S. 7 ff. <https://uet.edu.al/jus-justicia/wp-content/uploads/2024/07/jus-and-justicia-18-1.pdf>

ZWEIFEL MARTIN/BEUSCH MICHAEL/OESTERHELT STEFAN (Hrsg.), Kommentar zum Schweizerischen Steuerrecht, Amtshilfe, Basel 2020 (zit. KommStR-BEARBEITER)

Materialienverzeichnis

Botschaft BÜPF	Botschaft zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 27. Februar 2013, BBl 2013 2683 ff.
Botschaft CCC	Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18. Juni 2010, BBl 2010 4697 ff.
Botschaft NDG	Botschaft zum Nachrichtendienstgesetz vom 19. Februar 2014, BBl 2014 2105 ff.
Mitbericht GPDel	Mitbericht der Geschäftsprüfungsdelegation zum NDG vom 22. April 2014 (14.022)

Abkürzungsverzeichnis

a.A.	anderer Ansicht
Abs.	Absatz
AFP	Australian Federal Police
AJP	Aktuelle Juristische Praxis (Zürich)
AppGer BS	Appellationsgericht Basel-Stadt
Art.	Artikel
ASR	Abhandlungen zum schweizerischen Recht
Aufl.	Auflage
BAKOM	Bundesamt für Kommunikation
BBl	Bundesblatt
BE	Belgien
BeckOK D-StPO	Beck'scher Online-Kommentar zur deutschen Strafprozessordnung (siehe im Literaturverzeichnis GRAF JÜRGEN)
Beschl.	Beschluss
BG	Bezirksgericht
BGE	Bundesgerichtsentscheid
BGer	Bundesgericht
BGH	Bundesgerichtshof (Deutschland)
BKA	Bundeskriminalamt (Deutschland)
BSK BV	Basler Kommentar zur Bundesverfassung (siehe im Literaturverzeichnis WALDMANN BERNHARD/BELSER EVA MARIA/EPINEY ASTRID)
BSK EMRK	Basler Kommentar zur Europäischen Menschenrechtskonvention (siehe im Literaturverzeichnis KELLER HELEN/HERTIG RANDALL MAYA)
BSK IRSG	Basler Kommentar zum Internationalen Strafrecht (siehe im Literaturverzeichnis NIGGLI MARCEL ALEXANDER/HEIMGARTNER STEFAN)
BSK StGB II	Basler Kommentar zum Strafgesetzbuch, Art. 137–392 (siehe im Literaturverzeichnis NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS)

BSK StPO I	Basler Kommentar zur Strafprozessordnung, Art. 1–195 (siehe im Literaturverzeichnis NIGGLI MARCEL ALEXANDER/HEER MARIANNE/WIPRÄCHTIGER HANS)
BSK StPO II	Basler Kommentar zur Strafprozessordnung, Art. 196–457 (siehe im Literaturverzeichnis NIGGLI MARCEL ALEXANDER/HEER MARIANNE/WIPRÄCHTIGER HANS)
BStGer	Bundesstrafgericht
BÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 18. März 2016 (SR 780.1)
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (SR 101)
BVGer	Bundesverwaltungsgericht
bzw.	beziehungsweise
Cass. pen. sez.	Corte di Cassazione, sezione penale (Italien)
CCC	Übereinkommen über die Cyberkriminalität vom 23. November 2001 (SR 0.311.43)
cons.	considérant (Erwägung)
Cons. Const.	Conseil constitutionnel (Frankreich)
consid.	considerando (Erwägung)
CP	Code pénal (siehe StGB)
CPS	Crown Prosecution Service (Grossbritannien)
CR IRSG	Commentaire Romand zur internationalen Rechtshilfe in Strafsachen (siehe im Literaturverzeichnis MOREILLON LAURENT)
CR StGB II	Commentaire Romand zum Strafgesetzbuch, Art. 111–392 (siehe im Literaturverzeichnis MOREILLON LAURENT/MACALUSO ALAIN/QUELOZ NICOLAS)
CR StPO	Commentaire Romand zur Strafprozessordnung (siehe im Literaturverzeichnis JEANNERET YVAN/KUHN ANDRÉ/PERRIER DEPEURSINGE CAMILLE)
CSV-	Comma-separated values
déc.	décembre
Diss.	Dissertation
DOJ	Department of Justice (USA)
dpa	Deutsche Presse-Agentur
D-StPO	Deutsche Strafprozessordnung vom 7. April 1987

E.	Erwägung
ECLI	Europäischer Rechtsprechungsindikator
EEA	Europäische Ermittlungsanordnung
EGMR	Europäischer Gerichtshof für Menschenrechte
EMRK	Konvention zum Schutze der Menschenrechte vom 4. November 1950 (SR 0.101)
et al.	et alii
EU	Europäische Union
EUeR	Europäisches Übereinkommen über die Rechtshilfe in Strafsachen vom 20. April 1959 (SR 0.351.1)
EuGH	Gerichtshof der Europäischen Union
Eurojust	Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen
Europol	Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung
Eurostat	Statistische Amt der Europäischen Union
EWCA Crim	England and Wales Court of Appeal, Criminal division (Grossbritannien)
f.	folgende
FAZ	Frankfurter Allgemeine Zeitung (Frankfurt a.M.)
FBI	Federal Bureau of Investigation (USA)
Fedpol	Bundesamt für Polizei
ff.	fortfolgende
FMG	Fernmeldegesetz vom 30. April 1997 (SR 784.10)
FN	Fussnote
FR-CPP	Code de procédure pénale der Französischen Republik vom 31. Dezember 1957
FSI	Forensic Science International (Amsterdam)
GovWare	Government-Software
GPDel	Geschäftsprüfungsdelegation zum NDG
Habil.	Habilitation
h.L.	herrschende Lehre
HRRS	Online-Zeitschrift und Rechtsprechungsdatenbank für höchstrichterliche Rechtsprechung im Strafrecht (Hamburg)

Hrsg.	Herausgeber
i.Br.	im Breisgau
i.d.R.	in der Regel
i.e.	id est
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
insbes.	insbesondere
IP-	Internet Protocol
IRSG	Bundesgesetz über internationale Rechtshilfe in Strafsachen vom 20. März 1981 (SR 351.1)
ISO-	Internationale Organisation für Normung
i.S.v.	im Sinne von
IT-	Information Technology
i.Üe.	im Üechtland
i.V.m.	in Verbindung mit
JAAC	Jurisprudence des autorités administratives de la Confédération
JIT	Joint Investigation Team
JR	Juristische Rundschau (Berlin)
KG	Kreisgericht
KommKV/KO II	Kommentar Kriminelles Vermögen – Kriminelle Organisation (siehe im Literaturverzeichnis Ackermann Jürg-Beat)
KommStR	Kommentar zum Schweizerischen Steuerrecht, Amtshilfe (siehe im Literaturverzeichnis Zweifel Martin/Beusch Michael/ Oesterhelt Stefan)
LG	Landesgericht (Deutschland)
lit.	littera
m.H.a.	mit Hinweis auf
MITM-	Man-in-the-Middle-
MMR	Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT (München)
MüKo D-StPO	Münchener Kommentar zur deutschen Strafprozessordnung (siehe im Literaturverzeichnis Knauer Christof/Kudlich Hans/ Schneider Hartmut)
N	Randnote

NCA	National Crime Agency (Grossbritannien)
NDB	Nachrichtendienst des Bundes
NDG	Bundesgesetz über den Nachrichtendienst vom 25. September 2015 (SR 121)
NFI	Netherlands Forensic Institute
NHK EMRK	Nomos Handkommentar zur Europäischen Menschenrechtskonvention (siehe im Literaturverzeichnis Meyer-Ladewig Jens/Nettesheim Martin/von Raumer Stefan)
NJECL	New Journal of European Criminal Law (London)
Nr.	Nummer
NZZ	Neue Zürcher Zeitung (Zürich)
OGer AG	Obergericht des Kantons Aargau
OGer ZH	Obergericht des Kantons Zürich
OGH	Oberster Gerichtshof (Österreich)
OK CCC	Online Kommentar zum Übereinkommen über die Cyberkriminalität (siehe im Literaturverzeichnis Graf Damian K. (Hrsg.))
OK IRSG	Online Kommentar zum Bundesgesetz über internationale Rechtshilfe in Strafsachen (siehe im Literaturverzeichnis Ludwiczak Glassey Maria/Staffler Lukas)
OLG	Oberlandesgericht (Deutschland)
OSINT	Open Source Intelligence
o.V.	ohne Verfasser
PC IRSG	Petit commentaire zum Bundesgesetz über internationale Rechtshilfe in Strafsachen (siehe im Literaturverzeichnis Ludwiczak Glassey Maria/Moreillon Laurent)
PG SG	Polizeigesetz des Kantons St. Gallen vom 10. April 1980 (sGS 451.1)
PK StGB	Praxiskommentar zum Schweizerischen Strafgesetzbuch (siehe im Literaturverzeichnis Trechsel Stefan/Pieth Mark/Geth Christopher)
PK StPO	Praxiskommentar zur Schweizerischen Strafprozessordnung (siehe im Literaturverzeichnis Jositsch Daniel/Schmid Niklaus)
PK VwVG	Praxiskommentar zum Verwaltungsverfahrensgesetz (siehe im Literaturverzeichnis Waldmann Bernhard/Krauskopf Patrick L.)

PolG FR	Gesetz über die Kantonspolizei des Staats Freiburg vom 15. November 1990 (SGF 551.1)
PolG ZG	Polizeigesetz des Kantons Zug vom 30. November 2006 (BGS 512.1)
PolG ZH	Polizeigesetz des Kantons Zürich vom 23. April 2007 (Ordnungsnummer 550.1)
RAM	Random Access Memory
RL 2016/680	Richtlinie 2016/680/EU des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates vom 27. April 2016
RL EEA	Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates über die Europäische Ermittlungsanordnung in Strafsachen vom 3. April 2014
Rn.	Randnummer
r.o.	rechtsoverweging (Erwägung)
Rs.	Rechtssache
Rz	Randziffer
S.	Seite
S.A.	Société Anonyme
SDÜ	Schengener Durchführungsübereinkommen vom 19. Juni 1990 (Amtsblatt der EU Nr. L 239 vom 22/09/2000 S. 0019-0062)
SK StPO I	Schulthess Kommentar zur Schweizerischen Strafprozessordnung, Art. 1–195 (siehe im Literaturverzeichnis Donatsch Andreas et al.)
SK StPO II	Schulthess Kommentar zur Schweizerischen Strafprozessordnung, Art. 196–457 (siehe im Literaturverzeichnis Donatsch Andreas et al.)
sog.	sogenannt
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (SR 311.0)
StPO	Schweizerische Strafprozessordnung vom 5. Oktober 2007 (SR 312.0)

SysK D-StPO	Systematischer Kommentar zur deutschen Strafprozessordnung (siehe im Literaturverzeichnis WOLTER JÜRGEN/DEITERS MARK)
SZ	Süddeutsche Zeitung (München)
TPF	Tribunal pénal fédéral
u.a.	unter anderem
UKIPTrib	UK Investigatory Powers Tribunal (Grossbritannien)
Urt.	Urteil
v.	vom
VG	Verwaltungsgericht
vgl.	vergleiche
vs.	versus
VwVG	Bundesgesetz über das Verwaltungsverfahren vom 20. Dezember 1968 (SR 172.021)
z. B.	zum Beispiel
Ziff.	Ziffer
ZIS	Zeitschrift für Internationale Strafrechtsdogmatik (Gießen)
ZPO	Schweizerische Zivilprozessordnung vom 19. Dezember 2008 (SR 272)
ZStrR	Schweizerische Zeitschrift für Strafrecht (Bern)

A. Ereignisdarstellung

I. EncroChat

1. Eckdaten

Das Unternehmen «EncroChat S.A.» war ein Anbieter von Kommunikationsgeräten mit besonders hohem Vertraulichkeitsschutz.[1] Der Geschäftssitz von EncroChat S.A. lag in Panama, die Hauptniederlassung in Amsterdam.[2] Die Server von EncroChat S.A. befanden sich in Roubaix (Frankreich) und wurden von dem Telekommunikationsanbieter OVH gehostet.[3]

Im Verlauf der Jahre 2013/14 brachte EncroChat S.A. die Encrophones auf den Markt.[4] Bei diesen Geräten handelte es sich um Mobiltelefone des spanischen Unternehmens BQ (Modellreihe Aquaris), welche von EncroChat S.A. modifiziert wurden.[5] Den Ausgangsmodellen wurden der GPS-Chip, USB-Port, teils auch Kamera und Mikrofon entfernt.[6] Auf Software-Ebene wurden die Encrophones mit einem doppelten Betriebssystem (*dual operating system*) ausgestattet.[7] Dieses bestand aus einem funktionslosen Android-Betriebssystem und dem Betriebssystem EncroChat OS[8], welches die Encro-Funktionen zur

---

1 Vgl. GINOWSKI, S. 32.

2 GINOWSKI, S. 31.

3 Juge des libertés et de la détention du tribunal de grande instance Lille (nachfolgend: Tribunal judiciaire de Lille), 4.3.2020, S. 1; dieser Genehmigungsbeschluss sowie die Genehmigungsbeschlüsse vom 30.1.2020, 12.2.2020, 20.3.2020, 31.3.2020, 29.4.2020, 28.5.2020 und 10.6.2020 sind in englischer Sprache abrufbar unter <https://www.documentcloud.org/documents/24479116-lille-warrants>. Da die Parteinamen und teils die Verfahrensnummern unbekannt sind, werden diese Beschlüsse lediglich mit Datum angegeben.

4 Vgl. GINOWSKI, S. 106.

5 Stellungnahme Frankreichs v. 7. April 2022 vor dem EGMR (A.L. und E.J. vs. Frankreich, 44715/20 und 47930/21), § 7, abrufbar unter <https://media.licdn.com/dms/document/media/v2/C4E1FAQHuGwqAcc6fMQ/feedshare-document-pdf-analyzed/feedshare-document-pdf-analyzed/0/1672478168329?e=1743638400&v=beta&t=6n2g2_nM-UkaGjUj_8dQGzAR0YhlJRqqGS9kDjnwFDM>.

6 Vgl. BGH, Beschl. v. 2.3.2022 – 5 StR 457/21, Rn. 9; STOYKOVA, S. 5.

7 BGH, Beschl. v. 2.3.2022 – 5 StR 457/21, Rn. 9; STOYKOVA, S. 1.

8 Vgl. Regina v A, B, D & C [2021], EWCA Crim 128, [2021], § 11; BGH, Beschl. v. 2.3.2022 – 5 StR 457/21, Rn. 9.

Verfügung stellte.[9] Abhängig davon, mittels welcher Tastenkombination das Gerät eingeschaltet wurde, öffnete sich das eine oder andere Betriebssystem.[10]

Der Vertrieb der Geräte erfolgte über ein dezentrales Netzwerk bestehend aus lokalen und anonymen Verkäufern.[11] Eine Bestellung über die Website der EncroChat S.A. war nicht möglich.[12] Üblich war die Bezahlung in bar oder Kryptowährung, ebenso wie der Verzicht auf schriftliche Verträge.[13] Die Encrophones kosteten je nach Dauer der Nutzerlizenz zwischen EUR 800 und 1'600[14], wobei deren Hardware etwa einen Wert von EUR 200 hatte[15].

2. Funktionen

Die Encrophones waren mit verschiedenen Funktionen ausgestattet. Sie verfügten über eine Chatfunktion «EncroChat» und teils auch über eine Telefonfunktion «EncroTalk».[16] Daneben konnten Notizen als «EncroNotes» lokal gespeichert werden.[17] Die Encrophones konnten nur untereinander kommunizieren.[18]

Die Vertraulichkeit der Kommunikation sollte über verschiedene Funktionen gewährleistet werden. Zum einen war die Kommunikation End-to-End-verschlüsselt.[19] Zum anderen verfügten die Geräte über die Funktion, dass sich eine Nachricht nach einem gewissen Zeitablauf automatisch löscht (*Burn*

9 Ginowski, S. 112 f.

10 Regina v A, B, D & C [2021], EWCA Crim 128, [2021], § 11.

11 Ginowski, S. 87; vgl. LG Berlin, Urt. v. 19.12.2024 – 525 KLs 8/22, Rn. 131.

12 Stellungnahme Frankreichs v. 7. April 2022 vor dem EGMR (A.L. und E.J. vs. Frankreich, 44715/20 und 47930/21), § 7 (zum URL Fn 5); siehe aber Ginowski, S. 60 und 77, wonach anfänglich der Vertrieb der Encrophones über handelsübliche Verkäufer wie «Myntex» oder im Show-Room der EncroChat S.A. in Amsterdam erfolgte.

13 OLG Celle, Beschl. v. 12.8.2021 – 2 Ws 250/21, openJur 2021, 31403, Rn. 45.

14 Vgl. BGH, Beschl. v. 2.3.2022 – 5 StR 457/21, Rn. 10; Ginowski, S. 109.

15 Stellungnahme Frankreichs v. 7. April 2022 vor dem EGMR (A.L. und E.J. vs. Frankreich, 44715/20 und 47930/21), dortige Fn 1 zu § 7 (zum URL Fn 5).

16 Ginowski, S. 112; die Telefonfunktion setzte allerdings voraus, dass den Geräten das Mikrofon nicht entfernt wurde.

17 OLG München, Beschl. v. 19.10.2023 – 1Ws 525/23, BeckRS 2023, 30017, Rn. 41.

18 Rechtbank Amsterdam 17.3.2022, ECLI:NL:RBAMS:2022:1280, r.o. 3.2.

19 Ginowski, S. 112; zur Begriffsdefinition Hansjakob, Überwachungsrecht, N 224, wonach bei einer End-to-End-Verschlüsselung die Nachricht bereits auf dem Gerät des Absenders verschlüsselt, in verschlüsselter Form übertragen und erst auf dem Empfängergerät entschlüsselt wird.

Time).[20] Ebenfalls konnte der Nutzer durch eine bestimmte Tastenkombination sämtliche auf dem Gerät gespeicherten Daten löschen (*Panic Wipe*).[21]

3. Untersuchungsbeginn und involvierte Staaten

Der Überwachung der Encrophones ging die Überwachung des Messenger-Dienstes «Ennetcom» voraus. Ennetcom war ein Messenger-Dienst, der vorwiegend in der niederländischen organisierten Kriminalität genutzt worden ist.[22] Die Ennetcom-Server befanden sich in Kanada.[23] Mit Hilfe der kanadischen Behörden erlangten die niederländischen Behörden im September 2016 Zugriff auf 3.7 Millionen Nachrichten.[24] Bei deren Auswertung stellten die niederländischen Behörden fest, dass ein Teil der Ennetcom-Nutzer Encrophones verwendete.[25] Daraufhin leiteten die niederländischen Behörden Untersuchungen im Zusammenhang mit EncroChat ein.[26] Im Verlaufe der Jahre 2017/18 sind auch französische Behörden im Zuge von Ermittlungsverfahren im Betäubungsmittelbereich auf Encrophones gestossen.[27] Aufgrund der Verschlüsselung konnten sie die Geräte jedoch nicht auswerten.[28]

Aufgrund der internationalen Nutzung der Encrophones gingen die niederländischen und die französischen Behörden im Jahre 2017 eine Kooperation ein. Insbesondere teilten die niederländischen den französischen Behörden mit, dass sich die EncroChat-Server im Datenzentrum von OVH in Roubaix befinden.[29] Die Staatsanwaltschaft Lille eröffnete daraufhin im November 2018 eine Untersuchung in Form einer sog. «enquête préliminaire». Diese Untersuchung wurde wegen Verdachts auf Beteiligung an einer kriminellen Organisation und

20 Vgl. Stoykova, S. 1.

21 Vgl. Stoykova, S. 1; Sagittae, S. 279.

22 Vgl. Zhilla, S. 14.

23 Rechtbank Amsterdam 19.4.2018, ECLI:NL:RBAMS:2018:2504, r.o. 3.1.1.

24 Vgl. Hoge Raad 28.6.2022, ECLI:NL:HR:2022:900, r.o. 3.2; Sagittae, S. 275, der darauf hinweist, dass es den niederländischen Behörden offenbar untersagt gewesen sei, die Daten weiteren Staaten zu übermitteln, weshalb die Bedeutung der Ennetcom-Daten begrenzt gewesen sei.

25 Van de Pol, reconstructie, Abschnitt «Ennetcom en PGPSafe».

26 Van de Pol, rechtbanken, Abschnitt «Rook».

27 BGH, Beschl. v. 2.3.2022 – 5 StR 457/21, Rn. 8.

28 BGH, Beschl. v. 2.3.2022 – 5 StR 457/21, Rn. 8; vgl. Tribunal judiciaire de Lille, 30.1.2020, S. 2 (zum URL Fn 3).

29 Van de Pol, rechtbanken, Abschnitt «Frankrijk of Nederland?».

nicht angemeldeter Lieferung, Transfers und Imports eines Verschlüsselungsmittels (nachfolgend: unangemeldete Kryptologie) geführt.[30]

Im Jahr 2019 beteiligte sich auch Grossbritannien an den Ermittlungen.[31] Im Februar 2020 formalisierten die niederländischen und französischen Behörden ihre Zusammenarbeit in Form eines Joint-Investigation-Team-Abkommens (JIT).[32] Zur Koordinierung und späteren Datenübermittlung wurde ferner Eurojust involviert.[33]

4. Aufklärungszugriffe auf die Server

Über die Vorgehensweise der Überwachung ist wenig bekannt, da die eingesetzten Mittel unter das französische Verteidigungsgeheimnis fallen.[34] Bekannt ist zumindest, dass im frühen Operationsstadium erste Aufklärungsmassnahmen ergriffen wurden. Zu diesem Zweck genehmigte der juge des libertés et de la détention du tribunal de grande instance Lille (nachfolgend: Tribunal judiciaire de Lille) im Dezember 2018 und Oktober 2019, Kopien der Server anzufertigen.[35] Daraufhin griffen die Behörden auf die Server von EncroChat zu, möglicherweise unter Duldung des Datenzentrums OVH.[36] Im Rahmen dessen konnten die Behörden auf die virtual machines[37] zugreifen.[38] In diesen virtual machines befanden sich Daten wie IP-Adressen, IMEI-Num-

30 BGH, Beschl. v. 2.3.2022 – 5 StR 457/21, Rn. 8; Stellungnahme Frankreichs v. 7. April 2022 vor dem EGMR (A.L. und E.J. vs. Frankreich, 44715/20 und 47930/21), § 7 und 10 (zum URL Fn 5); Eurojust, l'enquête EncroChat en France, S. 2 <https://www.eurojust.europa.eu/sites/default/files/2020-07/2020-07-02_EncroChat-investigation-in-France_FR.pdf>.

31 NCA, Mitteilung v. 2.7.2020 <https://www.nationalcrimeagency.gov.uk/news/operation-venetic>.

32 Rechtbank Amsterdam 21.11.2022, ECLI:NL:RBAMS:2022:6816, r.o. 5.1.2.

33 Eurojust, Pressemitteilung v. 2.7.2020 <https://www.eurojust.europa.eu/news/dismantling-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe>.

34 Vgl. beispielsweise Tribunal judiciaire de Lille, 30.1.2020, S. 5 (zum URL Fn 3).

35 Die entsprechenden Genehmigungen liegen dem Verfasser nicht vor, das beschriebene Vorgehen lässt sich aber dem Tribunal judiciaire de Lille, 30.1.2020, S. 3 (zum URL Fn 3) entnehmen; EGMR A.L. und E.J. vs. Frankreich, Urteil vom 24. September 2024, 44715/20 und 47930/21, § 12 f.

36 Vgl. Ginowski, S. 191.

37 Siehe <https://www.vmware.com/topics/virtual-machine>, wonach es sich bei einer virtual machine um eine Rechenressource handelt, die die Funktionen eines physischen Computers nachbildet, um Programme auszuführen.

38 Gemäss Tribunal judiciaire de Lille, 30.1.2020, S. 3 (zum URL Fn 3) wurden die Schlüssel für die virtual machines offenbar in unverschlüsselten Tang-Servern gehalten.

mern[39] der Encrophones und IMSI-Nummern[40] der SIM-Karten.[41] Die technische Analyse dieser Zugriffe hat ergeben, dass 66'134 SIM-Karten im System eingetragen waren[42] und die Nutzer in ganz Europa verteilt waren.[43]

Bei diesen Zugriffen konnten 3'477 Nutzernotizen (EncroNotes) entschlüsselt werden.[44] Diese hätten gemäss Tribunal judiciaire de Lille «zweifelsfrei in Verbindung mit illegalen Aktivitäten, insbesondere Drogenhandel» gestanden.[45] Diese Aussage bezieht sich allerdings vermutlich auf Notizen *dreier* Encrophones.[46]

5. Genehmigungsbeschlüsse

Um die späteren Zugriffe auf die Endgeräte zu ermöglichen, waren mehrere Genehmigungen erforderlich. Die Staatsanwaltschaft beantragte am 29. Januar 2020 Überwachungsmassnahmen, um die Nutzer der Encrophones zu «identifizieren» und «festzusetzen».[47] In der Folge genehmigte das Tribunal judiciaire de Lille am 30. Januar 2020, ein «technisches Gerät» direkt an den Servern einzusetzen. Damit sollten die Nutzerdaten, wie sie auf den Geräten eingegeben oder empfangen werden, abgegriffen werden.[48] Am 12. Februar 2020 wurde diese Massnahme verlängert, mit der zusätzlichen Befugnis, das «Abfangtool»[49] auf die mit dem Server verbundenen Endgeräte aufzuspielen. Daraufhin wurden weitere Massnahmen genehmigt: die Blockade mehrerer Admi-

39 IMEI steht für International Mobile Equipment Identity und ist eine 15-stellige Nummer, die jeweils einem Mobilfunkgerät zugeordnet ist.

40 IMSI steht für International Mobile Subscriber Identity und ist eine 15-stellige Nummer, die jeweils einer SIM-Karte zugeordnet ist.

41 Tribunal judiciaire de Lille, 30.1.2020, S. 3 (zum URL Fn 3); EGMR A.L. und E.J. vs. Frankreich, Urteil vom 24. September 2024, 44715/20 und 47930/21, § 13.

42 Vgl. BGH, Beschl. v. 2.3.2022 – 5 StR 457/21, Rn. 11.

43 Vgl. Tribunal judiciaire de Lille, 30.1.2020, S. 4 (zum URL Fn 3).

44 BGH, Beschl. v. 2.3.2022 – 5 StR 457/21, Rn. 11; EGMR A.L. und E.J. vs. Frankreich, Urteil vom 24. September 2024, 44715/20 und 47930/21, § 14.

45 Tribunal judiciaire de Lille, 30.1.2020, S. 4 (zum URL Fn 3); BGH, Beschl. v. 2.3.2022 – 5 StR 457/21, Rn. 11.

46 LG Berlin, Urt. v. 19.12.2024 – 525 KLs 8/22, Rn. 125; vgl. Stellungnahme Frankreichs v. 7. April 2022 vor dem EGMR (A.L. und E.J. vs. Frankreich, 44715/20 und 47930/21), § 7 (zum URL Fn 5), wonach lediglich die französischsprachigen Geräte ausgewertet wurden; sowie Tribunal judiciaire de Lille, 30.1.2020, S. 4 (zum URL Fn 3), wonach drei Geräte französische Notizen enthielten.

47 LG Berlin, Beschl. v. 1.7.2021 – 525 KLs 10/21, openJur 2021, 21800, Rn. 11 mit Verweis auf den Antrag der französischen Staatsanwaltschaft v. 29.1.2020.

48 Tribunal judiciaire de Lille, 30.1.2020, S. 5 (zum URL Fn 3).

49 Diese Bezeichnung ist BGH, Beschl. v. 2.3.2022 – 5 StR 457/21, Rn. 17 entnommen.

nistratoren (4. März 2020), eine Umleitung von Datenströmen, die die Domain encrochat.ch mit Subdomains verbindet (20. März 2020) und die Umleitung der Daten auf die staatliche Abfangeinrichtung (31. März 2020).[50] Am 29. April und 28. Mai 2020 wurden die Massnahmen jeweils verlängert.[51]

6. Zugriff auf die Endgeräte

a) Aufspielen der Schadsoftware

Die französischen Behörden entwickelten eine Schadsoftware, welche die Daten in den Endgeräten abgreifen sollte. Unklar bleibt, inwiefern die niederländischen Behörden an der technischen Umsetzung beteiligt waren.[52] Am 1. April 2020 spielten die französischen Behörden die Schadsoftware auf den Update-Server von EncroChat auf.[53] Von diesem aus übertrug sich die Schadsoftware über Updates auf die einzelnen Endgeräte.[54] Technisch betrachtet bewirkte dieser Vorgang keine Installation einer weiteren Software, sondern eine Modifikation der bestehenden Software.[55] Offen bleibt dabei, ob die Schadsoftware im Zuge regulärer Sicherheitsupdates[56] oder durch staatlich simulierte Updates[57] auf die einzelnen Encrophones aufgespielt wurde.

b) Historical data collection

Die Schadsoftware führte auf den Encrophones eine zweistufige Datenerhebung durch.[58] In der ersten Stufe *(historical data collection)* wurden sämtliche Daten, die lokal auf dem Gerät gespeichert waren, abgegriffen und auf einen polizeilichen Server übermittelt.[59] Dies beinhaltete Daten wie IMEI-

50 BGH, Beschl. v. 2.3.2022 – 5 StR 457/21, Rn. 12 ff.

51 Tribunal judiciaire de Lille, 29.4.2020 und 28.5.2020 (zum URL Fn 3); gemäss Eurojust, L'enquête EncroChat en France, S. 2 (zum URL Fn 30), erfolgte am selben Datum die «ouverture d'information».

52 Vgl. Van de Pol, rechtbanken, Abschnitt «Frankrijk of Nederland?».

53 BGH, Beschl. v. 2.3.2022 – 5 StR 457/21, Rn. 17; LG Berlin, Beschl. v. 1.7.2021 – 525 KLs 10/21, openJur 2021, 21800, Rn. 12.

54 LG Berlin, Beschl. v. 19.10.2022, 525 KLs 8/22, openJur 2022, 19018, Rn. 31.

55 Vgl. Albrecht et al., S. 27.

56 So Ginowski, S. 198.

57 So LG Berlin, Beschl. v. 19.10.2022, 525 KLs 8/22, openJur 2022, 19018, Rn. 31 f.; Regina v A, B, D & C [2021], EWCA Crim 128, [2021], § 12.

58 SF and Ors v NCA [2023] UKIPTrib3, § 77.

59 SF and Ors v NCA [2023] UKIPTrib3, § 43 und 77 m.H.a. auf die E-Mails des französischen Amtsträgers Jeremy Décou.

Nummern, Benutzernamen, Notizen und nicht gelöschte Chatnachrichten.[60] Dadurch konnte typischerweise die Kommunikation der letzten sieben Tage abgegriffen werden.[61] Teilweise wurde während der ersten sieben Tage diese Datenerhebung mehrmals durchgeführt.[62]

c) Forward facing collection

Zeitgleich oder unmittelbar darauffolgend setzte die zweite Stufe ein (*forward facing collection*[63]).[64] Fortan wurde die Chatnachricht – vor der Verschlüsselung auf dem jeweiligen Endgerät – erfasst und an einen französischen Polizei-Server übermittelt.[65] Teilweise wird vermutet, dass die Ausleitung über eine *Keylogger*-Technologie, welche die Tastatureingabe protokolliert, erfolgte.[66] Allerdings wird darauf hingewiesen, dass eine derartige Technologie mit erheblichen Systemverzögerungen verbunden gewesen wäre.[67] Vor diesem Hintergrund ist davon auszugehen, dass die Nachricht mittels *Kopiervorgangs* erfasst wurde: Im versendenden Endgerät wurde mit Betätigen der Sendefunktion von der noch nicht verschlüsselten, aber im RAM[68] zwischengespeicherten Nachricht eine Kopie erstellt und einem Polizei-Server zugeleitet.[69] War das Gerät des Empfängers ebenfalls mit der Schadsoftware infiziert, wurde dort nach der Entschlüsselung der Nachricht erneut eine Kopie gefertigt und an den Polizei-Server übermittelt.[70]

60 SF and Ors v NCA [2023] UKIPTrib3, § 43; Regina v A, B, D & C [2021], EWCA Crim 128, [2021], § 77.

61 Regina v A, B, D & C [2021], EWCA Crim 128, [2021], § 12.

62 Regina v A, B, D & C [2021], EWCA Crim 128, [2021], § 14.

63 SF and Ors v NCA [2023] UKIPTrib3, § 43 m.H.a. auf die E-Mails des französischen Amtsträgers Jeremy Décou.

64 Vgl. Goodwin, EncroChat, Abschnitt «two stage extraction».

65 Regina v A, B, D & C [2021], EWCA Crim 128, [2021], § 13.

66 Ginowski, S. 198; Van de Pol, brits document.

67 LG Berlin, Urt. v. 19.12.2024 – 525 KLs 8/22, Rn. 108.

68 RAM steht für Random Access Memory.

69 So Regina v A, B, D & C [2021], EWCA Crim 128, [2021], § 14 m.H.a. ein erstinstanzliches Urteil; SF and Ors v NCA [2023] UKIPTrib3, § 77; vgl. LG Berlin, Urt. v. 19.12.2024 – 525 KLs 8/22, Rn. 108; Cox, Police Hack.

70 R v Coggins and Ors [2020], Liverpool Crown Court, § 83.

d) Ausmass der Überwachung

Die Echtzeitüberwachung begann am 1. April 2020[71] und dauerte gemäss der französischen Regierung bis zum 2. Juli 2020[72]. Insgesamt wurden 300 Millionen Nachrichten abgegriffen.[73]

Die Überwachung betraf jedoch nicht sämtliche, sondern rund 60 % (39'571) der Encrophones.[74] Es liegt nahe, dass dieser Umstand nicht auf eine beabsichtigte Einschränkung, sondern auf technische Gründe zurückzuführen ist. Vermutlich war lediglich das Modell «Aquaris X2» von der Überwachung betroffen. Die übrigen Modelle («Aquaris» und «Aquaris X3») sind offenbar unbeeinträchtigt geblieben.[75]

Von den 39'571 überwachten Encrophones befanden sich etwa 500-600 Geräte in Frankreich.[76] Insgesamt wurden Nutzer in 122 Staaten lokalisiert.[77] Die meisten EncroChat-Nutzer befanden sich in den Niederlanden, gefolgt von Grossbritannien, Deutschland und Spanien.[78]

7. Zwischenstaatlicher Informationsaustausch und Datenübermittlung

Die französischen und niederländischen Behörden informierten einen Teil der betroffenen Staaten im Vorfeld der Echtzeitüberwachung. Eine wesentliche Rolle nimmt dabei die Eurojust-Videokonferenz vom 9. März 2020 ein, anlässlich derer die französischen Behörden einige europäische Staaten über die bevorstehende Überwachung informierten.[79] Die technologischen Einzelheiten der Überwachung wurden zwar nicht preisgegeben[80], allerdings wurden die

71 LG Berlin, Beschl. v. 19.10.2022, 525 KLs 8/22, openJur 2022, 19018, Rn. 32.

72 Vgl. Stellungnahme Frankreichs v. 7. April 2022 vor dem EGMR (A.L. und E.J. vs. Frankreich, 44715/20 und 47930/21), § 17 (zum URL Fn 5); siehe allerdings Ginowski, S. 204, wonach EncroChat S.A. nach Systemauffälligkeiten die Nutzer am 12. Juni 2020 über die behördliche Infiltration informierte und angab, den Dienst vom Netz genommen zu haben.

73 Oerlemans/Royer, S. 441.

74 EGMR A.L. und E.J. vs. Frankreich, Urteil vom 24. September 2024, 44715/20 und 47930/21, § 33.

75 Vgl. Albrecht et al., S. 22.

76 Vgl. Tribunal judiciaire de Lille, 28.5.2020, S. 4 (zum URL Fn 3); BStGer RR.2024.121 vom 11. Februar 2025, E. 6.3.

77 Tribunal judiciaire de Lille, 28.5.2020, S. 4 (zum URL Fn 3).

78 Vgl. Eurojust, L'enquête EncroChat en France, S. 7 (zum URL Fn 30).

79 LG Berlin, Beschl. v. 19.10.2022, 525 KLs 8/22, openJur 2022, 19018, Rn. 35.

80 Vgl. LG Berlin, Urt. v. 19.12.2024 – 525 KLs 8/22, Rn. 154.

Staaten darüber informiert, dass die Überwachung mit einem Zugriff auf die Endgeräte einhergeht.[81]

In der späteren Datenerhebung kam Europol eine zentrale Funktion zu. Europol sortierte anhand der Standortdaten die erhobenen Kommunikationsdaten und stellte diese den einzelnen Staaten zur Verfügung.[82] Nach Medienberichten hat auch die Schweiz EncroChat-Daten erhalten[83] und in diesem Zuge Ermittlungen eröffnet.[84] Eine diesbezügliche Anfrage des Verfassers liess das Fedpol jedoch unbeantwortet. Publizierte Rechtsprechung zu EncroChat liegt jedoch lediglich im Bereich der Rechtshilfe vor, die EncroChat-Nutzer und -Betreiber betrifft.[85]

Unklar ist, zu welchem Zeitpunkt Schweizer Behörden von den Überwachungsmassnahmen Kenntnis erlangten.[86] Anhaltspunkte für eine Teilnahme Schweizer Behörden an der Eurojust-Videokonferenz vom 9. März 2020 sind nicht ersichtlich. Gegenüber dem Portal Nau.ch äusserte das Fedpol, seit Ende Mai 2020 Daten von Europol erhalten zu haben.[87]

8. Datenbearbeitung

Die französischen Behörden liessen Europol die Daten in Form von JSON-Dateien zukommen.[88] Bei diesen Daten handelte es sich um Rohdaten, die dem Nutzer noch nicht zugeordnet waren.[89] Europol nahm daraufhin eine grobe Sortierung anhand von Standortdaten («Country Sorter»[90]) und Stichwörtern mithilfe einer Software vor.[91] Anschliessend stellte Europol den zuständigen

81 LG Berlin, Urt. v. 19.12.2024 – 525 KLs 8/22, Rn. 154 und 159.

82 Vgl. Campbell, ab Minute 23:16.

83 Del Favero.

84 Vogt.

85 Vgl. BStGer RR.2023.47 vom 20. September 2023; BGer 1C_126/2025 vom 7. März 2025; ferner spielt EncroChat auch im Sachverhalt des Entscheids des OGer ZH SB200505 vom 16. August 2021 eine Rolle.

86 Die entsprechende Frage im Auskunftsgesuch des Verfassers an das fedpol wurde nicht beantwortet.

87 Vgl. Del Favero, Abschnitte «Tausende Festnahmen in Europa» und «Fedpol verteilt Informationen».

88 Campbell, ab Minute 23:16; vgl. auch Rechtbank Limburg 26.4.2022, ECLI:NL:RBLIM:2022:3227, r.o. 3.2.2.3.

89 Stellungnahme Frankreichs v. 7. April 2022 vor dem EGMR (A.L. und E.J. vs. Frankreich, 44715/20 und 47930/21), § 59 f. (zum URL Fn 5).

90 Campbell, ab Minute 23:16.

91 Vgl. SF and Ors v NCA [2023] UKIPTrib3, § 37.

Staaten die Daten als TAR-Dateien zur Verfügung.[92] Die nationalen Zentralstellen leiteten diese Daten weiter an die zuständigen Strafverfolgungsbehörden. Diese ordneten die Nutzerdaten einzelnen Personen zu und verarbeiteten die Bilder und CSV-Dateien in Excel-Dateien. Erst bei der händisch durchgeführten Excel-Bearbeitung wurden die Kommunikationsdaten zweier Nutzer zu einer Konversation zusammengeführt.[93] Als Excel-Datei fanden die Chatinhalte schliesslich Eingang in das Strafverfahren, wie etwa nachfolgende Darstellung[94] zeigt:

Uhrzeit	von „showking" ausgehend	bei „showking" eingehend
12:51:51	*Alles gut bei dir*	
…		
12:52:27		*Ja*
12:52:35	*Ok*	
12:52:36		*Warten noch da*
12:52:46	*Noch nicht gekommen*	
12:53:07		*Nein*
12:53:12	*Ok*	
…		
14:14:48	*Und gekommen oder immer noch nicht*	
14:21:34		*Ja*
14:21:45		*Ichbin heir*
14:21:49	*Okay*	
14:21:58	*Pass auf dich auf wexxer*	
15:18:30	*Wenn du Probe bringst lass mal dann laden bitte ich will auch sehen*	
15:25:48	*Alles gut wexxer*	
15:26:46		*Ja*
…		
20:45:54		[Foto, das offensichtlich einen angebrochenen Kokainblock zeigt]
20:46:29	*Gute*	
20:46:39		*Ja*
20:46:42		*Gut*
20:49:23		[Foto, das offensichtlich einen ganzen Kokainblock zeigt]
20:49:53	*Richt gut*	
…		
20:50:03		*Jaaaaaaaa*

Der Austausch beim Drogengeschäft, festgehalten in Gerichtsdokumenten
Quelle: Welt

92 Campbell, Videogespräch, ab Minute 23:16.

93 Campbell, ab Minute 23:16; Stellungnahme Frankreichs v. 7. April 2022 vor dem EGMR (A.L. und E.J. vs. Frankreich, 44715/20 und 47930/21), § 59 (zum URL Fn 5).

94 Hinrichs, Abschnitt «Die Anwälte kassieren juristische Niederlagen».

9. Ermittlungserfolge

Am 2. Juli 2020 fand eine Pressekonferenz bei Eurojust statt, anlässlich welcher die Überwachungsmassnahme bekannt gegeben wurde.[95] Ein knappes Jahr später waren europaweit 1'500 Ermittlungsverfahren eingeleitet und 1'800 Festnahmen durchgeführt worden.[96] Bis zum 27. Juni 2023 betrug die Anzahl von Festnahmen 6'558 (davon 197 sogenannte High Value Targets).[97] Die mutmasslichen Deliktsbereiche betreffen mit je einem Drittel die organisierte Kriminalität und den Betäubungsmittelhandel. Das übrige Drittel entfällt auf Geldwäscherei, Tötungsdelikte und Waffenhandel.[98] Darüber hinaus wurden gemäss Europol zahlreiche Tötungsdelikte, Gewalttaten, Korruption und Betäubungsmitteltransporte verhindert.[99]

10. Prozessuales: Zielperson und Verfahrensart

Aus den Genehmigungsentscheiden geht nicht hervor, gegen wen formal das Verfahren geführt wurde. Die Vorwürfe des Verdachts auf Beteiligung an einer kriminellen Organisation und unangemeldeter Kryptologie deuten darauf hin, dass das Verfahren formell zunächst gegen die Organe der EncroChat S.A. bzw. Zwischenhändler der Encrophones geführt wurde.[100] Dies ist auch mit der Ansicht der französischen Regierung vereinbar, wonach die Nutzer lediglich Drittbetroffene waren.[101]

Demgegenüber äusserte die Staatsanwaltschaft bereits in ihrem Überwachungsantrag vom 29. Januar 2020 die Absicht, die Nutzer zu «identifizieren», deren «kriminellen Aktivitäten aufzuzeigen» und diese «festzunehmen».[102]

---

95 EGMR A.L. und E.J. vs. Frankreich, Urteil vom 24. September 2024, 44715/20 und 47930/21, § 34.

96 Europäische Kommission, Mitteilung an das europäische Parlament et al. v. 14.4.2021, S. 1 <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52021DC0170>.

97 Europol, Pressemitteilung v. 27.6.2023 <https://www.europol.europa.eu/media-press/newsroom/news/dismantling-encrypted-criminal-encrochat-communications-leads-to-over-6-500-arrests-and-close-to-eur-900-million-seized>.

98 Europol, Pressemitteilung v. 27.6.2023 (zum URL Fn 97).

99 Europol, Pressemitteilung v. 27.6.2023 (zum URL Fn 97).

100 Vgl. Tribunal judiciaire de Lille, 29.4.2020, S. 1 f. und 28.5.2020, S. 1 f. (zum URL Fn 3), wonach die Untersuchung erst am 7. April 2020 auf potenzielle Nutzerdelinquenz wie Waffen- und Betäubungsmitteldelikte ausgeweitet wurde.

101 Stellungnahme Frankreichs v. 7. April 2022 vor dem EGMR (A.L. und E.J. vs. Frankreich, 44715/20 und 47930/21), § 96 (zum URL Fn 5).

102 LG Berlin, Beschl. v. 1.7.2021 – 525 KLs 10/21, openJur 2021, 21800, Rn. 11 m.H.a. den Antrag der französischen Staatsanwaltschaft v. 29.1.2020.

Zweifelsfrei waren somit die Nutzer bereits zu diesem Zeitpunkt Zielpersonen der Überwachungsmassnahmen.[103]

Das Verfahren wurde zunächst als «enquête préliminaire» geführt.[104] Erst zwei Monate nach Beginn der Echtzeitüberwachung erfolgte am 28. Mai 2020 die ouverture d'information.[105] Der Begriff der «enquête préliminaire» wird häufig als «Vorermittlung» übersetzt.[106] Diese Übersetzung kann insofern irreführend sein, als nach schweizerischer Systematik eine Vorermittlung eine präventivpolizeirechtliche Aufklärung darstellt.[107] Die enquête préliminaire hingegen ist eine *strafprozessuale* Verfahrensart, die in Art. 75 ff. FR-CPP geregelt ist. Als strafprozessuale Massnahme setzt diese einen Anfangstatverdacht voraus[108], welcher vorliegend mit der Beteiligung an einer kriminellen Organisation und unangemeldeter Kryptologie begründet wurde.[109]

II. SkyECC

1. Eckdaten

Ein weiterer Anbieter von Kryptophones war das kanadische Unternehmen SkyGlobal.[110] Die Server von SkyGlobal befanden sich bei OVH in Roubaix (FR).[111] Dieser Messenger-Dienst war ursprünglich für BlackBerry-Telefone konzipiert, spätere Versionen waren aber auch mit Apple und Android kompatibel. SkyGlobal stattete die Geräte mit dem End-to-End-verschlüsselten Messenger-Dienst SkyECC aus.[112] Technologisch basierte die Verschlüsselung auf einer elliptic-curve-cryptography (ECC).[113] Um die Ortung und Überwachung zu erschweren, wurde die Funktionalität der Kamera und des Mikrofons eingeschränkt oder aufgehoben und die GPS-Funktion deaktiviert.[114]

103 Vgl. EGMR A.L. und E.J. vs. Frankreich, Urteil vom 24. September 2024, 44715/20 und 47930/21, § 10, wonach sich die Untersuchung gegen Betreiber, Verkäufer und Nutzer richtete.
104 Vgl. Tribunal judiciaire de Lille, 30.1.2020, S. 2 (zum URL Fn 3).
105 Eurojust, L'enquête EncroChat en France, S. 2 (zum URL Fn 30).
106 Vgl. etwa BGH, Beschl. v. 2.3.2022 – 5 StR 457/21, Rn. 8.
107 Vgl. § 4 PolG ZH.
108 Vgl. Knytel, S. 98 und 112 f.
109 Vgl. Tribunal judiciaire de Lille, 30.1.2020, S. 2 (zum URL Fn 3).
110 Lödden/Makepeace, S. 385.
111 Vgl. Oerlemans/Royer, S. 437.
112 Lödden/Makepeace, S. 385.
113 Oerlemans/Royer, S. 434.
114 Vgl. Lödden/Makepeace, S. 385; Oerlemans/Royer, S. 435.

Der Vertrieb erfolgte nicht direkt über SkyGlobal, sondern über anonyme Drittverkäufer.[115] Ein Nutzer-Abo kostete je nach Nutzungsdauer zwischen EUR 600 und 2'200.[116] Nach Angaben von Europol hatte SkyECC 170'000 Nutzer[117], wobei sich 20 % von diesen in den Niederlanden und Belgien befanden.[118] Auf Frankreich entfielen etwa 2'000 bis 2'500 Nutzer.[119]

2. Funktionen und Verschlüsselung

Das SkyECC-App liess sich öffnen, indem eine bestimmte Zahlenkombination in einen simulierten Taschenrechner eingegeben wurde.[120] Das SkyECC-App stellte den Nutzern eine Chat-Funktion und eine E-Mail-Funktion zur Verfügung.[121] Über eine Telefonfunktion verfügten die Geräte nicht. Die Endgeräte liefen nicht über Telefonnummern, sondern über eine «Sky-ID».[122] Die Vertraulichkeit der Nachrichten sollte dadurch gewährleistet werden, dass die Nachrichten 30 Sekunden nach dem Öffnen gelöscht wurden (*Burn Time*).[123] War ein Gerät nicht erreichbar, so wurde die Nachricht für 48 Stunden gespeichert und anschliessend gelöscht.[124] Zudem verfügten die Geräte über die Funktion, dass bei Eingabe eines gewissen Passwortes sämtliche Daten gelöscht wurden (*Panic Wipe*).[125] Darüber hinaus konnten die Daten von SkyGlobal aus der Ferne gelöscht werden.[126] Die Kommunikation der SkyECC-Geräte war über eine sog. Public-Key-Verschlüsselung End-to-End chiffriert.[127] Bei dieser Verschlüsselungsart verfügt jedes Gerät über ein Schlüsselpaar, einen öffentlichen (*public key*) und einen privaten Schlüssel (*private key*).[128] Das

115 Vgl. Oerlemans/Royer, S. 436; Stahl et al., Abschnitt «Generalverdacht gegen die Nutzer».

116 Oerlemans/Royer, S. 436.

117 Vgl. Europol, Pressemitteilung v. 10.3.2021 <https://www.europol.europa.eu/media-press/newsroom/news/new-major-interventions-to-block-encrypted-communications-of-criminal-networks>.

118 Vgl. Europol, Pressemitteilung v. 10.3.2021 (zum URL Fn 117).

119 Vgl. Saintourens/Piel; Hizzir.

120 Stahl et al., Abschnitt «Trügerisches Sicherheitsgefühl».

121 Oerlemans/Royer, S. 436.

122 Oerlemans/Royer, S. 436, wonach die Sky-ID aus einer alphanumerischen Kombination bestand.

123 Lödden/Makepeace, S. 385, dortige Fn 5.

124 Goodwin, Police, Abschnitt «Sky phones claimed to be the most secure available».

125 Vgl. Sagittae, S. 279.

126 Oerlemans/Royer, S. 436.

127 BG Dietikon DG240038 vom 19. Juni 2025, E. 2.2.

128 BG Dietikon DG240038 vom 19. Juni 2025, E. 2.2; BG Dielsdorf DG230011 vom 19. Januar 2024, E. 4.1.2.

versendende Gerät verschlüsselt die Nachricht mit dem öffentlichen Schlüssel des empfangenden Gerätes. Das empfangende Gerät entschlüsselt sodann die Nachricht mit seinem privaten Schlüssel.[129]

3. Untersuchungsbeginn und involvierte Staaten

Belgische Strafverfolgungsbehörden sind erstmals im Jahr 2016 auf SkyECC-Geräte gestossen. Im Rahmen von Ermittlungen innerhalb des Betäubungsmittelmilieus am Hafen von Antwerpen stellten sie zahlreiche SkyECC-Geräte sicher.[130] Auch die niederländischen Behörden stellten die Nutzung von SkyECC-Geräten im Betäubungsmittelmilieu fest.[131] Vor diesem Hintergrund begannen niederländische und belgische Behörden im Jahre 2016 im Zusammenhang mit SkyECC zu ermitteln.[132]

Im Jahre 2018 beantragten die niederländischen Behörden bei einem Gericht in Amsterdam, die Kopie der SkyECC-Server zu genehmigen. Die richterliche Genehmigung erfolgte am 30. November 2018.[133] Die Genehmigung wurde aufgrund des fehlenden individualisierten Tatverdachts lediglich zur technischen Aufklärung der Infrastruktur erteilt. Vorbehältlich einer weiteren richterlichen Genehmigung durften die Erkenntnisse nicht strafprozessual verwertet werden.[134]

Ende des Jahres 2018 stellten die belgischen Behörden (21. November 2018) und die niederländischen Behörden (6. Dezember 2018) je ein Rechtshilfeersuchen an Frankreich.[135] In Ausführung dieser Rechtshilfeersuchen führten die französischen Behörden einen Aufklärungszugriff auf die Server durch.[136]

Im Dezember 2019 richteten die Niederlande, Frankreich und Belgien ein JIT ein.[137] Im Übrigen gibt es Berichte, denen zufolge die amerikanische Drug En-

129 OGer ZH SB240422 vom 15. August 2025, E. III. 3.1.
130 Goodwin, Ex-boxer, Abschnitt «Operation Argus».
131 Goodwin, Ex-boxer, Abschnitt «Operation Argus».
132 Lödden/Makepeace, S. 385; Oerlemans/Royer, S. 437.
133 Goodwin, Ex-boxer, Abschnitt «The Sky ECC hack».
134 Rechtbank Amsterdam, rc-Nummer 18/42030, parketnummer 13/728195-18 (YUCCA), die ECLI-Nr. ist dem Verfasser nicht bekannt.
135 Oerlemans/Royer, S. 437; Lödden/Makepeace, S. 386.
136 Rechtbank Amsterdam 21.11.2022, ECLI:NL:RBAMS:2022:6816, r.o. 5.1.3.
137 Goodwin, Ex-boxer, Abschnitt «The Sky ECC hack»; siehe Reisinger, nach dem die niederländischen Behörden an der technischen Umsetzung der Überwachung massgeblich beteiligt waren.

forcement Administration (DEA) verdeckte Ermittler in die SkyECC-Vertriebsstrukturen eingeschleust haben soll.[138]

4. Französische Server-Überwachung

Ähnlich wie bei der Überwachung von EncroChat fallen die Modalitäten der Überwachung unter das französische Staatsgeheimnis[139], weshalb die Überwachungsvorgänge nur grob umschrieben werden können. Am 13. Februar 2019 eröffneten die französischen Behörden ein selbstständiges Ermittlungsverfahren gegen SkyGlobal.[140] Dieses Verfahren wurde als «enquête préliminaire» wegen Verdachts auf unangemeldete Kryptologie, Betäubungsmitteldelikte und kriminelle Organisation geführt.[141]

Am 14. Juni 2019 genehmigte das Gericht in Lille erstmals, die Kommunikation über die Server-Infrastruktur in Roubaix abzufangen.[142] Diese Massnahme wurde im weiteren Verlauf mehrmals verlängert.[143] Gestützt auf diese Genehmigung richteten die französischen Behörden IP-Taps an der Server-Infrastruktur in Frankreich ein, welche den Datenverkehr abgriffen.[144]

Aufgrund der Verschlüsselung der Nachrichten versetzte dieser Zugriff die Behörden allerdings noch nicht in die Lage, die zweiseitige Kommunikation zu lesen. Nichtsdestotrotz griffen die Behörden über eineinhalb Jahre (von Ende Juni 2019 bis Mitte Dezember 2020) die verschlüsselte zweiseitige Kommunikation ab. Lediglich die Namen und möglicherweise auch der Inhalt von Gruppenchats konnten in diesem Stadium gelesen werden, wobei sich dies nicht als erkenntnisreich erwies.[145]

138 Van de Pol, DEA.

139 Vgl. Cass. pen. sez., sent. 07.11.2023, n. 44154/23, consid. 5.2.

140 Vgl. Lödden/Makepeace, S. 386; OGer ZH SB240422 vom 15. August 2025, E. III. 2.

141 Monnier, Abschnitt «des serveurs à Roubaix»; vgl. Goodwin, SkyECC, Abschnitt «French indictment», wonach der SkyECC-Händler Thomas Herdmann wegen dieser Vorwürfe angeklagt wurde; ferner OGer ZH SB240422 vom 15. August 2025, E. III. 2.

142 OGer ZH SB240422 vom 15. August 2025, E. III. 2.1.

143 OGer ZH SB240422 vom 15. August 2025, E. III. 2.

144 Rechtbank Amsterdam 21.11.2022, ECLI:NL:RBAMS:2022:6816, r.o. 5.1.3; OGH, 7.1.2025, 11 Os 147/24p, Rz 18.

145 Vgl. Rechtbank Amsterdam 21.11.2022, ECLI:NL:RBAMS:2022:6816, r.o. 5.1.3.

5. Provokation der Zugangsdaten und Kommunikationszugriff

Um die an den Servern abgefangenen, aber verschlüsselten Nachrichten lesbar zu machen, mussten die Strafverfolgungsbehörden an die kryptographischen Schlüssel gelangen. Dies erfolgte in einer Vorgehensweise, deren technische Details nach wie vor unklar sind. Insbesondere wirft die Tatsache, dass es sich um angeblich End-to-End-verschlüsselte Kommunikation handelte und die Kommunikation teils rückwirkend entschlüsselt wurde, Fragen auf.[146] Trotz dieser Unklarheiten lässt sich das behördliche Vorgehen wie folgt grob skizzieren: Am 14. Mai 2020 und am 3. Juni 2020 fertigten die französischen Behörden eine Kopie des Arbeitsspeichers eines SkyECC-Servers an. Bei diesem Vorgang erhielten die französischen Behörden technische Unterstützung der niederländischen Behörden. Dieser Aufklärungszugriff erlaubte den niederländischen und französischen Behörden einen sog. Man-in-the-Middle-Server zu entwickeln.[147]

Die generelle Verwendung des MITM-Servers wurde von der *commission consultative* am 12. November 2020 bewilligt.[148] Anschliessend genehmigte ein französisches Gericht den spezifischen Einsatz der MITM-Methode im Dezember 2020, woraufhin die Behörden einen MITM-Server vermutlich im Datenzentrum in Roubaix installierten.[149] Dieser MITM-Server kontaktierte fortan die Endgeräte mit einer sog. Push-Nachricht, sobald sich ein Endgerät mit der betroffenen Serverstruktur verbunden hatte.[150] Diese Nachrichten des MITM-Servers waren von den Anfragen aus der SkyECC-Infrastruktur nicht zu unterscheiden.[151] Das Endgerät gab infolge dieser Kontaktierung – ohne Kenntnis des Nutzers – den privaten Schlüssel frei.[152] Diese Provokation der privaten Schlüssel erlaubte den Behörden zweierlei[153]: Zum einen konnten die Behörden die seit eineinhalb Jahren blind abgefangene Kommunikation im Dezember 2020 rückwirkend entschlüsseln.[154] Zum anderen konnten sie ab Mitte

146 Vgl. Freiling et al., S. 434 f.
147 Vgl. OGH, 7.1.2025, 11 Os 147/24p, Rz 18.
148 Rechtbank Amsterdam 21.11.2022, ECLI:NL:RBAMS:2022:6816, r.o. 5.1.3; OGH, 7.1.2025, 11 Os 147/24p, Rz 18.
149 Vgl. OGH, 7.1.2025, 11 Os 147/24p, Rz 18; Oerlemans/Royer, S. 438; Lödden/Makepeace, S. 387.
150 OGer ZH SB240422 vom 15. August 2025, E. III. 3.1.
151 Vgl. Freiling et al., S. 434 f.
152 OGer ZH SB240422 vom 15. August 2025, E. III. 3.1.
153 Vgl. Lödden/Makepeace, S. 387.
154 Lödden/Makepeace, S. 386 f.

Februar 2021[155] bis zum 9. März 2021 die Kommunikation in Echtzeit überwachen.[156] Von dieser Echtzeitüberwachung waren global etwa 70'000 Geräte betroffen.[157] Insgesamt sollen während der gesamten Überwachungsdauer von 21 Monaten etwa 1,5 Milliarden Nachrichten samt Randdaten abgefangen worden sein.[158]

6. Informationsaustausch und Datenübermittlung

Die JIT-Staaten nahmen eine erste Datenbearbeitung mit Datenanalyseprogrammen wie «Hansken» oder «Chat-X» vor.[159] Zur internationalen Koordinierung der Datenübermittlung involvierten die JIT-Staaten Europol.[160] Bei Europol wurde daraufhin eine Task Force eingerichtet[161], vermutlich im März 2021[162]. Europol systematisierte die Daten und ordnete sie den Mitgliedstaaten zu.[163] Dazu erstellte Europol hunderte «intelligence reports», in denen die Chatnachrichten ausgewertet und den Nutzern zugeordnet wurden.[164]

Es ist unklar, wann die Schweiz Kenntnis von der Überwachung hatte; eine entsprechende Anfrage liess das Fedpol unbeantwortet. Die Schweiz trat der Europol-Task Force im September 2021 bei.[165] Gemäss Medienmitteilung des Fedpol erhielt dieses im Jahre 2021 «erste Einblicke in die sichergestellten und entschlüsselten» Daten.[166] Es bleibt spekulativ, ob diese Sichtung erst nach dem Beitritt in die Task Force im September 2021 erfolgte.

Anfang des Jahres 2022 erhielt das Fedpol einen permanenten Zugang zu den SkyECC-Daten mit Bezug zur Schweiz.[167] Das Fedpol leitete daraufhin die Da-

155 Oerlemans/Royer, S. 435.
156 OGH, 7.1.2025, 11 Os 147/24p, Rz 18.
157 Europol, Pressemitteilung v. 10.3.2021 (zum URL Fn 117).
158 Vgl. Monnier, Abschnitt «1,5 milliard de messages interceptés»; Lödden/Makepeace, S. 384, gehen von 1 Milliarde abgefangener Nachrichten aus.
159 Vgl. Oerlemans/Royer, S. 439; Van de Pol, geheim plan, Abschnitt «Chat X».
160 Lödden/Makepeace, S. 386.
161 Fedpol, Auskunft an den Verfasser, S. 1.
162 Vgl. Europol, Pressemitteilung v. 10.3.2021 (zum URL Fn 117).
163 Fedpol 2022 <https://2022.fedpol.report/de/schwerst-kriminalitat/verschlusselte-chats-der-organisierten-kriminalitat/>.
164 Lödden/Makepeace, S. 386.
165 Fedpol, Auskunft an den Verfasser, S. 1.
166 Vgl. fedpol 2022 (zum URL Fn 163).
167 Fedpol 2022 (zum URL Fn 163); Gemäss fedpol23 <https://fedpol.report/de/report-2023/editorial/fedpol-im-einsatz-fuer-die-schweiz-jederzeit-ueberall> habe die Schweiz ein «Countrypackage» erhalten.

ten den zuständigen Staatsanwaltschaften weiter.[168] Wie bereits bei den EncroChat-Verfahren fanden die SkyECC-Daten in Form von Excel-Dokumenten letztlich Eingang in die Verfahrensakten.[169]

7. Ermittlungserfolge

Am 9. März 2021, dem sog. «action day», führten die niederländischen und belgischen Behörden zahlreiche Hausdurchsuchungen und Festnahmen durch.[170] Tags darauf machte Europol die Überwachung bekannt.[171] Nachdem die US-Behörden in diesen Tagen die SkyGlobal-Website okkupierten, nahm SkyGlobal im März 2021 SkyECC vom Netz.[172]

Bis im März 2024 soll die SkyECC-Überwachung zu weltweit 5'270 Verhaftungen geführt haben.[173] Gemäss Europol seien durch die Operation 114 Tötungsdelikte verhindert worden.[174] In der Schweiz führte die Datenübermittlung bis im April 2024 zur Eröffnung von rund 60 Strafverfahren.[175]

III. Anom

1. Phantom Secure und Anom

Anom war ein weiterer Messenger-Dienst, der angeblich vorwiegend zu kriminellen Zwecken genutzt worden ist. In der Entstehung ist dieser eng mit dem Messenger-Dienst «Phantom Secure» verknüpft, weshalb in Kürze zunächst auf Phantom Secure einzugehen ist.

Phantom Secure war ein kanadisches Unternehmen, welches modifizierte, besonders abhörsichere BlackBerry-Telefone anbot.[176] Im Jahre 2017 leiteten das FBI und die australische Bundespolizei (AFP) eine Untersuchung gegen Phantom Secure ein, da sie eine kriminalitätsbezogene Nutzung vermuteten.[177] Im

168 Vgl. OGer AG SBK.2023.31 vom 23. November 2023, E. 2.3.1.
169 Vgl. Gall/Haskaya, S. 303; Van de Pol, Encrodata.
170 Cox, Dark Wire, S. 237 f.
171 Europol, Pressemitteilung v. 10.3.2021 (zum URL Fn 117).
172 Cox, Dark Wire, S. 239.
173 Hizzir.
174 Stahl et al., Abschnitt «Angeblich 114 Morde verhindert».
175 Della Valle, S. 8 f.
176 Cox, Dark Wire, S. 4.
177 Vgl. FBI, Application for a Warrant at US District Court of California v. 17.5.2021 ('21 MJ01948), S. 4 f.

Rahmen dieser Untersuchung versuchte das FBI erfolglos, über eine Kooperation mit Phantom Secure einen Zugriff auf die Kommunikation zu erhalten.[178] Im März 2018 verhaftete das FBI den CEO von Phantom Secure, Vincent Ramos, und nahm den Dienst zeitgleich vom Netz.[179] Letztlich wurde Ramos wegen Beteiligung an organisierter Kriminalität und Teilnahme am Betäubungsmittelhandel zu einer Freiheitsstrafe von neun Jahren verurteilt.[180]

Im Rahmen dieses Verfahrens sind das FBI und AFP auf den sich in Entwicklung befindenden Messenger-Dienst «Anom» gestossen.[181] Die Behörden gingen daraufhin eine Kooperation mit dem Entwickler von Anom ein.[182] Das FBI vereinbarte mit diesem – gegen Strafreduktion und Entschädigung –, dass Anom fortan vom FBI geführt werde.[183] In der Folge errichtete das FBI ein Scheinunternehmen mit Sitz in Panama, das die Weiterentwicklung und Distribution der Anom-Geräte in die organisierte Kriminalität bezweckte.[184]

2. Angepriesene Funktionen

Anom war als App ausgestaltet, welche auf Android betriebene Mobiltelefone aufgespielt wurde.[185] Die standardmässigen Telefon- und Messengerfunktionen wurden deaktiviert.[186] Die Kosten für eine halbjährige Nutzung lagen etwa bei EUR 750.[187]

Das Anom-App erschien vordergründig als Taschenrechnerfunktion. Bei Eingabe eines bestimmten Zahlencodes wurden die Anom-Funktionen dem Nutzer zugänglich.[188] Das App suggerierte, eine besonders vertrauliche, End-to-

178 Cox, Dark Wire, S. 74 ff.

179 FBI, Application for a Warrant at US District Court of California v. 17.5.2021 ('21 MJ01948), S. 5.

180 Vgl. FBI, Application for a Warrant at US District Court of California v. 17.5.2021 ('21 MJ01948), S. 4; Cox, Dark Wire, S. 70.

181 Supreme Court of South Australia, Question of Law (1 and 2 of 2023) SASCA 82 (27.6.2024), § 13; FBI, Application for a Warrant at US District Court of California v. 17.5.2021 ('21 MJ01948), S. 6.

182 FBI, Application for a Warrant at US District Court of California v. 17.5.2021 ('21 MJ01948), S. 6; Cox, Dark Wire, S. 76.

183 Cox, Dark Wire, S. 76 ff.; FBI, Application for a Warrant at US District Court of California v. 17.5.2021 ('21 MJ01948), dortige Fn 3.

184 OLG München, Beschl. v. 19.10.2023 – 1Ws 525/23, BeckRS 2023, 30017, Rn. 46; OGer AG SBK.2022.200 vom 24. Oktober 2022, E. 2.4.

185 Supreme Court of South Australia, Question of Law (1 and 2 of 2023) SASCA 82 (27.6.2024), § 18.

186 Supreme Court of South Australia, Question of Law (1 and 2 of 2023) SASCA 82 (27.6.2024), § 18.

187 Vgl. Cox, Dark Wire, S. 241.

188 Supreme Court of South Australia, Question of Law (1 and 2 of 2023) SASCA 82 (27.6.2024), § 68.

End-verschlüsselte Kommunikation zu ermöglichen.[189] Wie bei Kryptophones üblich, löschten sich die Nachrichten nach einem gewissen Zeitablauf vom Gerät.[190] Ferner erfolgte beim Eingeben einer bestimmten Tastenkombination die Löschung sämtlicher auf dem Gerät gespeicherten Daten.[191] Weiter wurde die Sicherheit damit beworben, dass die Server ausserhalb der Five-Eyes-Staaten[192] und der EU gehostet würden.[193]

3. Geheime Überwachungsfunktionen

Tatsächlich wurde jedoch jede einzelne Nachricht an die Strafverfolgungsbehörden geleitet. Nach Darstellung des Supreme Court of South Australia wurde beim Betätigen der Sendefunktion von der Nachricht – bevor sie verschlüsselt und versandt wurde – eine Kopie angefertigt.[194] Zudem wurden Randdaten vom Android-Betriebssystem der Kopie hinzugefügt.[195] Die Originalnachricht und deren Kopie wurden anschliessend End-to-End-verschlüsselt.[196] Die Originalnachricht wurde über einen Server an den vom Nutzer beabsichtigten Empfänger versandt. Die Kopie wurde ohne Wissen des Nutzers auf einen polizeilichen Server geleitet.[197] Auf diese Weise gingen den Behörden die unverschlüsselten Nachrichten der Nutzer zu.

Die Serverinfrastruktur hatte sich aufgrund des 4th Amendments[198] der amerikanischen Verfassung ausserhalb der USA zu befinden.[199] Entgegen den An-

189 Vgl. Cox, Dark Wire, S. 95.
190 Vgl. Cox, Dark Wire, S. 95.
191 Cox, Phone.
192 «Five-Eyes» ist die informelle Bezeichnung einer geheimdienstlichen Allianz zwischen USA, Kanada, Grossbritannien, Neuseeland und Australien.
193 Cox, Dark Wire, S. 95.
194 Supreme Court of South Australia, Question of Law (1 and 2 of 2023) SASCA 82 (27.6.2024), § 22 f.
195 Supreme Court of South Australia, Question of Law (1 and 2 of 2023) SASCA 82 (27.6.2024), § 73 und 80.
196 Supreme Court of South Australia, Question of Law (1 and 2 of 2023) SASCA 82 (27.6.2024), § 23 f. und 76.
197 Vgl. Supreme Court of South Australia, Question of Law (1 and 2 of 2023) SASCA 82 (27.6.2024), § 23 f.
198 Das 4th Amendment lautet: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
199 Vgl. OLG München, Beschl. v. 19.10.2023 – 1Ws 525/23, BeckRS 2023, 30017, Rn. 46; Finder, Abschnitt «Inside Law Enforcement's Operational Methodology».

preisungen befanden sich die Server zunächst in dem Five-Eyes-Staat Australien[200], später dann in einem nicht weiter bezeichneten EU-Staat[201].

4. Testphase in Australien

In Abstimmung mit der australischen AFP wurden testweise gut 50 Anom-Geräte in Australien in den Umlauf gebracht.[202] Über bestehende Phantom Secure Vertriebswege gelang es den Strafverfolgungsbehörden, die Anom-Geräte in der italienischen Mafia in Australien und der australischen Bikergang «Comancheros» zu verbreiten und so deren Kommunikation mitzulesen.[203] Dieser Überwachung lag keine gerichtliche Genehmigung in Australien, sondern lediglich eine polizeiliche Verfügung vom 25. September 2018 zugrunde.[204] Das australische Recht liess allerdings eine Herausgabe der Kommunikationsdaten an das FBI nicht zu. Das AFP teilte dem FBI lediglich grundsätzliche Informationen über die abgefangene Kommunikation, aber keine Kommunikationsinhalte mit.[205] Offenbar hat diese Testphase ergeben, dass sämtliche Geräte für kriminelle Zwecke genutzt worden seien.[206] Insbesondere sei Anom zur Abwicklung des Waffenhandels und des Betäubungsmittelhandels verwendet worden.[207]

5. Internationale Überwachung

Nach der Testphase in Australien wurde die Überwachung in Europa eingeleitet. Zu diesem Zweck liess das FBI im Sommer 2019 einen Server in einem rechtshilfefreundlichen Staat einrichten.[208] Nach Auskunft der US-Be-

200 Vgl. Cox, Dark Wire, S. 95; FBI, Application for a Warrant at US District Court of California v. 17.5.2021 ('21 MJ01948), S. 8.

201 Vgl. BGH, Beschl. v. 9.1.2025 – 1 StR 54/24, Rn. 12.

202 FBI, Application for a Warrant at US District Court of California v. 17.5.2021 ('21 MJ01948), S. 8.

203 Vgl. Cox, Dark Wire, S. 99 f.; FBI, Application for a Warrant at US District Court of California v. 17.5.2021 ('21 MJ01948), S. 7 f.

204 Siehe Government of South Australia, mit Hinweis darauf, dass die Nachricht vor dem Übermittlungsvorgang abgefangen worden sei und deshalb eine Genehmigung nicht erforderlich gewesen sei <https://www.dpp.sa.gov.au/prosecuting-crimes/cases-of-interest/questions-of-law-reserved-1-and-2-of-20232024sasca-82-27-june-2024>.

205 Rechtbank Oost-Brabant 18.7.2024, ECLI:NL:RBOBR:2024:3404, r.o. 3.2.

206 Vgl. Rechtbank Oost-Brabant 18.7.2024, ECLI:NL:RBOBR:2024:3404, r.o. 3.2 m.H.a. FBI-Unterlagen.

207 Cox, Dark Wire, S. 99 f.

208 Vgl. OLG München, Beschl. v. 19.10.2023 – 1Ws 525/23, BeckRS 2023, 30017, Rn. 46 f.; BGH, Beschl. v. 9.1.2025 – 1 StR 54/24, Rn. 12.

hörden befanden sich die Server fortan in einem Mitgliedstaat der Europäischen Union, dem aber Anonymität zugesichert worden ist.[209] Nach den Recherchen von Cox handelt es sich beim Genehmigungsstaat um Litauen, welches aufgrund der dortigen Rechtslage bewusst von den amerikanischen Behörden ausgesucht worden sei.[210] Auch die FAZ beleuchtete die Kooperation des FBI mit den litauischen Behörden. Aus dem der FAZ vorliegenden E-Mailverkehr soll hervorgehen, dass das FBI und die litauischen Strafverfolgungsbehörden den rechtshilfeweisen Genehmigungsantrag bewusst unvollständig und tatsachenwidrig formuliert hätten. So habe der amerikanische Genehmigungsantrag keinen Hinweis enthalten, dass Anom vom FBI entwickelt und distribuiert wurde.[211] Ferner sei tatsachenwidrig vorgebracht worden, dass der Server von litauischen Kriminellen eingerichtet worden sei.[212] In Unkenntnis über die tatsächlichen Begebenheiten habe das litauische Gericht die Überwachung des Servers und die Übermittlung der Daten an die amerikanischen Behörden am 3. Oktober 2019 genehmigt.[213]

In der Folge fingen die litauischen Behörden die Kommunikation, die über den besagten Server lief, vom 21. Oktober 2019 bis zum 7. Juni 2021 ab.[214] Es ist davon auszugehen, dass sich die Rolle der litauischen Behörden auf das Abfangen und Übermitteln der Kommunikationsdaten beschränkt.[215] Eigene Ermittlungsaktivitäten oder eine Auswertung der abgefangenen Nachrichten haben in Litauen vermutlich nicht stattgefunden.[216]

Auf diese Weise wurde die Kommunikation von etwa 12'000 Geräten, die zuvor in ganz Europa in den Umlauf gebracht worden waren, abgefangen.[217] Die Staaten, in denen Anom am meisten genutzt wurde, waren Deutschland, die Niederlande, Spanien, Australien und Serbien.[218]

209 Vgl. BGH, Beschl. v. 9.1.2025 – 1 StR 54/24, Rn. 12.
210 Vgl. Cox, Dark Wire, S. 107.
211 Klaubert, Heimlich, S. 3.
212 Vgl. Klaubert, Heimlich, S. 3.
213 Klaubert, Heimlich, S. 3.
214 Vgl. OLG Stuttgart, Beschl. v. 22.4.2024 – H 4 Ws 123/24, Burhoff-Online, E. II.
215 Vgl. Klaubert, Drittstaatsgeheimnis, S. 3.
216 Vgl. Rechtbank Oost-Brabant 18.7.2024, ECLI:NL:RBOBR:2024:3404, r.o. 3.2; BeckOK StPO-Graf, N 109 zu § 100a.
217 Europol, Pressemitteilung v. 8.6.2021 <https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication>.
218 Rechtbank Oost-Brabant 18.7.2024, ECLI:NL:RBOBR:2024:3404, r.o. 3.2.

6. Ausnahmen von der Überwachung

Die amerikanischen Behörden konnten die Überwachung auf bestimmte Staatsgebiete begrenzen. Aufgrund des 4th Amendments der amerikanischen Verfassung wurde das Abfangsystem dahingehend modelliert, dass die Nachrichten von Nutzern, die sich auf amerikanischem Boden befanden, nicht abgefangen wurden.[219] Daneben war zunächst auch das schweizerische Staatsgebiet von der Überwachung ausgenommen.[220] Nach Cox befürchtete das FBI, die Überwachung in der Schweiz stelle eine strafbare Handlung dar.[221] Die Restriktion betreffend die Schweiz wurde später allerdings aufgehoben[222], wobei unklar ist, zu welchem Zeitpunkt dies erfolgte.

7. Informationsaustausch

Litauen übermittelte dreimal pro Woche Datenpakete an das FBI.[223] Auf diese Weise erhielt das FBI etwa 27 Millionen Nachrichten inklusive Randdaten.[224] Nach dem Datenerhalt systematisierte und übersetzte gegebenenfalls das FBI die Kommunikationsinhalte.[225] Das FBI ordnete darüber hinaus die Jabber-Identifikation (JID) den einzelnen Nutzern zu.[226]

Zunächst stellte das FBI einzelnen Staaten die Daten zur Verfügung, indem es diesen Zugriff auf das Datenbearbeitungssystem «Hola iBot» erteilte.[227] Dieser Informationsaustausch war rein polizeilicher Natur. Die strafprozessuale Verwendung der Daten war nicht vom Übermittlungszweck gedeckt.[228] Die straf-

219 Klaubert, Heimlich, S. 3; siehe Cox, Dark Wire, S. 109, wonach die amerikanische Kommunikation über australische Polizei-Server geleitet worden sei und das FBI nur bei bevorstehender Lebensgefahr informiert worden sei.

220 Cox, Dark Wire, S. 215.

221 Vgl. Cox, Dark Wire, S. 215.

222 Cox, Dark Wire, S. 215.

223 Cox, Dark Wire, S. 111; FBI, Application for a Warrant at US District Court of California v. 17.5.2021 ('21 MJ01948), S. 9.

224 Vgl. Europol, Pressemitteilung v. 8.6.2021 (zum URL Fn 217); Cox, Dark Wire, S. 116 ff.

225 FBI, Application for a Warrant at US District Court of California v. 17.5.2021 ('21 MJ01948), S. 9; Rechtbank Oost-Brabant 18.7.2024, ECLI:NL:RBOBR:2024:3404, r.o. 3.2.

226 FBI, Application for a Warrant at US District Court of California v. 17.5.2021 ('21 MJ01948), S. 7, wonach die JID eine alphanumerische Kombination ist, die dem einzelnen Nutzer zugeordnet werden kann.

227 Cox, Dark Wire, S. 178 und 183, so erhielt beispielsweise das deutsche BKA im März 2021 Zugriff auf «Hola iBot».

228 Cox, Dark Wire, S. 183.

prozessuale Verwendung wurde erst durch die späteren Rechtshilfeersuchen an das FBI ermöglicht.[229]

Neben dem Direktzugang einzelner Staaten liess das FBI über Europol weiteren Staaten Daten separat zukommen.[230] Zu diesem Zweck richtete Europol im Oktober 2020 mit dem FBI die Operational Task Force «OTF Greenlight» ein.[231]

Die Schweiz partizipierte nicht an dieser Task Force.[232] Nichtsdestotrotz stand das Fedpol «in ständigem Kontakt» mit Europol und dem FBI.[233] Über Europol erhielten die Schweizer Strafverfolgungsbehörden die entsprechenden Anom-Daten, wobei der Zeitpunkt unklar ist.[234]

8. Ermittlungserfolge

Nach Ablauf der Überwachungsgenehmigung führten die australischen und europäischen Polizeieinheiten am 7. Juni 2021 zahlreiche Verhaftungen durch.[235] Tags darauf gab das FBI bekannt, dass Anom ein behördliches Überwachungsinstrument war.[236] Nach Angabe von Europol wurden bis zum 8. Juni 2021 über 800 Festnahmen in 16 Ländern durchgeführt.[237]

229 Vgl. OLG Stuttgart, Beschl. v. 22.4.2024 – H 4 Ws 123/24, Burhoff-Online, E. II; ferner OGH 14 Os14/24a, 5.11.2024, Rz 18, wo ein vergleichbares Vorgehen hinsichtlich Österreich beschrieben wird.

230 Vgl. Cox, Dark Wire, S. 260.

231 Europol, Pressemitteilung v. 8.6.2021 (zum URL Fn 217); Cox, Dark Wire, S. 260 f.; Sommer, S. 395.

232 Fedpol, Auskunft an den Verfasser, S. 2.

233 Wietlisbach, Abschnitt «welche Rolle spielt die Schweiz dabei?» m.H.a. eine Auskunft des fedpol an Keystone-SDA.

234 Vgl. OGer Bern BK 21 470 vom 12. November 2021, E. 8.1; vgl. aber BGer 7B_159/2022 und 7B_160/2022 vom 11. Januar 2024, dem der Sachverhalt zugrunde liegt, dass das Strafverfahren wegen einer Drittaussage gegen den Beschwerdeführer eröffnet wurde. Von der Anom-Nutzung des Beschwerdeführers erfuhren die Behörden erst im Laufe des Verfahrens, woraufhin sie ein Rechtshilfeersuchen an das FBI richteten.

235 Cox, Dark Wire, S. 271 und 287 ff.

236 Vgl. United States Attorney Office, Pressemitteilung v. 8.6.2021 <https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive>.

237 Europol, Pressemitteilung v. 8.6.2021 (zum URL Fn 217).

9. Prozessuales: Verfahrensart und Operationszweck

Die Überwachung von Anom erfolgte vermutlich weder in den USA noch in Litauen innerhalb eines Strafverfahrens.[238] Folglich handelte es sich dabei um eine amerikanische Aufklärungsoperation, innerhalb derer Litauen Amtshilfe leistete.[239] Da die amerikanische Kommunikation von der Überwachung ausgenommen war[240], lag der Operationszweck allein in der Erfassung ausländischer Kriminalität.

238 Vgl. OGer AG SBK.2022.200 vom 24. Oktober 2022, E. 2.5.

239 Vgl. FBI, Application for a Warrant at US District Court of California v. 17.5.2021 ('21 MJ01948), S. 9.

240 Vgl. FINDER, Abschnitt «Inside Law Enforcement's Operational Methodology».

B. Gemeinsame Merkmale der Kryptophones und deren Überwachung

I. Kryptophones als «grey infrastructure»

EncroChat, SkyECC und Anom ist gemeinsam, dass sie den Nutzern anpriesen, eine abhörsichere Kommunikation bereitzustellen. Zum (vermeintlichen) Schutz der Privatsphäre waren die Geräte auf rudimentäre Kommunikationsfunktionen reduziert. Technologisch war die Kommunikation jeweils End-to-End-verschlüsselt. Durch besondere Funktionen, wie das doppelte Betriebssystem, das automatische Löschen der Nachrichten nach Zeitablauf und das Löschen sämtlicher Daten bei Eingabe einer bestimmten Tastenkombination, sollte die Vertraulichkeit (vermeintlich) zusätzlich gestärkt werden.

Gewisse Ähnlichkeiten lassen sich auch in der Vertriebsweise erkennen. Die Vertriebsstrukturen waren intransparent, anonym und basierten auf persönlichen Beziehungen. Im Strafverfolgungsjargon werden Kommunikationsdienste, die nicht im sogenannten «weissen Markt» erhältlich sind und einen hohen Datenschutz bieten, auch als «grey infrastructure» bezeichnet.[241] Diese begriffliche Einordnung ist allerdings diffus, da eine Unterscheidung zu herkömmlichen Kommunikationsmitteln nicht ohne Weiteres möglich ist. Heute sind End-to-End-Verschlüsselungen sehr verbreitet.[242] Ebenso ist die Einstellung, dass sich die Nachrichten nach einem gewissen Zeitablauf automatisch löschen, auch bei herkömmlichen Messenger-Diensten möglich.[243] Zudem können auch Apple- und Androidgeräte aus der Ferne auf Werkseinstellung zurückgesetzt werden.[244]

---

241 Vgl. OERLEMANS/ROYER, S. 442; Stellungnahme Frankreichs v. 7. April 2022 vor dem EGMR (A.L. und E.J. vs. Frankreich, 44715/20 und 47930/21), § 7 und 113 (zum URL Fn 5); Nach OLG Celle, Beschl. v. 15.11.2021 – 2 HEs 24-30/21, openJur 2022, 5925, Rn. 35, seien die Vertriebsstrukturen von EncroChat und SkyECC «nicht legal» gewesen.

242 Die Kommunikation von WhatsApp und Signal ist derart verschlüsselt. Siehe WhatsApp-Website <https://faq.whatsapp.com/820124435853543#> und Signal-Website <https://support.signal.org/hc/en-us/articles/360007320391-Is-it-private-Can-I-trust-it#:~:text=Signal conversations are always end,the way that Signal works>.

243 Signal-Website > Signal Support > Features > Signal Messenger Features > set and manage disappearing messages (zum URL Fn 242); Whatsapp-Website > Chats > Einzelgruppenchats > Selbstlöschende Nachrichten ein- oder ausschalten (zum URL Fn 242).

244 Vgl. GRUBER/HARGREAVES/FREILING, S. 6.

Unter den Begriff der grey infrastructure liessen sich weitere Messenger-Dienste einreihen. Namentlich gegen folgende Messenger-Dienste wurden aufgrund der Vertriebsweise, deren Vertraulichkeitsschutzes und der angeblich kriminellen Nutzung ähnlich gelagerte Überwachungsoperationen durchgeführt:

Im Jahre 2016 erfolgte im Rahmen einer kanadisch-niederländischen Kooperation die Entschlüsselung des Messenger-Dienstes «Ennetcom».[245] Wenig später griffen die niederländischen Behörden im Jahr 2017 gemeinsam mit den Behörden Costa Ricas die Kommunikation des Messenger-Dienstes «PGPSafe» ab, dessen Server in Costa Rica lagen.[246] Ebenso erlangten die niederländischen Behörden im Jahre 2018 Zugriff auf die Kommunikation von «IronChat».[247] Im Jahre 2023 konnten die niederländischen Strafverfolgungsbehörden in Zusammenarbeit mit deutschen Behörden die Kommunikation von «Exclu» entschlüsseln und mit weiteren europäischen Strafverfolgungsbehörden teilen.[248] Im Jahre 2024 ist es den französischen und amerikanischen Behörden unter der Koordinierung von Europol gelungen, auf den Messenger-Dienst «Ghost» zuzugreifen.[249] Ende des Jahres 2024 entschlüsselten niederländische und französische Behörden den Messenger-Dienst «Matrix», sodass ihnen 2.3 Millionen Nachrichten zugänglich wurden.[250] Aus dieser unvollständigen Aufzählung lässt sich erkennen, dass es sich bei den EncroChat-, SkyECC- und Anom-Überwachungen nicht um Einzelphänomene, sondern um ein zwischenstaatliches System zur Verbrechensbekämpfung handelt.

II. Die Überwachungen als internationale Verbrechensbekämpfung

Der Grossteil der Nutzer von EncroChat, SkyECC und Anom befand sich nicht im Genehmigungsstaat, sondern in Drittstaaten. Die Überwachungsgenehmigungen betreffend EncroChat und SkyECC erteilte jeweils ein französisches

245 Sagittae, S. 275.
246 Sagittae, S. 275.
247 Openbaar Ministerie, Pressemitteilung v. 6.11.2018 <https://www.om.nl/actueel/nieuws/2018/11/06/doorbraak-in-onderscheppen-van-cryptocommunicatie>.
248 Openbaar Ministerie, Pressemitteilung v. 3.2.2023 <https://www.om.nl/actueel/nieuws/2023/02/03/politie-leest-opnieuw-mee-met-criminelen-cryptocommunicatiedienst-exclu-ontmanteld>.
249 Europol, Pressemitteilung v. 18.9.2024 <https://www.europol.europa.eu/media-press/newsroom/news/global-coalition-takes-down-new-criminal-communication-platform>.
250 Thomson.

Gericht.[251] In Frankreich befanden sich vermutlich weniger als 1 % (574 von 66'000) der EncroChat-Nutzer[252] bzw. weniger als 1.5 % (2'500 von 170'000) der SkyECC-Nutzer[253]. Die internationale Verwendung der Geräte ergab sich bereits vor der eigentlichen Überwachung der Endgeräte[254], sodass diese Operationen von Anfang an auf die internationale Verbrechensbekämpfung ausgerichtet waren. Gleiches gilt für die Anom-Überwachung. Die Genehmigung für die Anom-Überwachung wurde vermutlich in Litauen erteilt.[255] Aufgrund der geringen Einwohneranzahl von unter 3 Millionen[256] und fehlender Anhaltspunkte für eine dortige Nutzung[257] dürfte der dortige Nutzer-Anteil marginal sein. Die Kommunikation, die vom Territorium des Initiativstaates (USA) ausging, war ferner von der Überwachung ausgenommen. Zweifelsfrei diente somit auch diese Operation nicht der internen, sondern allein der internationalen Verbrechensbekämpfung.

III. Verdachtsbegründung und Verurteilungsrate

Strafverfolgungsbehörden und Gerichte begründen häufig den Verdacht gegen die einzelnen Nutzer mit Verweis auf den angeblich klandestinen Vertrieb, die hohen Nutzungskosten und den Vertraulichkeitsschutz der Geräte.[258] Im Folgenden wird versucht, sich quantitativ dieser Hypothese zu nähern, indem das Verhältnis zwischen der Anzahl Nutzer und Verurteilungen (nachfolgend: Verurteilungsrate) berechnet wird. Dies ist jedoch nur mit grossen Vorbehalten möglich. Zunächst ist die tatsächliche EncroChat- und SkyECC-Nutzung unbekannt, da die Überwachung bei weitem nicht sämtliche Geräte betraf.

251 Siehe vorstehend A. I. 5. und A. II. 3.

252 BStGer RR.2024.121 vom 11. Februar 2025, E. 6.3.

253 Hizzir.

254 Vgl. Tribunal judiciaire de Lille, 30.1.2020, S. 2 und 4 (zum URL Fn 3), wonach erste Aufklärungsmassnahmen die internationale Nutzung der EncroPhones aufzeigten; Rechtbank Amsterdam 21.11.2022, ECLI:NL:RBAMS:2022:6816, r.o. 5.1.3, wonach dem französischen Verfahren gegen SkyECC niederländische und belgische Rechtshilfeersuchen vorausgingen.

255 Vgl. Cox, Dark Wire, S. 107.

256 Eurostat, Database v. 9.1.2025 <https://ec.europa.eu/eurostat/databrowser/view/demo_gind__custom_-12532852/bookmark/table?lang=de&bookmarkId=f4e55477-525a-41d4-acee-f63b529ddfcc>.

257 Vgl. BeckOK D-StPO-Graf N 109 zu § 100a D-StPO; Eurojust, L'enquête EncroChat en France, S. 7, wonach Litauen auch bei der Nutzung von EncroChat nur eine geringe Dichte aufwies (zum URL Fn 30).

258 Vgl. BGH, Beschl. v. 9.1.2025 – 1 StR 54/24, Rn. 32 f.; Stellungnahme Frankreichs v. 7. April 2022 vor dem EGMR (A.L. und E.J. vs. Frankreich, 44715/20 und 47930/21), § 113 (zum URL Fn 5).

Zudem haben auf den gesamten erhobenen Datenbestand lediglich die JIT-Staaten (EncroChat/SkyECC) bzw. das FBI (Anom) Zugriff. Darüber hinaus bestehen hinsichtlich der verfügbaren Zahlen zahlreiche Unklarheiten. Bei den nationalen *Nutzerzahlen* geht aus den Quellen teils nicht hervor, ob sich diese auf die Anzahl *identifizierter* Nutzer oder sämtliche *bearbeiteten* Nutzer beziehen. Hinsichtlich der *Verurteilungszahlen* ist nicht bekannt, wie diese erfasst worden sind und ob die Verurteilungen rechtskräftig sind. Zudem stellt diese Anzahl nur eine Momentaufnahme dar. Im Lichte dessen sind folgende Werte lediglich als grobe Orientierung zu verstehen:

EncroChat	Frankreich	Deutschland	Grossbritannien	Insgesamt
Anzahl Nutzer	574[259]	4'600[260]	10'000[261]	66'134
Anzahl Verurteilungen	84 Strafverfahren (Stand 04.07.2024)[262]	974 (Stand: 30.05.2023)[263]	1'240 (Stand: 03.11.2023)[264]	unbekannt
Verurteilungsrate	**<15 %**[265]	**21 %**	**12 %**	unbekannt

SkyECC	Belgien	Insgesamt
Nutzer	6'000[266]	170'000
Verurteilungen	>1'000 (Stand: 15.12.2023)[267]	unbekannt
Verurteilungsrate	**16 %**	unbekannt

259 Vgl. BStGer RR.2024.121 vom 11. Februar 2025, E. 6.3. m.H.a. das französische Auslieferungsersuchen.

260 EuGH, Pressemitteilung 163/23 v. 26.10.2023 <https://curia.europa.eu/jcms/upload/docs/application/pdf/2023-10/cp230163de.pdf>.

261 NCA, Mitteilung v. 2.7.2020 (zum URL Fn 31).

262 Vgl. BStGer RR.2024.121 vom 11. Februar 2025, E. 6.3.

263 SZ (o.V.) m.H.a. dpa.

264 CPS, News v. 3.11.2023 <https://www.cps.gov.uk/cps/news/ex-police-employee-caught-leaking-information-about-operation-venetic-jailed>.

265 Da nicht jedes Strafverfahren in einer Verurteilung mündet, dürfte die Verurteilungsrate unter 15 % liegen.

266 Boffey.

267 Team Justice BE, Mitteilung v. 15.12.2023 <https://www.teamjustitie.be/fr/2023/12/15/15-12-dossier-sky-ecc-le-cap-des-1-000-condamnations-est-atteint/>.

Anom	Deutschland	Australien	Insgesamt
Nutzer	2'700[268]	1'659[269]	12'000
Verurteilungen	279 Urteile (Stand: Sept. 2024)[270]	63 (Stand: 27.06.2024)[271]	unbekannt
Verurteilungsrate	**<11 %**[272]	**4 %**	unbekannt

Die Verurteilungsraten der verschiedenen Staaten hinsichtlich desselben Messenger-Dienstes (z. B. EncroChat) unterscheiden sich erheblich. Dies könnte auf operativ-justizielle oder juristische Unterschiede zurückgeführt werden. Es könnte aber auch ein Anhaltspunkt für regionale Unterschiede in der Nutzungsweise sein.

Auch weisen die Verurteilungsraten hinsichtlich verschiedener Messenger-Dienste im selben Staat (siehe EncroChat und Anom in Deutschland) erhebliche Unterschiede auf. Dies kann damit zusammenhängen, dass die Datenbearbeitung einen gewissen Zeitraum in Anspruch nimmt, sodass die Verurteilungen erst mit Verzögerung erfolgen. Es könnte aber auch auf Unterschiede in der Nutzungsart zurückgeführt werden.

Bei aller Unsicherheit lässt sich zumindest festhalten, dass sich die angeblich vorwiegend kriminelle Nutzung retrospektiv nicht anhand der Verurteilungen ablesen lässt.

268 BKA, Pressemitteilung v. 5.7.2022, <https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2022/Presse2022/220705_PM_ANOM.html>.

269 AFP, Mitteilung v. 8.8.2024 <https://www.afp.gov.au/about-us/history/unique-stories/operation-ironside>.

270 Heise online (o.V.) m.H.a. dpa.

271 AFP, Pressemitteilung v. 27.6.2024 <https://www.afp.gov.au/news-centre/media-release/operation-ironside-third-anniversary-offenders-jailed-collective-307#:~:text=-The third anniversary of AFP,307 years' imprisonment in Australia>.

272 Da nicht jedes Urteil eine Verurteilung darstellt, dürfte die Verurteilungsrate unter 11 % liegen.

C. Verwertbarkeitsrecht

I. Beweiserhebungsverbote (Art. 140 StPO)

Das Gesetz unterscheidet zwischen *Beweiserhebungsverboten* (Art. 140 StPO) und *Beweisverwertungsverboten* (Art. 141 StPO). Die Beweiserhebungsverbote von Art. 140 StPO verbieten gewisse Methoden der Beweiserhebung. Unzulässig sind namentlich jene Beweiserhebungen, die auf Zwangsmittel, Gewaltanwendung, Drohung, Versprechen oder Täuschung zurückgreifen (Art. 140 Abs. 1 StPO).

II. Beweisverwertungsverbote (Art. 141 StPO)

1. Absolute Beweisverwertungsverbote

Eine unzulässige Beweiserhebung kann verschiedene Verwertbarkeitsfolgen nach sich ziehen. Eine mögliche Folge einer rechtswidrigen Beweiserhebung ist ein absolutes Verwertungsverbot. Ein absolutes Verwertungsverbot bedeutet, dass der Beweis unter keinen Umständen verwertet werden darf. Ein solches Verwertungsverbot entsteht, wenn ein Beweis mittels der in Art. 140 Abs. 1 StPO genannten Methoden erhoben wurde oder die StPO einen Beweis für unverwertbar bezeichnet (Art. 141 Abs. 1 StPO).

In der Literatur ist strittig, ob die absoluten Verwertbarkeitsverbote abschliessend in Art. 140 f. StPO genannt sind.[273] Der bundesgerichtlichen Praxis ist zu entnehmen, dass die gesetzliche Aufzählung nicht abschliessend ist. Namentlich folgert das Bundesgericht aus der Verletzung des Territorialitätsprinzips die absolute Unverwertbarkeit[274], obwohl dieser Verstoss nicht ausdrücklich von Art. 140 f. StPO erfasst ist[275].

---

273 Vgl. CR StPO-Bénédict, N 7a zu Art. 141, nach dem die absoluten Verwertbarkeitsverbote nicht abschliessend in Art. 141 StPO genannt sind; ähnlich BSK StPO I-Gless, N 15 zu Art. 141; a.A. Graf, Jusletter, S. 21.

274 Vgl. BGE 146 IV 36, E. 2.3; bestätigt in BGer 7B_120/2022 vom 5. Oktober 2023, E. 2.4.2.1.

275 Vgl. Graf, Jusletter, S. 21.

2. Relative Beweisverwertungsverbote

Neben den absoluten Verwertungsverboten sieht das Gesetz die relativen Verwertungsverbote vor. Ein relatives Verwertungsverbot bedeutet, dass ein Beweis unverwertbar ist, es sei denn, dessen Verwertung ist zur Aufklärung schwerer Straftaten unerlässlich (Art. 141 Abs. 2 StPO). Anders als ein absolutes Verwertungsverbot ist ein relatives Verwertungsverbot im Falle schwerer Straftaten somit einer Interessenabwägung zugänglich.

Ein relatives Beweisverwertungsverbot folgt, wenn eine Strafverfolgungsbehörde eine Beweiserhebung vornimmt, die ein strafbares Verhalten darstellt oder gegen eine Gültigkeitsvorschrift verstösst (Art. 141 Abs. 2 StPO). Eine Gültigkeitsvorschrift ist eine Verfahrensbestimmung, deren Zweck im Schutze von wesentlichen Interessen der betroffenen Person liegt.[276]

3. Verwertbarkeit bei Ordnungsvorschriftsverletzung

Rechtswidrig erlangte Beweise sind vorbehaltlos verwertbar, wenn Strafverfolgungsbehörden bei der Beweiserhebung lediglich eine Ordnungsvorschrift verletzen (Art. 141 Abs. 3 StPO). Ordnungsvorschriften erschöpfen sich darin, die äussere Ordnung des Verfahrens zu normieren.[277]

4. Folgebeweis

Ermöglicht ein relativ oder absolut[278] unverwertbarer Beweis die Erhebung eines weiteren Beweises, so ist der Folgebeweis nur verwertbar, wenn er ohne die vorhergehende Beweiserhebung möglich gewesen wäre (Art. 141 Abs. 4 StPO). Für die Verwendung eines Folgebeweises fordert das Bundesgericht eine grosse Wahrscheinlichkeit, dass die Strafverfolgungsbehörden den Folgebeweis hypothetisch auch rechtmässig hätten erlangen können.[279]

276 Vgl. BGE 139 IV 128, E. 1.6.
277 SK StPO I-Wohlers, N 33 zu Art. 141.
278 Vgl. BSK StPO I-Gless, N 89 zu Art. 141.
279 BGE 138 IV 169, E. 3.3.3.

III. Verwertbarkeit präventiv erhobener Informationen

Behörden können sich bei der Informationsbeschaffung auf verschiedene Rechtsgrundlagen stützen. Die StPO dient der Strafverfolgung, sodass deren Rechtsgrundlagen exklusiv anwendbar sind, sofern hinreichende Anhaltspunkte für eine begangene Straftat (Tatverdacht) vorliegen.[280] Ausserhalb dieser Verdachtslage können verfahrensrelevante Informationen namentlich gestützt auf das präventive kantonale Polizeirecht oder das Nachrichtendienstgesetz (NDG) erhoben werden. Während das kantonale Polizeirecht die Prävention und Gefahrenabwehr bezweckt[281], dient das NDG dem Schutz wichtiger Landesinteressen (Art. 2 f. NDG). Trotz der unterschiedlichen Zielsetzung ist eine strafprozessuale Verwendung derartig erhobener Informationen nicht ausgeschlossen. Namentlich im NDG ist der Transfer der Informationen in ein Strafverfahren gesetzlich vorgesehen (vgl. Art. 60 Abs. 2 und 3 NDG).[282] Typischerweise sind die Rechte der betroffenen Person im Strafverfahrensrecht jedoch stärker ausgebaut als im Sicherheitsrecht.[283] Darüber hinaus sind insbesondere im NDG Überwachungsmassnahmen vorgesehen, die der StPO gänzlich unbekannt sind.[284] Vor diesem Hintergrund ist es im Einzelfall eine delikate Frage, unter welchen Umständen sicherheitsrechtlich erhobene Informationen strafprozessual verwertet werden können. Ohne diese Frage ausführlich zu erörtern, wird hier mit der h.L. die Auffassung geteilt, dass eine sicherheitsrechtlich erhobene Information unter zwei Voraussetzungen strafprozessual verwertbar ist.[285] Zum einen muss die sicherheitsrechtlich erhobene Information *rechtmässig* erlangt worden sein.[286] Zum anderen kann eine sicherheitsrechtlich erhobene Information nur strafprozessual verwertet werden, wenn strafprozessuale Garantien *nicht umgangen* werden.[287] Dementsprechend sollten bei einer sicherheitsrechtlichen Informationserhebung die strafprozessualen Garantien beachtet

280 KIENER/SCHINDLER/BRUNNER, N 52 ff.; vgl. Art. 1 Abs. 1 und Art. 306 Abs. 3 StPO.

281 KIENER/SCHINDLER/BRUNNER, N 44 ff.

282 Vgl. BIAGGINI, N 284 ff.; kritisch dazu mit Hinweis auf das Trennungsgebot PIETH/GETH, S. 240.

283 Vgl. KIENER/SCHINDLER/BRUNNER, N 61.

284 Siehe nachstehend J.III.3.

285 Zu polizeirechtlich erhobenen Informationen siehe BSK StPO I-GLESS, N 38a zu Art. 141; KIENER/SCHINDLER/BRUNNER, N 61; zur umfassenden Betrachtung der Verwertbarkeit nachrichtendienstlicher Informationen siehe BIAGGINI, N 284 ff.

286 SK StPO II-LANDSHUT/BOSSHARD, N 3 zu Art. 306; vgl. KIENER/SCHINDLER/BRUNNER, N 1165.

287 BSK StPO I-GLESS, N 38a zu Art. 141; BSK StPO II-GALELLA/RHYNER, N 8 zu Art. 306; zu nachrichtendienstlich erhobenen Informationen siehe BIAGGINI, N 302 ff.

werden.[288] Dieser allgemeine Grundsatz spiegelt sich in Art. 60 Abs. 3 NDG wider. Demnach können nachrichtendienstlich erhobene Informationen bei Anhaltspunkten für eine Straftat den Strafverfolgungsbehörden bekannt gegeben werden, sofern die Strafverfolgungsbehörden hypothetisch eine *vergleichbare* strafprozessuale Massnahme hätten durchführen können.[289] Im Umkehrschluss sind somit Informationen aus einer sicherheitsrechtlichen Massnahme ohne strafprozessuales Pendant im Strafverfahren nicht verwertbar.[290]

288 KIENER/SCHINDLER/BRUNNER, N 61.

289 Vgl. ACKERMANN/VOGLER, S. 183.

290 Vgl. hinsichtlich präventiv-polizeirechtlicher Massnahmen KIENER/SCHINDLER/BRUNNER, N 61.

D. Lokalisierung von digitalen Beweisen

I. Lokalisierung anhand der Infrastruktur

Weist eine Beweiserhebung Berührungspunkte zu mehreren Jurisdiktionen auf, so ist es erforderlich, die Beweiserhebung zu lokalisieren. Eine Lokalisierung von digitalen Beweiserhebungen kann anhand verschiedener Anknüpfungspunkte erfolgen.

Greifen Strafverfolgungsbehörden auf im Ausland gespeicherte Daten zu, kann dieser Vorgang anhand der *betroffenen Infrastruktur* (z. B. des Datenträgers[291] oder Transitmediums[292]) verortet werden. Demnach ist eine behördliche Massnahme an dem Ort zu lokalisieren, wo die Behörden einen Datenverarbeitungsvorgang[293] auslösen. Eine Datenerhebung kann allerdings auch ohne Einwirkung auf eine Datenverarbeitungsanlage erfolgen, wie etwa beim Einsatz eines GPS-Trackers. In diesem Fall liegt keine betroffene Infrastruktur, sondern eine *Überwachungsinfrastruktur* vor. Die Lokalisierung erfolgt in diesem Fall anhand des Ortes der datengenerierenden Infrastruktur.[294]

Die beiden vorstehenden Ansätze knüpfen jeweils an die *Infrastruktur* an. Diese Anknüpfung entspricht der traditionellen Auffassung in der Literatur.[295] Zudem knüpft auch die zentrale Bestimmung des Völkerrechts von Art. 32 CCC ausdrücklich an den *Speicherort* – und somit an die datenhaltende Infrastruktur[296] – an. Die Anknüpfung an die Infrastruktur ist somit die grundsätzliche Lokalisierungsmethode, welche lediglich durch das nachstehend beschriebene *Zugriffsprinzip* durchbrochen werden kann.

---

291 Vgl. OK CCC-Graf, N 67 zu Art. 32; Dombrowski, S. 159.

292 Vgl. CR StGB II-Bottinelli, N 26 zu Art. 299, nach dem ein Staat berechtigt sei, Daten abzugreifen, die den Staat erreichen oder lediglich transitieren.

293 Unter einem Datenverarbeitungsvorgang wird vorliegend die Änderung des elektromagnetischen Zustands eines Datenverarbeitungssystems zum Zwecke der Datenbearbeitung verstanden.

294 Vgl. BGE 146 IV 36, E. 2.5, wonach im Falle eines GPS-Trackers der Aufnahmeort («lieux d'enregistrement») massgebend ist.

295 Vgl. Ryser, S. 576; Bär, S. 54; MüKo D-StPO-Hauschild, N 18 zu § 110; Heimgartner, S. 93 und 266 f.; vgl. KommStR-Oesterhelt/Frachebourd, N 24 zu § 29; Bangerter, S. 280; BeckOK D-StPO-Hegmann, N 15 zu § 110.

296 Vgl. OK CCC-Graf, N 23 zu Art. 32.

II. Lokalisierung anhand des Zugriffsberechtigten

1. Das Zugriffsprinzip

Die Lokalisierung anhand der *Infrastruktur* ist damit konfrontiert, dass Daten global verteilt, teils wechselhaft gespeichert werden. Mitunter ist der Speicherort nicht nachvollziehbar.[297]

Dieser Problematik begegnet das sog. *Zugriffsprinzip*. Dieses nimmt eine Lokalisierung nicht anhand der datenhaltenden Infrastruktur, sondern anhand der zugriffsberechtigten Person vor. Demnach ist ein Datenzugriff dort zu lokalisieren, von wo aus der Zugriffsberechtigte auf die Daten zugreifen kann (*Zugriffsort*).[298] Als zugriffsberechtigt gilt, wer die Kontrolle über die Daten und die Legitimität zur Datenbearbeitung hat.[299] Das Bundesgericht nimmt das Zugriffsprinzip auf, indem es festhält, dass «*nicht im Ausland*» handelt, wer über einen inländischen Internetzugang einen Kommunikationsdienst nutzt, dessen Daten im Ausland verwaltet werden.[300] Nach Ansicht des Bundesgerichts können folglich Schweizer Strafverfolgungsbehörden – bei Vorliegen eines Zugriffsorts in der Schweiz – auf ein Facebook-Konto zugreifen, obwohl die Daten im Ausland liegen.[301]

2. Anwendungsbereich des Zugriffsprinzips

Völkerrechtlich findet das Zugriffsprinzip eine Grundlage in Art. 18 Abs. 1 CCC. Diese Bestimmung betrifft die Edition von Computerdaten mit Auslandsbezug.[302] Art. 18 Abs. 1 CCC sieht vor, dass beim Datenberechtigten Daten ediert werden können, die im Ausland gespeichert sind. Anknüpfungspunkt dieser Bestimmung ist somit die Person, welche die Datenherrschaft hat.[303]

297 Vgl. OK CCC-Graf, N 6 zu Art. 32; SysK D-StPO-Jäger/Wohlers, N 9b zu § 110.
298 OK CCC-Graf, N 66 und 73 zu Art. 32; Wicker, S. 768 ff.; BeckOK D-StPO-Hegmann, N 15 zu § 110.
299 Council of Europe, Explanatory Report to the Convention on Cybercrime vom 23. November 2001, N 173.
300 Vgl. BGE 143 IV 270, E. 7.10.
301 Vgl. BGE 143 IV 270, E. 7.10.
302 Vgl. BGE 143 IV 21, E. 3.4.
303 OK CCC-Graf, N 10 zu Art. 18.

Über diese Völkerrechtsgrundlage hinaus erstreckt das Bundesgericht in nicht unumstrittener Weise das Zugriffsprinzip auf die Online-Recherche[304].[305] Auch in der deutschen (nicht höchstrichterlichen) Rechtsprechung wird teils in Bezug auf Online-Sichtungen an den Zugriffsort angeknüpft.[306] Der Anwendungsbereich des Zugriffsprinzips beschränkt sich somit in der Praxis auf offene Massnahmen mit geringerer Eingriffsintensität (*i.e.* Edition und Online-Recherche). Eine Limitation des Zugriffsprinzips ist jedoch nicht nur der Anwendungspraxis, sondern auch den bundesgerichtlichen Ausführungen zu entnehmen. Das Bundesgericht weist ausdrücklich darauf hin, dass eine Online-Recherche nicht vergleichbar ist mit dem Einsatz spezifischer Überwachungstechnologien.[307] Dies lässt den Schluss zu, dass das Zugriffsprinzip lediglich anwendbar ist, sofern keine spezifischen technischen Vorkehrungen getroffen wurden.[308]

III. Lokalisierung anhand des Netzwerkes?

Im Zusammenhang mit SkyECC wird von behördlicher Seite teils die Ansicht vertreten, ein Datenzugriff sei am Ort des Netzwerkes, mit dem das Datenverarbeitungssystem verbunden ist, zu verorten.[309] Diese Anknüpfung widerspricht jedoch den völkerrechtlichen Grundlagen. Vorstehend wurde dargelegt, dass das Völkerrecht eine Lokalisierung anhand des Datenträgers (vgl. Art. 32 CCC) oder des Zugriffsberechtigten (vgl. Art. 18 Abs. 1 CCC) vornimmt. Erfolgt nun ein Zugriff auf im Ausland gespeicherte Daten aufgrund der Nutzung eines inländischen Netzwerkes, so stellt dieser Zugriff eine Verletzung der völkerrechtlichen Ordnung dar.

---

304 Bei der Online-Recherche handelt es sich um eine Art der internetbasierten Durchsuchung, vgl. BGE 143 IV 270, E. 7.5 ff.

305 Vgl. BGE 143 IV 270, E. 7.10; zur Kritik siehe HUSMANN, Territorialitätsprinzip, S. 369 f.; ferner OK CCC-GRAF, N 67 zu Art. 32.

306 Vgl. LG Berlin, Beschl. v. 29.12.2022 – 519 Qs 8/22, diesem Beschluss liegt die Ausgangslage zugrunde, dass Behörden auf passwortgeschützte Daten zugriffen, wobei ein E-Mailkonto bereits geöffnet war und Login-Daten für weitere Accounts im Browser gespeichert waren; ferner LG Koblenz, Beschl. v. 24.8.2021 – 4 Qs 59/21, wo die Behörden im Rahmen der Durchsuchung von Räumlichkeiten an die Login-Daten gelangten und anschliessend mit diesen auf die Online-Konten des Beschuldigten zugriffen; ferner VG München, Beschl. v. 18.9.2023 – M 30 X 23.4359, Rz 51.

307 Vgl. BGE 150 IV 308, E. 2.6.2 «dans une telle configuration, elles ont en effet uniquement utilisé, et non mis en place pour ce faire, les possibilités usuelles de connexion».

308 Vgl. HUSMANN, Territorialitätsprinzip, S. 369.

309 Nach Informationen des Verfassers wird diese Ansicht seitens gewisser Behörden in der Schweiz vertreten.

Im Lichte dessen ist auch der in diesem Zusammenhang teils vorgebrachte Verweis auf die *Kopfschaltung* unbehilflich.[310] Eine Kopfschaltung ist eine zulässige Form der Kommunikationsüberwachung, bei der eine Person im Ausland überwacht wird, die mit einer Person in der Schweiz kommuniziert.[311] Hierbei wird die Kommunikation (der sich im Ausland befindenden Person) an *inländischen Netzknoten* erfasst.[312] Da somit die Erfassung an den *inländischen* Netzknoten heimischer Netzanbieter erfolgt[313], wird im Ausland *kein Datenverarbeitungsvorgang* ausgelöst. Anders ist die Situation, wenn die Überwachung nicht über heimische Netzanbieter, sondern über einen direkten Zugriff auf das (ausländische) Endgerät erfolgt. In diesem Fall wird im Ausland ein Datenverarbeitungsvorgang ausgelöst, sodass die Massnahme am Ort des Endgerätes zu verorten ist.[314]

Im Übrigen wäre eine Anknüpfung an das Netzwerk für die Strafverfolgungsbehörden äusserst unpraktikabel. Ein Nutzer in der Schweiz könnte sich etwa mit einem Netzwerk im Ausland verbinden und sich so dem Zugriff durch Schweizer Strafverfolgungsbehörden entziehen.

IV. Zusammenfassung

Aus dem Vorstehenden ergibt sich Folgendes: Eine Anknüpfung an die zugriffsberechtigte Person kann lediglich in Bezug auf offene Zwangsmassnahmen erfolgen. Geheime technische Zwangsmassnahmen hingegen sind anhand der entsprechenden Infrastruktur zu verorten. Ohne Bedeutung ist hingegen, mit welchem Netzwerk das entsprechende System verbunden ist.

310 Zur Zulässigkeit der Kopfschaltung siehe BVGer A-2335/2008, Urteil vom 10. März 2009.

311 HANSJAKOB, Überwachungsrecht, N 394 ff.

312 Ein Netzknoten verbindet das inländische Netz mit den ausländischen Netzen (sog. Auslandkopf), siehe dazu Drucksache des deutschen Bundestages 15/5199 (2005), Vorbemerkung der Bundesregierung sowie Antwort auf Frage 14 und 17; KOCHHEIM, S. 775.

313 BVGer A-2335/2008, Urteil vom 10. März 2009, E. 7.4; Drucksache des deutschen Bundestages 15/5199 (2005), Vorbemerkung der Bundesregierung sowie Antwort auf Frage 14 und 17; KOCHHEIM, S. 775.

314 Siehe vorstehend D.I.

V. In casu: Lokalisierung der Massnahmen

1. EncroChat

Bei der Lokalisierung der EncroChat-Überwachung ist auf den Datenverarbeitungsvorgang abzustellen. Die französischen Behörden spielten die Schadsoftware auf die einzelnen Endgeräte, was bewirkte, dass die Textnachrichten kopiert und die Kopien ausgeleitet wurden. Jede Nachrichtenausleitung stellt einen behördlich provozierten Datenverarbeitungsvorgang dar, weshalb die Massnahme am Ort des Endgerätes zu lokalisieren ist.

2. SkyECC

Bei der Lokalisierung der SkyECC-Überwachung ist der Zugriff auf die Inhaltsdaten von der Provokation der Zugangsdaten zu unterscheiden.

Die Erfassung der *Inhaltsdaten* erfolgte, indem die französischen Behörden die SkyECC-Server in Frankreich mit IP-Taps versahen. Diese Massnahme betraf die sich in Frankreich befindende Infrastruktur und erfolgte ohne Einwirkung auf die Endgeräte. Somit ist dieser Teil der Massnahme ausschliesslich in Frankreich zu verorten.

Anders ist hingegen die Provokation der Zugangsdaten zu lokalisieren. Die Zugangsdaten wurden erhältlich gemacht, indem ein von der Polizei in Frankreich eingerichteter MITM-Server die einzelnen Endgeräte kontaktierte. Die kontaktierten Endgeräte gaben infolgedessen das kryptographische Material preis. Die Preisgabe der kryptographischen Elemente stellt einen behördlich ausgelösten Datenverarbeitungsvorgang dar, weshalb die Massnahme am Ort des Endgerätes zu lokalisieren ist. Ohne Relevanz ist dabei, dass die SkyECC-Geräte möglicherweise mit einem französischen Netzwerk verbunden waren.

3. Anom

Die Anom-Geräte waren vom Betreiber (dem FBI) mit einer heimlichen Ausleitungsfunktion versehen. Da die heimliche Ausleitung technisch vorgesehen war, kam der Kommunikationsabgriff ohne Einwirkung auf das Endgerät aus. Folglich handelt es sich bei den Anom-Geräten um eine Überwachungsinfrastruktur, sodass die Lokalisierung anhand der Endgeräte vorzunehmen ist.[315]

[315] Vgl. in Bezug auf einen GPS-Tracker BGE 146 IV 36, insbes. E. 2.5.

E. Das Vertrauensprinzip

I. Die Bedeutung des Vertrauensprinzips

Bei der Beurteilung von Beweisen mit Auslandsbezug nimmt das Vertrauensprinzip eine zentrale Rolle ein. Das Vertrauensprinzip ist ein völkerrechtlicher Grundsatz, der insbesondere gegenüber Staaten mit «bewährter Rechtsstaatskultur» gilt.[316] Nach dem Vertrauensprinzip ist davon auszugehen, dass sich ein anderer Staat im Rechtsverkehr nach Treu und Glauben verhält.[317]

Um der Bedeutung des Vertrauensprinzips Konturen zu verleihen, ist es sinnvoll, das Vertrauensprinzip in das *tatsachenbezogene* und das *rechtsbezogene* Vertrauensprinzip zu unterteilen.[318] Das tatsachenbezogene Vertrauensprinzip besagt, dass – vorbehalten offenkundiger Unrichtigkeiten – die Richtigkeit der Sachverhaltsdarstellung eines anderen Staates zu vermuten ist.[319] Nach dem rechtsbezogenen Vertrauensprinzip wird die Rechtmässigkeit einer ausländischen Amtshandlung angenommen, sofern keine Anhaltspunkte einer Rechtswidrigkeit vorliegen.[320]

II. Das tatsachenbezogene Vertrauensprinzip

1. Funktion

Der herkömmliche Anwendungsbereich des Vertrauensprinzips ist die passive Rechtshilfe. Im Falle der passiven Rechtshilfe führt die Schweiz als ersuchter Staat die ersuchte Massnahme im Rahmen eines Rechtshilfeverfahrens durch. Das Rechtshilfeverfahren ist ein Verwaltungsverfahren, welches das ausländische Strafverfahren unterstützen soll.[321] Das Abstellen auf den vom ersuchenden Staat beschriebenen Sachverhalt soll verhindern, dass das Verwaltungsverfahren das Ergebnis des Strafverfahrens vorwegnimmt.[322] Ferner hat der

316 Vgl. BStGer RR.2023.47 vom 20. September 2023, E. 3.2.4.
317 Fiolka, S. 609.
318 Siehe nachfolgend II. und III.
319 Vgl. BGE 132 II 81, E. 2.1; BGer 2C_297/2017 vom 28. März 2017, E. 2.3; Fiolka, S. 606 f.
320 Vgl. Graf, Jusletter, S. 12; BGH, Beschl. v. 9.1.2025 – 1 StR 54/24, Rn. 29.
321 Fiolka, S. 608.
322 Fiolka, S. 609.

ersuchte Staat i.d.R. keinen engen Bezug zum Fall, sodass es sich aus praktischen Erwägungen anbietet, auf die Richtigkeit der ausländischen Sachverhaltsangaben zu vertrauen.[323]

2. Verfahrensmaximen im Rechtshilfe- und Strafverfahren

Das tatsachenbezogene Vertrauensprinzip stammt wie gesagt aus der (passiven) Rechtshilfe. Im Hinblick auf die Verfahrensgrundsätze bestehen allerdings erhebliche Unterschiede zwischen dem verwaltungsrechtlichen Rechtshilfeverfahren und dem strafprozessualen Strafverfahren.

Der *Untersuchungsgrundsatz* gilt zwar sowohl im Straf- als auch im Rechtshilfeverfahren (vgl. Art. 6 StPO und Art. 12 VwVG). In der Praxis besteht jedoch ein erheblicher Kontrast, inwiefern dieser zur Geltung kommt. Während es den Strafverfolgungsbehörden im Strafverfahren obliegt, sämtliche relevanten Umstände von Amtes wegen abzuklären (Art. 6 Abs. 1 StPO), wird in der passiven Rechtshilfe i.d.R. vorbehaltlos auf die Ausführungen des ersuchenden Staates abgestellt.[324] Besonders augenfällig wird dies in Bezug auf den dringenden Tatverdacht. In einem schweizerischen Strafverfahren haben die Strafverfolgungsbehörden bei Anordnung von eingriffsintensiven Zwangsmassnahmen den dringenden Tatverdacht durch konkrete Verdachtsmomente darzulegen.[325] Im Rechtshilfeverfahren hingegen wird die Intensität des Verdachts faktisch nicht überprüft.[326]

Zudem gilt im Strafverfahrensrecht die *Unschuldsvermutung* (Art. 32 Abs. 1 BV und Art. 10 StPO). Ein Aspekt dieser Vermutung ist die Beweislastregel, wonach es den Strafverfolgungsbehörden obliegt, den Schuldnachweis zu erbringen.[327] Daraus folgt, dass die vorgeworfenen Tatsachen nicht nur zu behaupten, sondern zu *beweisen* sind. Diese Beweislastregel gerät jedoch in Konflikt mit dem rechtshilferechtlichen Vertrauensprinzip, wonach die Richtigkeit lediglich *behaupteter* Tatsachen zu vermuten ist.[328] Diese Unterschiede in den

323 Fiolka, S. 610.

324 Vgl. Donatsch/Heimgartner/Simonek, S. 159.

325 Vgl. etwa Art. 269 Abs. 1 lit. a StPO.

326 Vgl. BSK IRSG-Heimgartner, N 39 zu Art. 64; CR IRSG-Ludwiczak Glassey, N 11 zu Art. 18a; namentlich die rechtshilfeweise Überwachung des Fernmeldeverkehrs nach Art. 18a IRSG bedürfte des dringenden Tatverdachts (Art. 18a Abs. 4 IRSG i.V.m. Art. 269 Abs. 1 lit. a StPO).

327 Statt vieler BGE 120 Ia 31, E. 2c.

328 Vgl. Fiolka, S. 616 f.

Verfahrensgrundsätzen zeigen auf, dass das tatsachenbezogene Vertrauensprinzip nicht ohne Weiteres in das Strafverfahren übertragbar ist.

3. Teilnahmerechte bei ausländischer Sachverhaltserstellung

Auch im Hinblick auf die strafprozessualen *Teilnahmerechte* kann das tatsachenbezogene Vertrauensprinzip nicht in das Strafverfahren übertragen werden. Dies zeigt sich namentlich anhand des Amtsberichtes gemäss Art. 195 StPO. Beabsichtigen Schweizer Behörden im Rahmen eines schweizerischen *Strafverfahrens*, bereits vorhandene Erkenntnisse einer ausländischen Behörde in Erfahrung zu bringen, so können sie bei dieser einen Amtsbericht (Art. 195 StPO) einholen. Ein derartiger Bericht hat allenfalls *Indizienwert*.[329] Sollen die Erkenntnisse der ausländischen Behörde in einem schweizerischen Strafverfahren hingegen rechtsgenügend erstellt werden, so kann dies durch eine Einvernahme des entsprechenden ausländischen Amtsträgers oder durch die Einholung eines Berichts i.S.v. Art. 145 StPO erfolgen. In beiden Fällen sind die (zeitversetzten) Teilnahmerechte der Parteien nach Art. 147 StPO zu wahren.[330] Demzufolge gilt, dass auch bei ausländischen Sachverhaltsdarstellungen die Teilnahmerechte zu wahren sind, welche durch das tatsachenbezogene Vertrauensprinzip unterlaufen würden.

4. Keine Übertragung des tatsachenbezogenen Vertrauensprinzips in das Strafverfahren

Die vorstehenden Ausführungen machen deutlich, dass das aus der (passiven) *Rechtshilfe* stammende tatsachenbezogene Vertrauensprinzip nicht vorbehaltlos in das schweizerische *Strafverfahrensrecht* integriert werden kann. Insbesondere ergibt sich aus den vorstehend beschriebenen Diskrepanzen hinsichtlich der Prozessmaximen und der Teilnahmerechte, dass das tatsachenbezogene Vertrauensprinzip den Sachverhalt nicht rechtsgenügend erstellen kann. Darüber hinaus ist es das Ziel des schweizerischen Strafverfahrens, den Sachverhalt verbindlich zu etablieren und gegebenenfalls den Strafanspruch durchzusetzen.[331] Da in einem schweizerischen Strafverfahren die vorgeworfene Handlung

329 BSK StPO I-Dzierzega-Zgraggen, N 3 zu Art. 195; PK StPO-Jositsch/Schmid, N 3 zu Art. 195.

330 Zum zeitversetzten Teilnahmerecht hinsichtlich des Berichts i.S.v. Art. 145 siehe SK StPO I-Godenzi, N 10 zu Art. 145; vgl. BSK StPO I-Häring, N 10 zu Art. 145.

331 Vgl. Donatsch/Heimgartner/Simonek, S. 25.

endgültig beurteilt wird, entfällt das Bedürfnis, eine Ergebnisvorwegnahme zu verhindern. Somit verliert das tatsachenbezogene Vertrauensprinzip seine Funktion in einem schweizerischen Strafverfahren.

III. Das rechtsbezogene Vertrauensprinzip

1. Vertrauensgrundlage als Voraussetzung

Nach dem rechtsbezogenen Vertrauensprinzip kann eine Schweizer Behörde vermuten, dass ausländische Rechtsakte nach ausländischem Recht rechtmässig erfolgten. Wird etwa im Ausland eine Kommunikationsüberwachung durchgeführt und gelangen deren Erkenntnisse später in ein schweizerisches Strafverfahren, so kann im Rahmen des schweizerischen Verfahrens vermutet werden, dass das ausländische Recht eingehalten wurde. Diese Vermutung beruht auf der Annahme, dass eine (ausländische) Behörde das eigene Recht besser auszulegen weiss als eine fremde (Schweizer) Behörde.[332] Dementsprechend soll das Vertrauensprinzip eine übergriffige und anmassende Rechtsanwendung durch einen fremden Staat unterbinden.[333]

Dieser Logik folgt auch die bundesgerichtliche Rechtsprechung, nach der bei Auslandsbeweisen das ausländische Recht zwar zu berücksichtigen ist, aber eine hiesige Behörde das ausländische Recht nicht eigenständig zu beurteilen hat.[334] Nach dem Bundesgericht kann eine hiesige Behörde zwecks Berücksichtigung des ausländischen Rechts einen *Bericht* bei der ausländischen Behörde einholen. Wird in diesem Bericht die Rechtmässigkeit gemäss ausländischem Recht bestätigt, so kann die Schweizer Behörde – vorbehalten gegenteiliger Anhaltspunkte – die ausländische Rechtmässigkeit vermuten.[335]

Diese Rechtsprechung konturiert die Voraussetzung des rechtsbezogenen Vertrauensprinzips. Das Vertrauen in die ausländische Rechtmässigkeit gilt nicht ohne Weiteres, sondern es bedarf einer konkreten ausländischen *Vertrauensgrundlage*.[336] Diese besteht nach dem Bundesgericht etwa aus einem

---

332 Graf, Jusletter, S. 13.

333 Vgl. Graf, Jusletter, S. 12.

334 Vgl. BGer 6B_1353/2023 vom 6. November 2024, E. 4.3.2.2 f.

335 BGer 6B_1353/2023 vom 6. November 2024, E. 4.3.2.3.

336 Vgl. auch TPF 2006 217, wonach der Nachweis der Rechtmässigkeit einer ausländischen Überwachung etwa durch die Kopie der Genehmigungsverfügung erbracht werden kann; ferner Graf, Verwertbarkeit, S. 536, wonach bei polizeirechtlichen Operationen eine Bestätigung über die Rechtmässigkeit bei der ausländischen Behörde einzuholen sei.

Bericht einer ausländischen Behörde.[337] Nach der hier vertretenen Auffassung kann darüber hinaus auch eine ausländische Verfügung[338] oder Rechtsprechung als Vertrauensgrundlage dienen. Voraussetzung dafür ist, dass diese Rechtsprechung oder Verfügung die Rechtmässigkeit des relevanten Vorganges nach ausländischem Recht hinreichend beurteilt.

2. Beschränkte Tragweite des Vertrauensprinzips

Im Kontext der Kryptophone-Verfahren messen Gerichte und Literatur dem Vertrauensprinzip teils eine uneingeschränkte Tragweite zu.[339] Aus dem Umstand, dass das Vertrauensprinzip eine Vertrauensgrundlage voraussetzt, ergibt sich allerdings eine inhaltliche Beschränkung. Eine ausländische Vertrauensgrundlage kann nur Auskunft über das ausländische Recht geben. Keine unmittelbare Wirkung hat die Vertrauensgrundlage hingegen hinsichtlich der Beurteilung nach schweizerischem Recht. Die Würdigung einer Beweiserhebung im Lichte des schweizerischen Rechts ist von einem Schweizer Gericht unabhängig von der Rechtsauffassung ausländischer Behörden vorzunehmen. Somit beschränkt sich das rechtsbezogene Vertrauensprinzip auf die Vermutung, dass die *innerstaatlichen Voraussetzungen* des beweiserhebenden Staates bei Anordnung, Genehmigung und Vollzug der Beweiserhebung vorlagen.[340]

3. Vertrauensprinzip und Beweiserhebungen in einem Drittstaat?

Im vorliegenden Kontext sind regelmässig Beweise zu beurteilen, die von einem anderen Staat in einem Drittstaat erhoben wurden. In diesem Fall gilt gleichermassen die Vermutung, dass der beweiserhebende Staat das *eigene* Recht eingehalten hat. Nicht umfasst vom Vertrauensprinzip ist die Vermutung, dass das Recht des *Drittstaates* eingehalten worden ist. Der beweiserhebende Staat hat kein Recht, das Recht eines Drittstaates anzuwenden. Die gegenteilige Auffassung führte in der Konsequenz dazu, dass das Recht des be-

337 Vgl. BGer 6B_1353/2023 vom 6. November 2024, E. 4.3.2.3.

338 Vgl. TPF 2006 217.

339 Vgl. OGer AG SST.2024.189 vom 23. Mai 2025, E. 2.7.3.1; BGH, Beschl. v. 9.1.2025 – 1 StR 54/24, Rn. 29 f.; Graf, Jusletter, S. 24.

340 Vgl. BGer 6B_1353/2023 vom 6. November 2024, E. 4.3.2.3, wonach «auf eine solche Erklärung […] für die Frage, ob die Massnahme nach *ausländischem Recht* zulässig war, grundsätzlich abgestellt werden [kann]»; ferner Sandner, S. 216 f.

troffenen Drittstaates übergangen würde, was wiederum einen Verstoss gegen das völkerrechtliche *Treu und Glauben* darstellte. Zudem widerspräche dies dem allgemeinen Rechtsprinzip *locus regit actum*, wonach der Ort eines Vorganges das einschlägige Recht bestimmt. Daraus folgt, dass eine Schweizer Behörde gehalten ist, Abklärungen hinsichtlich des einschlägigen drittstaatlichen Rechts zu treffen. Diesbezüglich bietet es sich an, dass die Schweizer Behörde Auskünfte bei einer Behörde des betroffenen Drittstaates einholt.

IV. Territorialitätsrechtliche Implikationen des Vertrauensprinzips?

Wie vorstehend dargelegt, darf das *tatsachenbezogene* Vertrauensprinzip den Untersuchungsgrundsatz in einem schweizerischen Strafverfahren nicht untergraben. Der Untersuchungsgrundsatz verpflichtet die Schweizer Behörden, alle bedeutsamen Tatsachen abzuklären (Art. 6 Abs. 1 StPO). Im grenzüberschreitenden, digitalen Kontext gehört zu diesen bedeutsamen Tatsachen insbesondere der Ort der Beweiserhebung.[341] Sofern eine Beweiserhebung in mehreren Staaten stattgefunden hat, sind sämtliche Erhebungsorte (und somit Jurisdiktionen) festzustellen.[342]

Liegen Anhaltspunkte vor, dass die Beweiserhebung in der Schweiz stattgefunden hat, so kann auch das *rechtsbezogene* Vertrauensprinzip hinsichtlich des schweizerischen (Territorialitäts-)Rechts keine Geltung beanspruchen. Wie vorstehend dargelegt, gilt das Vertrauensprinzip nur im Hinblick auf das Recht des beweiserhebenden Staates, nicht aber in Bezug auf das schweizerische Recht.[343] Die territoriale Integrität der Schweiz ist Teil der schweizerischen Rechtsordnung. Die Beurteilung des eigenen (schweizerischen) Territorialitätsrechts stellt somit keinen Akt der übergriffigen Rechtsanwendung fremden Rechts dar, sondern die Berücksichtigung eigenen Rechts. Dem Vertrauensprinzip ist folglich nicht zu entnehmen, dass eine ausländische Massnahme schweizerisches Territorialitätsrecht eingehalten hat.

Im Übrigen kann sich eine Pflicht, eine ausländische Beweiserhebung mit Bezug zur Schweiz umfassend zu prüfen, aus dem materiellen Recht ergeben. Eine unbewilligte Beweiserhebung einer ausländischen Behörde in der

341 BGE 146 IV 36, E. 2.5 «Faute de constatation claire à cet égard dans l'arrêt attaqué, la cause doit être renvoyée à l'autorité précédente pour qu'elle détermine les lieux d'enregistrement […]».

342 Vgl. BGE 146 IV 36, E. 2.5.

343 Siehe vorstehend E.III.2.

Schweiz kann nach Art. 271 StGB strafbar sein. Dieser Tatbestand ist ein Offizialdelikt und aufgrund des Verfolgungszwanges (Art. 7 Abs. 1 StPO) somit von Amtes wegen zu untersuchen.

Aus den vorstehenden Erwägungen ergibt sich, dass das Vertrauensprinzip die Strafverfolgungsbehörden nicht davon entbindet, den Ort der Beweiserhebung festzustellen und die Beweiserhebung gegebenenfalls im Lichte des schweizerischen Territorialitätsrechts zu würdigen.

V. Gültigkeit ausländischer Genehmigungen in der Schweiz?

Besonders eingriffsintensive Zwangsmassnahmen stehen im schweizerischen Recht unter dem Vorbehalt einer richterlichen Genehmigung.[344] Bei internationalen Massnahmen ist es möglich, dass eine Massnahme im Ausland richterlich genehmigt wurde. Dabei ist fraglich, ob die ausländische richterliche Genehmigung auch Geltung für die Schweiz beanspruchen kann. Mit anderen Worten ist zu prüfen, ob das Vertrauensprinzip bewirkt, dass eine ausländische richterliche Genehmigung eine schweizerische Genehmigung ersetzen kann.

Eine ausländische richterliche Genehmigung ist eine Vertrauensgrundlage, welcher zu entnehmen ist, dass die Massnahme dem ausländischen Recht entspricht. Keine Aussagekraft enthält eine ausländische Genehmigung hingegen hinsichtlich der Rechtskonformität nach schweizerischen Massstäben. Darüber hinaus kann eine richterliche Genehmigung aufgrund des Territorialitätsprinzips lediglich Geltung für das eigene Territorium beanspruchen.[345] Für eine Massnahme auf schweizerischem Territorium besteht eine exklusive Zuständigkeit Schweizer Behörden.[346] Diese exklusive Zuständigkeit spiegelt sich selbst im Rechtshilferecht – dem herkömmlichen Habitat des Vertrauensprinzips – wider. Im Rahmen der passiven Rechtshilfe kann lediglich ein Schweizer Zwangsmassnahmengericht eine genehmigungsbedürftige Überwachung in der Schweiz genehmigen (vgl. Art. 18a Abs. 3 IRSG).

Aus diesen Gründen kann eine ausländische Genehmigung – auch unter Geltung des Vertrauensprinzips – eine Genehmigung eines Schweizer Zwangsmassnahmengerichts nicht ersetzen.

344 Vgl. etwa Art. 226 und Art. 272 StPO.
345 Vgl. BGE 146 IV 36, E. 2.2.
346 CAPUS, S. 193.

VI. In casu: EncroChat, SkyECC, Anom und das Vertrauensprinzip

1. Ausländische Darstellungen als Arbeitshypothese

Die Darstellungen Schweizer Strafbehörden zur operativen und technischen Vorgehensweise stützten sich massgeblich auf ausländische Gerichtsentscheide, ausländische Behördenberichte und Medienmitteilungen. Derartigen Grundlagen kommt – analog zum Amtsbericht nach Art. 195 StPO – allenfalls Indizienwert zu.[347] Folglich sind die ausländischen Darstellungen über die Vorgehensweise lediglich *Arbeitshypothesen*, nicht aber rechtsgenügend erstellte Tatsachen. Dementsprechend gelten auch die in der vorliegenden Arbeit untersuchten Sachverhalte lediglich als Arbeitshypothese.

2. Vertrauen in EMRK-Konformität der Massnahmen?

Die EncroChat- und SkyECC-Überwachung wurde von den französischen Behörden – und somit von einem EMRK-Vertragsstaat – durchgeführt. Im Rechtsverkehr mit Frankreich greift unter den oben dargestellten Voraussetzungen das Vertrauensprinzip.

Gemäss Vertrauensprinzip ist zu vermuten, dass die französischen Behörden bei Anordnung, Genehmigung und Vollzug der Massnahme das interne Recht berücksichtigt haben. Die EMRK ist Teil des französischen Rechts, sodass grundsätzlich zu vermuten ist, dass die Massnahmen EMRK-konform (insbesondere Art. 6 und Art. 8 EMRK) erfolgten.

Nach der hier vertretenen Ansicht kann diese Vermutung der EMRK-Konformität jedoch nur für Vorgänge gelten, die in Frankreich stattgefunden haben. Ein Vorgang, der in der Schweiz zu verorten ist, ist vom Vertrauensprinzip ausgenommen. Dies ergibt sich aus Art. 1 EMRK. Diese Bestimmung verpflichtet jeweils den Vertragsstaat, allen Personen innerhalb *seiner* Hoheitsgewalt die Konventionsrechte zu garantieren. Dementsprechend sind die Schweizer Behörden Adressat der Konventionsrechte hinsichtlich der Rechtssubjekte in der Schweiz. Somit kommt den Schweizer Behörden die primäre Verantwortung zu, dass die Konventionsrechte eingehalten werden. Keinesfalls können

[347] Siehe vorstehend E.II.3.

sich Schweizer Behörden dieser Verantwortung mit dem Hinweis auf die (örtlich unzuständigen) französischen Behörden entledigen.

3. EncroChat

Die richterlichen Genehmigungen von EncroChat sind öffentlich im Internet in englischer Fassung abrufbar.[348] Bei diesen Dokumenten handelt es sich um nicht beglaubigte Übersetzungen, deren Ursprung unbekannt ist.[349] Sofern diesen Dokumenten eine hinreichende Authentizität beigemessen wird, läge eine Vertrauensgrundlage vor, sodass das rechtsbezogene Vertrauensprinzip zur Anwendung käme.[350] In diesem Falle wäre zu vermuten, dass die Massnahme nach französischem Recht rechtmässig ist.[351]

4. SkyECC

In den SkyECC-Verfahren sind die richterlichen Genehmigungen Teil der Akten.[352] Somit liegt eine hinreichende Vertrauensgrundlage vor, sodass das rechtsbezogene Vertrauensprinzip zur Anwendung gelangt. Folglich ist die Rechtmässigkeit nach französischem Recht zu vermuten.

5. Anom

a) Keine Anwendbarkeit des Vertrauensprinzips hinsichtlich des unbekannten Staates

Fraglich ist, gegenüber welchem Staat das Vertrauensprinzip bei der Anom-Operation potenziell Geltung beanspruchen kann. Die federführende Behörde hinter der Überwachung war das amerikanische FBI. Die Genehmigung erfolgte allerdings nicht in den USA, sondern in einem europäischen Drittstaat, der offiziell nie bekannt gegeben wurde (mutmasslich Litauen).[353]

---

348 Siehe Fn. 3.

349 Auch der BGH stellt auf die übersetzten Versionen der Genehmigungsbeschlüsse ab, siehe BGH, Beschl. v. 2.3.2022 – 5 StR 457/21, Rn. 11.

350 Siehe SANDNER, S. 216 ff., der darauf hinweist, dass zwar das nach französischem Recht erforderliche certificat de sincérité fehle, aber die höchstrichterliche französische Rechtsprechung keinen Nichtigkeitsmangel daraus erkenne, sodass das Vertrauensprinzip Geltung beanspruche.

351 Ähnlich hinsichtlich EncroChat BGH, Beschl. v. 2.3.2022 – 5 StR 457/21, Rn. 35.

352 Vgl. OGer ZH SB240422 vom 15. August 2025, E. II. 1 und III. 2.2.

353 Vgl. vorstehend A.III.5.

Wie dargelegt, bedarf das Vertrauensprinzip einer formalen Grundlage.[354] Eine derartige Grundlage kann namentlich eine richterliche Genehmigung darstellen, da diese die Rechtmässigkeit nach der einschlägigen Rechtsordnung bestätigt. Dementsprechend ist für die Geltung des Vertrauensprinzips primär an den Genehmigungsstaat anzuknüpfen. Der Genehmigungsstaat ist vorliegend jedoch unbekannt. Mangels Vertrauensgrundlage ist nicht bestimmbar, in wessen Recht und Institutionen vertraut werden soll, sodass das rechtsbezogene Vertrauensprinzip nicht zur Anwendung gelangt.

b) Keine Anwendbarkeit des rechtsbezogenen Vertrauensprinzips hinsichtlich der USA

Fraglich ist, ob das rechtsbezogene Vertrauensprinzip gegenüber den USA Geltung beanspruchen kann. Mangels amerikanischer richterlicher Genehmigung fällt eine Massnahmengenehmigung als Vertrauensgrundlage ausser Betracht. Sofern in der Praxis auf Unterlagen des DOJ verwiesen wird, könnten diese allenfalls als Vertrauensgrundlage gelten, sofern sie substanzielle Ausführungen zum amerikanischen Recht enthalten.[355]

Darüber hinaus sprechen die Umstände dafür, dass das interne US-Recht (*i.e.* 4th Amendment) eine Überwachung der amerikanischen Kommunikation nicht zugelassen hat. Zum einen war die vom US-Territorium ausgehende Kommunikation von der Überwachung ausgenommen.[356] Zum anderen wurden die Server in einem Drittstaat eingerichtet, wo auch die richterliche Genehmigung eingeholt wurde. Dieses Vorgehen der US-Behörden legt nahe, dass die rechtlichen innerstaatlichen Hindernisse umgangen werden sollten, was einem verpönten *forum shopping* entspräche.

Aufgrund der fehlenden richterlichen Genehmigung und des mutmasslichen *forum shopping* findet das rechtsbezogene Vertrauensprinzip gegenüber den USA keine Anwendung. Im Übrigen greift das Vertrauensprinzip nicht in Bezug auf extraterritoriale Massnahmen, da das Völkerrecht gebietet, das einschlägige Recht zu beachten (*locus regit actum*).[357] Folglich wären allfällig nach US-

354 Vgl. vorstehend E.III.1.

355 Vgl. etwa OGer AG SST.2024.189 vom 23. Mai 2025, E. 2.7.3.1. m.H.a. United States Attorney Office, Pressemitteilung v. 8.6.2021 (zum URL siehe Fn. 236), welche jedoch keine Ausführungen zum amerikanischen Recht enthält.

356 Vgl. OLG München, Beschl. v. 19.10.2023 – 1Ws 525/23, BeckRS 2023, 30017, Rn. 46; FINDER, Abschnitt «Inside Law Enforcement's Operational Methodology».

357 Siehe vorstehend E.III.3.

Recht rechtmässige Massnahmen ausserhalb des US-Territoriums nicht vom rechtsbezogenen Vertrauensprinzip umfasst.[358]

c) Folge: Fehlende Genehmigung und keine Rechtmässigkeitsvermutung

Die Nichtanwendbarkeit des rechtsbezogenen Vertrauensprinzips hat zweierlei Konsequenzen. In *formeller* Hinsicht ist die Genehmigung des unbekannten EU-Staates als inexistent zu erachten.

In *materieller* Hinsicht hätte ein Schweizer Gericht die Rechtmässigkeit nach dem einschlägigen ausländischen Recht zu prüfen. Demnach hätte ein Schweizer Gericht nach dem ausländischen Recht zu prüfen, ob die Massnahmenvoraussetzungen vorgelegen haben. Insbesondere wäre zu prüfen, ob eine Überwachung ohne richterliche Genehmigung nach dem einschlägigen (ausländischen) Recht zulässig ist. Vorliegend ist allerdings das einschlägige ausländische Recht (des unbekannten Genehmigungsstaates) nicht bestimmbar, oder es lässt derartige Massnahmen auf eigenem Staatsgebiet nicht zu (US-Recht). Im Ergebnis kann somit nicht die Vermutung gelten, dass die Anom-Überwachung nach ausländischem Recht zulässig war. Die sich nach dem US-Recht richtende Rechtmässigkeit der – nichtbewilligten – Überwachung wäre somit von den US-Behörden darzulegen.

358 Siehe vorstehend E.III.3.

F. Beurteilung von Auslandsbeweisen

I. Unterteilung von Auslandsbeweisen

Beweise, die von ausländischen Behörden erhoben werden, können einen unterschiedlich starken Bezug zur Schweiz aufweisen. Vor diesem Hintergrund ist es nach der hier vertretenen Ansicht sinnvoll, zwischen «reinen» und «gemischten» Auslandsbeweisen zu unterscheiden.

Ein reiner Auslandsbeweis liegt vor, wenn eine ausländische Behörde eine Beweiserhebung durchführt und die Beweiserhebung keinen Anknüpfungspunkt zur Schweiz aufweist. Ein gemischter Auslandsbeweis hingegen liegt vor, wenn eine ausländische Behörde eine Beweiserhebung vornimmt, die zumindest in Teilen in der Schweiz stattfindet.

II. Beurteilung von «reinen» Auslandsbeweisen

1. Zweistufige Bewertung

Die bisherige Streitfrage, nach welchem Recht Auslandsbeweise zu bewerten sind, bezieht sich implizit auf «reine» Auslandsbeweise. In der Literatur gab es verschiedene Ansichten, nach welchem Recht diese zu bewerten sind.[359] Das Bundesgericht hat dieser Frage nun erste Konturen verliehen.[360] Gemäss Bundesgericht befindet das in der Schuldfrage entscheidende Gericht nach den Vorgaben *seiner Rechtsordnung* über die Verwertbarkeit des Auslandsbeweises.[361] Dabei ist allerdings zu berücksichtigen, ob die Behörden des beweiserhebenden Staates bei der Beweiserhebung *ihr Recht* berücksichtigt haben.[362] Das Bundesgericht nimmt somit implizit die von RIEDI vorgeschlagene Differenzierung zwischen der Beurteilung eines *Verfahrensverstosses* und derjenigen der *Verwertbarkeit* auf.[363] Während sich der Verfahrensverstoss nach dem

359 WOHLERS, S. 297 bietet einen Überblick über die verschiedenen Auffassungen in der Literatur.

360 Vgl. BGer 6B_1353/2023 vom 6. November 2024.

361 BGer 6B_1353/2023 vom 6. November 2024, E. 4.3.2.1.

362 BGer 6B_1353/2023 vom 6. November 2024, E. 4.3.2.2; vgl. auch BGE 146 IV 36, E. 2.4 f.

363 Vgl. RIEDI, S. 112 ff.

lokal anwendbaren Recht (lex loci) beurteilt, richten sich dessen allfällige Verwertbarkeitsfolgen nach schweizerischem Recht (lex fori).[364]

2. Beurteilung des Verfahrensverstosses nach lex loci

Bei einem reinen Auslandsbeweis ist zunächst zu beurteilen, ob die Beweiserhebung nach dem Recht des beweiserhebenden Staates rechtmässig war.[365] Dies richtet sich nach ausländischem Recht, sodass eine Schweizer Behörde diesbezüglich einen Bericht bei der ausländischen Behörde einholen kann.[366] In Anwendung des Vertrauensprinzips kann in die Richtigkeit dieses Berichts vertraut werden. Lediglich bei berechtigten Zweifeln an der Richtigkeit des Berichts haben sich die Schweizer Behörden damit auseinanderzusetzen.[367]

3. Vorgehensweise bei Verfahrensverstoss nach lex loci

Liegt ein Verfahrensverstoss nach dem ausländischen Recht (lex loci) vor, bestimmen sich die Verwertbarkeitsfolgen nach schweizerischem Recht (lex fori).[368] Nach schweizerischer Rechtsauffassung folgt aus einem ausländischen Verfahrensverstoss ein Verwertbarkeitsverbot, sofern die Massnahme bei hypothetischer Durchführung in der Schweiz eine Norm des schweizerischen Rechts verletzen würde.[369] Diese Methode setzt jedoch voraus, dass die verletzte ausländische Norm im schweizerischen Recht ein Pendant hat.[370]

Fehlt es an einer äquivalenten Norm im schweizerischen Recht, so ist nach Riedi ein Verwertungsverbot anzunehmen, sofern die ausländische Norm *Individualinteressen* schützt und schwer verletzt wurde.[371] Dieser Auffassung ist zu folgen. Denkbar ist, dass eine ausländische Massnahme nicht im schweizerischen Strafprozessrecht vorgesehen ist und somit auch kein Pendant finden kann. Verletzen nun aber die ausländischen Behörden in grober Weise ihr ei-

364 Riedi, S. 157.

365 BGE 146 IV 36, E. 2.5. […] la cause doit être renvoyée à l'autorité précédente pour qu'elle détermine les *lieux d'enregistrement*, le *droit applicable en fonction du pays en cause* […].

366 BGer 6B_1353/2023 vom 6. November 2024, E. 4.3.2.3.

367 Vgl. BGer 6B_1353/2023 vom 6. November 2024, E. 4.3.2.3.

368 Vgl. Riedi, S. 157; vgl. BGer 6B_1353/2023 vom 6. November 2024, E. 4.3.2.1.

369 Vgl. Graf, Jusletter, S. 12.

370 Vgl. BGer 6B_1353/2023 vom 6. November 2024, E. 4.3.2.3 und 4.5., hinsichtlich einer ausländischen Überwachung, der es an der nach ausländischem Recht erforderlichen Bewilligung fehlte, woraus nach schweizerischem Recht die absolute Unverwertbarkeit gemäss Art. 277 StPO folgt; Riedi, S. 152.

371 Riedi, S. 156.

genes Recht, so sollte dies auch bei einer Verwertung in der Schweiz Berücksichtigung finden.

4. Vorgehen bei Rechtmässigkeit nach lex loci

a) Ordre public-Vorbehalt im Allgemeinen

Fraglich ist, wie eine nach ausländischem Recht rechtmässige Massnahme zu bewerten ist, die bei hypothetischer Durchführung in der Schweiz gegen hiesiges Verfahrensrecht verstossen hätte.[372] Nach einhelliger Ansicht in der Literatur folgt in diesem Fall ein Verwertbarkeitsverbot, sofern die ausländische Beweiserhebung gegen den schweizerischen *Ordre public* verstösst.[373] Zum Ordre public gehören fundamentale Institute einer Rechtsordnung.[374] Dazu zählen etwa das Verbot unmenschlicher Behandlung sowie wesentliche Verfahrensrechte wie die Belehrung über Auskunfts- und Aussageverweigerungsrechte.[375] Welche Rechtsinstitute darüber hinaus Teil des Ordre public sind, ist umstritten. Nach der hier vertretenen Auffassung setzt der Ordre public zumindest voraus, dass bei hypothetischer Durchführung der Massnahme in der Schweiz eine *absolute* Unverwertbarkeit folgte.

b) Beweisausforschungsverbot als Ordre public?

Die Literatur[376] und Teile der Praxis[377] zählen das Verbot der Beweisausforschung zum Ordre public. Nach der hier vertretenen Ansicht ist diese Einordnung jedoch unzutreffend.

Zum einen erachtet die bundesgerichtliche Rechtsprechung einen sog. Antennensuchlauf als zulässig.[378] Bei dieser Massnahme werden die Randdaten sämtlicher Nutzer, die in die betroffene Antennenzelle eingeloggt sind, erfasst.[379] Hinsichtlich des Verdachtserfordernisses genügt «die mögliche Individualisierbarkeit der Zielpersonen gemäss Raster- bzw. Schnittmengenergeb-

372 Graf, Jusletter, S. 13.
373 Vgl. BSK StPO I-Gless, N 32 zu Art. 141; Riedi, S. 140 f.; Graf, Jusletter, S. 13.
374 Popp, N 393.
375 Riedi, S. 167.
376 Vgl. Wohlers, S. 299; Graf, Jusletter, S. 18.
377 OGer ZH SB240422 vom 15. August 2025, E. IV. 1.3.2, wonach die SkyECC-Daten, die an französischen Servern abgegriffen worden sind, mangels Tatverdachts in der Schweiz unverwertbar sind.
378 BGE 137 IV 340, E. 5 f.
379 Vgl. BGE 137 IV 340, E. 5.4.

nis».[380] Bei Anordnung dieser Massnahme kann die Täterschaft noch gänzlich unbekannt sein. Somit wird der Tatverdacht gegen eine Person erst durch die Massnahme generiert. Dementsprechend wird diese Massnahme auch als «verdachtsbegründende» Ermittlungsmethode bewertet[381] und teils einer Beweisausforschung gleichgestellt.[382] Zum anderen führt eine verdachtsunabhängige strafprozessuale Massnahme nicht zur absoluten, sondern lediglich zur relativen Unverwertbarkeit i.S.v. Art. 141 Abs. 2 StPO.[383] Dementsprechend wird bei einem überwiegenden Verfolgungsinteresse ein Verstoss gegen das Verbot der Beweisausforschung toleriert.[384] Nach der hier vertretenen Auffassung ist es allerdings ein Charakteristikum des Ordre public, dass dessen hypothetische Verletzung in der Schweiz unter keinen Umständen zu einem verwertbaren Beweis führen darf.[385] Letztlich erlaubt auch das präventive Polizeirecht verdachtsunabhängige Massnahmen. Wäre die Verdachtsabhängigkeit Teil des Ordre public, so liessen sich präventiv-polizeilich erhobene Informationen unter keinen Umständen strafprozessual verwerten.[386] Dies entspricht allerdings nicht der allgemeinen Praxis, wonach rechtmässig gesammelte Informationen in einem späteren Strafverfahren als Beweise verwertbar sind. Aus den vorstehenden Gründen ist die Verdachtsabhängigkeit einer Massnahme nicht Teil des schweizerischen Ordre public.

c) Territorialitätsprinzip als Ordre public?

Die Rechtsprechung misst dem Territorialitätsprinzip grosse Bedeutung zu. Gemäss Bundesgericht kommt eine Territorialitätsverletzung «einer Verletzung des internationalen öffentlichen Rechts» gleich.[387] Folglich sind Beweise, die unter Verletzung (fremder) Territorialität erhoben wurden, absolut unverwertbar.[388]

380 BGE 137 IV 340, E. 5.6.

381 Biaggini, N 178.

382 Vgl. Jeker/Roos, S. 179 f.

383 BGer 6B_821/2021 vom 6. September 2023 (=BGE 149 IV 369), E. 1.4.2. und 1.5; a.A. BSK StPO I-Gless, N 81 zu Art. 141.

384 Das überwiegende Verfolgungsinteresse setzt eine schwere Straftat voraus, vgl. Art. 141 Abs. 2 StPO.

385 Siehe vorstehend F.II.4.a).

386 Vgl. BSK StPO II-Galella/Rhyner, N 8 zu Art. 306.

387 BGer 7B_120/2022 vom 5. Oktober 2023, E. 2.4.2.1.

388 Vgl. BGE 146 IV 36, E. 2.3; bestätigt in BGer 7B_120/2022 vom 5. Oktober 2023, E. 2.4.2.1; ebenso BGer 7B_273/2023 et al. vom 11. April 2024, E. 3.3; Riedo/Fiolka/Niggli, N 3204 ff., wonach Beweiserhebungen im Ausland treuwidrig sein können.

Diese Erwägungen legen nahe, die Achtung des Territorialitätsprinzips im Ordre public einzuordnen.[389]

Nach der hier vertretenen Auffassung setzt der Vorbehalt des Ordre public allerdings voraus, dass eine Beweiserhebung vorliegt, die keinen territorialen Anknüpfungspunkt zur Schweiz aufweist (sog. «reiner Auslandsbeweis»). Der Vorbehalt des Ordre public ist eine analoge Anwendung schweizerischen Rechts auf einen ausländischen Sachverhalt. Sobald eine Beweiserhebung zumindest teilweise in der Schweiz zu verorten ist, kommt das schweizerische Recht nicht analog, sondern unmittelbar und umfassend zur Geltung.[390]

Im Falle eines Territorialitätseingriffes ist die ausländische Massnahme notwendigerweise in der Schweiz zu verorten. In diesem Fall gelangt zwingend das schweizerische Territorialitätsrecht direkt und umfassend zur Anwendung, sodass dieses nicht als Ordre public zu bezeichnen ist.

III. Beurteilung von «gemischten» Auslandsbeweisen

Ein gemischter Auslandsbeweis liegt vor, wenn eine ausländische Behörde eine Beweiserhebung vornimmt, die zumindest in Teilen in der Schweiz stattfindet. Gemäss dem allgemeinen Rechtsgrundsatz *locus regit actum* ist in diesem Fall jene Rechtsordnung massgebend, in welcher sich der rechtserhebliche Vorgang verwirklicht hat.[391] Dieser Grundsatz spiegelt sich ausnahmslos im internationalen polizeilichen Amtshilferecht wider. In engen staatsvertraglichen Grenzen kann es der Polizei gestattet sein, eine polizeiliche Massnahme auf nachbarstaatlichem Territorium fortzuführen. Allerdings haben die Beamten auch in diesem Fall das Recht des Territorialstaates einzuhalten.[392]

Auch das internationale Rechtshilferecht ist von dem Grundsatz locus regit actum geprägt. Nimmt die Schweiz rechtshilfeweise eine Beweiserhebung in der Schweiz vor, so ist das schweizerische Recht massgebend (vgl. Art. 63 Abs. 1 IRSG). Ausnahmsweise kann ausländisches Recht akzessorisch beachtet werden, um ausländische Verfahrens- oder Formvorschriften zu wahren (vgl.

389 Vgl. OK CCC-Graf, N 70 zu Art. 32, wonach eine Qualifizierung des Territorialitätsprinzips als Ordre public abzulehnen ist; ferner Wildhaber, S. 103.

390 Siehe nachstehend F.III.

391 Piotet, S. 165.

392 Vgl. Art. 40 Ziff. 3 lit. a SDÜ; Art. 41 Ziff. 5 lit. a SDÜ; ferner Art. 14 Ziff. 3 Nr. 1, 2 und 8 Schweizerisch-deutscher Polizeivertrag.

Art. 8 ZP II EUeR und Art. 65 Abs. 1 und 2 IRSG).[393] Erfolgt nun eine Beweiserhebung ausserhalb der Rechtshilfe, so gilt der Grundsatz locus regit actum ausnahmslos. In Bezug auf einen gemischten Auslandsbeweis richtet sich somit der Teil der Beweiserhebung, der in der Schweiz stattfindet, nach schweizerischem Recht. Abhängig davon, ob ein Tatverdacht vorliegt, gelangt das Strafprozessrecht oder das Polizeirecht des betroffenen Kantons zur Anwendung.[394]

IV. EncroChat, SkyECC und Anom als «gemischte» Auslandsbeweise

Die vorstehende Unterscheidung zwischen «reinen» und «gemischten» Auslandsbeweisen lässt sich anhand der *SkyECC*-Überwachung illustrieren. Der Abgriff der *Inhaltsdaten* fand an den Servern in Frankreich statt, weshalb es sich um einen «reinen» Auslandsbeweis handelt. Dieser Abgriff ist nach französischem Recht zu bewerten, wobei aufgrund des Vertrauensprinzips die Rechtmässigkeit dieser Massnahme zu vermuten ist. Allein der Vorbehalt des Ordre public könnte diesbezüglich ein Verwertbarkeitshindernis darstellen. Anders hingegen ist die Provokation der *Zugangsdaten* zu bewerten. Diese fand in den einzelnen Endgeräten statt, sodass dieser Teil der Massnahme in der Schweiz zu verorten ist. Somit handelt es sich um einen gemischten Auslandsbeweis, der sich nach schweizerischem Recht richtet.

Die *EncroChat*– und *Anom*-Beweise können hingegen ohne Weiteres als «gemischte» Auslandsbeweise bezeichnet werden, da die Inhaltsdaten in den Endgeräten ausgeleitet wurden und die Massnahme insofern in der Schweiz zu verorten ist. Dementsprechend sind auch diese Beweiserhebungen nach schweizerischem Recht zu beurteilen.

393 Vgl. BGE 131 II 132, E. 2.2, wonach Art. 65 IRSG keine Grundlage darstellt, Massnahmen durchzuführen, die dem schweizerischen Recht unbekannt sind.

394 Vgl. Graf, Verwertbarkeit, S. 536 f.

G. Die Massnahmen im Lichte des Verdachtskriteriums

I. Der Tatverdacht als Abgrenzungskriterium

Wie vorstehend dargelegt, sind Beweiserhebungen, die in der Schweiz zu lokalisieren sind, stets im Lichte des schweizerischen Rechts zu würdigen. Im schweizerischen Recht können grundrechtsinvasive Massnahmen namentlich auf das präventive kantonale Polizeirecht oder auf das repressive Strafverfahrensrecht der StPO gestützt werden. Die Abgrenzung, ob das kantonale Polizeirecht oder das bundesrechtliche Strafverfahrensrecht anwendbar ist, erfolgt anhand des Verdachtskriteriums.[395] Während eine polizeirechtliche Massnahme ohne Tatverdacht auskommt, bedarf eine strafprozessuale Massnahme eines solchen.[396]

II. Das Verdachtserfordernis im Strafprozessrecht

Das Vorliegen eines Tatverdachts stellt aus strafprozessualer Optik eine Legitimationsgrundlage für einen Grundrechtseingriff dar.[397] Das verdachtsbezogene Handeln ist Ausdruck des rechtsstaatlichen Verhältnismässigkeitsprinzips und somit ein rechtsstaatliches Erfordernis nach Art. 36 BV.[398] Nach dem Verhältnismässigkeitsprinzip steigen die Anforderungen an den Verdachtsgrad mit der Schwere des Grundrechtseingriffs.[399] Neben dem materiellen Gehalt der Verhältnismässigkeit hat der Tatverdacht eine formell-rechtliche Komponente. Diese zeigt sich darin, dass der vorgeworfene Sachverhalt als Arbeitshypothese so zu formulieren ist, dass eine vorläufige Subsumtion möglich ist.[400] Dies setzt die betroffene Person darüber in Kenntnis, was ihr vorgeworfen wird.[401] Infolgedessen ist sie in der Lage, das staatliche Handeln zu kontrollieren und allenfalls anzufechten.[402]

---

395 BSK StPO II-Weber, N 6a zu Art. 197.

396 Vgl. BGE 140 I 353, E. 8.8.

397 Pieth/Geth, S. 142.

398 Ackermann, S. 322.

399 Vgl. Ackermann, S. 331.

400 Ackermann, S. 334; ferner BGer 1B_516/2011 vom 17. November 2011, E. 2.1.

401 Ackermann, S. 334.

402 Ackermann, S. 334.

1. Der Begriff des Tatverdachts

a) Dreigliedriger Begriff

Eine begriffsscharfe Definition des Verdachtskriteriums fällt schwer. Mit einem Teil der Literatur wird vorliegend auf einen dreigliedrigen Verdachtsbegriff abgestellt.[403] Demnach liegt ein Verdacht vor, wenn

- konkrete Tatsachen
- aufgrund besonderer Kenntnisse oder Erfahrungen
- zum Schluss führen, dass ein strafbares Verhalten vorliegt.[404]

b) Konkrete Tatsachen

Der Ausgangspunkt der Verdachtsbegründung ist das Vorliegen von Tatsachen. Diese bestehen aus einem tatsächlich wahrgenommenen Lebensvorgang bzw. Zustand der Gegenwart oder Vergangenheit.[405] Die Tatsachen müssen ausser Zweifel stehen[406]; reine Mutmassungen, Gerüchte und generelle Vermutungen sind nicht verdachtsbegründend.[407]

c) Erfahrungssatz

Mithilfe des Erfahrungssatzes lässt sich anhand eines unvollständigen Geschehensablaufs auf einen vollständigen Sachverhalt schliessen.[408] Dies setzt voraus, dass die bereits feststehenden Tatsachen tatbezogen sind und sich nicht in personenbezogenen Tatsachen erschöpfen.[409] Die Schlussfolgerung von den bekannten Tatsachen auf den gesamten Sachverhalt muss nachvollziehbar und plausibel sein.[410]

403 Vgl. HÜRLIMANN, S. 96 ff.; ACKERMANN, S. 325; ähnlich WALDER ET AL., S. 135.
404 ACKERMANN, S. 325.
405 HÜRLIMANN, S. 97.
406 HÜRLIMANN, S. 97.
407 BGer 1B_516/2011 vom 17. November 2011, E. 2.1.
408 HÜRLIMANN, S. 97 f.
409 ACKERMANN, S. 332 f.
410 Vgl. HÜRLIMANN, S. 98.

d) Tatbestandsmässigkeit als Bezugspunkt

Bezugspunkt für den Tatverdacht ist stets das materielle Strafrecht.[411] Die Tatsachen in Verbindung mit dem Erfahrungssatz müssen ein *tatbestandsmässiges* Verhalten ergeben. Solange das Verhalten straflos ist – auch bei sozialer Anrüchigkeit – kann ein Verdacht gar nicht erst entstehen.[412]

2. Die Abstufungen des Tatverdachts

a) Der Verdacht als dynamisches Kriterium

Das Strafverfahrensrecht knüpft an unterschiedliche Verdachtsgrade an. Dabei wird der Verdachtsgrad dynamisch ausgelegt. Die Intensität des erforderlichen Verdachts hängt neben der gesetzlichen Vorgabe von der Art und Dauer der Zwangsmassnahme sowie dem Verfahrensstadium ab.[413]

b) Anfangsverdacht

Die Strafverfolgung setzt voraus, dass zumindest ein Anfangsverdacht vorliegt.[414] Ein Anfangsverdacht liegt bereits vor, wenn eine *geringe* Wahrscheinlichkeit für die Tatbeteiligung des Beschuldigten vorliegt.[415] Der Tatvorwurf muss zu Beginn der Untersuchung lediglich glaubhaft sein[416], aber auf einer plausiblen Tatsachengrundlage beruhen[417] und objektiv begründbar sein.[418]

c) Hinreichender Tatverdacht

Nach der Konzeption des schweizerischen Rechts sind Zwangsmassnahmen zulässig, sofern ein hinreichender Tatverdacht vorliegt (Art. 197 Abs. 1 lit. b StPO). Ein hinreichender Tatverdacht besteht, wenn eine *gewisse Wahrscheinlichkeit* für die Verurteilung des Beschuldigten vorliegt.[419]

---

411 Walder et al., S. 135 f.
412 Walder et al., S. 135 f.; Ackermann, S. 327.
413 BSK StPO II-Weber, N 8a zu Art. 197.
414 Vgl. Pieth/Geth, S. 239; BSK StPO II-Riedo/Boner, N 4 zu Art. 300.
415 Hürlimann, S. 104.
416 BSK StPO II-Vogelsang, N 30 zu Art. 309.
417 Vgl. BGer 6B_335/2020 vom 7. September 2020, E. 3.3.4.
418 BSK StPO II-Vogelsang, N 32 zu Art. 309.
419 Vgl. BStGer BV.2009.16 vom 14. Juli 2009, E. 2.2 e contrario.

d) Dringender Tatverdacht

Besonders eingriffsintensive Massnahmen bedürfen in der Regel eines dringenden Tatverdachts. Ein dringender Tatverdacht liegt vor, wenn eine *erhebliche Wahrscheinlichkeit* für die Tatbeteiligung des Beschuldigten vorliegt.[420]

3. Zufallsfund und fishing expedition

Das Vorliegen eines Tatverdachts ist die Legitimation einer strafprozessualen Zwangsmassnahme.[421] Dementsprechend kann sich eine Zwangsmassnahme nur auf einen *vorbestehenden* Tatverdacht stützen.[422] Dieser Grundsatz findet mit der Regelung des Zufallsfundes seine Ausnahme. Ein Zufallsfund liegt vor, wenn die Behörden bei der Durchführung einer rechtmässigen (verdachtsabhängigen) Massnahme konkrete Anhaltspunkte für eine andere Straftat (oder anderen Beschuldigten) finden. Die zufällig gefundenen Anhaltspunkte sind verwertbar, sofern die Massnahme zur Verfolgung des neu im Raum stehenden Deliktes (oder des neu Beschuldigten) hätte angeordnet werden dürfen.[423]

Abzugrenzen ist der Zufallsfund von der unzulässigen Beweisausforschung, der sog. *fishing expedition*. Während ein Zufallsfund einer verdachtsabhängigen Primärmassnahme bedarf[424], erfolgt eine fishing expedition gänzlich ohne vorbestehenden Verdacht[425]. Eine fishing expedition dient geradezu der Verdachtsbegründung, indem der Staat «ohne Verdacht seine Netze auslegt, um Anhaltspunkte erst einzufangen».[426]

4. Exkurs: Verwertbarkeitsfolgen des fehlenden Tatverdachts

In der vorliegenden Arbeit kommt dem Verdachtskriterium primär eine Zuordnungsfunktion zu. Anhand des Verdachtskriteriums wird bestimmt, ob die Massnahmen einen präventiv-sicherheitsrechtlichen oder repressiv-strafpro-

420 Vgl. BGer 1B_412/2016 vom 5. Dezember 2016, E. 3.2.
421 Pieth/Geth, S. 142.
422 BSK StPO II-Gfeller/Thormann, N 3 zu Art. 243.
423 Diese Regelung ist ausdrücklich vorgesehen im Bereich der Überwachungsmassnahmen (Art. 278 StPO) und der verdeckten Ermittlung (Art. 296 StPO), gilt aber bei sämtlichen Zufallsfunden, siehe dazu CR StPO-Hohl-Chirazi, N 8 ff. zu Art. 243.
424 Hürlimann, S. 109 f.
425 Vgl. CR StPO-Hohl-Chirazi, N 3a zu Art. 243.
426 Ackermann/Vogler, S. 164.

zessualen Charakter haben. Da es sich bei den Massnahmen – wie noch zu zeigen bleibt – nicht um rein strafprozessuale Massnahmen handelt, dient das Verdachtskriterium vorliegend nicht unmittelbar der Verwertbarkeitsbeurteilung. Dementsprechend sei die strafprozessuale Folge des fehlenden Tatverdachts nur kurz erwähnt. Während sich ein Teil der Literatur im Falle einer Beweisausforschung für ein absolutes Verwertbarkeitsverbot ausspricht[427], löst nach Ansicht des Bundesgerichts eine verdachtslose Beweiserhebung ein *relatives* Verwertbarkeitsverbot aus.[428]

III. In casu: Verdachtsbeurteilung

1. Verdacht auf kriminelle Organisation und Betäubungsmitteldelikte?

Ein Tatverdacht hat sich stets auf einen Tatbestand zu beziehen. Die vorliegenden Überwachungsmassnahmen basieren i.d.R. auf dem Vorwurf der Beteiligung an einer kriminellen Organisation und/oder der Betäubungsmitteldelikte. Diese Delikte weisen – zumindest im schweizerischen Recht – eine sehr weitgehende Strafbarkeit auf. Für die Beteiligung an einer kriminellen Organisation (Art. 260ter StGB) genügt bereits jeder bewusste legale oder illegale Beitrag zur Stärkung der Organisation.[429] Nicht erforderlich ist, dass der Täter der Organisation angehört.[430] Im Betäubungsmittelrecht ist bereits das «Anstalten treffen» zu Besitzes- oder Vermittlungshandlungen unter Strafe gestellt (Art. 19 Abs. 1 lit. g BetmG). Allerdings setzt diese Tatbestandsvariante voraus, dass die fragliche Tätigkeit nicht ebenso gut einem legalen Zweck dienen könnte. Nach dem äusseren Erscheinungsbild muss die Tätigkeit klar die deliktische Bestimmung erkennen lassen.[431]

427 Vgl. BSK StPO II-Gfeller, N 47 zu Vor Art. 241-254; BSK StPO I-Gless, N 81 zu Art. 141; a.A. CR StPO-Hohl-Chirazi, N 9 zu Art. 243.

428 BGer 6B_821/2021 vom 6. September 2023 (=BGE 149 IV 369), E. 1.4.2. und 1.5; BGer 6B_628/2013 vom 26. Juni 2014, E. 1.4.1 f.

429 KommKV/KO II-Pajarola/Oehen/Thommen, N 488 zu Art. 260ter StGB.

430 KommKV/KO II-Pajarola/Oehen/Thommen, N 426 zu Art. 260ter StGB.

431 BGer 6B_273/2013 vom 4. November 2013, E. 2.2.

2. Vorliegende Tatsachen?

Die vorliegenden Überwachungsmassnahmen wurden gegen tausende unbekannte Kryptophone-Nutzer durchgeführt. Als verdachtsbegründende Tatsache kann gegen die Nutzer von *EncroChat* und *SkyECC* lediglich aufgeführt werden, dass sie den entsprechenden Messenger-Dienst nutzten. Demgegenüber waren bei Einleitung der *Anom*-Überwachung die späteren Anom-Nutzer noch gar nicht in Besitz der Anom-Geräte, da diese erst vom FBI in den Umlauf gebracht werden mussten. Folglich waren die späteren Anom-Nutzer selbst theoretisch noch nicht bestimmbar. Somit lassen sich bei Anom keine Tatsachen beschreiben, die für eine Verdachtsbegründung nutzbar gemacht werden können.

3. Schluss auf strafbares Verhalten?

a) Kein Rückschluss anhand der Sicherheitsarchitektur

Der Verdacht gegen die Kryptophone-Nutzer wird teils mit der Sicherheitsarchitektur der Endgeräte begründet.[432] Demnach deuteten die zahlreichen Vertraulichkeitsfunktionen, wie die End-to-End-Verschlüsselung, der verdeckte Appzugang und die selbstlöschenden Nachrichten auf eine kriminalitätsbezogene Nutzung hin.[433]

Allerdings sind End-to-End-Verschlüsselungen heute auch bei herkömmlichen Messenger-Diensten verbreitet.[434] Ebenso sind selbstlöschende Nachrichten – etwa bei Signal – nicht unüblich.[435] Darüber hinaus gibt es Anbieter, die äusserst sichere Mobiltelefone anbieten. Namentlich preisen diese Hardware-Modifizierungen (z. B. Entfernung der Kamera) und besondere Software-Funktionen (z. B. Preisgabe eines Scheindatensatzes im Falle der Kompromittierung) an.[436] Dementsprechend ist eine Abgrenzung zwischen «verdächtigen» und «unverdäch-

---

432 Vgl. Graf, Jusletter, S. 16 f.

433 Vgl. Graf, Jusletter, S. 16 f.; ferner OGer AG SST.2024.189 vom 23. Mai 2025, E. 2.7.3.2.

434 Die Kommunikation von WhatsApp und Signal ist auf diese Weise verschlüsselt, siehe WhatsApp-Website <https://faq.whatsapp.com/820124435853543#> und Signal-Website <https://support.signal.org/hc/en-us/articles/360007320391-Is-it-private-Can-I-trust-it#:~:text=Signal conversations are always end,the way that Signal works>.

435 Siehe zu Signal <https://support.signal.org/hc/en-us/articles/360007320771-Set-and-manage-disappearing-messages>; zu WhatsApp <https://faq.whatsapp.com/673193694148537/?locale=de_DE>.

436 Vgl. u.a. das Armadillo-phone <https://www.armadillophone.com/#hardware>.

tigen» Kommunikationsmitteln anhand der Funktionen schlichtweg unmöglich. Richtigerweise lassen derartige Vertraulichkeitsfunktionen allein den Schluss zu, dass der Nutzer Wert auf eine vertrauliche Kommunikation legt.

b) Kein Rückschluss anhand der Vertriebsumstände

Teilweise wird der Rückschluss auf ein strafbares Verhalten mit den Vertriebs- und Verkaufsumständen der Kryptophones begründet.[437] Auffällig sei, dass die Endgeräte nicht in allgemein zugänglichen Erwerbsmöglichkeiten erhältlich seien, der Erwerb anonym erfolge und üblicherweise mit Bargeld oder Kryptowährung bezahlt werde.[438]

Diese Kriterien sind jedoch ungeeignet, die fraglichen Kryptophones von «unverdächtigen» Kommunikationsgeräten abzugrenzen. Zum einen waren etwa die EncroPhones auch auf allgemein zugänglichen Vertriebswegen – etwa eBay – erhältlich.[439] Darüber hinaus sind auch im öffentlich zugänglichen Handel erhältliche Kommunikationsgeräte über Kryptowährungen wie Bitcoin oder Monero bezahlbar.[440] Die Vertriebsumstände lassen somit allein den Schluss zu, dass die Käufer Wert auf Anonymität gelegt haben. Ein objektiv beschreibbarer Tatverdacht lässt sich hingegen aus diesen nicht ableiten.[441]

c) Kein Rückschluss anhand der Hersteller und Vertreiber

Weiter wird als Verdachtsbegründung vorgebracht, dass die Hersteller und Verkäufer der Kryptophones dem kriminellen Umfeld entstammen.[442] Es ist völlig offenkundig, dass eine derartige Verdachtsbegründung in einem Schuldstrafrecht einen Tatverdacht nicht im Ansatz zu begründen vermag. Es ist nicht nachvollziehbar, wie aus einem völlig legalen Rechtsgeschäft ein angeblich krimineller Hintergrund des (nicht bestimmbaren) Geschäftspartners begründet werden kann. Eine derart konstruierte Kontaktschuld ist geradezu Ausdruck dessen, dass gegen die konkrete Person keine Verdachtsmomente vorliegen.

---

437 Graf, Jusletter, S. 16 f.; ferner BGH, Beschl. v. 9.1.2025 – 1 StR 54/24, Rn. 33.

438 Vgl. BGH, Beschl. v. 9.1.2025 – 1 StR 54/24, Rn. 33; OGer AG SST.2024.189 vom 23. Mai 2025, E. 2.7.2 und 2.7.3.2.

439 BGH, Beschl. v. 2.3.2022 – 5 StR 457/21, Rn. 10.

440 Vgl. etwa die Zahlungsmodalitäten von Armadillo <https://www.armadillophone.com/store>.

441 Im schweizerischen Recht macht sich lediglich der Fernmeldeanbieter oder professionelle Wiederverkäufer strafbar, wenn er es unterlässt, die Kundendaten zu erfassen (Art. 39 Abs. 1 lit. c BÜPF).

442 Vgl. Graf, Jusletter, S. 16 f.; ferner OGer AG SST.2024.189 vom 23. Mai 2025, E. 2.7.3.2.

d) Kein Rückschluss anhand der angeblichen Nutzung

Weiter wird der Verdacht teils damit begründet, dass die allgemeine Kommunikation der vorliegenden Dienste nahezu ausschliesslich kriminalitätsbezogenen Inhalt aufgewiesen habe. Diese These wird teils mit quantitativen Annahmen untermauert.[443]

Ein Verdacht muss sich stets auf eine spezifische Tat richten. Eine angeblich allgemeine kriminalitätsbezogene Nutzung eines Messenger-Dienstes vermag mitnichten einen individualisierten, deliktsspezifischen Verdacht zu begründen. Im Übrigen sind die quantitativen Hypothesen weder qualitativ (nach Deliktarten) noch quantitativ (nach Deliktsprävalenz) überprüfbar und somit auch nicht widerlegbar. Es ist aber davon auszugehen, dass derartige Hypothesen auf der Auswertung einzelner weniger Geräte beruhen[444], sodass ein Schluss auf eine allgemeine, internationale Nutzung nicht möglich ist.

e) Zwischenfazit: Kein Tatverdacht

Das Vorstehende lässt sich zusammenfassen und würdigen. Hinsichtlich der *Anom*-Überwachung fehlt es bereits an tauglichen verdachtsbegründenden Tatsachen, da die betroffenen Personen bei Massnahmeneinleitung noch nicht in Besitz des Gerätes und somit nicht bestimmbar waren. Eine Formulierung eines Tatverdachtes fällt somit aus.

Hinsichtlich *EncroChat* und *SkyECC* wird als verdachtsbegründende Tatsache auf die Charakteristika (Sicherheitsarchitektur, Vertriebsumstände, Nutzungshypothesen) des genutzten Messenger-Dienstes verwiesen. Allerdings lässt sich aus diesen angeblich verdachtsbegründenden Tatsachen kein Tatverdacht herleiten.[445] Aus den Tatsachen lässt sich allein der Schluss ableiten, dass die Nutzer einen hohen Wert auf vertrauliche Kommunikation und auf einen anonymen Erwerb der Geräte legten.

Der fehlende Tatverdacht zeigt sich nicht zuletzt daran, dass das fragliche Delikt nach Art, Ort oder Zeit unbestimmbar ist. Dies ist keine ungenügende,

---

443 Vgl. hinsichtlich *EncroChat* etwa BGH, Beschl. v. 2.3.2022 – 5 StR 457/21, Rn. 11, wo auf die 3'477 ausgewerteten Notizen abgestellt wird; hinsichtlich *Anom* siehe MROKON, S. 228 f.

444 Hinsichtlich *EncroChat* verweist etwa der BGH darauf, dass vor der Echtzeitüberwachung 3'477 Notizen ausgewertet wurden. Diese entstammen jedoch vermutlich drei Geräten, siehe dazu vorstehend A.I.4. Bei *SkyECC* wird teils von einer kriminalitätsbezogenen Quote von 99.9 % ausgegangen, vgl. GRAF, Jusletter, S. 16. Hinsichtlich *Anom* wird teils auf die Testphase in Australien mit etwa 50 Geräten verwiesen, siehe MROKON, S. 228 f.

445 Vgl. auch GLESS, ZStrR, S. 99 f.

sondern eine inexistente Verdachtsbegründung. Eine derartig substanzlose Verdachtshypothese höhlt die Beschuldigtenrechte völlig aus. Dem Beschuldigten wird die Möglichkeit genommen, den vorläufigen Tatvorwurf – etwa durch ein Alibi – zu entkräften. Gleichzeitig wird es dem Beschuldigten dadurch verunmöglicht, die Massnahme sinnvoll – etwa im Hinblick auf die Verhältnismässigkeit – zu kontrollieren und anzufechten.[446]

Das Vorstehende lässt sich anhand des folgenden fiktiven Sachverhaltes illustrieren: Anzeigeerstatter A sieht, wie sein Nachbar N ein angeblich besonders verschlüsseltes Chatgerät nutzt. Allein gestützt auf diesen Umstand reicht A eine Strafanzeige wegen Widerhandlung gegen das BetmG bei der Staatsanwaltschaft ein. Er begründet den Vorwurf – ohne Belege – damit, dass N das Gerät bei einem zwielichtigen Händler gekauft und mit Bitcoin bezahlt habe und das Gerät besonders verschlüsselt kommuniziere. In diesem Fall ist eine Verdachtsbegründung schlichtweg nicht möglich, sodass die Staatsanwaltschaft das Verfahren selbstverständlich nicht eröffnen kann und eine Nichtanhandnahme verfügen muss (Art. 309 Abs. 4 StPO).

IV. Einordnung in das präventiv-polizeirechtliche Recht?

Vorstehend wurde aufgezeigt, dass die Massnahmen nicht auf einem vorbestehenden Tatverdacht beruhen. Auch wenn die Massnahmen von ausländischen Behörden durchgeführt wurden, sind diese in die schweizerische Rechtssystematik einzuordnen. Im Lichte dieser weisen sie Elemente des *präventiven Polizeirechts* auf, da es sich um grundrechtsinvasive, verdachtslose Massnahmen zum Zwecke der Kriminalitätsbekämpfung handelt. In den nachfolgenden Kapiteln wird jedoch aufgezeigt, dass die Massnahmen darüber hinaus *geheimdienstliche* und *strafprozessuale* Elemente aufweisen, sodass es sich um hybride Massnahmen handelt.[447]

V. Exkurs: Zufallsfund?

In der schweizerischen Praxis kommt es vor, dass Zwangsmassnahmengerichte die Kryptophonedaten als Zufallsfunde genehmigten.[448] Aufgrund der

446 Vgl. ACKERMANN, S. 332.

447 Siehe nachstehend Abschnitt J.V.II.

448 Vgl. OGer ZH SB240422 vom 15. August 2025, E. IV. 1.2.2. m.H.a. die Zufallsfundsgenehmigung durch das Zwangsmassnahmengericht.

fehlenden verdachtsabhängigen Primärmassnahme kann aus struktureller Sicht jedoch kein Zufallsfund vorliegen.[449] Darüber hinaus sind die Regelungen über den Zufallsfund nach bundesgerichtlicher Rechtsprechung nur einschlägig, wenn die Primärmassnahme von Schweizer Behörden innerhalb eines schweizerischen Strafverfahrens durchgeführt wird.[450]

449 Siehe vorstehend G.III.; ferner Gless, ZStrR, S. 100.

450 BGE 150 IV 139, E. 5.6 hinsichtlich der Anom-Überwachung.

H. Die Massnahmen als Massenüberwachungen

I. Begriff und Zulässigkeit der Massenüberwachung

1. Begriffskriterien der Massenüberwachung (bulk interception)

Vorstehend wurde dargelegt, dass es sich bei den vorliegenden Massnahmen um verdachtsunabhängige Massnahmen handelt.[451] Eine qualifizierte Form der verdachtsunabhängigen Überwachung ist die *Massenüberwachung*. Eine Massenüberwachung ist eine verdachtsunabhängige Massnahme, die eine Vielzahl von Personen betrifft. Nach der Rechtsprechung des EGMR weist eine Massenüberwachung (sog. *bulk interception*) folgende Begriffsmerkmale auf:

- Keine Ausrichtung auf eine bestimmte Person[452]
- Erfassung grosser Datenmengen, die von einer grossen Anzahl von Individuen stammen[453]
- Erfassung internationaler Kommunikation[454]
- Nachträgliche Auswertung über computerforensische Suchkriterien[455]

2. Zulässigkeit der Massenüberwachung nach EGMR

Nach Ansicht des EGMR kann eine Massenüberwachung unter Umständen zulässig sein. Aufgrund des erheblichen Missbrauchspotentials muss eine solche Massnahme jedoch strikten Rahmenbedingungen unterworfen werden.[456]

---

451 Siehe vorstehend G.III.3.e).

452 EGMR Big Brother Watch et al. vs. Vereinigten Königreich, Urteil vom 25. Mai 2021, 58170/13, 62322/14 und 24960/15, § 343 und 346.

453 EGMR Big Brother Watch et al. vs. Vereinigten Königreich, Urteil vom 25. Mai 2021, 58170/13, 62322/14 und 24960/15, § 326.

454 EGMR Centrum för Rättvisa vs. Schweden, Urteil vom 25. Mai 2021, 35252/08, § 258.

455 EGMR Big Brother Watch et al. vs. Vereinigten Königreich, Urteil vom 25. Mai 2021, 58170/13, 62322/14 und 24960/15, § 346.

456 Vgl. EGMR Centrum för Rättvisa vs. Schweden, Urteil vom 25. Mai 2021, 35252/08, § 262.

Dementsprechend hat eine gesetzliche Grundlage zur Massenüberwachung nachfolgende Aspekte vorzusehen:[457]

- Voraussetzungen der Anordnung
- Umstände der Durchführung
- Genehmigung durch eine unabhängige Behörde
- Auswahl, Auswertung und Verwendung der erhobenen Daten
- Schutzmassnahmen bei der Weitergabe von Überwachungsmaterial
- Vorgaben zu Dauer, Speicherung und Vernichtung der Daten
- Unabhängige Aufsicht über die Einhaltung der Schutzvorgaben
- Nachträgliche Überprüfungsmöglichkeit der Rechtmässigkeit

3. Massenüberwachung als geheimdienstliche Massnahme (Art. 38 f. NDG)

Das schweizerische Strafverfahrensrecht kennt keine massenhafte Überwachung der Kommunikations*inhalte*. Lediglich die *Randdaten* können unspezifisch im Rahmen eines strafprozessualen Antennensuchlaufs erfasst werden (vgl. Art. 273 StPO).[458] Ebenso wenig kennen die kantonalen Polizeigesetze eine massenhafte Fernmeldeüberwachung, da diese von Bundesrechts wegen allenfalls Ausführungsvorschriften zur Fernmeldeüberwachung zwecks Personensuche enthalten können.[459]

Im schweizerischen Recht können einzig über die geheimdienstliche Funk- und Kabelaufklärung (Art. 38 f. NDG) massenhafte Kommunikationsinhalte erfasst werden.[460] Art. 38 f. NDG dient lediglich als Rechtsgrundlage für die Informationsbeschaffung durch Schweizer Behörden im Ausland. Keinesfalls kann sie für den vorliegend umgekehrten Fall, der Informationsbeschaffung ausländischer Behörden in der Schweiz, dienen. Nichtsdestotrotz kann die Betrachtung von Art. 38 f. NDG dazu beitragen, die Massnahmen in der schweizerischen Rechtssystematik einzuordnen.

Zum einen kann über die *Funkaufklärung* elektromagnetische Ausstrahlung von Telekommunikationssystemen im Ausland erfasst werden (Art. 38

457 EGMR Big Brother Watch et al. vs. Vereinigten Königreich, Urteil vom 25. Mai 2021, 58170/13, 62322/14 und 24960/15, § 361.

458 Vgl. BGE 137 IV 340.

459 Siehe nachstehend J.I.

460 Vgl. BIAGGINI, N 255 ff.

Abs. 1 NDG). Zum anderen erlaubt die *Kabelaufklärung* den Abgriff grenzüberschreitender leitungsgebundener Kommunikation (Art. 39 Abs. 1 NDG).[461] Diese Überwachungsformen sind nicht auf Anschlüsse von bestimmten Personen ausgerichtet[462] und dienen der Beschaffung sicherheitspolitischer Informationen im Ausland (Art. 38 Abs. 2 und Art. 39 Abs. 1 NDG). Allerdings ist darauf hinzuweisen, dass das BVGer jüngst festgestellt hat, dass die Funk- und Kabelaufklärung, wie sie derzeit vom NDG durchgeführt wird, nicht BV- und EMRK-konform ist.[463]

II. EncroChat, SkyECC, Anom als Massenüberwachung

1. Qualifizierung als Massenüberwachung

In der internationalen Literatur ist umstritten, ob die vorliegenden Überwachungen *Massenüberwachungen (bulk interception)* im Sinne der EGMR-Rechtsprechung darstellen.[464]

Den massgebenden EGMR-Urteilen liegt aus technischer Sicht möglicherweise eine breitere Kommunikationserfassung als den vorliegenden Massnahmen zugrunde. In den Sachverhalten von *Big Brother Watch et al. vs. Vereinigten Königreich* und *Centrum för Rättvisa vs. Schweden* griffen die Geheimdienste die Kommunikation an der Übertragungsinfrastruktur (etwa Kabel und Knotenpunkten) ab. Diese Überwachungsformen waren nach Ansicht der Beschwerdeführer geeignet, die Kommunikation von Millionen von Bürgern zu überwachen.[465] Demgegenüber wurden vorliegend spezifische Messenger-Dienste überwacht. Diese wiesen einen vergleichsweise kleinen Nutzerkreis auf, sodass von den Überwachungen lediglich (zehn-)tausende Nutzer betroffen waren.

Nichtsdestotrotz sind die Begriffsmerkmale der Massenüberwachung vorliegend gegeben. Die Überwachungsmassnahmen waren nicht auf eine bestimmte Person ausgerichtet, sondern erfassten die Kommunikation von tau-

461 Vgl. Biaggini, N 255 ff.; gemäss Art. 39 Abs. 2 NDG ist eine Kabelüberwachung bei einem Datenverkehr innerhalb der Schweiz ausgeschlossen.

462 Botschaft NDG, 2171.

463 BVGer A-6444/2020 vom 19. November 2025.

464 Bejahend Oerlemans/Royer, S. 455; verneinend Sagittae, S. 278.

465 Vgl. Website der Beschwerdeführer <https://bigbrotherwatch.org.uk/press-releases/uk-mass-surveillance-challenged-in-europes-highest-human-rights-court/>.

senden noch völlig unbekannten Nutzern. Die Anzahl der überwachten Personen war lediglich durch die Grösse des Nutzerkreises und die technische Machbarkeit beschränkt. Auch das Charakteristikum der Erfassung von internationaler Kommunikation ist vorliegend gegeben, ebenso wie die Erzeugung enormer Datenmengen.

Ferner erfolgte die nachträgliche Datenauswertung und Nutzeridentifizierung allein anhand computerforensischer Suchkriterien (etwa IMEI-Nummern). Somit sind die Begriffskriterien des EGMR vorliegend erfüllt, sodass es sich bei den Massnahmen um Massenüberwachungen handelt.

2. Folge: Strukturell geheimdienstähnliche Massnahmen

Wie dargelegt, stellen die vorliegenden Massnahmen *Massenüberwachungen* dar. Der massenhafte Kommunikationsabgriff ist im schweizerischen Recht jedoch lediglich dem NDG bekannt (vgl. Art. 38 f. NDG). Im Lichte dessen rücken die vorliegenden Massnahmen aus Sicht der schweizerischen Systematik in die Nähe der nachrichtendienstlichen Überwachungen.[466] Für die geheimdienstliche Bewertung spricht ferner der Umstand, dass es sich vorliegend um Informationsbeschaffung durch *fremde Behörden* in der Schweiz handelt. Letztlich deutet auch die *unterlassene nachträgliche Mitteilung* auf eine geheimdienstliche Massnahme hin. Anders als bei den übrigen Formen der Fernmeldeüberwachung besteht bei der geheimdienstlichen Funk- und Kabelaufklärung im schweizerischen Recht keine Pflicht, die überwachte Person nachträglich zu informieren.[467] Zu beachten ist jedoch, dass die Überwachungen auch präventiv-polizeirechtliche und strafprozessuale Elemente aufweisen, sodass es sich um hybride Massnahmen handelt.[468]

466 Vgl. STOYKOVA, S. 3 hinsichtlich EncroChat.
467 Vgl. BVGer A-6444/2020 vom 19. November 2025, E. 5.7.
468 Siehe vorstehend G.IV. und nachstehend J.VII.

I. Die Massnahmen als Eingriff in das Fernmeldegeheimnis (Art. 13 Abs. 1 BV)

I. Das Fernmeldegeheimnis als Einordnungskriterium

Das vorstehende Kapitel hat aufgezeigt, dass die vorliegenden Massnahmen die Strukturen einer Massenüberwachung aufweisen. Im nun folgenden Kapitel wird untersucht, ob die Massnahmen in das verfassungsrechtlich geschützte Fernmeldegeheimnis eingreifen. Nach Art. 13 Abs. 1 BV hat jede Person Anspruch auf Achtung ihres Brief-, Post- und *Fernmeldeverkehrs*. Diese Bestimmung schützt das Fernmeldegeheimnis.[469] Eine gleich gelagerte Garantie stellt der *Schutz der Korrespondenz* nach Art. 8 Ziff. 1 EMRK dar.[470]

Das Fernmeldegeheimnis ist ein zentraler Anknüpfungspunkt, um eine Massnahme rechtlich einzuordnen. Im Strafverfahrensrecht kann der Fernmeldeverkehr[471], der dem Fernmeldegeheimnis untersteht, lediglich mit dem abschliessenden Massnahmenkatalog von Art. 269 ff. StPO überwacht werden. *Vor* dem Einsetzen des Fernmeldegeheimnisses können Kommunikationsdaten über den Einsatz technischer Geräte wie dem Keylogger (Art. 280 f. StPO) erhältlich gemacht werden.[472] *Nach* Abschluss des Fernmeldegeheimnisses gelten die Regeln der Durchsuchung (Art. 246 ff. StPO), der Edition (Art. 265 StPO) und der Beschlagnahme (Art. 263 ff. StPO).[473]

469 Vgl. BGE 140 IV 181, E. 2.3.

470 BGE 126 I 50, E. 5a.

471 Der Fernmeldeverkehr bezeichnet die elektromagnetische Übertragung von Informationen (Art. 2 i.V.m. Art. 3 lit. c FMG).

472 Vgl. BGE 147 IV 424, E. 5.2; vgl. BSK StPO II-Jean-Richard-dit-Bressel, N 4 zu Art. 269bis.

473 SK StPO II-Hansjakob/Pajarola, N 16 zu Art. 269.

II. Schutzbereich des Fernmeldegeheimnisses

1. Zeitlicher Geltungsbereich

a) Beginn des Übermittlungsvorganges

Das Fernmeldegeheimnis schützt den Kommunikationsvorgang[474], mithin die Übermittlung der Kommunikationsinhalte.[475] Somit definiert sich das Fernmeldegeheimnis grundsätzlich anhand des *Übermittlungsvorganges*.[476]

Im Hinblick auf Textnachrichten beginnt der Übermittlungsvorgang, sobald der Versender die Datenherrschaft über die Nachricht abgibt.[477] Unter Datenherrschaft versteht man die Möglichkeit, von Daten Kenntnis zu nehmen, diese weiterzuleiten und zu löschen.[478] Zu welchem Zeitpunkt die Datenherrschaft tatsächlich aufgegeben wird, kann unterschiedlich bewertet werden. Nach einer Auffassung sind sämtliche Vorgänge im Endgerät vom Versender beherrschbar, da der Versender durch das Abschalten des Geräts eine Datenübermittlung verhindern kann. Demnach gibt der Versender erst mit Einspeisung der Daten in das Kommunikationsnetz die Datenherrschaft ab.[479] Nach einer anderen Auffassung gibt der Versender bereits mit Auslösen des Sendevorgangs die Datenherrschaft ab.[480] Demzufolge fallen bereits die Datenverarbeitungsvorgänge, die nach Betätigen der Sendefunktion im sendenden Endgerät stattfinden, unter das Fernmeldegeheimnis.

Nach der hier vertretenen Ansicht ergibt sich aus der Systematik der StPO, dass das Betätigen der Sendefunktion und damit die letztgenannte Auffassung massgebend ist. Die StPO normiert in Art. 269ter den *Einsatz von besonderen Informatikprogrammen zur Überwachung des Fernmeldeverkehrs*. Dieser sog. GovWare-Einsatz stellt einen Eingriff in das Fernmeldegeheimnis dar.[481] Eine GovWare leitet eine Textnachricht vor deren Verschlüsselung – und somit *vor*

474 BGE 140 IV 181, E. 2.4.
475 Vgl. BGE 140 IV 181, E. 2.4.
476 Einzig bei Randdaten und Zugangsdaten ist nicht an den Übermittlungsvorgang anzuknüpfen.
477 Vgl. BSK StPO II-Jean-Richard-dit-Bressel, N 23 zu Art. 269.
478 BSK StPO II-Jean-Richard-dit-Bressel, N 23 zu Art. 269.
479 So Rückert, S. 51, 54 und 57.
480 So BSK StPO II-Jean-Richard-dit-Bressel, N 23 zu Art. 269.
481 Kühne/Rütsche, S. 353.

der Einspeisung in das Kommunikationsnetz – aus dem Endgerät aus.[482] Daraus ist zu schliessen, dass das Fernmeldegeheimnis vor Einspeisung in das Kommunikationsnetz ansetzt. Darüber hinaus lässt sich diese Auslegung auch mit dem Willen des Versenders begründen. Das Betätigen der Sendefunktion ist die Willensmanifestation des Versenders, den Kommunikationsvorgang zu starten. Zu welchem Zeitpunkt die Nachricht tatsächlich das Endgerät verlässt und in das Netz eingespiesen wird, entzieht sich der Kenntnis und Herrschaft des Nutzers.

b) Abschluss des Übermittlungsvorganges

Der Kommunikationsvorgang ist abgeschlossen, wenn sich die Kommunikationsdaten im alleinigen Herrschaftsbereich des Empfängers befinden. Dies realisiert sich, sobald der Empfänger das Nachrichten-Programm öffnet. Die tatsächliche Kenntnisnahme der Nachricht durch den Empfänger ist nicht von Bedeutung.[483]

2. Sachlicher Geltungsbereich

a) Schutz der Vertraulichkeitserwartung

Art. 13 Abs. 1 BV schützt die Vertraulichkeit der Kommunikation.[484] Sofern die Kommunikation über Kommunikationsträger erfolgt, soll dies ohne staatliche Kenntnisnahme geschehen.[485] Geschützt ist die Kommunikation zwischen Einzelpersonen, nicht aber jene mit einer unspezifizierten Allgemeinheit. Massgebend ist, ob mit vertraulicher Behandlung der Kommunikation gerechnet werden kann.[486] Der Schutz bezieht sich somit auf die Vertraulichkeits*erwartung*. Insbesondere ist das Vertrauen in die Integrität der genutzten Infrastruktur und die vertrauliche Datenbehandlung durch den Infrastrukturbetreiber vom Fernmeldegeheimnis erfasst.[487] Nicht erfasst hingegen ist das Vertrauen in die Identität oder Integrität des Kommunikationspartners.[488]

---

482 BSK StPO II-Jean-Richard-dit-Bressel, N 2 zu Art. 269ter.

483 BGE 140 IV 181, E. 2.4 ff.; a.A. CR StPO-Métille, N 41 zu Intro 269-281, wonach das Fernmeldegeheimnis erst abgeschlossen sei, sobald der Empfänger eine Löschungsmöglichkeit hatte; vgl. auch Jositsch/Schmid, N 1139.

484 BGE 126 I 50, E. 6a.

485 BGE 126 I 50, E. 6a.

486 BSK BV-Diggelmann/Elmer, N 29 zu Art. 13.

487 Rückert, S. 73 und 76 und 109.

488 Rückert, S. 109.

b) Geschützte Daten: Inhalts- und Randdaten

Die Rechtsprechung des EGMR geht von einem umfassenden Garantieschutz aus, indem er jede Erfassung elektronischer Kommunikationsdaten als Eingriff in Art. 8 Ziff. 1 EMRK bezeichnet.[489] Im schweizerischen Überwachungsrecht wird zwischen Inhalts-, Rand- und Bestandsdaten unterschieden.[490] Während die Inhalts- und Randdaten dem Fernmeldegeheimnis unterstehen[491], erstreckt sich dieses nicht auf Bestandsdaten[492]. Inhaltsdaten beziehen sich auf den materiellen Inhalt der Kommunikation.[493] Randdaten geben Auskunft über die Kommunikationsumstände, wer mit wem, wann, wie lange und von wo aus in Verbindungen gestanden hat (Art. 8 lit. b BÜPF). Bei Bestandsdaten handelt es sich um Daten, die über Abonnementverhältnisse, nicht aber über die Korrespondenz, Auskunft geben.[494]

c) Akzessorische Beurteilung von Zugangsdaten

Nicht besonders gesetzlich geregelt ist die Behandlung von Zugangsdaten. Zugangsdaten sind Daten, die den Zugriff auf weitere Daten ermöglichen.[495] Namentlich fallen kryptographische Schlüssel in diese Kategorie.[496] Nach RÜCKERT ist zur Beurteilung von Zugangsdaten die Schutzwürdigkeit der Primärdaten massgeblich.[497] Erlauben Zugangsdaten den Zugriff auf Daten, die dem Fernmeldegeheimnis unterstehen, fallen auch die Zugangsdaten unter dieses.[498] Die akzessorische Anknüpfung von Zugangsdaten ist nach der hier vertretenen Auffassung sinnvoll. Zum einen erfolgt ein Zugriff auf Zugangsdaten nicht als Selbstzweck, da es sich lediglich um einen Zwischenschritt für die Kenntnisnahme der Primärdaten handelt. Zum anderen greift der Abgriff von Zugangsdaten in die Vertraulichkeitserwartung ein, da die Vertraulichkeit nun nur noch vom Willen desjenigen abhängig ist, der über die Zugangsdaten verfügt.

489 EGMR Kirdök et al. vs. Türkei, Urteil vom 3. Dezember 2019, 14704/12, § 34.
490 SIMMLER, S. 136.
491 BGE 140 I 353, E. 8.3.
492 Vgl. SIMMLER, S. 134.
493 Vgl. HANSJAKOB, Überwachungsrecht, N 1455.
494 HANSJAKOB, Überwachungsrecht, N 888.
495 RÜCKERT, S. 104.
496 RÜCKERT, S. 104.
497 RÜCKERT, S. 258 m.H.a. § 100j D-StPO.
498 Vgl. RÜCKERT, S. 258.

III. Die Geltung des Fernmeldegeheimnisses in casu

1. EncroChat

a) Historical data collection

Bei der EncroChat-Überwachung sind zwei unterschiedliche Datenerhebungen zu unterscheiden. Gemäss Arbeitshypothese griff die Schadsoftware in der *historical data collection* sämtliche Daten ab, die lokal auf dem Gerät gespeichert waren (z. B. gespeicherte Chatnachrichten).[499] Da sich diese Daten nicht mehr im Übermittlungsstadium befanden, gilt das Fernmeldegeheimnis als abgeschlossen.[500] Folglich greift diese Datenerhebung nicht in das Fernmeldegeheimnis ein.

b) Forward facing collection

Nachdem die Schadsoftware die lokal gespeicherten Daten abgriff, leitete die Schadsoftware fortan die Kommunikation in Echtzeit aus (*forward facing collection*).[501] Hierbei wurde die Nachricht nach Betätigen der Sendefunktion – aber vor deren Verschlüsselung – kopiert und an einen französischen Polizei-Server übermittelt.[502] Da die Datenausleitung nach Betätigen der Sendefunktion erfolgte, hat das Fernmeldegeheimnis bereits eingesetzt.[503]

499 SF and Ors v NCA [2023] UKIPTrib3, § 43; Regina v A, B, D & C [2021], EWCA Crim 128, [2021], § 77.

500 Vgl. vorstehend I.II.1.

501 Regina v A, B, D & C [2021], EWCA Crim 128, [2021], § 13; SF and Ors v NCA [2023] UKIPTrib3, § 43.

502 Regina v A, B, D & C [2021], EWCA Crim 128, [2021], § 13; SF and Ors v NCA [2023] UKIPTrib3, § 43.

503 Sofern auch das *empfangende* Gerät mit der Software befallen war, leitete auch dieses die Nachrichten aus. Hinsichtlich des empfangenden Gerätes lässt sich der Ausleitungszeitpunkt und somit die Geltung des Fernmeldegeheimnisses nicht eindeutig bestimmen. Da allerdings in der Praxis nicht nachvollziehbar ist, aus welchem Endgerät die Daten entstammen, kann offenbleiben, ob auch die Ausleitung aus dem empfangenden Gerät in das Fernmeldegeheimnis eingreift.

2. SkyECC

a) Qualifizierung als Zugangsdaten

Gemäss Arbeitshypothese erlangten die französischen Behörden die kryptographischen Schlüssel der SkyECC-Kommunikation, indem der MITM-Server die Endgeräte kontaktierte. Bei den erhältlich gemachten Schlüsseln handelt es sich um *Zugangsdaten*, da sie die Entschlüsselung der erfassten Inhaltsdaten ermöglichten. Zugangsdaten sind hinsichtlich des Fernmeldegeheimnisses akzessorisch zu den zugänglich gemachten Daten zu bewerten[504], weshalb nachfolgend der Abgriff der Inhaltsdaten betrachtet wird.

b) Vorfrageweise Beurteilung des Inhaltsdatenabgriffes

Der Abgriff der Inhaltsdaten erfolgte durch die französischen Behörden an den SkyECC-Servern in Frankreich und ist somit in Frankreich zu verorten. Als Rechtsgrundlage dienten Art. 100, 100-1 und 100-3 bis 100-8 des FR-CPP.[505] Diese Bestimmungen befinden sich unter dem Titel «Des interceptions de *correspondance* émises par la voie des communications électroniques»[506], was als Überwachung des Fernmeldeverkehrs («interceptions de correspondance») übersetzt werden kann. Nach französischem Verständnis stellen Massnahmen dieses Titels Eingriffe in das Privatleben («atteinte à la vie privée»)[507], insbesondere in das Fernmeldegeheimnis («secret de correspondance»)[508] dar.[509] Gemäss Anknüpfung an das französische Recht ist der Inhaltsdatenabgriff somit als Eingriff in das Fernmeldegeheimnis zu werten. Auch bei hypothetischer Anknüpfung an das schweizerische Recht wäre diese Massnahme ein Eingriff in das Fernmeldegeheimnis (Art. 13 Abs. 1 BV), da der Abgriff während des geschützten Übermittlungsvorganges erfolgte.[510] Zum gleichen Ergebnis führt indes auch die Anknüpfung an den gemeinsamen Rechtsrahmen beider Jurisdiktionen, dem Schutz der Korrespondenz nach Art. 8 Ziff. 1 EMRK. Diese Bestimmung entspricht dem Schutz von Art. 13 Abs. 1 BV.[511] Art. 8 Ziff. 1 EMRK

504 Siehe vorstehend I.II.2.c).
505 OGer ZH SB240422 vom 15. August 2025, E. III. 2.1.
506 FR-CPP, «Livre Ier», «Titre III», «Chapitre Ier», «Section 3», «Sous-section 2».
507 Desportes/Lazerges-Cousquer, N 2247.
508 Vgl. Collet, N 1241.
509 Diese Garantien leiten sich aus Art. 2 und 4 der «Déclaration des droits de l'homme et du citoyen» ab, siehe dazu Cons. const., déc. n° 2004-492 DC, 2 mars 2004, cons. 4.
510 Vgl. BGE 140 IV 181 E. 2.4.
511 BGE 126 I 50, E. 5a.

greift bei jeder Erfassung elektronischer Kommunikationsdaten[512] und somit auch bei den hier interessierenden Kommunikationsabgriffen. Das Vorstehende zeigt, dass der vorliegende Abgriff der Inhaltsdaten in das Fernmeldegeheimnis eingreift, unabhängig von der vorfrageweise referenzierten Rechtsordnung.

c) Akzessorische Beurteilung der Zugangsdaten

Wie soeben dargelegt, fallen die erfassten Inhaltsdaten unter das Fernmeldegeheimnis. Dementsprechend fallen aufgrund der Akzessorietät auch die kryptographischen Elemente unter das Fernmeldegeheimnis (Art. 13 Abs. 1 BV und Art. 8 Ziff. 1 EMRK).[513] Aufgrund der Akzessorietät gilt dies unabhängig davon, ob die kryptographischen Elemente zum Zeitpunkt der stillen Kontaktierung bereits im Endgerät vorhanden waren oder anlässlich der Kontaktierung erst generiert wurden.

3. Anom

Das Charakteristikum der Anom-Überwachung bestand darin, dass der Betreiber (das FBI) die Nutzer über die Integrität der Kommunikationsgeräte täuschte. Der Vertrieb erfolgte unter Anpreisung des hohen Vertraulichkeitsschutzes. Tatsächlich aber waren die Geräte vom Betreiber derart ausgestattet, dass jede Nachricht nach Betätigen der Sendefunktion kopiert und die Kopie an einen Polizei-Server ausgeleitet wurde. Diese Täuschung stellt einen Eingriff in das Fernmeldegeheimnis dar, da dieses das *Vertrauen in die Integrität* der Infrastruktur schützt.[514] Darüber hinaus greift das Fernmeldegeheimnis auch in zeitlicher Hinsicht. Gemäss der Arbeitshypothese wurde die Nachricht nach Betätigen der Sendefunktion kopiert und ausgeleitet, weshalb das Fernmeldegeheimnis bereits eingesetzt hat.[515]

512 EGMR Kirdök et al. vs. Türkei, Urteil vom 3. Dezember 2019, 14704/12, § 34.
513 Vgl. RÜCKERT, S. 104 und 258.
514 Siehe vorstehend I.II.2.a).
515 Siehe vorstehend I.II.1.a).

J. Fernmelderechtliche Massnahmenqualifikation

I. Fernmeldeüberwachung als Bundeskompetenz

Das vorstehende Kapitel hat gezeigt, dass die Massnahmen in das Fernmeldegeheimnis eingreifen. Nun wird ein Überblick über die Erscheinungsformen der Fernmeldeüberwachung im schweizerischen Recht gegeben und versucht, die Massnahmen dort einzuordnen. Zu beachten ist, dass nach Art. 92 Abs. 1 BV das Fernmeldewesen Sache des Bundes ist. Dabei handelt es sich um eine umfassende und *ausschliessliche Bundeskompetenz*.[516] Diese ausschliessliche Kompetenz bezieht sich auch auf die Überwachung des Fernmeldeverkehrs.[517] Für eine eigenständige kantonale (polizeirechtliche) Regelung zur Überwachung des Fernmeldeverkehrs besteht aus verfassungsrechtlicher Sicht somit kein Raum.

II. Strafprozessuale Fernmeldeüberwachungen

1. Konventionelle Überwachung (Art. 269 StPO)

Die Grundform der Fernmeldeüberwachung stellt die Überwachung gemäss Art. 269 StPO dar. Diese erfolgt unter Mitwirkung eines Bundesverwaltungsorgans, dem Dienst nach Art. 3 Abs. 1 BÜPF[518], und dem jeweiligen Fernmeldedienstanbieter. Der Dienst nimmt die Anordnung der Staatsanwaltschaft entgegen und leitet diese dem entsprechenden Fernmeldedienstanbieter weiter (Art. 16 lit. d BÜPF).[519] Der Fernmeldedienstanbieter liefert daraufhin dem Dienst den Inhalt des Fernmeldeverkehrs der überwachten Person (Art. 26 Abs. 1 lit. a BÜPF). Der Dienst leitet die erfasste Kommunikation sodann den Strafverfolgungsbehörden weiter.

---

516 BSK BV-Kern, N 4 zu Art. 92.

517 Dementsprechend erliess der Bundesgesetzgeber das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) u.a. gestützt auf Art. 92 Abs. 1 BV.

518 Der Dienst für die Überwachung des Post- und Fernmeldeverkehrs ist dem Eidgenössischen Justiz- und Polizeidepartement zugeordnet (Art. 3 Abs. 1 und 2 BÜPF).

519 Hansjakob, Überwachungsrecht, N 534 und 1555.

2. Besondere technische Geräte zur Überwachung des Fernmeldeverkehrs (Art. 269bis StPO)

Ist die konventionelle Überwachung nach Art. 269 StPO ungeeignet[520], kann die Staatsanwaltschaft den Einsatz von besonderen technischen Geräten nach Art. 269bis StPO anordnen. Die Bestimmung regelt den Einsatz von sog. *IMSI-Catchern* und ähnlichen Geräten.[521] Ein IMSI-Catcher wird in der Umgebung der überwachten Person durch die Polizei eingerichtet[522], sodass diese Überwachung ohne Mitwirkung des Dienstes oder des Fernmeldedienstanbieters erfolgt[523].

Ein IMSI-Catcher simuliert eine Funkzelle, wobei dieser eine stärkere Sendeleistung hat als die echte Funkzelle.[524] Die umliegenden Mobiltelefone verbinden sich daraufhin statt mit der echten Funkzelle mit dem IMSI-Catcher.[525] Diese Umleitung der Datenströme ermöglicht den Behörden, die Kommunikationsdaten zu erfassen. Der Wortlaut von Art. 269bis Abs. 1 StPO beschränkt den Einsatz auf das *Mithören* oder *Aufnehmen* von *Gesprächen*.[526] Nicht gedeckt von der Bestimmung ist hingegen die Aufzeichnung von Textnachrichten.[527]

Nach Hansjakob kann ein IMSI-Catcher dazu eingesetzt werden, um die Verschlüsselung des Datenverkehrs zu entfernen.[528] Zweifelhaft ist allerdings, ob dies vom Gesetzestext gedeckt ist, da die Einsatzzwecke abschliessend in Art. 269bis Abs. 1 StPO genannt sind.[529] Sollte eine Entschlüsselung als zulässig erachtet werden, so könnte sich dies aber lediglich auf die von der Bestimmung erfassten Telefongespräche, nicht aber auf Textnachrichten beziehen.

---

520 BSK StPO II-Jean-Richard-dit-Bressel, N 6 zu Art. 269bis; nach dem ein IMSI-Catcher subsidiär zur konventionellen Überwachung ist, da dieser auch in das Fernmeldegeheimnis Unbeteiligter eingreift.

521 BSK StPO II-Jean-Richard-dit-Bressel, N 3 f. zu Art. 269bis.

522 Vgl. Hansjakob, Überwachungsrecht, N 573; die eingesetzte Technologie ist vorgängig durch das Bundesamt für Kommunikation (BAKOM) zu bewilligen (Art. 269bis Abs. 1 lit. c). Dies soll sicherstellen, dass die eingesetzte Technik den allgemeinen Kommunikationsverkehr nicht beeinträchtigt, siehe dazu Hansjakob, Überwachungsrecht, N 563.

523 BSK StPO II-Jean-Richard-dit-Bressel, N 3 zu Art. 269bis.

524 Rückert, S. 343.

525 Hansjakob, Überwachungsrecht, N 543.

526 Darüber hinaus kann ein IMSI-Catcher zur Identifizierung von Personen oder Sachen oder zur Standortermittlung eingesetzt werden.

527 Kritisch dazu BSK StPO II-Jean-Richard-dit-Bressel, N 5 zu Art. 269bis.

528 Hansjakob, Überwachungsrecht, N 547.

529 BSK StPO II-Jean-Richard-dit-Bressel, N 5 zu Art. 269bis.

3. Besondere Informatikprogramme zur Überwachung des Fernmeldeverkehrs (Art. 269ter StPO)

a) Art. 269ter StPO als gesetzliche Grundlage für die GovWare

Ist die konventionelle Überwachung nach Art. 269 StPO ungeeignet, kann die Staatsanwaltschaft den Einsatz von besonderen Informatikprogrammen nach Art. 269ter StPO anordnen. Diese Bestimmung erlaubt namentlich den Einsatz von Government Software (sog. *GovWare*).[530] Eine GovWare wird gestützt auf die staatsanwaltliche Anordnung von der Polizei auf das Endgerät aufgespielt.[531] Diese Überwachungsart erfolgt – wie der Einsatz eines IMSI-Catchers – ohne Involvierung des Dienstes oder des Fernmeldedienstanbieters.[532]

Der Zweck dieser Bestimmung liegt darin, eine End-to-End-Verschlüsselung zu umgehen.[533] Hierzu sieht Art. 269ter Abs. 1 StPO vor, dass die aufgespielte GovWare den Kommunikationsinhalt in unverschlüsselter Form abfängt. Dies erfolgt, indem die GovWare die Nachrichten vor deren Verschlüsselung oder nach deren Entschlüsselung aus dem Datenverarbeitungssystem ausleitet.[534]

b) Die Zieldaten der GovWare

Eine GovWare darf nicht dazu verwendet werden, sämtliche Daten eines Gerätes auszuleiten. Aus dem Wortlaut von Art. 269ter Abs. 1 StPO geht hervor, dass nur das Abfangen von *unverschlüsselten* Daten zulässig ist. Dementsprechend ist nur eine *Umgehung* der Verschlüsselung erlaubt, nicht aber eine *Entschlüsselung* von chiffrierten Nachrichten.[535] Eine weitere Einschränkung besteht darin, dass die GovWare nur Daten ausleiten darf, welche dem *Fernmeldegeheimnis* unterstehen. Andernfalls liegt eine unzulässige heimliche Online-Durchsuchung vor.[536]

---

530 HANSJAKOB, Überwachungsrecht, N 586 ff.

531 HANSJAKOB, Überwachungsrecht, N 654.

532 Vgl. HANSJAKOB, Überwachungsrecht, N 654.

533 HANSJAKOB, Überwachungsrecht, N 576; BSK StPO II-JEAN-RICHARD-DIT-BRESSEL, N 2 zu Art. 269ter.

534 BSK StPO II-JEAN-RICHARD-DIT-BRESSEL, N 2 zu Art. 269ter.

535 Vgl. HANSJAKOB, Überwachungsrecht, N 589; die Entfernung von Verschlüsselung wäre allenfalls über den Einsatz eines Gerätes i.S.v. Art. 269bis StPO zu bewerkstelligen, siehe dazu HANSJAKOB, Überwachungsrecht, N 547, jedoch kritisch dazu vorstehend J.II.2.

536 BSK StPO II-JEAN-RICHARD-DIT-BRESSEL, N 5 zu Art. 269^{quater}; HANSJAKOB, Überwachungsrecht, N 647; Botschaft BÜPF, 2702 und 2776.

c) Die GovWare als gerätspezifische Massnahme

Die Massnahme von Art. 269ter StPO ist als gerätspezifische Massnahme ausgestaltet. Aus der Bestimmung geht hervor, dass die Massnahme stets ein einzelnes Datenverarbeitungssystem betrifft.[537] Nach HANSJAKOB muss darüber hinaus in der Überwachungsanordnung spezifiziert werden, welche App im einzelnen Endgerät zu überwachen ist.[538] Zudem ist in der Überwachungsanordnung anzugeben, welche Daten von der fraglichen App ausgeleitet werden sollen (Art. 269ter Abs. 2 lit. a StPO).[539] Dementsprechend handelt es sich um eine äusserst zielgenaue Überwachungsform.

4. Exkurs: Online-Recherche

a) Voraussetzungen der Online-Recherche

Ein Zugriff auf digitale Daten kann ferner auch im Rahmen einer *Online-Recherche* (bzw. vorläufigen Sicherstellung) erfolgen.[540] Eine Online-Recherche ist eine behördliche Durchsuchung elektronisch gespeicherter Daten, die nicht dem Fernmeldegeheimnis unterstehen.[541] Mangels Eingriffs in das Fernmeldegeheimnis erfolgen die nachfolgenden Erörterungen im Sinne eines Exkurses.

Die gesetzlichen Grundlagen der Online-Recherche befinden sich in Art. 246 i.V.m. Art. 263 Abs. 1 lit. a StPO. Nach Art. 246 StPO können Datenträger *durchsucht* werden, wenn zu vermuten ist, dass sich darin *beschlagnahmefähige* Informationen befinden. Die Beschlagnahmefähigkeit nach Art. 263 Abs. 1 lit. a StPO setzt voraus, dass der Gegenstand voraussichtlich als Beweismittel gebraucht werden kann. Die Beweismitteltauglichkeit ist jedoch weit ausgelegt, sodass auch Objekte beschlagnahmt werden können, die lediglich geeignet sind, Beweise aufzufinden.[542]

---

537 Vgl. Art. 269ter Abs. 1 StPO, wonach Informatikprogramme in *ein* Datenverarbeitungssystem eingeschleust werden können; ebenso Abs. 2 wonach *das betreffende* Datenverarbeitungssystem in der Überwachungsanordnung zu bezeichnen ist.

538 HANSJAKOB, Überwachungsrecht, N 638.

539 HANSJAKOB, Überwachungsrecht, N 639.

540 Vgl. BGE 143 IV 270, E. 7.5.

541 Vgl. BGE 144 IV 74, E. 2.4.

542 Vgl. HEIMGARTNER, S. 132.

b) Erstes Abgrenzungskriterium: Kein Fernmeldegeheimnis

Die Online-Recherche ist von der Überwachung des Fernmeldeverkehrs abzugrenzen. Dies erfolgt primär anhand des Übermittlungsstadiums der betroffenen Daten. Die Online-Recherche erlaubt den Zugriff auf *gespeicherte* Daten.[543] Befinden sich hingegen Daten im *Übermittlungsvorgang*, so greift das Fernmeldegeheimnis.[544] Daten, die dem Fernmeldegeheimnis unterliegen, sind ausschliesslich über den Massnahmenkanon von Art. 269 ff. StPO zu erheben.[545]

c) Zweites Abgrenzungskriterium: Offene Zwangsmassnahme

Eine Online-Recherche unterscheidet sich von der Fernmeldeüberwachung ferner durch ihren offenen Charakter. Als offene Zwangsmassnahme erfolgt eine Online-Recherche grundsätzlich mit Kenntnis der betroffenen Person.[546] Eine gänzlich geheime Durchsuchung ist dem schweizerischen Recht unbekannt.[547] Demgegenüber ist die Überwachung des Fernmeldeverkehrs eine verdeckte Massnahme, welche der betroffenen Person erst im Nachhinein mitgeteilt wird (vgl. Art. 279 StPO).

Der offene Charakter der Online-Recherche manifestiert sich daran, dass der betroffenen Person vor der Massnahme rechtliches Gehör zu gewähren ist (Art. 247 Abs. 1 StPO). Im Rahmen dessen kann die betroffene Person die Siegelung geltend machen (Art. 248 StPO).[548] Unter gewissen Umständen können jedoch auch Durchsuchungen zunächst ohne Wissen der betroffenen Person erfolgen. Namentlich ist dies bei Vorliegen einer konkreten Kollusionsgefahr der Fall.[549] Gleiches gilt bei einer Durchsuchung, die ohne vorgängige Ankündi-

543 BGE 144 IV 74, E. 2.4.

544 BGE 144 IV 74, E. 2.4; zu beachten ist jedoch, dass bei Zugangsdaten nicht der Übermittlungsvorgang, sondern die Akzessorietät massgebend ist, siehe dazu vorstehend I.II.2.c).

545 Vgl. BGE 140 IV 181, E. 2.4.

546 Vgl. BSK StPO II-Thormann/Brechbühl, N 4 zu Art. 246.

547 Vgl. Hansjakob, forumpoenale, S. 303, nach dem eine heimliche Durchsuchung denkbar wäre, sofern ein Zwangsmassnahmengericht diese genehmigen würde; ferner Graf, Praxishandbuch, N 142, nach dem es sinnvoll sei, de lege ferenda eine geheime Durchsuchung mit Richtervorbehalt vorzusehen.

548 Vgl. BGE 144 IV 74, E. 2.4.

549 Vgl. BGE 143 IV 270, E. 7.3 ff., wonach in diesem Fall die Daten grob gesichtet werden dürfen, aber eine Auswertung erst erfolgen darf, nachdem die betroffene Person eine Äusserungsmöglichkeit (Siegelungsmöglichkeit) hatte.

gung erfolgt und bei der die betroffene Person nicht anwesend ist.[550] In diesen Fällen wird die betroffene Person jedoch zeitnah über die Massnahme informiert[551] oder deren Siegelungsrecht wird von Amtes wegen beachtet.[552] Erfolgt eine Massnahme hingegen ohne jegliche Mitteilung und Siegelungsmöglichkeit, so liegt eine geheime Massnahme vor.

III. Ausserstrafprozessuale Fernmeldeüberwachungen

1. Fernmeldeüberwachung zwecks Personensuche (Art. 35 f. BÜPF)

Auch ausserhalb des Strafverfahrens kann der Fernmeldeverkehr überwacht werden. Das Bundesrecht erlaubt mit Art. 35 f. BÜPF die Fernmeldeüberwachung zwecks Notsuche oder zur Fahndung nach einer verurteilten Person. Auch einige kantonale Polizeigesetze enthalten Bestimmungen zur Fernmeldeüberwachung zwecks Personensuche.[553] Da die Fernmeldeüberwachung jedoch in die ausschliessliche Bundeskompetenz fällt, handelt es sich bei diesen kantonalen Bestimmungen lediglich um organisatorische Ausführungsbestimmungen zur bundesrechtlichen Personensuche nach Art. 35 f. BÜPF.[554]

2. Rechtshilfeweise Überwachung (Art. 18a f. IRSG)

Beabsichtigt eine ausländische Behörde, eine Fernmeldeüberwachung in der Schweiz durchzuführen, so hat sie um Rechtshilfe zu ersuchen. Die Schweizer Behörde führt in der Folge rechtshilfeweise die Fernmeldeüberwachung in der Schweiz durch (vgl. Art. 18a f. IRSG).

Art. 18a Abs. 4 IRSG verweist hinsichtlich der Voraussetzungen und des Verfahrens auf Art. 269-279 StPO. Zweifelsfrei kann in der Rechtshilfe die konventionelle Überwachung nach Art. 269 StPO durchgeführt werden (vgl. auch Art. 1 Abs. 1 lit. b BÜPF). Nach der hier vertretenen Ansicht ist der Verweis auf

550 BSK StPO II-Thormann/Brechbühl, N 11 zu Art. 247.

551 Vgl. BGE 143 IV 270, E. 7.5.

552 BSK StPO II-Thormann/Brechbühl, N 11 zu Art. 247.

553 Vgl. etwa Art. 31c PolG FR; Art. 50bis PG SG; § 10c Abs. 2 PolG ZG.

554 Vgl. Hansjakob, Überwachungsrecht, N 1760, nach dem eine Regelung der Fernmeldeüberwachung zwecks Notsuche in den kantonalen Polizeigesetzen nicht opportun sei.

Art. 269 ff. StPO umfassend zu verstehen, sodass auch der Einsatz eines *IMSI-Catchers* (Art. 269bis StPO) und einer *GovWare* (Art. 269ter StPO) in der passiven Rechtshilfe möglich ist.

3. Nachrichtendienstrechtliche Überwachung (Art. 26 NDG)

a) Ausgewählte Überwachungsmassnahmen nach Art. 26 NDG

Auch der Nachrichtendienst des Bundes (NDB) kann den Fernmeldeverkehr überwachen. Nach Art. 26 Abs. 1 NDG stehen ihm dazu verschiedene Möglichkeiten zur Verfügung. Namentlich kann der NDB den Fernmeldeverkehr über den Einsatz von technischen Geräten (lit. a^{bis}) überwachen. Ein technisches Gerät kann im NDG weitreichender als im strafprozessualen Kontext eingesetzt werden (vgl. Art. 269bis StPO). Anders als in der StPO ist der Einsatz nicht auf das Mithören oder Aufnehmen von Gesprächen beschränkt, sondern lässt die Erfassung jeglicher *Übermittlungen* zu.

Darüber hinaus besteht die Möglichkeit, in ein Computersystem einzudringen, um dort Informationen zu beschaffen (Art. 26 Abs. 1 lit. d Ziff. 1 NDG). Diese Bestimmung hat einen besonderen Charakter, da sie den Zugriff auf *gespeicherte*, aber auch auf *übermittelte* Informationen vorsieht. Somit kann auf Fernmeldedaten, aber auch auf Daten, die nicht dem Fernmeldegeheimnis unterstehen, zugegriffen werden. Insbesondere kann etwa eine – im Strafverfahren unzulässige – Online-Durchsuchung durchgeführt werden.[555] Aufgrund der offenen Formulierung der Bestimmung ist der Einsatz von Technologien, die dem Strafverfahrensrecht gänzlich unbekannt sind, denkbar.

b) Die Massnahmen nach Art. 26 NDG als zielgerichtete Massnahmen

Bei den Massnahmen nach Art. 26 NDG handelt es sich um zielgerichtete, personenspezifische Massnahmen. Dies zeigt sich zum einen daran, dass im Überwachungsantrag Angaben zu den betroffenen Personen zu machen sind (Art. 29 Abs. 1 lit. b NDG) und diese Personen nachträglich zu informieren sind (Art. 33 Abs. 1 NDG). Zum anderen äussert es sich daran, dass Massnahmen gegenüber Drittpersonen nur zulässig sind, wenn die Zielperson Objekte der

[555] Vgl. Mitbericht GPDel, S. 21.

Drittperson zur Informationsübermittlung nutzt (Art. 28 Abs. 1 NDG). Folglich ist diese Überwachungsform als zielgenaue Massnahme konzipiert.

IV. Strafprozessuale Würdigung

1. Vorgehenshinweis

Die dargelegten Rechtsgrundlagen stellen einzig für Schweizer Behörden eine Ermächtigungsgrundlage dar (ausdrücklich Art. 1 Abs. 1 StPO). Die vorliegenden Massnahmen sind zwar teils in der Schweiz zu verorten, doch wurden sie eigenständig von ausländischen Behörden durchgeführt. Folglich lässt sich das Vorgehen nicht auf die betrachteten Rechtsgrundlagen (StPO, BÜPF, IRSG oder NDG) stützen. Dies stellt zwar fraglos eine territorialitätsrechtliche Problematik dar, was jedoch weiter unten beleuchtet wird.[556] An dieser Stelle soll eine typologische Einordnung der zu untersuchenden Überwachungen anhand der vorstehenden Rechtsgrundlagen erfolgen.

Dabei ist zu beachten, dass die Massnahmen zwar präventiv-polizeiliche und nachrichtendienstliche Elemente aufweisen.[557] Gleichermassen ist aber zu berücksichtigen, dass die Überwachungsergebnisse in Strafverfahren verwendet werden. Somit dienen sie letztlich dem strafprozessualen Zweck der Strafverfolgung. Die strafprozessuale Verwertung von sicherheitsrechtlich erhobenen Informationen setzt voraus, dass die Massnahme auch dem Strafverfahrensrecht bekannt ist.[558] Dementsprechend folgt nachstehend zunächst eine strafprozessuale Würdigung, bevor die sicherheitsrechtliche Einordnung folgt.

2. EncroChat

a) Schadsoftware als GovWare

Gemäss Arbeitshypothese erfolgte die EncroChat-Überwachung über eine Schadsoftware. Bei dieser Schadsoftware handelt es sich um ein Informatikprogramm, welches auf die Endgeräte eingeschleust wurde. Die Funktion der Schadsoftware bestand darin, die Daten des betroffenen Endgerätes in unver-

556 Siehe nachstehend P.
557 Siehe vorstehend G.IV. und H.II.2.
558 Siehe vorstehend C.III.

schlüsselter Form auszuleiten. Dieses Instrument entspricht somit einer *GovWare* i.S.v. Art. 269ter Abs. 1 StPO.

b) EncroChat-Überwachung als unbekannte Massnahme

In der StPO ist der Einsatz der GovWare als zielgenaue, gerätspezifische Massnahme ausgestaltet.[559] Zudem darf eine GovWare nur jene Daten erfassen und ausleiten, die dem Fernmeldegeheimnis unterstehen.[560] Diesen Charakteristiken entspricht die EncroChat-Überwachung jedoch keinesfalls. Bei der EncroChat-Überwachung wurden über einen Update-Server *zehntausende* (knapp 40'000[561]) Geräte mit der GovWare infiziert und überwacht, sodass es sich um eine Massenüberwachung handelt.[562] Zudem griff die GovWare nicht nur Fernmeldedaten, sondern auch lokal gespeicherte Daten ab (*historical data collection*). Dementsprechend liegt eine zweckwidrige geheime Online-Durchsuchung vor. Im Ergebnis sprengt dieses Vorgehen sowohl in quantitativer Hinsicht (Massenüberwachung) als auch qualitativer Hinsicht (Zugriff auf gespeicherte Daten) den gesetzlichen Rahmen. Insofern handelt es sich somit nicht um einen (rechtswidrigen) GovWare-Einsatz i.S.v. Art. 269ter StPO, sondern um eine der StPO völlig fremde Massnahme.

3. SkyECC

a) Provokation der Zugangsdaten als IMSI-Catcher i.S.v. Art. 269bis StPO?

Zu beurteilen ist, ob sich die SkyECC-Überwachung in das schweizerische Strafverfahrensrecht einordnen lässt. Gemäss Arbeitshypothese wurden die kryptographischen Schlüssel erhältlich gemacht, indem der MITM-Server die einzelnen Endgeräte kontaktierte. Diese Vorgehensweise gleicht insofern einem IMSI-Catcher gemäss Art. 269bis StPO, als sich der MITM-Server als legitime Kommunikations-Gegenstelle ausgab. Allerdings kann ein technisches Gerät i.S.v. Art. 269bis StPO lediglich zum Mithören und Aufnehmen von *Gesprächen* eingesetzt werden. Der Abgriff von *Textnachrichten* oder deren Zu-

559 Siehe vorstehend J.II.3.c).
560 Siehe vorstehend J.II.3.b).
561 Siehe vorstehend A.I.6.d).
562 Siehe vorstehend H.II.1.

gangsdaten ist hingegen nicht vom gesetzlichen Zweck gedeckt.[563] Somit lässt sich das vorliegende Vorgehen nicht auf Art. 269bis StPO stützen.

b) Provokation der Zugangsdaten als GovWare i.S.v. Art. 269ter StPO?

Eine weitere Art, den Fernmeldeverkehr zu überwachen, ist der GovWare-Einsatz nach Art. 269ter StPO. Bei dieser Massnahme wird ein *Informatikprogramm* in ein Datenverarbeitungssystem eingeschleust, welches den *Inhalt* der Kommunikation unverschlüsselt ausleitet.

Die vorliegende Vorgehensweise entspricht jedoch nicht dieser Massnahmenstruktur. *Erstens* erfolgte die Preisgabe der Zugangsdaten über das heimliche Kontaktieren der Endgeräte, nicht aber über das heimliche Aufspielen eines Programmes. *Zweitens* stellt Art. 269ter StPO lediglich eine Grundlage für den Zugriff auf unverschlüsselte Inhaltsdaten, nicht aber für den Zugriff auf die kryptographischen Elemente dar. Eine GovWare darf lediglich zur Umgehung der Verschlüsselung, nicht aber zur Entschlüsselung eingesetzt werden.[564] Aus diesen Gründen fällt auch eine Massnahme i.S.v. Art. 269ter StPO ausser Betracht.

c) Provokation der Zugangsdaten als geheime Online-Recherche?

Daten auf einem Datenträger können ferner über eine Online-Recherche gesichtet werden. Dabei handelt es sich bei einer Online-Recherche um eine Art der Durchsuchung.[565] Dementsprechend ist eine Online-Recherche als *offene* Zwangsmassnahme ausgestaltet, sodass der betroffenen Person das rechtliche Gehör (Art. 247 ff. StPO) zukommt.[566] Auch offene Zwangsmassnahmen können indes unter einstweiliger Geheimhaltung erfolgen. In diesem Fall ist jedoch das rechtliche Gehör nachzuholen oder zu kompensieren.[567] Neben der Offenheit der Massnahme charakterisiert sich eine Online-Recherche dadurch, dass der Zugriff auf Fernmeldedaten ausgeschlossen ist.[568]

563 Hansjakob, Überwachungsrecht, N 543; ferner vorstehend J.II.2.
564 Hansjakob, Überwachungsrecht, N 589.
565 Vgl. BGE 143 IV 270, E. 7.4.
566 Siehe vorstehend J.II.4.c).
567 Siehe vorstehend J.II.4.c).
568 Siehe vorstehend J.II.4.b).

Vorliegend hatte der Nutzer zu keinem Zeitpunkt Kenntnis von der Kontaktierung durch den MITM-Server und der Preisgabe der Zugangsdaten. Das fehlende rechtliche Gehör wurde weder nachgeholt noch von Amtes wegen berücksichtigt. Eine Benachrichtigung unterblieb selbst nach Beendigung der Massnahme. Zweifelsfrei handelte es sich somit nicht um eine offene Massnahme, die einstweilen geheim gehalten wurde, sondern um eine gänzlich geheime Massnahme. Aufgrund des geheimen Charakters lässt sich das Vorgehen nicht als Online-Durchsuchung qualifizieren. Im Übrigen wäre eine Online-Recherche aufgrund der akzessorischen Geltung des Fernmeldegeheimnisses ausgeschlossen.[569]

d) Provokation der Zugangsdaten als unbekannte Massnahme

Im Ergebnis lässt sich das vorliegende Provozieren der Zugangsdaten nicht im Massnahmenkatalog von Art. 269 ff. StPO einordnen. Ebenso fällt eine Qualifizierung als Online-Recherche ausser Betracht. Dementsprechend handelt es sich aus strafprozessualer Sicht um eine unbekannte Massnahme.

4. Anom

Die Arbeitshypothese bei Anom lautet, dass die Anom-Geräte eine heimliche, vom Betreiber (FBI) vorgesehene Ausleitungsfunktion hatten. Diese Täuschung über die Integrität des Kommunikationsgeräts bewirkt, dass ein Eingriff in das Fernmeldegeheimnis vorliegt.[570] Nach der Konzeption der StPO ist die Überwachung des Fernmeldeverkehrs abschliessend in Art. 269 ff. StPO geregelt. Der Massnahmenkatalog sieht das Distribuieren von Kommunikationsgeräten mit verdeckter Überwachungsfunktion jedoch nicht vor. Namentlich können die Anom-Geräte nicht als technisches Gerät i.S.v. Art. 269bis StPO qualifiziert werden, da diese Bestimmung keinen Zugriff auf Textnachrichten zulässt.[571] Somit handelt es sich aus strafprozessualer Sicht um eine unbekannte Massnahme.

569 Siehe vorstehend I.II.2.c).
570 Vgl. RÜCKERT, S. 73 und 76 und 109.
571 Siehe vorstehend J.II.2.

V. Sicherheitsrechtliche Würdigung

1. Präventiv-polizeirechtliche Bewertung

Die vorliegenden Überwachungen haben nicht zuletzt wegen ihrer Verdachtsunabhängigkeit präventiv-polizeirechtliche Elemente.[572] Insofern bietet es sich an, die Massnahmen im Lichte des (kantonalen) Polizeirechts typologisch zu bewerten.[573] Allerdings kann das kantonale Polizeirecht – wie vorstehend dargelegt – nur organisatorische Ausführungsbestimmungen zur Personensuche nach Art. 35 f. BÜPF enthalten.[574] Folglich entfällt eine typologische Einordnung der vorliegenden Massnahmen in das kantonale Polizeirecht.

2. Nachrichtendienstliche Bewertung (Art. 26 NDG)

Verdachtsunabhängige Massnahmen können auch nachrichtendienstlicher Natur sein. Das NDG erlaubt namentlich das Eindringen in ein Computersystem, um dort vorhandene Informationen zu beschaffen (Art. 26 Abs. 1 lit. d Ziff. 1 NDG).

Hinsichtlich *SkyECC* lautet die Arbeitshypothese, dass der MITM-Server die Endgeräte kontaktierte, woraufhin diese die privaten Schlüssel preisgaben. Diese privaten Schlüssel stellen Informationen dar, die im Computersystem *vorhanden* waren. Sofern dieser Vorgang unter Ausnutzung einer Sicherheitslücke erfolgte, liegt auch ein *Eindringen* in ein Computersystem vor.[575] Insofern weist die Provokation der Zugangsdaten typologisch Ähnlichkeiten mit einer Massnahme i.S.v. Art. 26 Abs. 1 lit. d Ziff. 1 NDG auf.[576]

Allerdings wurde vorstehend dargelegt, dass es sich bei den Massnahmen nach Art. 26 NDG um Massnahmen handelt, die sich gegen einzelne Personen richten.[577] *Massenüberwachungen* sind hingegen nur im Rahmen der Funk- und Ka-

572 Siehe vorstehend G.IV.

573 Vgl. GRAF, Verwertbarkeit, S. 536 f.

574 Siehe vorstehend J.I. und III.1.

575 Das Ausnutzen von Sicherheitslücken stellt zumindest im Kontext von Art. 143bis StGB ein «Eindringen» dar, siehe dazu BSK StGB II-WEISSENBERGER, N 17 zu Art 143bis.

576 Gleiches gilt für die EncroChat-Überwachung; die Variante von Art. 26 Abs. 1 lit. a^{bis} NDG (Einsatz besonderer technischer Geräte) ist unpassend, da das «Erfassen» nach der hier vertretenen Ansicht keine Grundlage für aktive Einwirkungen auf ein Datenverarbeitungssystem darstellt.

577 Siehe vorstehend J.III.3.b).

belaufklärung nach Art. 38 f. NDG möglich.[578] Von der SkyECC-Überwachung waren etwa 70'000 Geräte betroffen. Der MITM-Server kontaktierte sämtliche Geräte, die sich mit ihm in Verbindung setzten.[579] Aufgrund dieser Streubreite handelt es sich um eine Massenüberwachung[580], die sich keinesfalls in Art. 26 NDG einsortieren lässt.

3. Exkurs: Unverwertbarkeit von sicherheitsrechtlichen Informationen

In diesem Kapitel geht es um die typologische Einordnung der Massnahmen, nicht um deren Verwertbarkeitsbeurteilung. Im Sinne eines Exkurses sei allerdings daran erinnert, dass eine sicherheitsrechtlich erhobene Information strafprozessual nur verwertet werden kann, wenn das Strafverfahrensrecht eine Parallelmassnahme kennt.[581] Dementsprechend wäre selbst eine allfällige typologische Einordnung der Überwachungsmassnahmen in Art. 26 NDG insofern unbehilflich, als keine strafprozessuale Parallelmassnahme besteht.

VI. Kapitelzusammenfassung

In diesem Kapitel wurde ein Überblick über das schweizerische Überwachungsrecht gegeben.

Da die vorliegenden Massnahmen von ausländischen Behörden durchgeführt wurden, sind die schweizerischen Rechtsgrundlagen nicht einschlägig. Nichtsdestotrotz ist das schweizerische Recht örtlich anwendbar und die Massnahmen somit typologisch in dieses einzuordnen.

Bei einer strafprozessualen Beurteilung findet zwar die *EncroChat*-Überwachung in Art. 269ter StPO einen Anknüpfungspunkt. Allerdings verlässt die Massnahme in quantitativer und qualitativer Hinsicht den gesetzlichen Rahmen derart, dass es sich nicht mehr um die gesetzlich vorgesehene Massnahme handelt. Dagegen sind die *SkyECC*- und *Anom*-Überwachungen ohne jeglichen Anknüpfungspunkt in der StPO.

Ausserhalb des Strafverfahrens kann der Fernmeldeverkehr sicherheitsrechtlich überwacht werden. Während das kantonale Polizeirecht lediglich Ausfüh-

578 Siehe vorstehend H.I.3.
579 Siehe vorstehend A.II.5.
580 Siehe vorstehend H.II.1.
581 Siehe vorstehend C.III.

rungsbestimmungen zur Personensuche nach Art. 35 f. BÜPF enthalten kann, sieht das NDG Massnahmen vor, die deutlich über die strafprozessualen Möglichkeiten hinausgehen (vgl. Art. 26 und 38 f. NDG). Dies zeigt sich namentlich im Kontext von SkyECC. Die Provokation der Zugangsdaten weist typologische Ähnlichkeiten mit einer Massnahme nach Art. 26 Abs. 1 lit. d NDG auf. Allerdings sind auch die Massnahmen nach Art. 26 NDG als zielgerichtete Massnahmen konzipiert. Aufgrund der enormen Streubreite lässt sich die MITM-Kontaktierung dementsprechend dort nicht einordnen.

VII. Die Massnahmen als hybride Überwachungsmassnahmen

In den vorstehenden Kapiteln wurden die Massnahmen aus unterschiedlichen Perspektiven betrachtet. Dabei zeigt sich, dass sie Merkmale mehrerer Regelungsbereiche aufweisen, sodass es sich um *Mischformen* handelt. Als verdachtsunabhängige Massnahmen, die der Kriminalitätsbekämpfung dienen, sind sie zunächst *systematisch* dem Polizeirecht zuzuordnen. Da die Überwachung tausende, nicht im Vorhinein bestimmbare Personen betraf, lassen sich die Massnahmen als Massenüberwachungen bewerten. Dies rückt die Massnahmen *strukturell* in die Nähe der nachrichtendienstlichen Überwachung. Auch die Vorgehensweise erinnert namentlich bei SkyECC typologisch an nachrichtendienstrechtliche Überwachungen (vgl. Art. 26 Abs. 1 lit. d Ziff. 1 NDG). *Funktional* betrachtet handelt es sich jedoch um strafprozessuale Massnahmen, da es sich um Fernmeldeüberwachungen zwecks Strafverfolgung handelt.

Wie nachfolgend jedoch zu zeigen bleibt, ähneln sich die formellen Anforderungen sämtlicher Fernmeldeüberwachungen. Insofern ist es letztlich für die Verwertbarkeitsbeurteilung nicht entscheidend, ob an die strafprozessuale, polizeirechtliche oder nachrichtendienstliche Rechtsnatur der Massnahmen angeknüpft wird.

K. Anforderungen an Fernmeldeüberwachungen

I. Verfassungsrechtliche Anforderungen

Das vorstehende Kapitel hat gezeigt, dass es schwerfällt, die Massnahmen in die schweizerische Rechtssystematik einzuordnen. Vor diesem Hintergrund werden im hiesigen Kapitel allgemeine Anforderungen, die für sämtliche Fernmeldeüberwachungen gelten, herausgearbeitet. Ein wesentlicher Bezugspunkt ist dabei das Verfassungsrecht, welches für alle Fernmeldeüberwachungen gilt. Von Verfassungs wegen geniesst das Fernmeldegeheimnis einen besonderen Schutz (Art. 13 Abs. 1 BV). Folglich hat eine Überwachung des Fernmeldeverkehrs verfassungsmässigen Anforderungen zu entsprechen. Namentlich sind die Erfordernisse der gesetzlichen Grundlage, des öffentlichen Interesses und der Verhältnismässigkeit zu beachten (Art. 36 BV). Der bundesgerichtlichen Rechtsprechung sind folgende Konkretisierungen dieser Grundsätze zu entnehmen[582]:

- Eine Überwachung ist nur zulässig, wenn gewichtige Rechtsgüter in schwerer Weise betroffen sind[583]
- Die Überwachung bedarf einer Genehmigung durch eine Genehmigungsinstanz[584]
- Die Überwachung ist der betroffenen Person nachträglich mitzuteilen[585]
- Der betroffenen Person muss die Möglichkeit offenstehen, die Rechtmässigkeit der Überwachung bei einer Beschwerdeinstanz überprüfen zu lassen[586]
- Die vorstehenden Voraussetzungen sind im Gesetz selbst zu regeln[587]

582 Vgl. BGE 140 I 353, E. 5.2. und 8.8.

583 Vgl. BGE 140 I 353, E. 8.7.2., wonach eine präventiv-polizeiliche Überwachung nur zur Verhinderung schwerwiegender Gefahr zulässig ist.

584 BGE 140 I 353, E. 8.7.2.3 ff.; vgl. auch BGE 109 Ia 273, E. 10.

585 BGE 140 I 353, E. 8.7.2.3 ff.

586 BGE 140 I 353, E. 8.7.2.3 ff.

587 BGE 140 I 353, E. 8.7.2.5.

II. Anforderungen an eine strafprozessuale Fernmeldeüberwachung

1. Allgemeine Voraussetzungen für Zwangsmassnahmen

Neben den verfassungsmässigen Vorgaben sind im strafprozessualen Kontext die Massgaben der StPO zu beachten. Die StPO bezeichnet grundrechtsinvasive Massnahmen als Zwangsmassnahmen (Art. 196 Abs. 1 StPO). Nach Art. 197 Abs. 1 StPO ist eine Zwangsmassnahme im Allgemeinen zulässig, wenn

- sie gesetzlich vorgesehen ist (lit. a);
- ein hinreichender Tatverdacht vorliegt (lit. b);
- die angestrebten Ziele nicht durch mildere Massnahmen erreicht werden können (lit. c);
- die Bedeutung der Straftat die Massnahme rechtfertigt (lit. d).

2. Strafprozessuale Voraussetzungen für die Fernmeldeüberwachung

Das Strafprozessrecht stellt in Art. 269 ff. StPO den Strafverfolgungsbehörden verschiedene Instrumente für die Fernmeldeüberwachung zur Verfügung. Art. 269 StPO normiert die *konventionelle Überwachung*, Art. 269bis StPO den Einsatz eines *IMSI-Catchers* und Art. 269ter StPO den *GovWare*-Einsatz. Diese Massnahmen haben jeweils spezifische Anordnungsvoraussetzungen. Nichtsdestotrotz sind ihnen folgende Erfordernisse gemeinsam:[588]

- Dringender Tatverdacht
- Vorliegen einer Katalogtat (wobei die Kataloge nicht deckungsgleich sind[589])
- Anordnung durch eine Staatsanwaltschaft
- Genehmigung durch ein Zwangsmassnahmengericht

[588] Art. 269bis Abs. 1 lit. a und Art. 269ter Abs. 1 lit. a StPO verweisen auf die Voraussetzungen nach Art. 269 StPO.

[589] Bei Massnahmen nach Art. 269 StPO und Art. 269bis StPO richtet sich der Katalog nach Art. 269 Abs. 2 StPO; bei Massnahmen i.S.v. Art. 269ter StPO richtet sich der Katalog hingegen nach Art. 286 Abs. 2 StPO.

– Subsidiarität (unterschiedliche Subsidiaritätsgrade zwischen den Massnahmen[590])

Ferner gleichen sich die Massnahmen darin, dass sie der betroffenen Person nachträglich mitzuteilen sind und dieser ein Beschwerdeweg offensteht (Art. 279 und Art. 393 StPO).

III. Anforderungen an ausserstrafprozessuale Fernmeldeüberwachungen

Die formellen Voraussetzungen der ausserstrafprozessualen Fernmeldeüberwachungen weisen grosse Ähnlichkeit mit den strafprozessualen Voraussetzungen auf. Dies wird anhand des folgenden Abrisses dargelegt:

Ausserhalb des Strafverfahrens kann eine Fernmeldeüberwachung namentlich zwecks Personensuche (Art. 35 f. BÜPF) durchgeführt werden. Hinsichtlich des Verfahrens verweist Art. 37 Abs. 1 BÜPF weitgehend auf die strafprozessualen Bestimmungen. Dieser Verweis auf die StPO gilt für das Genehmigungsverfahren, das Mitteilungsverfahren[591], eine allfällige Ausnahme der Mitteilung und den Beschwerdeweg (Art. 37 Abs. 1 BÜPF).[592]

Ähnliches gilt für die rechtshilfeweise Überwachung, deren Bestimmung ebenfalls auf die StPO verweist (Art. 18a Abs. 4 IRSG i.V.m. Art. 269-279 StPO). Für das richterliche Genehmigungsverfahren sieht Art. 18a Abs. 2 IRSG eine spezifische Zuständigkeitsordnung vor. Ansonsten richten sich die Genehmigungsmodalitäten und die Mitteilung nach der StPO (Art. 18a Abs. 4 IRSG i.V.m. Art. 279 StPO).[593] Hinsichtlich der Beschwerde besteht Uneinigkeit, ob der betroffenen Person der Beschwerdeweg nach StPO oder IRSG zur Verfügung steht.[594]

Einzig die nachrichtendienstliche Überwachung kommt ohne Verweis auf die StPO aus.[595] Die formelle Grundstruktur ist jedoch mit der strafprozessualen

590 Massnahmen nach Art. 269bis und Art. 269ter StPO sind subsidiär zu den Massnahmen nach Art. 269 StPO.

591 Die Mitteilung hat im Falle der Notsuche gemäss Art. 37 Abs. 2 BÜPF so bald als möglich zu erfolgen; im Falle der Fahndung nach einer verurteilten Person hat die Mitteilung kurz nach der Festnahme zu erfolgen, siehe dazu Hansjakob, Überwachungsrecht, N 1797.

592 Hansjakob, Überwachungsrecht, N 1795 ff.

593 Vgl. BSK IRSG-Aepli, N 30 ff. zu Art. 18a IRSG.

594 Siehe dazu BSK IRSG-Aepli, N 44 ff.; PC IRSG-Ludwiczak Glassey, N 13 zu Art. 18a.

595 Eine nachrichtendienstliche Überwachung ist zulässig, wenn eine konkrete Bedrohung hinsichtlich eines Katalogdelikts i.S.v. Art. 19 Abs. 2 lit. a-d NDG vorliegt (Art. 27 Abs. 1 lit. a NDG).

vergleichbar: Die Überwachung bedarf einer richterlichen Genehmigung (durch das Bundesverwaltungsgericht; zudem ist die Zustimmung des Vorstehers des VBS erforderlich, vgl. Art. 27 Abs. 2 NDG). Der überwachten Person ist nach Beendigung der Massnahme die Überwachung mitzuteilen (Art. 33 Abs. 1 NDG), wobei unter gewissen Umständen die Mitteilung mit Genehmigung des Bundesverwaltungsgerichts aufgeschoben oder unterlassen werden kann (Art. 33 Abs. 2 und 3 NDG). Die betroffene Person kann anschliessend beim Bundesverwaltungsgericht Beschwerde gegen die Überwachung führen (Art. 83 Abs. 1 NDG).

IV. Kapitelzusammenfassung

Aus dem Vorstehenden geht hervor, dass die verschiedenen Fernmeldeüberwachungen des schweizerischen Rechts – ob strafprozessual oder ausserstrafprozessual – starke formelle Ähnlichkeiten aufweisen. Sämtliche Fernmeldeüberwachungen bedürfen einer gesetzlichen Grundlage, einer richterlichen Genehmigung, einer nachträglichen Mitteilung und der Bereitstellung eines Beschwerdeweges. In den nachfolgenden Kapiteln wird untersucht, welche Verwertbarkeitsfolgen entstehen, wenn diese formellen Anforderungen nicht eingehalten werden.

L. Massnahmenbezogene Verwertbarkeitsbeurteilung

I. Verletzung des Legalitätsprinzips (Art. 36 BV)

In diesem Kapitel wird erörtert, welche Verwertbarkeitsfolgen sich aus massnahmenbezogenen Mängeln ergeben. Dabei ist zunächst auf das Legalitätsprinzip einzugehen, welches sowohl verfassungsrechtlich als auch strafprozessual normiert ist (Art. 36 Abs. 1 BV und Art. 197 Abs. 1 lit. a StPO).[596]

Nach Ansicht des Bundesgerichts zieht eine aussergesetzliche Massnahme ein relatives Verwertbarkeitsverbot i.S.v. Art. 141 Abs. 2 StPO nach sich.[597] Diese Rechtsprechung bezieht sich auf Grundrechtseingriffe *mittleren* Grades, bei denen öffentlich wahrnehmbare Vorgänge erfasst wurden (etwa eine präventiv-polizeirechtliche automatische Fahrzeugfahndung und Verkehrsüberwachung (AFV)[598] oder eine Observation durch einen Privatdetektiv im Auftrag der Sozialversicherung[599]).

Nach der hier vertretenen Auffassung sollte eine aussergesetzliche Beweiserhebung, die einen *schweren* Grundrechtseingriff darstellt (etwa eine Fernmeldeüberwachung), zu einem absoluten Verwertbarkeitsverbot nach Art. 141 Abs. 1 StPO führen. Insbesondere hat dies zu gelten, wenn die Massnahme von ihrer *Art und Weise* dem Rechtssystem *gänzlich unbekannt* ist. Dies ergibt sich aus dem Umstand, dass schwere Grundrechtseingriffe von Verfassungs wegen im Gesetz selbst vorzusehen sind (Art. 36 Abs. 1 BV). Diese Auslegung spiegelt sich bei einer Fernmeldeüberwachung in Art. 269ter Abs. 3 StPO wider. Gemäss dieser Bestimmung sind Daten, die mittels aussergesetzlicher Funktionen einer GovWare erhoben wurden, absolut unverwertbar. Nach der hiesigen Auffassung ist diese Norm nur deklaratorischer Ausdruck dessen, dass sämtliche aussergesetzlichen Überwachungen des Fernmeldeverkehrs absolut unverwertbar sind.

---

596 BSK StPO II-Weber, N 4 zu Art. 197; die gesetzliche Grundlage wird in der Praxis teils äusserst extensiv ausgelegt, beispielsweise BGE 137 IV 340, E. 5.4, wonach ein Antennensuchlauf ein «nicht ausdrücklich» geregelter Spezialfall der rückwirkenden Randdatenerhebung gemäss Art. 273 StPO sei.

597 BGE 146 I 11, E. 4.2 f.

598 BGE 146 I 11.

599 BGer 6B_1311/2017 vom 23. August 2018, E. 2.3.

II. Verletzung der Genehmigungspflicht (Art. 13 BV und Art. 277 StPO)

Der Genehmigungsvorbehalt ist eine verfassungsrechtliche Anforderung an eine Kommunikationsüberwachung. Nach dem Bundesgericht sollte die Genehmigungsinstanz von Verfassungs wegen grundsätzlich aus einer richterlichen Behörde bestehen.[600] Eine Genehmigung soll eine wirksame Überprüfung der Rechtmässigkeit der Überwachung gewährleisten.[601] Vor diesem Hintergrund kann allein ein Schweizer Zwangsmassnahmengericht – nicht aber eine ausländische Instanz – eine entsprechende Genehmigung erteilen.[602]

Der Genehmigungsvorbehalt ist sowohl bei den strafprozessualen (Art. 272 Abs. 1 StPO) als auch bei den ausserstrafprozessualen Fernmeldeüberwachungen nach BÜPF[603], IRSG[604] und NDG[605] gesetzlich vorgesehen. Der Genehmigungsvorbehalt kennt weder verfassungsrechtliche noch gesetzliche Ausnahmen. Somit handelt es sich um eine Voraussetzung, die uneingeschränkt Geltung beansprucht.

Die Verwertbarkeitsfolge einer nicht genehmigten Überwachung ist vom Strafprozessrecht vorgegeben. Erfolgt eine strafprozessuale Überwachung ohne die erforderliche Genehmigung, so sind deren Ergebnisse von Gesetzes wegen *absolut unverwertbar* (Art. 277 Abs. 2 i.V.m. Art. 141 Abs. 1 StPO). Diese Verwertbarkeitsfolge gilt selbstverständlich auch für nicht genehmigte Überwachungen ausserhalb des Strafverfahrens (nach IRSG, BÜPF, NDG), deren Erkenntnisse in ein Strafverfahren gelangen. Dies ergibt sich aus der Überlegung, dass die strafprozessuale Verwertbarkeit von Erkenntnissen abschliessend von der StPO geregelt wird.[606]

600 BGE 140 I 353, E. 8.7.2.3 ff.
601 Vgl. BGE 140 I 353, E. 8.7.2.4.
602 Siehe vorstehend E.V.
603 Art. 37 Abs. 1 BÜPF i.V.m. Art. 272 Abs. 1 StPO
604 Art. 18a Abs. 3 IRSG.
605 Art. 26 Abs. 1 und Art. 27 Abs. 1 NDG.
606 Im Übrigen verweisen das BÜPF und das IRSG auf Art. 279 StPO, siehe Art. 37 Abs. 1 BÜPF und Art. 18a Abs. 4 IRSG.

III. Verletzung des Täuschungsverbots (Art. 141 Abs. 1 StPO)

Fernmeldeüberwachungen haben stets eine täuschende Komponente. Vor diesem Hintergrund lohnt es sich, das Täuschungsverbot von Art. 140 Abs. 1 StPO zu betrachten, welches ein absolutes Verwertbarkeitsverbot nach sich zieht (Art. 141 Abs. 1 StPO).

Eine Täuschung liegt vor, wenn die Behörden bei der betroffenen Person einen Irrtum hervorrufen[607], also eine Diskrepanz zwischen Vorstellung und Wirklichkeit bewirken[608]. Eine Täuschung ist stets zulässig, wenn sie gesetzlich vorgesehen ist (etwa bei der verdeckten Ermittlung nach Art. 285a ff. StPO oder bei der verdeckten Fahndung nach Art. 298 ff. StPO).

Ausserhalb der gesetzlich vorgesehenen Täuschungen ist die Abgrenzung zwischen der verpönten Täuschung und der zulässigen List aufgrund der spezifischen Umstände zu treffen.[609] Nach einem Teil der Literatur greift das Täuschungsverbot lediglich, wenn die Täuschung auf einem ausdrücklichen oder konkludenten *Kommunikationsprozess* basiert.[610] Vom Täuschungsverbot erfasst sind demnach Täuschungen, die über die Einwirkung auf die Vorstellung herbeigeführt werden. Nicht vom Täuschungsverbot umfasst sind demnach jene Täuschungen, die über die Änderung der Wirklichkeit (aber ohne Kommunikationsprozess) erfolgen.[611] Das Bundesgericht unterstellt auch *nicht kommunikative* Täuschungen unter das Täuschungsverbot (Wanze in Gefängnisräumlichkeiten), ohne sich ausdrücklich mit dieser Frage auseinandergesetzt zu haben.[612]

Zumindest in Bezug auf eine Fernmeldeüberwachung sollte der ersten Auffassung gefolgt und auf den Kommunikationsvorgang abgestellt werden. Bei einer Fernmeldeüberwachung rufen die Behörden stets einen Irrtum über

607 BGE 144 IV 23, E. 4.2.

608 MIESCHER, S. 6.

609 BGE 144 IV 23, E. 4.2.

610 MIESCHER, S. 6 f. und S. 139; SK StPO I-WOHLERS, N 10.

611 Vgl. MIESCHER, S. 139; zur Veranschaulichung dieser Unterscheidung verwendet MIESCHER, S. 6 f. das Standardbeispiel vom blinden Passagier. Schleicht sich ein blinder Passagier auf ein Schiff, ohne dass der Kapitän dies merkt, so hat der blinde Passagier die Wirklichkeit verändert. Verkleidet sich der blinde Passagier hingegen als Matrose und stellt sich so dem Kapitän vor, verändert dieser die Vorstellung des Kapitäns in einem Kommunikationsvorgang.

612 Vgl. BGE 144 IV 233, E. 4.2.

die Vertraulichkeit der Kommunikation hervor.[613] Würde bereits dieser Irrtum als relevante Täuschung bezeichnet werden, so griffe das Täuschungsverbot stets, wenn die Fernmeldeüberwachung den gesetzlichen Vorgaben nicht entspricht. Nach der hier vertretenen Ansicht ist dies aber primär eine legalitätsrechtliche Problematik. Anders ist hingegen der Fall gelagert, wenn eine Fernmeldeüberwachung nicht Art. 269 ff. StPO entspricht und zusätzlich eine kommunikative Täuschung von Seiten der Behörden vorliegt. In diesem Fall bekommt das Täuschungsverbot einen eigenständigen Gehalt. Dementsprechend wird nachstehend lediglich die Anom-Überwachung im Hinblick auf das Täuschungsverbot geprüft. Im Gegensatz zu den EncroChat- und SkyECC-Überwachungen – die rein technischer Natur waren – basiert die Anom-Überwachung nämlich auf einer kommunikativen Täuschung.

IV. Verwertbarkeitsbeurteilung in casu

1. Verletzung des Legalitätsprinzips / Territorialitätsrecht?

Bei den vorliegenden Massnahmen handelt es sich um Überwachungen ausländischer Behörden. Auf die Ermächtigungsgrundlagen des schweizerischen Rechts können sich jedoch allein die Schweizer Behörden berufen. Folglich liegen aus Sicht des schweizerischen Rechts aussergesetzliche Massnahmen vor. Dieser Umstand kann entweder als Verstoss gegen das Legalitätsprinzip oder als territorialitätsrechtliche Problematik berücksichtigt werden. Nach der hier vertretenen Ansicht geht die territorialitätsrechtliche Betrachtung als spezifischere Perspektive vor. Da jedoch beide Betrachtungen zu einem absoluten Verwertbarkeitsverbot führen[614], ist es letztlich nicht von Relevanz, unter welchem Titel dieses Defizit betrachtet wird. Unabhängig von dieser Problematik weisen die Massnahmen im Lichte des schweizerischen Rechts zahlreiche Defizite auf, deren Verwertbarkeitsfolgen nachfolgend dargelegt werden.

613 MIESCHER, S. 54 ff.

614 Siehe L.I. hinsichtlich des Legalitätsprinzips und P.V. hinsichtlich des Territorialitätsprinzips.

2. EncroChat

a) Verletzung des Legalitätsprinzips

Die EncroChat-Überwachung weist funktionelle Ähnlichkeiten mit einem GovWare-Einsatz i.S.v. Art. 269ter StPO auf. Nichtsdestotrotz handelt es sich um eine der StPO typologisch unbekannte Massnahme, da die Massnahme in quantitativer Hinsicht (Massenüberwachung) und qualitativer Hinsicht (geheime Online-Durchsuchung) den gesetzlichen Rahmen sprengt.[615] Da es sich dabei um einen schweren Grundrechtseingriff handelt, folgt nach der hier vertretenen Ansicht daraus ein absolutes Verwertbarkeitsverbot.[616]

b) Verletzung des Richtervorbehaltes

Die EncroChat-Überwachung stellt in der *forward facing collection* einen Eingriff in das Fernmeldegeheimnis dar.[617] Eine Fernmeldeüberwachung bedarf von Verfassungs wegen einer Genehmigung von einer Schweizer Genehmigungsinstanz.[618] Eine allfällige französische richterliche Genehmigung vermag – trotz allfälliger Geltung des Vertrauensprinzips – die Genehmigung einer Schweizer Instanz nicht zu ersetzen.[619] Mangels einer Genehmigung einer Schweizer Genehmigungsinstanz folgt sowohl aus verfassungsrechtlichen als auch gesetzlichen Erwägungen ein *absolutes Verwertbarkeitsverbot* (Art. 277 i.V.m. Art. 141 Abs. 1 StPO).[620]

3. SkyECC

a) Verletzung des Legalitätsprinzips

Gemäss Arbeitshypothese kontaktierte bei der SkyECC-Überwachung ein MITM-Server die Endgeräte, um in diesen die Preisgabe von kryptographischen Schlüsseln auszulösen. Aus strafprozessualer und präventiv-polizei-

615 Siehe vorstehend J.IV.2.b).

616 Siehe vorstehend L.I.; in der historical data collection griff die GovWare auf lokal gespeicherte Daten zu. Dies ist eine geheime Online-Durchsuchung, sodass das gesetzlich vorgesehene, absolute Verwertbarkeitsverbot greift (Art. 269ter Abs. 3 i.V.m. Art. 141 Abs. 1 StPO).

617 Siehe vorstehend I.III.1.b).

618 Vgl. BGE 140 I 353, E. 8.7.2.3 ff.; vgl. auch BGE 109 Ia 273, E. 10.

619 Siehe vorstehend E.V.

620 Siehe vorstehend L.II.

rechtlicher Sicht stellt diese Massnahme eine völlig unbekannte Form der Fernmeldeüberwachung dar.[621] Trotz gewisser Ähnlichkeiten handelt es sich auch aus nachrichtendienstrechtlicher Perspektive[622] um eine typologisch unbekannte Massnahme.[623] Somit lässt sich die Massnahme nicht in das schweizerische Recht einordnen. Aufgrund des schweren Grundrechtseingriffes folgt daraus nach der hier vertretenen Ansicht ein *absolutes* Verwertbarkeitsverbot.[624]

b) Verletzung des Richtervorbehaltes

Die vorliegende Provokation der Zugangsdaten stellt aufgrund der akzessorischen Betrachtung einen Eingriff in das Fernmeldegeheimnis dar.[625] Eine Überwachung des Fernmeldeverkehrs bedarf von Verfassungs wegen einer Genehmigung einer Schweizer Genehmigungsinstanz.[626] Die SkyECC-Massnahmen wurden in Frankreich, nicht aber in der Schweiz richterlich genehmigt. Das Vertrauensprinzip kann die erforderliche Genehmigung durch eine Schweizer Genehmigungsinstanz nicht ersetzen.[627] Sowohl aus verfassungsmässigen Erwägungen als auch aus gesetzlichen Vorgaben ergibt sich aus der fehlenden Genehmigung ein *absolutes Verwertbarkeitsverbot* (Art. 277 i.V.m. Art. 141 Abs. 1 StPO).[628]

4. Anom

a) Verletzung des Legalitätsprinzips

Gemäss Arbeitshypothese verfügten die Anom-Geräte über eine heimliche Ausleitungsfunktion, was einen Eingriff in das Fernmeldegeheimnis darstellt.[629] Diese Massnahme ist dem schweizerischen Recht von ihrer Struktur her jedoch gänzlich unbekannt.[630] Da es sich um einen schweren Grundrechts-

621 Siehe vorstehend J.IV.3.d) und J.V.1.
622 Vgl. Art. 26 Abs. 1 lit. d Ziff. 1 NDG.
623 Siehe vorstehend J.V.2.
624 Siehe vorstehend L.I.
625 Siehe vorstehend I.III.2.c).
626 Vgl. BGE 140 I 353, E. 8.7.2.3 ff.; ferner BGE 109 Ia 273, E. 10.
627 Siehe vorstehend E.V.
628 Siehe vorstehend L.II.
629 Siehe vorstehend I.III.3.
630 Siehe vorstehend J.IV.4. und V.

eingriff ohne Rechtsgrundlage handelt, folgt nach der hier vertretenen Auffassung ein *absolutes* Verwertbarkeitsverbot.[631]

b) Verletzung des Richtervorbehaltes

Eingriffe in das Fernmeldegeheimnis stehen unter dem Vorbehalt einer Genehmigung durch eine Schweizer Genehmigungsinstanz. Dieses Erfordernis ergibt sich bei einer aussergesetzlichen Massnahme direkt aus Art. 13 Abs. 1 BV.[632] Vorliegend ist aufgrund der fehlenden Anwendbarkeit des Vertrauensprinzips eine allfällige ausländische richterliche Genehmigung als inexistent zu erachten.[633] Selbst wenn eine solche vorläge, ersetzte diese keinesfalls die Genehmigung einer Schweizer Genehmigungsinstanz.[634] Mangels Genehmigung einer Schweizer Instanz sind die Daten *absolut unverwertbar* (Art. 277 i.V.m. Art. 141 Abs. 1 StPO).[635]

c) Verletzung des Täuschungsverbots

Im Rahmen der Anom-Überwachung führten die amerikanischen Strafverfolgungsbehörden eine angeblich private Scheinfirma in Panama. Über verdeckte Ermittler wurden die Endgeräte anschliessend in den Umlauf gebracht. Darüber hinaus verfügten die Geräte über zahlreiche speziell auf Datensicherheit ausgerichtete Funktionen. Diese Machenschaften sind als konkludenter Kommunikationsvorgang zu bewerten, der bei den Käufern die Vorstellung hervorrufen sollte, ein äusserst sicheres Kommunikationsgerät zu erwerben.[636] Anstatt eine abhörsichere Kommunikation zu ermöglichen, verfügten die Geräte über eine heimliche Ausleitungsfunktion.[637] Da somit durch eine konkludente Kommunikation eine Diskrepanz zwischen Vorstellung und Wirklichkeit hervorgerufen wurde, liegt eine unzulässige Täuschung vor.

Zwar könnte eingewendet werden, dass die Täuschung nicht durch Schweizer, sondern durch ausländische Behörden bewirkt wurde. Allerdings ist nach der hier vertretenen Ansicht jede heimliche Datenausleitung eine Manifestation der Täuschung, da sich der Nutzer nach wie vor im Irrtum über die Vertrau-

631 Siehe vorstehend L.I.
632 Vgl. BGE 140 I 353, E. 8.7.2.3 ff.; ferner BGE 109 Ia 273, E. 10.
633 Siehe vorstehend E.VI.5.
634 Siehe vorstehend E.V.
635 Siehe vorstehend L.II.
636 Zu den Funktionen und Vertriebsumstände hinsichtlich der Anom-Geräte siehe vorstehend A.III.
637 Siehe vorstehend A.III.3.

lichkeit der Kommunikation befindet. Sofern sich der Nutzer zum Zeitpunkt der Datenausleitung in der Schweiz befand, ist das schweizerische Recht anwendbar, sodass das Täuschungsverbot von Art. 140 StPO greift. Was den inländischen Behörden rechtlich versagt ist, kann den ausländischen Behörden nicht gestattet sein. Infolgedessen sind die von der Schweiz aus versendeten Nachrichten absolut unverwertbar (Art. 141 Abs. 1 StPO).

V. Verwertbarkeit bei transnationaler Kommunikation

Bei einer transnationalen Kommunikation ist ein Teil der Überwachungsmassnahme jeweils in einem anderen Staat zu lokalisieren. Grundsätzlich hätten die Strafverfolgungsbehörden in diesem Fall festzustellen, in welchem Staat die jeweilige Nachrichtenausleitung/Schlüsselpreisgabe stattgefunden hat. Anschliessend wäre die Massnahme nach dem einschlägigen drittstaatlichen Recht zu würdigen.

Allerdings sind die vorliegenden Darstellungen zur Vorgehensweise lediglich *Arbeitshypothesen*.[638] Dementsprechend ist nicht rechtsgenügend erstellt, in welchem Endgerät die Nachrichtenausleitung/Schlüsselpreisgabe stattgefunden hat.[639] Gemäss dem Grundsatz *in dubio pro reo* ist somit die gesamte Kommunikation – unabhängig vom Aufenthaltsstaat des Chatpartners – als bemakelt zu erachten und diese *in toto* absolut unverwertbar.

638 Siehe vorstehend E.VI.1.

639 Im Kontext von EncroChat ist ferner nicht bestimmbar, aus welchem Endgerät die Nachricht ausgeleitet wurde, da die Schadsoftware sowohl die versandten als auch die empfangenen Nachrichten ausleitete.

M. Die Überwachungsmassnahmen und der nachträgliche Rechtsschutz

I. Die Rechtsweggarantie nach Art. 29a BV

Vorstehend wurden die Mängel, die sich aus der Durchführung der Überwachungsmassnahmen ergeben, beleuchtet. Allerdings sind auch nach Durchführung einer Überwachung die rechtsstaatlichen Garantien der nachträglichen Mitteilung und der Bereitstellung eines Beschwerdewegs zu beachten. Da diese Garantien vorliegend nicht eingehalten wurden, ist auf diese Garantien genauer einzugehen.

Die Rechtsweggarantie verleiht den Anspruch, eine Rechtsstreitigkeit durch eine *richterliche* Behörde beurteilen zu lassen (Art. 29a Abs. 1 BV). In Bezug auf eine Fernmeldeüberwachung leiten sich daraus zwei behördliche Pflichten ab. Zum einen ist die Strafverfolgungsbehörde von Verfassungs wegen verpflichtet, der betroffenen Person die Überwachung nachträglich mitzuteilen.[640] Zum anderen besteht die verfassungsrechtliche Pflicht, der betroffenen Person einen Beschwerdeweg zur Verfügung zu stellen.[641]

Die Mitteilungspflicht und Beschwerdemöglichkeit weisen einen starken inneren Zusammenhang auf, was sich daran zeigt, dass der Erhalt der Mitteilung die Beschwerdefrist auslöst (Art. 279 Abs. 3 StPO). Da jedoch auch gewisse Unterschiede bestehen (namentlich hinsichtlich der Einschränkung), werden sie nachfolgend separat dargelegt.

640 BGE 140 I 353, E. 8.7.2.4; BGE 109 Ia 273, E. 12.

641 Vgl. BGE 140 I 353, E. 8.7.2.3 ff.

II. Mitteilungspflicht

1. Mitteilung als verfahrensrechtliche Obliegenheit

a) Mitteilungspflicht und Mitteilungsmodalitäten gemäss StPO

Eine Fernmeldeüberwachung ist der betroffenen Person von Verfassungs wegen nachträglich mitzuteilen. Diese Verfassungsvorgabe ist gesetzlich in der StPO verankert. Gemäss Art. 279 Abs. 1 StPO hat die Staatsanwaltschaft der überwachten Person die Überwachung spätestens mit Abschluss des Vorverfahrens mitzuteilen. Diese Mitteilung hat in Form einer formalen Verfügung samt Rechtsmittelbelehrung zu erfolgen.[642] Die Mitteilung hat zumindest über die verdächtige Person, die untersuchten Delikte, die betroffenen Anschlüsse, die Datenart und die Überwachungsdauer Auskunft zu geben.[643] Wird eine überwachte Person – etwa im Rahmen einer Einvernahme – lediglich mit Überwachungsergebnissen konfrontiert, so konstituiert dies keine Mitteilung.[644]

Die Mitteilungspflicht erstreckt sich jedoch nicht auf sämtliche überwachte Personen. Nicht zu informieren sind die Kommunikationspartner der Zielperson, sofern deren Kommunikationsanteile nicht im Strafverfahren verwendet werden.[645]

b) Mitteilungspflicht bei ausserstrafprozessualen Fernmeldeüberwachungen

Bei der Mitteilungspflicht handelt es sich um eine verfassungsmässige Anforderung, weshalb diese für die gesamte Rechtsordnung gilt. Dementsprechend ist die Mitteilungspflicht auch bei den Fernmeldeüberwachungen ausserhalb des Strafverfahrens (nach BÜPF[646], IRSG[647] und NDG[648]) gesetzlich vorgesehen.

642 Vgl. Hansjakob, Überwachungsrecht, N 1258.
643 PK StPO-Jositsch/Schmid, N 5 zu Art. 279; Hansjakob, Überwachungsrecht, N 1242.
644 BGer 1P.15/2003 vom 14. Februar 2003, E. 2.
645 Hansjakob, Überwachungsrecht, N 1237; Drittpersonen i.S.v. Art. 270 lit. b StPO sind aber zu informieren.
646 Vgl. Art. 37 BÜPF i.V.m. Art. 279 StPO.
647 Vgl. Art. 18a Abs. 4 IRSG i.V.m. Art. 279 StPO.
648 Vgl. Art. 33 NDG.

Einzig bei der geheimdienstlichen Funk- und Kabelaufklärung nach Art. 38 f. NDG besteht keine Mitteilungspflicht[649], was durch deren Massnahmenzweck gerechtfertigt wird.[650] Diese Überwachungsformen dienen nicht der umfassenden Überwachung der Individualkommunikation, sondern der Beschaffung sicherheitsrelevanter Informationen im Ausland.[651]

2. Aufschub und Unterlassung der Mitteilung

a) Ausnahmeregelung gemäss StPO

Der Grundsatz der Mitteilungspflicht erfährt gesetzliche Ausnahmen. Nach Art. 279 Abs. 2 StPO kann die Benachrichtigung der betroffenen Person aufgeschoben oder unterlassen werden. In formeller Hinsicht bedarf ein Aufschub der Mitteilung oder deren Verzicht der Zustimmung des *Zwangsmassnahmengerichts* (Art. 279 Abs. 2 StPO). Darüber hinaus dürfen die Erkenntnisse *nicht zu Beweiszwecken* verwendet werden (Art. 279 Abs. 2 lit. a StPO). In materieller Hinsicht bedarf es überwiegender privater oder öffentlicher Interessen (Art. 279 Abs. 2 lit. b StPO). Ein überwiegendes Interesse kann namentlich bei der Bekämpfung organisierter Kriminalität vorliegen.[652] Während ein Verzicht auf eine Mitteilung äusserst restriktiv zu bewilligen ist, sind die Anforderungen an einen Aufschub geringer.[653]

b) Verwertbarkeitsfolge

Das Gesetz sieht für eine richterlich genehmigte Mitteilungsunterlassung eine spezifische Folge vor. Gemäss Art. 279 Abs. 2 lit. a StPO dürfen die Überwachungserkenntnisse bei einer rechtmässigen Mitteilungsunterlassung nicht zu Beweiszwecken verwendet werden. Nach der Auffassung von Métille handelt es sich bei dieser Bestimmung um ein absolutes Verwertbarkeitsverbot.[654] Hansjakob geht grundsätzlich davon aus, dass die Erkenntnisse nicht zum

649 Siehe BVGer A-6444/2020 vom 19. November 2025, E. 5.7.
650 Botschaft NDG, 2171.
651 Botschaft NDG, 2171.
652 Hansjakob, Überwachungsrecht, N 1265.
653 Hansjakob, Überwachungsrecht, N 1227.
654 CR StPO-Métille, N 28 zu Art. 279.

Nachteil des Beschuldigten verwertet werden dürfen.[655] Nach der hier vertretenen Ansicht handelt es sich um ein gesetzlich vorgesehenes, und somit um ein absolutes Verwertbarkeitsverbot (Art. 279 Abs. 2 lit. a StPO i.V.m. Art. 141 Abs. 1 StPO).[656]

Da bereits eine rechtmässig, richterlich genehmigte Mitteilungsunterlassung zu einem absoluten Verwertbarkeitsverbot führt, gilt dies selbstverständlich auch für rechtswidrige, nicht genehmigte Mitteilungsunterlassungen. Dementsprechend spricht Vieles dafür – entgegen der Auffassung von Hansjakob[657] – eine absolute Unverwertbarkeit auch bei einer fahrlässig unterlassenen Mitteilung anzunehmen. Diese Frage muss jedoch an dieser Stelle nicht abschliessend beurteilt werden, da es sich im vorliegenden Kontext nicht um fahrlässige, sondern systematische Mitteilungsunterlassungen handelt.

c) Ausnahmeregelung bei ausserstrafprozessualen Fernmeldeüberwachungen

Die Ausnahme der Mitteilungspflicht gilt auch für die Fernmeldeüberwachungen ausserhalb des Strafverfahrens. Während das BÜPF und das IRSG diesbezüglich auf die StPO verweisen[658], hat das NDG hinsichtlich der Überwachungsmassnahmen nach Art. 26 NDG eine eigenständige, aber ähnliche Bestimmung.[659] Auch bei den ausserstrafprozessualen Überwachungen bedarf die Mitteilungsunterlassung einer richterlichen Genehmigung.

655 Hansjakob, Überwachungsrecht, N 1263 f., nach dem hinsichtlich belastender Beweise nur ein Aufschub der Mitteilung, nicht aber ein Verzicht zulässig sei; ferner SK StPO II-Hansjakob/Pajarola, N 45 zu Art. 279, nach denen die Erkenntnisse weiterhin zu Ermittlungszwecken verwendet werden dürfen.

656 Auch bei einem nicht genehmigten Zufallsfund i.S.v. Art. 278 StPO regelt die Bestimmung nicht die «Verwertung», sondern die «Verwendung». Nichtsdestotrotz wird dies als ein absolutes Verwertbarkeitsverbot i.S.v. Art. 141 Abs. 1 Satz 2 StPO bewertet, vgl. dazu BGE 144 IV 254, E. 1.4.3 f.

657 Hansjakob, Überwachungsrecht, N 1274 ff., nach dem die Rechtmässigkeit der Überwachung in diesem Fall vom Sachrichter überprüft werden könne. Eine Unverwertbarkeit folge lediglich, sofern der Umstand der Überwachung nicht offengelegt werde und auch vergessen wurde, dem Betroffenen Einsicht in die Überwachungsergebnisse zu gewähren.

658 Art. 37 Abs. 1 BÜPF und Art. 18a Abs. 4 IRSG verweisen auf Art. 279 StPO.

659 Art. 33 Abs. 3 i.V.m. Art. 29 NDG.

III. Beschwerdegarantie

1. Verfassungsrechtliche Anforderungen an die Beschwerdeinstanz

Im Rahmen des Rechtsschutzes ist neben der Mitteilung auch die Beschwerdemöglichkeit zu beurteilen. Die Rechtsweggarantie von Art. 29a BV garantiert den Zugang zu einem Gericht, stellt aber grundsätzlich keine Rechtsmittelgarantie dar.[660] Im Hinblick auf die Überwachung des Fernmeldeverkehrs leitet das Bundesgericht jedoch aus Art. 13 BV und Art. 29a BV den Anspruch auf eine Beschwerdeinstanz ab.[661] Eine Beschwerdeinstanz muss einen *wirksamen Rechtsschutz* ermöglichen.[662] Die effektive Rechtsdurchsetzung erfordert, dass der Beschwerdeweg nicht durch eine Behördenpraxis oder Regelung übermässig erschwert ist.[663] Unzulänglich ist ein *rein theoretischer* Zugang zu einer gerichtlichen (Beschwerde-)Instanz.[664] Aus dem Effektivitätserfordernis ergibt sich weiter, dass die richterliche Behörde über eine in *tatsächlicher* und *rechtlicher* Hinsicht umfassende Prüfungskognition zu verfügen hat.[665]

2. Beschwerdemöglichkeit nach StPO

Im Einklang mit den verfassungsrechtlichen Anforderungen sieht die Strafprozessordnung vor, dass eine überwachte Person Beschwerde gemäss Art. 393 StPO führen kann (Art. 279 Abs. 3 StPO). Die Beschwerdeinstanz kann sowohl den Sachverhalt als auch die Rechtsanwendung umfassend prüfen (Art. 393 Abs. 2 StPO).

3. Beschwerdemöglichkeit bei ausserstrafprozessualer Fernmeldeüberwachung

Entsprechend den verfassungsrechtlichen Vorgaben steht der überwachten Person ein Beschwerdeweg auch dann zur Verfügung, wenn der Fernmeldeverkehr ausserhalb des Strafverfahrens überwacht wurde. Im Falle der Fern-

660 BSK BV-Waldmann, N 5 zu Art. 29a.
661 Vgl. BGE 140 I 353, E. 8.7.2.4.
662 BGE 140 I 353, E. 8.7.2.4.
663 BSK BV-Waldmann, N 15 zu Art. 29a.
664 BGE 149 I 2, E. 2.1.
665 Vgl. BGE 142 II 49, E. 4.4.

meldeüberwachung zwecks Personensuche nach Art. 35 f. BÜPF steht der strafprozessuale Beschwerdeweg offen (Art. 37 Abs. 3 BÜPF i.V.m. Art. 279 Abs. 3 StPO).[666] Im Kontext der Rechtshilfe kann die überwachte Person in der Schweiz die Beschwerde führen (vgl. Art. 18a Abs. 4 IRSG i.V.m. Art. 279 Abs. 3 StPO). Uneinigkeit besteht hinsichtlich der Frage, ob der Beschwerdeweg gemäss StPO bei der kantonalen Beschwerdeinstanz oder gemäss IRSG beim Bundesstrafgericht einzuschlagen ist.[667] Bei der nachrichtendienstlichen Überwachung nach Art. 26 NDG kann die betroffene Person Beschwerde beim Bundesverwaltungsgericht führen (Art. 83 Abs. 1 NDG).

4. Verletzungsfolgen

Die Bereitstellung eines Beschwerdewegs stellt eine verfassungsmässige Anforderung an eine Kommunikationsüberwachung dar. Das Beschwerdeverfahren garantiert einen raschen Rechtsschutz. Der separate Beschwerdeweg ist Teil der institutionellen Trennung zwischen der Anordnung/Überprüfung der Überwachung einerseits und der Beweisverwertung durch das Sachgericht andererseits.

Teilweise wird die Auffassung vertreten, ein mangelhafter Beschwerdeweg (namentlich bei fehlender Mitteilung der Überwachung) könne durch das Sachgericht kompensiert werden.[668] Nach der hier vertretenen Ansicht kommt eine Kompensation eines fehlenden Beschwerdewegs durch das Sachgericht lediglich bei einer rechtmässig unterlassenen Mitteilung (i.S.v. Art. 279 Abs. 2 StPO) in Betracht. In diesem Fall drängt es sich auf, dass das Sachgericht die Rechtmässigkeit vorfrageweise behandelt, um der betroffenen Person den Beschwerdeweg gegen den Zwischenentscheid zu eröffnen.[669] Ist der Beschwerdeweg hingegen nicht aufgrund der unterlassenen Mitteilung i.S.v. Art. 279 Abs. 2 StPO, sondern aufgrund institutioneller Gründe verunmöglicht, kann keinesfalls eine Kompensation durch das Sachgericht erfolgen. Da in diesem Fall eine grobe Missachtung des verfassungsmässigen Beschwerdewegs ohne gesetzliche Grundlage vorliegt, sollte ein strenges, absolutes Verwertbarkeitsverbot angenommen werden.

666 Hansjakob, Überwachungsrecht, N 1799 ff.

667 Vgl. BSK IRSG-Aepli, N 44 ff.; PC IRSG-Ludwiczak Glassey, N 13 zu Art. 18a.

668 Siehe Hansjakob, Überwachungsrecht, N 1274.

669 Würde über die Rechtmässigkeit in einem Endentscheid befunden, riskierte die betroffene Person in einem Berufungsverfahren bei allfälliger Anschlussberufung der Staatsanwaltschaft einen ungünstigeren Entscheid.

IV. In Casu (EncroChat, SkyECC und Anom)

1. Verletzung der Mitteilungspflicht

Im Rahmen einer strafprozessualen oder ausserstrafprozessualen Überwachung ist die betroffene Person über die Überwachung zu unterrichten. Keine Mitteilungspflicht besteht lediglich gegenüber Personen, die nicht Zielpersonen sind und deren Kommunikationsanteile nicht in einem Verfahren verwendet werden.[670] Liegt eine Mitteilungspflicht vor, so kann eine Mitteilung nur mit Zustimmung des Zwangsmassnahmengerichts unterbleiben. Diese genehmigte Unterlassung hat aber zur Folge, dass die Überwachungsergebnisse absolut unverwertbar sind (vgl. Art. 279 Abs. 2 lit. a StPO).[671]

Vorliegend wurden die Überwachungsergebnisse individuell zugeordnet, ausgewertet und letztlich in einem Strafverfahren verwendet. Somit bestand fraglos eine Mitteilungspflicht. Ungeachtet dessen wurden die Nutzer weder von den ausländischen noch von den Schweizer Behörden über die Überwachungen unterrichtet. Dieser Mitteilungsunterlassung fehlt es – entgegen der gesetzlichen Vorgabe – an einer Genehmigung eines Schweizer Zwangsmassnahmengerichts. Da im schweizerischen Recht bereits die rechtmässige Mitteilungsunterlassung zu einem *absoluten Verwertbarkeitsverbot* führt, gilt dieses zweifelsfrei auch für rechtswidrige, nicht genehmigte Mitteilungsunterlassungen.

2. Unzulänglichkeit einer ausländischen Beschwerdeinstanz

Die Anordnung, Genehmigung und operative Durchführung der vorliegenden Überwachungen erfolgten durch ausländische Behörden/Gerichte. Aus formaler Perspektive hätte somit der Genehmigungsstaat – nicht die Schweiz – den Beschwerdeweg zu gewährleisten.[672] Dies ergibt sich daraus, dass nur aus-

---

670 Hinsichtlich der strafprozessualen Mitteilung siehe HANSJAKOB, Überwachungsrecht, N 1237; hinsichtlich der Funk- und Kabelaufklärung nach Art. 38 f. NDG siehe Botschaft NDG, 2171.

671 Siehe vorstehend M.II.2.b).

672 Der EGMR stellt hinsichtlich der Ausschöpfung des internen Instanzenzuges darauf ab, auf wessen Initiative hin die Massnahme erfolgte und in welchem Staat das originäre Verfahren durchgeführt wurde, siehe EGMR A.L. und E.J. vs. Frankreich, Urteil vom 24. September 2024, 44715/20 und 47930/21, § 131.

ländische Anfechtungsobjekte (Überwachungsanordnungen/Genehmigungen) vorliegen.[673] Darüber hinaus hat lediglich die Beschwerdeinstanz des Genehmigungsstaates eine hinreichende Informationsbasis, um die Rechtmässigkeit der Überwachung beurteilen zu können. Letztlich hat auch nur die Beschwerdeinstanz des Genehmigungsstaates die Möglichkeit, das Recht effektiv gegenüber den operierenden Behörden durchzusetzen.

Nichtsdestotrotz wäre im vorliegenden Kontext eine Beschwerde im Genehmigungsstaat mangelhaft. Teile der vorliegenden Überwachungsmassnahmen sind in der Schweiz zu lokalisieren.[674] Dies hat zur Folge, dass die Überwachung dem schweizerischen Verfahrensrecht untersteht. Das schweizerische Verfahrensrecht kann jedoch nur durch eine Schweizer Instanz adäquat überprüft werden, sodass ein ausländisches Gericht als Beschwerdeinstanz ausfällt.

3. Beeinträchtigung/Verunmöglichung des ausländischen Beschwerdewegs

a) EncroChat und SkyECC

Soeben wurde dargelegt, dass ein Beschwerdeweg im Ausland unzureichend ist, da die Massnahmen teilweise in der Schweiz zu lokalisieren sind. Hinzu kommt, dass ein Beschwerdeweg im Ausland rein praktisch mit grossen Hindernissen verbunden wäre. Hinsichtlich der EncroChat- und SkyECC-Überwachung ist äusserst fraglich, ob einem Schweizer Nutzer ein Beschwerdeweg in Frankreich offen stünde. Im Rahmen eines EGMR-Beschwerdeverfahrens eines britischen EncroChat-Nutzers vertrat die französische Regierung die Ansicht, dass der britische Nutzer über keinen Beschwerdeweg in Frankreich verfüge.[675] Der EGMR hielt hingegen fest, dass auch der britische Nutzer den französischen Instanzenzug auszuschöpfen hat und das französische Recht mit Art. 694-41 FR-CPP dem britischen Nutzer eine hinreichende Beschwerdemöglichkeit zur Verfügung stellt.[676]

---

673 Nach schweizerischer Auffassung stellt die Genehmigung das Anfechtungsobjekt dar, vgl. BGer 7B_813/2025 vom 17. November 2025, E. 1.

674 Siehe vorstehend D.1.

675 Stellungnahme Frankreichs v. 7. April 2022 vor dem EGMR (A.L. und E.J. vs. Frankreich, 44715/20 und 47930/21), § 71 und 96 (zum URL Fn 5).

676 EGMR A.L. und E.J. vs. Frankreich, Urteil vom 24. September 2024, 44715/20 und 47930/21, § 131 ff.

Das französische Verfahrensrecht sieht in Art. 170 und Art. 173 FR-CPP vor, dass eine von einer französischen Untersuchungsmassnahme betroffene Person Beschwerde führen kann.[677] Voraussetzung ist, dass die betroffene Person Verfahrenspartei in einem *französischen* Strafverfahren ist.[678] Eine Ausnahme stellt das Beschwerderecht gemäss Art. 694-41 FR-CPP dar. Demnach sind auch Personen eines *ausländischen Strafverfahrens* beschwerdeberechtigt, sofern die französische Untersuchungsmassnahme im Rahmen einer Europäischen Ermittlungsanordnung (EEA) erfolgte.[679]

In Bezug auf einen Schweizer EncroChat- oder SkyECC-Nutzer ist jedoch zumindest fragwürdig, ob Art. 694-41 FR-CPP einschlägig ist. Zum einen erfolgte die EncroChat- oder SkyECC-Überwachung auf Initiative der französischen Behörde und nicht im Rahmen eines Rechtshilfeersuchens. Die Datenübermittlung in die Schweiz ist vermutlich nicht mit jener nach Grossbritannien vergleichbar. Während der Übermittlung nach Grossbritannien eine EEA vorausging[680], gibt es keine Anzeichen dafür, dass der Datenübermittlung an die Schweiz ein Rechtshilfeersuchen der Schweizer Behörden vorausging. Zum anderen kann die Schweiz – mangels Anwendbarkeit der Europäischen Direktive – keine EEA, sondern lediglich herkömmliche Rechtshilfeersuchen ausstellen. Vor diesem Hintergrund erscheint es äusserst fraglich, ob einem EncroChat- oder SkyECC-Nutzer, gegen den in der Schweiz ein Strafverfahren geführt wird, überhaupt ein Beschwerdeweg in Frankreich zur Verfügung steht.

b) Anom

Die Anom-Überwachung wurde in einem unbekannten Staat genehmigt. Dies verunmöglicht es dem betroffenen Anom-Nutzer, eine Beschwerde im Genehmigungsstaat zu führen.

4. Keine Überprüfung vor Schweizer Instanzen

Teile der Überwachungsmassnahmen haben in der Schweiz stattgefunden. Fraglich ist deshalb, ob eine Schweizer Gerichtsinstanz (Sachgericht oder Beschwerdeinstanz) eine wirksame Überprüfung der Überwachung vornehmen

677 Martine, Abschnitt «The problems posed by the French legal framework».
678 Martine, Abschnitt «The problems posed by the French legal framework».
679 Martine, Abschnitt «The problems posed by the French legal framework».
680 Vgl. EGMR A.L. und E.J. vs. Frankreich, Urteil vom 24. September 2024, 44715/20 und 47930/21, § 35 f. und 131.

könnte. Die Überprüfung durch ein Schweizer Gericht wäre mit dem Vertrauensprinzip vereinbar, da dieses nur im Hinblick auf das ausländische – nicht aber auf das schweizerische – Recht gilt.[681]

Allerdings würde eine Überprüfung durch ein Schweizer Gericht erhebliche Mängel aufweisen. *Erstens* fehlt es an einem tauglichen *Anfechtungsobjekt*, da eine Beschwerde in der Schweiz nur hinsichtlich einer schweizerischen Verfügung durchgeführt werden kann. *Zweitens* hätte ein Schweizer Gericht keine *Rechtsdurchsetzungsmacht* hinsichtlich der operierenden ausländischen Behörden. *Drittens* fehlte es einem Schweizer Gericht aufgrund der Geheimhaltung an *tatsächlicher Kenntnis* über die Überwachungsoperation. Somit entfällt selbst eine inzidente Überprüfung durch das Sachgericht. Aus diesen Gründen kann auch ein Schweizer Gericht die fehlende ausländische Beschwerdemöglichkeit nicht kompensieren.

V. Kapitelzusammenfassung

Im Ergebnis liegen im Hinblick auf den Rechtsschutz zweierlei Verfahrensmängel vor. Zum einen liegt eine Verletzung der Mitteilungspflicht vor. Bereits eine rechtmässige Mitteilungsunterlassung führt zur absoluten Unverwertbarkeit (vgl. Art. 279 Abs. 2 lit. a StPO). Fraglos gilt diese Verwertbarkeitsfolge auch für die vorliegenden rechtswidrigen – da richterlich nicht genehmigten – Mitteilungsunterlassungen.

Zum anderen steht dem Nutzer weder im überwachenden Staat noch in der Schweiz eine wirksame Beschwerdemöglichkeit zur Verfügung. Einerseits wäre eine ausländische Instanz unzuständig, da die Überwachung in der Schweiz zu lokalisieren ist und sich nach schweizerischem Recht richtet. Anderseits ist auch eine Überprüfung durch ein Schweizer Gericht – namentlich wegen unzureichender Sachverhaltskenntnis – unzulänglich. Somit ist die Garantie des wirksamen Rechtsschutzes verletzt.[682]

681 Siehe vorstehend E.III.2.

682 MARTINE, Abschnitte «Genesis of the procedure» und «The problems posed by the French legal framework» hinsichtlich eines belgischen SkyECC-Nutzers.

N. Akteneinsichtsrecht

I. Rechtliches Gehör nach Art. 29 Abs. 2 BV

Nach der vorstehenden Beurteilung von überwachungsspezifischen Kriterien, erfolgt nun eine Bewertung im Lichte einer allgemeinen prozessualen Verfahrensgarantie, dem rechtlichen Gehör (Art. 29 Abs. 2 BV). Diese Garantie beinhaltet das *Akteneinsichtsrecht* der Parteien.[683] Das Korrelat des Akteneinsichtsrechts ist die *Aktenführungspflicht*, die sich ebenfalls aus Art. 29 Abs. 2 BV ableitet.[684] Diese verpflichtet die Behörden, sämtliche verfahrensrelevanten Informationen zu dokumentieren und in die Strafakte aufzunehmen.[685] Die Aktenführungspflicht und das Akteneinsichtsrecht werden nachfolgend im Einzelnen näher betrachtet.

II. Strafprozessuale Aktenführungspflicht (Art. 100 StPO)

1. Grundsatz der Aktenvollständigkeit

Die sich aus dem Verfassungsrecht ergebende behördliche Aktenführungspflicht wird in Art. 100 StPO konkretisiert. Art. 100 Abs. 1 StPO verpflichtet die Behörden zum Anlegen eines Aktendossiers. Das Aktendossier hat sämtliche Spurenelemente zu enthalten, die im Verfahren – sei es nur mit geringer Wahrscheinlichkeit – von Relevanz sein können (sog. *Aktenvollständigkeit*).[686] Insbesondere haben die Behörden sämtliche Beweiserhebungen aktenkundig zu machen.[687] Dementsprechend haben die Untersuchungsakten zu belegen, wie die einzelnen Beweismittel produziert wurden.[688]

---

683 BGE 132 V 387, E. 3.

684 BGE 142 I 86, E. 2.2.

685 Statt vieler BGE 138 V 218, E. 8.1.2.

686 BGer 6B_403/2018 vom 14. Januar 2019, E. 2.3.1; BGer 2C_779/2019 vom 29. Januar 2020, E. 3.3.2.

687 Vgl. BGE 115 Ia 97, E. 4c.

688 BGE 129 I 85, E. 4.1.

2. Aktenführung bei digitalen Beweisen

Bei der Aktenführung ist zu berücksichtigen, dass elektronische Daten flüchtig und fehleranfällig sind.[689] In der schweizerischen Rechtsprechung existiert jedoch bislang kein einheitlicher Standard zur Aktenführung hinsichtlich elektronischer Daten.[690] Das Bundesgericht fordert generell, dass die Produktionsweise eines Beweismittels aktenmässig belegt sein muss.[691] Der EGMR-Rechtsprechung ist zu entnehmen, dass dem Grundsatz nach *Rohdaten*[692] in die Verfahrensakte zu integrieren sind.[693] Auch in der schweizerischen Literatur wird die Auffassung vertreten, dass die Rohdaten in die Strafakten gehören.[694]

Darüber hinaus fordert die Literatur, dass bei elektronischen Datenerfassungen dokumentiert wird, wer Gewahrsam an den Daten hatte (*chain of custody*) und welche Bearbeitungsschritte an diesen vorgenommen wurden (*chain of evidence*).[695] Bei elektronischen Beweismitteln sollte zudem gewährleistet werden, dass sich die Daten nach der Beweiserhebung nicht mehr verändern (*Datenintegrität*).[696] Ferner sollte der Ursprungsort der Daten nachvollziehbar sein (*Datenauthentizität*).[697] Die Authentizität kann insbesondere mittels *Hash-Werten* überprüft werden.[698] Ein Hashwert repräsentiert einen «digitalen Fingerabdruck», was bedeutet, dass zwei Dateien mit demselben Hash-Wert identisch sind.[699]

---

689 Vgl. EGMR Yüksel Yalçinkaya vs. Türkei, Urteil vom 26. September 2023, 15669/20, § 312, 329 und 332.

690 Vgl. TPF 2020 96, E. 5.1.2 ff., wo auf den Leitfaden zur IT-Forensik des deutschen Bundesamts für Sicherheit in der Informationstechnik verwiesen wird; auch den ISO-Regelwerken zur IT-Forensik wird in der strafrechtlichen Rechtsprechung keine grosse Aufmerksamkeit geschenkt.

691 BGE 129 I 85, E. 4.1.

692 Rohdaten sind jene Daten, die aus der erzeugenden Quelle stammen, siehe dazu Sarre/Pruss, § 2 N 40.

693 Siehe EGMR Yüksel Yalçinkaya vs. Türkei, Urteil vom 26. September 2023, 15669/20, § 327 und 333 ff., wonach das Fehlen von Rohdaten eine Kompensationspflicht von Seiten der Behörden auslöst.

694 Vgl. Gall/Haskaya, S. 305; Wohlers, S. 299 f.; Gless, forumpoenale, S. 120; ferner zum deutschen Recht Rückert, S. 721; Kipker/Bruns, S. 367 f.

695 Vgl. Bangerter, S. 266; Gall/Haskaya, S. 305.

696 Rückert, S. 23; vgl. EGMR Yüksel Yalçinkaya vs. Türkei, Urteil vom 26. September 2023, 15669/20, § 312.

697 Rückert, S. 23; vgl. auch Gless, ZStrR, S. 94.

698 Rückert, S. 369.

699 Bangerter, S. 271.

3. Ausnahmen vom Grundsatz der Aktenvollständigkeit

a) Schutz nicht staatlicher Geheimnisse

Das Gebot der Aktenvollständigkeit kennt gewisse Ausnahmen. Verschiedene Bestimmungen in der StPO sehen vor, dass bestimmte Informationen ausserhalb der Strafakte aufzubewahren und allenfalls zu vernichten sind.[700] Diese Bestimmungen schützen primär die betroffenen Individualinteressen (vgl. Art. 141 Abs. 5 StPO) oder nicht staatliche Geheimhaltungsinteressen wie das Berufsgeheimnis (vgl. Art. 271 Abs. 1 StPO).

b) Schutz staatlicher Geheimnisse

Staatliche Geheimhaltungsinteressen hingegen werden weniger umfassend geschützt. Dieser Umstand rührt aus dem *Verbot der Geheimakten*.[701] Vereinbar mit dem Verbot der Geheimakten ist es jedoch, gewisse operative und polizeitaktische Informationen nicht in die Verfahrensakte aufzunehmen.[702] Diese Ausnahme betrifft aber lediglich *Elemente der Beweiserhebung*, wie die identifizierenden Angaben eines verdeckten Ermittlers[703] oder den Quellcode einer GovWare[704]. Der Schutz der staatlichen Interessen führt jedoch nicht dazu, dass ein *Beweismittel* als solches aus den Verfahrensakten herausgehalten werden kann.

Bei einem derartigen Zurückhalten von Informationen behalten die Strafbehörden jedoch ihre Kontrollpflichten. So haben die Gerichte Zugriff auf die geheimen, identifizierenden Angaben hinsichtlich des verdeckten Ermittlers.[705] Auch bei der Verwendung einer GovWare muss die Strafverfolgungsbehörde sicherstellen, dass sie eine Überprüfung des Quellcodes veranlassen kann (Art. 269^{quater} Abs. 3 StPO).

---

700 Vgl. Art. 141 Abs. 5, Art. 248 Abs. 1, Art. 276 Abs. 1 StPO, die eine Beweisvernichtung nach rechtskräftigem Verfahrensabschluss vorsehen sowie Art. 269ter Abs. 3, 271 Abs. 1, 277 Abs. 1, 289 Abs. 6 StPO die eine sofortige Vernichtung vorsehen.

701 SK StPO I-Brüschweiler/Grünig, N 1b zu Art. 100.

702 BSK StPO I-Hans/Wiprächtiger/Schmutz, N 18 zu Art. 100.

703 Die identifizierenden Angaben werden in einem sog. «Schattendossier» geführt, siehe dazu BSK StPO I-Hans/Wiprächtiger/Schmutz, N 24 zu Art. 100; PK StPO-Jositsch/Schmid, N 3 zu Vor Art. 76-79.

704 Siehe SK StPO II-Pajarola/Hansjakob, N 27 ff. zu Art. 269^{quater}, diese schlagen vor, dass bei Beschaffung der GovWare ein Einsichtsrecht eines allfälligen Sachverständigen vertraglich vereinbart werden sollte; ähnlich Rückert, S. 708, demnach ein externer Quellcode nur zu den Akten zu nehmen ist, sofern der Hersteller zustimmt.

705 Vgl. BSK StPO I-Hans/Wiprächtiger/Schmutz, N 24 zu Art. 100.

c) Faktische Einschränkung des Akteneinsichtsrechts

Eine Ausnahme von der Aktenführungspflicht stellt eine faktische Beeinträchtigung des Akteneinsichtsrechts dar. Da es sich um eine Rechtseinschränkung handelt, muss sich eine Ausnahme von der Aktenvollständigkeit auf eine gesetzliche Grundlage stützen (etwa Art. 151 StPO).[706] Fraglich ist, ob darüber hinaus die allgemeine Bestimmung zur Einschränkung des Akteneinsichtsrechts (Art. 108 StPO) auch zu Ausnahmen der Aktenvollständigkeit dienen kann. Nach der hier vertretenen Ansicht vermag Art. 108 StPO allein das *Parteirecht* der Akteneinsicht einzuschränken. Bei Vorliegen eines Einschränkungsgrundes wird hingegen die Strafverfolgungsbehörde nicht von ihren *Aktenführungspflichten* befreit. Dies zeigt sich auch daran, dass selbst im Falle eines Einschränkungsgrundes dem Rechtsbeistand grundsätzlich die Akte zugänglich zu machen ist (Art. 108 Abs. 3 StPO).

4. Aktenführungs-, Untersuchungs- und Beschaffungspflicht

Die Aktenführungspflicht weist einen Zusammenhang mit dem Untersuchungsgrundsatz auf. Der *Untersuchungsgrundsatz* stellt die Pflicht zur prozessualen Wahrheitsfindung dar.[707] Dementsprechend sind die Behörden verpflichtet, von Amtes wegen die bedeutsamen Tatsachen abzuklären (Art. 6 Abs. 1 StPO). Bedeutsam sind Informationen, die in einem potenziellen Zusammenhang mit dem Verfahren stehen. Die *Aktenführungspflicht* hingegen verpflichtet die Behörden, die Ergebnisse der Wahrheitsfindung ordnungsgemäss zu dokumentieren.[708] Die Aktenführungspflicht stellt sodann die Grundlage für das verfassungsmässige Akteneinsichtsrecht der Parteien dar.[709]

Das Abklären von bedeutsamen Tatsachen und deren aktenmässige Dokumentation führt zu einer *Beschaffungspflicht* der Strafverfolgungsbehörden. Bei einer Beweiserhebung durch eine Privatperson oder durch eine andere (ausländische) Behörde ist eine Schweizer Strafverfolgungsbehörde verpflichtet, die bedeutsamen Tatsachen zu beschaffen und in die Akte aufzunehmen. Diese

706 Nach der hier vertretenen Auffassung stellt auch Art. 269^{quater} Abs. 3 StPO eine hinreichende Grundlage dar, den Quellcode einer GovWare den Verfahrensparteien vorzuenthalten, da sich die Norm an die Behörden richtet.

707 PK StPO-Jositsch/Schmid, N 1 zu Art. 6.

708 Vgl. BGE 115 Ia 97, E. 4c.

709 Vgl. BGE 142 I 86, E. 2.2.

Beschaffungspflicht gilt namentlich im Hinblick auf Rohdaten von ausländischen Überwachungen.[710]

III. Strafprozessuales Einsichtsrecht (Art. 101 StPO)

1. Voraussetzungsloser Parteianspruch

Der verfassungsrechtliche Parteianspruch auf Akteneinsicht wird in Art. 101 StPO konkretisiert. Das Akteneinsichtsrecht gilt für die Verfahrensparteien ohne Nachweis eines besonderen Interesses.[711] Insbesondere ist es nicht erforderlich, dass die um Einsicht ersuchende Partei Anhaltspunkte für einen Verfahrensfehler geltend macht. Dieser voraussetzungslose Einsichtsanspruch bringt zum Ausdruck, dass die Parteien nicht in das ordnungsgemässe Verhalten der Behörden zu vertrauen haben.[712]

2. Umfang

Das Akteneinsichtsrecht des Beschuldigten erstreckt sich auf die gesamte Strafakte.[713] Somit besteht ein Einsichtsrecht hinsichtlich sämtlicher Akten, die geeignet sind, Grundlage des bevorstehenden Entscheides zu bilden.[714] Der Umfang des Akteneinsichtsrechts bestimmt sich nicht anhand der jeweils vorliegenden Verfahrensakte, sondern anhand der hypothetisch ordnungsgemäss geführten Akte.[715] Andernfalls bestünde die Gefahr, dass das Akteneinsichtsrecht umgangen würde, indem die fragliche Information nicht in die Akte aufgenommen wird.

3. Exkurs: Primär-, Sekundär- und Tertiärdatensatz

In der niederländischen Literatur wird hinsichtlich der EncroChat-Daten vorgeschlagen, den Datensatz in Primär-, Sekundär- und Tertiärdaten zu unter-

710 Vgl. Kipker/Bruns, S. 367.
711 Vgl. BGE 137 IV 280, E. 2.2.1.
712 Vgl. Wohlers, S. 299.
713 BSK StPO I-Hans/Wiprächtiger/Schmutz, N 8 zu Art. 101.
714 BGE 132 V 387, E. 3.
715 BGer 6B_403/2018 vom 14. Januar 2019, E. 2.3.1, wonach die Akteneinsicht eine vollständige Verfahrensakte voraussetzt; vgl. auch Jositsch/Schmid, N 625; Wohlers, S. 299; ferner EGMR Yüksel Yalçinkaya vs. Türkei, Urteil vom 26. September 2023, 15669/20, § 327.

teilen.[716] Diese Einteilung erfolgt mit Rückgriff auf den EGMR[717], weshalb diese Einteilung im Sinne eines kurzen Exkurses betrachtet wird.

Der *Primärdatensatz* enthält sämtliche Rohdaten betreffend sämtliche überwachte Personen in unstrukturierter Form.[718] Der *Sekundärdatensatz* besteht aus jenen Daten, die für die Gesamtheit der Strafverfahren von Relevanz sind.[719] Die *Tertiärdaten* sind jene Daten, die im einzelnen Strafverfahren von Bedeutung sind.[720] Ein voraussetzungsloses Einsichtsrecht besteht nur hinsichtlich der Tertiärdaten[721]; die Einsicht in die Sekundärdaten ist vom Vorliegen eines besonderen Interesses abhängig[722]. Auch der EGMR operiert teilweise mit dieser Einordnung.[723]

Diese Einteilung ist jedoch nicht auf das schweizerische Recht anwendbar. Von Verfassungs wegen hat eine beschuldigte Person den Anspruch, *sämtliche* Daten einzusehen, die geeignet sind, Grundlage des bevorstehenden Entscheides zu bilden.[724] Sofern eine Verfahrensrelevanz besteht, gilt dieser Anspruch *voraussetzungslos*[725] – unabhängig davon, welchem Datensatz die Daten zuzuordnen sind. Einschränkungen unterliegen somit nicht dem Vorbehalt des mangelnden Interesses, sondern gegebenenfalls überwiegender Drittinteressen. Darüber hinaus wäre dies auch aus formellen Gründen nicht sachgerecht, da eine Einschränkung des Einsichtsrechts formell zu verfügen ist.[726]

716 Vgl. Oerlemans/van Toor, S. 323 ff.

717 Oerlemans/van Toor, S. 323 f. m.H.a. auf EGMR Sigurdur Einarsson and others vs. Island, Urteil vom 4. Juni 2019, 39757/15 sowie Rook vs. Deutschland, Urteil vom 25. Juli 2019, 1586/15.

718 Oerlemans/van Toor, S. 323.

719 Oerlemans/van Toor, S. 323.

720 Oerlemans/van Toor, S. 323.

721 Oerlemans/van Toor, S. 323 f. m.H.a. EGMR Rook vs. Deutschland, Urteil vom 25. Juli 2019, 1586/15, § 58.

722 Oerlemans/van Toor, S. 324; vgl. EGMR Matanovic vs. Kroatien, Urteil vom 4. April 2017, 2742/12, § 157.

723 Vgl. EGMR Sigurdur Einarsson and others vs. Island, Urteil vom 4. Juni 2019, 39757/15, § 75, 90 und dissenting opinion, § 6 ff.

724 BGE 132 V 387, E. 3.

725 Vgl. BGE 137 IV 280, E. 2.2.1.

726 BSK StPO I-Vest, N 4 zu Art. 108; ferner wäre eine Einschränkung gegenüber dem Rechtsbeistand unzulässig (vgl. Art. 108 Abs. 2 StPO).

IV. Einschränkung der Akteneinsicht (Art. 108 StPO)

1. Einschränkungsvoraussetzungen

Das von Art. 101 StPO garantierte Akteneinsichtsrecht kann unter den Voraussetzungen von Art. 108 StPO eingeschränkt werden.[727] Aus *formeller* Hinsicht bedarf die Einschränkung der Akteneinsicht einer schriftlich begründeten Verfügung der Verfahrensleitung[728], welche beschwerdefähig ist[729]. In *materieller* Hinsicht ist gemäss Art. 108 Abs. 1 StPO eine Einschränkung nur zulässig, wenn ein begründeter Missbrauchsverdacht vorliegt, oder die Einschränkung für die Sicherheit von Personen oder zur Wahrung öffentlicher oder privater Geheimhaltungsinteressen erforderlich ist. In *zeitlicher* Hinsicht ist zu beachten, dass die Einschränkung zu befristen ist. Bei anhaltendem Einschränkungsgrund kann die Einschränkung andauern, allerdings ist der Partei der wesentliche Inhalt zur Kenntnis zu bringen (Art. 101 Abs. 3 und 4 StPO).

2. Berücksichtigung ausländischer Interessen?

Fraglich ist, ob ein rein ausländisches staatliches Interesse eine Einschränkung der Akteneinsicht zu begründen vermag.[730] Nach Art. 108 Abs. 1 lit. b StPO können *öffentliche Geheimhaltungsinteressen* einen Einschränkungsgrund darstellen. Darunter fallen insbesondere Interessen des Staatsschutzes.[731] Nach der hier vertretenen Auffassung zielt diese Bestimmung lediglich auf den Schutz *eidgenössischer*, *kantonaler* oder *kommunaler* Interessen, nicht aber auf den Schutz ausländischer Staatsinteressen ab. Eine Berücksichtigung ausländischer Interessen bedürfte einer ausdrücklichen gesetzlichen Grundlage. Eine derartige Gesetzesgrundlage befindet sich etwa im Rechtshilferecht (Art. 80b Abs. 2 lit. a IRSG), welches aber in einem Strafverfahren keine Anwendung findet. Dementsprechend sollte eine Einschränkung des Akteneinsichtsrechts in

727 Darüber hinaus kann das Akteneinsichtsrecht gestützt auf Art. 70 und Art. 149 ff. StPO eingeschränkt werden, siehe dazu PK StPO-Jositsch/Schmid, N 6 zu Art. 108.

728 BSK StPO I-Vest, N 4 zu Art. 108; vgl. EGMR Yüksel Yalçinkaya vs. Türkei, Urteil vom 26. September 2023, 15669/20, § 331.

729 Vom Sachgericht angeordnete Einschränkungen sind mittels Endentscheid anzufechten (Art. 65 Abs. 1 StPO), siehe dazu SK StPO I-Lieber, N 16 zu Art. 108.

730 LG Berlin, Urt. v. 19.12.2024 – 525 KLs 8/22, Rn. 323, wonach ausländische Staatsinteressen grundsätzlich eine Zurückhaltung von Informationen rechtfertigen können.

731 PK StPO-Jositsch/Schmid, N 6 zu Art. 108.

einem schweizerischen Strafverfahren zumindest mit einem mittelbaren inländischen Staatsinteresse begründet werden.

Selbst bei gegenteiliger Auffassung muss zumindest anerkannt werden, dass ein ausländisches Staatsinteresse keinesfalls umfassender als ein inländisches Staatsinteresse geschützt werden kann. In einem reinen Binnenverfahren genügt der alleinige Hinweis auf die vertrauenswürdige Arbeit der Behörden nicht als Einschränkungsgrund.[732] Dementsprechend ist auch im internationalen Kontext das Vertrauen in die ausländische Behördenarbeit als Einschränkungsgrund unzureichend. Folglich vermag das rechtsbezogene Vertrauensprinzip (wonach die Rechtmässigkeit der ausländischen Tätigkeit zu vermuten ist) keinesfalls das Einsichtsrecht einzuschränken.

3. Einschränkung des Einsichtsrechts des Rechtsbeistands?

Das Einsichtsrecht des Rechtsbeistandes ist resistenter als das Einsichtsrecht der beschuldigten Person. Nach Art. 108 Abs. 2 StPO sind Einschränkungen gegenüber dem Rechtsbeistand nur zulässig, wenn der Rechtsbeistand selbst Anlass für die Beschränkung gibt. Anders als das Akteneinsichtsrecht des Beschuldigten kann das Einsichtsrecht des Rechtsbeistandes grundsätzlich nicht aufgrund eines Geheimhaltungsinteresses einer Drittperson eingeschränkt werden.[733] Ausnahmsweise kann jedoch das Anonymitätsinteresse eines Verfahrensbeteiligten das Einsichtsrecht des Rechtsbeistandes gestützt auf Art. 149 Abs. 2 lit. e StPO einschränken.[734] Derartige Einschränkungen sind mit einem fairen Verfahren aber nur vereinbar, sofern die Einschränkung wirklich unabdingbar ist.[735]

732 Vgl. Wohlers, S. 299.

733 Vgl. CR StPO-Bendani, N 12a zu Art. 108; BSK StPO I-Vest, N 7 zu Art. 108.

734 Vgl. BSK StPO I-Wehrenberg, N 27 zu Art. 149.

735 BSK StPO I-Wehrenberg, N 32 zu Art. 149; deutlich einschränkungsfreundlicher zeigt sich hingegen der EGMR, demnach der Grundrechtsschutz von Drittpersonen das Einsichtsrecht des Rechtsbeistandes zu beschränken vermag, siehe dazu EGMR Yüksel Yalçinkaya vs. Türkei, Urteil vom 26. September 2023, 15669/20, § 329.

V. Verletzungsfolgen

1. Folgen der Verletzung der Aktenführungspflicht

Es stellt sich die Frage, welche Folge die Verletzung der Aktenführungspflicht – das unrechtmässige Nichtaufnehmen von Informationen – hat. Die Verwertbarkeit eines Beweises setzt voraus, dass dieser in den Akten dokumentiert wurde.[736] Das Gericht hat die Möglichkeit, unvollständige Akten zu ergänzen oder durch die Staatsanwaltschaft ergänzen zu lassen (Art. 329 Abs. 1 lit. a und Art. 339 Abs. 5 StPO). Unterlässt es das Gericht, die Unvollständigkeit der Akte zu beheben, so muss das Gericht davon absehen, sich auf die nicht aktenmässig belegte Tatsache zu stützen. Betrifft die nicht dokumentierte Tatsache eine Beweiseigenschaft – etwa die Datenintegrität – beeinträchtigt dies den *Beweiswert*.[737] Sofern ein Beweis von der Einhaltung gewisser Formen abhängt, kann eine unvollständige Dokumentation auch eine *Unverwertbarkeit* nach sich ziehen (etwa bei fehlender Dokumentation der Hinweise nach Art. 158 StPO). Fehlt hingegen ein Beweis in den Akten, so kann sich das Gericht selbstverständlich nicht auf den fehlenden Beweis stützen. Andernfalls kann eine offensichtlich unrichtige – und somit willkürliche[738] – *Sachverhaltsfeststellung* vorliegen[739]. Im Ergebnis ist festzuhalten, dass die jeweiligen Verletzungsfolgen massgeblich von den fallspezifischen Umständen abhängen.

2. Folgen der Verletzung des Akteneinsichtsrechts

Die Verletzung des Akteneinsichtsrechts stellt einen Mangel formeller Natur dar.[740] Aus öffentlich-rechtlicher Betrachtung führt ein formeller Verfahrensfehler grundsätzlich zur Anfechtbarkeit der Rechtshandlung.[741] Ausnahmsweise kann eine Heilung erfolgen, sofern die Verletzung nicht gravierend ist und die betroffene Person sich vor der Beschwerdeinstanz mit umfassender Kognition erneut äussern kann.[742]

---

736 Vgl. BSK StPO II-Schwendener, N 24 zu Art. 339.

737 Vgl. Wohlers, S. 300.

738 Vgl. BGE 133 II 249, E. 1.2.2.

739 Vgl. BGer 4A_82/2016 vom 6. Juni 2016, E. 5.2, wonach eine offensichtlich falsche Sachverhaltsdarstellung (i.S.v. Art. 393 lit. e ZPO) vorliegt, wenn ein Gericht irrig davon ausgeht, dass eine Tatsache aktenmässig belegt sei.

740 BGE 127 V 431, E. 3d.

741 BGE 142 II 218, E. 2.8.1.

742 Vgl. u.a. BGE 142 II 218, E. 2.8.1; BGE 133 I 201, E. 2.2.

Dieser Heilungsmechanismus lässt sich jedoch nicht ohne Weiteres in das Strafverfahrensrecht übertragen. Teilweise sieht das Strafverfahrensrecht bei formellen Fehlern spezifische Folgen vor. So sieht Art. 147 Abs. 4 StPO vor, dass bei einer unrechtmässigen Einschränkung des Teilnahmerechts die Beweise nicht zu Lasten der Partei verwertet werden dürfen. Diese Rechtsfolge bietet sich auch bei anderen Formen der Gehörsverletzung an. Nach der hier vertretenen Ansicht sollte auch eine Verletzung der Akteneinsicht dazu führen, dass der zu Unrecht geheim gehaltene Beweis nicht zu Ungunsten der betroffenen Person verwertet werden darf, zumindest wenn es sich um den einzigen oder einen ausschlaggebenden Beweis handelt.[743]

VI. In Casu (EncroChat, SkyECC und Anom)

1. Verletzung der Beschaffungs- und Aktenführungspflichten

Gemäss EGMR-Rechtsprechung[744] und Literatur[745] sind bei elektronischen Beweiserhebungen die *Rohdaten* grundsätzlich in die Verfahrensakte aufzunehmen. Sind die Strafverfolgungsbehörden nicht in deren Besitz, so besteht – wie vorstehend dargelegt – eine diesbezügliche Beschaffungspflicht.[746] Ferner sollte über eine lückenlose *Hashwert*-Dokumentation der Datenweg nachvollziehbar gemacht werden.[747]

In den vorliegenden Verfahren verfügen die federführenden Staaten (Frankreich, USA, Europol) über die Rohdaten. Folglich wären die hiesigen Strafverfolgungsbehörden verpflichtet gewesen, die Rohdaten sowie die Hashwert-Dokumentation bei den ausländischen Behörden zu beschaffen und diese in die Strafakte aufzunehmen. Das vorliegende Fehlen dieser Daten stellt eine Verletzung der Beschaffungs- und Aktenführungspflicht dar. Dies führt – isoliert betrachtet – zur erheblichen Beeinträchtigung des Beweiswertes der Chat-Daten.[748]

743 Vgl. Wohlers, S. 300 mit Hinweis auf das Fairness-Gebot.

744 Siehe EGMR Yüksel Yalçinkaya vs. Türkei, Urteil vom 26. September 2023, 15669/20, § 327 und 333 ff., wonach das Fehlen von Rohdaten eine Kompensationspflicht von Seiten der Behörden auslöst.

745 Vgl. Gall/Haskaya, S. 305; Wohlers, S. 299 f.; ferner Rückert, S. 721; Kipker/Bruns, S. 367 f.

746 Siehe vorstehend N.II.4.

747 Siehe vorstehend N.II.2.

748 Vgl. Kipker/Bruns, S. 367.

2. Verletzung des Akteneinsichtsrechts

Darüber hinaus ist das Fehlen der Rohdaten im Lichte des Akteneinsichtsrechts zu bewerten. Das Akteneinsichtsrecht verleiht grundsätzlich den Anspruch, Einsicht in die hypothetisch ordnungsgemäss geführte Akte – inklusive Rohdaten – zu nehmen. Das vorliegende Fehlen der Rohdaten stellt somit faktisch eine Einschränkung des Einsichtsrechts dar.[749] Diese faktische Einschränkung entspricht allerdings nicht den gesetzlichen Anforderungen von Art. 108 StPO. Aus formaler Hinsicht fehlt es an einer *förmlichen*, *begründeten* und *anfechtbaren Verfügung*. Aus materieller Hinsicht liegt kein gültiges Einschränkungsinteresse vor, da ein *ausländisches Staatsinteresse* – mangels Rechtsgrundlage – keine Einschränkung zu rechtfertigen vermag. Im Übrigen hätte die vollständige Akte – sofern der Nutzer anwaltlich vertreten ist – dem Rechtsbeistand eröffnet werden müssen (Art. 108 Abs. 2 StPO). Somit liegt ein schwerer Verstoss gegen das rechtliche Gehör vor.

Eine Heilung dieser Gehörsverletzung durch das Sachgericht entfällt, da auch dieses keinen Zugriff auf die Rohdaten hat, sodass eine unheilbare Gehörsverletzung vorliegt. Bei den in den Akten liegenden Chat-Dateien handelt es sich i.d.R. um ein zentrales Beweismittel. Aufgrund der schweren Gehörsverletzung und der Bedeutung des Beweismittels dürfen nach der hier vertretenen Ansicht die Chat-Dateien nicht zu Ungunsten des Beschuldigten verwertet werden (Art. 147 Abs. 4 StPO analog).

3. Fazit

Das Fehlen der Rohdaten in den Akten verletzt die behördliche Beschaffungspflicht. Die Verletzung der Beschaffungspflicht wirkt sich zunächst auf den *Beweiswert* der verarbeiteten Daten aus. Allerdings schränkt das Fehlen der Rohdaten gleichzeitig faktisch das Akteneinsichtsrecht ein. Aus formellen und materiellen Gründen fällt vorliegend jedoch eine gesetzeskonforme Einschränkung des Akteneinsichtsrechts ausser Betracht, weshalb die Chat-Dateien *nicht* zu Ungunsten des Beschuldigten verwertet werden dürfen.

[749] Ähnlich Kipker/Bruns, S. 368, nach denen das Vorbehalten der Rohdaten die Verfahrensfairness verletze.

O. Faires Verfahren nach Art. 6 EMRK (Fair Trial)

I. Anwendungsbereich

Neben den Verfahrensgarantien des internen schweizerischen Rechts sind auch die prozessualen Garantien der EMRK zu beachten. Der räumliche Anwendungsbereich der EMRK erstreckt sich auf die Mitgliedstaaten des Europarates.[750] Die Verfahrensgarantien von Art. 6 EMRK sind sachlich auf zivilrechtliche Ansprüche und strafrechtliche Anklagen anwendbar.[751] Das Anklagekriterium von Art. 6 EMRK ist allerdings weit auszulegen. Dieses Kriterium knüpft nicht an die formelle Anklageerhebung, sondern an den Inhalt der durchgeführten Handlung an.[752] Die Garantie greift bereits, wenn sich aus einer Untersuchungshandlung ergibt, dass gegen eine bestimmte Person ermittelt wird. Massgebend ist somit der materielle Beschuldigtenstatus[753], sodass die Garantie bereits im Vorverfahren Anwendung findet.[754]

II. Grundsatz der Verfahrensfairness

1. Der Fair Trial Grundsatz als Gesamtrecht

Das Fair Trial Prinzip von Art. 6 EMRK beinhaltet einen Strauss an Verfahrensrechten, die nachfolgend teils im Einzelnen dargestellt werden. Während Art. 6 Ziff. 1 EMRK ein *faires Verfahren* garantiert, stellen die Bestimmungen von Ziff. 3 eine nicht abschliessende Konkretisierung dieser Garantie dar[755]. Bei der Verfahrensfairness gemäss Art. 6 EMRK handelt es sich um ein Gesamtrecht[756], sodass im Einzelfall aufgrund der fallspezifischen *Gesamtbetrachtung* die Verfahrensfairness zu bewerten ist[757].

---

750 Siehe Präambel der EMRK.
751 BSK EMRK-Misic/Prantl, N 92 zu Art. 6.
752 Stelzer-Wieckowska, S. 66.
753 Stelzer-Wieckowska, S. 66 f.
754 Villiger, N 473.
755 Villiger, N 577.
756 Demko, S. 232.
757 Demko, S. 232 ff.

2. Die Rechtsweggarantie

Ein Teilgehalt von Art. 6 Ziff. 1 EMRK ist die Rechtsweggarantie.[758] Diese gewährt den Zugang zu einem Gericht, welches in unabhängiger Weise über die Streitfrage befinden kann.[759] Die Instanz muss eine wirksame Überprüfung vornehmen können, weshalb eine umfassende Kognition in tatsächlicher und rechtlicher Hinsicht erforderlich ist.[760] Weiter muss das Gericht die tatsächliche Durchsetzung des Urteils gewährleisten können.[761] Aus Art. 6 EMRK ergibt sich kein Anspruch auf ein Rechtsmittel. Ist ein solches jedoch vorgesehen, so gilt Art. 6 EMRK auch für die Rechtsmittelinstanz.[762]

3. Die Waffengleichheit

Aus dem Fairnessgrundsatz von Art. 6 EMRK ergibt sich das Prinzip der Waffengleichheit.[763] Demnach sind die Strafverfolgungsbehörden und der Beschuldigte verfahrensrechtlich gleichgestellt.[764] Das Verfahren ist so zu gestalten, dass die Parteien gleichwertige Informations- und Äusserungsmöglichkeiten haben.[765] Das Gebot der Waffengleichheit soll eine Informationsasymmetrie zwischen Behörden und der beschuldigten Person vermeiden.[766]

4. Das rechtliche Gehör

Ein weiterer elementarer Teilgehalt von Art. 6 EMRK ist der Anspruch auf rechtliches Gehör.[767]

Das rechtliche Gehör verleiht das Recht, von Beweismitteln Kenntnis zu erhalten, zu erheblichen Umständen Stellung zu nehmen und Beweise anzubieten.[768] Das Zugangsrecht erstreckt sich auf sämtliche Informationen, die

758 Villiger, N 504.
759 NHK EMRK-Harrendorf/König/Voigt, N 63 zu Art. 6.
760 Vgl. u.a. EGMR Terra Woningen B.V. vs. Niederlande, Urteil vom 17. Dezember 1996, 20641/92, § 52.
761 Villiger, N 505.
762 NHK EMRK-Harrendorf/König/Voigt, N 55 zu Art. 6.
763 Villiger, N 557.
764 Villiger, N 557.
765 Vgl. BSK EMRK-Misic/Prantl, N 151 zu Art. 6; ferner EGMR Bulut vs. Österreich, Urteil vom 22. Februar 1996, 17358/90, § 47.
766 Vgl. Kipker/Bruns, S. 367.
767 Villiger, N 565.
768 BSK EMRK-Misic/Prantl, N 134; Villiger, N 566.

eine potentielle Verfahrensrelevanz haben, selbst wenn die Strafverfolgungsbehörden die Information als unbeachtlich bewerten.[769] In Bezug auf digitale Beweiserhebungen erfordert die EGMR-Rechtsprechung, dass die *Rohdaten* grundsätzlich in die Akte aufzunehmen sind.[770]

5. Einschränkungen und kompensatorische Massnahmen

Das rechtliche Gehör und dessen Teilgarantien von Art. 6 EMRK können unter Umständen eingeschränkt werden. Zunächst bedarf es eines *legitimen Einschränkungsgrundes*.[771] Darüber hinaus muss die Beschränkung *verhältnismässig* sein.[772] Ferner macht eine Einschränkung *kompensatorische Massnahmen* erforderlich. Diese sollen es der betroffenen Person ermöglichen, sich trotz der Einschränkung am Verfahren zu beteiligen.[773] Insgesamt gilt, je gravierender die Einschränkung und je wichtiger das belastende Beweismittel ist, desto wirksamer müssen die kompensatorischen Massnahmen ausfallen.[774] Bei der Beurteilung der Fairness ist zu berücksichtigen, ob das Gericht Einsicht in die Rohdaten hat[775], inwiefern die Verteidigung die Möglichkeit hat, die Beweise anzufechten[776] und wie die Geheimhaltung gegenüber der betroffenen Person begründet wird[777]. Bei umfassenden Datensätzen hält es der EGMR für zulässig, lediglich einen reduzierten Datensatz in die Verfahrensakte zu integrieren. In diesem Fall können die Beschuldigtenrechte etwa dadurch gewahrt wer-

769 EGMR Yüksel Yalçinkaya vs. Türkei, Urteil vom 26. September 2023, 15669/20, § 327.

770 Siehe EGMR Yüksel Yalçinkaya vs. Türkei, Urteil vom 26. September 2023, 15669/20, § 327 und 333 ff., wonach das Fehlen von Rohdaten eine Kompensationspflicht von Seiten der Behörden auslöst.

771 Vgl. BGer 6B_1067/2023 vom 2. April 2025, E. 3.1.3. m.H.a. EGMR Schatschaschwili vs. Deutschland, Urteil vom 15. Dezember 2015, § 113.

772 EGMR Waite and Kennedy vs. Deutschland, Urteil vom 18. Februar 1999, 26083/94, § 59.

773 Vgl. BGer 6B_1067/2023 vom 2. April 2025, E. 3.1.3. m.H.a. EGMR Schatschaschwili vs. Deutschland, Urteil vom 15. Dezember 2015, § 113.

774 Vgl. EGMR Sigurdur Einarsson and others vs. Island, Urteil vom 4. Juni 2019, 39757/15, § 345.

775 Grundsätzlich entsteht die Pflicht zur besonders strengen gerichtlichen Prüfung der Beweisqualität beim Fehlen der Rohdaten («greater onus»). Aus der alleinigen Tatsache, dass das Gericht keine Einsicht in die Rohdaten hat, kann keine Verletzung von Art. 6 EMRK geschlossen werden, siehe dazu EGMR Yüksel Yalçinkaya vs. Türkei, Urteil vom 26. September 2023, 15669/20, § 334 f.

776 EGMR Yüksel Yalçinkaya vs. Türkei, Urteil vom 26. September 2023, 15669/20, § 328.

777 Gemäss EGMR Yüksel Yalçinkaya vs. Türkei, Urteil vom 26. September 2023, 15669/20, § 333 besteht im Einschränkungsfall eine «duty of properly responding to him».

den, dass die Verteidigung in die Selektionskriterien einbezogen wird.[778] Eine Pflicht zu kompensatorischen Massnahmen entsteht namentlich, wenn sich die Rohdaten einer digitalen Beweiserhebung nicht in den Akten befinden.[779]

6. Faire Handhabung von Beweismitteln

Die Zulässigkeit von Beweiserhebungen und die Beweiswürdigung unterliegen dem internen Recht des Staates.[780] Die Art und Weise der Beweiserhebung ist jedoch eine Komponente der Gesamtwürdigung des fairen Verfahrens.[781] Relevant sind dabei die konkreten Umstände[782], namentlich:

- Welches Konventionsrecht wurde auf welche Art verletzt[783]
- Hatte die Verteidigung die Möglichkeit, die Datenintegrität und -authentizität überprüfen zu lassen[784]
- Welche Relevanz hat das fragliche Beweismittel im Verfahren[785]

7. Verletzungsfolgen

Art. 6 EMRK garantiert lediglich den Anspruch auf ein faires Verfahren.[786] Ob und inwiefern ein Verwertbarkeitsverbot bei einer Garantieverletzung vorliegt, ist nach Massgabe des schweizerischen Verfahrensrechts zu bestimmen.[787] Nach schweizerischer Auffassung kann ein Verfahrensfehler unter Umständen geheilt werden, was grundsätzlich auch bei Verletzung von Art. 6 EMRK in Betracht kommt.[788] Ist eine Heilung nicht möglich, so kann sich aus der StPO ein (relatives oder absolutes) Verwertbarkeitsverbot ergeben.

778 EGMR Sigurdur Einarsson and others vs. Island, Urteil vom 4. Juni 2019, 39757/15, § 90.
779 EGMR Yüksel Yalçinkaya vs. Türkei, Urteil vom 26. September 2023, 15669/20, § 334.
780 Vgl. EGMR Bykov vs. Russland, Urteil vom 10. März 2009, 4378/02, § 89.
781 EGMR Bykov vs. Russland, Urteil vom 10. März 2009, 4378/02, § 89.
782 Vgl. EGMR Gäfgen vs. Deutschland, Urteil vom 1. Juni 2010, 22978/05, § 164.
783 EGMR Bykov vs. Russland, Urteil vom 10. März 2009, 4378/02, § 89.
784 EGMR Yüksel Yalçinkaya vs. Türkei, Urteil vom 26. September 2023, 15669/20, § 303.
785 EGMR Gäfgen vs. Deutschland, Urteil vom 1. Juni 2010, 22978/05, § 164.
786 BGE 143 IV 387, E. 4.3.
787 BGE 143 IV 387, E. 4.3; BGer 6B_462/2025 vom 25. März 2026, E. 2.4.5.
788 Vgl. BSK EMRK-Misic/Prantl, N 124 zu Art. 6; EGMR Riepan vs. Österreich, Urteil vom 14. November 2000, 35115/97, § 41.

III. In Casu: Gesamtwürdigung der Fairness (EncroChat, SkyECC, Anom)

1. Vorbemerkungen

Die interessierenden Überwachungen wurden jeweils (mutmasslich) in einem EU-Staat und somit einem Konventionsstaat genehmigt.[789] Ferner werden sie in der Schweiz – und somit ebenfalls einem Konventionsstaat – strafprozessual verwendet. Fraglos sind somit die Überwachungen und die strafprozessuale Verwendung ihrer Ergebnisse an den Vorgaben der EMRK zu messen. In der Gesamtwürdigung der Fair Trial Garantie (Art. 6 EMRK) sind die einzelnen Aspekte der Überwachungsmassnahmen zu bewerten. Im Rahmen dessen ist von Relevanz, welches Konventionsrecht auf welche Art verletzt wurde.[790] Vorliegend ist insbesondere der Schutz der Korrespondenz nach Art. 8 Ziff. 1 EMRK betroffen, sodass die nachfolgende Würdigung im Lichte von Art. 6 und Art. 8 EMRK erfolgt.

2. Rechtswidriger Eingriff in den Korrespondenzschutz (Art. 8 EMRK)

Aus Sicht von Art. 8 EMRK weisen die vorliegenden Überwachungen schwerste Mängel auf. Wie bereits dargelegt, handelt es sich bei den Überwachungsmassnahmen um ausländische *Massenüberwachungen* in der *Schweiz*.[791] Nach der Rechtsprechung des EGMR bedarf eine Massenüberwachung u.a.[792] einer *gesetzlichen Grundlage*, einer *Genehmigung* durch eine unabhängige Behörde und der Bereitstellung eines *Beschwerdewegs*.[793]

Diese Voraussetzungen sind – wie bereits im Einzelnen dargelegt – vorliegend nicht gegeben. Erstens fehlt es zumindest im schweizerischen Recht an einer Rechtsgrundlage.[794] Die Massnahmen sind in ihrer Ausgestaltung typologisch dem schweizerischen Recht unbekannt und allfällige Eingriffsnormen des

789 Zur Problematik, ob hinsichtlich der EncroChat- und Anom-Überwachung die richterlichen Genehmigungen als existent zu erachten sind, siehe E.VI.3. ff.

790 EGMR Bykov vs. Russland, Urteil vom 10. März 2009, 4378/02, § 89.

791 Siehe vorstehend H.II.1.

792 Zu den übrigen Kriterien siehe vorstehend H.I.2.

793 EGMR Big Brother Watch et al. vs. Vereinigten Königreich, Urteil vom 25. Mai 2021, 58170/13, 62322/14 und 24960/15, § 361.

794 Siehe vorstehend H.I.3. und J.II f.

schweizerischen Rechts stellen keine Ermächtigungsgrundlagen für ausländische Behörden dar.

Zweitens fehlt es den Massnahmen an einer richterlichen Genehmigung, die für die Schweiz Gültigkeit beanspruchen kann. Die Massnahmen wurden (allenfalls) im Ausland genehmigt.[795]

Eine wirksame Genehmigung kann allein von einem Schweizer Zwangsmassnahmengericht verfügt werden, da nur dieses das schweizerische Recht hinlänglich prüfen kann. Aus schweizerischer Sicht liegt somit keine hinreichende Genehmigung vor.

Drittens steht dem überwachten Nutzer kein wirksamer Beschwerdeweg offen. Wie dargelegt, ist ein Beschwerdeweg im Ausland nicht nur unwirksam, sondern auch faktisch beeinträchtigt (EncroChat/SkyECC) oder gar ausgeschlossen (Anom).[796] Ferner könnte auch ein Schweizer Gericht keine wirksame Überprüfung vornehmen, da es diesem an Kenntnis über die Überwachungen und Rechtsdurchsetzungsmacht fehlt.[797] Im Ergebnis verstösst die Beweiserhebung somit in schwerer Weise gegen Art. 8 EMRK.

3. Nicht überprüfbare Datenqualität (Art. 6 EMRK)

In der Gesamtwürdigung ist weiter zu beachten, dass sich die *Rohdaten* und *Hashwert*-Dokumentation i.d.R. nicht in den Verfahrensakten befinden.[798] Dies beeinträchtigt die Möglichkeit des Beschuldigten, Rückschlüsse auf die technischen Modalitäten der Datenerhebung zu ziehen und die Zuverlässigkeit der Daten zu überprüfen.[799] Diese Umstände lösen somit zweifelsfrei eine Kompensationspflicht seitens der Strafbehörden aus.

795 Zur Problematik, ob hinsichtlich der EncroChat- und Anom-Überwachung die richterlichen Genehmigungen als existent zu erachten sind, siehe vorstehend E.VI.3. ff.

796 Siehe vorstehend M.IV.2 f.

797 Siehe vorstehend M.IV.4.

798 Vgl. United States District Court, Eastern District of New York v. 31.10.2025 (22-CR-493), 16 ff., wonach dem von den französischen Behörden erstellten certificat de sincérité keine substantiellen Informationen zur Datenbearbeitung zu entnehmen sind.

799 Ähnlich Gless, forumpoenale, S. 120.

4. Fehlende kompensatorische Massnahmen (Art. 6 EMRK)

Die mangelnden Informationen über die Vorgehensweise und die fehlenden Rohdaten führen zu einer Kompensationspflicht seitens der Strafbehörden. Insbesondere wäre das Sachgericht verpflichtet, die Datenqualität besonders kritisch zu prüfen[800] und die Rechtseinschränkung rechtmässig zu begründen[801].

Vorliegend sind jedoch hiesige Strafbehörden aus computerforensischer Sicht ausser Stande, kompensatorische Massnahmen zu ergreifen. Namentlich haben die hiesigen Behörden weder Einsicht in die Rohdaten, noch in die vollständige Hashwert-Dokumentation noch in den Quellcode. Somit haben diese keine Möglichkeit, die eingesetzte Technologie auf ihre Rechtmässigkeit und Zuverlässigkeit zu prüfen. Theoretisch denkbar wären allenfalls kompensatorische Massnahmen durch Personalbeweise (etwa die Einvernahme des Chatpartners, der gegebenenfalls die Identität seines Gesprächspartners und den Chatinhalt bestätigt[802]). In der Praxis dürfte jedoch eine völlige Abwesenheit von kompensatorischen Massnahmen vorherrschen.

5. Fazit zur Gesamtwürdigung

Gesamtwürdigend ist festzuhalten, dass die Massnahmen Art. 6 und Art. 8 EMRK verletzen. Zunächst entsprechen die Massnahmen nicht den EGMR-Kriterien hinsichtlich der *Massenüberwachung*. Es fehlt ihnen aus schweizerischer Sicht an einer *gesetzlichen Grundlage*, einer *gültigen Genehmigung* und einer *hinreichenden Beschwerdemöglichkeit*. Darüber hinaus sind die Aspekte der Verfahrensfairness (Art. 6 EMRK) verletzt. Namentlich führt das *Fehlen belastbarer Informationen* zur Datenbearbeitung (Rohdaten und Hash-Werte) zu einem erheblichen Informationsdefizit des Nutzers. Dieses Informationsdefizit lässt eine *Kompensationspflicht* der Schweizer Strafbehörden entstehen. Diese sind jedoch ausser Stande, wirksame kompensatorische Massnahmen zu ergreifen, da sie unter demselben Informationsdefizit leiden. In der Gesamtbetrachtung ist der Grundsatz der Verfahrensfairness von Art. 6 EMRK in grober Weise verletzt, dessen Verwertbarkeitsfolgen sich nach StPO richten.[803] Wie in den vorstehenden Kapiteln aufgezeigt, führen bereits die einzelnen Mängel für sich genommen zu Verwertbarkeitsverboten.

800 EGMR Yüksel Yalçinkaya vs. Türkei, Urteil vom 26. September 2023, 15669/20, § 334.
801 EGMR Yüksel Yalçinkaya vs. Türkei, Urteil vom 26. September 2023, 15669/20, § 329.
802 Vgl. United States District Court, Eastern District of New York v. 31.10.2025 (22-CR-493), S. 19.
803 BGE 143 IV 387, E. 4.3; BGer 6B_462/2025 vom 25. März 2026, E. 2.4.5.

P. Die Massnahmen im Lichte des Territorialitätsprinzips

I. Schutzweck des Territorialitätsprinzips

Nachdem die Massnahmen im Lichte des Fernmelderechts und der Verfahrensgarantien erörtert wurden, erfolgt nun eine Prüfung vor dem Hintergrund des Territorialitätsprinzips. Die Achtung fremder Gebietshoheit ist ein Fundament des Völkerrechts.[804] Das Territorialitätsprinzip beschränkt das Handeln der Strafverfolgungsbehörden auf das inländische Staatsgebiet[805] und ist Ausfluss der völkerrechtlichen *Kompetenzordnung*.[806] Als Völkerrechtssubjekte sind somit die Staaten in ihren Interessenkreisen geschützt.[807] Die Funktion des Territorialitätsprinzips beschränkt sich allerdings nicht auf die Wahrung der völkerrechtlichen Kompetenzordnung. Vielmehr ist das Territorialitätsprinzip auch Gewähr, dass *Grundrechte* nur durch die zuständigen Organe kraft des anwendbaren Rechts eingeschränkt werden.[808] Somit schützt das Territorialitätsprinzip auch Individualinteressen[809], weshalb diesem ein zweigliedriger Schutzzweck zukommt.[810]

II. Territorialitätseingriff

1. Territorialitätsprinzip als Schutz der exklusiven Zuständigkeit

Das Territorialitätsprinzip schützt den Exklusivanspruch eines Staates, hoheitliche Handlungen innerhalb des Staatsgebietes vorzunehmen.[811] Innerhalb des schweizerischen Territoriums haben folglich allein Schweizer Behörden

---

804 Dombrowski, S. 5.

805 Vgl. BGE 141 IV 108, E. 5.3; BGE 146 IV 36, E. 2.2.

806 Vgl. Graf, Verwertbarkeit, S. 526.

807 Vgl. Dombrowski, S. 5 f.

808 Vgl. Wildhaber, S. 103.

809 Vgl. Wildhaber, S. 103; ferner EuGH, Rs. C-670/22, ECLI:EU:C:2024:372, Ziff. 124 zu Art. 31 der RL EEA.

810 Vgl. im Kontext von EncroChat EuGH, Rs. C-670/22, ECLI:EU:C:2024:372, Ziff. 124.

811 Capus, S. 193.

die Kompetenz, autoritativ zu agieren. Diese exklusive Zuständigkeit erfährt in engen Grenzen Ausnahmen in der polizeilichen *Amtshilfe*. So besteht im Hinblick auf die Nachbarstaaten regelmässig die Möglichkeit, dringliche polizeiliche Massnahmen auf fremdem Territorium kurzzeitig fortzusetzen.[812] Im Rahmen der *Rechtshilfe* hingegen nimmt stets die Schweiz als ersuchter Staat eine Untersuchungshandlung für einen anderen Staat vor. Ausländische Amtsträger dürfen nur im engen Rahmen gesetzlicher Bestimmungen[813] an Beweiserhebungen in der Schweiz teilnehmen.

Abgesehen von der Amts- und Rechtshilfe kann eine Aufweichung der Exklusivität nur im Rahmen einer *Bewilligung nach Art. 271 StGB* erfolgen. Diese Bestimmung pönalisiert Handlungen für einen fremden Staat auf schweizerischem Gebiet ohne Bewilligung und schützt die schweizerische Gebietshoheit.[814] Im Rahmen von Art. 271 StGB kann ausländischen Amtsträgern die selbstständige Vornahme von Amtshandlungen in der Schweiz bewilligt werden.[815] Bewilligungsfähig sind allerdings nur Massnahmen, die dem Schweizer (Rechtshilfe-)Recht bekannt sind, aber im Einzelfall praktisch sinnlos oder unmöglich erscheinen, wie etwa im Falle eines Augenscheins.[816]

Die Amts- und Rechtshilfe sowie Art. 271 StGB umreissen somit das Schweizer Territorialitätsrecht. Jede ausländische Untersuchungshandlung auf Schweizer Territorium ausserhalb dieser Rechtssysteme verletzt die Schweizer Souveränität.[817]

2. Eingriffsintensität von Datenverarbeitungsvorgängen

Eine Territorialitätsverletzung liegt vor, wenn ein Amtsträger physisch auf fremdem Territorium agiert. Ein physisches Handeln auf fremdem Territorium ist jedoch nicht notwendig. Es genügt, dass die Handlung mit hinreichender Intensität ihre Wirkung auf fremdem Territorium entfaltet.[818] Namentlich kön-

812 Vgl. etwa Art. 14 ff. des Schweizerisch-deutschen Polizeivertrags.

813 Etwa Art. 4 EUeR und Art. 65a Abs. 1 IRSG.

814 PK StGB-Trechsel/Vest, N 1 zu Art. 271.

815 BSK IRSG-Sprenger, N 27 zu Art. 65a IRSG.

816 Siehe Entscheid des Bundesrates vom 25. Juni 1997, JAAC 61.82, S. 4 f.; ferner BGE 106 Ib 260, E. 2, wonach sich die Bewilligung auf die Rechtshilfemassnahme beschränkt; BSK StGB II-Husmann, N 87 zu Art. 271.

817 Vgl. Donatsch/Heimgartner/Simonek, S. 5.

818 Vgl. BGer 7B_120/2022 vom 5. Oktober 2023, E. 2.4.2.1; BStGer SK.2012.20 vom 29. Januar 2013, E. 2.1; Graf, Verwertbarkeit, S. 525; im Kontext von Art. 271 StGB wird teils an die

nen Datenverarbeitungsvorgänge, die Behörden im Ausland auslösen, eine derartige Eingriffsintensität erreichen.[819] Delikat ist allerdings die Frage, anhand welcher Kriterien die *Eingriffsintensität* von Datenverarbeitungsvorgängen bemessen werden kann. Diesbezüglich lassen sich jedoch gewisse Konturen ausmachen[820]:

Die Verletzung des Exklusivitätsanspruches setzt voraus, dass der Datenzugriff eine Zwangsmassnahme darstellt. Somit ist erforderlich, dass eine Massnahme einen *Grundrechtseingriff* konstituiert (vgl. Art. 196 StPO).[821] Namentlich kann unter Umständen ein Zugriff auf öffentlich abrufbare Daten (OSINT[822]) ohne Grundrechts- und Territorialitätseingriff auskommen.[823]

Mangels Eingriffsintensität liegt ferner keine Verletzung des Exklusivanspruches vor, wenn Behörden über einen *bestehenden Übermittlungskanal* auf Daten zugreifen.[824] Aus Sicht des Bundesgerichts ist es zulässig, wenn Behörden mit rechtmässig erhaltenen Login-Daten eine Online-Recherche durchführen, obwohl sich der Server im Ausland befindet.[825] Diese Variante des Zugriffsprinzips[826] beschränkt sich allerdings auf offene Massnahmen und findet keine Anwendung bei der Überwachung des Fernmeldeverkehrs.[827]

Ebenso wenig ist der Exklusivitätsanspruch verletzt, wenn die betroffene Person die *Kontrolle über den Kommunikationsvorgang* hat, in dessen Rahmen der Datenverarbeitungsvorgang erfolgt. Zulässig ist gemäss Bundesgericht die Textnachrichten-Kommunikation zwischen verdeckten Ermittlern von der

---

Zwangswirkung, teils an den amtlichen Charakter einer Massnahme geknüpft, siehe dazu BGer 6B_804/2018 vom 4. Dezember 2024, E. 3 und BGE 140 IV 86, E. 2.

819 Graf, Jusletter, S. 21 f., nach dem etwa eine hinreichende Eingriffsintensität bei der EncroChat-Überwachung gegeben sei; ferner Dombrowski, S. 159.

820 Diese Konturen hat der Verfasser bereits in Jaklin, Datenverarbeitungsvorgänge, S. 1 ff. dargelegt.

821 Vgl. OK CCC-Graf, N 35 zu Art. 32.

822 OSINT kurz für Open Source Intelligence.

823 Vgl. OK CCC-Graf, N 34 f. zu Art. 32; sofern ein OSINT-Abgriff einen Grundrechtseingriff darstellt, ist dieser durch Völkergewohnheitsrecht gerechtfertigt, vgl. dazu Dombrowski, S. 158.

824 Vgl. BGE 143 IV 270, E. 7.10; BGE 146 IV 36, E. 2.3.

825 BGE 143 IV 270, E. 7.10; BGE 146 IV 36, E. 2.3; Auch vereinzelte deutsche (nicht höchstinstanzliche) Gerichte erlauben eine Online-Sichtung von ausländischen Daten über zuvor erhaltene Zugangsdaten, vgl. etwa LG Koblenz, Beschl. v. 24.8.2021 – 4 Qs 59/21; VG München, Beschl. v. 18.9.2023 – M 30 X 23.4359; LG Berlin, Beschl. v. 29. Dezember 2022 – 519 Qs 8/22.

826 Diese Variante des Zugriffsprinzips betrifft nicht die Lokalisierung der Massnahme, sondern deren Eingriffsintensität.

827 Siehe vorstehend D.II.2.

Schweiz aus mit einer Zielperson im Ausland.[828] Ungeachtet des Umstandes, dass diese Kontaktierung im Ausland einen Datenverarbeitungsvorgang auslöst, liegt keine Zwangseinwirkung vor. Der kontaktierten Person steht es frei, ob sie auf die Kommunikation mit den Amtsträgern eingeht oder diese beendet und welchen Inhalt sie preisgibt. Somit ist dieser Vorgang lediglich «une simple invitation à communiquer».[829] Allerdings ist diese Rechtsprechung nur einschlägig, sofern über die *Funktion* als Polizeiangehöriger getäuscht wird. Keine Geltung kann diese Rechtsprechung beanspruchen, wenn die Behörden über die *technische Integrität* des Kommunikationsmittels täuschen (wie etwa bei den Anom-Geräten, die über eine heimliche Ausleitungsfunktion verfügten). Die Täuschung über die Integrität des Kommunikationsmittels fällt nämlich – anders als die Täuschung über die Identität der Person – unter das *Fernmeldegeheimnis*.[830]

Die vorstehend erörterten Aufweichungen des Territorialitätsprinzips sind somit nur einschlägig, sofern das Fernmeldegeheimnis nicht betroffen ist. Im Umkehrschluss greift jeder Datenverarbeitungsvorgang im Ausland, der im Rahmen einer *Fernmeldeüberwachung* erfolgt, in die ausländische territoriale Integrität ein.

3. Bewusster Auslandsbezug?

In der Literatur wird teilweise die Ansicht vertreten, ein Territorialitätseingriff setze ein bewusstes Handeln der Behörden in fremdem Territorium voraus. Kein Territorialitätseingriff liege demnach vor, sofern der Speicherort der Daten nicht aufklärbar ist oder dieser ständig wechselt.[831]

Gemäss Bundesgericht ist das Territorialitätsprinzip verletzt, wenn ein von Schweizer Behörden verwanztes Fahrzeug die Grenze ins Ausland überschreitet.[832] Da diese Situation nur schwerlich für die Schweizer Strafverfolgungsbehörden zu antizipieren ist, lässt diese Rechtsprechung wenig Raum, auf eine Vorwerfbarkeit der Behörden abzustellen.[833] Vor diesem Hintergrund ist eine Vorwerfbarkeit wohl nicht zwingend erforderlich. Für den vorliegenden Kon-

828 BGE 150 IV 308, E. 2.4.1 f. und 2.8.3.
829 BGE 150 IV 308, E. 2.4.1 f. und 2.8.3.
830 Vgl. Rückert, S. 73 und 76 und 109.
831 SysK D-StPO-Jäger/Wohlers, N 9b zu § 110; BeckOK D-StPO-Hegmann, N 15 zu § 110; vgl. OK CCC-Graf, N 23 zu Art. 32 CCC.
832 BGer 1B_93/2021 vom 19. Juli 2021, E. 2.2.
833 Vgl. BGer 1B_93/2021 vom 19. Juli 2021, E. 2.2; Graf, Verwertbarkeit, S. 526.

text muss diese Problematik allerdings nicht abschliessend beurteilt werden. Bei den interessierenden Überwachungsmassnahmen zeigten die federführenden Staaten nämlich keine Bemühungen, die Massnahmen auf das eigene Territorium zu beschränken. Vielmehr bestand der Massnahmenzweck geradezu in der internationalen Verbrechensbekämpfung[834], sodass die Eingriffe in fremdes Territorium bewusst erfolgten.

III. Rechtfertigung von Territorialitätseingriffen

1. Information request gemäss Art. 32 lit. b CCC

Ein Territorialitätseingriff kann durch eine völkerrechtliche Grundlage gerechtfertigt sein. Relevant im Kontext von Datenzugriffen ist Art. 32 lit. b CCC. Diese Bestimmung erlaubt in Durchbrechung des Territorialitätsprinzips den Zugriff auf im Ausland gespeicherte Computerdaten. Die Norm entbindet die handelnde Behörde, den betroffenen Staat um Rechtshilfe zu ersuchen oder diesen über den Datenzugriff zu informieren.[835] Art. 32 lit. b CCC spiegelt den völkerrechtlichen Minimalkonsens für den rechtshilfefreien Datenzugriff wider.[836] Es steht einem Staat frei, sein eigenes Territorialitätsrecht weniger restriktiv zu definieren und weiterreichende Datenzugriffe zuzulassen. Sofern ein Staat davon jedoch nicht Gebrauch macht, stellt ein von Art. 32 lit. b CCC nicht gedeckter Datenzugriff eine Territorialitätsverletzung dar.[837]

Die Voraussetzung für den transnationalen Datenzugriff nach Art. 32 lit. b CCC ist die rechtmässige und freiwillige Zustimmung des Zustimmungsberechtigten. Die zustimmende Person muss nicht nur zum Datenzugriff, sondern auch zur Datenweitergabe befugt sein.[838] Zustimmungsberechtigt kann auch der Service-Provider sein, sofern das Weiterleitungsrecht an die Behörden in den Nutzungsbedingungen vereinbart wurde.[839]

---

834 Siehe vorstehend B.II.

835 Vgl. OK CCC-Graf, N 56 zu Art. 32; siehe ferner BGer 6B_1353/2023 vom 6. November 2024, E. 4.4.3., wonach die innerstaatlichen Anordnungsvoraussetzungen auch im Rahmen von Art. 32 CCC zu beachten sind.

836 Vgl. BGE 141 IV 108, E. 5.9.

837 Vgl. OK CCC-Graf, N 67 zu Art. 32.

838 Vgl. Botschaft CCC, 4738.

839 BGE 141 IV 108, E. 5.10.

2. Rechtfertigungsnorm von Art. 349b StGB?

Vereinzelt wird im Kontext von SkyECC die Auffassung vertreten, Art. 349b StGB hebe innerhalb des Schengenraums das Territorialitätsprinzip auf.[840] Dieser Auffassung kann allerdings nicht gefolgt werden. Diese Bestimmung betrifft die Datenbekanntgabe durch Schweizer Behörden an andere Schengen-Staaten.[841] Konkret sieht Art. 349b StGB vor, dass an die Datenbekanntgabe an andere Schengen-Staaten keine strengeren Anforderungen als an eine Bekanntgabe innerhalb der Schweiz gestellt werden dürfen (Gleichbehandlungsgebot). Diese Bestimmung betrifft die *Datenbekanntgabe*, stellt aber keine Eingriffsnorm für transnationale Zwangsmassnahmen dar.[842] Des Weiteren richtet sich diese Norm an Schweizer Behörden, ausländische Behörden sind nicht deren Adressat. Folglich kann dieser Norm keine Rechtfertigung für ausländische Amtshandlungen in der Schweiz entnommen werden.

3. Gewohnheitsrecht (insbes. Art. 32 lit. a CCC)

Ein Territorialitätseingriff kann ferner durch völkerrechtliches Gewohnheitsrecht gerechtfertigt werden.[843] Ein solches Gewohnheitsrecht besteht in Bezug auf den Zugriff auf öffentlich zugängliche Daten.[844] Sofern ein OSINT-Zugriff einen Territorialitätseingriff darstellt, ist dieser Eingriff gewohnheitsrechtlich gerechtfertigt.[845] Dieses Gewohnheitsrecht ist deklaratorisch in Art. 32 lit. a CCC kodifiziert.[846]

840 So wird Markus Mohler in der Solothurner Zeitung, E-Paper vom 13. Oktober 2025, «Ganz nach dem Gusto der Mafia», zitiert; abrufbar auf <https://www.strafprozess.ch/wordpress/wp-content/uploads/SZ-SkyECC.pdf>.

841 Art. 349b StGB ist die nationale Umsetzung von Art. 9 Abs. 3 f. der europäischen RL 2016/680, siehe dazu PK StGB-Dufour/Mona, N 1 zu Art. 349b.

842 So auch Gless, forumpoenale, S. 119.

843 Vgl. BGer 7B_120/2022 vom 5. Oktober 2023, E. 2.4.2.1.

844 Vgl. Dombrowski, S. 158.

845 Vgl. Dombrowski, S. 158.

846 Vgl. Dombrowski, S. 158.

4. Einwilligung

a) Rechtsgründe der Einwilligung

Ein Eingriff in die territoriale Integrität eines anderen Staates kann durch die Einwilligung des betroffenen Staates gerechtfertigt werden.[847] Eine Einwilligung in einen Territorialitätseingriff kann aus verschiedenen Rechtsgründen erfolgen. Zum einen kann eine derartige Einwilligung gemäss den Bestimmungen des Rechts- und Amtshilferechts erfolgen.[848] Zum anderen stellt auch eine Bewilligung nach Art. 271 StGB eine Einwilligung in einen Territorialitätseingriff dar.[849] Eine Bewilligung nach Art. 271 StGB kann erteilt werden, wenn die Rechtshilfe nicht zielführend ist.[850] Unabhängig vom Rechtsgrund lassen sich gemeinsame Konturen einer Einwilligung in einen Territorialitätseingriff erkennen[851]:

b) Zuständigkeit

Das Territorialitätsprinzip schützt die Schweizerische Eidgenossenschaft. Somit sind grundsätzlich eidgenössische Behörden für Bewilligungen nach Art. 271 StGB zuständig (vgl. Art. 31 Abs. 1 RVOV).[852] Auch die Rechtshilfe erfolgt i.d.R. über die Involvierung einer Bundesbehörde.[853] Dementsprechend haben lediglich *eidgenössische* Behörden die Kompetenz, in einen Territorialitätseingriff einzuwilligen.[854]

---

847 Vgl. BGE 146 IV 36, E. 2.2.

848 Vgl. BGE 146 IV 36, E. 2.2, wonach ein «consentement préalable de l'Etat concerné dans le respect des règles régissant l'entraide judiciaire» erforderlich sei.

849 Husmann, Bewilligung, S. 132.

850 BSK IRSG-Sprenger, N 27 zu Art. 65a IRSG; strittig ist allerdings, ob die Bewilligung nur erteilt werden kann, sofern eine rechtshilfebedürftige und rechtshilfefähige Handlung vorliegt, siehe dazu BSK StGB II-Husmann, N 85 ff. zu Art. 271; KommStR-Oesterhelt/Fracheboud, N 17 zu § 29.

851 Die nachfolgenden Konturen hat der Verfasser bereits in Jaklin, Kryptophones, S. 1015 f. dargestellt.

852 Vgl. BSK StGB II-Husmann, N 79 zu Art. 271.

853 Unter Vorbehalt der direkten Übermittlung nach Art. 78 IRSG ist das Bundesamt für Justiz in das Rechtshilfeverfahren involviert.

854 Die direkte Übermittlung an die kantonale Staatsanwaltschaft (Art. 78 Abs. 1 IRSG) bedarf einer vom Bundesgesetzgeber geschaffenen (völkerrechtlichen) Rechtsgrundlage.

c) Zeitpunkt

Sowohl die Einwilligung gemäss Art. 271 StGB[855] als auch die Rechtshilfe[856] ist grundsätzlich *vor* der entsprechenden Handlung zu erteilen. Das schweizerische Rechtshilferecht kennt keine Grundlage, eine Handlung eines anderen Staates in der Schweiz durch die nachträgliche Entgegennahme eines Rechtshilfeersuchens zu genehmigen.[857] Namentlich ist das 3. ZP zum EUeR, das in engen Grenzen eine nachträgliche Benachrichtigung kennt (Art. 3), noch nicht von der Schweiz ratifiziert. Mangels Rechtsgrundlage fällt somit eine nachträgliche Heilung eines Territorialitätseingriffes ausser Betracht.[858]

d) Verwaltungsverfahren

Sowohl die Rechtshilfe als auch die Bewilligung nach Art. 271 StGB erfolgt in einem Verwaltungsverfahren.[859] Dementsprechend ergeht eine Einwilligung in einen Territorialitätseingriff in einem *formalen* Verfahren.[860] Der gegenteiligen Ansicht, wonach ein Territorialitätseingriff durch eine widerspruchlose Duldung gerechtfertigt werden kann[861], ist deshalb nicht zu folgen.[862] Vielmehr stellt ein informelles, stillschweigendes Dulden aufgrund schwerer Formmängel eine nichtige Amtshandlung dar.[863]

855 Vgl. BSK StGB II-Husmann, N 78 zu Art. 271, wonach die Bewilligung tatbestandsausschliessend, nicht rechtfertigend wirkt, und eine nachträgliche Genehmigung die Tatbestandsmässigkeit nicht aufhebt.

856 Vgl. BGE 146 IV 36, E. 2.2.

857 Siehe BGer 7B_612/2025 vom 12. Februar 2026, E. 3.4.2.

858 Siehe BGer 7B_612/2025 vom 12. Februar 2026, E. 3.4.2 und 3.5.1, wonach ein nachträgliches Rechtshilfeersuchen an einen anderen Staat möglich ist, sofern die schweizerischen Behörden den betroffenen Staat darauf hinweisen, dass die Schweiz in einer vergleichbaren Situation die Rechtshilfe nicht erteilen könnte und das Rechtshilfeersuchen unmittelbar nach Kenntnis des Grenzübertrittes gestellt wurde.

859 Vgl. Husmann, Bewilligung, S. 91, wonach es sich bei einer Bewilligung i.S.v. Art. 271 StGB um eine Verfügung i.S.v. Art. 5 VwVG handelt.

860 Vgl. Art. 28 IRSG; OK IRSG-Dangubic/Purtscheller, N 7 zu Art. 80a hinsichtlich der Eintretens- und Schlussverfügung im Rechtshilfeverfahren; ferner Dombrowski, S. 165.

861 So etwa Graf, Jusletter, S. 20.

862 Vgl. ferner Dombrowski, S. 145.

863 Vgl. PK VwVG-Uhlmann/Schilling-Schwank, N 7 zu Art. 34.

e) Zusammenfassung

Zusammengefasst hat die Einwilligung in einen Territorialitätseingriff in einem *vorgängigen formalen Verwaltungsverfahren* durch eine *eidgenössische* Behörde zu erfolgen.[864] Eine informelle Duldung stellt keine Rechtfertigung dar.

IV. Exkurs: «Hacking» als Eingriffsvoraussetzung?

Umstritten ist, ob eine Territorialitätsverletzung eine technische Kompromittierung des Datenverarbeitungssystems «Hacking» voraussetzt.[865] Aus strafrechtlicher Sicht ist unter «Hacking» das unbefugte *Eindringen* in ein *zugriffsgesichertes* Datenverarbeitungssystem zu verstehen (vgl. Art. 143bis Abs. 1 StGB). Aus den vorstehenden Ausführungen ergibt sich, dass *ein unbefugtes Eindringen* in ein Datenverarbeitungssystem nicht notwendig für eine Territorialitätsverletzung ist.[866] Massgebend ist allein die *hinreichende Eingriffsintensität*.[867] Eine hinreichende Eingriffsintensität kann auch durch einen *protokollkonformen* Vorgang bewirkt werden, bei dem nicht in das Gerät eingedrungen wird. So stellt etwa ein IMSI-Catcher[868] (Art. 269bis StPO) eine hochinvasive Fernmeldeüberwachung ohne Eindringen in das überwachte Gerät dar.[869]

Auch aus Art. 32 lit. b CCC geht hervor, dass weder ein Eindringen in ein Datenverarbeitungssystem noch das Umgehen von Zugriffsbeschränkungen erforderlich ist. Diese Bestimmung erlaubt den Zugriff auf Daten, die im Ausland gespeichert sind, sofern der Datenberechtigte in den behördlichen Zugriff einwilligt. Aus dem Einwilligungserfordernis folgt, dass lediglich ein konsensualer, nicht aber ein *unilateraler* Datenzugriff zulässig ist. Die Bestimmung erfasst somit den einwilligungsbedürftigen, *protokollkonformen* Datenzugriff.[870] Es wäre widersinnig, die Zulässigkeit einer technischen Kompromittierung von der Einwilligung des Berechtigten abhängig zu machen. Greifen Behörden nun *ohne die erforderliche Einwilligung* unter Auslösen einer regulären Proto-

---

864 Ähnlich Dombrowski, S. 165.

865 Graf, Jusletter, S. 22; ferner Kommentar von «Laie» vom 26.08.2025 zum Blogbeitrag vom 23.08.2025 «Absolut unverwertbar: SkyECC-Daten» auf strafprozess.ch <https://www.strafprozess.ch/skyecc/>.

866 Vgl. Dombrowski, S. 159.

867 So bereits Jaklin, Datenverarbeitungsvorgänge, S. 5.

868 Ein IMSI-Catcher simuliert eine Mobilfunkantenne, sodass sich die in Reichweite befindenden Endgeräte nicht mit der tatsächlich zuständigen Funkzelle, sondern mit dem IMSI-Catcher verbinden, siehe dazu Hansjakob, Überwachungsrecht, N 543.

869 So bereits Jaklin, Datenverarbeitungsvorgänge, S. 5.

870 So bereits Jaklin, Datenverarbeitungsvorgänge, S. 5.

kollfunktion auf ausländische Daten zu, liegt ein von Art. 32 lit. b CCC nicht gedeckter Datenzugriff vor – was eine Territorialitätsverletzung darstellt.

V. Folgen der Territorialitätsverletzung

1. Absolute Unverwertbarkeit bei Verletzung fremder Territorialität

Gemäss Bundesgericht stellt eine Verletzung des Territorialitätsprinzips eine Verletzung des «internationalen öffentlichen Rechts» dar.[871] Das Bundesgericht folgert daraus, dass Beweise, die Schweizer Behörden unter Verletzung fremder Territorialität erheben, *absolut* unverwertbar sind.[872]

2. Kritik und Praxisänderung?

Diese Rechtsprechung ist auf Kritik gestossen. Nach der Ansicht von Graf sei eine Beweiserhebung im Ausland zwar völkerrechtswidrig und möglicherweise strafbar, nicht aber vom absoluten Verwertbarkeitsverbot von Art. 141 Abs. 1 StPO erfasst.[873] Ferner schütze das Territorialitätsprinzip keine Individualinteressen, da es lediglich eine Kompetenzordnung sei.[874] Folglich ergebe sich aus einer Territorialitätsverletzung allenfalls eine relative Unverwertbarkeit.[875]

Diese Kritik zielt auf eine Praxisänderung. Das Bundesgericht hat allerdings die Rechtsfolge der absoluten Unverwertbarkeit mehrmals bestätigt.[876] Zudem setzte es sich bereits mit der Frage, ob eine Praxisänderung vorzunehmen ist, ausdrücklich und ablehnend auseinander.[877]

Nach der hier vertretenen Ansicht sprechen gute Gründe für die bisherige Rechtsprechung. Zwar kann Graf darin gefolgt werden, dass das Territorialitätsprinzip Ausfluss der völkerrechtlichen Kompetenzordnung ist. Daraus

871 BGer 7B_120/2022 vom 5. Oktober 2023, E. 2.4.2.1.

872 Vgl. BGE 146 IV 36, E. 2.3; bestätigt in BGer 7B_120/2022 vom 5. Oktober 2023, E. 2.4.2.1; ebenso BGer 7B_273/2023 et al. vom 11. April 2024, E. 3.3.

873 Graf, Jusletter, S. 21.

874 Graf, Jusletter, S. 21.

875 Graf, Jusletter, S. 21.

876 BGE 146 IV 36, E. 2.3; bestätigt in BGer 7B_120/2022 vom 5. Oktober, E. 2.4.2.1; ebenso BGer 7B_273/2023 et al. vom 11. April 2024, E. 3.3; siehe BGer 7B_612/2025 vom 12. Februar 2026, E. 3.2.2.

877 BGer 7B_273/2023 et al. vom 11. April 2024, E. 3.3.

folgt aber, dass eine hoheitliche Handlung in fremdem Staatsgebiet einen örtlichen Zuständigkeitsmangel und somit einen Nichtigkeitsgrund aufweist.[878] Darüber hinaus beschränkt sich das Territorialitätsprinzip nicht auf den Schutz staatlicher Interessen, da es auch gewährleistet, dass wesentliche innerstaatliche individualrechtliche Garantien eingehalten werden.[879] Letztlich sind keine Umstände ersichtlich, die eine Neubewertung des Territorialitätsprinzips aufdrängen. Eine Praxisänderung ist nach der hier vertretenen Auffassung deshalb nicht angezeigt.

3. Ausweitung der Rechtsprechung

Die bisherige Rechtsprechung des Bundesgerichts bezieht sich auf die Verletzung fremder Territorialität durch Schweizer Behörden. Allerdings ist die Rechtsprechung der absoluten Unverwertbarkeit auf die Verletzung der schweizerischen territorialen Integrität auszuweiten. Zum einen wiegt nach der hier vertretenen Ansicht die Verletzung der schweizerischen Gebietshoheit mindestens so schwer wie diejenige der ausländischen. Zum anderen gilt auch bei der Verletzung der schweizerischen Gebietshoheit, dass die ausländische Amtshandlung an einem Zuständigkeitsmangel leidet.[880]

4. Berücksichtigung ausländischen Territorialitätsrechts

Steht in einem schweizerischen Strafverfahren das Territorialitätsrecht eines Drittstaates in Frage, so ist nach dessen Recht zu bestimmen, ob eine Territorialitätsverletzung vorgelegen hat. Die allfälligen Rechtsfolgen sind hingegen nach schweizerischem Recht zu beurteilen.[881]

Nach bundesgerichtlicher Rechtsprechung führt die Verletzung fremder Territorialität *durch Schweizer Behörden* zur absoluten Unverwertbarkeit. Das Bundesgericht bedient sich dabei einer universellen Begründung, indem es auf die Verletzung des internationalen öffentlichen Rechts verweist.[882] Eine Verletzung des internationalen Rechts liegt gleichermassen vor, wenn nicht Schweizer, sondern die Behörden eines anderen Staates drittstaatlicher Terri-

878 Dies vertrat auch Graf, Verwertbarkeit, S. 526.
879 Siehe vorstehend P.I.
880 Graf, Verwertbarkeit, S. 526.
881 Vgl. BGer 6B_1353/2023 vom 6. November 2024, E. 4.3.2.2 f.
882 BGer 7B_120/2022 vom 5. Oktober 2023, E. 2.4.2.1.

torialität verletzen. Es liegt daher nahe, auch Beweise, die durch ausländische Behörden unter Verletzung drittstaatlicher Territorialität erhoben wurden, für absolut unverwertbar zu erachten. Da sich die Verwertbarkeitsfolge einer Territorialitätsverletzung nach schweizerischem Recht richtet, ist diese unabhängig von der Auffassung des betroffenen Staats. Somit kann die Schweiz bei einer Verletzung drittstaatlicher Territorialität eine absolute Unverwertbarkeit annehmen, obwohl der betroffene Staat dies mit einer relativen Unverwertbarkeit sanktionieren würde.[883]

VI. EncroChat

Das schweizerische Recht kennt ausserhalb von Art. 32 lit. b CCC keine Bestimmung, die ausländische Behörden dazu ermächtigt, in der Schweiz eigenständig Untersuchungshandlungen vorzunehmen. Bei der EncroChat-Überwachung handelt es sich um eine eigenständige Untersuchungshandlung französischer Behörden.

Der französische Datenabgriff erfolgte, indem eine Schadsoftware auf tausende Endgeräte aufgespielt wurde, welche die Daten aus diesen ausleitete.[884] Dies stellt nicht nur einen *hochinvasiven Eingriff in das Fernmeldegeheimnis*[885], sondern aufgrund der Streubreite auch eine dem schweizerischen Recht *unbekannte* Massnahme dar[886]. Somit wäre diese Massnahme selbst hypothetisch weder der Rechtshilfe noch der Bewilligung nach Art. 271 StGB zugänglich gewesen. Zweifelsfrei liegt somit eine Territorialitätsverletzung vor[887], sodass die Daten, die in der Schweiz ausgeleitet wurden, *absolut unverwertbar* sind.

VII. SkyECC

1. Uneinheitliche Bewertung

Die territorialitätsrechtliche Beurteilung der SkyECC-Überwachung ist umstritten. Teils bewerten kantonale Gerichte die Kontaktierung durch den

883 Vgl. LG Berlin, Urt. v. 19.12.2024 – 525 KLs 8/22, Rn. 215 ff., wonach die Verletzung von Art. 31 RL EEA zu einer relativen Unverwertbarkeit führt.

884 Siehe vorstehend A.I.6.

885 Siehe vorstehend I.III.1.

886 Siehe vorstehend J.IV.2.b) und V.

887 So auch Graf, Jusletter, S. 21 f.

MITM-Server als Territorialitätseingriff,[888] was jedoch nicht ohne Widerspruch geblieben ist.[889] Gegen einen Territorialitätseingriff wird angeführt, dass die Massnahme nicht in der Schweiz zu verorten sei, da die Endgeräte mit dem SkyECC-Netzwerk in Frankreich verbunden waren.[890] Ferner sei die Provokation der Zugangsdaten nicht durch Hacking, sondern unter Auslösen einer protokollkonformen Funktion erfolgt, sodass es an einer Eingriffsintensität fehle.[891]

2. Territorialitätsverletzung

Richtigerweise ist die Kontaktierung der Endgeräte durch den MITM-Server in der *Schweiz zu verorten*, da diese Kontaktierung einen *Datenverarbeitungsvorgang* im Endgerät auslöste.[892] Ohne Bedeutung ist, über welches Netzwerk die Kommunikation abgewickelt wurde.[893]

Das schweizerische Recht kennt ausserhalb von Art. 32 lit. b CCC keine Bestimmung, die ausländische Behörden dazu ermächtigt, in der Schweiz eigenständig Untersuchungshandlungen vorzunehmen.[894] Bei der Kontaktierung durch den MITM-Server handelt es sich um eine eigenständige Fernmeldeüberwachung der französischen Behörden auf schweizerischem Territorium. Dieser Datenabgriff erfolgte in einer Weise, die dem schweizerischen Recht unbekannt ist[895], sodass die Massnahme auch hypothetisch nicht der Rechtshilfe oder der Bewilligung nach Art. 271 StGB zugänglich gewesen wäre.

Aufgrund der akzessorischen Bewertung von Zugangsdaten stellt diese Kontaktierung einen Eingriff in das *Fernmeldegeheimnis* (Art. 13 Abs. 1 BV) dar.[896] Dies bewirkt, dass eine hinreichende Eingriffsintensität vorliegt – unabhängig

888 Von einer Territorialitätsverletzung gingen namentlich das OGer ZH SB240422 vom 15. August 2025, AppGer BS SB.2023.48 vom 3. Oktober 2025 (SB.2023.48), das BG Dietikon DG240038 vom 19. Juni 2025, sowie das KG See-Gaster Uznach ST.2025.7-GS1S vom 21. Oktober 2025 aus.

889 Vgl. GRAF, Jusletter, S. 22 f.

890 Nach Informationen des Verfassers wird die Ansicht von Teilen der Behörden in der Schweiz vertreten.

891 GRAF, Jusletter, S. 22 f.; siehe Kommentar von «Laie» vom 26.08.2025 zum Blogbeitrag vom 23.08.2025 «Absolut unverwertbar: SkyECC-Daten» auf strafprozess.ch <https://www.strafprozess.ch/skyecc/>.

892 Siehe vorstehend D.V.2.

893 Siehe vorstehend D.III.

894 Vgl. GLESS, ZStrR, S. 90.

895 Siehe vorstehend J.IV.3.d) und V.2.

896 Siehe vorstehend I.III.2.c).

davon, dass die Massnahme möglicherweise protokollkonform (ohne Hacking) erfolgte.[897] Eine allfällige informelle Duldung seitens Schweizer Behörden vermag diesen Eingriff nicht zu rechtfertigen. Dementsprechend liegt eine Territorialitätsverletzung vor, sodass jene Daten, die mit den in der Schweiz generierten Zugangsdaten entschlüsselt wurden, *absolut unverwertbar* sind.

VIII. Anom

1. Uneinheitliche Bewertung

Umstritten ist, ob die Anom-Überwachung einen Eingriff in die territoriale Integrität der Schweiz darstellt. In der Literatur wird die Anom-Operation als Territorialitätseingriff gewertet.[898] In vereinzelter kantonaler Praxis hingegen wird ein Territorialitätseingriff verneint.[899] Gegen einen Territorialitätseingriff wird angeführt, dass die Datenbearbeitung in den USA stattgefunden hat und die Nachrichtenausleitung nicht über eine technische Manipulation, sondern über Täuschung erfolgt sei.[900]

2. Territorialitätsverletzung

Die Anom-Überwachung ist anhand der Endgeräte und somit in der Schweiz zu lokalisieren.[901]

Darüber hinaus stellt die Anom-Operation richtigerweise eine Territorialitätsverletzung dar.[902]

Das schweizerische Recht kennt ausserhalb von Art. 32 lit. b CCC keine Bestimmung, die ausländische Behörden dazu ermächtigt, in der Schweiz eigenständig Untersuchungshandlungen vorzunehmen. Das Distribuieren von Geräten mit heimlicher Ausleitungsfunktion stellt eine dem schweizerischen Recht gänzlich unbekannte Form der *Fernmeldeüberwachung* dar.[903] Aufgrund des Eingriffs in das Fernmeldegeheimnis ist es unbeachtlich, dass der Nutzer

897 Vgl. vorstehend P.II.2. und P.IV.
898 Vgl. Graf, Jusletter, S. 23; Jaklin, Kryptophones, S. 1015.
899 OGer AG SST.2024.189 vom 23. Mai 2025.
900 OGer AG SST.2024.189 vom 23. Mai 2025, E. 2.7.4.
901 Siehe vorstehend D.V.3.
902 Vgl. Graf, Jusletter, S. 23; Jaklin, Kryptophones, S. 1015.
903 Siehe vorstehend I.III.3. sowie J.IV.4. und V.

das Gerät eigeninitiativ erwarb und freiwillig kommunizierte. Darüber hinaus bewirkt das Fernmeldegeheimnis, dass die bundesgerichtliche Rechtsprechung hinsichtlich verdeckter Ermittlungen mit Auslandsbezug nicht anwendbar ist.[904] Eine allfällige informelle Duldung seitens der Schweizer Behörden könnte den Territorialitätseingriff nicht rechtfertigen. Dementsprechend liegt eine Territorialitätsverletzung vor, sodass jene Daten, die in der Schweiz ausgeleitet wurden, *absolut unverwertbar* sind.

IX. Verwertbarkeit bei transnationaler Kommunikation

Bei einer transnationalen Kommunikation ist ein Teil der Überwachungsmassnahme jeweils in einem anderen Staat zu lokalisieren. Grundsätzlich hätten die Strafverfolgungsbehörden in diesem Fall festzustellen, in welchem Staat die jeweilige Nachrichtenausleitung/Schlüsselpreisgabe stattgefunden hat. Dies wäre dann im Lichte des einschlägigen drittstaatlichen Territorialitätsrechts zu würdigen. Allerdings sind die vorliegenden Darstellungen zur Vorgehensweise lediglich *Arbeitshypothesen*.[905] Dementsprechend ist nicht rechtsgenügend erstellt, in welchem Endgerät die Nachrichtenausleitung/Schlüsselpreisgabe stattgefunden hat. Gemäss dem Grundsatz *in dubio pro reo* ist somit die gesamte Kommunikation – unabhängig vom Aufenthaltsstaat des Chatpartners – als bemakelt zu erachten und diese *in toto* absolut unverwertbar.

904 Siehe vorstehend P.II.2.
905 Siehe vorstehend E.VI.1.

Q. Zusammenfassung

I. Lokalisierung der Massnahmen und anwendbares Recht

Bei den Überwachungsmassnahmen von EncroChat, SkyECC und Anom handelt es sich um Massnahmen, die von ausländischen Behörden durchgeführt worden sind. Sofern sich jedoch das einzelne Endgerät in der Schweiz befand, sind die Massnahmen in der Schweiz zu verorten[906] und insofern im Lichte des *schweizerischen Rechts* typologisch einzuordnen und zu würdigen[907].

II. Vertrauensprinzip

Im Rahmen der internationalen Strafverfolgung ist das Vertrauensprinzip zu berücksichtigen. Dieses aus der Rechtshilfe stammende Prinzip ist nur im limitierten Ausmass auf das Strafverfahren übertragbar. Im Strafverfahren ist das Vertrauensprinzip in *rechtlicher Hinsicht* auf die Vermutung zu beschränken, dass eine ausländische Massnahme nach dem ausländischen Recht rechtmässig war. Im Hinblick auf die *Sachverhaltserstellung* hat das Vertrauensprinzip hingegen keine Bedeutung im Strafverfahrensrecht. Dementsprechend handelt es sich bei den ausländischen Darstellungen zum Überwachungsvorgehen allenfalls um *Arbeitshypothesen*, nicht aber um rechtsgültig erstellte Tatsachen.[908]

III. Hybrider Massnahmencharakter

Die Qualifizierung der Massnahmen erweist sich als anspruchsvoll, da die Überwachungen einen hybriden Charakter aufweisen. Aus *systematischer* Optik liegen *präventiv-polizeirechtliche* Massnahmen vor, da es sich um verdachtsunabhängige, grundrechtsinvasive Massnahmen zum Zwecke der Verbrechensbekämpfung handelt.[909] Aus *struktureller* Perspektive rücken die Massnahmen in die Nähe von *geheimdienstlichen* Operationen. Dies ergibt

906 Siehe vorstehend D.
907 Siehe vorstehend F.III.
908 Siehe vorstehend E.
909 Siehe vorstehend G.IV.

sich zum einen aus der Tatsache, dass die Massnahmen Massenüberwachungen (bulk interception) darstellen, was im schweizerischen Recht nur im NDG (Art. 38 f.) vorgesehen ist.[910] Zum anderen erinnert auch die Vorgehensweise teils an das geheimdienstliche Instrumentarium (vgl. Art. 26 Abs. 1 lit. d Ziff. 1 NDG). Aus *funktioneller* Betrachtung handelt es sich jedoch um *strafprozessuale* Massnahmen, da es sich um Fernmeldeüberwachungen zum Zwecke der Strafverfolgung handelt.[911]

IV. Typologisch unbekannte Massnahmen

Unabhängig von der vorstehenden Zuordnung handelt es sich bei den Überwachungen um Eingriffe in das Fernmeldegeheimnis (Art. 13 Abs. 1 BV).[912] Die Überwachung des Fernmeldeverkehrs ist abschliessend vom Bundesrecht geregelt (vgl. Art. 92 Abs. 1 BV). Das Strafprozessrecht sieht einen Massnahmenkatalog zur Fernmeldeüberwachung in Art. 269 ff. StPO vor. Ausserhalb des Strafverfahrens kann das Fernmeldegeheimnis im Rahmen der Rechtshilfe (Art. 18a f. IRSG), der Personensuche (Art. 35 f. BÜPF) oder nachrichtendienstrechtlich (Art. 26 NDG) überwacht werden.[913] Diese ausserstrafprozessualen Massnahmen dürfen jedoch das Strafverfahrensrecht nicht umgehen. Dementsprechend sind Ergebnisse von ausserstrafprozessualen Überwachungen strafprozessual nur verwertbar, wenn die Massnahme auch im Strafverfahrensrecht vorgesehen ist.[914]

Vorliegend wurden die Massnahmen eigenständig von ausländischen Behörden durchgeführt, sodass die vorstehenden Bestimmungen von Vornherein nicht einschlägig sind. Nichtsdestotrotz sind die Massnahmen im Lichte des schweizerischen Rechts typologisch einzuordnen.[915] Während die EncroChat-Überwachung gewisse Ähnlichkeiten mit einer GovWare i.S.v. Art. 269ter StPO aufweist, verfügt die Provokation der SkyECC-Schlüssel über Ähnlichkeiten mit der nachrichtendienstrechtlichen Massnahme nach Art. 26 Abs. 1 lit. d Ziff. 1 NDG. Nichtsdestotrotz können die Massnahmen aufgrund ihrer Streubreite nicht in diese Bestimmungen eingeordnet werden. Überhaupt keinen Anknüpfungspunkt im schweizerischen Recht hat die Anom-Überwachung.

910 Siehe vorstehend H.II.
911 Vgl. vorstehend J.IV.1.
912 Siehe vorstehend I.III.
913 Siehe vorstehend J.
914 Siehe vorstehend C.III.
915 Zur typologischen Einordnung siehe vorstehend J.IV f.

Im Ergebnis handelt es sich somit bei sämtlichen Überwachungen um Massnahmen, die dem schweizerischen Recht typologisch unbekannt sind. Nach der hier vertretenen Ansicht führt dieser Umstand, da es sich um schwere Grundrechtseingriffe handelt, zur absoluten Unverwertbarkeit.[916]

V. Verletzung des Richtervorbehaltes

Eine Fernmeldeüberwachung bedarf von Verfassungs wegen einer *richterlichen Genehmigung*. Der Genehmigungsvorbehalt gilt ausnahmslos bei sämtlichen Formen der Fernmeldeüberwachung des schweizerischen Rechts (strafprozessual und ausserstrafprozessual). Einzig ein Schweizer Gericht kann diese verfassungsrechtliche Anforderung erfüllen, da allein dessen Genehmigung Gewähr leistet, dass das schweizerische Recht eingehalten ist. Entgegen der verfassungsrechtlichen Vorgabe fehlt es den vorliegenden Überwachungen an einer Genehmigung eines Schweizer Zwangsmassnahmengerichts. Aus diesem Defizit folgt die absolute Unverwertbarkeit (Art. 277 StPO).[917]

VI. Verletzung des Täuschungsverbotes

Ferner ist bei den Überwachungsmassnahmen das Täuschungsverbot von Art. 140 Abs. 1 StPO zu beachten, welches ein absolutes Verwertbarkeitsverbot nach sich zieht (Art. 141 Abs. 1 StPO). Nach der hier vertretenen Ansicht stellt lediglich die Anom-Überwachung eine unzulässige Täuschung dar. Anders als bei der EncroChat- und SkyECC-Überwachung, die rein technischer Natur sind, basiert die Anom-Überwachung auf einer kommunikativen und somit unzulässigen Täuschung.[918]

VII. Verletzung der Mitteilungspflicht

Eine Fernmeldeüberwachung ist der betroffenen Person von Verfassungs wegen nachträglich mitzuteilen. Diese Garantie gilt sowohl bei den strafprozessualen als auch den ausserstrafprozessualen Fernmeldeüberwachungen.[919] Das schweizerische Strafverfahrensrecht kennt indes eine gesetzliche Grund-

916 Siehe vorstehend L.I.
917 Siehe vorstehend L.II.
918 Siehe vorstehend L.III.
919 Siehe vorstehend M.II.; einzig bei der nachrichtendienstlichen Funk- und Kabelaufklärung nach Art. 38 f. NDG besteht keine Mitteilungspflicht.

lage für einen Mitteilungsverzicht (Art. 279 Abs. 2 StPO, ähnlich Art. 33 Abs. 2 NDG). Die gesetzliche Folge einer *rechtmässigen* Mitteilungsunterlassung ist jedoch, dass die Erkenntnisse *nicht* zu Beweiszwecken verwertet werden dürfen (Art. 279 Abs. 2 lit. a StPO). Dabei handelt es sich nach der hier vertretenen Auffassung um ein *absolutes Verwertbarkeitsverbot*.

Vorliegend wurden die Nutzer weder von den ausländischen noch von den Schweizer Behörden nachträglich über die Überwachung informiert. Dieser Mitteilungsunterlassung liegt entgegen der gesetzlichen Vorgabe keine richterliche Zustimmung zugrunde. Da jedoch bereits die rechtmässige Mitteilungsunterlassung zu einem absoluten Verwertbarkeitsverbot führt, hat die fehlende richterliche Zustimmung keine spezifische Folge.[920]

VIII. Verletzung der Beschwerdegarantie

Eine überwachte Person hat von Verfassungs wegen einen Anspruch auf eine Beschwerdemöglichkeit. Diese Beschwerdegarantie gilt sowohl bei einer strafprozessualen als auch bei einer ausserstrafprozessualen (IRSG, BÜPF oder NDG) Überwachung. Ist der Beschwerdeweg aufgrund institutioneller Gründe ausgeschlossen, so kann die fehlende Beschwerde nicht durch das Sachgericht geheilt werden. Bei den vorliegenden Überwachungsmassnahmen stand dem Nutzer weder im überwachenden Staat noch in der Schweiz eine Beschwerdemöglichkeit zur Verfügung. Ein hypothetischer Beschwerdeweg im Ausland wäre unzureichend, da dieser keine hinreichende Überprüfung des schweizerischen Rechts gewährleistet. Ein hypothetischer Beschwerdeweg (oder Überprüfung durch das Sachgericht) entfällt auch in der Schweiz, nicht zuletzt wegen des Informationsdefizites eines Schweizer Gerichts. Aus diesem rechtsstaatlichen Defizit folgt nach der hier vertretenen Auffassung die absolute Unverwertbarkeit.[921]

IX. Verletzung des rechtlichen Gehörs

Stützt sich eine Beweisführung auf digitale Kommunikationsdaten, so sind die Rohdaten grundsätzlich in die Verfahrensakte aufzunehmen. Das vorliegende Fehlen der Rohdaten verletzt zunächst die *Aktenführungs-* und *Beschaffungspflicht*. Gleichzeitig führt das Fehlen der Rohdaten zu einer faktischen, nicht formal verfügten Einschränkung des *Akteneinsichtsrechts*. Aus materi-

920 Siehe vorstehend M.II.2.b).
921 Siehe vorstehend M.III.4.

eller Sicht vermag ein ausländisches Staatsinteresse im Strafverfahren das Akteneinsichtsrecht mangels Rechtsgrundlage nicht einzuschränken (Art. 108 StPO *e contrario*). Aufgrund dieser Defizite liegen schwere, nicht heilbare Gehörsverletzungen vor. Diese führen dazu, dass die Beweise nicht zum Nachteil des Beschuldigten verwendet werden dürfen.[922]

X. Verletzung des Fair Trial-Grundsatzes (Art. 6 und Art. 8 EMRK)

Gemäss Art. 6 Ziff. 1 EMRK hat die beschuldigte Person Anspruch auf ein faires Verfahren. In der Gesamtbetrachtung ist zu berücksichtigen, dass es sich bei den Massnahmen um *Massenüberwachungen* handelt. Die vom EGMR aufgestellten Kriterien zur Massenüberwachung sind in grober Weise verletzt. Ferner befindet sich die beschuldigte Person aufgrund der fehlenden Rohdaten und mangels belastbarer Informationen zur Datenerhebung in einem Informationsdefizit. Dieses Defizit lässt zweifelsfrei eine Kompensationspflicht seitens der Strafverfolgungsbehörden entstehen. Schweizer Strafbehörden sind jedoch ausser Stande, wirksame kompensatorische Massnahmen zu ergreifen, da sie unter denselben Informationsdefiziten leiden. Somit sind die Garantien von Art. 6 und Art. 8 EMRK in grober Weise verletzt, wobei sich die Verwertbarkeitsfolgen nach der StPO richten.[923]

XI. Verletzung des Territorialitätsprinzips

Das Territorialitätsprinzip schützt den Exklusivitätsanspruch der Schweizer Behörden, innerhalb der Staatsgrenzen staatliche Handlungen vorzunehmen. Das Territorialitätsprinzip ist verletzt, wenn eine ausländische Massnahme in der Schweiz eine hinreichende Wirkung entfaltet. Bei den vorliegenden Überwachungen handelt es sich um schwerwiegende Eingriffe in das Fernmeldegeheimnis, die eigenständig von ausländischen Behörden in der Schweiz durchgeführt wurden. Das schweizerische Recht kennt jedoch ausserhalb von Art. 32 lit. b CCC keine Bestimmung, die ausländische Behörden dazu ermächtigt, in der Schweiz eigenständig Untersuchungshandlungen vorzunehmen. Darüber hinaus sind die Massnahmen dem schweizerischen Recht typologisch gänzlich unbekannt, sodass sie weder der Rechtshilfe noch der Bewilligung nach Art. 271 StGB zugänglich gewesen wären.

---

922 Siehe vorstehend N.

923 Siehe vorstehend O.

Ein allfälliges stillschweigendes Dulden von Seiten der Schweizer Behörden vermag einen Territorialitätseingriff nicht zu rechtfertigen. Dementsprechend verletzen die Massnahmen die territoriale Integrität der Schweiz, woraus ein absolutes Verwertbarkeitsverbot resultiert.[924]

[924] Siehe vorstehend P.

R. Fazit

Die vorliegenden Überwachungsmassnahmen stellen eine massive Überforderung unseres Rechtssystems dar. Aufgrund des hybriden Massnahmencharakters, der polizeirechtliche, nachrichtendienstrechtliche und strafprozessuale Komponente aufweist, ist eine Einordnung in das schweizerische Rechtssystem unmöglich.

Bei Lichte betrachtet treten jedoch – unabhängig von der strukturellen Einordnung – schwere Verletzungen von BV und EMRK zu Tage. Das Schlüsselelement ist, dass die Massnahmen in das *Fernmeldegeheimnis* (Art. 13 Abs. 1 BV) eingreifen. Die damit verbundenen verfassungsrechtlichen Anforderungen (Gesetzesvorbehalt, Genehmigungsvorbehalt, nachträgliche Mitteilung, Bereitstellung eines Beschwerdewegs) sind nicht erfüllt. Gleiches gilt ferner für die allgemeinen Verfahrensgarantien des Akteneinsichtsrechts und des fairen Verfahrens. Zu guter Letzt ist auch das Territorialitätsprinzip verletzt. All diese Gründe führen bereits für sich betrachtet zu strikten Verwertbarkeitsverboten.

Die Anzahl und Eindeutigkeit dieser Verwertbarkeitshindernisse wirft die Frage auf, wieso überhaupt ein Dissens hinsichtlich der Verwertbarkeit besteht. Bestenfalls ist dies darauf zurückzuführen, dass einige Strafbehörden vor lauter Bäumen den Wald nicht mehr sehen. Schlimmstenfalls liegt es an einer groben Geringschätzung unseres Verfahrensrechts und Rechtsstaates.

Es ist trivial, dass eine internationale Kooperation der Strafverfolgungsbehörden zur Bekämpfung der organisierten Kriminalität unerlässlich ist. Ebenso trivial ist es jedoch, dass die Strafverfolgungsbehörden dabei an die BV, das Völkerrecht und das inländische Verfahrensrecht gebunden sind. Die untersuchten Massnahmen sind keinesfalls mit diesen Rechtsquellen vereinbar.

Die Verwertung der vorliegend interessierenden Daten würde substantielle Änderungen der BV, StPO, EMRK und CCC voraussetzen. Nicht zuletzt wäre eine gänzlich neue Abgrenzungskonzeption zwischen präventivem Sicherheitsrecht und repressivem Strafprozessrecht erforderlich. All diese Änderungen sind jedoch allein dem entsprechenden legiferierenden Organ vorbehalten, keinesfalls den Gerichten.

Die Überwachungsoperationen betreffend SkyECC, Anom und EncroChat beschäftigen derzeit Gerichte in ganz Europa. Die vorliegende Dissertation untersucht die Verwertbarkeit der abgefangenen Textnachrichten im Lichte des schweizerischen Strafverfahrensrechts.

Dabei wird auf unterschiedliche Verwertungshindernisse eingegangen, etwa das Fehlen einer schweizerischen Überwachungsgenehmigung, den mangelhaften Rechtsschutz oder das Territorialitätsprinzip. Die Arbeit kommt zum Ergebnis, dass die Daten nicht verwertbar sind.