

Die Verwertbarkeit von AnomChat-Daten im Strafprozess

von Alicia Althaus und Justin Samek*

Abstract

Die steigende Bedeutung digitaler Daten als Beweismittel im Strafverfahren zeigt sich am Beispiel des AnomChats. In jüngster Zeit konnten deutsche Ermittlungsbehörden mit Hilfe von Chatdaten aus einem Chat namens Anom Erfolge bei der Bekämpfung der organisierten Kriminalität erzielen. Die Erhebung der Daten erfolgte jedoch über unbekannte ausländische Behörden unter unklaren Umständen, was die Gefahr der Umgehung rechtsstaatlicher Prinzipien in sich birgt. Der Beitrag widmet sich der Beweisverwertung der im Ausland gewonnenen AnomChat-Daten im deutschen Strafprozess. Dazu wird zunächst auf die europarechtliche Dimension der Datenerhebung eingegangen, um in einem zweiten Schritt die Verwertbarkeit im deutschen Strafprozess zu beurteilen. Der Beitrag schließt mit einer rechtspolitischen Diskussion der Thematik und der Forderung nach Einhaltung rechtsstaatlicher Verfahren.

The increasing importance of digital data as evidence in criminal proceedings is illustrated by the example of AnomChat. Recently, German investigative authorities have achieved success in the fight against organized crime using chat data from a chat called Anom. However, this data was collected by unknown foreign authorities under unclear circumstances, which bears the risk of circumventing the principles of the rule of law. This article examines the use of AnomChat data obtained abroad as evidence in German criminal proceedings. It begins by exploring the European law dimension of data collection, then assesses its usability in German criminal proceedings. The article concludes with a legal policy discussion on the topic and the demand for compliance with constitutional procedures.

I. Einleitung

Die Verwertbarkeit von EncroChat-Daten im Strafprozess war bereits Gegenstand höchstrichterlicher Rechtsprechung in Deutschland, in anderen europäischen Staaten¹ und in Luxemburg, wo der *EuGH* kürzlich über eine Vorlagefrage des *LG Berlin* entschied.² Auch vor dem *EGMR* sind zwei Verfahren anhängig, die Rechtsfragen über die

Verwertbarkeit von EncroChat-Daten betreffen.³ Bevor die Fragen nach der Verwertbarkeit von EncroChat-Daten vollends geklärt sind, bahnt sich bereits ein neuer Chat namens Anom seinen Weg durch den Instanzenzug der deutschen Strafgerichtsbarkeit. Bisher besteht zum AnomChat noch keine einheitliche Rechtsprechungslinie.⁴ Die Unterschiede in den Sachverhalten zwischen AnomChat und EncroChat sind so signifikant, dass eine bloße Verweisung auf höchstrichterliche Urteile wie in Luxemburg nicht ausreicht, um die rechtlichen Fragen bezüglich der Verwertbarkeit von AnomChat-Daten in Deutschland zu klären. Angesichts der erheblichen Unterschiede zwischen den Hintergründen von AnomChat und EncroChat ist eine eingehende Untersuchung dieser Thematik erforderlich. Die nachfolgende Untersuchung stellt zunächst die wesentlichen Unterschiede zwischen dem EncroChat und dem AnomChat dar. Anschließend wird die europäische Rechtslage bewertet, bevor auf mögliche Beweisverwertungsverbote auf nationaler Ebene eingegangen wird.

1. Der AnomChat

Das Federal Bureau of Investigation (FBI) entwickelte vor etwa fünf Jahren einen Krypto-Messengerdienst namens AnomChat. Der AnomChat wurde in „kriminellen Kreisen“ beworben, indem das System den Nutzern abhörsichere und verschlüsselte Anonymität für ihre Kommunikation vortäuschte. Der tatsächliche Zweck des AnomChats war jedoch das heimliche Abfangen und Mitlesen von Nachrichten. Mit welchem Ziel das FBI das System einführte, ob zur Gefahrenabwehr oder Strafverfolgung, ist unbekannt.⁵

Um seinen Zweck zu erfüllen, kopierte der AnomChat automatisch alle außerhalb der USA versendeten Nachrichten und leitete diese an einen zentralen Server an einem unbekanntem Standort außerhalb der USA weiter. Es ist nur so viel bekannt, dass das FBI im Sommer 2019 nach einem „Drittland“ außerhalb der USA suchte, um dort einen Server zur Erhebung der AnomChat-Daten einzurichten. Fündig wurde das FBI angeblich in einem Mitgliedsstaat der EU. Dem „Drittland“ sicherte das FBI aus unbe-

* Alicia Althaus ist Rechtsanwältin in der Kanzlei Traut, Wiesbaden, und promoviert an der Goethe-Universität im Bereich des Strafrechts. Ass. Jur. Justin Samek ist LL.M.-Kandidat an der NYU und promoviert an der Goethe-Universität im Bereich des Europarechts und Individualrechtsschutzes.

¹ *BGH*, NJW 2022, 1539; *Französischer Conseil constitutionnel*, Entscheidung v. 8.4.2022 – 2022-987 QPC, online abrufbar unter: <https://www.conseil-constitutionnel.fr/decision/2022/2022987QPC.htm> (zuletzt abgerufen am 21.6.2024); *Corte di Cassazione IV Criminal Section* v. 15.7.2022 – 32915/22, online abrufbar unter: <https://canestrinilex.com/en/readings/du-process-requires-transparency-of-evidence-gathering-in-sky-ecc-proceeding-cass-3291522> (zuletzt abgerufen am 21.6.2024).

² *EuGH*, Urt. v. 30.4.2024 – Rs. C-670/22.

³ *EGMR*, Urt. v. 3.1.2022 – 44715/20 und 47930/21.

⁴ *OLG Frankfurt a.M.*, NJW 2022, 710; *OLG Saarbrücken*, MMR 2023, 697 Rn. 5; *OLG München*, BeckRS 2023, 30017; *LG Memmingen*, BeckRS 2023, 26989.

⁵ Eine ausführliche Sachverhaltsdarstellung findet sich in: *United States District Court (California)*, v. 17.5.2021 – 21MJ01948, S. 6 ff., online abrufbar unter: <https://storage.courtlistener.com/recap/gov.uscourts.casd.707623/gov.uscourts.casd.707623.1.0.pdf> (zuletzt abgerufen am 21.6.2024); *LG Memmingen*, BeckRS 2023, 26989 Rn. 54 ff.

kannten Gründen zu, dass dessen Identität geheim gehalten wird. Ab Oktober 2019 erhob das unbekanntes Drittland die Daten des AnomChat-Servers bis ins Jahr 2021 aufgrund eines (unbekannten) gerichtlichen Beschlusses und leitete sie an das FBI im Wege einer Rechtshilfe weiter.

Nachdem die Generalstaatsanwaltschaft Frankfurt am Main erfuhr, dass die Daten Informationen über mögliche Straftaten in Deutschland enthalten, stellte sie ein Rechtshilfeersuchen an die US-amerikanischen Justizbehörden. Das FBI erteilte die Erlaubnis zur offiziellen Verwendung der Daten in Ermittlungs- und Gerichtsverfahren, machte jedoch deutlich, dass keine weiteren Informationen über das „Drittland“ preisgegeben werden würden.⁶

Derzeit ist die Identität des „Drittlands“ sowohl dem Bundeskriminalamt als auch der Generalstaatsanwaltschaft Frankfurt M. unbekannt. Auch die Bundesregierung antwortete auf Anfrage einer Bundestagsfraktion vom 29.3.2023 hinsichtlich der Frage „Ist dem BKA dieser Drittstaat bekannt, und falls nein, aus welchem Grund bleibt dieser geheim?“: „Der Drittstaat ist dem Bundeskriminalamt ebenso wenig bekannt wie der Grund für dessen Geheimhaltung durch das FBI.“⁷

2. Wesentliche Unterschiede zum EncroChat

Der wesentliche Unterschied zwischen den AnomChat- und EncroChat-Fällen liegt in der Herkunft der Daten. Bei den EncroChat-Fällen war der Server bekanntermaßen in Frankreich und es gab gerichtliche Beschlüsse zur Datenbeschlagnahme.⁸ Im Gegensatz dazu ist im Fall des AnomChats die Herkunft der Daten unbekannt und nicht überprüfbar. Dies führt zu erheblicher Unsicherheit, da sich das „Drittland“ theoretisch auch außerhalb der EU befinden könnte. Eine weitere Theorie ist, dass es sich bei dem „Drittland“, aus dem die Daten stammen, möglicherweise um Deutschland handelt.⁹ Dieser Unterschied führt zu einer komplexen rechtlichen Situation in den Verfahren um AnomChat.

II. Der AnomChat und europäisches Recht

Bevor die Verwertbarkeit der AnomChat-Daten auf nationaler Ebene einer rechtlichen Bewertung unterzogen wird, soll vorab die europäische Rechtslage beleuchtet werden. Dabei beschränkt sich die Darstellung auf die europäische Rechtshilfe, die Gegenstand der *EuGH*-Entscheidung im EncroChat-Verfahren war, und mögliche Verletzungen der EMRK, die Gegenstand der EncroChat-Verfahren vor dem *EGMR* sind.

1. Europäische Rechtshilfe und der AnomChat

Die Befugnisse von nationalen Ermittlungsbehörden beschränken sich grundsätzlich auf ihr Hoheitsgebiet. Europaweit leisten sich die Ermittlungsbehörden auf der Grundlage verschiedener Abkommen in Strafsachen jedoch Rechtshilfe.¹⁰ Die europäische Rechtshilfe basiert auf dem Grundsatz der gegenseitigen Anerkennung nach Art. 82 AEUV und erfordert ein hohes Maß an Vertrauen zwischen den Mitgliedstaaten.¹¹ Die Anwendung des Grundsatzes stößt im Fall der AnomChat-Daten auf unterschiedliche Hindernisse.

a) Anwendung der RL-EAA auf den AnomChat

Die Anwendung der Richtlinie 2014/41/EU über die Europäische Ermittlungsanordnung in Strafsachen (RL-EAA) im Kontext der EncroChats war Gegenstand eines Vorabentscheidungsverfahrens vor dem *EuGH*.¹² Gegenstand der Vorlagefragen war die Vereinbarkeit der deutschen Ermittlungsanordnungen mit der RL-EAA.¹³ Nachfolgend werden die wesentlichen Erkenntnisse der Entscheidung dargestellt und erklärt, wieso der AnomChat die Anforderungen des *EuGH* an eine rechtmäßige Ermittlungsanordnung gemäß der RL-EAA nicht erfüllen kann.

Der *EuGH* betont, dass die RL-EAA interne Mechanismen vorsieht, durch die die Grundrechte der betroffenen Personen, wie die Verteidigungsrechte und das Recht auf ein faires Verfahren, gewahrt werden.¹⁴ Die Gerichte können solche schwerwiegenden Verstöße im jeweiligen Verfahren, das sich gegen die Ermittlungsanordnung richtet, überprüfen und gegebenenfalls prozessuale Konsequenzen hinsichtlich der Beweismittel ziehen.¹⁵ Zudem bestätigte der *EuGH*, dass der Mitgliedstaat, in dessen Hoheitsgebiet die Überwachung stattfindet, von der Überwachungsmaßnahme unterrichtet werden muss.¹⁶ Damit soll der zuständigen Behörde des Mitgliedstaates die Möglichkeit gegeben werden, die Überwachungsmaßnahmen zu beenden, wenn die innerstaatlichen Voraussetzungen für deren Durchführung nicht vorliegen.¹⁷ Schließlich stellt der *EuGH* fest, dass die Verteidigungsrechte der Betroffenen gewahrt werden müssen. Dazu gehört insbesondere die Einhaltung eines fairen rechtsstaatlichen Verfahrens. Konkret muss sich der Betroffene gegen die Beweismittel verteidigen können. Ist dies nicht der Fall, müssen die Beweismittel im Zweifel unberücksichtigt bleiben.¹⁸

Der AnomChat erfüllt keine der drei dargestellten Voraussetzungen. Denn die Daten wurden bereits nicht durch eine Ermittlungsanordnung nach der RL-EAA von einem bekannten europäischen Staat erlangt. Die Daten des AnomChats übermittelte zunächst ein unbekanntes Drittland, welches sie erhoben und gespeichert hat, im Wege

⁶ *LG Memmingen*, BeckRS 2023, 26989 Rn. 62-63.

⁷ BT-Drs. 20/1249, S. 6.

⁸ Das Untersuchungsgericht in Lille, Frankreich, ordnete die Erhebung der Daten nach französischem Recht an. Am 13.6.2020 genehmigte es die Übersendung und Verwendung der Daten in Deutschland. Diese wurden bis zum 28.6.2020 nach Deutschland versendet. Eine konkrete Darstellung des Ablaufs und weitere Einzelheiten finden sich in *Gebhard/Michalke*, NJW 2022, 655 (656).

⁹ *LG Memmingen*, BeckRS 2023, 26989 Rn. 89.

¹⁰ *Schuster*, ZIS 2016, 564 (565).

¹¹ *EuGH*, Ur. v. 8.12.2020 – Rs. C-584/19, Rn. 39-40.

¹² *LG Berlin*, BeckRS 2022, 28421.

¹³ *GA Capeta*, Schlussantr. v. 26.10.2023 – C-670/22, Rn. 15-16.

¹⁴ *EuGH*, Ur. v. 30.4.2024, Rs. C-670/22, Rn. 104.

¹⁵ *EuGH*, Ur. v. 30.4.2024, Rs. C-670/22, Rn. 103.

¹⁶ *EuGH*, Ur. v. 30.4.2024, Rs. C-670/22, Rn. 108 ff.

¹⁷ *EuGH*, Ur. v. 30.4.2024, Rs. C-670/22, Rn. 118.

¹⁸ *EuGH*, Ur. v. 30.4.2024, Rs. C-670/22, Rn. 130 f.

eines Rechtshilfeersuchens an das FBI in die USA. Das FBI wiederum leitete die Daten dann über Europol an das BKA weiter.¹⁹ Es erfolgte kein unmittelbares Rechtshilfeersuchen einer deutschen Ermittlungsbehörde an denjenigen Mitgliedsstaat, der die Daten erhoben hat. Dies bedeutet, dass die Gerichte keine Möglichkeit haben, das Verfahren auf schwerwiegende Fehler zu überprüfen, da keine Informationen über die unmittelbare Erhebung vorliegen. Darüber hinaus fehlt eine Unterrichtung der deutschen Behörden nach Art. 31 der RL-EEA für eine Erhebung der AnomChat-Daten auf dem Gebiet der Bundesrepublik Deutschland.²⁰ Schließlich können sich die Betroffenen mangels Kenntnis des überwachenden Staates und des dort ergangenen richterlichen Beschlusses sowie anderer Verfahrenshandlungen auch nicht angemessen verteidigen. Über die vom *EuGH* aufgestellten Voraussetzungen hinaus wird der AnomChat-Sachverhalt dem Sinn und Zweck der RL-EEA, gegenseitiges Vertrauen zwischen den Mitgliedstaaten in einem gemeinsamen Raum der Freiheit, der Sicherheit und des Rechts zu schaffen, nicht gerecht. Denn vorliegend fungiert ein Staat außerhalb der EU als Datenmittler.

b) Ein Drittstaat als Datenmittler

Statt der RL-EEA dürften für die Übermittlung der AnomChat-Daten andere Rechtshilfeabkommen relevant sein, da die Daten über einen Umweg aus den USA nach Deutschland gelangten. Zwischen der EU und den USA besteht ein eigenes Rechtshilfeabkommen in Strafsachen.²¹ Im AnomChat-Sachverhalt ist das Abkommen gleich zweimal relevant: zunächst bei der Übermittlung der Daten aus dem unbekanntem Drittland an die USA, wenn es sich um einen Mitgliedstaat handelt. Ein zweites Mal für die Übermittlung der Daten aus den USA nach Deutschland. Da es sich um eine Übermittlung von personenbezogenen Daten gehandelt hat, sind zusätzlich datenschutzrechtliche Aspekte zu berücksichtigen. So besteht für Datenübermittlungen aus der EU in die USA zum Zwecke der Strafverfolgung ein eigenes Abkommen.²² Ohne die Anwendbarkeit der Abkommen vorliegend rechtlich abschließend einzuordnen, ist bereits die Annahme einer Rechtshilfe zweifelhaft.²³ Die Daten aus dem unbekanntem Drittland sind nicht zum Zwecke der Strafverfolgung in die USA weitergeleitet worden. Das Rechtshilfeabkommen zwischen der EU und den USA ist darauf ausgerichtet, dass sich die Staaten gegenseitig bei Ermittlungen im Rechtsraum der EU oder den USA helfen. Die USA fungierte nach derzeitigem Kenntnisstand jedoch nur als Mittler für die Weitergabe der Daten. Sollte es sich bei dem unbekanntem Drittland tatsächlich um einen Mitgliedstaat der EU handeln, würde eine Umgehung der

EEA-RL vorliegen, die Art. 6 Abs. 1 lit. b) EEA-RL verhindern soll.²⁴ Ähnlich dürfte die Rechtslage zu bewerten sein, soweit auf bilaterale Verträge zwischen den USA und Deutschland abgestellt wird.²⁵

2. Die EMRK und der AnomChat

Die Zulässigkeit der Verwertbarkeit von in anderen Mitgliedstaaten gewonnenen Beweismitteln ist bisher unionsrechtlich nicht geregelt.²⁶ Im Einzelfall kann eine Verwertung jedoch einen Verstoß gegen die EMRK darstellen. Aus diesem Grund prüft derzeit auch der *EGMR* die Vereinbarkeit der Erhebung der EncroChat-Daten mit der EMRK.²⁷ Es geht insbesondere um die Frage, ob den betroffenen Personen in Frankreich wirksame Rechtsbehelfe gegen die Maßnahmen zur Verfügung standen oder die Ermittlungsmaßnahmen die Art. 6, 8 und 13 der EMRK verletzen.

Im Unterschied zum AnomChat erfolgte die Datenerhebung in Frankreich auf der Grundlage richterlicher Beschlüsse.²⁸ Im Kontext der AnomChat-Daten sind in den bisher entschiedenen Verfahren keine Informationen über etwaige Beschlüsse in dem unbekanntem Drittland bekannt. Eine Verletzung von Art. 8 EMRK kann nicht ausgeschlossen werden, da vorliegend nicht überprüfbar ist, ob die Verletzung nach Art. 8 Abs. 2 EMRK gerechtfertigt war.²⁹ Zudem könnte ein Verstoß gegen das Recht auf ein faires Verfahren nach Art. 6 EMRK vorliegen. Zwar kann der *EGMR* nicht entscheiden, ob im nationalen Verfahren ein Beweisverwertungsverbot vorliegt. Stattdessen nimmt der *EGMR* eine Gesamtbetrachtung des Sachverhalts vor und prüft, ob das Verfahren insgesamt fair abgelaufen ist.³⁰ Dafür muss der *EGMR* die Umstände der Beweiserlangung überprüfen können, um zu bewerten, ob ein solcher Verstoß vorliegt.³¹ Die Umstände sind vorliegend jedoch nicht bekannt. Es besteht daher die Gefahr, dass anerkannte rechtsstaatliche Prinzipien im Rahmen der Beweiserhebung umgangen worden sein könnten.

Die Kenntnis des für die Erhebung zuständigen Staates und der dortigen Verfahrensweisen ist für die Ausübung des Rechts auf einen wirksamen Rechtsbehelf nach Art. 13 EMRK unerlässlich. Dieses Recht garantiert die Möglichkeit einer rechtsstaatlichen Beschwerde gegen Ermittlungsmaßnahmen.³² Im Rahmen von geheimen Ermittlungsmaßnahmen müssen die betroffenen Personen nicht sofort informiert werden.³³ Die betroffenen Personen sollten spätestens dann informiert werden, wenn die Maßnahme abgeschlossen ist und die Offenlegung keine Gefahr für den weiteren Ermittlungserfolg mehr darstellt.³⁴ Den Betroffenen muss die Entscheidung über die

¹⁹ *OLG München*, BeckRS 2023, 30017, Rn. 60.

²⁰ *GA Čapeta*, Schlussantr. v. 26.10.2023 – C-670/22, Rn. 104 ff.

²¹ Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über Rechtshilfe, ABl. Nr. 2003 L 181/34.

²² Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über den Schutz personenbezogener Daten bei der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten, ABl. 2016 L 336/3.

²³ Näheres zur der Komplexität der Datenübermittlung aus den USA zum Zwecke der Strafverfolgung: *Hilgers*, DÖV 2021, 1074.

²⁴ *EuGH*, Urt. v. 30.4.2024, Rs. C-670/22, Rn. 97.

²⁵ Zu den Rechtshilfeabkommen zwischen Deutschland und USA siehe: *Hilgers*, DÖV 2021, 1074 (1079).

²⁶ *GA Čapeta*, Schlussantr. v. 26.10.2023 – C-670/22, Rn. 116 ff.

²⁷ *EGMR*, Urt. v. 3.1.2022 – 44715/20 und 47930/21.

²⁸ *BGH*, NJW 2022, 1539 Rn. 11.

²⁹ *EGMR*, Urt. v. 10.3.2009 – 4378/02, Rn. 72 ff.

³⁰ *EGMR*, Urt. v. 17.1.2017 – 43000/11 und 49380/11, Rn. 96.

³¹ *EGMR*, Urt. v. 10.3.2009 – 4378/02, Rn. 89 f.

³² *EGMR*, Urt. v. 13.12.2012 – 22689/07, Rn. 78 f.

³³ *EGMR*, Urt. v. 31.7.2012 – 36662/04, Rn. 67.

³⁴ *EGMR*, Urt. v. 7.2.2017 – 35285/08, Rn. 97-99.

Datenerhebung derart mitgeteilt werden, dass sie sich gegen diese rechtlich zu Wehr setzen können.³⁵ Vorliegend ist der Staat, der die Datenerhebung durchgeführt hat, jedoch nicht bekannt. Die Betroffenen hatten nach derzeitigem Kenntnisstand der deutschen Gerichte zu keinem Zeitpunkt die Möglichkeit, einen Rechtsbehelf gegen die Datenerhebung zu erheben.

III. AnomChat und Beweisverwertungsverbote in Deutschland

Mangels höchstrichterlicher Rechtsprechung ist bisher umstritten, ob in der AnomChat-Verfahrensreihe ein Beweisverwertungsverbot vorliegt. Das deutsche Recht kennt kein ausdrückliches Verwertungsverbot für im Wege der Rechtshilfe aus dem Ausland erlangte Daten. Daher entfaltet sich im Diskurs um die Verwendung von erlangten Daten aus dem AnomChat eine komplexe Problematik bezüglich ihrer Zulässigkeit vor deutschen Gerichten. Ein essentieller Aspekt ist hierbei, dass deutsche Gerichte grundlegend nicht verpflichtet sind, die Rechtmäßigkeit von Ermittlungsmaßnahmen, die im Ausland durchgeführt wurden, anhand der dortigen Gesetze zu überprüfen.³⁶ Das impliziert, dass die Verwertbarkeit von im Ausland gesammelten Beweisen grundsätzlich nicht von den nationalen deutschen Vorschriften beeinflusst wird. Dies hat zur Folge, dass die Anwendung von Beweisverwertungsverböten auf Ausnahmefälle beschränkt ist. Ein solcher Ausnahmefall könnte etwa dann vorliegen, wenn die im Ausland erlangten Beweise gegen völkerrechtlich bindende Garantien verstoßen, die dem Schutz individueller Rechte dienen, wie dies in Art. 3 oder Art. 6 EMRK festgelegt ist.³⁷ Zusätzlich kann das Vorliegen eines Beweisverwertungsverbots angenommen werden, wenn die im Ausland durchgeführten Ermittlungen grundlegende rechtsstaatliche Prinzipien verletzt haben oder wenn die Ermittlungen dazu dienen, nationale Vorschriften zu umgehen.³⁸

In der AnomChat-Verfahrensreihe tendiert der Trend innerhalb der Rechtsprechung mittlerweile zu der Annahme eines Beweisverwertungsverbotes, das auf einer Vielzahl von rechtlichen Grundlagen und Umständen der Datenerhebung beruht.³⁹ Entscheidend ist dabei, dass sich die Oberlandesgerichte, die Daten aus dem AnomChat für verwertbar hielten, im Rahmen von Haftvorlagen oder Beschwerdeentscheidungen in einem sehr frühen Stadium mit dem Anom-Komplex befassten. Die Generalstaatsanwaltschaft Frankfurt am Main stellte wesentliche Ermitt-

lungserkenntnisse erst Anfang des Jahres 2023 zur Verfügung. Im Folgenden werden die Argumente dargelegt, welche für ein Beweisverwertungsverbot sprechen.

1. Fehlender konkreter Tatverdacht

Teile der aktuellen Rechtsprechung tendieren dazu, das Vorliegen eines Beweisverwertungsverbots mit der Begründung anzunehmen, dass die Behörden Ermittlungen gegen die Beschuldigten im Rahmen der Anom-Operation ohne konkreten Tatverdacht einleiteten.⁴⁰

Gemäß § 100a StPO ist die Überwachung der Kommunikation nur unter bestimmten Voraussetzungen erlaubt, wozu insbesondere das Vorliegen eines konkreten Tatverdachts gehört. Im Falle von Anom jedoch fehlt es an einem solchen konkreten Tatverdacht, da die Datenerhebung ohne einen spezifischen Verdacht gegen individuelle Nutzer der Anom-App durchgeführt wurde. Die Voraussetzungen des § 100a StPO wurden somit nicht erfüllt und die Datenerhebung kann nicht darauf gestützt werden.⁴¹ Wesentlich ist hierbei, dass das FBI als zentrale Sicherheitsbehörde der USA Strafverfolgungsbehörden und Inlandsgeheimdienst in sich vereint. Dies führt dazu, dass das FBI die Vorfeldaufklärung möglicher Bedrohungen unabhängig von einem konkreten Verdacht betreibt.⁴² Dieses Vorgehen steht allerdings im klaren Widerspruch zu den rechtlichen Anforderungen, die nach deutschem Recht für die Datenerhebung gemäß § 100a StPO gelten. Daher liegt ein Verstoß gegen die grundlegenden Prinzipien rechtsstaatlicher Ermittlungen vor.⁴³

Wesentlich ist daneben, dass die Datenerhebung nicht gegen individualisierte Nutzer, sondern gegen sämtliche Nutzer der App erfolgte. Es existierte gerade keine Einschränkung hinsichtlich bestimmter Zielpersonen, sondern es wurde ohne Vorliegen eines konkreten Tatverdachts ermittelt. Dies erlaubt den Schluss, dass das Hauptziel darin bestand, Verdachtsmomente erst zu generieren. Durch dieses Vorgehen rief der AnomChat einen Irrtum über das Vorliegen abhörsicherer Kommunikation hervor und täuschte die Nutzer. Diese „anlasslose Massenüberwachung“ führte in der Folge zu einem massiven Eingriff in die Privatsphäre und die grundlegenden rechtsstaatlichen Prinzipien. Diese schwerwiegende Verletzung der individuellen Freiheitsrechte ist mit den Prinzipien eines freiheitlich demokratischen Rechtsstaats nicht vereinbar.⁴⁴

³⁵ EGMR, Urt. v. 7.2.2017 – 35285/08, Rn. 105.

³⁶ EuGH, Urt. v. 30.4.2024 – Rs. C-670/22, Rn. 93 ff.; LG Memmingen, BeckRS 2023, 26989 Rn. 72-75 mit Verweis auf BGH, NJW 2022, 1539.

³⁷ LG Memmingen, BeckRS 2023, 26989 Rn. 80.

³⁸ LG Memmingen, BeckRS 2023, 26989 Rn. 84.

³⁹ So etwa LG Memmingen, BeckRS 2023, 26989; a.A. OLG Frankfurt a.M., NJW 2022, 710; OLG Saarbrücken, Beschl. v. 30.12.2022 – 4 HE 35/22; OLG Karlsruhe, Beschl. v. 17.1.2022 – 3 Ws 476/21; OLG Stuttgart, Beschl. v. 21.12.2021 – H 6 Ws 176-177/21; LG Frankenthal, Beschl. v. 7.5.2024 – 2 KLS 5027 Js 19772/23; OLG München, Beschl. v. 19.10.2023 – 1 Ws 525/23; LG Darmstadt, Beschl. v. 14.2.2022 – 18 KLS 1200 Js 83736/21 und Beschl. v. 3.6.2024 – 15 KLS 950 Js 46577/20.

⁴⁰ So auch Derin/Singelstein, NSZ 2021, 449 (452); OLG München, BeckRS 2023, 30017 Rn. 38.

⁴¹ Dies ist auch bei EncroChat der Fall und wird vertieft ausgeführt in Gebhard/Michalke, NJW 2022, 655 (658).

⁴² OLG München, BeckRS 2023, 30017 Rn. 38.

⁴³ A.A. OLG Frankfurt a.M., NJW 2022, 710.

⁴⁴ Derin/Singelstein, StV 2022, 130 (134).

Aufgrund dieser Täuschung stellt sich auch die Frage, ob dieses Vorgehen mit einer rechtsstaatswidrigen Tatprovokation vergleichbar ist. Eine solche liegt vor, wenn ein „agent provocateur“ eingesetzt wurde. Bei einem agent provocateur handelt es sich regelmäßig um verdeckte Ermittler der Polizei, die von den Ermittlungsbehörden eingesetzt werden, um überhaupt erst einen Anfangsverdacht zu generieren.⁴⁵ Dieses Verhalten verstößt gemäß Art. 2 Abs. 1 i.V.m. Art. 20 Abs. 3 GG und Art. 6 Abs. 1 EMRK gegen die allgemeinen Grundsätze eines fairen Strafverfahrens.⁴⁶ In einem solchen Fall wäre das Ermittlungsverfahren gemäß §§ 206a, 260 StPO sofort einzustellen.⁴⁷ Die Gerichte haben daher von Amts wegen zu prüfen, ob ein solcher rechtswidrig zustande gekommener Anfangsverdacht vorliegt. Entscheidend ist dabei, dass objektive Anhaltspunkte für einen Anfangsverdacht vor dem Tätigwerden der Behörde gerade nicht vorgelegen haben.⁴⁸ Darüber hinaus liegt eine rechtsstaatswidrige Tatprovokation insbesondere dann vor, wenn gegen an sich unverdächtige Personen „hartnäckig“ ermittelt wird.⁴⁹ Dies ist beim AnomChat der Fall. Sämtliche Nachrichten wurden zunächst unabhängig von einem Anfangsverdacht über eine vermeintlich sichere Kommunikationsmethode abgefangen und dazu verwendet, überhaupt erst einen Tatverdacht gegen die Betroffenen zu generieren. Sollten die Gerichte dieses Vorgehen als rechtsstaatswidrige Tatprovokation werten, würde dies zu einem Verfahrenshindernis führen.

2. Fehlende Möglichkeit einer Überprüfung der ursprünglichen Ermittlungsmaßnahme

Ein Beweisverwertungsverbot kann zudem auch bestehen, wenn den Beschuldigten die Möglichkeit zur Überprüfung und Verteidigung gegen die Datenerhebung fehlt. Vorliegend ist den deutschen Gerichten die Überprüfung der angelegten Gerichtsbeschlüsse unmöglich. Es existiert noch nicht einmal ein Nachweis darüber, dass die behaupteten Gerichtsbeschlüsse tatsächlich eingeholt wurden.⁵⁰ Diese mangelnde Offenlegung des „Drittlandes“, in dem der Server platziert war, und der fehlende Zugang zu den dort ergangenen gerichtlichen Beschlüssen schaffen eine erhebliche Rechtsschutzlücke.

Wesentlich ist also auch an dieser Stelle, dass das Drittland nicht preisgegeben wird. Dies führt zu dem „paradoxen Ergebnis“, dass ein deutsches Gericht sogar den Gerichtsbeschluss eines anderen deutschen Gerichtes, sollte Deutschland das Drittland sein, nicht überprüfen kann.⁵¹ Es ist daher äußerst fraglich, ob die Daten tatsächlich aufgrund eines Gerichtsbeschlusses erlangt wurden, der rechtsstaatlichen Grundsätzen genügt, wie sie zumindest nach europäischem Recht gelten. Zweifelhaft ist nämlich

insgesamt die Existenz von gerichtlichen Beschlüssen zur Datenerhebung. Es kann nach alledem gerade nicht darauf vertraut werden, dass es sich bei dem Drittstaat um ein europäisches Land handelt und dieses einen rechtmäßigen Gerichtsbeschluss vorweisen kann. Es ist deutschen Gerichten angesichts sämtlicher fehlender Informationen unmöglich, die Herkunft der Daten zu klären, die Einhaltung rechtsstaatlicher Grundsätze zu überprüfen und die Authentizität von Daten und Dokumenten zu verifizieren.

3. Beschneidung der Verteidigungsrechte der Beschuldigten

Aus der fehlenden Möglichkeit der Überprüfbarkeit der ursprünglichen Ermittlungsmaßnahme folgt auch eine Beschneidung der Verteidigungsrechte der Beschuldigten. Dies liegt insbesondere an der bereits erörterten Trennung zwischen beweishebendem und beweisverwertendem Staat, wobei der beweishebende Staat völlig unbekannt bleibt.⁵² Es ist Beschuldigten mangels zugänglicher Gerichtsbeschlüsse oder weiteren Daten zu der Erhebung der Daten nicht möglich, diese zu überprüfen und sich gegebenenfalls gegen sie zu verteidigen.⁵³ Insbesondere ist es aber noch nicht einmal den deutschen Gerichten möglich, diese Gerichtsbeschlüsse zu überprüfen. Auch ihre Aufklärungsarbeit ist daher erheblich eingeschränkt. Dieser Eingriff wirkt sich auch deshalb aus, da zu Beginn der Ermittlungen in den USA gar kein individualisierter Tatverdacht gegen die Betroffenen bestand.⁵⁴ Der in der EU festgelegte Grundsatz der gegenseitigen Anerkennung beruht auf dem Vertrauen der Mitgliedsstaaten in die Fähigkeit der jeweiligen nationalen Rechtsordnungen, einen gleichwertigen Schutz der anerkannten Grundrechte auf Unions- und Grundrechtscharta-Ebene zu gewährleisten.⁵⁵ Jedoch darf dieser Grundsatz nicht dazu führen, dass dem Beschuldigten die Möglichkeit fehlt, die Ursprungsmaßnahme, insbesondere im Hinblick auf die Datenerhebung in einem Drittstaat, vor Gericht zu überprüfen.⁵⁶ Hier offenbart sich eine Rechtsschutzlücke, welche die Grundprinzipien eines fairen Verfahrens verletzt und die Rechte des Beschuldigten einschränkt.

4. Vergleich zu EncroChat-Fällen nicht gegeben

Der BGH entschied unlängst, dass sog. EncroChat-Daten verwertbar seien. Diese Rechtsprechung ist allerdings aufgrund der unterschiedlichen Sachverhalte nicht auf AnomChat-Verfahren übertragbar.⁵⁷ Im Gegensatz zu den EncroChat-Fällen, bei denen der Server in Frankreich stand und von einem französischen Gericht überwacht wurde, gibt es keine vergleichbaren rechtlichen Überprüfungen oder Sicherheitsmaßnahmen in den AnomChat-

⁴⁵ Heine/Weißer, in: Schönke/Schröder, StGB, 30. Aufl. (2019), § 26 Rn. 21.

⁴⁶ EGMR, NStZ 1999, 47 (48).

⁴⁷ BGH, NJW 2016, 91 (95 ff.).

⁴⁸ EGMR, NJW 2015, 3631.

⁴⁹ BGH, NStZ 1984, 520 (520).

⁵⁰ OLG München, BeckRS 2023, 30017 Rn. 61 und 65; hierauf stellt auch LG Darmstadt, Beschl. v. 3.6.2024 – 15 KLS 950 Js 46577/20 ab. Das Gericht betont, dass es der Staatsanwaltschaft nicht gelang, den Beschluss des europäischen Gerichts vorzulegen, mit dem die Überwachungsmaßnahmen bzgl. Anom genehmigt worden seien.

⁵¹ LG Memmingen, BeckRS 2023, 26989 Rn. 89.

⁵² OLG München, BeckRS 2023, 30017 Rn. 63.

⁵³ LG Memmingen, BeckRS 2023, 26989 Rn. 83.

⁵⁴ OLG München, BeckRS 2023, 30017 Rn. 63.

⁵⁵ Ähnlich EuGH, Urt. v. 30.4.2024 – Rs. C-670/22, Rn. 86.

⁵⁶ LG Memmingen, BeckRS 2023, 26989 Rn. 84.

⁵⁷ OLG München, BeckRS 2023, 30017 Rn. 65.

Verfahren. In den AnomChat-Fällen wurde das angebliche Drittland nie bekanntgegeben. Die fehlende Offenlegung des „Drittlandes“ und der gerichtlichen Beschlüsse macht eine Überprüfung nach allgemeinen rechtsstaatlichen Grundsätzen und dem Grundsatz des „ordre public“ unmöglich.⁵⁸ Es kann in den AnomChat-Verfahren gerade nicht geklärt werden, dass die Daten aus einem europäischen Land stammen. Das *LG Darmstadt* führte im Rahmen einer Haftbeschwerde dazu aus:

„Mit dem Problem ‚gerichtlicher Beschlüsse vom Hörensagen‘ sah sich die Rechtsprechung – soweit ersichtlich – noch nicht konfrontiert. Die mit dieser neuen Rechtsfigur verbundenen Probleme liegen auf der Hand: Was nicht bekannt ist, lässt sich nicht prüfen. Eine belastbare Prüfung der vorliegend relevanten Frage, ob im Rahmen der Beweismittelerlangung rechtsstaatliche Mindeststandards eingehalten wurden, lässt sich ohne Betrachtung der ihr zugrundeliegenden richterlichen Entscheidungen nicht beantworten.“⁵⁹

5. Umgehung von StPO-Vorschriften zur Kommunikationsüberwachung

Die Umgehung der StPO hinsichtlich der Kommunikationsüberwachung, insbesondere in AnomChat-Verfahren, eröffnet ein rechtliches Dilemma, wie jüngst das *LG Memmingen* hervorgehoben hat.⁶⁰ Eine potenzielle Umgehung, bei der Deutschland als „Drittland“ ins Spiel kommt, wirft ein absurdes Problem auf: Deutsche Gerichte könnten daran gehindert sein, Ermittlungsbeschlüsse nach den nationalen Vorschriften der StPO zur Telekommunikationsüberwachung zu überprüfen, obwohl die Ermittlung innerhalb Deutschlands stattfand.⁶¹

Ein derartiges Szenario würde auf eine bewusste und vorsätzliche Umgehung der einschlägigen Vorschriften der StPO zur Kommunikationsüberwachung hinweisen, was wiederum zur Unverwertbarkeit der erhobenen Beweise führen müsste.⁶² Dies verdeutlicht die Notwendigkeit einer gründlichen Untersuchung und Überwachung von Fällen, in denen die StPO-Vorschriften zur Kommunikationsüberwachung möglicherweise umgangen werden, um sicherzustellen, dass rechtsstaatliche Grundsätze gewahrt bleiben und ein faires Verfahren gewährleistet ist.

6. Fazit zum Beweisverwertungsverbot

Die Diskussion um die Verwertbarkeit von im AnomChat erlangten Daten vor deutschen Gerichten stellt eine komplexe Problematik dar. Das Vorliegen eines Beweisverwertungsverbots ist umstritten, da deutsche Gerichte grundsätzlich nicht verpflichtet sind, die Rechtmäßigkeit ausländischer Ermittlungsmaßnahmen zu überprüfen. Dennoch neigen nunmehr einige Obergerichte in der AnomChat-Verfahrensreihe dazu, ein Beweisverwertungsverbot anzunehmen – dies insbesondere, da ein konkreter Tatverdacht zu Beginn der Ermittlungsmaßnahmen

fehlte, eine Überprüfung der angeblich erlangten Gerichtsbeschlüsse nicht möglich ist und die Verteidigungsrechte der Beschuldigten massiv beschnitten werden.⁶³ Zu beachten ist, dass es den Strafverfolgungsbehörden obliegt, zu beweisen, dass keine zu einem Beweisverwertungsverbot führende Situation vorlag. Dazu ist es kaum ausreichend, Ermittlungsmaßnahmen durchzuführen, wenn diese nicht förmlich genehmigt waren. Ein verständliches und vorhersehbares Verfahren braucht eine Genehmigung, damit eine ordnungsgemäße Überwachung gewährleistet werden kann.⁶⁴

IV. Forderung und Ausblick

Angesichts der erheblichen rechtlichen Unklarheiten im Zusammenhang mit AnomChats steht die deutsche Strafjustiz zweifellos vor der anspruchsvollen Aufgabe, ein eigenes Verständnis und eine eigenständige Position zu dieser Thematik zu entwickeln. Das Fehlen von Informationen über den europäischen Drittstaat und die behaupteten eingeholten Gerichtsbeschlüsse sprechen für ein klares Verbot der Beweisverwertung. Sollten deutsche Gerichte bestätigen, dass eine Tatprovokation gegen den Rechtsstaat vorliegt, würde dies sogar ein Verfahrenshindernis darstellen.

Aufgrund der offensichtlichen mangelnden Informationsgrundlage und der damit verbundenen unklaren Herkunft sowie möglichen unrechtmäßigen Erlangung der Daten sollten Ermittlungsverfahren, die ausschließlich auf Nachrichten aus dem AnomChat als einzigem Beweismittel basieren, gemäß § 170 Abs. 2 StPO eingestellt werden. Personen mit US-Staatsangehörigkeit wurden von Anfang an aus den AnomChat-Daten herausgefiltert, da diese in den USA nicht für Strafverfolgungszwecke genutzt werden dürfen. In der EU gelten ebenfalls rechtsstaatliche Standards, die vorliegend nicht eingehalten worden sind.

Die *Verfasser* ignorieren keineswegs, dass die Daten des AnomChat zur Aufklärung von kriminellen Handlungen beitragen können. Die zahlreichen Ermittlungserfolge dank der AnomChat-Daten quer über den europäischen Kontinent haben verdeutlicht, dass Strafverfolgungsbehörden effektivere rechtliche Instrumente benötigen, um gegen organisierte Kriminalität vorzugehen. Aus diesem Grund sollte die EU in Zusammenarbeit mit den Mitgliedstaaten den notwendigen Rechtsrahmen schaffen, um in Zukunft die Verwertbarkeit von Daten in Strafverfahren auf eine solide rechtsstaatliche Grundlage zu stellen. Die Regelung dieser Frage auf nationaler Ebene kann nicht erfolgreich sein, da Daten keine Staatsgrenzen kennen. Die aktuelle Rechtslage ist den dynamischen Anforderungen des digitalen Zeitalters nicht mehr gewachsen. Mit einem Rechtsrahmen wäre nicht nur den Ermittlungsbehörden geholfen, sondern auch den Gerichten und letztendlich der Rechtsstaatlichkeit.

⁵⁸ *LG Memmingen*, BeckRS 2023, 26989 Rn. 80, 81.

⁵⁹ *LG Darmstadt*, Beschl. v. 14.2.2022 – 18 KLS 1200 Js 83736/21.

⁶⁰ *LG Memmingen*, BeckRS 2023, 26989 Rn. 91.

⁶¹ *LG Memmingen*, BeckRS 2023, 26989 Rn. 90.

⁶² *LG Memmingen*, BeckRS 2023, 26989 Rn. 91.

⁶³ Siehe Fn. 39.

⁶⁴ *EGMR*, NJW 2015, 3631.