

WOLFGANG WOHLERS\*

## Beweise aus der Blackbox

### I. Die Kommunikation über «Kryptohandys» als Beweismittel im Strafprozess

Der Strafprozess dient der Abklärung eines Straftatverdachts,<sup>1</sup> wobei die Aufgabe, den Beweis zu führen, dass die Geschehensabläufe, die in der Anklageschrift behauptet werden, tatsächlich stattgefunden haben, der Staatsanwaltschaft bzw. dem erkennenden Gericht obliegt. Die Mittel, mit denen dieser Beweis geführt werden kann, werden unter anderem auch durch den Stand der gesellschaftlichen Entwicklung beeinflusst. Abgesehen von der stetigen Fortentwicklung praktisch aller forensisch relevanten Beweismethoden kommt es immer wieder einmal zu disruptiven Ereignissen, von denen das jüngste wohl die in den letzten Jahrzehnten des 20. Jahrhunderts zur praktischen Anwendungsreife als forensisches Instrument gelangte DNA-Analyse sein dürfte.<sup>2</sup> Auch wenn der Beweiswert einer am Tatort und/oder an bestimmten, deliktsrelevanten Gegenständen oder Personen festgestellten DNA-Spur deutlich

---

\* Der Verfasser ist als Student, als Referendar und nach dem zweiten Staatsexamen mehrere Jahre als Rechtsanwalt für die Kanzlei Strate und Ventzke tätig gewesen, bis der Wechsel in die Schweiz ein weiteres Tätigsein praktisch verunmöglicht hat. Die Einschränkung des Kontaktes zur Kanzlei, der für den Verfasser dieser Zeilen aus fachlich-beruflicher und persönlicher Sicht höchst wertvoll war und ist, stellt einen der (wenigen) mit dem Wechsel von der norddeutschen Tiefebene in die Berge verbundenen negativen Aspekte dar.

<sup>1</sup> Wohlers in SK-StPO, 5. Aufl. (2018), Einleitung Rn. 6 m.w.N.

<sup>2</sup> Wohlers in Geth (Hrsg.), Die revidierte Strafprozessordnung, Basel 2023, § 5 Rn. 5.1 und 5.7 ff.

weniger eindeutig ist, als dies verbreitet angenommen wird,<sup>3</sup> lässt sich doch nicht ernsthaft bestreiten, dass die DNA-Analyse schon in ihrer traditionellen Form der Erstellung von DNA-Profilen die Möglichkeiten der Beweisführung in verschiedener Hinsicht revolutioniert hat. Ob die in den letzten Jahren heiß diskutierte neue Variante der «Phänotypisierung»<sup>4</sup> vergleichbare Effekte hervorrufen wird, bleibt abzuwarten, muss im vorliegenden Zusammenhang aber auch schon deswegen nicht weiter vertieft werden, weil die Phänotypisierung keine Beweise kreiert, sondern ein Fahndungsinstrument darstellt, mittels dessen die Strafverfolgungsbehörden Ermittlungsansätze schaffen wollen, die zu Beweisen führen sollen.<sup>5</sup>

Für die Frage, wie bzw. mit welchen Mitteln im Strafverfahren Beweis geführt wird, ist neben der technischen Entwicklung von besonderer Bedeutung, wie in einer Gesellschaft kommuniziert und ob und wie (potenziell beweisrelevante) Informationen gesichert werden. In modernen Gesellschaften, die verbreitet – und in der Sache vollkommen zu Recht – als Informations- bzw. Datengesellschaften charakterisiert werden, schlägt sich die im Zuge der ubiquitären Nutzung digitaler Systeme und vernetzter Geräte exponentiell steigende Datenmenge letztlich auch im Strafverfahren nieder. Die Daten, die wir alle im Rahmen unserer geschäftlichen und privaten Tätigkeiten fortlaufend produzieren und die aufgezeichnet und gespeichert für eine Auswertung zur Verfügung stehen, stellen eine wahre Fundgrube für Strafverfolger dar und wecken damit natürlich Begehrlichkeiten. Dies gilt gerade für die Deliktsbereiche, bei denen die Strafverfolgungsbehörden, wie z.B. im Bereich des Betäubungsmittelhandels und der Organisierten Kriminalität im Allgemeinen, darauf angewiesen sind, die interne Kommunikation der Zielpersonen auszuwerten und beweissicher dokumentieren zu können, um auch in den Fällen zu

---

<sup>3</sup> Vgl. hierzu Wohlers ZStrR 141 (2023), 383, 393 ff.; ders. ZStrR 141 (2023), 347, 349 m.w.N.

<sup>4</sup> Wohlers a.a.O. (Fn. 2), § 5 Rn. 5.59 ff.

<sup>5</sup> Wohlers a.a.O. (Fn. 2), § 5 Rn. 5.59.

einer Verurteilung kommen zu können, in denen die Beteiligten von ihrem Schweigerecht Gebrauch machen und – wie im Regelfall – weder außenstehende Zeugen noch sonstige objektive Beweismittel zur Verfügung stehen.

Jedenfalls dann, wenn sich die Strafverfolgungsbehörde nicht von vornherein darauf beschränken will, allein die vor Ort agierenden Mitglieder auf der untersten Hierarchiestufe ins Visier zu nehmen, geht kein Weg daran vorbei, dass auf die interne Kommunikation zugegriffen werden muss. Die Beweisführung über Erkenntnisse, die im Rahmen heimlich durchgeführter Überwachungsmaßnahmen gewonnen werden, hat sich zu einer Art Wettlauf entwickelt, bei dem der technischen Entwicklung wiederum eine nicht zu überschätzende Bedeutung zukommt. Die vorerst letzte Etappe in diesem Rennen bestand darin, dass Personen, die sich einer Überwachung ihrer Kommunikation entziehen möchten, vor einigen Jahren dazu übergegangen sind, Kommunikationsgeräte zu nutzen, die von den Strafverfolgungsbehörden nicht überwacht werden können bzw. bei denen die Kommunikation verschlüsselt abläuft und deren Verschlüsselung – angeblich – nicht durchbrochen werden kann. Die Annahme, dass die sog. Kryptohandys eine von staatlicher Überwachung freie Kommunikation ermöglichen, hat sich allerdings, wie wir jetzt wissen, als Fehlannahme herausgestellt. Tatsächlich ist es ausländischen Stellen gelungen, die Verschlüsselung zu knacken (Fälle «Encrochat» und «Sky ECC»). In anderen Fällen hat sich herausgestellt, dass die angeblichen abhörsicheren Kryptohandys tatsächlich von Unternehmen stammen, die von (ausländischen) staatlichen Stellen gegründet worden sind und bei denen die Kommunikation damit von vornherein mitgehört werden konnte und sollte (Fall «Anom»).

Für die Strafverfolgungsbehörden ist die abgefangene Kommunikation von großer Bedeutung, zum einen, weil auf diese Weise möglicherweise auch die Personen erreicht werden können, die auf höheren Hierarchiestufen stehen, zum anderen aber auch – und vor allem – deshalb, weil die Kommunikation über die angeblich abhörsicheren Kommunikationskanäle relativ offen geführt worden ist und damit potenziell einen höheren Beweiswert verspricht.

Letzteres ist insbesondere dann von nicht zu unterschätzender Bedeutung, wenn es sich bei der abgehörten Kommunikation – wie nicht selten – um das einzige Beweismittel handelt, dass die Strafverfolgungsbehörden in den Händen halten. Von einzelnen der mit diesen Verfahren befassten Verteidigern wird denn auch gar nicht in Abrede gestellt, dass sich die in den entsprechenden Auswertungen enthaltenen Chats «faszinierend schlüssig» lesen. Es wird aber vollkommen zu Recht auch darauf hingewiesen, *«dass die [mit den Auswertungen] präsentierten Storys gerade im Hinblick auf Schlüssigkeit und ‘Lesbarkeit’ von Kriminalbeamten zusammengestellt wurden»*.<sup>6</sup>

Aus alledem folgt, dass eine lege artis agierende Verteidigung zunächst einmal ihrem Mandanten zu raten hat, von seinem Schweigerecht Gebrauch zu machen. Daneben muss sich die Verteidigung dann aber darauf konzentrieren, die Verwertung der Erkenntnisse aus den Überwachungsmaßnahmen in Frage zu stellen. Die Besonderheit, mit der man sich hierbei in Deutschland und in vielen anderen Staaten, wie z.B. auch in der Schweiz, konfrontiert sieht, ist die, dass die Überwachungsmaßnahmen nicht von deutschen Stellen durchgeführt wurden. Die ausländischen Stellen haben die von ihnen gewonnenen Erkenntnisse den deutschen Strafverfolgungsbehörden teilweise unaufgefordert zur Verfügung gestellt, teilweise hat sich die Anfrage bei den entsprechenden ausländischen Stellen aber auch schon zu einer Art Standardmaßnahme entwickelt, auf die jedenfalls dann zurückgegriffen wird, wenn im Zuge von Ermittlungen Hinweise darauf auftauchen, dass von den Beschuldigten entsprechende Kommunikationsmittel eingesetzt wurden. Die Frage ist, ob die Art und Weise, in der die Überwachungsmaßnahmen durchgeführt worden sind, ein Verwertungsverbot zu begründen vermag. Handelt es sich bei den Überwachungsmaßnahmen um anlasslos durchgeführte Ausforschungsmaßnahmen, deren Verwertung in einem deutschen Strafverfahren nicht in Betracht kommen kann, weil die entsprechenden Erkenntnisse nach deutschem Recht

---

<sup>6</sup> Sommer StraFo 2023, 250, 258.

nicht rechtmäßig hätten gewonnen werden können und/oder deren Verwertung gegen den ordre public verstößt?

Angesichts dessen, dass die Erwartungen, dass die deutschen Strafgerichte ein so begründetes Verwertungsverbot annehmen werden, von vornherein – und wie die bisherigen Entscheidungen belegen: zu Recht – nicht sehr hoch waren, kommt einem zweiten Gesichtspunkt besondere Bedeutung zu: Den Strafverfolgungsbehörden und Strafgerichten werden üblicherweise aufgearbeitete Auswertungen zur Verfügung gestellt, die sich, wie bereits erwähnt, für sich gesehen durchaus überzeugend lesen. Die Problematik besteht hierbei darin, dass man die Beweiskraft dieser Auswertungen nur dann beurteilen kann, wenn man auf die im Zuge der Überwachungsmaßnahmen angefallenen Rohdaten zurückgreifen und überprüfen kann, auf welche Art und Weise diese Rohdaten aufgearbeitet worden sind. Ist dies nicht möglich, haben weder die Verteidigung noch das mit der Sache befasste Gericht irgendwelche Ansatzpunkte, um die Auswertungen zu hinterfragen bzw. deren Beweiswert zu prüfen. Man kann den Auswertungen nur glauben – oder eben nicht.

Dass die Auswertungen – vorsichtig ausgedrückt – durchaus nicht über jeden Zweifel erhaben sind, hat die Praxis bereits gezeigt. So hat sich z.B. im Hinblick auf die Fälle, in denen der Tatvorwurf auf «Encrochat»-Daten gestützt wird, ergeben, dass es gemäß bekannt gewordenen Informationen

*«[d]utzende Nachrichten eines Nutzers innerhalb einer Sekunde [gibt], zum Teil antworten Nutzer auf Fragen eines anderen Nutzers, die gar nicht an sie gerichtet waren, zum Teil gibt es für die gleiche Nachricht drei Zeitstempel, die sich teilweise um mehrere Tage unterscheiden etc.».*<sup>7</sup>

---

<sup>7</sup> Erhard/Lödden StraFo 2021, 366, 368 Fn. 7; vgl. auch Kipker/Bruns MMR 2022, 363, 366.

Die Frage, die an diesen Befund anknüpft, ist die, welche Voraussetzungen eigentlich gegeben sein müssen, damit die Auswertungen Beweiskraft erlangen, und was die Folge ist, wenn diese Voraussetzungen nicht gewährleistet sind. Konkret geht es darum, ob die Problematik im Rahmen der Beweiswürdigung gelöst werden kann bzw. muss oder aber ein Verwertungsverbot anzunehmen ist. Letzteres erscheint zumindest aus der Sicht der Verteidigung betrachtet aus zwei Gründen vorzugswürdig: Zum einen würde bei Annahme eines Verwertungsverbots der entscheidende und häufig auch einzige belastende Beweis wegfallen, was zur Entlassung des Mandanten aus der Untersuchungshaft und zur Einstellung des Verfahrens führen muss. Zum anderen werden mit dem Verdikt der Unverwertbarkeit die Unwägbarkeiten umgangen, die der «freien» Beweiswürdigung aus der Sicht der die Würdigung nicht selbst vornehmenden Verfahrensbeteiligten notwendigerweise anhaften.

Die Tatsache, dass der Beweiswert von digitalen Beweisen, an deren ordnungsgemäßes Zustandekommen man nur glauben, den man aber nicht verifizieren kann, praktisch gesehen gegen Null tendiert,<sup>8</sup> muss jedenfalls im Rahmen der Beweiswürdigung berücksichtigt werden. Nach der in der deutschen Strafjustiz ganz vorherrschend vertretenen Auffassung bleibt es dann aber auch dabei. So hat sich das OLG Brandenburg in einem «Encrochat»-Daten betreffenden Verfahren explizit auf den Standpunkt gestellt, die Frage der Datenauthentizität und Datenintegrität sei

*«einer einzelfallbezogenen tatgerichtlichen Bewertung zugänglich und obliegt insoweit der Aufklärung und abschließenden Prüfung des Landgerichts im Rahmen der zu treffenden Beweiswürdigung. Diesbezügliche Einschränkungen hinsichtlich*

---

<sup>8</sup> So auch bereits Gall/Haskaya *forum*poenale 2023, 301, 306 f.; Albrecht *jurisPR-StrafR* 20/2021 Anm. 3 (Abschnitt D.); Kipker/Bruns *MMR* 2022, 363, 364 f. und 367.

*des Beweiswertes der Daten führen insoweit nicht dazu, dass ein generelles Verwertungsverbot anzunehmen wäre.»<sup>9</sup>*

Entgegen der von der Verteidigung vertretenen Auffassung sei

*«eine Verwertung der Chat-Dateien auch nicht im Hinblick darauf ausgeschlossen, dass die zugrunde liegenden ‚Rohdaten‘ (bislang) nicht vorliegen, das konkrete (nachrichtendienstliche) Vorgehen bei der Datengewinnung seitens der französischen Ermittlungsbehörden nicht bekannt ist und die Kommunikationsinhalte von den Endgeräten möglicherweise bereits vor einer Versendung entschlüsselt und gesichert wurden».<sup>10</sup>*

Im Ausland wird dies durchaus anders gesehen: Der EGMR geht in ständiger Rechtsprechung davon aus, dass der Beschuldigte als Teil des Anspruchs auf ein faires Verfahren i.S. von Art. 6 Abs. 1 EMRK die Möglichkeit haben muss, die Belastungsbeweise zu hinterfragen, wozu auch gehört, dass er deren ordnungsgemäßes Zustandekommen prüfen und sodann substantiiert bestreiten können muss.<sup>11</sup> Und aus eben diesem Grund hat der Corte di Cassazione in einem Entscheid vom 15.07.2022 die Verwendung der durch Zugriff auf die

---

<sup>9</sup> OLG Brandenburg, Beschluss vom 3.8.2021 – 2 Ws 102/21 = BeckRS 2021, 23525 Rz. 17.

<sup>10</sup> OLG Brandenburg, Beschluss vom 3.8.2021 – 2 Ws 102/21 = BeckRS 2021, 23525 Rz. 16.

<sup>11</sup> EGMR v. 26.09.2023, Yüksel Yalcinkaya vs. Türkei, §§ 303, 306 und 324 ff. (bezogen auf digitale Beweise); EGMR v. 25.07.2013, Erkapić v. Kroatien, §§ 73; EGMR v. 25.07.2013, Zahirović v. Kroatien, § 42; EGMR v. 05.06.2009, Mirilashvili v. Russland, § 91; Meyer in Karpenstein/Mayer (Hrsg.), EMRK, 3. Aufl. (2021), Art. 6 Rn. 127; Harrendorf/König/Voigt in Meyer-Ladewig/Nettesheim/von Raumer (Hrsg.), Handkommentar EMRK, 5. Aufl. (2023), Art. 6 Rn. 117.

unter «Sky ECC» gelaufene Kommunikation abgelehnt.<sup>12</sup> Der EuGH hat im Zusammenhang mit der sog. Vorratsdatenspeicherung festgehalten, dass Daten von der Verwendung auszuschließen sind, wenn die Verfahrensbeteiligten

*«nicht in der Lage sind, sachgerecht zu den Informationen und Beweisen Stellung zu nehmen, die einem Bereich entstammen, in dem das Gericht nicht über Sachkenntnis verfügt, und geeignet sind, die Würdigung der Tatsachen maßgeblich zu beeinflussen».*<sup>13</sup>

Und auch das Schweizerische Bundesgericht hat ebenfalls schon vor einigen Jahren festgehalten, dass das Recht, sich effektiv verteidigen zu können, nicht nur voraussetzt, dass die Beweismittel in den Akten vorhanden sind, sondern

*«dass aktenmäßig belegt sein muss, wie sie produziert wurden, damit der Angeklagte in der Lage ist zu prüfen, ob sie inhaltliche oder formelle Mängel aufweisen und gegebenenfalls Einwände gegen deren Verwertbarkeit erheben kann. Dies ist Voraussetzung dafür, dass er seine Verteidigungsrechte überhaupt wahrnehmen kann».*<sup>14</sup>

---

<sup>12</sup> Corte Suprema di Cassazione, Entscheid vom 15.07.2022, 32915, E. 1; vgl. auch Lödden/Makepeace HRRS 2023, 384, 390; Sommer StraFo 2023, 259.

<sup>13</sup> EuGH, Große Kammer, Urteil v. 20.09.2022, C-339/20, Rn. 106; zur Übertragbarkeit dieser Rechtsprechung auf die hier vorliegenden Konstellationen vgl. Meyer-Mews HRRS 2023, 110, 114 f.

<sup>14</sup> BGE 129 I 85, 88 f.; vgl. auch Gless in Niggli/Wiprächtiger/Heer (Hrsg.), Basler Kommentar Strafprozessordnung, 3. Aufl. (2023), Art. 141 N 33: Soweit ein die Zuverlässigkeit der strafprozessualen Beweisführung oder die Fairness des Verfahrens in Frage stellender Umstand nicht kompensiert werden kann, «kann das Beweismittel aus dem Ausland nicht verwertet werden».

Mit den nachfolgenden Ausführungen sollen beide vorstehend erwähnten Ansatzpunkte für ein Verwertungsverbot näher analysiert werden: Zum einen die Umstände, unter denen die Erkenntnisse aus der Kommunikation über Kryptohandys gewonnen worden sind (dazu unten III.), zum anderen die Frage, ob ein in seiner Beweiskraft nicht hinterfragbares Beweismittel überhaupt Eingang in die Beweiswürdigung finden darf und deshalb von vornherein aus dieser herausgehalten werden muss (dazu unten IV.). Zuvor soll aber noch kurz auf die Frage eingegangen werden, wie die Erkenntnisse über den Kommunikationsinhalt in den Fällen «Encrochat», «Sky ECC» und «Anom» konkret gewonnen worden sind und wie deutsche und ausländische Gerichte bisher deren Verwertbarkeit beurteilt haben (vgl. nachfolgend II.).

## II. Die Erkenntnisse aus der Überwachung der Kommunikation in den Fällen «Encrochat», «Sky ECC» und «Anom» vor den deutschen Strafgerichten

### 1. Die Fälle «Encrochat», «Sky ECC» und «Anom»

Das Unternehmen «Encrochat» hatte im Jahre 2016 Mobiltelefone auf den Markt gebracht, die – so die Eigenwerbung – von den Strafbehörden nicht abgehört werden konnten. Tatsächlich ist es den französischen Behörden unter Mitwirkung niederländischer Behörden, Eurojust und Europol gelungen, auf den Server der «Encrochat»-Betreiber zuzugreifen und mittels einer als Softwareupdate getarnten Spionagesoftware letztlich auch auf die Endgeräte zuzugreifen. Dieser Zugriff dauerte an bis zur Abschaltung des Servers durch den Anbieter im Jahre 2020, die offenbar erfolgte, nachdem Anhaltspunkte für die Infiltrierung des Systems bekannt geworden waren. Die ausgelesenen Informationen – Kommunikationsinhalte und Memos – wurden von Europol ausgewertet, aufbereitet und mit dem Einverständnis der französischen Behörden an die zuständigen Stellen verschiedener Staaten weitergeleitet. In Deutschland wurden die Daten vom Bundeskriminalamt ausgewertet,

nochmals aufgearbeitet und in der Folge eine Vielzahl von Strafverfahren eingeleitet. Auf ein – unzutreffenderweise als eine europäische Ermittlungsanordnung eingekleidetes<sup>15</sup> – Ersuchen der Generalstaatsanwaltschaft Frankfurt am Main hin hat das zuständige französische Gericht die Zustimmung zur Verwertung der übermittelten Daten erteilt.<sup>16</sup>

Auch «Sky ECC» ist ein Kommunikationsdienst, der von einem kanadischen Unternehmen betrieben wurde, das seinen Nutzern eine abhörsichere Kommunikation versprach. Die Kommunikation konnte nur über fertig vorinstallierte Geräte erfolgen, die direkt vom Anbieter bezogen werden mussten. Zu unterscheiden sind bilaterale Chats, bei denen die Chatinhalte nur einseitig gespeichert wurden, und Gruppen-Chats, bei denen die Kommunikation umfassend gespeichert wurde. Auch hier ist es einer Gruppe französischer, niederländischer und belgischer Behörden, unterstützt durch Europol, gelungen, den Datenverkehr zu entschlüsseln, aufzubereiten und dann den nationalen Strafverfolgungsbehörden zur Verfügung zu stellen.<sup>17</sup>

Der Fall «Anom» war bzw. ist etwas anders gelagert als die beiden vorerwähnten Fälle: Hier hatte das FBI ein in Panama domiziliertes und auf abhörsicher verschlüsselte Kommunikation spezialisiertes Unternehmen gegründet. Dieses Unternehmen hat in der Folge rund 12'000 angeblich abhörsichere Geräte an Endkunden veräußert, wobei die Kommunikation tatsächlich überwacht werden konnte und auch tatsächlich im Auftrag des FBI überwacht wurde. Die

---

<sup>15</sup> Vgl. hierzu *Strate* HRRS 2022, 15, 16 f.; vgl. auch *Swoboda* in FS Ignor (2023), S. 812 und 833 ff.

<sup>16</sup> Vgl. die ausführliche Darstellung des Sachverhalts bei BGH, Beschluss vom 02.03.2022 – 5 StR 457/21 = NStZ 2022, 435; vgl. auch *Erhard/Lödden* StraFo 2021, 366 f.; *Gebhard/Michalke* NJW 2022, 655 f.; *Kipker/Bruns* MMR 2022, 363 f.; *Ruppert* NZWiSt 2022, 221 f.; *Schmidt* ZStW 134 (2022), 982 f.; *Sommer* StV-S 2021, 67 f.; *Swoboda* in FS Ignor (2023), S. 811 und 814 ff.; *Theume* KJ 2021, 444 f.; *Wahl* ZIS 2021, 452; *Zeyher* ZWH 4/2022, 81, 82; *Zimmermann* ZfStW 2022, 173 ff.

<sup>17</sup> Vgl. die Darstellung der Hintergründe bei *Gall/Haskaya* forumpoenale 2023, 301, 302 f.; *Lödden/Makepeace* HRRS 2023, 384, 385 ff.

Überwachung erfolgte so, dass die Daten außerhalb der USA abgefangen und auf einen außerhalb der USA gelegenen Server weitergeleitet und entschlüsselt wurden. Nach einer ersten Testphase schaltete das FBI einen unbekannten Drittstaat ein, bei dem es sich um ein Mitglied der EU handeln soll. Dieser Drittstaat richtete einen Server ein, auf den die Daten weitergeleitet wurden. Der Drittstaat erwirkte einen richterlichen Beschluss, der es ihm gestattete, die Daten im Wege der Rechtshilfe in Kopie an das FBI weiterzuleiten. Die Auswertung der Daten soll durch das FBI in Zusammenarbeit mit Behörden des Drittstaates und Europol erfolgt sein. Die aufbereiteten Daten wurden über das FBI den Strafverfolgungsbehörden anderer Staaten zur Verfügung gestellt, unter anderem den Strafverfolgungsbehörden in Deutschland und in der Schweiz.<sup>18</sup>

## 2. Die Reaktion der deutschen Strafjustiz

Wie nicht anders zu erwarten, hat die Verteidigung in allen drei Fällen den Versuch unternommen, die Erkenntnisse aus der Überwachung für unverwertbar zu erklären. In einem «Encrochat»-Daten betreffenden Verfahren hat das LG Berlin ein Verwertungsverbot unter Verweis auf die Missachtung von Art. 31 RiLi EEA und § 91g Abs. 6 IRG sowie das Fehlen eines Anfangsverdachts angenommen,<sup>19</sup> die Entscheidung ist aber umgehend durch das

---

<sup>18</sup> Vgl. dazu OLG Frankfurt, Beschluss vom 22.11.2021 – 1 HEs 427/21 = NJW 2022, 710; OLG Saarbrücken, Beschluss vom 30.12.2022 – 4 HEs 35/22 = NStZ 2023, 764; OLG München, Beschluss vom 19.10.2023 – 1 Ws 525/23 = StV 2024, 18; LG Darmstadt StV 2022, 280 mit Anm. Nestler; vgl. auch BGer vom 11.01.2024, 7B\_159/2022 und 7B\_160/2022 mit Bespr. Wohlers *forum*poenale 2024, 293 ff.

<sup>19</sup> LG Berlin, Beschluss vom 01.07.2021 – (525 Kls) 254 Js 592/20 (10/21) = NStZ 2021, 696, 700 f. mit abl. Anm. Labusga und zust. Besprechung Erhard/Lödden *StraFo* 2021, 366, 368 ff. sowie Theune *KJ* 2021, 444 ff.

Kammergericht aufgehoben worden,<sup>20</sup> wobei das Kammergericht sich zu dem markigen Statement bemüßigt sah:

*«Die Nichtverwertung von legal durch Behörden der Republik Frankreich – nicht nur eines Gründungsmitglieds der europäischen Union, sondern auch eines der Mutterländer des modernen Menschenrechtsverständnisses – beschaffter Informationen über derart schwerwiegende Straftaten, verstieße auch in erheblicher Weise gegen das allgemeine Gerechtigkeitsempfinden der rechtstreuen Bevölkerung.»<sup>21</sup>*

Mit der Ablehnung eines Verwertungsverbots steht das Kammergericht aber keineswegs allein, sondern reiht sich in die Phalanx der Oberlandesgerichte ein, die – im Hinblick auf «Encrochat»-Daten und «Sky ECC»-Daten unisono – die Verwertbarkeit der erlangten Erkenntnisse aus der im Ausland erfolgten Überwachung ebenfalls bejaht haben, wobei sie sich verschiedener, vom Bundesgerichtshof entwickelter bzw. vorgegebener Instrumente bedient haben, die es praktisch weitgehend ausschließen, dass es in Bezug auf sog. Auslandsbeweise zur Annahme eines Verwertungsverbotes kommen kann:

So gehen einzelne Oberlandesgerichte zwar durchaus davon aus, dass es zu Verstößen gegen das in § 31 EEA und § 91g IRG statuierte Mitteilungsgebot gekommen ist. Dennoch seien die Erkenntnisse aufgrund einer Abwägung verwertbar, da auch im Falle des Vorliegens des Verstoßes das Interesse an einer Strafverfolgung überwiege.<sup>22</sup> Teilweise wird auch darauf verwiesen, dass

---

<sup>20</sup> KG Berlin, Beschluss vom 30.08.2021 – 2 Ws 79/21 = BeckRS 2021, 24213 = NStZ-RR 2021, 353 mit Anm. Diessner Fachdienst Strafrecht 2021, 442178 und krit. Bespr. Theune KJ 2021, 444, 448 f.

<sup>21</sup> KG Berlin BeckRS 2021, 24213 Rz. 49 = NStZ-RR 2021, 353, 354.

<sup>22</sup> KG Berlin, Beschluss vom 30.08.2021 – 2 Ws 79/21 = BeckRS 2021, 24213 = NStZ-RR 2021, 353 und Anm. Diessner Fachdienst Strafrecht 2021, 442178; OLG Brandenburg, Beschluss vom 03.08.2021 – 2 Ws 102/21 = BeckRS 2021, 23525; OLG Brandenburg, Beschluss vom 16.12.2021 – 2 Ws 197/21 (S) = BeckRS 2021,

Beweisverwertungsverbote nur im Ausnahmefall eingreifen und eine fehlerhafte Beweisgewinnung bei Auslandsbeweisen im Hinblick auf das Prinzip der gegenseitigen Anerkennung nur angenommen werden könne, wenn es um eklatante Fehler geht,<sup>23</sup> konkret um die Verletzung völkerrechtlich verbindlicher und dem Individualschutz dienender Garantien oder um einen Verstoß gegen den Grundsatz des *ordre public* (vgl. § 73 IRG).<sup>24</sup> Beweiserhebungen, die im Ausland erfolgt sind, werden unter Verweis auf den Grundsatz der gegenseitigen Anerkennung praktisch weitgehend einer Überprüfung entzogen, was vom Bundesgerichtshof im Ergebnis bestätigt wurde.<sup>25</sup> Die weitere These einiger Oberlandesgerichte, dass im deutschen Recht mit § 100e Abs. 6 Nr. 1 StPO eine Rechtsgrundlage zur Verfügung stehen soll, mit der die im Ausland

---

42283 mit Anm. *Knierim* Fachdienst Strafrecht 2022, 445089; OLG Bremen, Beschluss vom 18.12.2020 – 1 Ws 166/20 = NStZ-RR 2021, 158, 159 f. mit Bespr. *Vizcaino* jurisPR-StrafR 10/2021 Anm. 1 und Bespr. *Stehr/Rakow* StRR 4/2021, 6 ff., *Wahl* ZIS 2021, 452 ff.; OLG Celle, Beschluss vom 12.08.2021 – 2 Ws 250/21 = BeckRS 2021, 24319 Rz. 34 ff., 50 ff. mit Bespr. *Albrecht* jurisPR-StrafR 20/2021 Anm. 3; OLG Hamburg, Beschluss vom 29.01.2021 – 1 Ws 2/21 = BeckRS 2021, 2226 Rz. 98 ff. mit Bespr. *Stehr/Rakow* StRR 4/2021, 6 ff. sowie Bespr. *Nadeborn/Kempgens* jurisPR-StrafR 12/2021 Anm. 4 und *Wahl* ZIS 2021, 452 ff.; OLG Rostock, Beschluss vom 23.02.2021 – 20 Ws 70/21 = MMR 2021, 572; OLG Schleswig, Beschluss vom 29.04.2021 – 2 Ws 47/21 = NStZ 2021, 693, 695; vgl. auch *Labusga* NStZ 2021, 702 ff.; *Zeyher* ZWH 4/2022, 81, 83 f.; *Zimmermann* ZfStW 2022, 173, 177 f.; bestätigt durch BGH NStZ 2022, 435, 440 ff. mit krit. Anm. *Rückert*; kritisch *Gebhard/Michalke* NJW 2022, 655, 657 f.; *Schmidt* ZStW 134 (2022), 982, 999 ff. und 1012 f.; zweifelnd *Wahl* ZIS 2021, 452, 457 f.; kritisch *Swoboda* in FS Ignor (2023), S. 828 ff.

<sup>23</sup> OLG Brandenburg BeckRS 2021, 23525 Rz. 7 ff.; OLG Brandenburg BeckRS 2021, 42283 Rz. 9 ff.; OLG Hamburg BeckRS 2021, 2226, Rz. 74 ff.

<sup>24</sup> OLG Bremen NStZ-RR 2021, 158, 160; OLG Frankfurt NJW 2022, 710, 711 Rn. 6; OLG Saarbrücken NStZ 2023, 764, 765; KG Berlin NStZ-RR 2021, 353.

<sup>25</sup> BGH, Beschluss vom 02.03.2022 – 5 StR 457/21 = NStZ 2022, 435, 437 ff. mit Anm. *Sommerer/Rehberger* RDJ 2022, 304 ff. und Bespr. *Ruppert* NZWiSt 2022, 221 ff.

gewonnenen Erkenntnisse als Zufallsfunde i.S. von § 100e verwertet werden können,<sup>26</sup> wird vom BGH zwar nicht geteilt, er sieht eine Rechtsgrundlage für die Verwertung aber in § 261 StPO.<sup>27</sup>

In Bezug auf «Anom»-Daten haben die OLGe Frankfurt und Saarbrücken das Vorliegen eines Verwertungsverbots mit den bereits bekannten Argumenten verneint,<sup>28</sup> während das OLG München die Verwertbarkeit der «Anom»-Daten für zweifelhaft erklärt hat, wobei es den relevanten Unterschied zu der vom BGH gebilligten Verwertung der «Encrochat»-Daten darin sieht, dass die «Anom»-Daten aus einer vom FBI initiierten und geleiteten Überwachungsmaßnahme stammen, wobei das in die Umsetzung einbezogene «Drittland weder vom FBI noch vom US-amerikanischen Justizministerium benannt wird, und zugleich von den befragten US-amerikanischen Stellen nur behauptet wird, dass in einem Drittland gerichtliche Entscheidungen ergangen seien».<sup>29</sup>

---

<sup>26</sup> So – bezogen auf Encrochat – OLG Celle BeckRS 2021, 24319 Rz. 22 ff.; OLG Hamburg BeckRS 2021, 2226 Rz. 58 ff.; OLG Schleswig NStZ 2021, 693, 695 f.; KG Berlin NStZ-RR 2021, 353 f. mit Anm. *Immel*; kritisch hierzu *Strate* HRRS 2022, 15, 16; *Swoboda* in FS Ignor (2023), S. 831 f.; vgl. auch *Gebhard/Michalke* NJW 2022, 655, 658 f.; *Lödden/Makepeace* HRRS 2023, 384, 389; *Ruppert* NZWiSt 2022, 221, 225 ff.; *Schmidt* ZStW 134 (2022), 982, 994 ff.; *Zeyher* ZWH 4/2022, 81, 85 ff.; vgl. aber auch – bezogen auf Anom – OLG Frankfurt NJW 2022, 710, 711 Rz. 5.

<sup>27</sup> BGH NStZ 2022, 435, 443 Rn. 61 mit abl. Anm. *Rückert* und abl. Bespr. *Ruppert* NZWiSt 2022, 221, 224 f.; kritisch auch *Schmidt* ZStW 134 (2022), 982, 1006; *Swoboda* in FS Ignor (2023), S. 813 f. sowie *Wohlers* in SK-StPO, Einleitung Rn. 273.

<sup>28</sup> OLG Frankfurt NJW 2022, 710; OLG Saarbrücken NStZ 2023, 764 f.

<sup>29</sup> OLG München StV 2024, 18, 20.

### III. Die Verwertung von Erkenntnissen aus ausländischen Überwachungsmaßnahmen in einem deutschen Strafverfahren

Aus der Sicht der Verteidigung betrachtet, fällt zunächst einmal ins Auge, dass die hier in Frage stehenden Erkenntnisse in Deutschland nicht hätten gewonnen werden können. Für die Anwendung von Überwachungsmaßnahmen nach der StPO fehlt es an einem auf eine konkrete Tat bezogenen Anfangsverdacht, was letztlich auch von den Gerichten anerkannt wird.<sup>30</sup> Ob die Überwachungsmaßnahmen stattdessen auf polizeirechtlicher Grundlage hätten ergriffen werden können, kann offenbleiben, weil die Maßnahme praktisch gesehen jedenfalls daran gescheitert wäre, dass die deutschen Polizeibehörden offensichtlich nicht über die Fähigkeiten verfügen, die Verschlüsselung der Kommunikationssysteme selbst durchbrechen zu können. Letztlich kommt es auf dies alles aber gar nicht an, denn die Erkenntnisse sind nun einmal im Ausland gewonnen worden und es muss deshalb danach gefragt werden, ob diese Erkenntnisse in einem in Deutschland durchgeführten Strafverfahren verwertet werden dürfen oder nicht.

Bezogen auf die Frage, unter welchen Voraussetzungen im Ausland gewonnene Erkenntnisse in einem deutschen Strafverfahren verwertet werden dürfen, besteht in der Literatur weitgehende Einigkeit dahingehend, die Verwertung in einem deutschen Strafverfahren sei ein Akt der deutschen Hoheitsgewalt, der sich nach deutschem Recht zu beurteilen habe.<sup>31</sup> Damit muss das

---

<sup>30</sup> OLG Brandenburg, Beschluss vom 03.08.2021 – 2 Ws 102/21 = BeckRS 2021, 23525 Rz. 10; OLG Brandenburg, Beschluss vom 16.12.2021 – 2 Ws 197/21 (S) = BeckRS 2021, 42283 Rz. 11.

<sup>31</sup> *Ambos* Beweisverwertungsverbote (2010), S. 81; *Böse* ZStW 114 (2002), 148 (149); *Derin/Singelstein* NStZ 2021, 449, 453; *Gless* JR 2008, 317, 321; *Schmidt* ZStW 134 (2022), 982, 984; *Zeyher* ZHW 4/2022, 81, 84; *Zimmermann* ZfStW 2022, 173, 184; vgl. auch *Wohlers* in SK-StPO, Einleitung Rn. 317; *Gleß* JR 2008, 317, 321, jeweils m.w.N.

Vorliegen eines Verwertungsverbots auf der Grundlage der in Deutschland geltenden Grundsätze für die Annahme von Verwertungsverböten entschieden werden, was in der Praxis bedeutet, dass der vom Bundesgerichtshof entwickelte Abwägungsansatz<sup>32</sup> zur Anwendung kommen würde. Dass die Bäume hier nicht in den Himmel wachsen, wird schon dadurch sichergestellt, dass die Annahme eines Verwertungsverbots nach ständiger Rechtsprechung nicht etwa die Default-Lösung darstellt, sondern die einer besonderen Begründung bedürftige Ausnahme.<sup>33</sup>

Soweit es um Auslandsbeweise geht, wird diese Barriere noch durch andere Gesichtspunkte verstärkt. Ursprünglich war die Rechtsprechung im Hinblick auf Auslandsbeweise von einer differenzierenden Lösung ausgegangen: Vorrangig sollte auf das Recht des Staates abzustellen sein, in dem der Beweis erhoben wurde. War die Erhebung gemessen an diesem Recht ordnungsgemäß erfolgt, war der Beweis auch in einem deutschen Strafverfahren verwertbar; war die Erhebung gemessen am ausländischen Recht prozessordnungswidrig erfolgt, sollte eine Abwägung erforderlich sein, die aber nur dann zu einem Verwertungsverbot führen sollte, wenn eklatante Mängel vorlagen und unverzichtbare rechtsstaatliche Grundsätze nicht eingehalten worden waren.<sup>34</sup> In seiner neueren Rechtsprechung geht nun auch der BGH davon aus, dass es für die Frage der Verwertbarkeit auf das Recht des ersuchenden Staates ankommen soll.<sup>35</sup> Gleichzeitig geht der BGH aber auch davon aus, dass es eine Überprüfung von im Ausland erfolgten Akten der Beweisgewinnung durch die

---

<sup>32</sup> Vgl. dazu Wohlers in SK-StPO, 5. Aufl. (2018), Einleitung Rn. 280 ff.

<sup>33</sup> Vgl. BVerfGE 130, 1, 28; BGHSt 37, 30, 32; BGHSt 40, 211, 217; BGHSt 42, 372, 377; BGHSt 44, 243, 249 f.; BGHSt 51, 285, 289 f.; kritisch hierzu Wohlers in SK-StPO, Einleitung Rn. 272 f.

<sup>34</sup> Vgl. BGH StV 1982, 153, 154; BGH NStZ 1983, 181; kritisch zur Unklarheit der Kriterien: Gless in FS Grünwald (1999), S. 204; Wohlers in SK-StPO, 5. Aufl. (2018), Einleitung Rn. 319; Gless JR 2008, 317, 320 f.

<sup>35</sup> BGHSt 38, 263, 265; BGHSt 58, 32, 36 Rn. 21; BGH NStZ 2022, 435, 438 Rn. 26; BGH NStZ 2014, 608; OLG Schleswig NStZ 2021, 693, 695.

deutschen Gerichte im Hinblick auf den Grundsatz der gegenseitigen Anerkennung nur eingeschränkt erfolgen kann, nämlich dahingehend, ob völkerrechtlich verbindliche Garantien und rechtsstaatliche Grundsätze eingehalten worden sind.<sup>36</sup>

Konkret bedeutet dies, dass Auslandsbeweise gegen Verwertungsverbote praktisch immun sind:

Zunächst einmal macht die eingeschränkte Überprüfung es schon sehr schwer – um nicht zu sagen: praktisch unmöglich –, einen im Rahmen der Beweisgewinnung erfolgten Verstoß auch nur festzustellen. In der Literatur wird verbreitet der von den Verteidigungen aufgegriffene Standpunkt vertreten, dass es sich bei den im Ausland erfolgten Überwachungsmaßnahmen um anlasslos erfolgte Massenüberwachungen handelt,<sup>37</sup> was in der schweizerischen Strafprozessrechtsdogmatik mit dem plastischen Begriff der «fishing expedition» umschrieben wird<sup>38</sup> und in der Schweiz nach ganz herrschender Meinung ein Verwertungsverbot zur Folge hat.<sup>39</sup> Dass es sich beim Zugriff auf die «Sky ECC»-Daten um eine «fishing expedition» handelt, ergibt sich allein schon daraus, dass es hier um die Abschöpfung des Kommunikationsverkehrs von 170'000 Endgeräten ging.<sup>40</sup> Die Annahme, dass insoweit ein individualisierter Anfangsverdacht bestanden haben soll, erscheint geradezu absurd; es handelt sich mithin um eine anlasslose Massenerhebung zum Zweck der gezielten

---

<sup>36</sup> BGHSt 58, 32, 42 Rn. 33 ff.; BGH NStZ 2022, 435, 438 ff.; vgl. auch *Pauli* NStZ 2021, 146, 148; kritisch hierzu *Sommer* StV-S 2021, 67, 69; *Zimmermann* ZfStW 2022, 173, 177; vgl. auch *Wahl* ZIS 2021, 452, 454 mit dem Hinweis darauf, dass konkrete Maßstäbe für die Ausfüllung dieses Kriterium nicht ersichtlich seien.

<sup>37</sup> Vgl. nur *Derin/Singelstein* NStZ 2021, 449, 452; *Strate* HRRS 2022, 15, 16; *Wahl* ZIS 2021, 452 f.; *Wohlers* forumpoenale 2024, 293, 297.

<sup>38</sup> Vgl. *Oberholzer* Grundzüge des Strafprozessrechts, 4. Aufl., Bern 2020, Rn. 1126; *Wohlers* in *Donatsch/Lieber/Summers/Wohlers* (Hrsg.), Kommentar zur Schweizerischen Strafprozessordnung, 3. Aufl., Zürich 2020, Art. 141 Rn. 32.

<sup>39</sup> Vgl. *Wohlers* forumpoenale 2024, 293, 297 f. m.w.N.

<sup>40</sup> *Lödden/Makepeace* HRRS 2023, 384, 389.

Generierung von Zufallsfunden.<sup>41</sup> Gleiches gilt für die «Anom»-Daten: Hier ging es zwar «nur» um 12'000 Kunden. Dass, wie das Obergericht Aargau als Vorinstanz in einem vom schweizerischen Bundesgericht entschiedenen Fall angenommen hatte, von einem individualisierten Tatverdacht keine Rede sein kann, ist auch vom Bundesgericht nicht beanstandet worden.<sup>42</sup> Anders soll es dagegen im Fall «Encrochat» liegen, weil der Zugriff hier in einem Verfahren erfolgt sei, das sich gegen die Betreiber des Servers gerichtet haben soll.<sup>43</sup> Dieser Begründungsansatz erscheint fragwürdig bzw. vorgeschoben, weil von Anfang an – jedenfalls: auch – die Nutzer im Visier der Strafverfolger waren – und zwar potenziell alle.<sup>44</sup> Der BGH ist den sich damit ergebenden Fragen nicht weiter nachgegangen, sondern akzeptiert die Behauptung der französischen Behörden, dass sich alle Nutzer verdächtig gemacht hätten.<sup>45</sup>

Selbst wenn sich ein prozessualer Fehler im Vorgehen der ausländischen Strafbehörden feststellen lässt, führt dies aber nur dazu, dass nun die zweite Hürde zu überspringen ist: Es darf sich nicht um irgendeinen Fehler handeln, sondern um einen solchen, durch den völkerrechtlich verbindliche Garantien und/oder rechtsstaatliche Grundsätze in Frage gestellt werden. Auch hier liegt die Latte in der Praxis hoch. Dass es sich um eine anlasslos erfolgte Massenüberwachung («fishing expedition») gehandelt haben könnte, begründet nach OLG Saarbrücken keinen elementaren Verstoß gegen rechtsstaatliche

---

<sup>41</sup> Lödden/Makepeace HRRS 2023, 384, 389 f.; Strate HRRS 2022, 15, 16.

<sup>42</sup> Vgl. BGer, Urteil vom 11.01.2024, 7B\_159/2022, 7B\_160/2022, E. 2 und E. 5.5 mit Bespr. Wohlers *forumpoenale* 2024, 293, 297 f.

<sup>43</sup> Vgl. KG Berlin, Beschluss vom 30.08.2021 – 2 Ws 79/21 = BeckRS 2021, 24213 Rz. 23 ff.; OLG Hamburg, Beschluss vom 29.01.2021 – 1 Ws 2/21 = BeckRS 2021, 2226 Rz. 5 ff.; Zimmermann *ZfStW* 2022, 173.

<sup>44</sup> Vgl. hierzu auch LG Berlin *NStZ* 2021, 696, 698 Rn. 28; Strate HRRS 2022, 15, 16; Derin/Singelstein *NStZ* 2021, 449, 451 f.; Sommer *StraFo* 2023, 250, 253; Swoboda in FS Ignor (2023), S. 822 ff.

<sup>45</sup> Vgl. BGH *NStZ* 2022, 435, 440 Rn. 37.

Grundsätze.<sup>46</sup> Dass es für die Überwachungsmaßnahmen an einer Rechtsgrundlage im deutschen Recht fehlt, reicht ebenfalls nicht aus. Das Fehlen der Rechtsgrundlage führe entgegen einer in der Literatur verbreitet vertretenen Auffassung<sup>47</sup> zu keinem Verstoß gegen den *ordre public*. Der Umstand, dass die entsprechenden Überwachungsmaßnahmen in Deutschland nicht hätten durchgeführt werden können, begründe *«in der Gesamtschau der hierbei zu würdigenden Umstände noch kein Beweisverwertungsverbot, denn eine Verletzung allgemeiner rechtsstaatlicher und völkerrechtlicher Grundsätze, gemessen u.a. an Art. 6 Abs. 1 EMRK und dem ordre public, liegt nicht vor»*.<sup>48</sup>

Und selbst wenn es sich um einen eklatanten Verstoß handelt, bleibt immer noch die letzte Hürde, die für die Annahme eines Verwertungsverbots erforderliche Gesamtabwägung, die den Gerichten maximale Freiheit gibt, Beweise aus dem Verfahren herauszuhalten oder – der Regelfall – auch dann zuzulassen, wenn die Beweisgewinnung nicht sauber gelaufen ist.<sup>49</sup> Auch dieses Instrument wird im Hinblick auf die Erkenntnisse aus der Überwachung von Kryptohandys genutzt.<sup>50</sup>

Im Ergebnis bleibt festzuhalten, dass die Bemühungen, die Erkenntnisse aus den von ausländischen Stellen durchgeführten Überwachungsmaßnahmen für unverwertbar erklären zu lassen – angesichts der gestaffelt aufgestellten Verteidigungslinien der Rechtsprechung durchaus vorhersehbar – gescheitert sind. Die Rechtsprechung hat demonstriert, dass sie keinerlei Interesse hat, die Art und Weise der im Ausland erfolgten Beweisgewinnung in irgendeiner Hinsicht zu hinterfragen. Damit manifestieren und realisieren sich die

---

<sup>46</sup> OLG Saarbrücken NStZ 2023, 764, 765.

<sup>47</sup> Schmidt ZStW 134 (2022), 982, 1009; Wahl ZIS 2021, 452, 456; Zimmermann ZfJStW 2022, 173, 189.

<sup>48</sup> OLG Brandenburg BeckRS 2021, 23525 Rz. 10.

<sup>49</sup> Vgl. Wohlers in SK-StPO, 5. Aufl. (2018), Einleitung Rn. 270, 290 m.w.N.

<sup>50</sup> OLG Brandenburg BeckRS 2021, 42283 Rz. 11; KG Berlin BeckRS 2021, 24213 Rz. 38.

Gefahren, die von Patchwork-Verfahren ausgehen und vor denen in der Literatur immer wieder gewarnt wurde:<sup>51</sup> Die in den verschiedenen Nationalstaaten unterschiedlich ausgestalteten Regelungen zur Zulässigkeit von Zwangsmaßnahmen<sup>52</sup> und zu den Verwertungsregeln führen dazu, dass Beweise Eingang in ein Strafverfahren finden können, die in diesem Verfahren selbst gar nicht hätten gewonnen werden können.

Zu konstatieren ist, dass die Rechtsprechung diesen Befund offenbar nicht als ein Risiko für die Rechtsstaatlichkeit des Strafprozesses versteht, sondern vielmehr als Chance, auf Mittel zur Wahrheitsfindung zurückgreifen zu können, die im eigenen nationalen Recht nicht zur Verfügung stehen. Dass es bei den «Anom»-Daten um Erkenntnisse geht, die aus Ermittlungen stammen, die vom FBI initiiert worden sind, die aber in den USA selber ganz offenbar nicht verwertet werden können,<sup>53</sup> wirft ein Schlaglicht darauf, dass es den deutschen Strafgerichten vollkommen egal zu sein scheint, auf welche Art und Weise die in Frage stehenden Erkenntnisse generiert worden sind.

---

<sup>51</sup> Vgl. dazu *Gless* ZStW 115 (2003), 131, 143 ff.; *dies.* ZStW 2004, 353, 365 f.; *dies.* ZStW 125 (2013), 573, 575 ff.; *Swoboda* in FS Ignor (2023), S. 826 f.; *Zimmermann* ZfJStW 2022, 173, 185 f.

<sup>52</sup> Vgl. hierzu *Gless* JR 2008, 317, 320 sowie ausführlich *Riedi*, Auslandsbeweise und ihre Verwertung im schweizerischen Strafverfahren, Zürich 2018, S. 298 ff.; speziell zur Rechtslage in Frankreich bezogen auf Überwachungsmaßnahmen vgl. *Swoboda* in FS Ignor (2023), S. 825 f.; *Wahl* ZIS 2021, 452, 455

<sup>53</sup> Vgl. *Nestler* StV 2022, 280, 282.

## IV. Die Verwertung von nicht verifizierbaren Beweisen

### 1. Der Zugriff auf die zur Prüfung der Datenauthentizität und Datenintegrität notwendigen Unterlagen als Teil des Anspruchs auf ein faires Verfahren

Wie in der Einleitung bereits dargelegt, liegt der Charme der Erkenntnisse aus den Überwachungsmaßnahmen – aus der Warte der Strafverfolgungsbehörden betrachtet – darin, dass die Beschuldigten, weil sie sich sicher fühlten, recht offen miteinander kommuniziert haben. Der Pferdefuß besteht darin, dass sich die Auswertungsberichte zwar flüssig lesen, dass aber niemand verifizieren kann, dass die Kommunikation wirklich so abgelaufen ist, wie dies anhand der Auswertungsberichte der Fall sein soll. Dass es so gewesen ist, kann und muss man glauben – oder eben auch nicht.

Dieser Befund kontrastiert damit, dass auch nach Auffassung des BVerfG gewährleistet sein muss, dass die beschuldigte Person (und ihre Verteidigung) die Informationen zur Kenntnis nehmen und prüfen können, aus denen sich ergibt, wie die Beweise gewonnen wurden.<sup>54</sup> Vom Beschuldigten kann in diesem Zusammenhang weder verlangt werden, darauf zu vertrauen, dass staatliche Stellen sich ordnungsgemäß verhalten haben, noch darf er darauf verwiesen werden, dass das Strafgericht diese Prüfung für ihn vornehmen wird.<sup>55</sup> Er muss vielmehr die Möglichkeit haben, die Strafbehörden bezogen auf die ordnungsgemäße Gewinnung der Erkenntnisse *«auf Zweifel aufmerksam zu machen und einen entsprechenden Beweisantrag zu stellen»*.<sup>56</sup> Dies setzt voraus, dass der

---

<sup>54</sup> Vgl. BVerfG, NJW 2021, 455; Verfassungsgerichtshof Saarland, NJW 2019, 2456, 2457 mit Anm. Krumm; Gall/Haskaya forumpoenale 2023, 301, 304.

<sup>55</sup> Vgl. Wohlers in Donatsch/Forster/Schwarzenegger (Hrsg.), Strafrecht, Strafprozessrecht und Menschenrechte, Festschrift für Stefan Trechsel zum 65. Geburtstag, Zürich 2002, 831.

<sup>56</sup> BVerfG NJW 2021, 455, 457 Rz. 45.

Beschuldigte nicht nur pauschale Behauptungen ins Blaue hinein erhebt, sondern er «konkrete Anhaltspunkte» benennen kann, aufgrund derer die Zuverlässigkeit der Messung in Zweifel zu ziehen ist.<sup>57</sup> Und hieraus folgt letztlich:

*«Der Beschuldigte hat deshalb ein Recht auf möglichst frühzeitigen und umfassenden Zugang zu Beweismitteln- und Ermittlungsvorgängen und auf die Vermittlung der erforderlichen materiell- und prozessrechtlichen Informationen, ohne die er seine Rechte nicht wirkungsvoll wahrnehmen könnte»,<sup>58</sup>*

wobei dieses Recht sich nicht darin erschöpft, die Beweismittel zur Kenntnis nehmen zu können, welche die Anklagebehörde zur Akte genommen hat, sondern darüber hinaus einen Anspruch darauf begründet, «Kenntnis von solchen Inhalten zu erlangen, die zum Zweck der Ermittlung entstanden sind, aber nicht zur Akte genommen wurden».<sup>59</sup>

Die Rechtsprechung verschiedener Gerichte, insbesondere des EGMR und des BVerfG, nach der es ein Teilgehalt des Anspruchs auf ein faires Verfahren ist, dass der Beschuldigte und seine Verteidigung zu den belastenden Beweisen sachgerecht Stellung nehmen können, gilt grundsätzlich für alle Arten von Beweisen, besondere praktische Bedeutung hat sie aber für digitale Beweise, denn hier gilt:

---

<sup>57</sup> BVerfG NJW 2021, 455, 457 Rz. 46.

<sup>58</sup> BVerfG NJW 2021, 455, 458 Rz. 50.

<sup>59</sup> BVerfG NJW 2021, 455, 458 Rz. 51; vgl. auch EGMR v. 26.9.2023, Yüksel Yalcinkaya vs. Türkei, § 327; Kipker/Bruns MMR 2022, 363, 366.

*«Digitale Beweise sind regelmäßig anfällig für Fehler und Manipulationen. Die Beurteilung der Validität der Daten setzt zwingend eine genaue Kenntnis der Rohdaten, der technischen Aufbereitung und des Interpretationsweges voraus.»<sup>60</sup>*

Aus diesem Grund muss die Sicherung, Aufbereitung und Aufbewahrung der Rohdaten den Grundsätzen gerecht werden, die sich im Rahmen der IT-Forensik als Vorgehen *lege artis* entwickelt haben,<sup>61</sup> was indes bei den hier in Frage stehenden Fallgestaltungen offenbar nicht durchgängig geschehen ist.<sup>62</sup>

## 2. Das Akteneinsichtsrecht als Instrument zur Umsetzung des Zugriffs

Des Weiteren muss die Verteidigung in die Lage versetzt werden, den Weg von den Rohdaten zu den Auswertungsberichten nachvollziehen zu können. Die Verteidigung muss *«die Art und Weise der Beweismittelbeschaffung (sog. Chain of Evidence)»* überprüfen können.<sup>63</sup> Dies setzt voraus, dass der Verteidigung bekannt ist, wie die Daten gewonnen worden sind<sup>64</sup> und sie nachvollziehen kann, wie das für die Verfahrensbeteiligten lesbare Ergebnis durch

---

<sup>60</sup> Albrecht jurisPR-Strafrecht 20/2021 Anm. 3 (Abschnitt D.); Kipker/Bruns MMR 2022, 363, 364 f.; Nadeborn/Kemptions jurisPR-StrafR 12/2021 Anm. 4 (Abschnitt D.); vgl. auch EGMR v. 26.09.2023, Yüksel Yalcinkaya vs. Türkei, § 312; Sommer StraFo 2023, 250, 257; Zimmermann ZfStW 2022, 173, 187.

<sup>61</sup> So auch Kipker/Bruns MMR 2022, 363, 365.

<sup>62</sup> Vgl. Kipker/Bruns MMR 2022, 363, 365 f.; Swoboda in FS Ignor (2023), S. 820 und 827.

<sup>63</sup> Gall/Haskaya forumpoenale 2023, 301, 304; Sommerer/Rehberger RDi 2022, 304, 308.

<sup>64</sup> Sommer StraFo 2023, 250, 257; vgl. auch Gall/Haskaya forumpoenale 2023, 301, 303; vgl. auch OLG München StV 2024, 18, 22.

individuelle Datenselektion zustande gekommen ist,<sup>65</sup> was unter anderem auch den Zugang zu den Rohdaten voraussetzt<sup>66</sup> sowie eine Kenntnis der technischen Aufbereitung und des Interpretationsweges.<sup>67</sup>

Der Weg, auf dem die Verteidigung tätig werden muss, wird durch eine leider viel zu wenig beachtete Entscheidung des 3. Strafsenats vom 18. Juni 2009 vorgezeichnet:<sup>68</sup> Die Verteidigung muss sich mit einem Antrag auf Akteneinsicht an die Staatsanwaltschaft bzw. – im Verfahren nach Anklageerhebung – an das erkennende Gericht wenden. Soweit die Rohdaten und die sonstigen zur Verifizierung der «Chain of Evidence» notwendigen Unterlagen sich bei den Akten befinden, ist der Verteidigung im Rahmen des Akteneinsichtsrechts nach § 147 StPO Zugang zu gewähren.<sup>69</sup> Zu den Akten i.S. des § 147 StPO gehören auch die bei einem LKA oder beim BKA gespeicherten Unterlagen, wenn und soweit sie dem Gericht vorzulegen sind.<sup>70</sup> Dies gilt insbesondere auch für Auswertungen der Rohdaten, die weder als ein rein polizeiinternes Arbeitsinstrument eingestuft werden können, noch Spurenakten gleichstehen.<sup>71</sup> Soweit die Rohdaten und die für den Nachvollzug der Auswertung relevanten Unterlagen offengelegt werden, hat die Verteidigung

---

<sup>65</sup> Lödden/Makepeace HRRS 2023, 384, 388; Kipker/Bruns MMR 2022, 363, 364; Sommer StraFo 2023, 250, 257.

<sup>66</sup> Verfassungsgerichtshof Saarland NJW 2019, 2456, 2457 mit Anm. Krumm; Lödden/Makepeace HRRS 2023, 384, 388; Kipker/Bruns MMR 2022, 363, 364.

<sup>67</sup> Nadeborn/Kemppens jurisPR-StrafR 12/2021 Anm. 4 (Abschnitt D).

<sup>68</sup> BGH StV 2010, 228 mit Anm. Stuckenberg.

<sup>69</sup> Zur parallelen Fallgestaltung der Einsichtnahme in die für Geschwindigkeitsmessungen relevanten Unterlagen vgl. OLG Oldenburg DAR 2015, 406, 407 mit Anm. Deutscher; OLG Düsseldorf NZV 2016, 140, 141 mit Anm. Fromm; a.A. OLG Bamberg NStZ 2018, 724, 725 f.

<sup>70</sup> BGH StV 2010, 228, 229; vgl. aber auch BGH NStZ 2023, 116: Daten, die beim BKA gespeichert sind, unterliegen nicht dem Akteneinsichtsrecht, wobei der Senat verlangt, dass direkt beim BKA um Einsicht gebeten wird.

<sup>71</sup> BGH StV 2010, 228, 230 mit zust. Anm. Stuckenberg.

– sinnvollerweise unterstützt durch einen Sachverständigen – das Vorgehen der Strafverfolgungsbehörden nachzuvollziehen.

Dass es dazu kommen wird, dass die Verteidigung Einsicht in die relevanten Unterlagen erhält, erscheint allerdings eher zweifelhaft. Bei den «Encrochat»-Daten haben die französischen Behörden die technische Umsetzung der Entschlüsselung als ein der nationalen Verteidigung unterliegendes Geheimnis eingestuft.<sup>72</sup> Bei den «Sky ECC»-Daten sind offenbar bisher nur aufbereitete Datenbestände, nicht aber die gesamten Rohdaten in die deutschen Strafverfahren gelangt.<sup>73</sup> Und bei den «Anom»-Daten mauert das FBI, was sich schon daran zeigt, dass von dem in die Aktion eingeschalteten ominösen Drittstaat bisher nur bekannt ist, dass es sich um einen Mitgliedsstaat der EU handeln soll.

### 3. Konsequenz im Falle der Nichtgewährung der Einsicht in die Unterlagen

Werden die zur Verifizierung der «Chain of Evidence» notwendigen Unterlagen nicht zur Verfügung gestellt, reduziert sich die Rolle der Verteidigung auf ein *«dekoratives Element im Gerichtssaal»*.<sup>74</sup> Klar ist aber auch, dass auch das Gericht vor exakt den gleichen Schwierigkeiten steht wie die Verteidigung.<sup>75</sup> Wenn aber das Gericht den Beweiswert der in Frage stehenden Informationen nicht verifizieren kann, kann bzw. darf es auch nicht davon ausgehen, dass die in Frage stehenden Informationen den wahren Sachverhalt belegen. Kipker/Bruns haben diesen Befund zutreffend wie folgt auf den Punkt gebracht:

---

<sup>72</sup> Erhard/Lödden, StraFo 2021, 366, 367; Sommer StraFo 2023, 250, 252 f. und 257.

<sup>73</sup> Lödden/Makepeace HRRS 2023, 384, 388.

<sup>74</sup> Sommer StraFo 2023, 250, 258.

<sup>75</sup> Schmidt ZStW 134 (2022), 982, 1012; vgl. auch Sommer StraFo 2023, 250, 257; Zimmermann ZfStW 2022, 173, 187 sowie EGMR v. 26.9.2023, Yüksel Yalcinkaya vs. Türkei, § 312.

*«Bei dem verwendeten Datenmaterial ist offensichtlich, dass dieses zwischenzeitlich vielfach verarbeitet wurde: Zunächst wurden die Daten von den Endgeräten mithilfe von Programmen abgeschöpft, anschließend gespeichert, zusammengeführt, mehrfach versandt, aufbereitet und zusammengestellt. Sie gelangten so dann in das behördliche Verfahren und wurden hier weiterbearbeitet, etwa zur Löschung ‘unerheblicher’ Teile oder um sie mit dem Ziel ‘besserer Lesbarkeit’ neu anzuordnen. Gemessen an den an die Datenauthentizität und Datenintegrität anzulegenden Maßstäben erscheint es deshalb fragwürdig, ob die Daten noch zu dem in der Lage sind, was sie eigentlich sollen, nämlich den Beweis der Begründung einer Straftat zu führen.»<sup>76</sup>*

Wollte man sich allein darauf verlassen, dass die Gerichte den marginalen bzw. nicht existenten Beweiswert der nicht verifizierbaren Auswertungsberichte erkennen und entsprechend würdigen werden, würde man unberücksichtigt lassen bzw. ignorieren, dass es sich nicht nur um Beweise handelt, deren Beweiswert fragwürdig ist, sondern um solche, deren Verwertung nur unter Verletzung zentraler Verteidigungsrechte möglich ist. Insoweit ist eine Parallele zu den Fallgestaltungen zu ziehen, in denen bei personalen Beweismitteln das Konfrontationsrecht nicht gewahrt werden kann und bei denen trotz des auch hier deutlich relativierten Beweiswerts eine Verurteilung jedenfalls dann nicht in Betracht kommt, wenn es sich bei dem kontaminierten Beweismittel um den alleinigen oder ausschlaggebenden Beweis handelt.<sup>77</sup>

---

<sup>76</sup> Kipker/Bruns MMR 2022, 363, 364.

<sup>77</sup> EGMR v. 15.06.1992, Lüdi c. Schweiz, § 49; EGMR v. 28.08.1992, Artner v. Österreich, § 21; EGMR v. 23.04.1997, van Mechelen v. Niederlande, § 52 ff.; EGMR v. 15.12.2011, Al-Khawaja und Taery v. United Kingdom, §§ 146 ff. mit Besprechung *Arquint/Summers* forumpoenale 2012, 113 sowie Anm. Meyer HRRS 2012, 117 ff.; EGMR v. 06.12.2012, Pesukic v. Schweiz, §§ 44 ff. mit Anm. Wohlers forumpoenale 2013, 87 ff.; Meyer in Karpenstein/Mayer (Hrsg.), Kommentar EMRK, 3. Aufl.

Die in diesem Zusammenhang vom BGH ins Spiel gebrachte besonders vorsichtige Beweiswürdigung ist als solche kritisch zu sehen.<sup>78</sup> Im vorliegenden Zusammenhang vermag sie aber von vornherein keine Rolle zu spielen, weil es allein darum geht, ob die Auswertungsberichte den Kommunikationsinhalt zutreffend wiedergeben oder nicht, d.h. es gibt schlicht und einfach nichts, was man hypothetisch in die Beweiswürdigung einstellen könnte. Und damit kommt es zum Schwur: Will man Beweise verwerten, deren Beweiskraft in keiner Weise zu verifizieren ist, oder lehnt man dies ab? Nach hier vertretener Auffassung, die sich auf die Rechtsprechung des EGMR, des BVerfG und auch des italienischen Corte Suprema di Cassazione stützen kann, muss man in den Fällen, in denen die «Chain of Evidence» nicht überprüft werden kann, von einem Verwertungsverbot ausgehen.<sup>79</sup> Die Verwertung der in Frage stehenden Beweise würde einen Konventionsverstoß begründen und die Fairness des Verfahrens aufheben.<sup>80</sup>

---

(2021), Art. 6 Rn. 232; *Harrendorf/König/Voigt* in Meyer-Ladewig/Nettesheim/von Raumer, Handkommentar EMRK, 5. Aufl. (2023), Art. 6 Rn. 228.

<sup>78</sup> Vgl. *Wohlers StV* 2014, 563, ff.; vgl. auch *Wohlers/Singelstein* in SK-StPO, 6. Aufl. (2023), § 96 Rn. 35 ff.

<sup>79</sup> Corte Suprema di Cassazione, 4. Strafkammer, Entscheid vom 15.07.2022, 32915, E. 1; *Gall/Haskaya* forumpoenale 2023, 301, 305 f.; *Kipker/Bruns* MMR 2022, 363, 367 f.

<sup>80</sup> EGMR v. 26.09.2023, *Yüksel Yalcinkaya v. Türkei*, §§ 341, 345.