hängig zu machen, scheidet auch eine Anwendung des § 263 Abs. 5 StGB aus.

Die in gewisser Hinsicht gewollte Privilegierung der Steuerhinterziehung im Vergleich zu den allgemeinen Strafnormen zeigt sich schließlich auch an der Möglichkeit der strafbefreienden Selbstanzeige (§ 371 AO). Zwar besteht diese nicht, wenn bestimmte Regelbeispiele des § 370 Abs. 3 S. 2 AO einschlägig sind oder die Hinterziehungssumme eine bestimmte Höhe erreicht (§ 371 Abs. 2 S. 1 Nr. 3 und 4); selbst in diesen Fällen wird der Täter einer Steuerhinterziehung indes dadurch privilegiert, dass unter den Voraussetzungen des § 398a AO von der Strafverfolgung abzusehen ist. Durch die Anwendbarkeit des § 263 Abs. 5 StGB würden die Privilegien der Selbstanzeige bzw. des § 398a AO in den Fällen gewerbs- und bandenmäßig begangener Steuerhinterziehung *contra legem* faktisch wegfallen. […]

Mitgeteilt von RA Prof. Dr. *Werner Leitner*, München.

Anm. d. Red.: Die Entscheidung ist rechtskräftig. Das OLG Frankfurt/M. hat durch Beschl. v. 06.05.2021 (3 Ws 282/21) die Beschwerde der GStA als unzulässig verworfen.

Anmerkung: Der vorstehende Beschluss des *LG Frankfurt/M.* ist im Kontext eines dort anhängigen und zwischenzeitlich in der Hauptverhandlung befindlichen »cum/ex«-Verfahrens ergangen.

I. *Kontext*. Anlass war die vom *LG* vorgenommene und von der Generalstaatsanwaltschaft Frankfurt angefochtene Abtrennung des Verfahrens eines Mitangeklagten vor Beginn der Hauptverhandlung. Die GenStA hatte bei der Begründung ihrer Beschwerde ganz aktuell und ganz wesentlich auf die Entscheidung des *2. Strafsenats* des *OLG Frankfurt* vom 09.03.2021 abgestellt, wonach bei »cum/ex«-Sachverhalten auch der Tatbestand des gewerbsmäßigen Bandenbetruges im Sinne von § 263 Abs. 5 StGB erfüllt sein könne.[1] Dieser Umstand mache umso mehr eine gemeinsame Hauptverhandlung erforderlich. Das *LG* ist in seinem Nichtabhilfebeschluss der Auffassung des (eigenen) *OLG* nicht gefolgt. Der Betrugstatbestand werde »durch die spezielleren Strafnormen des Steuerstrafrechts, vorbehaltlich weiterer, durch die Taten erlangter, über den Steuervorteil hinausgehender Vorteile in seiner Anwendbarkeit gesperrt.«

II. *Inhalt.* Die in jeder Hinsicht überzeugenden Ausführungen des *LG* beleuchten die vom *2. Strafsenat* des *OLG* aufgeworfene Rechtsfrage nicht nur von allen Seiten, sondern auch mit der erforderlichen Präzision. Indes hat der *2. Strafsenat* des *OLG*, der sich im Rahmen einer Gehörsrüge im selben Verfahrensgang nochmals mit der Thematik zu befassen hatte, sich bei dieser Gelegenheit nochmals selbst bestätigt.[2]

Das *LG* kann für sich die st. Rspr. des *BGH* beginnend mit dem Jahr 1989 in Anspruch nehmen und tut dies auch. Demnach ist § 370 AO sogar dann anzuwenden, wenn der steuerliche Vorgang vom Steuerpflichtigen insgesamt erfunden ist. Selbst dann bleibt für die Anwendung von § 263 StGB kein Raum.[3] Sogar von Finanzbeamten zur eigenen Bereicherung erfundene und im Datenbestand des Finanzamts geführte Steuerpflichtige unterfallen nach Auffassung des *BGH* ausschließlich dem Anwendungsbereich von § 370 AO.[4] Zutreffend spricht das *LG* von der »vollständigen Exklusivität des Steuerstrafrechts«[5] und weist darauf hin, dass anders als in der Begründung des *2. Strafsenats* des *OLG* in der Rechtsprechung des *BGH* eine Differenzierung nach dem Grundtatbestand des § 263 StGB, einem Regelbeispiel (§ 263 Abs. 3 StGB) oder dem vom *OLG* angenommenen Qualifikationstatbestand des gewerbsmäßigen Bandenbetruges (§ 263 Abs. 5 StGB) gerade nicht vorgenommen wird. Das *OLG* führt für die Anwendbarkeit des § 263 Abs. 5 StGB dessen schärferen Strafrahmen ins Feld. Weniger populistisch, aber juristisch zutreffender weist das *LG* darauf hin, dass unterschiedliche Strafrahmen kein Argument für das Abweichen vom Grundsatz der Spezialität[6] sein können:

»Die Verdrängung einer allgemeinen Strafnorm durch eine speziellere geht von der gesetzgeberischen Entscheidung aus, an eine bestimmte Unrechtsausprägung, die im Einzelfall in den Anwendungsbereich der allgemeinen Strafnorm fallen kann, andere Rechtsfolgen – das heißt schärfere *oder mildere* – zu knüpfen« (*Hervorh. i. Orig.*).

Und schließlich verfängt der Hinweis auf die Selbstanzeige nach § 371 AO als entscheidendes Abgrenzungskriterium.

III. *Weiteres Verfahren.* Über die Beschwerde der GenStA hatte zuständigkeitshalber nicht der *2.*, sondern der *3. Strafsenat* des *OLG Frankfurt* zu befinden. Dort wurde die Beschwerde als unzulässig verworfen, weil Abtrennungsbeschlüsse des erkennenden Gerichts grundsätzlich nach § 305 StPO unanfechtbar seien. Die Ausnahmefälle der Willkür oder der Verfolgung verfahrensfremder Zwecke lägen erkennbar nicht vor. Die Formenstrenge half dem *3. Senat* aus dem Dilemma. Man wäre schon gespannt gewesen, ob und wie er sich zur Rechtsauffassung des *2. Strafsenats* verhalten hätte. Bleibt nur abzuwarten, ob der *BGH* das Thema nochmals aufgreift.

Rechtsanwalt und Fachanwalt für Strafrecht
Prof. Dr. *Werner Leitner*, München.

Unverwertbarkeit von EncroChat-Daten

GG Art. 10; RiLi-EEA Art. 31; IRG § 91g Abs. 6; StPO §§ 100a, 100b, 100e Abs. 5, 479 Abs. 2

Die Datenabschöpfung bei EncroChat-Nutzern auf deutschem Staatsgebiet wurde unter Missachtung individualschützender Rechtshilfevorschriften und ohne den nach den insoweit maßgeblichen Regelungen des deutschen Rechts erforderlichen konkreten Tatverdacht durchgeführt; dies führt zur Unverwertbarkeit der Daten.

LG Berlin, Beschl. v. 01.07.2021 – 525 KLs 10/21 n.r.

Aus den Gründen: Die Voraussetzungen für die Eröffnung des Hauptverfahrens liegen nicht vor. Der Angesch. ist der ihm vorgeworfenen Taten aus tatsächlichen Gründen nicht hinreichend verdächtig. Die Tatvorwürfe werden mit den zur Verfügung stehenden Beweismitteln nicht zu belegen sein. Die Anklage stützt sich im Wesentlichen nur auf die über den EncroChat-Dienst geführte Kommunikation des Angesch. Diese unterliegt jedoch einem Verwertungsverbot.

1 OLG Frankfurt StV 2021, 456 m. krit. Anm. *Ransiek* StV 2021, 458 und m. krit. Anm. *Adick/Linke* NZWiSt 2021, 238; abl. auch *Mosbacher* NJW 2021, 1916.
2 OLG Frankfurt, Beschl. v. 06.05.2021 – 2 Ws 132/20, vgl. Pressemitteilung Nr. 42/2021 v. 31.05.2021, https://ordentliche-gerichtsbarkeit.hessen.de/sites/ordentliche-gerichtsbarkeit.hessen.de/files/PI%2002ws13220%20%28Anh%C3%B6rungsr%C3%BCge%20Cum-Ex%29_0.pdf. (URL zuletzt abgerufen am 30.06.2021).
3 BGH StV 1990, 207 m.w.N. zum damaligen Stand der Diskussion.
4 BGHSt 51, 356 = NJW 2007, 2864; die Anwendbarkeit von § 263a StGB neben § 370 AO wurde ausdrücklich abgelehnt.
5 Unter Verweis auf *Gaede*, Der Steuerbetrug, 2016, S. 193 ff.
6 Lat. *lex specialis derogat legii generalii*.

I. Die StA legt dem Angesch. 16 Fälle des unerlaubten Handeltreibens mit Btm in nicht geringer Menge zur Last. Für die Absprachen mit seinen Lieferanten und Abnehmern sowie seinen mutmaßlichen Mittätern M., G. und R. soll er sich des als besonders sicher beworbenen niederländischen Kommunikationsdienstes EncoChat bedient haben. Dieser bot über ein Händlernetz Endgeräte (Krypto-Handys) mit modifizierter Hardware und spezieller Software nebst Nutzungslizenzen zu Preisen zwischen 1.000 und 2.000 € an und ermöglichte damit über einen in Roubaix (Frankreich) stationierten Server eine Ende-zu Ende verschlüsselte Kommunikation.

Die Anklagevorwürfe beruhen im Wesentlichen auf von dem Angesch. verfassten bzw. an ihn gerichteten Chatnachrichten, die mit hoher Wahrscheinlichkeit die in der Anklage beschriebenen Handelsgeschäfte zum Gegenstand haben und auch seine Identifizierung ermöglichen würden. Weitere aussagekräftige Beweismittel stehen nicht zur Verfügung.

Die Chatnachrichten wurden durch eine TKÜ-Maßnahme der französischen Behörden im Rahmen dort geführter Ermittlungen erlangt. Die technischen Einzelheiten dieser Überwachungsmaßnahmen sind nicht bekannt; diese unterliegen in Frankreich dem *secret de Ia défense nationale* (d.h. der Geheimhaltung der Landesverteidigung – vgl. etwa den Beschl. des *Juge des Libertés et de* Ia *Détention* – »Richter der Freiheiten und der Haft«, im Folgenden: JLD in Lille v. 20.03.2020, S. 5). Die Ermittlungen lassen sich aber in den wesentlichen Zügen anhand der ab dem 30.01.2020 ergangenen französischen Gerichtsbeschl. und der zugrunde liegenden Anträge der französischen StA nachvollziehen. Ergänzende Informationen ergeben sich aus den zum Themenkomplex »EncroChat« bisher ergangenen Beschl. deutscher OLG (*OLG Bremen* v. 18.12.2020 – 1 Ws 166/20; *OLG Hamburg* v. 29.01.2021 – 1 Ws 2/21; *OLG Rostock* v. 23.03.2021 – 20 Ws 70/21 und *OLG Schleswig* v. 29.04.2021 – 2 Ws 47/21; jew. in juris, sowie *OLG Rostock* v. 11.05.2021 – 20 Ws 121/21, BeckRs 11981), aus der im Internet veröffentlichten Entscheidung des englischen *High Court* v. 26.10.2020 – [2020] EWHC 2967 (Admin) – über den Antrag eines Besch. auf gerichtliche Überprüfung der dortigen Europäischen Ermittlungsanordnung und aus der Entscheidung des englischen *Court of Appeal* v. 05.05.2021 – [2021] EWCA Crim 128-, die die Beschwerde gegen eine Vorabentscheidung des Crown Court über die Zulassung der EncroChat-Daten als Beweismittel im Strafverfahren zum Gegenstand hatte.

Danach stellt sich der Sachverhalt wie folgt dar:

1. In den Jahren 2017 und 2018 wurden in ca. 15 französischen Ermittlungsverfahren, die überwiegend Drogenhandel im mehrstelligen Kilobereich betrafen, EncroChat-Handys festgestellt. ln der Folgezeit wurde eine Vorermittlung *(enquête préliminaire)* u.a. wegen des Verdachts der Bildung einer kriminellen Vereinigung eingeleitet. l.d.R. gelang es mit richterlicher Genehmigung, Kopien der auf dem Server vorhandenen Daten zu beschlagnahmen. Deren Analyse ergab 66.134 im System eingetragene SIM-Karten eines niederländischen Betreibers aus einer Vielzahl von Ländern. Ferner konnten 3.477 auf dem Server gespeicherte Memodateien von Nutzern entschlüsselt werden. Insb. die Memos dreier französischer Nutzer wurden von den Behörden als Aufzeichnungen über kriminelle Handelsaktivitäten bewertet.

2. Da die Entschlüsselung der zwischen den Nutzern gewechselten Chat-Nachrichten auf dem Server nicht möglich war, entschlossen sich die französischen Behörden, unmittelbar auf die Endgeräte zuzugreifen. Erklärtes Ziel dieser Maßnahme war es, die kriminellen Nutzer zu »identifizieren«, »ihre kriminellen Aktivitäten aufzuzeigen« und sie »festzunehmen« (vgl. den Antrag der französischen StA v. 29.01.2020, S. 2 [12]). ln mehreren Beschl. ab dem 30.01.2020 genehmigten zunächst der JLD und – nach Eröffnung der zweiten Ermittlungsphase der Untersuchungsrichter *(Juge d'instruction)* auf der Grundlage der französischen Regelung über die Online-Durchsuchung und die Quellen-TKÜ (Art. 706-102-1 der französischen StPO CPP) die Installation einer Abfangeinrichtung auf den Krypto-Handys und den dafür erforderlichen Zugriff auf den Server. Zur Verdachtslage heißt es dort, dass in mehreren Strafverfahren entsprechende Telefone aufgefallen seien (Beschl. des JLD v. 30.01.2020, S. 4 f.); ferner seien auf dem Server Memos einiger Nutzer mit mutmaßlichem Bezug zu kriminellen Aktivitäten gefunden und entschlüsselt worden (a.a.O. S. 4 f.). Zur Verhältnismäßigkeit wird ausgeführt, die Maßnahme sei erforderlich, weil es sich um das einzige Mittel handele, um zur Identifizierung und Festnahme der kriminellen Nutzer zu gelangen; sie sei auch der Schwere der Taten, die Gegenstand der Ermittlungen seien, angemessen (a.a.O. S. 5).

ln der Folgezeit wurden diese Maßnahmen mit Unterstützung niederländischer Experten i.R.e. gemeinsamen Ermittlungsgruppe umgesetzt. Um die Verschlüsselung zu umgehen, wurde auf dem Server eine Schadsoftware installiert, die sodann über ein simuliertes Update auf alle Endgeräte des Typs BQ X2 – eines von mehreren am Markt angebotenen Modellen – eine Trojaner-Software aufspielte. Insg. waren von der Maßnahme 32.477 Nutzer in 122 Ländern betroffen. Die Datenabschöpfung geschah sodann in zwei Phasen. In Phase 1 wurden ab dem 01.04.2020 zunächst die auf dem Telefon gespeicherten Daten – insb. Chat-Nachrichten, aber auch die Geräte-IMEI, Benutzernamen, Adressbücher und Memos – ausgelesen. Wegen der von den meisten Nutzern verwendeten Löscheinstellungen wurden dabei überwiegend nur Nachrichten der zurückliegenden sieben Tage erlangt; auch bei dem Angesch. wurden Nachrichten erst ab dem 26.03.2020 ermittelt. in Phase 2 wurden sodann die laufenden ein und ausgehenden Chat-Nachrichten (wahrscheinlich durch Keylogging und/oder Screenshots) abgefangen. Die Daten wurden durch den Trojaner an einen Server des Cybercrime-Zentrums der französischen Gendarmerie (C3N) übermittelt und von dort an einen Europol-Server weitergeleitet

Die Auswertung der in Frankreich betriebenen Geräte ergab per 29.04.2020 für 242 von insg. 380 Nutzern (= 63,7 %) Belege dafür, dass das Krypto-Telefon zu kriminellen Zwecken, überwiegend im Bereich des Drogenhandels, genutzt wurde (vgl. Beschl. des JLD v. 29.04.2020, S. 2). Mit Stand v. 12.06.2020 betrug die Zahl mutmaßlich krimineller französischer Nutzer 317 von insg. 471 (= 67,3 %) (vgl. den Beschl. des Untersuchungsrichters v. 12.06.2020, S. 4).

3. Die auf den Endgeräten der ausländischen Nutzer abgeschöpften Daten wurden ab dem 03.04.2020 den Ermittlungsbehörden der jeweiligen Heimatländer laufend zur Verfügung gestellt. Dabei handelte es sich namentlich um die IMEI des in dem jeweiligen Land festgestellten Endgerätes, dessen E-Mail-Adresse, E-Mail-Adressen der Kontaktpartner, Datum und Uhrzeit der Kommunikation, den Standort des Funkmastes, über den das Endgerät eingebucht war, sowie die in den Chats übermittelten Texte und Bilder.

ln der Zeit v. 03.04.2020 bis zur Einstellung des EncroChat-Betriebs am 28.01.2020 erhielt das BKA von Europol tägliche Datenlieferungen (vgl. den Datenlieferungsbericht des BKA v. 26.08.2020). Auf die EEA der GStA Frankfurt/M. v. 02.06.2020 genehmigte das Untersuchungsgericht in Lille mit Beschl. v. 13.06.2020 die Übersendung und Verwendung in deutschen Strafverfahren.

Die dem BKA übermittelten Datenpakete wurden i.R.d. von der GStA Frankfurt/M. u.a. wegen des Verdachts des bandenmäßigen Handeltreibens mit Btm in nicht geringer Menge und der Bildung einer kriminellen Vereinigung eingeleiteten Verfahrens […] auf behördeneigene Server übertragen, entschlüsselt, entpackt, aufbereitet und ausgewertet. Dies führte u.a. zu dem Trennverfahren gegen den hiesigen Angesch.

II. Die Chat-Daten des Angekl., auf die die Anklage sich als maßgebliches Beweismittel stützt, können die Tatvorwürfe nicht belegen. Sie sind nicht verwertbar.

1. *Prüfung der Verwertbarkeit von Amts wegen*. Die Frage der Verwertbarkeit ist im Zwischenverfahren zu prüfen, obwohl insoweit von der Verteidigung bislang keine Einwände erhoben wurden.

Die vom *BGH* in st. Rspr. für das Revisionsverfahren entwickelte Widerspruchslösung steht dem nicht entgegen. Danach kann

der Revisionsführer sich auf ein Beweiserhebungs- oder Beweisverwertungsverbot nur berufen, wenn er der Erhebung bzw. Verwertung in der Hauptverhandlung widersprochen hat. Das erkennende Gericht ist gleichwohl nicht daran gehindert, mit Blick auf ein solches Verbot von Amts wegen von der Erhebung bzw. Verwertung der Beweise abzusehen; es ist sogar nicht anders als die StA im Ermittlungsverfahren – grds. verpflichtet, diese Frage von Amts wegen zu prüfen (*BGH*, Beschl. v. 01.08.2002, 3 StR 122/02, juris Rn. 12 [= StV 2003, 2]; enger – Recht des Tatrichters zur Prüfung von Amts wegen, aber regelmäßig keine Pflicht – *BGH*, Beschl. v. 07.03.2006 – 1 StR 316/05, juris Rn. 8 [= StV 2006, 225]). Die Widerspruchslösung postuliert in erster Linie eine Obliegenheit des Revisionsführers. Zwar räumt sie ihm damit zugleich eine Dispositionsfreiheit ein, ob er sich auf den Rechtsverstoß berufen will. Diese geht indes nicht so weit, das Tatgericht zu zwingen, sehenden Auges sein Urt. auf rechtsstaatswidrig erlangtes belastendes Beweismaterial stützen und damit den Rechtsverstoß perpetuieren zu müssen.

Für das Zwischenverfahren folgt daraus, dass das Tatgericht bereits die Eröffnung ablehnen muss, wenn durchgreifende Anhaltspunkte für eine Unverwertbarkeit entscheidender Beweismittel bestehen und nicht zu erwarten ist, dass die Hauptverhandlung insoweit andere Erkenntnisse erbringen wird.

So liegt es hier. Die Datenabschöpfung bei den EncroChat-Nutzern auf deutschem Staatsgebiet wurde unter Missachtung individualschützender Rechtshilfevorschriften und ohne den nach den insoweit maßgeblichen Regelungen des deutschen Rechts erforderlichen konkreten Tatverdacht durchgeführt (dazu **2.**). Dies führt zur Unverwertbarkeit der Daten (dazu **3.** und **4.**). Abweichende Erkenntnisse sind von der Hauptverhandlung nicht zu erwarten (dazu **5.**).

2. *Verletzung des IT-Grundrechts und des Art. 10 GG*. Die der Anklage zugrunde gelegten Chat-Nachrichten stammen aus der heimlichen technischen Infiltration des Mobiltelefons des Angesch. mit dem Ziel, längerfristig Zugriff auf darauf gespeicherte Daten zu erlangen (Online-Durchsuchung) und die laufende Kommunikation zu überwachen (Quellen-TKÜ). Eine solche Maßnahme greift in besonders schwerwiegender Weise in das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Schutz der Vertraulichkeit und Integrität von informationstechnischen Systemen (im Folgenden: IT-Grundrecht) bzw. in das Telekommunikationsgeheimnis (Art. 10 GG) ein (vgl. grdl. *BVerfG* v. 27.02.2008 – 1 BvR 370/07 und 595/07, juris Rn 187ff. [= StV 2008, 169 [Ls]]). Bei Überwachungsmaßnahmen ausländischer Behörden, die im Rahmen dort geführter Ermittlungsverfahren nach den dort geltenden Vorschriften angeordnet wurden, begründet die nachträglich im Wege der Rechtshilfe ermöglichte Verwendung in einem deutschen Strafverfahren einen eigenständigen Eingriff (*BGH* v. 21.11.2012 – 1 StR 310/12, juris Rn. 45 m.w.N. [= StV 2014, 193]).

Dieser Eingriff ist hier nicht gerechtfertigt. Dabei kann offenbleiben, ob bei der *Übermittlung der Daten an die deutschen Behörden* die einschlägigen Rechtshilfevorschriften in jeder Hinsicht beachtet wurden und welche Folgen ggf. ein Verstoß hätte (vgl. dazu *OLG Bremen* a.a.O. Rn. 29 ff.; *OLG Hamburg*, a.a.O. Rn. 106 ff.). Die Rechtswidrigkeit ergibt sich hier bereits daraus, dass die Daten unter Verstoß gegen die Richtlinie 2014/41/EU über die Europäische Ermittlungsanordnung (im Folgenden: RiLiEEA) und gegen die zu ihrer Umsetzung erlassenen Regelungen im Gesetz über die internationale Rechtshilfe in Strafsachen (IRG) *erlangt* wurden (dazu **a**). Die Maßnahme ist zudem auch deshalb rechtswidrig, weil bei ihrer Anordnung und Durchführung der nach §§ 1OOa, 100b StPO erforderliche qualifizierte Tatverdacht nicht vorlag (dazu **b**).

a) *Art. 31 RiLi-EEA, § 91g Abs. 6 IRG*. Wenn ein Mitgliedstaat den Telekommunikationsverkehr von Personen auf deutschem Hoheitsgebiet überwachen will, muss er die zuständige deutsche Stelle vor Beginn der Maßnahme (bzw. sobald ihm der Aufenthalt der Person bekannt wird) darüber unterrichten (Art. 31 Abs. 1 Richtlinie 2014/41/EU – im Folgenden: RiLi-EEA). Das dafür im Anhang C der Richtlinie vorgesehene Formblatt fordert u.a. »alle erforderlichen Angaben, einschließlich einer Beschreibung des Falles (...), damit die unterrichtende Behörde bewerten kann, ob die Überwachung in einem ähnlichen innerstaatlichen Fall genehmigt würde und ob das dabei erlangte Material in einem Gerichtsverfahren verwendet werden kann«. Kommt die deutsche Stelle auf der Grundlage dieser Angaben zu dem Ergebnis, dass die Maßnahme in einem vergleichbaren innerstaatlichen Fall nicht genehmigt würde, hat sie dieser binnen 96 Std. zu widersprechen. Die ausländische Maßnahme kann dann nicht durchgeführt bzw. nicht fortgeführt werden; etwaige schon gesammelte Daten dürfen vom ersuchenden Staat nicht oder nur unter bestimmten Bedingungen verwendet werden(§§ 91g Abs. 6, 91c Abs. 2 Nr. 2 c) dd), 59 Abs. 3 IRG; Art. 31 Abs. 3 RiLi-EEA).

Nach den bislang bekannt gewordenen Informationen ist davon auszugehen, dass es ein solches Ersuchen des französischen Staats und eine Überprüfung durch die zuständige deutsche Stelle hier nicht gegeben hat (vgl. *OLG Schleswig* a.a.O. Rn. 25; *OLG Hamburg* a.a.O. Rn. 99 [104]; *OLG Bremen* a.a.O. Rn. 26). Entgegen *OLG Hamburg* (a.a.O. Rn. 103) und *OLG Schleswig* (a.a.O. Rn. 25) war die Unterrichtung nicht entbehrlich. Insb. lässt sich dies nicht damit begründen, »Zielpersonen« der Maßnahme seien die Betreiber von EncroChat gewesen (so aber *OLG Schleswig* a.a.O. Rn. 25). Dabei kommt es an dieser nicht einmal darauf an, ob die Nutzer der Endgeräte im französischen Verfahren den formalen Status eines Besch. hatten oder zumindest ein Tatverdacht gegen sie bestand. Art. 31 RiLiEEA knüpft nicht an den verfahrensrechtlichen Status des Betr. an, sondern stellt allein darauf ab, dass sich der Nutzer des überwachten Endgerätes auf ausländischem Hoheitsgebiet befindet. Dies war hier jedenfalls bei dem Angesch. und dem größten Teil der anderen Nutzer der Fall. Die Unterrichtung nach Art. 31 RiLi-EEA hätte sich somit selbst dann, wenn die Nutzer nur Kontaktpersonen der Besch. gewesen wären, nicht nur »angeboten« (so *OLG Schleswig* a.a.O. Rn. 25), sondern wäre zwingend erforderlich gewesen.

b) *§§ 100a, 100b StPO*. Die Prüfung nach Art. 31 RiLi-EEA, § 91g Abs. 6 IRG hätte hier ergeben, dass die Maßnahme mit den §§ 100a, 100b StPO nicht vereinbar ist. Der danach erforderliche qualifizierte Tatverdacht gegen die betroffenen deutschen Nutzer einschließlich des hiesigen Angesch. – lag nicht vor (dazu **aa**).

Dieser Umstand ist für die Frage der Verwertbarkeit auch unabhängig von dem formalen Verstoß gegen das Rechtshilferecht beachtlich. Die Überwachungsmaßnahme ist in vollem Umfang am Maßstab der deutschen Strafprozessordnung zu überprüfen (dazu **bb**). Zudem würde man auch bei einer nur beschränkten Prüfungstiefe zu keinem anderen Ergebnis gelangen (dazu **cc**).

aa) *Kein konkreter Verdacht einer Katalogtat*. Eine heimliche TKÜ zum Zweck der Strafverfolgung setzt nach §§ 100a, 100b

StPO wie jede andere strafprozessuale Zwangsmaßnahme auch (vgl. *BVerfG* NStZ RR 2004, 143) – den Verdacht einer Straftat voraus. §§ 100a, 100b StPO schränken den Kreis der Anlasstaten – abgestuft nach der Schwere des Grundrechtseingriffs auf bestimmte Katalogtaten ein, wobei der Tatverdacht sich jew. auf »bestimmte Tatsachen« gründen muss. Damit soll den Vorgaben des *BVerfG* Rechnung getragen werden, wonach bei einem heimlichen Zugriff auf personenbezogene Telekommunikationsdaten wegen der besonderen Schwere der damit verbundenen Eingriffe in Art. 10 GG bzw. in das Grundrecht auf IT-Sicherheit erhöhte Anforderungen sowohl an die Bedeutung der aufzuklärenden Straftat als auch an den Verdachtsgrad zu stellen sind (vgl. etwa *BVerfG*, Beschl. v. 16.06.2009 – 2 BvR 902/06, »E-Mail-Beschlagnahme«, juris Rn. 75 [79] [= StV 2009, 617]; grdl. zu der entsprechenden Frage im präventiven Bereich: *BVerfG*, Urt. v. 27.02.2008 –1 BvR 370/07 – »Online-Durchsuchung«, juris Rn. 250 f. [= StV 2008, 169 [Ls]]). Die den Verdacht begründenden Tatsachen müssen jew. so beschaffen sein, dass sie den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen. Vage Anhaltspunkte, bloße Vermutungen oder allgemeine Erfahrungssätze reichen nicht (*BVerfG*, Urt. v. 27.02.2008 – 1 BvR 370/07, juris Rn. 250 f. [= StV 2008, 169 [Ls]]).

Ein diesen Anforderungen genügender konkreter Verdacht einer der in §§ 100a, 100b StPO genannten Straftaten lag gegen die Nutzer vor der Durchführung der Maßnahme nicht vor.

(1) Die Nutzer der Endgeräte waren als Besch. des französischen Ermittlungsverfahrens anzusehen. Sie waren zudem – unabhängig vom Beschuldigtenstatus – »Zielpersonen« der Maßnahme.

Aus den französischen Anträgen und Beschl. ergibt sich, dass die Infiltration der Endgeräte und das Abschöpfen der Daten hier als eine Maßnahme der Strafverfolgung wegen des Verdachts der Bildung einer kriminellen Vereinigung und wegen verschiedener Delikte im Zshg. mit der Bereitstellung der Verschlüsselungstechnik erfolgte. Konkrete Besch. werden weder in den Anträgen der StA noch in den Gerichtsbeschl. benannt. Angesichts der Vorwürfe im Zshg. mit der Verschlüsselungstechnik dürften die Ermittlungen sich jedenfalls gegen die – möglicherweise namentlich noch unbekannten – Betreiber des EncroChatServices gerichtet haben.

Darüber hinaus zielten die Ermittlungen auch von Anfang an gegen die – damals ebenfalls namentlich noch nicht bekannten – Nutzer; zumindest nach deutschem Rechtsverständnis waren diese ebenfalls als Besch. anzusehen. Ziel der Überwachungsmaßnahme war es, »die Nutzer zu identifizieren«, »ihre kriminellen Aktivitäten aufzuzeigen« und sie »festzunehmen« (Antrag der französischen StA v. 29.01.2020, S. 2 [12]). Zu diesem Zweck wurden die von den Mobiltelefonen ausgeleiteten Daten den Strafverfolgungsbehörden in den Heimatländern der betroffenen Nutzer laufend mit nur geringem zeitlichem Verzug zur Verfügung gestellt. Ab dem 07.04.2020 wurden die Ermittlungen zudem unmittelbar wegen Straftaten der Nutzer (Btm- und Waffendelikte) geführt (vgl. den Antrag der französischen StA v. 29.04.2020, S. 4).

Auch wenn die Ermittlungen sich noch gegen weitere Besch. – insb. die Betreiber des EncroChat-Dienstes – richteten, waren ausschließlich die Nutzer Adressaten der Maßnahme i.S.v. § 100 Abs. 3 StPO. Die Nutzer waren nicht etwa als »Annex« zu einer Ausspähung des Severs betroffen. Auch handelte es sich nicht um eine Maßnahme gegen »das EncroChatSystem« oder »die Firma EncroChat« (so *OLG Hamburg* a.a.O. Rn. 91; ähnlich *OLG Schleswig* a.a.O. Rn. 24 f.), von der die mit dem System verbundenen Nutzer notwendigerweise mitbetroffen gewesen wären. Die Infiltration der Endgeräte zielte vielmehr *ausschließlich* auf die Überwachung der Kommunikation der Nutzer mit dem Ziel der Feststellung etwaiger von ihnen begangener Straftaten (von denen letztlich auch die Strafbarkeit der EncroChat-Betreiber abhing) ab. Bei diesen Kommunikationsdaten handelt es sich nicht um »Daten der Firma EncroChat« (vgl. *OLG Hamburg* a.a.O.), sondern ausschließlich um solche der Nutzer. Das Unternehmen EncroChat war von der Maßnahme nur insoweit betroffen, als der Server als »Sprungbrett« benutzt wurde, um das Implantat auf die Endgeräte aufspielen zu können.

(2) Zum Zeitpunkt der Anordnung und Durchführung gab es keinen Tatverdacht gegen die Nutzer der Endgeräte, der die Überwachung gerechtfertigt hätte.

Es mag sein – worauf das *OLG Hamburg* (a.a.O. Rn. 93) maßgeblich abstellt-, dass es bereits bei der Kopie des Servers im Jahr 2018 den Verdacht gab, dass »jemand« eine schwere Straftat begangen hat. Diese Verdachtsmomente richteten sich aber nur gegen einzelne konkrete Besch., gegen die Betreiber des EncroChat-Dienstes und möglicherweise auch gegen Händler. Die Überwachung der Kommunikation dieser Personenkreise wäre danach möglicherweise gerechtfertigt gewesen. Davon zu unterscheiden ist aber die hier in Rede stehende Datenabschöpfung auf den Endgeräten. Die Überwachung der Nutzer hätte einen gerade gegen sie gerichteten Tatverdacht vorausgesetzt.

Ausreichende Tatsachen, die den unterschiedslosen Zugriff auf die Daten sämtlicher Nutzer eines bestimmten Gerätemodells einschließlich des Angesch. gerechtfertigt hätten, gab es nicht. Die Verdachtsmomente gegen die Nutzer der Endgeräte erschöpften sich darin, dass das EncroChat-System mit besonders aufwändigen und für die Nutzer vergleichsweise kostenintensiven Sicherungen versehen war, dass in mehreren – überwiegend wegen Btm-Straftaten, aber auch wegen anderer Delikte geführten – Strafverfahren die Verwendung solcher Endgeräte für kriminelle Zwecke festgestellt wurde und dass die Adressaten der Maßnahme ebenfalls derartige Endgeräte nutzten.

Um konkrete Tatsachen in dem oben beschriebenen Sinne handelt es sich dabei nicht. Die bloße Verwendung eines Krypto-Handys auch eines solchen mit weit überdurchschnittlich hohem Sicherheitsstandard – lässt nicht nur keinen Schluss auf ein seiner Art nach und in zeitlicher Hinsicht zumindest in groben Zügen umrissenes strafbares Verhalten zu; sie trägt für sich gesehen (entgegen *OLG Rostock*, Beschl. v. 23.03.2021 – 20 Ws 70/21, juris Rn. 11 und v. 11.05.2021 – 20 Ws 121/21, BeckRS 2021, 11981 Rn 14 sowie *OLG Bremen* a.a.O. Rn. 16) nicht einmal den allgemeinen Schluss auf *irgendeine* Straftat.

(a) Dass Straftäter häufig ein besonderes Interesse am Schutz ihrer Kommunikation gegen staatliche Zugriffe haben und deshalb schwer zu überwachende Kommunikationswege – etwa die VoIPTelefonie über Messenger-Dienste oder den Tor Browser – bevorzugen, ist allg. bekannt. Ein genereller Schluss aus einem besonderen Sicherungsbedürfnis auf ein strafbares Verhalten wäre aber genauso unzulässig, wie etwa allein der Besitz von typischerweise bei Einbrüchen oder Fahrraddiebstählen genutzten Werkzeugen (Brechstangen, Bolzenschneider) nicht den für eine Durchsuchung nötigen Anfangsverdacht liefern kann.

(b) Verschlüsselungstechnologien sind auch deshalb für sich gesehen kein tauglicher Anknüpfungspunkt für einen Tatverdacht, weil ihre

Nutzung aus staatlicher Sicht nicht etwa unerwünscht ist, sondern im Gegenteil zum Schutz vertraulicher Daten vor den Zugriffen Dritter gestärkt werden soll. So heißt es in der Digitalen Agenda der Bundesregierung für 2014–2017 (S. 3), einfach zu nutzende Verschlüsselungsverfahren müssten gefördert werden, um »die wirtschaftlichen und gesellschaftlichen Potenziale des digitalen Wandels zu erschließen«. Auf diese politischen Entscheidungen nimmt auch die Gesetzesbegründung zu §§ 100a, 100b StPO n.F. Bezug (BT-Drs. 18/12785, S. 48). Von der Möglichkeit, Anbieter derartiger Dienste zur Implementierung von »Hintertüren« (*back doors*) zu verpflichten, wollte der deutsche Gesetzgeber deshalb bewusst keinen Gebrauch machen (a.a.O., S. 48).

Die 2017 neu eingeführten Ermittlungsmaßnahmen der Online-Durchsuchung und Quellen-TKÜ sollten also nicht etwa der Nutzung von verschlüsselter Kommunikation entgegenwirken, sondern lediglich eine effektive Strafverfolgung auch unter den – grds. erwünschten – veränderten technischen Gegebenheiten ermöglichen (a.a.O.., S. 48). Dem lag der Befund zugrunde, dass sich die in allen Lebensbereichen zu beobachtende Verlagerung der Kommunikation auf IP-basierte und häufig verschlüsselte Dienste auch in der Kommunikation von Straftätern niederschlägt und deren Überwachung mit den Mitteln der »klassischen« TKÜ i.d.R. technisch nicht möglich ist (vgl. die Gesetzesbegründung, a.a.O. S. 46 ff.).

Auch auf europäischer Ebene werden Verschlüsselungstechnologien grds. befürwortet. So heißt es in der Entschließung des Rates der EU zur Verschlüsselung v. 24.11.2020 – 13084/1120 (abrufbar im Internet), die EU unterstütze »uneingeschränkt die Entwicklung, Umsetzung und Nutzung starker Verschlüsselung«; diese sei »ein notwendiges Mittel zum Schutz der Grundrechte und der digitalen Sicherheit von Regierungen, Industrie und Gesellschaft« (a.a.O., S. 2). Kryptotechnologien sind danach kein »schwerer Angriff«, auf die Rechtsordnung (*OLG Schleswig* a.a.O. Rn. 20), sondern dienen im Gegenteil deren Schutz; Nutzer verschlüsselter Kommunikation begeben sich nicht etwa »sehenden Auges in eine nicht schützenswerte Sphäre« (so *OLG Rostock* v. 11.05.2021 – 20 Ws 121/21, BeckRS 2021, 11981 Rn. 18) und setzen auch keinen »Rechtsschein für die Verwertbarkeit« (a.a.O. Rn. 23), sondern müssen lediglich mit dem Zugriff der Strafverfolgungsbehörden auf diese Sphäre – ebenso wie auf andere schützenswerte Bereiche – *in dem gesetzlich vorgesehenen Rahmen,* d.h. unter den vom Gesetzgeber dafür im Einzelnen bestimmten Voraussetzungen rechnen.

(c) Mit diesen gesetzgeberischen Wertungen ist es nicht vereinbar, einen Tatverdacht allein an die Nutzung eines verschlüsselten Kommunikationsdienstes zu knüpfen. Für den im Vergleich zu anderen, ebenfalls Ende-zu-Ende verschlüsselten Diensten wie WhatsApp oder Facebook Messenger lediglich noch stärker abgesicherten EncroChat-Dienst kann nichts anderes gelten. Ein staatlich grds. erwünschtes Verhalten – Schutz der eigenen Daten vor fremdem Zugriff – kann nicht dadurch zum Ausgangspunkt strafrechtlicher Zwangsmaßnahmen werden, dass es besonders perfektioniert wird.

Allerdings drängt sich auf, dass EncroChat durch seine besonderen Sicherheitsvorrichtungen auch in besonderem Maße attraktiv für Kriminelle wurde; ein entscheidender Unterschied zu anderen verschlüsselten Diensten liegt darin aber nicht. Der besonders hohe Sicherheitsstandard machte EncroChat zudem gleichermaßen interessant für andere Personen mit ausgeprägtem Sicherungsbedürfnis – wie etwa Journalisten, politische Aktivisten, die eine staatliche Verfolgung oder die Beobachtung durch Geheimdienste fürchten oder Mitarbeiter von Unternehmen, die sich vor Industriespionage schützen wollen. In der Entschließung des Rates der EU v. 24.11.2020 (a.a.O. S. 3) heißt es dazu, Verschlüsselungstechnologien würden zunehmend »in allen Bereichen des öffentlichen und privaten Lebens eingesetzt« und trügen dazu bei, »Einzelpersonen, die Zivilgesellschaft, kritische Infrastrukturen, die Medien sowie die Journalistinnen und Journalisten, die Industrie und die Regierungen zu schützen, indem sie die Privatsphäre, Vertraulichkeit, Datenintegrität und Verfügbarkeil von Kommunikationsdaten und personenbezogenen Daten sicherstellen«: besonders bedeutsam seien diese zur Sicherung des erforderlichen Schutzniveaus bei der Übertragung personenbezogener Daten in Gebiete außerhalb der EU. Die berechtigten Interessen der Nutzer ohne strafrechtlichen Hintergrund können so gewichtig gewesen sein, dass sie ohne weiteres bereit waren, die vergleichsweise hohen, angesichts des technischen Aufwands aber auch nicht offensichtlich übersetzten Kosten für die Anschaffung und laufende Nutzung der EncroChat-Telefone zu akzeptieren. Auch unabhängig davon können die Preise der Telefone keinen Tatverdacht begründen. Diese liegen keinesfalls in einem typischerweise nur durch Straftaten zu erwirtschaftendem Bereich und entfernen sich nicht wesentlich von den Preisen für handelsübliche Mobiltelefone der Oberklasse, die ebenfalls weit über 1.000 € liegen können.

(d) Soweit sich im Verlauf der Maßnahme Anhaltspunkte dafür ergeben haben, dass die Betreiber den EncroChat-Dienst gezielt auf die Zielgruppe krimineller Nutzer zugeschnitten hatten und dass sie die Händler mit Tipps zum Schutz vor der Polizei unterstützten, um die Taten zu fördern (vgl. dazu *OLG Hamburg* a.a.O. Rn. 91; Antrag der französischen StA v. 29.04.2020, S. 4), mag dies Zwangsmaßnahmen gegen die Betreiber rechtfertigen, ist aber ebenfalls ungeeignet, einen Verdacht gegen den individuellen Nutzer zu begründen.

Es gibt keine Anhaltspunkte dafür, dass kriminelle Aktivitäten Voraussetzung für die Nutzung des Dienstes gewesen wären oder diese auch nur wesentlich erleichtert hätten. Konkrete Anhaltspunkte für ein »kriminelles Netzwerk« in dem Sinne, dass alle oder zumindest ein sehr großer Teil der Nutzer miteinander in Verbindung gestanden hätten, sind ebenfalls nicht bekannt geworden; angesichts der hohen Zahl von über 60.000 registrierten Nutzern erscheint dies auch nahezu ausgeschlossen. Insofern lässt sich nicht annehmen, dass allen oder nur dem ganz überwiegenden Teil der Nutzer eine etwaige kriminelle Zielsetzung der Betreiber bekannt war.

Etwas anderes folgt auch nicht daraus, dass Hinweise darauf gefunden worden sein sollen, dass die Telefone von den Händlern nur an ausgewählte Personen abgegeben wurden (vgl. den – gegen Ende der Maßnahme erlassenen – Beschl. der Untersuchungsrichterin v. 10.06.2020, S. 3). Es ist schon nicht ersichtlich, zu welchem Zeitpunkt diese Hinweise erlangt wurden, worauf diese sich gründen und nach welchen Kriterien die Käufer ausgewählt worden sein sollen; in dem Antrag der französischen StA v. 29.01.2020 (S 3 f.) hieß es noch, die Telefone seien im Internet bei Ebay angeboten worden. Jedenfalls spricht auch insoweit die sehr hohe Zahl von Nutzern dafür, dass die Vorgaben an die Händler nicht sehr eng gewesen sein können. Nach dem im Beschl. des *OLG Bremen* (a.a.O. Rn. 13) zitierten Vermerk des BKA v. 02.10.2020 sollen die Kunden per E-Mail an den Händler herangetreten sein, der sich dann mit ihnen anonym in Verbindung gesetzt und das Geschäft anonym gegen Barzahlung an öffentlichen Orten abgewickelt habe. Diese Vorgehensweise passt zu den von EncroChat für sich in Anspruch genommenen besonders hohen Sicherheitsstandards und einem entsprechenden besonders ausgeprägten Sicherheitsbedürfnis der Kunden, lässt aber keinen Rückschluss auf strafbare Nutzungszwecke zu.

(e) Bei den in den Beschl. genannten Ermittlungsverfahren aus den Jahren 2017/2018, in denen die. Nutzung von EncroChat-Handys festgestellt wurde, sowie den auf dem Server beschlagnahmten und entschlüsselten Memos mutmaßlicher Drogenverkäufer handelte es sich nicht um eine »Vielzahl« (so *OLG Hamburg* a.a.O. Rn. 91), sondern um eine geringe Zahl von Einzelfällen im untersten zweistelligen Bereich, die keinen Schluss auf sämtliche übrigen Nutzer rechtfertigte.

Auch während des Laufs der Überwachungsmaßnahme hat sich die Verdachtslage insoweit nicht entscheidend konkretisiert. Bei den französischen Nutzern belief sich der mutmaßlich kriminelle Anteil zuletzt auf lediglich 67,3%; die absolute Zahl von 317 war im Vergleich zur Gesamtzahl von über 60.000 bei EncroChat eingetragenen bzw. über 30.000 ausgespähten Personen verschwindend gering. Welche Erkenntnisse sich im Laufe der Maßnahme zum Anteil mutmaßlich krimineller Nutzer außerhalb Frankreichs ergeben haben, lässt sich den französischen Unterlagen nicht entnehmen.

Eine andere Beurteilung ist auch nicht mit Blick auf die durch die Maßnahme ermöglichten europaweiten Ermittlungserfolge geboten.

Spätere Erkenntnisse, insb. solche aus der Überwachungsmaßnahme selbst, haben bei der Beurteilung des Tatverdachts außer Betracht zu bleiben; ob ein solcher begründet war, ist allein auf der Grundlage des Ermittlungsstandes zum Zeitpunkt der Anordnung zu beurteilen (*BGH* NStZ 1995, 510 [511]). Zudem sind die Erfolge – so spektakulär etwa die großen sichergestellten Drogenmengen oder der in den Niederlanden entdeckte »Folter-Container« auch anmuten mögen – selbst rückblickend nicht geeignet, die Vermutung eines vollständig oder zumindest zum ganz überwiegenden Teil kriminellen Nutzerkreises zu bestätigen. Nach einer Mitteilung der Europäischen Kommission v. 14.04.2021 (COM/2021/170, abrufbar bei juris) waren bis zu diesem Zeitpunkt, d.h. fast ein Jahr nach Beendigung der Maßnahme, insg. nur 1500 Ermittlungsverfahren eingeleitet und 1800 Personen (entspricht 2,72% der Gesamtnutzer bzw. 5,54% der überwachten Nutzer) festgenommen worden.

(3) Die Datenerhebung auf den deutschen Endgeräten lässt sich auch dann nicht rechtfertigen, wenn man sie nicht als Strafverfolgungsmaßnahme i.e.S. begreift, sondern dem Vorfeld der Strafverfolgung zuordnet.

Eine TKÜ im Vorfeld der Strafverfolgung mit dem Ziel, »auf Vorrat« Beweise für künftige, noch ungewisse Strafverfahren zu sammeln oder damit einen konkreten Anfangsverdacht erst zu begründen, ist im deutschen Recht bisher nicht vorgesehen. Der deutsche Gesetzgeber könnte eine solche Maßnahme von Verfassungs wegen auch nur in sehr engen Grenzen einführen. Es wäre widersprüchlich, wenn die TKÜ im noch ungewissen Vorfeld einer Tat unter geringeren rechtsstaatliehen Anforderungen möglich wäre als dann, wenn der Täter schon konkret zur Rechtsgutverletzung. angesetzt hat (*BVerfG*, Urt. v. 27.07.2005 – 1 BvR 668/04, juris Rn. 114 [= StV 2007, 226 [Ls]]).

Unverzichtbar wären auch insoweit hinreichende tatsächliche Grundlagen, die die Annahme einer das Schutzgut gefährdenden Handlung der Endgerätenutzer rechtfertigen. Auch wenn mit zunehmendem Gewicht des betroffenen Rechtsguts die Anforderungen an den Wahrscheinlichkeitsgrad sinken, so bedürfte es doch stets eines konkret umrissenen Ausgangspunktes im Tatsächlichen (*BVerfG* a.a.O. Rn. 150 f.). Erhöhte Anforderungen würden sich zudem auch insoweit für die besonders schwerwiegenden Eingriffe der Online-Durchsuchung bzw. Quellen-TKÜ ergeben.

Die hier gegebenen Umstände, die über vage Vermutungen und »diffuse Anhaltspunkte« (vgl. *BVerfG* a.a.O. Rn. 123) nicht hinausgehen, genügen auch insoweit nicht, um eine flächendeckende Ausspähung sämtlicher Teilnehmer des Chatdienstes zu rechtfertigen.

(4) Die Überwachung der Nutzer ließe sich schließlich selbst dann nicht rechtfertigen, wenn man lediglich die EncroChat-Betreiber als Besch. und die Nutzer als »Dritte« einordnen würde. Nach § 100a Abs. 3 S. 2 StPO wäre dann zwar ein Tatverdacht gegen die Nutzer entbehrlich. Die Vorschrift stellt aber weitere – wiederum durch bestimmte Tatsachen zu belegenden – Anforderungen an den zu überwachenden Personenkreis. Ebenso wie beim Tatverdacht gegen den Besch. können auch hier vage Anhaltspunkte nicht ausreichen (MeyerGoßner/Schmitt-StPO/*Köhler*, 64. Aufl. 2021, Rn. 100a Rn. 18).

Solche bestimmten Tatsachen liegen hier nicht vor. Die EncroChat-Betreiber benutzten nicht die informationstechnischen Systeme der Endgerätenutzer; vielmehr nutzen diese umgekehrt das System von EncroChat. Die Chat-Nachrichten, auf deren Ausleitung die Maßnahme abzielte, wurden ausschließlich unter den Nutzern gewechselt; darauf war das System gerade ausgerichtet.

Hinweise darauf, dass die Nutzer auch Mitteilungen von den EncroChat-Betreibern oder für diese entgegennahmen oder weitergaben, gibt es nicht. Insb. sind keine konkreten Anhaltspunkte dafür bekannt geworden, dass die EncroChat-Betreiber sämtliche anonymen Nutzer mit Tipps für die Begehung von Straftaten unterstützten. Vorrangig wäre dann auch als mildere Maßnahme zu versuchen gewesen, diese Nachrichten direkt auf dem EncroChat-Server abzufangen. Es ist nicht ersichtlich, dass insoweit nur der Zugriff auf die Endgeräte erfolgversprechend gewesen wäre. Es ist schon zweifelhaft, ob eine etwaige Kommunikation der EncroChat-Betreiber mit ihren Nutzern genauso verschlüsselt gewesen wäre wie die Nachrichten der Nutzer untereinander; zudem wäre dann auch der Server als »Quelle« in Betracht gekommen, an der die Nachrichten vor dem Verschlüsseln hätten abgefangen werden können. Jedenfalls aber wäre für den Fall, dass die Maßnahme nur auf die Kommunikation zwischen den Betreibern und den Nutzern gerichtet gewesen wäre, das Auslesen der kompletten Kommunikation auf den Endgeräten; d.h. auch der unter den Nutzern gewechselten Nachrichten, überschießend und unverhältnismäßig gewesen.

bb) *§§ 100a, 100b StPO als Prüfungsmaßstab*. Die Voraussetzungen der bei einem vergleichbaren innerstaatlichen Sachverhalt zu beachtenden §§ 100a, 100b StPO sind i.R.d. hier zu treffenden Entscheidung über die Verwertung der Chat-Nachrichten in vollem Umfang zu prüfen.

Allerdings unterliegen TKÜ-Maßnahmen eines ausländischen Hoheitsträgers, die von diesem originär durchgeführt – d.h. nicht erst durch ein deutsches Rechtshilfeersuchen veranlasst – und von einem ausländischen Gericht genehmigt wurden, regelmäßig nur einer eingeschränkten Rechtmäßigkeitskontrolle. Der europarechtliche Grundsatz der gegenseitigen Anerkennung gerichtlicher Entscheidungen und die völkerrechtlich gebotene Achtung der Souveränität des anderen Staates verbieten es, die Maßnahme umfassend am Maßstab des ausländischen Rechts zu überprüfen (*BGH* v. 21.11.2012 – 1 StR 310/12, juris Rn. 33 f. [= StV 2014, 193]). Danach wäre es grds. unzulässig, die Unverwertbarkeit der Maßnahme im deutschen Strafverfahren damit zu begründen, dass die Voraussetzungen der französischen Eingriffsnorm Art. 706-102-1 CPP entgegen der Einschätzung der französischen Gerichte nicht gegeben gewesen seien. Ebenso kann·nicht mit Blick auf den deutschen Richtervorbehalt beanstandet werden, dass die Maßnahme »nur« von einem französischen Gericht angeordnet wurde.

Etwas anderes gilt hier aber hinsichtlich der Anforderungen, die das deutsche Strafprozessrecht an die Durchführung derartiger Überwachungsmaßnahmen stellt. Deren Beachtung ist hier in vollem Umfang zu überprüfen. Soweit die bisher zu den EncroChat-Daten ergangenen Entscheidungen die Prüfung auf die Einhaltung rechtsstaatlicher Mindeststandards beschränken wollen (*OLG Hamburg* a.a.O. Rn. 77 ff., 81f.; *OLG Bremen* a.a.O. Rn 35; ähnlich *OLG Bremen* a.a.O. Rn. 20 f.; zust. *OLG Rostock* v: 23.03.2021 – 20 Ws 70/21, juris Rn. 11), ist dem nicht zu folgen.

Der Fall liegt hier insb. anders als in dem in diesem Zshg. häufig zitierten Beschl. des *BGH* v. 21.11.2012 – 1 StR 310/12 (juris). Dort ging es um die Verwertung von Erkenntnissen aus einer

tschechischen Telefonüberwachung, deren Rechtmäßigkeit der *BGH* am Maßstab des Rechtshilferechts und i.Ü. nur auf die Verletzung völkerrechtlich verbindlicher individualschützender Garantien sowie des ordre public (§ 73 IRG) überprüfte (a.a.O., juris Rn. 38). Im Unterschied zum hiesigen Fall waren die Telekommunikationsdaten dort jedoch auf tschechischem Staatsgebiet, d.h. dem Gebiet des Anordnungsstaates erhoben worden. Die Richtlinie 2014/41/EU und die zu ihrer Umsetzung erlassenen §§ 91a ff. IRG waren damals noch nicht in Kraft, und insb. Art. 31 RiLi-EEA wäre – da es sich nicht um eine transnationale Maßnahme handelte – auch nicht einschlägig gewesen. Für die hier einschlägige Konstellation einer französischen TKÜ auf deutschem Staatsgebiet zielt Art. 31 RiLi-EEA aber gerade auf die Überprüfung am Maßstab des deutschen Strafprozessrechts ab. Die Einschätzung des französischen Gerichts nach französischem Recht soll danach gerade keinen Vorrang vor den möglicherweis abweichenden Vorstellungen des deutschen Rechts haben. Der das Rechtshilferecht ansonsten beherrschende Grundsatz der gegenseitigen Anerkennung von Entscheidungen wird für den Bereich der TKÜ eingeschränkt; die Gestaltung der Maßnahme durch den französischen Staat nach dessen eigenem Willen lässt (entgegen *OLG Hamburg* a.a.O. Rn. 79) die grundrechtliche Verantwortlichkeit der deutschen öffentlichen Gewalt in diesem Fall gerade nicht entfallen.

Aus der Richtlinie ergibt sich auch nicht, dass die Überprüfung im Unterrichtungsverfahren nach Art. 31 RiLi-EEA abschließenden Charakter haben und eine spätere Prüfung am Maßstab des deutschen Rechts bei einer Verwendung der Erkenntnisse im deutschen Strafverfahren unzulässig sein soll. Eine »Sperrwirkung« des Unterrichtungsverfahrens kann es hier schon deshalb nicht geben, weil die Unterrichtung unterlassen wurde und die Überprüfung nach Art. 31 Abs. 3 RiLi EEA deshalb nicht stattgefunden hat. Selbst wenn aber Art. 31 RiLi-EEA hier beachtet worden wäre, wäre eine erneute Überprüfung nach deutschem Prozessrecht bei der Verwendung im deutschen Strafverfahren zulässig und geboten. Soweit das Verfahren nach Art. 31 RiLi-EEA Rechtssicherheit über die Verwendbarkeit der Daten schaffen soll, gilt dies allein für die Verwendung in Frankreich. Gerade vor dem Hintergrund, dass die Prüfung nach Art. 31 RiLi-EEA im Beschleunigungsinteresse an eine sehr kurze Frist gebunden ist und daher nur summarisch erfolgen kann, wird eine erneute Prüfung im deutschen Strafverfahren auf einer dann möglicherweise sogar breiteren Tatsachengrundlage dem individualschützenden Anliegen der Richtlinie in besonderem Maße gerecht.

Hinzu kommt, dass die französische Maßnahme von Beginn an darauf abzielte, die Strafverfolgung der ausländischen Nutzer in deren Heimatländern zu ermöglichen. So wurden die ausgeleiteten Daten laufend und sehr zeitnah – und damit offensichtlich ohne eine vorherige inhaltliche Auswertung durch die französischen Behörden – den entsprechenden nationalen Strafverfolgungsbehörden übermittelt. Auch wenn man darin kein der Umgehung dienendes »Befugnis-Shopping« sieht, verstärkt ein solches Vorgehen das Bedürfnis nach einer Kontrolle am Maßstab des deutschen Rechts.

c) *Hilfsweise: Beschränkter Prüfungsmaßstab*. Die Maßnahme erwiese sich aber selbst dann als rechtswidrig, wenn man sie (wie etwa das *OLG Hamburg* a.a.O. Rn. 81) nur auf die Einhaltung rechtsstaatlicher Mindeststandards überprüfen wollte. Denn das Erfordernis eines konkreten Tatverdachts ist eine solche unverzichtbare grundlegende Wertentscheidung des deutschen Rechts.

Eine anlasslose TKÜ ist dem deutschen Recht grds. fremd. Abgesehen von dem hier nicht einschlägigen Sonderfall der strategischen Auslandsüberwachung durch den BND als Behörde ohne operative Befugnisse (vgl. dazu *BVerfG*, Beschl. v. 19.05.2020 – 1 BvR 2835/17, juris Rn. 166) ist in allen denkbaren Konstellationen sowohl im präventiven wie im repressiven Bereich stets ein konkreter, durch Tatsachen belegter Anlass von erhöhtem Gewicht erforderlich. Besonders hoch sind die Anforderungen bei der heimlichen Infiltration eines informationstechnischen Systems, durch die die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können (vgl. – zur Gefahrenabwehr – *BVerfG*, Urt. v. 27.02.2008 – 1 BvR 370/07 – »Online-Durchsuchung«, juris Rn. 245 ff. [= StV 2008, 169 [Ls]]). Das gilt umso mehr, wenn eine große Zahl von Personen von der Maßnahme betroffen sind, es um sich um personenbezogene Daten mit jedenfalls nicht von vornherein ausschließbarem Bezug zur privaten Lebensführung handelt und die Betroffenen dem Eingriff in einer Situation vermeintlicher besonderer Vertraulichkeit ausgesetzt sind (vgl. *BVerfG*, Urt. v. 27.07.2005 – 1 BvR 668/04, juris Rn. 138 ff. [= StV 2007, 226 [Ls]]; vgl. auch *BVerfG*, Urt. v. 27.02.2008 – 1 BvR 370/07 – »Online-Durchsuchung«, juris Rn. 231 [= StV 2008, 169 [Ls]]).

Die hier durchgeführte Überwachung von über 30.000 Personen, über die außer der Nutzung des EncroChat-Dienstes nichts bekannt war, ist mit diesen Vorgaben und i.Ü. auch mit dem Grundsatz der Verhältnismäßigkeit i.e.S. nicht vereinbar.

3. *Verwertungsverbot*. Aus dem Vorstehenden ergibt sich ein Verwertungsverbot.

Eine rechtswidrige Beweiserhebung zieht nicht in jedem Fall ein Beweisverwertungsverbot nach sich. Ein (ungeschriebenes) Verwertungsverbot kann vielmehr nur ausnahmsweise nach einer Abwägung aller Umstände eingreifen und setzt einen besonders schwerwiegenden Rechtsverstoß voraus. Es müssen übergeordnete wichtige Gründe im Einzelfall vorliegen, die das staatliche Interesse an der Wahrheitsermittlung und die Belange einer funktionstüchtigen Strafrechtspflege überwiegen (*BGH* v. 03.05.2018 – 3 StR 390/17, juris Rn. 24 m.w.N.).

a) *Missachtung von Art. 31 RiLi-EEA, § 91g Abs. 6 IRG*. Die Unverwertbarkeit ergibt sich bereits aus der Missachtung der rechtshilferechtlichen Unterrichtungspflicht Diese ist so gewichtig, dass sie das staatliche Interesse an der Strafverfolgung überwiegt.

aa) Art. 31 RiLi-EEA und die dessen Umsetzung dienenden Regelungen im Gesetz über die internationale Rechtshilfe in Strafsachen (IRG) zielen unmittelbar auf den Schutz der Grundrechte der Betroffenen ab (vgl. zum individualschützenden Charakter als Voraussetzung für ein Verwertungsverbot *BGH* v. 21.11.2012 –1 StR 310/12, juris Rn. 25 [= StV 2014, 193]). Es handelt sich um. Sonderregelungen für die transnationale TKÜ, die mit Blick auf deren hohe Grundrechtssensibilität sicherstellen sollen, dass die nationalen Schutzniveaus sowohl des Anordnungs- wie des Vollstreckungsstaates nicht unterschritten werden (*Wörner*, in: Ambos/König/Rackow, Rechtshilferecht in Strafsachen, 2. Aufl. 2020, Rn. 439). ln der Gesetzesbegründung (RegE, BR-Drs. 421/16 v. 12.08.2016, S. 83, bei juris) heißt es dazu, § 91g Abs. 6 IRG bezwecke neben dem Schutz der deut-

schen Staatssouveränität auch den Schutz der Grundrechte der Betroffenen. Der Gesetzgeber wollte dem Risiko begegnen, dass sensible Daten aus nach deutschem Recht unzulässigen TKÜ von den ausländischen Behörden verwendet werden können. Wegen der besonderen Bedeutung des Widerspruchsverfahrens hat der deutsche Gesetzgeber den Widerspruch nach § 91g Abs. 6 IRG – anders als Art. 31 Abs. 3 RiLi-EEA, der nur eine Genehmigungsfiktion nach Ablauf von 96 Std. vorsieht – als Verpflichtung ausgestaltet (RegE a.a.O.).

Bei der Unterrichtung nach § 91g IRG, Art. 31 RiLi-EEA und dem daran anknüpfenden Widerspruchsverfahren handelt es sich somit keinesfalls um eine notfalls verzichtbare bloße Formalie, sondern um einen wesentlichen Verfahrensschritt, der unmittelbar auf Sicherung der Rechtsstaatlichkeit der Ermittlungen abzielt. Erschwerend kommt hinzu, dass die Voraussetzungen für eine derartige Maßnahme nach nationalem Recht mangels konkreten Tatverdachts nicht vorlagen.

Wäre die Unterrichtung wie vorgeschrieben unter Erläuterung der Verdachtslage erteilt und das daraufhin gesetzlich vorgesehene Widerspruchsverfahren eingehalten worden, hätte die zuständige deutsche Stelle der Maßnahme widersprochen, und es wäre zu der Datenerhebung auf den Endgeräten der deutschen Nutzer einschließlich des Angesch. nicht gekommen. Dass ein erheblicher Teil der Endgeräte auf deutschem Staatsgebiet genutzt wurde, war den französischen Behörden schon vor dem ersten richterlichen Genehmigungsbeschl. v. 30.01.2020 bekannt (vgl. etwa den Antrag der StA v. 29.01.2020, S. 8).

Die nach Art. 31 Abs. 1 RiLi-EEA gebotene Unterrichtung und die an eine kurze Frist gebundene deutsche Reaktion darauf wären noch deutlich vor dem Beginn der Überwachung erfolgt mit dem Ergebnis, dass die deutschen Nutzer von der Maßnahme hätten ausgenommen werden müssen.

Es wäre widersprüchlich, wenn die zuständige deutsche Stelle i.R.d. Unterrichtungsverfahrens nach § 91g Abs. 6 IRG zur Untersagung der Datenerhebung in Frankreich verpflichtet gewesen wäre, aber gleichwohl die unter Verstoß gegen diese Vorschrift gewonnenen Daten dann von einem deutschen Strafgericht verwertet werden dürften. Dabei ist auch zu berücksichtigen, dass die französische Maßnahme, wie dargelegt, von Beginn an die Strafverfolgung der ausländischen Nutzer in deren Heimatländern ermöglichen sollte. Da somit die Interessen des deutschen Staates durch die Maßnahme erkennbar in besonderem Maße betroffen waren, kam den auf die Einhaltung der nationalen Schutzstandards gerichteten europäischen Verfahrensregeln eine besondere Bedeutung zu.

Unerheblich ist es in diesem Zshg., dass die deutschen Ermittlungsbehörden durch die EEA und die Einleitung von Strafverfahren zum Ausdruck gebracht haben, die Maßnahme nicht zu beanstanden. Dieses Verhalten begründet keine Heilung des Rechtsfehlers und kommt ihr auch nicht »zumindest nahe« (so aber *OLG Hamburg* a.a.O. Rn. 105) oder gar »gleich« (*OLG Schleswig* a.a.O. Rn. 25; zust. *OLG Rostock* v. 11.05.2021 – 20 Ws 121/21, BeckRS 2021, 11981 Rn. 19 f.). Die GStA Frankfurt/M. und die mit den Trennverfahren befassten lokalen StA waren für eine solche Entscheidung nicht zuständig (§ 92d Abs. 1 Nr. 1 IRG). Die von Konkreten Verwertungsinteressen motivierte Anforderung und Entgegennahme der Daten bot auch nicht die Gewähr für die vom Gesetzgeber beabsichtigte kritische und unabhängige rechtliche Prüfung.

bb) Der Verstoß gegen Art. 31 RiLi-EEA ist danach so gewichtig, dass er das staatliche Strafverfolgungsinteresse überwiegt (a.A. *OLG Schleswig* a.a.O. Rn. 38). Allerdings ist das Gewicht der dem Angesch. hier zur Last gelegten Taten hoch. Dies ist jedoch in den Fällen, in denen sich die Frage der Verwertbarkeit von Telekommunikationsdaten überhaupt stellt, regelmäßig der Fall. Dem hohen Gewicht der Taten steht zudem ein ebenfalls hohes Gewicht der betroffenen Grundrechte und eine besondere Schwere des Eingriffs entgegen. Der Einhaltung der individualschützenden Verfahrensregeln kommt danach eine überragende Bedeutung zu, der ggü. die Erfordernisse der Strafrechtspflege nicht überwiegen.

b) *Fehlender qualifizierter Tatverdacht*. Unabhängig davon begründet das Fehlen eines qualifizierten Tatverdachts auch für sich gesehen die Unverwertbarkeit der Chat-Daten.

Im Fall der TKÜ sind ein Verwertungsverbot auslösende übergeordnete wichtige Gründe anzunehmen, wenn wesentliche sachliche Voraussetzungen für die Anordnung der Überwachungsmaßnahme fehlen (*BGH*, Beschl. v. 07.03.2006 – 1 StR 316/05, juris Rn. 7 m.w.N.; v. 01.08.2002 – 3 StR 122/02, juris Rn. 10). Das gilt erst recht, wenn es sich bei der Maßnahme um den besonders intensiven Eingriff der heimlichen Online-Durchsuchung bzw. Quellen-TKÜ handelt.

aa) Der konkrete Tatverdacht ist eine grundlegende Voraussetzung, ohne die die Maßnahme nach deutschem Rechtsverständnis als objektiv nicht mehr rechtsstaatlich angesehen werden kann.

Etwas anderes ergibt sich auch nicht dann, wenn man dem mit der Anordnung befassten Gericht bei der Beurteilung des Tatverdachts einen Beurteilungsspielraum zugesteht und die Unverwertbarkeit nur dann annimmt, wenn die Entscheidung diesen Spielraum überschreitet (*BGH* v. 01.08.2002 – 3 StR 122/20, juris Rn. 10; NStZ 1995, 510 [511] m. abl. Anm. *Bernsmann*). Dabei kann offenbleiben, ob dieser Grundsatz sich überhaupt auf die von einem ausländischen Recht nach den dortigen Vorschriften getroffene Entscheidung übertragen lässt. Denn die französischen Gerichtsentscheidungen, die offenbar maßgeblich EncroChat als »Gesamtsystem« im Blick hatten und auf individuelle Verdachtsmomente gegen die Nutzer nicht eingehen, haben jedenfalls von einem derartigen Entscheidungsspielraum keinen Gebrauch gemacht. Inwieweit dies an abweichenden Voraussetzungen des französischen Prozessrechts liegt, das etwa in der Phase der Voruntersuchung an die Verdachtsmomente generell nur geringe Anforderungen stellt und schon eine Vermutung ausreichen lässt (vgl. dazu *Knytel*, Die Europäische Ermittlungsanordnung und ihre Umsetzung in die deutsche und französische Rechtsordnung, Diss. Strasbourg/Freiburg 2019, S. 134), mag dahinstehen. Die französischen Beschl. enthalten jedenfalls keine auf die Nutzer bezogenen Verdachts- und Verhältnismäßigkeitserwägungen, die einer umfassenden Überprüfung und der Annahme eines Verwertungsverbotes im hiesigen Strafverfahren entgegenstehen könnten.

bb) Der fehlende Tatverdacht erweist sich i.R.d. Abwägung nicht etwa deshalb als weniger gewichtig, weil die Durchführung der Maßnahme allein in der Verantwortung des französischen Staates lag und von den deutschen Behörden nicht zu beeinflussen war.

Der Fall ist insb. nicht vergleichbar mit den Schweizer Steuer-CDs, für deren Verwertbarkeit zulässigerweise darauf abgestellt wurde, dass diese nicht durch die staatlichen Strafverfolgungsbe-

hörden, sondern durch Private erlangt worden seien (vgl. *BVerfG* v. 09.11.2010 – 2 BvR 2101/09, juris Rn. 58 [= StV 2011, 65]). Hier wurden die Daten durch eine – wenn auch ausländische – staatliche Maßnahme erlangt. Die deutschen Behörden waren zudem von Beginn an in die Maßnahme eingebunden, indem sie durch die laufende Entgegennahme der Daten zugleich ein eigenes Interesse an der Fortsetzung der Maßnahme bekundet haben. Auch darin unterscheidet sich der Fall etwa von dem der Steuer-CDs, die von dem Privaten ohne jedes staatliche Zutun beschafft und allein auf dessen Veranlassung den Behörden angeboten worden waren (vgl. dazu *BVerfG* a.a.O. Rn. 59). Auch wenn man in der hier gewählten Vorgehensweise kein der Umgehung nationaler Schutzvorschriften dienendes »Befugnis-Shopping« sieht, begründet dies doch eine stärkere Verantwortlichkeit des deutschen Staates, als dies bei einer ausschließlich in ausländischer Verantwortung durchgeführten Maßnahme der Fall wäre.

cc) Auch das hohe Gewicht der hier in Rede stehenden Straftaten kann zu keiner anderen Entscheidung führen. Die besondere Schwere der aufzuklärenden Taten ist ohnehin Tatbestandsvoraussetzung für Maßnahmen nach §§ 100a, 100b StPO. Dass die Überwachungsmaßnahme auf Katalogtaten abzielte und im Nachhinein auch Belege für solche Taten erbracht hat, kann das Fehlen eines konkreten Tatverdachts als weitere Tatbestandsvoraussetzung nicht ausgleichen. Selbst die Vermutung schwerster Taten wäre nicht geeignet, die fehlende Konkretisierung von Verdachtstatsachen zu kompensieren (vgl. *BVerfG*, Urt. v. 27.07.2005 – 1 BvR 668/04, juris Rn. 130 [= StV 2007, 226]). Würde man das anders sehen, würde die für den Grundrechtsschutz überragend wichtige Voraussetzung des konkreten Verdachts praktisch leerlaufen; dies wäre dann eine vom deutschen Gesetzgeber nicht gewollte »Strafverfolgung um jeden Preis«.

Soweit also das *OLG Hamburg* (a.a.O. Rn. 98) meint, die »hochwahrscheinlich begangenen« schweren Straftaten des dortigen Bf. hätten »jedenfalls zielgerichtet erforscht« werden müssen, kann dies über die offensichtliche Missachtung rechtsstaatlicher Mindestanforderungen nicht hinweghelfen. Die massenhafte Ausspähung von Telefonen ohne konkreten Tatverdacht entfernt sich so weit von grundlegenden Gerechtigkeitsvorstellungen des deutschen Rechts, dass die Verwertung in einem rechtsstaatliehen Verfahren ausscheidet.

c) *Hilfsweise: Nutzer sind keine Nachrichtenmittler*. Ein Verwertungsverbot besteht schließlich auch dann, wenn man die Nutzer nicht als Besch., sondern als Dritte ansieht Die Rechtswidrigkeit der Maßnahme nach dem Maßstab des deutschen Rechts ergibt sich dann aus § 100a Abs. 3 S. 2 StPO, weil die dort vorausgesetzte Verbindung zu den beschuldigten EncroChat-Betreibern nicht durch bestimmte Tatsachen belegt wird. Da das Gewicht der betroffenen Grundrechte und die Schwere des Eingriffs nicht anders sind als bei einer Maßnahme gegen den Besch., kann die Abwägung hier nicht anders ausgehen. Dem Erfordernis bestimmter Tatsachen in § 100a Abs. 3 S. 2 StPO kommt die gleiche grundrechtssichernde Funktion zu wie bei einer Maßnahme gegen den Besch. Die Anforderungen an die Verhältnismäßigkeit sind noch höher als bei diesem (vgl. die Nachweise bei Meyer-Goßner-Schmitt-StPO/*Köhler*, a.a.O., § 100 Rn. 18.), und die Schwere der Tat und die Effektivität der Strafverfolgung können bei einem Nichtverdächtigen auch nur mit verringertem Gewicht in die Abwägung eingestellt werden.

4. *§§ 100e Abs. 5, 479 Abs. 2 StPO*. Die Verwertbarkeit der Daten lässt sich schließlich auch nicht auf eine entsprechende Anwendung von § 100e Abs. 6 StPO (für die Online-Durchsuchung) bzw. § 479 Abs. 2 StPO (für die Quellen-TKÜ) stützen.

Diese Vorschriften regeln lediglich die Weiterverwendung der Daten in anderen Verfahren. Sie setzen deren Verwertbarkeit voraus; diese richtet sich nach den oben dargelegten allgemeinen Grundsätzen (vgl. *Köhler*, a.a.O. § 100e Rn. 21, § 479 Rn. 9). §§ 100e Abs. 6, 479 Abs. 2 StPO sind i.Ü. auch nicht einschlägig. Es handelt sich bei den auf dem Telefon des Angesch. abgeschöpften Daten nicht um »Zufallsfunde« aus einem anderen Verfahren (a.A. *OLG Hamburg* a.a.O. Rn. 59; *OLG Schleswig* a.a.O. Rn. 30; *OLG Rostock* v. 11.05.2021 – 20 Ws 121/21, BeckRS 2021, 11981 Rn. 19 f.); deren Verwendung im hiesigen Strafverfahren wäre keine »Zweckumwidmung« (vgl. dazu *Köhler*, a.a.O. § 479 Rn. 3). Der Schwerpunkt der Maßnahme lag hier nicht etwa (worauf *OLG Hamburg* a.a.O. Rn. 68 abstellt) auf der Umleitung von Datenströmen aus dem von dem Unternehmen EncroChat betriebenen Server, sondern auf dem Zugriff auf die Endgeräte. Aus den französischen Anträgen und Beschl. ergibt sich eindeutig, dass die Entschlüsselung auf dem Server nicht möglich war. Dies war gerade der Grund, dass die Ermittlungsbehörden den Zugriff auf die Endgeräte für erforderlich hielten. Anlasstaten waren dabei – neben dem Vorwurf der kriminellen Vereinigung – sämtliche Straftaten der Nutzer (begrenzt auf bestimmte Delikte, namentlich aus dem Btm-Bereich), auf die sich Hinweise in den ausgeleiteten Chatnachrichten ergaben mithin auch die hier angeklagten Taten des Angesch.

Die Maßnahme war zudem, wie dargelegt, von Beginn darauf gerichtet, die Strafverfolgung der ausländischen Nutzer in deren Heimatländern zu ermöglichen. Das von der GStA Frankfurt/M. eingeleitete Ermittlungsverfahren […], bei dem zunächst die Deliktsbezeichnungen des französischen Verfahrens übernommen wurden, und die daraus entstandenen Trennverfahren der örtlichen StA gegen die einzelnen Besch. – darunter auch den Angesch. – stellen sich insoweit nicht als »andere Verfahren« dar, sondern als Fortführung des französischen Verfahrens dies wäre bei einem rein nationalen Sachverhalt mit einer Abtrennung und Abgabe des Verfahrens vergleichbar.

5. *Keine besseren Erkenntnismöglichkeiten in der Hauptverhandlung*. Die Voraussetzungen für eine Eröffnung des Hauptverfahrens liegen damit nicht vor. Es ist auch nicht zu erwarten, dass die Hauptverhandlung insoweit noch maßgeblich andere Erkenntnisse erbringen wird. Insb. ist nicht ersichtlich, dass die Erkenntnismöglichkeiten in der Hauptverhandlung denen im Zwischenverfahren wesentlich überlegen wären. Auch in der Hauptverhandlung wäre die Frage der Verwertbarkeit im Wesentlichen auf der Grundlage der schon in der Akte vorhandenen Unterlagen zu prüfen. Soweit Zeugen – etwa Beamte des BKA – zu vernehmen wären, stehen vorrangig der Hauptverhandlung zu überlassene Fragen des persönlichen Eindrucks und der Glaubhaftigkeit der Aussagen jedenfalls nach dem jetzigen Stand nicht im Vordergrund.

Neue Beweismittel, die insb. zur hier zentralen Frage des Tatverdachtes vor Beginn der Überwachung noch abweichende Erkenntnisse erbringen könnten, sind nicht ersichtlich. Das BKA hat zudem auf Nachfrage der *Kammer* mitgeteilt, dass dort keine weiteren Informationen zu den französischen Maßnahmen vorlägen und die französischen Behörden zur Erteilung weiterer Auskünfte nicht bereit seien. Insofern verspräche auch die Vernehmung der französischen Ermittler keinen Erfolg und es drängen sich auch keine sonstigen Ermittlungsschritte auf, die die *Kammer* im Zwischenverfahren hätte ergreifen können. […]

Mitgeteilt von RA *André Miegel*, Duisburg.

Anm. d. Red.: Die Entscheidung war bei Redaktionsschluss nicht rechtskräftig.