„Vertrauen ist gut“

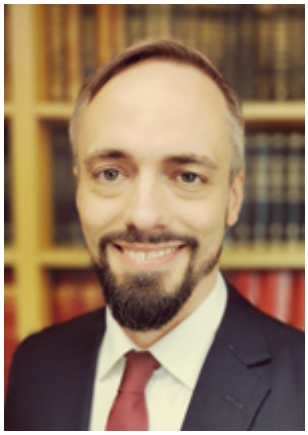
Von der Verwertbarkeit erlangter Daten bezüglich sogenannter Kryptohandys

Von Oberstaatsanwalt Dr. Sören Pansa und Staatsanwalt Dr. Marius Heller, Schleswig/Kiel[1]

1 Einleitung

Im Frühjahr 2020 brandete ein Ruf wie Donnerhall über die Flure der Landeskriminalämter und Staatsanwaltschaften: *„ENCROCHAT“.* Eine genaue Vorstellung, was genau sich dahinter verbarg, dürften die meisten dabei nicht gehabt haben. Aber man hatte viel gehört: Angeblich überwachungssichere Mobiltelefone, welche von Kriminellen genutzt wurden, die jedoch sehr unvorsichtig vorgegangen sein sollen. Hierzu muss gesagt werden, dass bis zu diesem Zeitpunkt Telekommunikationsüberwachungen, insbesondere bezüglich des Betäubungsmittelhandels eher ernüchternd verliefen. Dies resultierte zum einen aus dem typischerweise konspirativen Vorgehen der Beteiligten. Zum anderen aus der bereits seit Längerem zunehmenden Nutzung sog. Messenger-Dienste, welche eine Überwachung stark erschwerten. Hierauf hat der Gesetzgeber am 17. August 2017 durch die Schaffung der *„Online-Durchsuchung“* i.S.d. § 100b StPO und der *„Quellen-Telekommunikationsüberwachung“* i.S.d. § 100a Abs. 1 S. 2 StPO reagiert.[2] Doch bereits die erste oberflächliche Sichtung der Encrochat-Kommunikationsinhalte machte die zuletzt durchwachsene Entwicklung der Telekommunikationsüberwachung schlagartig vergessen. So hatten die Nutzer in vollkommenen Vertrauen auf die Qualität ihrer Mobiltelefone tatsächlich meist nicht nur Betäubungsmittel fotografiert, sondern oftmals auch gleich den Abholer samt Ausweisdokumenten, denn der Verkäufer musste schließlich wissen, wem er die große Tasche in die Hand drücken sollte. Im Anschluss an die Auswertung der Daten folgten in der gesamten Bundesrepublik Deutschland zunächst Vollstreckungen zahlreicher Untersuchungshaftbefehle und anschließend rechtskräftige Verurteilungen zu teils langjährigen Freiheitsstrafen. Daraufhin äußerten sich zahlreiche Strafverteidiger bezüglich der Verwertbarkeit der Daten, welche, wenig überraschend, einhellig abgelehnt wurde.[3] Der 5. Strafsenat des Bundesgerichtshofes hat inzwischen ausführlich zu dem Themenkomplex *„Encrochat“* Stellung genommen.[4] Ein gebührender Anlass, sich nunmehr einen umfassenden Überblick über den gegebenen Sachverhalt und die hiermit verbundenen rechtlichen Probleme zu verschaffen.

2 Sachverhalt



Am 15. Juli 2021 hat das Landgericht Hamburg einen Angeklagten wegen Verstößen gegen das Betäubungsmittelgesetz zu einer Freiheitsstrafe von 5 Jahren verurteilt. Maßgeblich für die Überzeugungsbildung des Landgerichts war dabei die Kommunikation des Angeklagten, welche dieser über das verschlüsselte Nachrichtensystem EncroChat geführt hat. Den in Frankreich durchgeführten Ermittlungsmaßnahmen zur Erlangung der relevanten EncroChat-Kommunikation lag folgender verfahrensrechtlicher Sachverhalt zugrunde:

In den Jahren 2017 und 2018 stellten französische Behörden in mehreren nicht im Zusammenhang stehenden Ermittlungsverfahren – in denen es überwiegend um den Handel mit Betäubungsmitteln im Kilogrammbereich ging – fest, dass die Tatverdächtigen jeweils über sog. Kryptohandys verfügten, die über eine sog. EncroChat-Architektur verschlüsselt waren. Aufgrund der Verschlüsselung war eine Auswertung dieser Mobiltelefone nicht möglich. Nach ersten Ermittlungsergebnissen wurden die Kryptohandys mit folgenden Produktmerkmalen beworben: *„Garantie der Anonymität, personalisierte Android Plattform, doppeltes Betriebssystem, allerneueste Technik, automatische Löschung von Nachrichten (‚Advanced Burn'), schnelles Löschen (‚Panic Wipe'), Unantastbarkeit (‚Tamper Proofing'), Kryptografie-Hardwaremodul".* Folgende Anwendungen waren auf dieser Art von Telefonen verfügbar: *„EncroChat (Instant-Secure Messaging Kunde), EncroTalk (Chiffrierung der Sprachkonversationen auf IP), EncroNotes (Chiffrierung der lokal auf dem Gerät gespeicherten Notizen)".* Telefonieren oder das Internet benutzen, konnte man mit diesen Geräten hingegen nicht. Kommunikation war nur zwischen Kunden von EncroChat möglich. Über offizielle Vertriebskanäle konnten derartige Telefone nicht erworben werden. Auf Internetplattformen wurden entsprechende Geräte für 1.610 Euro angeboten, wobei dieser Preis eine Nutzerlizenz für die Dauer von sechs Monaten beinhaltete. Ein existierendes Unternehmen *„EncroChat"* war ebenso wenig zu lokalisieren wie diesbezüglich verantwortlich handelnde Personen oder ein Unternehmenssitz.

In Frankreich leitete die Staatsanwaltschaft Lille im November 2018 aufgrund des wiederholten Auftauchens[5] dieser Geräte ein Ermittlungsverfahren u.a. wegen des Verdachts einer kriminellen Vereinigung ein und fand heraus, dass die verschlüsselte Kommunikation zwischen EncroChat-Nutzern über einen im französischen Roubaix betriebenen Server lief. Nach Einholung eines richterlichen Beschlusses wurden am 21. Dezember 2018 und im Oktober 2019 die Daten des Servers kopiert und in der Folgezeit ausgewertet. Hierbei ergab sich, dass 66.134 SIM-Karten eines niederländischen Anbieters im System eingetragen waren, die in einer Vielzahl europäischer Länder verwendet wurden. Eine Dechiffrierung mehrerer tausend *„Notizen"* von EncroChat-Nutzern belegte, dass diese zweifelsfrei mit illegalen Aktivitäten wie Betäubungsmittelhandel mit bis zu 60 kg Kokain in Verbindung standen. Dabei belegten die Notizen das Handeltreiben in einer ungewohnt offenen Weise, da die Nutzer von einer Abhörsicherheit und *„Unverletzlichkeit"* ihrer Telefone ausgegangen waren.

Am 30. Januar 2020 genehmigte das Gericht in Lille auf Antrag der Staatsanwaltschaft den Einsatz einer Datenabfangeinrichtung sowohl auf dem Server als auch auf den mit diesem Server verbundenen Endgeräten, wobei die Installation dieser *„Trojanersoftware"* in Einklang mit der französischen Strafprozessordnung durch den damit beauftragten Generaldirektor für innere Sicherheit unter Rückgriff auf der Geheimhaltung der Nationalen Verteidigung unterliegende Staatsmittel ausgeführt werden sollte. Mangels anderer Ermittlungsmöglichkeiten, den Chiffrierungsschutz zu umgehen, genehmigte das Gericht in Lille am 20. März 2020 darüber hinaus u.a. eine Umleitung aller Datenströme (DNS-Umleitung) des Servers in Roubaix ab dem 1. April 2020. Zur Begründung hatte die Staatsanwaltschaft Lille darauf verwiesen, die bisherigen Ermittlungen hätten bestätigt, dass EncroChat-Geräte für kriminelle Zwecke verwendet würden und es aufgrund der Unmöglichkeit, die Endgeräte zu *„analysieren",* nur die Installation einer Datenabfangeinrichtung ermöglichen könne, die Chiffrierung zu umgehen.

Das durch den technischen Dienst für die justiziellen Abfangmaßnahmen entwickelte Softwaretool wurde sodann durch die französischen Behörden per *„Ferninjektion"* eingebracht, wobei auf Mittel zurückgegriffen wurde, die der Geheimhaltung der nationalen Verteidigung unterliegen. Dabei wurde bekannt, dass von der Datenabfangmaßnahme 32.477 Nutzer in 121 Ländern betroffen waren. Von den 380 in Frankreich aktiven Telefonen wurden nach ersten Erkenntnissen jedenfalls 63,7% für kriminelle Zwecke verwendet. Die übrigen Geräte waren entweder teils inaktiv oder noch nicht ausgewertet.

Am 7. April 2020 wurden die Ermittlungen auf Transport, Besitz, Erwerb, Anbieten oder Abgabe von Betäubungsmitteln und den Besitz und Erwerb von Waffen ohne Genehmigung ausgedehnt, nachdem die ausgewerteten Gespräche und die Überprüfung der ausgetauschten Fotos das ganze Ausmaß des von den Nutzern betriebenen Betäubungsmittelhandels offenlegten. Ein durch das Abfangen der Daten erlangter Leitfaden zur Vermarktung der chiffrierten Telefone enthielt folgende Hinweise: a) Es soll vorzugsweise in Kryptowährung gezahlt werden, b) Man soll sich gegenüber der Polizei bedeckt halten und insbesondere vermeiden, durch mengenmäßig zu große Lieferungen aufzufallen. Ein Verkäufer der Mobiltelefone wies insbesondere darauf hin, dass die Polizei die Telefone nicht lokalisieren könne, sie nicht abgehört werden und nicht genutzt werden könnten, wenn sie *„in schlechte Hände“* fielen. Insgesamt gingen Staatsanwaltschaft und Gericht in Auswertung der im ersten Monat erlangten Daten von einem *„nahezu ausschließlich kriminelle(n) Klientel“* der EncroChat-Nutzer aus.[6]

Anhand dieser Erkenntnisse wurden die aufgrund der richterlichen Anordnung zeitlich begrenzten technischen Maßnahmen zunächst für einen Monat ab 1. Mai 2020 und darauffolgend für weitere vier Monate ab 1. Juni 2020 – jeweils mit richterlichem Beschluss – verlängert und die Deliktstatbestände, derentwegen ermittelt wurde, erweitert.

Dem Bundeskriminalamt wurden in der Folgezeit über Europol Erkenntnisse zugleitet, wonach in Deutschland eine Vielzahl schwerster Straftaten, insbesondere Einfuhr und Handeltreiben mit Betäubungsmitteln in nicht geringen Mengen von EncroChat-Nutzern begangen würden. Bei der Generalstaatsanwaltschaft Frankfurt am Main, Zentralstelle zur Bekämpfung der Internetkriminalität, wurde ein Verfahren gegen Unbekannt u.a. wegen des Verdachts von Betäubungsmittelstraftaten eingeleitet. In diesem Verfahren erging am 2. Juni 2020 eine an Frankreich gerichtete Europäische Ermittlungsanordnung mit dem Antrag, die Deutschland betreffenden EncroChat-Daten zu übermitteln und deren unbeschränkte Verwendung in deutschen Strafverfahren zu erlauben. Beides genehmigte ein französisches Gericht am 13. Juni 2020. Die im Rahmen des Rechtshilfeersuchens übermittelten Informationen könnten dabei von den deutschen Behörden im Rahmen eines jeden Ermittlungsverfahrens und im Hinblick auf ein jedwedes Gerichts-, Strafverfolgungs- oder Untersuchungsverfahren oder Urteil verwendet werden.[7]

Auf Bitte der französischen Behörden übermittelte Europol der Generalstaatsanwaltschaft Frankfurt am Main die zwischen dem 1. April 2020 und dem 30. Juni 2020 auf den EncroChat-Servern erfassten Daten, die sich auf Geräte bezogen, die zu einer Auslösung von Mobilfunkantennen auf deutschem Boden geführt hatten. In diesem Zeitraum wurden auch die Landeskriminalämter, der Zoll und die Bundespolizei über das Vorliegen der EncroChat-Daten informiert. Mit Zustimmung der Generalstaatsanwaltschaft Frankfurt am Main wurden ihnen die Daten zur Verfügung gestellt, um eine gemeinsame Auswerte- und Ermittlungstätigkeit unter der Sachleitung der Generalstaatsanwaltschaft Frankfurt am Main zu realisieren. Die Schwierigkeit bestand dabei darin, die Identität der Nutzer der Krypto-Handys zu ermitteln, da bisher ja ausschließlich deren *„Nicknames“* bekannt waren. Dabei wurden die Nutzer anhand ihrer Geodaten den örtlich zuständigen Ermittlungsbehörden vorläufig zugeordnet. Durch eine solche Zuordnung sollte zunächst die Erstbearbeitung eines Nutzers erfolgen und der Datenbestand koordiniert gesichtet werden. Eine endgültige Festlegung der örtlichen und sachlichen Zuständigkeiten erfolgte erst nach inhaltlicher Auswertung der EncroChat-Daten. Für die inhaltliche Auswertung war es in der Folgezeit in einer Vielzahl von Verfahren erforderlich, mehrere zigtausend Chatzeilen in die deutsche Sprache zu übersetzen. Sodann mussten die Chatverläufe akribisch mit erheblichem Aufwand nach Anhaltspunkten für eine Identifizierung des jeweiligen Nutzers durchsucht werden. Eine Identifizierung konnte dabei vielfach durch versandte Lichtbilder (der Person des Nutzers selbst, ihrer PKW, Strafzettel, Wohnungen etc.) oder durch Hinweise auf den Wohnort, die persönlichen/familiären Verhältnisse sowie verbüßte Freiheitsstrafen erfolgen. Es kann dabei nicht oft genug betont werden, dass hierbei eine effektive Bearbeitung nur möglich war, da keine der involvierten Ermittlungsbehörden starr auf örtlichen Zuständigkeiten beharrte. Denn die Taten eines Nutzers erstreckten sich typischerweise auf zahlreiche Städte. Ferner waren oftmals mehrere Personen beteiligt, welche ebenfalls an unterschiedlichen Orten aufhältig waren. Insofern kann der Encrochat-Komplex wohl als eines der erfolgreichsten Beispiele deutscher Strafverfolgung bezeichnet werden, an welchem Ermittlungsbehörden nahezu aller Bundesländer beteiligt waren.

3 Erwägungen des Bundesgerichtshofes

Im Weiteren werden die rechtlichen Erwägungen des Bundesgerichtshofs hinsichtlich der Verwertbarkeit der erlangten EncroChat-Daten dargestellt.

3.1 Rechtsgrundlage für die Verwertung der Daten

Der Bundesgerichtshof stellt seiner Entscheidung voran, dass die verfassungsgemäße Rechtsgrundlage für die Verwertung von Beweisen im Strafprozess § 261 StPO (Grundsatz der freien richterlichen Beweiswürdigung) bildet. Dies gilt unabhängig davon,

ob diese Beweise im Inland oder auf sonstige Weise – etwa im Wege der Rechtshilfe – erlangt worden sind. Eine ausdrückliche Regelung, dass im Wege der Rechtshilfe aus dem Ausland erlangte Daten nur eingeschränkt verwendet werden dürfen, enthält das deutsche Recht nicht, insbesondere ist § 100e Abs. 6 StPO hierauf nicht unmittelbar anwendbar.[8]

Ein von der Revision des Angeklagten in Einklang mit großen Teilen des Schrifttums und vereinzelter Rechtsprechung[9] geltend gemachtes Beweisverwertungsverbot hinsichtlich der erlangten EncroChat-Daten besteht nach Auffassung des Bundesgerichtshofs unter keinem rechtlichen Gesichtspunkt. Ein solches ergibt sich weder aus rechtshilfespezifischen Gründen (vgl. 3.2) noch aus nationalem Verfassungs- oder Prozessrecht (vgl. 3.3). Auch die Vorgaben der Europäischen Menschenrechtskonvention (EMRK) stehen einer Beweisverwertung nicht entgegen (vgl. 3.4).

3.2 Kein Beweisverwertungsverbot aus rechtshilfespezifischen Gründen

Im Rahmen der Entscheidung erfolgen umfangreiche Ausführungen bezüglich eines potentiellen Beweisverwertungsverbotes unter rechtshilfespezifischen Aspekten. Hierbei handelt es sich zwar um eine vergleichsweise spezielle Materie, welcher Staatsanwälten und Polizeibeamten bei der täglichen Arbeit noch eher selten begegnen. Dessen ungeachtet soll im Folgenden auf die wesentlichen Problempunkte eingegangen werden. Denn zum einen nimmt die internationale Zusammenarbeit von Ermittlungsbehörden (glücklicherweise) stetig zu, weshalb auch die praktische Relevanz der diesbezüglichen Vorschriften exponentiell steigt. Zum anderen werden diese vom Bundesgerichtshof dargestellten Grundsätze auch für zukünftige vergleichbare Verfahren vollumfängliche Gültigkeit beanspruchen können.

Zunächst soll aufgrund der für einige Leser wohl eher unbekannten Materie kurz auf die Grundsätze der internationalen Zusammenarbeit in Strafsachen innerhalb der Europäischen Union eingegangen werden. Prägend für diese ist das Prinzip gegenseitiger Anerkennung strafjustizieller Entscheidungen der Mitgliedstaaten.[10] Hieraus folgen zahlreiche Aspekte, welche eine Rechtshilfe innerhalb der Europäischen Union stark vereinfachen. Etwa eine grundsätzlich bestehende gegenseitige Unterstützungspflicht. Sowie ein weitreichender Verzicht auf die sachliche Überprüfung ausländischer Entscheidungen. Am 3. April 2014 sind diese Grundsätze in der Richtlinie über die Europäische Ermittlungsanordnung (RL-EEA) manifestiert worden - 2014/41/EU -, deren Vorschriften der deutsche Gesetzgeber in den §§ 91a ff. des Gesetzes über die internationale Rechtshilfe in Strafsachen (IRG) am 22. Mai 2017 im Wesentlichen übernommen hat.[11] Seitdem kooperien die Mitgliedstaaten mittels der Europäischen Ermittlungsanordnung, wie es auch die Bundesrepublik Deutschland und Frankreich auf die beschriebene Weise im Juni 2020 getan haben. Der Bundesgerichtshof befasste sich daher mit der Frage, ob die Übermittlung der Encrochat-Daten an die Bundesrepublik Deutschland von den bezeichneten Rechtsgrundlagen getragen wird.

Zunächst wird dabei auf einen möglichen Verstoß gegen den sog. orde-public-Grundsatz eingegangen, welcher unter anderem in § 91b IRG und § 73 IRG Eingang gefunden hat. Dieser besagt im Wesentlichen, dass eine Rechtshilfe zu unterbleiben hat, wenn eine solche gegen elementare rechtstaatliche Grundsätze verstoßen, insbesondere eine erhebliche Grundrechtsverletzung darstellen würde.[12] Der Bundesgerichtshof führt diesbezüglich aus, dass allein aufgrund der beschriebenen Verwendung der Encrochat-Kryptohandys ein Anfangsverdacht gegen die Nutzer wegen schwerer Straftaten aus dem Bereich der Betäubungsmittelkriminalität gegeben war. Insofern habe gerade keine rechtswidrige verdachtslose Telekommunikationsüberwachung stattgefunden. Vielmehr waren die französischen Ermittlungsbehörden angesichts der Verdachtslage und aufgrund des staatlichen Auftrags zum Schutz der Bürger vor den von organisierter Betäubungsmittelkriminalität ausgehender Gefahren sowie des verfassungsrechtlichen Gebots einer funktionsfähigen Strafrechtspflege zur Vornahme von Ermittlungsmaßnahmen befugt. Grundlegende Rechtsstaatsdefizite oder Verstöße gegen menschen- bzw. europarechtliche Grundwerte wären hierin nicht zu erkennen.[13]

Des Weiteren käme auch ein Verstoß gegen Art. 31 RL-EEA und dessen Umsetzung in § 91g Abs. 6 IRG in Betracht. Art. 31 RL-EEA sieht eine Pflicht zur Benachrichtigung des von einer grenzüberschreitenden Telekommunikationsüberwachung betroffenen Zielstaates durch den überwachenden Staat vor. Der Zielstaat soll dann innerhalb von 96 Stunden entscheiden können, ob die Maßnahmen abgebrochen und die gewonnenen Erkenntnisse durch den überwachenden Staat nicht oder nur eingeschränkt verwendet werden dürfen. Im konkreten Fall wäre daher fraglich, ob Frankreich die Bundesrepublik Deutschland unmittelbar von den Maßnahmen bezüglich der EncroChat-Server hätte unterrichten müssen, jedenfalls soweit hiervon auch Nutzer auf dem Gebiet der Bundesrepublik Deutschland betroffen waren. Der Bundesgerichtshof lässt dahinstehen, ob es sich bei der Infiltration der Server überhaupt um eine mitteilungsbedürftige Telekommunikationsüberwachung gehandelt haben könnte. Ferner wird ausgeführt, dass ein Individualschutz des Art. 31 RL-EEA hinsichtlich betroffener Bürger wohl lediglich bezüglich einer Verwendung der erlangten Daten in etwaigen französischen Ermittlungsverfahren bestehen würde. Denn nur vor einer nicht gewollten Datenverwendung außerhalb des von der Telekommunikationsüberwachung betroffenen Zielstaates soll die Mitteilungspflicht des Art 31 RL-EEA schützen.[14] Letztlich lässt der Bundesgerichtshof aber auch dies dahinstehen. Denn selbst wenn Art. 31 RL-EEA individualschützender Charakter zukäme, würde ein etwaiger Verstoß nicht zu einem

Beweisverwertungsverbot bezüglich der an die Bundesrepublik Deutschland übermittelten Daten führen. Dem Strafverfahrensrecht lässt sich kein allgemein geltender Grundsatz entnehmen, wonach jeder potentielle Verstoß gegen Rechtsnormen ein strafprozessuales Verwertungsverbot nach sich zieht. Ob ein solches eingreift, ist vielmehr jeweils nach den Umständen des Einzelfalls, insbesondere nach der Art des Verbots und dem Gewicht des Verstoßes, unter Abwägung der widerstreitenden Interessen zu entscheiden. Maßgeblich beeinflusst wird das Ergebnis der Abwägung einerseits durch das Ausmaß des staatlichen Aufklärungsinteresses, dessen Gewicht im konkreten Fall vor allem unter Berücksichtigung der Verfügbarkeit weiterer Beweismittel, der Intensität des Tatverdachts und der Schwere der Straftat bestimmt wird. Andererseits ist das Gewicht des in Rede stehenden Verfahrensverstoßes von Belang, das sich vor allem danach bemisst, ob der Rechtsverstoß gutgläubig, fahrlässig oder vorsätzlich begangen wurde.[15] Dabei muss beachtet werden, dass die Annahme eines Verwertungsverbots, auch wenn die Strafprozessordnung nicht auf Wahrheitserforschung um jeden Preis gerichtet ist, eines der wesentlichen Prinzipien des Strafverfahrensrechts einschränkt, nämlich den Grundsatz, dass das Gericht die Wahrheit zu erforschen und dazu die Beweisaufnahme von Amts wegen auf alle relevanten Tatsachen und Beweismittel zu erstrecken hat. Daran gemessen bedeutet ein Beweisverwertungsverbot eine Ausnahme, die nur nach ausdrücklicher gesetzlicher Vorschrift oder aus übergeordneten wichtigen Gründen im Einzelfall anzuerkennen ist.[16] Dies kommt etwa in Betracht, bei schwerwiegenden, bewussten oder willkürlichen Verfahrensverstößen, bei denen die grundrechtlichen Sicherungen planmäßig oder systematisch außer Acht gelassen werden.[17] Im Rahmen der erforderlichen Abwägung führt der Bundesgerichtshof dann prägnant aus: *„Es geht um die Aufklärung besonders schwerwiegender Straftaten, nämlich Verbrechen nach § 29a Abs. 1 Nr. 2 BtMG, die im Höchstmaß mit Freiheitsstrafe von 15 Jahren bedroht sind. Andere Beweismittel stehen hier für die Überführung des Angeklagten in den von seinem Geständnis nicht erfassten Fällen nicht zur Verfügung, so dass ohne die Verwertung dieser Beweismittel eine Überführung des Angeklagten in den relevanten Fällen nicht möglich wäre. Die EncroChat-Protokolle sind als Beweismittel besonders ergiebig, da darin offen über Drogengeschäfte in erheblichem Umfang kommuniziert wird. Demgegenüber fiele ein etwaiger individualschutzbezogener Rechtsverstoß […] nicht entscheidend ins Gewicht“.*

Zuletzt soll bezüglich dieses Themenkomplexes eine mögliche Verletzung des Art. Art 6 RL-EEA problematisiert werden. Art. Art 6 RL-EEA sieht u.a. vor, dass mittels einer Europäische Ermittlungsanordnung nur Maßnahmen erbeten werden können, welche in einem vergleichbaren innerstaatlichen Fall unter denselben Bedingungen angeordnet werden könnten. Der Bundesgerichtshof erklärt diese Regelung in der gegebenen Konstellation jedoch für nicht anwendbar. Denn es handele sich lediglich um die Übermittlung der durch einen anderen Mitgliedstaat aufgrund eigener Ermittlungstätigkeit nach dessen nationalem Recht bereits erlangten Beweismittel. Die Durchführung einer Ermittlungsmaßnahme wäre also seitens der Bundesrepublik Deutschland gerade nicht erbeten worden; vielmehr wäre diese ja bereits seitens der französischen Behörden erfolgt. Der Anordnungsstaat müsse in Konstellationen, in welchen auf die erlangten Erkenntnisse eines anderen Staates zugegriffen werden soll, lediglich prüfen, ob der Erlass der Europäischen Ermittlungsanordnung für die Zwecke des Verfahrens unter Berücksichtigung der Rechte der Verfahrensbeteiligten notwendig und verhältnismäßig ist. Diese Voraussetzung erfüllt dabei die Europäische Ermittlungsanordnung der Generalstaatsanwaltschaft Frankfurt am Main von Juni 2020, da insbesondere unter Berücksichtigung der sehr hohen Kosten für Erwerb und Nutzung von EncroChat-Handys klare Anhaltspunkte dafür vorlagen, dass die Beweismittel sich auf schwerste Straftaten aus dem Bereich der organisierten Kriminalität bezogen, deren Aufklärung ohne Zugriff auf die in Frankreich erlangten Informationen ansonsten kaum möglich gewesen wäre.[18]

3.3 Kein Beweisverwertungsverbot aus nationalem Verfassungsrecht

Ein Beweisverwertungsverbot ergibt sich nach den Ausführungen des Bundesgerichtshofs auch nicht unmittelbar aus deutschem Verfassungsrecht. Ein absolutes Beweisverwertungsverbot unmittelbar aus den Grundrechten, kann überhaupt nur im absoluten Kernbereich privater Lebensgestaltung bestehen, was bei der Planung und Durchführung von Straftaten hingegen nicht der Fall ist.[19]

Die Verwertung personenbezogener Informationen wie der EncroChat-Kommunikation greift zwar grundsätzlich in das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) ein. Dabei hängt die durch die Verwertung der Daten liegende Eingriffsintensität maßgeblich davon ab, welchen Grad an Persönlichkeitsrelevanz die betroffenen Daten haben und auf welchem Weg sie erlangt wurden.[20] Bei wie hier erlangten Daten, die mit einen Eingriff in das von Art. 10 GG geschützte Fernmeldegeheimnis einhergehen, muss von Verfassungs wegen der Verhältnismäßigkeitsgrundsatz besonders beachtet werden.

Im Rahmen innerstaatlicher Ermittlungen wird der Grundrechtseingriff durch die unterschiedlichen Voraussetzungen für verschiedene Ermittlungsmaßnahmen bereits bei der Anordnung der Maßnahme selbst limitiert (etwa Beschränkung auf besonders schwere Straftaten oder Fälle qualifizierten Verdachts). Kann diese Beschränkung in Fällen wie dem vorliegenden nicht geleistet werden, weil hier durch einen anderen Mitgliedstaat (Frankreich) in originärer Anwendung seines nationalen Rechts in die Grundrechte Betroffener eingegriffen wird, sind die dadurch möglichen Unterschiede bei den Eingriffsvoraussetzungen auf der Ebene der Beweisverwendung zu kompensieren.[21]

Zu diesem Zweck greift der Bundesgerichtshof in seiner Entscheidung sodann auf die in den strafprozessualen Verwendungsbeschränkungen verkörperten Wertungen zurück, die insoweit als verfassungsrechtliche Schutzmechanismen für die Beweisverwertung dienen. Demnach dürfen aufgrund der Bedeutung der französischen Ermittlungsmaßnahmen in Anlehnung an die Verwendungsschranke mit dem höchsten Schutzniveau – § 100e Abs. 6 Nr. 1 StPO[22]– derart erlangte Daten zur Überführung solcher besonders schwerer Straftaten verwendet werden, für deren Aufklärung die eingriffsintensivsten Ermittlungsmaßnahmen des deutschen Strafverfahrensrechts – namentlich eine Online-Durchsuchung gem. § 100b StPO oder eine akustische Wohnraumüberwachung gem. § 100c StPO – hätten angeordnet können.[23]

Die im vorliegenden Fall in Rede stehenden Verbrechen erfüllen die Voraussetzungen für eine Beweisverwertung nach dieser gebotenen strikten Verhältnismäßigkeitsprüfung. Die Vorwürfe wiegen auch im Einzelfall schwer, da es jeweils um den Handel mit Betäubungsmitteln im Kilogrammbereich geht und die Erforschung des Sachverhalts ohne dieses Beweismittel nicht möglich wäre.

Weiter betont der Bundegerichtshof, es wäre unter verfassungsrechtlichen Aspekten gerade nicht geboten, dass das deutsche Strafprozessrecht eine entsprechende Ermittlungsmaßnahme vorsieht. Die bloße Nichteinhaltung deutschen Rechts bei einer ausländischen Ermittlungsmaßnahme kann nicht per se ein unselbstständiges Beweisverwertungsverbot begründen.[24] Die Einhaltung rechtstaatlicher Mindeststandards wird in solchen Fällen – wie vorstehend ausgeführt – insbesondere durch eine strikte Verhältnismäßigkeitsprüfung unter (entsprechender) Anwendung besonderer nationaler Verwendungsvorbehalte gewährleistet.[25]

3.4 Kein Verstoß gegen Vorgaben der Europäischen Menschenrechtskonvention (EMRK)

Schließlich führt der Bundesgerichtshof aus, dass die Verwertung der EncroChat-Daten auch mit den Regelungen der EMRK vereinbar ist. Insbesondere sind zu einem Beweisverwertungsverbot führende Verstöße gegen Art. 8 EMRK (Recht auf Achtung des Privat- und Familienlebens) sowie Art. 10 EMRK (Freiheit der Meinungsäußerung) bei einer durch einen Richter angeordneten Maßnahme bezüglich der gegenständlichen schweren Straftaten nicht festzustellen.[26]

4 Resümee

Die Entscheidung des Bundesgerichtshofes ist absolut zu begrüßen und in ihren Formulierungen erfreulich deutlich. Es wäre aber wohl auch kaum dem *„Bürger von der Straße“* zu vermitteln, wenn derartige Daten, welche sich nahezu ausschließlich auf schwerste Straftaten beziehen, und die geeignet sind, diese unmittelbar zu beweisen, nicht seitens der Ermittlungsbehörden verwertet werden dürften. Ferner muss es diesen möglich sein, bezüglich technischer Aufrüstungsmaßnahmen krimineller Organisationen reagieren zu können. Denn insbesondere dieser Ermittlungskomplex hat wieder einmal nachhaltig verdeutlicht, wie umfassend die Beteiligten bereits technische Neuerungen genutzt und wie wenig sie ihr Handeln an Landesgrenzen ausgerichtet haben. Die Bekämpfung derartiger krimineller Netzwerke setzt daher entschlossenes Vorgehen der Ermittlungsbehörden, einen steten überregionalen bzw. internationalen Austausch der jeweiligen Erkenntnisse und die Koordinierung der Ermittlungshandlungen voraus. Von der Bereitschaft zu überobligatorischem Einsatz ganz zu schweigen. All dies haben die beteiligten Behörden in beeindruckendem Maße bezüglich des *„Encrochat-Komplexes“* umgesetzt und so sicherlich einige Wirkungstreffer im Bereich des internationalen Betäubungsmittelhandels landen können. Die dabei eingeübten Handlungsroutinen dürften sich auch in naher Zukunft bei der Auswertung der erlangten Daten aus den mit Encrochat vergleichbaren Krypto-Netzwerken *„SkyECC“*[27] und *„ANOM“*[28] als nützlich erweisen. Angesichts dieses wegweisenden Beschlusses des Bundesgerichtshofes dürften der Verwertbarkeit auch dieser Daten in deutschen Strafprozessen keine Bedenken entgegenstehen.

Anmerkungen

1. Dr. Sören Pansa ist bei der Generalstaatsanwaltschaft Schleswig-Holstein und Dr. Marius Heller bei der Staatsanwaltschaft bei dem Landgericht Kiel tätig. Der Beitrag gibt ausschließlich die persönliche Auffassung der Verfasser wieder.
2. BGBl. I 2017, 3202ff.

3. Vgl. statt vieler Gerhard/Michalke, NJW 2022, 655; Strate HRRS 2022, 15; Nadeborn/Albrecht, NZWiSt 2021, 420.
4. BGH, Beschluss vom 2. März 2022 – 5 StR 457/21 –, zitiert nach juris; inzwischen hat der 4. Strafsenat des Bundesgerichtshofes diese Entscheidung inhaltlich bestätigt: Beschluss vom 5. Juli 2022 - 4 StR 61/22 -, zitiert nach juris.
5. Nach einer im Jahr 2019 durch das Bundeskriminalamt durchgeführten Abfrage sollen im Zeitraum von Oktober 2018 bis September 2019 etwa 75% der bekannt gewordenen Kryptohandys in Deutschland solche des Anbieters EncroChat gewesen sein.
6. BGH, Beschluss vom 2. März 2022 – 5 StR 457/21 -, Rn. 18, zitiert nach juris.
7. BGH, Beschluss vom 2. März 2022 – 5 StR 457/21 -, Rn. 22, zitiert nach juris.
8. BGH, Beschluss vom 2. März 2022 – 5 StR 457/21 -, Rn. 25, zitiert nach juris.
9. Derin/Singelnstein, NStZ 2021, 449; dies., StV 2022, 130; Erhard/Lödden, StraFo 2021, 366; Gebhard/Michalke, NJW 2022, 655; Wahl, ZIS 2021, 452; LG Berlin, Beschluss vom 1. Juli 2021 – [^{525} KLs] 254 Js 592/20 [^{10}/21], NStZ 2021, 696.
10. Hierzu zusammenfassend: BGH, Beschluss vom 23. April 2020 – 1 StR 15/20 –, NJW 2020, 3185 (3188).
11. BGBl. I 2017, S. 31ff.
12. Vgl. hierzu umfassend Gleß/Wahl/Zimmermann in Schomburg/Lagodny, Internationale Rechtshilfe in Strafsachen, 6. Aufl. 2020, § 73 IRG Rn. 1 ff.
13. BGH, Beschluss vom 2. März 2022 – 5 StR 457/21 -, Rn. 36ff., zitiert nach juris.
14. So auch Wahl, ZIS 2021, 452 (457).
15. Vgl. statt vieler BGH, Urteil vom 20. Oktober 2021 – 6 StR 319/21 –, zitiert nach juris.
16. BGH, Urteil vom 18. April 2007 – 5 StR 546/06 –, BGHSt 51, 285.
17. BGH, Beschluss vom 21. April 2016 – 2 StR 394/15 –, StV 2016, 539.
18. BGH, Beschluss vom 2. März 2022 – 5 StR 457/21 -, Rn. 46ff., zitiert nach juris.
19. BGH, Beschluss vom 2. März 2022 – 5 StR 457/21 -, Rn. 62, zitiert nach juris.
20. BGH, Beschluss vom 2. März 2022 – 5 StR 457/21 -, Rn. 64, zitiert nach juris.
21. BGH, Beschluss vom 2. März 2022 – 5 StR 457/21 -, Rn. 68, zitiert nach juris.
22. Die Vorschrift des § 100e Abs. 6 StPO ist nach ihrem Wortlaut auf die vorliegende Konstellation nicht anwendbar, da die in Rede stehenden Daten nicht nach den §§ 100b, 100c StPO, sondern durch eigenständige Maßnahmen nach französischem Prozessrecht erlangt wurden.
23. Für diese Prüfung ist dabei auf den Erkenntnisstand im Zeitpunkt der Verwertung der Beweisergebnisse abzustellen, auf die Rekonstruktion der Verdachtslage im Anordnungszeitpunkt kommt es indes nicht an, BGH, Beschluss vom 2. März 2022 – 5 StR 457/21 -, Rn. 70, zitiert nach juris; a. A. LG Berlin, Beschluss vom 1. Juli 2021 – [^{525} KLs] 254 Js 592/20 [^{10}/21], NStZ 2021, 696.
24. BGH, Beschluss vom 2. März 2022 - 5 StR 457/21 -, Rn. 72 f, zitiert nach juris.
25. Ob für den Fall eines – hier nicht ersichtlichen – sog. „Befugnis-Shoppings“, also eines Rechtshilfeersuchens zwecks bewusster Umgehung strengerer inländischer Anordnungsvorrausetzungen, eine andere Bewertung vorzunehmen wäre, hat der BGH offengelassen, vgl. BGH, Beschluss vom 2. März 2022 - 5 StR 457/21 -, Rn. 75, zitiert nach juris.
26. BGH, Beschluss vom 2. März 2022 – 5 StR 457/21 -, Rn. 77, zitiert nach juris.
27. Vgl. OLG Celle, Beschluss vom 15. November 2021 – 2 HEs 24 - 30/21 –, NdsRpfl 2022, 87.
28. Vgl. OLG Frankfurt, Beschluss vom 22. November 2021 – 1 HEs 427/21 –, NJW 2022, 710.