

Verwertung von im Ausland überwachter Chatnachrichten im Strafverfahren

Zugleich Besprechung der EncroChat-Beschlüsse des OLG Bremen v. 18.12.2020 – 1 Ws 166/20, und OLG Hamburg v. 29.1.2021 – 1 Ws 2/21

Von **Thomas Wahl**, Freiburg im Breisgau*

Die Beschlüsse des OLG Bremen und des OLG Hamburg sind die ersten obergerichtlichen Entscheidungen, die sich mit der justiziellen Aufarbeitung des sog. EncroChat-Falles in Deutschland befassen. Im Kern geht es darum, ob sich in deutschen Strafverfahren Beweisverwertungsverbote ergeben, weil die Übermittlung von Massendaten über Kommunikationsteilnehmer aus Frankreich an Deutschland gegen nationale oder rechtshilferechtliche Standards verstoßen hat. Während die beiden Oberlandesgerichte ein Beweisverwertungsverbot verneinen, kommt der Beitrag zu einem gegensätzlichen Ergebnis.

I. Ausgangslage

Nach der Sachverhaltsschilderung in den Beschlüssen und Pressemeldungen¹ begannen in Frankreich Ermittlungen, nachdem Ermittler in Einzelfällen entdeckt hatten, dass durch das Unternehmen EncroChat speziell verschlüsselte Smartphones auffällig häufig von Straftätern aus dem Bereich der organisierten Kriminalität verwendet wurden. EncroChat mietete Server des Internetdienstleisters OVH in Roubaix/Frankreich, über den verschlüsselte End-to-End Nachrichten geleitet wurden. Den französischen Ermittlungsbehörden gelang es schließlich durch technische Vorrichtungen, Daten von EncroChat auf diesen Servern zu kopieren und auszuwerten. Anschließend spielten sie (nach vorheriger richterlicher Genehmigung) eine vom französischen Militär entwickelte „Spionagesoftware“ auf die EncroChat Geräte der Nutzer auf,

* Der Verfasser ist Senior Researcher am Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht, Freiburg im Breisgau.

¹ Gemeinsame Pressemeldung von Eurojust und Europol v. 2.7.2020, abrufbar unter

<https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe> (21.6.2021); *Diehl/Lehberger/Meyer-Heuer/Rosenbach*, Operation „Festspiele“, Spiegel Nr. 52/2020, S. 52, online abrufbar unter

<https://www.spiegel.de/panorama/justiz/drogenfahnder-knackten-krypto-handys-eine-superwaffe-gegen-das-organisierte-verbrechen-a-00000000-0002-0001-0000-000174544047> (21.6.2021); *Kabisch/Strunz*, tagesschau.de v. 23.9.2020, abrufbar unter

<https://www.tagesschau.de/investigativ/ndr/bka-chats-schwerkriminalle-101.html> (21.6.2021); *Stukenberg*, Netzpolitik v. 22.2.2021, abrufbar unter

<https://netzpolitik.org/2021/streit-um-encrochat-ermittlungen-vor-gericht/> (21.6.2021); *Cox*, VICE v. 3.7.2020, abrufbar unter

<https://www.vice.com/de/article/3aza95/encrochat-hack-wie-die-polizei-ein-handynetzwerk-fur-drogengangs-infiltrierte> (21.6.2021); *Symonds*, BBC v. 5.2.2021, abrufbar unter <https://www.bbc.com/news/uk-55953247> (21.6.2021).

wovon über 32.000 Geräte betroffen waren. Hierbei befand sich nur ein kleiner Teil der Nutzer (380) ganz oder teilweise im französischen Hoheitsgebiet. Durch die Operation waren die Ermittler nicht nur in der Lage, weitere Computerdaten wie IMEI-Nummern oder Standortdaten der Handys abzufangen, sondern zwischen April und Juni 2020 auch Chatverläufe live mitzulesen. Vor allem durch das Mitlesen der Chat-Verläufe habe sich ergeben, dass sich über das mutmaßlich sichere Kommunikationsnetzwerk, wie von EncroChat zur Verfügung gestellt, „vorwiegend“² Kriminelle in ganz Europa austauschten. Ein Indiz sei schon der satte Abonnementpreis für die Nutzung der „Krypto-Handys“ gewesen. Die Überwachung und erste Auswertung geschah zunächst im Rahmen einer gemeinsamen Ermittlungsgruppe, in der französische und niederländische Behörden mit Unterstützung von Europol und Eurojust teilnahmen. Deutschland war offiziell zunächst nicht an der Operation unmittelbar beteiligt gewesen. Es ist jedoch mit Folgeverfahren befasst, wenn sich aus der Auswertung Anhaltspunkte ergeben, dass deutsche Kommunikationsteilnehmer betroffen sind. Nach erster Auswertung durch Europol hat das BKA mit Einverständnis der französischen Polizei Datenpakete zur weiteren Identifizierung möglicher Straftäter im Rahmen des polizeilichen Informationsaustausches übermittelt bekommen. Parallel hat die auf Computerkriminalität spezialisierte Generalstaatsanwaltschaft Frankfurt a.M. Ermittlungsverfahren gegen unbekannt eröffnet und per europäischer Ermittlungsanordnung vom 2.6.2020 beim zuständigen Gericht in Lille nachträglich um die Verwertung aller im Datenpaket enthaltenen Informationen in laufenden und zukünftigen deutschen Strafverfahren gebeten. Diesem Ersuchen hat eine Richterin in Lille am 13.6.2020 stattgegeben. Die genauere Auswertung der Datenpakete durch das BKA hat zur Identifizierung der Beschwerdeführer geführt; aus den Chatverläufen ergab sich deren Beteiligung an Straftaten im Bereich des Drogen- oder Waffenhandels.

II. Ausgangspunkt: Verwertbarkeit von „Massentelekomunikationsdaten“

Die Besonderheit des Falles liegt darin, dass nicht – wie „im Normalfall“ – ein strafrechtlicher Anfangsverdacht gegen eine Einzelperson vorliegt, gegen die dann gezielt weitere Ermittlungsschritte (ggf. im Wege der Rechtshilfe), wie die Überwachung ihrer Telekommunikation, eingeleitet werden. Vielmehr wird den nationalen Ermittlungsbehörden ein umfangreiches Datenpaket „zur weiteren Verwendung“ bereitgestellt. Zu Beginn einer staatlichen Überwachung stand nicht die konkrete Erkenntnis in Bezug auf eine (mögliche) Straftat, sondern lediglich die pauschale, erst im späteren Verlauf

² In der Presse ist, basierend auf Einschätzungen der Strafverfolgungsbehörden, teilweise von 90 %, teilweise von 60 % die Rede.

der Ermittlungsverfahren verifizierte Vermutung, dass das EncroChat-Netzwerk (auch/überwiegend?) von Kriminellen benutzt worden ist. Überwacht worden sind damit auch diejenigen EncroChat-Nutzer, welche das Netzwerk nicht für kriminelle Zwecke genutzt haben. Damit folgt nicht der Beweis dem Fall, sondern der Fall dem „Beweis“ (welcher in den Daten schlummert). Klassische Rechtshilfe an sich spielt damit gar keine Rolle mehr. Das erinnert an den Ankauf der Steuer-CDs und die nachfolgende Auswertung durch die Steuerfahndungsbehörden.³ Allerdings wäre es gefährlich, hierzu Analogieschlüsse zu ziehen.⁴ Der entscheidende Unterschied besteht darin, dass im EncroChat-Fall das Datenrohmaterial nicht von Privaten erworben wurde, sondern von ausländischen Behörden selbst, für welche die strengen Befugnis- und Ermächtigungsnormen des nationalen Strafprozessrechts und des internationalen Rechtshilferechts gelten. Beweisverwertungsverbotsregeln, welche für den staatlichen Ankauf von Datenmaterial von Privaten entwickelt worden sind,⁵ können nicht auf den Informationsaustausch unter staatlichen Stellen übertragen werden.⁶

Die beiden OLGe hatten jeweils inzident im Rahmen der Beschwerde gegen die Anordnung der Untersuchungshaft gegen die Beschuldigten zu prüfen, ob die grenzüberschreitende Operation und Kooperation mit Rechtsverstößen behaftet war, welche ein Beweisverwertungsverbot nach sich ziehen. Bejahendenfalls hätten sie den dringenden Tatverdacht verneinen und die Untersuchungshaftbefehle aufheben müssen. Im Ausgangspunkt ist weitgehend unbestritten, dass sich die Frage nach der Verwertbarkeit allein nach dem Recht des Forumstaates richtet (hier: deutsches Recht).⁷ Für die Beweiserhebung gilt damit grundsätzlich⁸ das Prinzip „*locus regit actum*“, für die Beweisverwertung das Prinzip „*forum regit actum*“. Welche Konsequenzen daraus jedoch konkret zu ziehen sind, ist oftmals unklar. Anders als z.B. in Belgien⁹ existiert in Deutschland keine eindeutige Regelung zur Verwertbarkeit des im Ausland gewonnenen Datenmaterials im Strafprozess, so dass auf die allgemeinen, bisher entwickelten Grundsätze zurückzugreifen ist. Rechtsverstöße führen nur ausnahmsweise zu einem Verwertungsverbot der generierten Informationen.¹⁰ Sie können sich in der vorliegenden Konstellation ergeben, weil eine Diskrepanz zwischen dem nach dem Recht des Erhebungsortes „Möglichen“, aber nach dem

Recht des Forumstaates „Unzulässigen“ besteht (III.) oder weil Voraussetzungen des Rechtshilferechts nicht eingehalten worden sind (IV.).

III. Beweisverwertungsverbot wegen Nichteinhaltung des deutschen Rechts

Die OLGe Bremen und Hamburg gehen der Frage nach, ob ein Verwertungsverbot im deutschen Strafverfahren folgt, weil der Beweis am Erhebungsort (hier: Frankreich) ggf. rechtswidrig gewonnen wurde. Im Ergebnis ergaben sich für beide OLGe hierfür keine Anhaltspunkte. Sie hätten jedoch darüber hinaus ein weiteres mögliches Beweisverwertungsverbot prüfen bzw. die Frage anders stellen müssen, nämlich dahingehend: Sind in Frankreich Zwangsmaßnahmen möglich, die in Deutschland so nicht angeordnet werden können und was folgt daraus für das deutsche Strafverfahren? Die Frage lautet also nicht, ob die Anwendung des französischen Rechts rechtswidrig war, sondern, ob die Abweichungen zum deutschen Recht hinsichtlich der Art der Beweisgewinnung so groß sind, dass aus rechtsstaatlichen Gründen die übermittelten Informationen nicht als Beweis verwertet werden können.¹¹ Diese Frage ist bisher speziell für den Bereich der heimlichen Telekommunikationsüberwachung (im Folgenden: TKÜ) höchstrichterlich nicht entschieden worden. Zwar setzte sich der BGH in seiner Leitentscheidung aus dem Jahre 2012 ausführlich mit der prozessualen Verwertbarkeit von Erkenntnissen aus einer im Ausland durchgeführten Maßnahme der TKÜ auseinander.¹² Gegenstand der Entscheidung war aber die Frage nach der Beweisverwertung wegen Nichteinhaltung des Rechts am Erhebungsort.¹³ Indes bestehen gerade im EncroChat-Fall massive Anhaltspunkte dafür, auf die Art von Beweisverwertungsverbot wegen Abweichungen zum Recht des Forumstaates näher einzugehen. Im Gegensatz zum französischen Recht ist nach deutschem Recht der streubreite Einsatz technischer Mittel gegen eine unbestimmte Gruppe von Verdächtigen – zudem noch unter Nutzung von Spy- oder Malware – gerade nicht erlaubt.¹⁴ Wie ist ein (mögliches) Beweisverwertungsverbot zu begründen?

1. *Ordre public*-Maßstab und Einpassungsfähigkeit der Norm als Konkretisierung

Welche Maßstäbe in solchen Fallkonstellationen an die Beweisverwertung anzulegen sind, ist bisher schon für Beweismittel außerhalb von TKÜ weitgehend ungeklärt. Die Rechtsprechung hatte sich bisher vor allem mit Fällen im Zusam-

³ LG Bochum NStZ 2010, 351; Sieber, NJW 2008, 881.

⁴ In diese Richtung jedoch Pauli, NStZ 2021, 146.

⁵ Michaelis, MMR 2020, 586.

⁶ Wohlers, JZ 2011, 253; Trück/Habetha, NStZ 2008, 481 (490).

⁷ Ambos/Rackow/Schork, StV 2021, 126 (133); Oehmichen/Schneider/v. Wistinghausen, StraFo 2015, 230; Böse, ZStW 114 (2002), 148 (149); Ambos, Beweisverwertungsverbote, 2010, S. 82; zu anderen Ansätzen außerhalb Deutschlands Ligeti/Garamvölgyi/Ondrejová/v. Galen, eucrim 2020, 201.

⁸ Zu Ausnahmen siehe Art. 9 Abs. 2 RL EEA und Art. 4 EU-RhÜbk.

⁹ Boulet/de Hert, in: Sieber/v. zur Mühlen (Hrsg.), Access to Telecommunication Data in Criminal Justice, 2016, S. 227.

¹⁰ Radtke, NStZ 2017, 109.

¹¹ Entgegen Pauli, NStZ 2021, 146, kommt es deshalb gar nicht darauf an, ob die französischen Behörden gegenüber Deutschland Bedingungen gesetzt haben oder das in Art. 9 Abs. 2 RL EEA enthaltene *forum regit actum*-Prinzip bei der Beweiserhebung beachten mussten. Zusammenfassend zu den verschiedenen Konstellationen Radtke, NStZ 2017, 109.

¹² BGHSt 58, 32.

¹³ Siehe auch Schuster, StV 2014, 198 (199).

¹⁴ Kochheim, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Aufl. 2018, Rn. 2134; Dietrich, GSZ 2021, 1 (4).

menhang mit Vernehmungen von Zeugen oder Beschuldigten im Ausland auseinanderzusetzen, die nicht deutschen Maßstäben entsprachen.¹⁵ Vor dem Hintergrund, dass die Rechtsprechung die Art der Beweisgewinnung, mithin die Frage nach der Rechtmäßigkeit oder Rechtswidrigkeit der Beweiserhebung im Ausland für unbeachtlich hält, neigt die h.M. dazu, die Kautelen für nach der Fremdrechtsordnung rechtswidrige Erhebungen spiegelbildlich anzuwenden.¹⁶

Eine Unverwertbarkeit kann sich danach nur dann ergeben, wenn die Beweisgewinnung im Ausland gegen die unverzichtbaren allgemeinen rechtsstaatlichen Grundsätze der deutschen Rechtsordnung verstoßen (ordre public-Grenze) oder den menschenrechtlichen Mindeststandard nicht eingehalten hat, wie er sich aus der EMRK und den IPbpR ergibt (Grenze des völkerrechtlichen Individualschutzes).¹⁷ Mit diesem Ansatz wird die Latte für die Annahme eines Beweisverwertungsverbots sehr hoch gelegt, zumal die Rechtsprechung bisher handfeste Kriterien dafür, was unter den „unverzichtbaren allgemeinen rechtsstaatlichen Grundsätzen“ zu verstehen ist, nicht entwickelt hat.¹⁸ Vielmehr blieb es bisher bei Einzelfallentscheidungen. Konsensfähige Maßstäbe der ordre public-Prüfung wurden nicht gefunden. Aus verschiedenen Entscheidungen des Bundesverfassungsgerichts zu § 73 IRG lässt sich ablesen, dass der ordre public „nur“ den Kerngehalt der Grund- und Menschenrechte, sowie die Grundsätze der Rechtsstaatlichkeit, einschließlich der Verhältnismäßigkeit, und ein Minimum an Verfahrensgerechtigkeit beinhaltet.¹⁹ Damit ist freilich ebenfalls nicht viel gewonnen. Konkretisierungen dieses Maßstabes in der Literatur fehlen weitgehend.²⁰

Schuster hat diesen ordre-public Ansatz für die sonstige Rechtshilfe – ausgehend von der deutschen Dogmatik zu den selbständigen Beweisverwertungsverböten – dahingehend konkretisiert, dass er fragt, ob ein nach deutschen Maßstäben den Grundrechten noch genügender Zustand gewährleistet wäre, wenn man sich vorstelle, dass die ausländische Norm isoliert in das deutsche Strafverfahrensrecht mit dem Zweck

der Beweisgewinnung inkorporiert würde.²¹ Zu ähnlichen Ergebnissen dürfte der von Vogel entwickelte Ansatz führen, wonach Abweichungen im ausländischen Recht von wesentlichen Grundsätzen, „Maximen“ und Zwecksetzungen des deutschen Gesetzesrechts als „unerträglich“ erscheinen müssten, was sich nicht selten (aber nicht notwendigerweise) in einer verfassungsrechtlichen Verankerung wie den Grundrechten und grundrechtsgleichen Rechten des GG niederschläge.²²

An diesem – am nationalen ordre public – ausgerichteten Maßstab für die Beweisverwertung ändert sich auch nichts durch das Unionsrecht. Insbesondere kann nicht argumentiert werden, die auf dem Grundsatz der gegenseitigen Anerkennung justizieller Entscheidungen basierende, seit 2017 die justizielle Rechtshilfe innerhalb der Europäischen Union regelnde Richtlinie über die Europäische Ermittlungsanordnung (RL EEA) erlaube lediglich die Prüfung eines „europäischen ordre public“. Dann wäre die französische Maßnahme lediglich an den Grundrechten der Grundrechtecharta in Verbindung mit dem Standard der EMRK zu messen. Richtig ist, dass Art. 11 Abs. 1 lit. f RL EEA einen auf dem europäischen ordre public basierenden Rechtshilfeverweigerungsgrund regelt, allerdings betrifft dieser nur die Ermächtigung zur Leistung der Rechtshilfe, nicht die Verwertung des durch Rechtshilfe erworbenen Materials. Wie die bisherigen Rechtshilfekonventionen spart auch die RL EEA die Beweisverwertungsfrage substantiiert aus.²³ Das ergibt sich mittelbar aus Art. 14 Abs. 7 RL EEA, der den Einfluss des Unionsrechts auf die Beweisverwertung allenfalls apodiktisch regelt und schließlich die Beweisverwertung unter die Maßgabe des nationalen Rechts stellt (S. 1). Nach Art. 14 Abs. 7 S. 2 RL EEA soll unterste Grenze lediglich die Wahrung der Verteidigungsrechte und die Gewährleistung eines fairen Verfahrens sein, was bereits in der oben beschriebenen Formel zur Verwertung ausländischer Beweise inkludiert ist.²⁴ Deshalb kann entgegen OLG Hamburg der Maßstab auch nicht unter Berufung auf die jüngste Rechtsprechung des BVerfG zum Europäischen Haftbefehl weiter auf eine bloße Identitätskontrolle reduziert werden.

Auf dieser Grundlage empfiehlt es sich zunächst, die Grundlinien des ausländischen Verfahrensrechts anzusehen, wobei es nicht darum geht, die ausländische Norm als „rechtsstaatswidrig“ zu qualifizieren (2.). In einem zweiten Schritt sind die Parameter des deutschen ordre public zu bestimmen (3.), bevor dann die „Einpassungsfähigkeit“ des ausländischen Rechts in das Gesamtkonzept der deutschen Strafprozessordnung zu beurteilen ist (4.).²⁵

¹⁵ BGHSt 7, 15; BGH NStZ 1983, 181; BGH NJW 1988, 2187; BGH NStZ 1992, 394; BGH NStZ 1994, 595; BGH NStZ 2000, 307; BGH NStZ 2007, 417; BGH NStZ 2010, 410. Vgl. auch den Überblick bei Pitsch, Strafprozessuale Beweisverbote, 2009, S. 110 ff.

¹⁶ Hackner/Schierholt, Internationale Rechtshilfe in Strafsachen, 3. Aufl. 2017, Rn. 237; Gless, JR 2008, 317 (320).

¹⁷ Oehmichen/Schneider/v. Wistinghausen, StraFo 2015, 231 f.; Ambos (Fn. 7), S. 83; Beulke, JURA 2008, 663; vgl. auch Gleß, JR 2008, 317, 320; Schuster, ZIS 2016, 564 (568 f.); Nagel, Beweisaufnahme im Ausland, 1988, S. 302.

¹⁸ Schädel, Die Bewilligung internationaler Rechtshilfe in Strafsachen in der Europäischen Union, 2005, S. 209.

¹⁹ BVerfGE 63, 366 (377 f.); 75, 1 (16); BVerfG NVwZ 2016, 201; vgl. auch Schädel (Fn. 18), S. 209; Gleß/Wahl/Zimmermann, in: Schomburg/Lagodny, Internationale Rechtshilfe in Strafsachen, 6. Aufl. 2020, IRG § 73, Rn. 7a.

²⁰ Zu weitergehenden Alternativansätzen siehe z.B. Pitsch (Fn. 15), S. 135 ff.; Gleß, Beweisrechtsgrundsätze einer grenzüberschreitenden Strafverfolgung, 2006, S. 411 ff.

²¹ Schuster, Verwertbarkeit im Ausland gewonnener Beweise im deutschen Strafprozess, 2006, S. 130.

²² Vogel, in: Grütznert/Pötz/Kreß/Gazeas (Hrsg.), Internationaler Rechtshilfeverkehr in Strafsachen, 3. Aufl., Stand: 2001, I. 2. § 73 IRG, Rn. 32.

²³ Ligeti/Garamvölgyi/Ondrejová/v. Galen, eucrim 2020, 201 (205); Kubiciel, in: Ambos/König/Rackow (Hrsg.), Rechtshilferecht in Strafsachen, 2. Aufl. 2020, 4. Hauptteil, Rn. 408.

²⁴ Vgl. auch BT-Drs. 18/9757, S. 18.

²⁵ Vgl. auch Schuster (Fn. 1), S. 131.

2. Erforderliche Betrachtung des Fremdrechts

Das französische Recht unterscheidet verschiedene Phasen des strafprozessualen Vorverfahrens. Französischen Behörden sind bestimmte Befugnisse in der Voruntersuchungsphase (*enquête préliminaire*) eingeräumt, in der lediglich der Verdacht oder Indizien einer Straftat im Raum stehen und noch kein Verdacht gegen eine bestimmte Person begründet werden kann, die Ermittlungsbehörden also mit einer Hypothese arbeiten.²⁶ In der Regel werden Voruntersuchungen nicht mit dem Einsatz grundrechtsintensiver Eingriffsmaßnahmen durchgeführt.²⁷ Dies ändert sich jedoch, wenn bestimmte mit organisierter Kriminalität verbundene Delikte untersucht werden. Hierfür hat das „loi Perben II“ ein gesondertes Verfahren eingeführt, das den Ermittlungsbehörden den Einsatz umfangreicher spezifischer Zwangsmaßnahmen erlaubt.²⁸ Das Verfahren ist deutlich auf Effektivität der Ermittlungen ausgerichtet, d.h. die Befugnisse der Ermittlungsbehörden werden ausgeweitet und Operationen möglicherweise bremsende (rechtliche) Zwänge minimiert.²⁹

Während Voruntersuchungen von Straftaten der organisierten Kriminalität kann die „elektronische Kommunikation“ (*communication électronique*) abgehört, aufgezeichnet und transkribiert werden.³⁰ Die Maßnahme ist zeitlich zu begrenzen und vom „Freiheits- und Haftrichter“ (*juge des libertés et de la détention*) zu autorisieren. Als materielles Kriterium wird hierbei abgesehen vom recht weitgehenden Straftatenkatalog lediglich vorausgesetzt, dass der Bedarf an Informationen die TKÜ erfordert („*lorsque les nécessités de l'information l'exigent*“).³¹

Schließlich ist es möglich, dass die französische Polizei heimlich eine „technische Vorrichtung“ (*dispositif technique*) an „jedem Ort“ platzieren kann, damit sie so auf Daten zugreifen kann, wie sie auf dem Informationssystem gespeichert sind, wie sie auf dem Bildschirm des Nutzers erscheinen, wie sie in Form von Zeichen eingegeben werden oder wie sie durch Peripheriegeräte empfangen bzw. ausgesendet werden.³² Erlaubt ist damit der heimliche Fernzugriff auf Daten unter Einsatz von Computerabfangeinrichtungen.³³ Grenze ist wiederum die formale Voraussetzung richterlicher Autorisierung, wobei die beantragende Staatsanwaltschaft den Ort der Anbringung der Vorrichtung sowie die im Raum stehenden Straftaten genau bezeichnen muss.³⁴ Auch ist die

Operation zeitlich auf vier Monate (mit erneuter Verlängerungsmöglichkeit) zu befristen.³⁵

Alle aufgeführten heimlichen Ermittlungsmaßnahmen werden in Frankreich nicht nur durch den Richter – je nach Verfahrensphase der Ermittlungsrichter oder der Freiheits- und Haftrichter – genehmigt, sondern auch von diesem kontinuierlich begleitet und überwacht. Die ausführenden Polizeibehörden haben dem Richter gegenüber Berichtspflichten. Besonders bedeutsam ist einerseits, dass die Formalitäten eingehalten werden, bei Verstößen droht das Gesetz mitunter die Nichtigkeit der Maßnahme an.³⁶ Der Eingriff in die Freiheits- und Grundrechte wird dadurch kompensiert, dass Beschuldigte, die in „Polizeigewahrsam“ (*garde à vue*) genommen oder vorgeladen wurden, frühzeitig Akteneinsichtsrechte zugesprochen bekommen.³⁷ Andererseits genügt die Einhaltung der in der Ermächtigung zur Ermittlungsmaßnahme niedergelegten Voraussetzungen, um die Operation durchzuführen. Dazu gehören insbesondere die Bezeichnung der Straftat, welche die Operation rechtfertigt (oder ggf. nur rechtfertigen kann), die Spezifizierung der einer Überwachung unterliegenden Örtlichkeiten und die Dauer der Maßnahme. Nach französischem Verständnis ist damit gleichzeitig der Verhältnismäßigkeit der Zwangsmaßnahme im Hinblick auf die Schwere der Straftat genüge getan. Innerhalb dieser Grenzen spezifiziert die französische Strafprozessordnung weder, welche Personen unter die Überwachungsmaßnahme fallen (etwa Verdächtige, Kommunikationsmittler oder Kommunikationspartner), noch wird gefordert, dass weniger einschneidende Mittel als die Kommunikationsüberwachung vorrangig zu erwägen oder durchzuführen wären.³⁸

Geht es wie im EncroChat-Fall um strafrechtliche Ermittlungen im Bereich der organisierten Kriminalität, war es vor diesem Hintergrund aus der Perspektive des französischen Rechts nicht nur unproblematisch, dass zunächst alle auf den von EncroChat genutzten Servern enthaltenen Daten „konserviert“ wurden, sondern auch, dass französische Behörden „technische Vorrichtungen“ an einer Vielzahl von EncroChat-Endgeräten aufspielen konnten, welche ihnen dann das Mitlesen von Kommunikationsinhalten erlaubte.

3. Grenzbestimmung des deutschen *ordre public*

Aus der Perspektive des deutschen Rechts erweist sich insbesondere die Überwachung des laufenden Datenverkehrs als problematisch, welche nicht durch eine den Beschlagnahmenvorschriften nach § 94 Abs. 2 StPO unterfallende Serverüberwachung gedeckt wäre.³⁹ Überwachungen des Inhalts der Kommunikation sind nur an §§ 100a ff. StPO zu messen. Nutzen die Ermittlungsbehörden – wie im EncroChat-Fall – Infiltrationssoftware, um Verschlüsselungen zu umgehen und – ohne Einschaltung der Diensteanbieter – unmittelbar Zu-

²⁶ *Debove/Falletti/Dupic*, Précis de droit pénal et de procédure pénale, 5. Aufl. 2013, S. 787.

²⁷ *Debove/Falletti/Dupic* (Fn. 26), S. 787.

²⁸ *Debove/Falletti/Dupic* (Fn. 6), S. 792. Welche Straftaten darunter fallen wird enumerativ in einem Straftatenkatalog aufgeführt, welcher sich aus Art. 706-73, 706-73-1 und 706-74 CPP ergibt. Das können auch Straftaten sein, welche nicht im Kernstrafrecht des französischen Strafgesetzbuches geregelt sind.

²⁹ *Debove/Falletti/Dupic* (Fn. 6), S. 792.

³⁰ Article 706-95 CPP.

³¹ Article 706-95 i.V.m. Article 100 CPP.

³² Article 706-102-1 CPP.

³³ *De Marco*, in: Sieber/v. zur Mühlen (Fn. 9), S. 461.

³⁴ Article 706-102-3 CPP.

³⁵ *De Marco* (Fn. 33), S. 475.

³⁶ Vgl. z.B. Article 706-102-3 CPP.

³⁷ *Debove/Falletti/Dupic* (Fn. 26), S. 794.

³⁸ Dies gilt für alle der hier vorgestellten Zwangsmaßnahmen. Siehe *De Marco* (Fn. 33), S. 473 f.

³⁹ Vgl. *Kochheim* (Fn. 14), Rn. 2114.

griff auf die Inhaltsdaten in Echtzeit zu erhalten, müssen die in den Vorschriften zur Quellen-TKÜ (§ 100a Abs. 1 S. 2 und 3 StPO) und Online-Durchsuchung (§ 100b StPO) enthaltenen Wertungen beachtet werden.

Die entscheidenden rechtsstaatlichen Parameter hat das Bundesverfassungsgericht in seiner Entscheidung zur Zulässigkeit der Onlinedurchsuchung des VSG NRW gezogen.⁴⁰ Sie sind auch Maßstab für die Bewertung der in die StPO eingeführten „Bundestrojaner“ für repressive Zwecke. Die deutschen Befugnisnormen erlauben den verfassungsmäßigen Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.⁴¹ Das Bundesverfassungsgericht sieht die technische Infiltrierung in ein komplexes informationstechnisches System zum Zweck der TKÜ als besonders schwerwiegenden Grundrechtseingriff an und zieht demzufolge enge Grenzen für die Rechtfertigung, wofür sowohl technische als auch rechtliche Vorgaben notwendig sind.⁴² Die in §§ 100a und 100b StPO gefundene Lösung, Infiltrierungsmaßnahmen nur für einen Katalog schwerer oder als besonders schwer anzusehender Straftaten zuzulassen (Eingriffsanlass nur bei hinreichendem Gewicht), die Gewichtung der Schwere im Einzelfall und der Subsidiaritätsgrundsatz, sind Ausdruck der Verhältnismäßigkeit i.e.S. Diese Bedingungen tariieren das Spannungsverhältnis der widerstreitenden Interessen aus: den (durch die Strafverfolgung zum Ausdruck kommenden) Rechtsgüterschutz auf der einen Seite und die Erwartung des Einzelnen in die Gewährleistung von Vertraulichkeit und Integrität des informationstechnischen Systems auf der anderen Seite.⁴³ Das Bundesverfassungsgericht fordert zudem einen tatsachen- und evidenzbasierten Eingriff, so dass sich die Überwachung nur aus Anlass eines konkreten Geschehens und gegen bestimmte Beschuldigte richten kann, gegen die sich vor der Überwachung (also ex ante) der Anfangsverdacht insoweit konkretisiert und die bereits „identifizierbar erscheinen“, als sie als Betroffene der Eingriffsmaßnahme in Betracht kommen und ihre Beteiligung an einer Katalogtat wahrscheinlich ist.⁴⁴ Nur so lassen sich dadurch erstens die Gewährleistung effektiven Rechtsschutzes gegen Fehler bei der Eingriffsgestaltung aufrechterhalten⁴⁵ und zweitens der weitgehend ungezielte Einsatz der Überwachungsmaßnahme durch staatliche Behörden verhindern. Letzteren Aspekt hebt das Bun-

desverfassungsgericht ausdrücklich hervor, wenn es eine nicht hinreichend konkretisierte oder auf ambivalenter Tatsachenlage erfolgende Überwachung angesichts der Schwere des Eingriffs als „verfassungsrechtlich nicht hinnehmbar“ einstuft.⁴⁶ Die verdachtslose Überwachung der Kommunikation wäre durch die deutschen Grundrechte nicht mehr gedeckt.⁴⁷ Zudem kann die Überwachung von (zunächst nicht-beschuldigten) Dritten nur unter engen Grenzen erfolgen.⁴⁸

4. Folgen fehlender Einpassungsfähigkeit der ausländischen Norm

Wendet man die genannten Leitlinien an und fragt sich, ob die französische Regelung sich in diese Grundlinien des deutschen Rechts einfügen ließe oder ob sie „unerträglich“ wäre (s.o. 1.), fällt der Befund negativ aus. Zwar sieht das französische Recht auch einige verfahrenssichernde Vorkehrungen vor, wie sie auch das Bundesverfassungsgericht für essentiell hält. Hierzu zählt z.B. die Notwendigkeit richterlicher Genehmigung der Maßnahme. Allerdings würde der deutsche ordre public eine eingehendere Verhältnismäßigkeitsprüfung zum Schutz des Freiheitsrechts verlangen. Ungeachtet dessen, dass auch das französische Recht für eine Art Quellen-TKÜ einen Straftatenkatalog kennt, gibt es keine zusätzlichen Voraussetzungen, welche die Verhältnismäßigkeit der Maßnahme rechtfertigen würden. Insbesondere genügt nach französischer Auffassung lediglich „der Bedarf an Informationen“ zur Erforschung der Wahrheit.⁴⁹ Alternativmaßnahmen werden nicht erwogen. Der deutschen Grundauffassung zuwider läuft zudem, dass die Abfangeinrichtung zunächst auf allen EncroChat Endgeräten aufgespielt werden konnte, obwohl ex ante betrachtet noch kein konkreter Tatverdacht gegen bestimmte, zumindest bestimmbar Beschuldigte bestand. Dieser ergab sich erst nachträglich infolge des Mitlebens der Chat-Nachrichten. Erst ex post wurde – wie sich aus der Pressemitteilung von Europol/Eurojust vom 2. Juli 2020 entnehmen lässt – die Erkenntnis gewonnen, dass der Dienstleister EncroChat „vorwiegend“ (!) von Kriminellen benutzt worden sein soll. Betroffen durch die Abhöreinrichtung war damit zunächst eine Vielzahl von Personen, darunter auch solche, die EncroChat für nichtkriminelle Zwecke genutzt haben. Eine solche Regelung würde sich nicht in das deutsche Strafprozessrecht zulässiger Ermittlungsmaßnahmen einpassen lassen, da es den grundrechtlichen Schutz, den die entsprechende Grundlage in der StPO bietet, in wesentlichen Punkten unterläuft. Gerade vor dem Hintergrund der in Deutschland geführten Diskussion, wie weit staatliche Eingriffe in Verschlüsselungsmechanismen gehen können,⁵⁰ muss das gegenüber deutschen Behörden geschützte Interesse

⁴⁰ BVerfGE 120, 274 = NJW 2008, 822.

⁴¹ Hauck, in: Becker/Erb/Esser/Graalman-Scheerer/Hilger/Ignor (Hrsg.), Löwe-Rosenberg, Die Strafprozeßordnung und das Gerichtsverfassungsgesetz, Großkommentar, Bd. 3/1, 27. Aufl. 2019, StPO § 100a, Rn. 99.

⁴² BVerfGE 120, 274 (308f., 322).

⁴³ BVerfGE 120, 274 (326).

⁴⁴ Eschelbach, in: Satzger/Schluckebier/Widmaier (Hrsg.), Strafprozessordnung, Kommentar, 4. Aufl. 2020, § 100a StPO, Rn. 12, 17; vgl. auch BVerfG NJW 2020, 2699, wonach bereits die allgemeine Befugnis zur Übermittlung und zum Abruf von Bestandsdaten für die Strafverfolgung trotz ihres gemäßigten Eingriffsgewichts eines Anfangsverdachts bedarf.

⁴⁵ Eschelbach (Fn. 44), § 100a Rn. 12.

⁴⁶ BVerfGE 120, 274 (329).

⁴⁷ Schuster (Fn. 21), S. 243.

⁴⁸ Eisenberg, Beweisrecht der StPO, 10. Aufl. 2017, Rn. 2487; Eschelbach (Fn. 44), § 100a Rn. 18.

⁴⁹ Vgl. hierzu auch die im EGMR-Urteil *Kusin/Frankreich* angeführte Doktrin des französischen Cour de Cassation (Urt. v. 24.4.1990 – 11801/85, § 12).

⁵⁰ Dietrich, GSZ 2021, 1; Martini/Fröhlingsdorf, NJW 2020, 1803.

an der Wahrung der Vertraulichkeit und Integrität des informationstechnischen Systems auch gegenüber im Ausland durchgeführten Überwachungsmaßnahmen gelten.

Demzufolge würde der ordre public-Maßstab im vorliegenden Fall die Verwertung der von Frankreich übermittelten Informationen hindern. Allerdings ist damit noch nichts darüber gesagt, ob es nicht doch zu einer Verurteilung des Betroffenen kommen kann. Da das deutsche Strafprozessrecht nach der Rechtsprechung des BGH keine Fernwirkung von Beweisverboten kennt, blieben die aus Frankreich übermittelten Informationen als Spuren- und Ermittlungsansatz bestehen, so dass sich die in Rede stehenden Straftaten durch weitere Beweismittel, etwa Durchsuchungen und Beschlagnahmen oder Zeugenaussagen, bestätigen ließen.⁵¹ Diese Konsequenz müssten die Gerichte im weiteren Prozessverlauf klären.

IV. Rechtshilferechtliche Beweisverwertungsverbote

Eine Unverwertbarkeit von Beweisen kann sich auch daraus ergeben, dass rechtshilferechtliche Bestimmungen, welche die Übertragung der erhobenen Beweismittel von Staat zu Staat regeln, verletzt worden sind.⁵² Der EncroChat-Fall bietet hier zwei Ansatzpunkte, die auch vom OLG Bremen und OLG Hamburg aufgegriffen wurden: Es könnte ein Verstoß gegen die Regeln der grenzüberschreitenden Überwachung des Telekommunikationsverkehrs vorliegen (1.) oder es könnten Regeln bei der Informationsübermittlung nicht eingehalten worden sein (2.).

1. Beweisverwertungsverbot wegen Verstoßes gegen Vorschriften grenzüberschreitender Telekommunikationsüberwachung

a) Regelungssystematik der TKÜ ohne technische Hilfe eines Staates (Art. 31 RL EEA)

Für die grenzüberschreitende TKÜ innerhalb der Europäischen Union sieht das Rechtshilferecht zwei Spezialregelungen vor: 1. TKÜ, für welche die technische Hilfe eines anderen Staates notwendig ist (Art. 30 RL EEA) und 2. solche, die ohne technische Hilfe eines anderen Staates durchgeführt werden können, Art. 31 RL EEA. Im EncroChat-Fall einschlägig ist die letztere Konstellation. Art. 31 RL EEA geht auf Art. 20 EU-RhÜbk zurück. Beide Bestimmungen haben bisher in Rechtsprechung und Literatur eher ein Schattendasein geführt. Der Uniongesetzgeber hat die Norm als Form der passiven Rechtshilfe analog der in der physischen Welt vorkommenden grenzüberschreitenden Nacheile und Observation konzipiert. Ursprünglich war vor allem an die Fälle gedacht worden, dass trotz Überschreitens einer Grenze

durch die überwachte Person der Zugang zur Telekommunikation im Überwachungsstaat bestehen bleibt, z.B. wenn das Mobiltelefon der Zielperson, welche sich von Straßburg in Frankreich nach Kehl in Deutschland begibt, im französischen Heimatnetz eingeloggt bleibt. Allerdings sind die Normen bewusst technikoffen gestaltet worden und erfassen einen viel weiteren Anwendungsbereich.⁵³ Deshalb ist von Art. 31 RL EEA auch die Überwachung der internetbasierten Kommunikation gedeckt, wie sie von den französischen Ermittlern durchgeführt worden ist.⁵⁴

Befindet sich die Zielperson auf dem Hoheitsgebiet eines anderen als dem überwachenden Mitgliedstaat und nutzt dort den Kommunikationsanschluss, wird eine Unterrichtungspflicht ausgelöst. Der unterrichtete Mitgliedstaat (hier: Deutschland) muss dann innerhalb einer bestimmten Frist (nach der RL EEA maximal 96 Stunden) reagieren, wenn er die Überwachung mit seinem innerstaatlichen Recht für unvereinbar hält. Gegebenenfalls kann er über das Setzen von Bedingungen der Verwertung der erlangten Informationen widersprechen. Art. 31 RL EEA normiert damit positiv eine Beweisverwertungsverbotsregel; diese gilt jedoch nur in eine Richtung, nämlich vom unterrichteten Staat zum überwachenden Staat. Sie griffe in der EncroChat-Konstellation nur, wenn Frankreich ein Strafverfahren gegen den Betroffenen durchführen würde und hier von Deutschland Bedingungen gemacht worden wären. Solche Bedingungen sollten standardmäßig z.B. dahingehend aufgestellt werden, dass Informationen aus dem absolut geschützten Bereich privater Lebensgestaltung (§ 100d StPO) oder aus Kommunikationen mit absolut geschützten Berufsgeheimnistägern (§ 160a Abs. 1 StPO) nicht verwertet werden könnten. Für den hier interessierenden Fall, dass Informationen über den Betroffenen wieder an den unterrichteten Staat zurückgespielt werden, verbunden mit der Bitte, gegen ihn ein eigenes Strafverfahren anzustrengen, existiert keine Regelung. Selbst im Falle gesetzter Bedingungen zu Lasten des überwachenden Staates wird in dieser Fallkonstellation per se kein Beweisausschluss begründet.

b) Abwägungslösung als Maßstab eines Beweisverwertungsverbots

Ob im vorliegenden Fall überhaupt eine Unterrichtung stattgefunden hat und ob Deutschland reagiert hat, bleibt offen. Beide OLGs führen jedoch aus, dass selbst bei einem Verstoß gegen das rechtshilferechtliche Verfahren des Art. 31 RL EEA kein Beweisverwertungsverbot anzunehmen wäre und rekurrieren dabei auf die Abwägungslösung in der deutschen Beweisverbotslehre. Begrüßenswert ist, dass die OLGs hier über die BGH-Rechtsprechung hinausgehen, welche bei Verletzung rechtshilferechtlicher Bestimmungen lediglich dann ein Verwertungsverbot annehmen möchte, wenn allgemeine

⁵¹ Kritisch konstatierend *Beulke*, JURA 2008, 665; *Trück/Habetha*, NSStZ 2008, 481 (491). Generell zur zunächst möglichen Verwendung von durch TKÜ gewonnenen, auf dem Rechtshilfeweg übermittelten Inhalte als polizeilicher Ermittlungsansatz und der nachträglichen Beschränkung der Beweisverwertung siehe *Fabbri/Furger*, ZStrR 2010, 394.

⁵² BGHSt 58, 32 Rn. 23; *Ambos/Rackow/Schork*, StV 2021, 126 (133).

⁵³ Erläuternder Bericht zu dem Übereinkommen vom 29. Mai 2000 über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union, ABl. EU Nr. C 379 v. 29.12.2000, 7, 21.

⁵⁴ *Schierholt*, in: Schomburg/Lagodny (Fn. 19), IRG § 91g, Rn. 10.

völkerrechtliche Grundsätze wie das allgemeine Fairnessgebot nach Art. 6 Abs. 1 EMRK nicht eingehalten werden.⁵⁵ Ein aus dem BGH-Ansatz abzuleitendes Verwertungsverbot dürfte praktisch ausgeschlossen sein.⁵⁶

c) Folgen einer unterlassenen Unterrichtung nach Art. 31 RL EEA

Bei der Anwendung der Abwägungslösung kommen beide OLGe jedoch zum Schluss, dass der Wahrheitsfindung und damit dem Interesse der Strafverfolgung Vorrang einzuräumen sei. Gestützt wird das Ergebnis darauf, dass den deutschen Behörden im Verfahren nach Art. 31 RL EEA nur eine eingeschränkte Prüfungskompetenz eingeräumt werde (so OLG Bremen), das Verhalten der deutschen Ermittlungsbehörden quasi einer Heilung des Verstoßes zumindest nahekomme und die Ermittlungsmaßnahme sowieso genehmigt worden wäre, da die Voraussetzungen der Quellen-TKÜ und Onlinedurchsuchung (§§ 100a, 100b StPO) vorgelegen hätten (so OLG Hamburg). Diesen Begründungsansätzen kann nicht zugestimmt werden, die Abwägung hätte differenzierter vorgenommen werden müssen.

Zunächst ist der im Beschluss des OLG Bremen anklingenden Tendenz entgegenzutreten, die Zustimmung des unterrichteten Staates wäre lediglich „eine Formsache“ und eine Prüfung könnte „eh nur summarisch“ vorgenommen werden. In Umsetzung des Art. 31 RL EEA geht der deutsche Gesetzgeber davon aus, dass das Prüfprogramm nicht schwächer ist als jenes bei der TKÜ mit technischer Hilfe Deutschlands nach Art. 30 RL EEA.⁵⁷ Infolgedessen müssen vollumfänglich § 59 Abs. 3 IRG i.V.m. §§ 100a ff. StPO geprüft und die entsprechenden Maßnahmen analog Nr. 77a Abs. 4 RiVAST eingeleitet werden. Insbesondere müssen in Deutschland geltende Beweisverwertungsverbote, welche in einem vergleichbaren innerstaatlichen Fall bestehen würden, auch grenzüberschreitend zur Geltung gebracht werden.⁵⁸ An der Begründung des OLG Hamburg ist problematisch, dass die Voraussetzungen einer Quellen-TKÜ oder Onlinedurchsuchung nach §§ 100a, 100b StPO, wie unter III. 3. aufgezeigt, nicht vorgelegen haben dürften. Ferner kann im Vorgehen der Generalstaatsanwaltschaft Frankfurt a.M. keine „nachträgliche Heilung“ des Verstoßes gesehen werden, da die Generalstaatsanwaltschaft nicht zuständige Bewilligungsbehörde im Verfahren des Art. 31 RL EEA ist.⁵⁹

In die Abwägung hätte stärker eingestellt werden müssen, dass die französische Ermittlungsmaßnahme umfangreiche Ermittlungen gegen eine Vielzahl von Nutzern in Deutsch-

land zuließ, ohne dass gegen Einzelne zunächst ein konkreter Verdacht einer Katalogtat vorlag. Mangels Konkretheit hätte eine sinnvolle Prüfung zum Schutz der Grundrechte, insbesondere Art. 10 GG als auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), vom für den Widerspruch zuständigen AG Stuttgart gar nicht vorgenommen werden können. Deshalb muss gefragt werden, ob – zumindest bei groben Verstößen gegen *auch* individual-schützende Rechtshilfevoraussetzungen – ein Verfahrensverstoß nicht folgenlos bleiben kann.⁶⁰ In der anderen Waagschale liegt, dass der Unionsgesetzgeber in Abweichung vom Wortlaut der Vorgängerregelung in Art. 20 Abs. 1 EU-RhÜbk in Art. 31 RL EEA von einer gewissen Spezifität der verfolgten Straftat als Voraussetzung absieht. Ferner verständigen sich die Nationen im Ausgangspunkt, dass sich Telekommunikationsüberwachungen nach dem geltenden Recht des überwachenden Staates auch auf die Hoheitsgebiete anderer Staaten, gar einer Vielzahl von Staaten ausdehnen können. Die Unterrichtungs- und Widerspruchslösung dient deshalb vorwiegend der Wahrung der Souveränitätsinteressen, wie auch bei den anderen Formen der passiven Rechtshilfe.⁶¹ Schließlich ist zu beachten, dass der durch Art. 31 RL EEA konzipierte Grundrechtsschutz durch die Widerspruchslösung gerade im hier in Rede stehenden Fall wegfällt, wenn aus der grenzüberschreitenden Überwachung Informationen gewonnen werden, die auch ein strafbares Verhalten im von der Maßnahme betroffenen Staat (Deutschland) zu Tage fördern. Das Ergebnis der beiden Gerichtsbeschlüsse ließe sich damit rechtfertigen, zwingend ist es jedoch nicht.

2. Beweisverwertungsverbot wegen aufgetretener Defizite in der Informationsrechtshilfe

a) Ausgangsproblem: Unklare Abgrenzung zwischen polizeilicher und justizieller Rechtshilfe durch die Unionsrechtsakte

OLG Bremen und OLG Hamburg gehen richtigerweise auch darauf ein, ob sich aus verfahrensrechtlichen Anforderungen des Rechtshilferechts eine Rechtswidrigkeit ergeben hat. Einen Verstoß können beide Gerichte nicht feststellen: Die Datenübermittlung erfolgte als sog. spontaner Informationsaustausch nach Art. 7 des Rahmenbeschlusses 2006/960/JI (RB-Informationsaustausch) i.V.m. den französischen Umsetzungsvorschriften zwischen den Polizeibehörden. Aufgrund der Verwendungsbeschränkung in Art. 1 Abs. 4 RB-Informationsaustausch wurde die Verwertung als Beweismittel nachträglich durch die Generalstaatsanwaltschaft Frankfurt a.M. über eine EEA vom französischen Gericht autorisiert, was ebenfalls nicht zu beanstanden sei. Diese rein formaljuristische Betrachtung offenbart jedoch eine wesentliche Schwachstelle des RB-Informationsaustauschs: Er überschneidet sich mit der justiziellen Rechtshilfe (seit 2017 in der EU

⁵⁵ BGHSt 58, 32 Rn. 29.

⁵⁶ So auch *Zehetgruber*, NZWiSt 2013, 464, 465, zumal sich aus der Rechtsprechung des EGMR kaum etwas gewinnen lässt (vgl. *Wahl*, in: Schomburg/Lagodny [Fn. 19], HT VII B1, Überblick Rn. 15; *Meese*, ERA Forum 18 [2017], 297 [306 ff.]; *Gleiß* [Fn. 20], S. 173 ff., 190 f.; *Esser*, Auf dem Weg zu einem europäischen Strafverfahrensrecht, 2002, S. 628 f.).

⁵⁷ BT-Drs. 18/9757, S. 75.

⁵⁸ Ebenso *Ahlbrecht*, StV 2018, 601 (606).

⁵⁹ Vgl. dazu die Sonderregelung in § 92d IRG.

⁶⁰ So *Zehetgruber*, NZWiSt 2013, 464.

⁶¹ Zur grenzüberschreitenden Nacheile: *Soiné*, Kriminalistik 2016, 459; *Bovendamm*, Kriminalistik 2016, 38; zur grenzüberschreitenden Observation: *Wüurz*, Das Schengener Durchführungsübereinkommen, 1997, Rn. 82.

auf der Grundlage der RL EEA). Beide Instrumente erzielen im Wesentlichen die gleichen Ergebnisse,⁶² lassen jedoch einen Gleichklang vermissen, weil der den polizeilichen Informationsaustausch fördernde RB⁶³ viel weniger dem Individualschutz dienende Gegenrechte enthält als die justizielle Rechtshilfe. Dadurch werden Schutzstandards umgangen, welche zugunsten des Betroffenen bestehen.⁶⁴

Im Gegensatz zu seiner Vorgängervorschrift in Art. 46 SDÜ, der eine klare Linie dahingehend gezogen hat, dass der spontane polizeiliche Austausch für bereits begangene Straftaten unzulässig, also nur unter vorheriger Einschaltung der für die Rechtshilfe zuständigen Justizbehörden auf der Grundlage der Bestimmungen der justiziellen Rechtshilfe möglich ist,⁶⁵ erweitert der RB-Informationsaustausch die polizeiliche Rechtshilfe entscheidend: Nach Art. 7 RB 2006/960 genügt es für die Spontanübermittlung, vorbehaltlich der (wenigen) Zurückhaltungsgründe in Art. 10 RB, wenn die Strafverfolgungsbehörde eines Mitgliedstaats „konkrete Gründe für die Annahme“ hat, die Informationen und Erkenntnisse könnten dazu beitragen, die in Art. 2 Abs. 2 des Rahmenbeschlusses über den Europäischen Haftbefehl aufgelisteten Delikte aufzudecken, zu verhüten oder *aufzuklären*. Damit wird ein Fremdkörper in das System der Rechtshilfe eingeführt, da der Austausch von potentiell sämtlichem, später im Strafverfahren zu nutzendem Beweismaterial jedenfalls bei schwerer Kriminalität wie Drogen- oder Waffenhandel vom RB gedeckt wird.⁶⁶ Die einzige Abgrenzung zur Rechtshilfe zwischen Justizbehörden besteht nach dem RB-Informationsaustausch im repressiven Bereich lediglich darin, dass die übermittelten Informationen nicht ohne Einwilligung der

Justizbehörde als Beweismittel verwendet werden können.⁶⁷ Das Verfahren für die Einwilligung der Justizbehörden bereits übermittelter Informationen auf dem Polizeiweg ist jedoch ebenso offen wie der Prüfungsmaßstab.

b) Umgehung justizieller Rechtshilfevoraussetzungen als Prüfungsmaßstab der nachträglichen Einwilligung

In der Kommentarliteratur wird – insoweit zutreffend – vorgeschlagen, dass das Mittel für die nachträgliche Einholung der Einwilligung eine EEA sei.⁶⁸ Allerdings liefe der justizielle Einwilligungsvorbehalt weitgehend leer, wenn man zusätzlich annimmt, dass infolge der Konzeption des RB-Informationsaustausches die polizeilich übermittelten Informationen bereits für die Begründung von Zwangsmaßnahmen im Vorverfahren, etwa wie hier, der Ausstellung eines Haftbefehls (und damit zur Begründung eines dringenden Tatverdachts) verwendet werden dürfen, die Verwendungsbeschränkung in Art. 1 Abs. 4 RB sich lediglich auf die Begründung des Schuldverdachts beziehe und erst in der Hauptverhandlung relevant werde.⁶⁹ Diese Prämisse muss mit der Einschränkung versehen werden, dass nicht nur erstens die Informationsrechtshilfe nach dem RB 2008/960, sondern zweitens auch die nachträglich ersuchte Rechtshilfe über die RL EEA rechtmäßig war und sich aus Rechtshilfeverstößen ergebende Beweisverwertungsverbote nicht auf das Vorverfahren auswirken. Nur so kann sichergestellt werden, dass auch im Ermittlungsverfahren gerade bei Begründung des dringenden Tatverdachts bei U-Haft Beweisverwertungsverbote zu prüfen sind.⁷⁰ Da die Verwendungsbeschränkungsregelung in Art. 1 Abs. 4 RB-Informationsaustausch die Überprüfung bezweckt, ob die Informationen auch unter Einhaltung des justiziellen Rechtshilfeweges hätten erlangt werden können, und somit keine Rechtshilfestandards unterlaufen worden sind,⁷¹ müssen im Rahmen der Beweisverwertungsproblematik die in Umsetzung der RL EEA erfolgten rechtshilferechtlichen Voraussetzungen für die Leistung von Rechtshilfe geprüft werden. Diese Prüfung bezieht sich insbesondere darauf, ob – ggf. nach erster Auswertung des Materials – Rechtshilfeverweigerungsgründe des nationalen Rechts in Umsetzung von Art. 11 RL EEA gegeben sind. Diese Gegenrechte tariieren den Individualschutz der von der Rechtshilfe betroffenen Person und das staatliche Interesse an Strafverfolgung aus. Besonders relevant ist hier die Prüfung des rechtshilferechtlichen Grundsatzes des *ordre public*. Dadurch

⁶² Nach Art. 1 RL EEA fällt auch die bloße Übermittlung von für die Vollstreckungsbehörde (hier: Frankreich) verfügbaren Beweismitteln in den Anwendungsbereich der RL. Zu den Überschneidungen ausführlich *Lauer*, Informationshilfe im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen, 2018, S. 193.

⁶³ Zum Zweck des RB siehe Art. 1 Abs. 1 RB 2006/960/JI; *Trautmann*, in: Schomburg/Lagodny (Fn. 19), IRG Vor § 92, Rn. 9.

⁶⁴ *Böse*, Der Grundsatz der Verfügbarkeit von Informationen in der strafrechtlichen Zusammenarbeit der Europäischen Union, 2007, S. 130; *Wörner*, in: Ambos/König/Rackow (Fn. 23), HT 4, Rn. 643, 644.

⁶⁵ *Gleiß*, in: Schomburg/Lagodny (Fn. 19), III E 1 SDÜ Art. 46 Rn. 1.

⁶⁶ Zur Definition austauschbarer Informationen siehe Art. 2 lit. d RB 2006/960. Vgl. auch Leitlinien für die Umsetzung des Rahmenbeschlusses 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union, Ratsdok. 9512/3/19 REV 3 vom 1. März 2011, Anlage III, S. 52, wonach Frankreich erklärt hat, dass es alle Informationen, die im Rahmen von in Frankreich anhängigen oder abgeschlossenen administrativen oder justiziellen Ermittlungen vorliegen, weitergeben wird, sofern sie für die im RB definierten Zwecke relevant sind.

⁶⁷ Art. 1 Abs. 4 RB 2006/960. Die justizielle Genehmigung muss auch bei spontan übermittelten Informationen eingeholt werden: *Trautmann* (Fn. 63), IRG § 92b, Rn. 1; *Böse*, in: Grützner/Pötz/Kreß/Gazeas (Hrsg.), Internationaler Rechtshilfeverkehr in Strafsachen, 3. Aufl., Stand: Oktober 2013, I. 2., § 92b IRG, Rn. 1.

⁶⁸ *Trautmann* (Fn. 63), Kurzübersicht HT III B 2b, Rn. 14.

⁶⁹ *Trautmann* (Fn. 63), IRG § 92, Rn. 13.

⁷⁰ BGH NJW 2019, 2627 (2629); *Schmitt*, in: Meyer-Goßner/Schmitt, Strafprozessordnung, 64. Aufl. 2021, § 112, Rn. 5.

⁷¹ *Böse* (Fn. 67), III. A. 3.12, Rn. 4.

können „rote Linien“ des eigenen Strafverfahrensrechts exportiert werden.⁷²

c) Folgen eines Verstoßes gegen rechtshilferechtliche Prinzipien

An den beiden obergerichtlichen Beschlüssen ist richtig, dass eine EEA auch schon dann gestellt werden kann, wenn ein Strafverfahren gegen „unbekannt“ geführt wird und die Rechtshilfe die Identifizierung von Beschuldigten unterstützen kann.⁷³ Richtig ist auch, dass bei Ersuchen um bereits vorhandene Informationen die EEA auf die Verwertung von Zufallsfunden im Sinne des deutschen Rechts gerichtet werden kann.⁷⁴ Allerdings ist die von der Generalstaatsanwaltschaft Frankfurt a.M. gestellte als „Pauschalgenehmigung“ avisierte EEA mit dem rechtshilferechtlichen Ersuchensprinzip unvereinbar. Das Ersuchensprinzip definiert durch einen bestimmten Formerfordernissen unterliegenden „request“ Gegenstand und Umfang der Prüfung durch den ersuchten Staat und hat deshalb eine Begrenzungsfunktion.⁷⁵ Am Ersuchensprinzip hat sich auch nichts durch das Prinzip der gegenseitigen Anerkennung geändert, ungeachtet der Bezeichnung der Vorlage vom Ausstellungstaat an den Vollstreckungsstaat als „Anordnung“.⁷⁶ Die Darstellung muss der ersuchten Behörde die Prüfung erlauben, ob die Voraussetzungen zur Leistung von Rechtshilfe bzw. Rechthilfehindernisse gegeben sind und ob das Ersuchen bewilligt werden kann.⁷⁷ Das Ersuchen hat ferner den Sinn, dass sich der ersuchende Staat klar darüber wird, ob die Maßnahme auch nach seinem Recht zulässig ist, womit illegales forum shopping vermieden wird. Bei einer Anordnung gerichtet auf Verwendung des Informationsmaterials für alle – auch zukünftigen – Strafverfahren in Deutschland gegen EncroChat-Nutzer ist diese Begrenzungsfunktion der justiziellen Rechtshilfe jedoch nicht mehr gegeben. Insbesondere können die französischen

Justizbehörden nicht mehr die in der RL EEA gefundenen Voraussetzungen z.B. zur Verhältnismäßigkeit von Ersuchen nach Art. 6 und 10 RL EEA, geschweige denn etwaige Rechtshilfe-Gegenrechte in Art. 11 RL EEA prüfen. Die Zulassung der deutschen EEA durch die beiden OLGe negiert in letzter Konsequenz den spätestens mit der Soering-Entscheidung des EGMR anerkannten Grundsatz der dreidimensionalen Sichtweise der internationalen Strafrechtskooperation,⁷⁸ denn für die Justizbehörden bleibt gar kein Ansatz zur Prüfung. Rechtshilfe kann nur insoweit erbeten und geleistet werden, als sich ein bestimmtes Strafverfahren bereits konkretisiert hat.

Zudem widerspricht die Annahme des OLG Hamburg, für die EEA hätte es keines richterlichen Beschlusses bedurft, dem einen legitimen Beweistransfer von Telekommunikationsüberwachungen zulassenden und etablierten Prinzip der „beiderseitigen Legalität“. Art. 30, 31 RL EEA enthalten im Gegensatz zu bilateralen Rechtshilfeabkommen⁷⁹ für die Herausgabe von zuvor für eigene Verfahren erhobene TKÜ-Daten zwar keine explizite Regelung, weshalb die allgemeinen Regelungen der RL gelten, insbesondere Art. 10 Abs. 2 RL EEA. Diese Regelung für den Zugriff auf bereits verfügbare Beweismittel und Informationen im ersuchten Staat ist hingegen teleologisch dahingehend zu reduzieren, dass der bezweckte reibungslose „Beweisherausgabeverkehr“ lediglich für weniger invasive Grundrechtseingriffe anwendbar ist.⁸⁰ Ansonsten würden Friktionen zur TKÜ auf Ersuchen entstehen und ein nicht gerechtfertigtes Umgehungspotential eröffnet.⁸¹ Bei TKÜs auf Ersuchen ist es jedoch der rechtshilferechtliche Standard, dass erforderliche richterliche Genehmigungen vor Stellung des Rechtshilfeersuchens im ersuchenden Staat beizubringen sind. Ungeachtet dessen hätte die Generalstaatsanwaltschaft Frankfurt a.M. analog der für eingehende Ersuchen getroffenen Regelung in Nr. 77a Abs. 2 i.V.m. Nr. 1a RiVAST zumindest zusichern müssen, dass die Voraussetzungen der TKÜ vorlägen, wenn diese in Deutschland durchgeführt worden wäre, denn nur so kann der eherne rechtshilferechtliche Grundsatz eingehalten werden, dass ein Ersuchen nur dann zulässig und möglich ist, wenn eine entsprechende innerstaatliche Anordnung ergehen durfte.⁸² Daran bestehen aber wie unter III. ausgeführt gerade erhebliche Zweifel.

⁷² Durch das Setzen entsprechender Bedingungen können solche ordre public-Grundsätze zu einem Beweisverwertungsverbot im Empfangsstaat (also dem Forumstaat) führen. Beim Austausch von Telekommunikationsdaten zur Strafverfolgung sehen die einschlägigen Vorschriften der Beweisrechtshilfe das Setzen von Bedingungen ausdrücklich vor (siehe Art. 30 Abs. 5 und 31 Abs. 3 lit. b RL EEA). Dazu Wahl, in: Sieber/v. zur Mühlen (Fn. 9), S. 593 (595). Zur französischen Umsetzung des RB und der Möglichkeit, Bedingungen zu setzen, siehe *De Marco* (Fn. 33), S. 494.

⁷³ Das ergibt sich u.a. daraus, dass sich der Unionsgesetzgeber der Schwierigkeiten in Bezug auf die Identifizierung bei TKÜ bewusst war und sich deshalb die einschlägigen Regelungen lediglich auf die Identifiziermöglichkeit des Telekommunikationsanschlusses, nicht des Nutzers, konzentrierten. Im Übrigen verlangt Formblatt A, Abschnitt E der RL EEA Angaben zur Identität der Person nur „soweit bekannt“.

⁷⁴ BGHSt 58, 32.

⁷⁵ Grützner, in: Bassiouni/Nanda (Hrsg.), *A Treatise on International Criminal*, 1973, S. 189 (229).

⁷⁶ *Ambos/Gronke*, in: *Ambos/König/Rackow* (Fn. 23), HT 1, Rn. 14.

⁷⁷ Grützner (Fn. 75), S. 230.

⁷⁸ Ausführlich Schomburg/Lagodny (Fn. 19), Einleitung Rn. 7 ff. sowie Rn. 145 ff. zur Stellung des Individuums als Rechtssubjekt im „international-arbeitsteiligen Strafverfahren“. Zur Bedeutung des Soering-Urteils für die Rechtshilfe siehe *Lagodny*, NJW 1990, 2189.

⁷⁹ Dazu Art. 17 Abs. 5 CZ-D ErgV EuRhÜbk; Art. 16 Abs. 7 PL-D ErgV EuRhÜbk.

⁸⁰ Die Invasivität der TKÜ nicht absprechend Erwägungsgrund 30 RL EEA a.E.

⁸¹ Im Verfahren zur Umsetzung der RL EEA in Deutschland hat der Gesetzgeber (vgl. BT-Drs. 18/9757, S. 28, 43) die Problematik nicht weiterverfolgt, so dass die Rechtslage derzeit unklar ist.

⁸² *Gleiß* (Fn. 20), S. 109.

Unter Zugrundelegung der Abwägungslösung wäre vor diesem Hintergrund die Annahme eines rechtshilferechtlichen Beweisverwertungsverbots gerechtfertigt gewesen. Der Verstoß gegen grundlegende Prinzipien der Rechtshilfe ist derart gravierend, dass auch das Interesse an der Verfolgung schwererer Straftaten nicht überwiegen kann. Denn letztlich ist die eine auf Pauschalermächtigung gerichtete deutsche EEA einer sinnvollen, notwendigen Prüfung der justiziellen Rechtshilfe gar nicht zugänglich, wodurch die Position des Individuums im System der dreidimensionalen Rechtshilfe gänzlich negiert wird. Der rechtshilferechtliche Schutzstandard kann bei einer solchen EEA mangels Spezifität nicht garantiert werden.

V. Fazit

Die beiden Entscheidungen des OLG Bremen und des OLG Hamburg zum EncroChat-Fall zeigen zwei Dinge auf: Erstens haben Beschuldigte geringe Erfolgchancen vor deutschen Gerichten, die Unverwertbarkeit im Ausland erworbener Beweismittel zu erreichen.⁸³ Das liegt vor allem daran, dass die Gerichte fast blind der Leitentscheidung des BGH aus dem Jahre 2012 folgen, die durch juristische Kunstgriffe die Nichtzulassung ausländischer Beweismittel de facto ausschließt. Nicht berücksichtigt wurde jedoch, dass die BGH-Entscheidung einige Fallgruppen nicht abdeckt. Insbesondere hätte festgestellt werden müssen, dass das französische Recht in weit größerem Umfang den Einsatz technischer Mittel zur Überwachung der Telekommunikation auch gegen zunächst nicht im Verdacht einer Straftat stehende Personen wegen eines speziellen Vorermittlungsverfahrens bei Straftaten der organisierten Kriminalität erlaubt. Die entscheidende Frage, ob hier – allen Kompensationsmöglichkeiten im französischen Recht zum Trotz – die Wertungen der deutschen Quellen-TKÜ und Onlinedurchsuchung nach *ordre public*-Maßstäben noch aufrechterhalten werden können, wurde nicht beantwortet. Das geschah u.a. auch, weil es an konkreten Leitlinien fehlt, was für unsere „Rechtsstaatlichkeit“ als unverzichtbar angesehen wird. Die deutsche Rechtsprechung ist zu stark von Kasuistik, Normrelativismus und Pragmatismus geprägt.⁸⁴ An die Zuverlässigkeit eines Beweises dahingehend, ob sich die Beweisgewinnung in die Rechtsordnung des Urteilsstaates einpassen lässt, werden grundsätzlich keine

Anforderungen gestellt,⁸⁵ weshalb Friktionen zwischen Beweiserhebung und Beweisverwertung bewusst in Kauf genommen werden. Auch die Außerachtlassung des Ineinandergreifens von polizeilicher Informationsrechtshilfe und justizieller Rechtshilfe lässt eine Schiefelage entstehen. Sowohl ein *ordre public*-rechtliches als auch rechtshilferechtliches Beweisverwertungsverbot hätte angenommen werden müssen. Zu klären wäre dann gewesen, inwieweit Fernwirkungen eingreifen und die ausgewerteten Chats als Ermittlungs- und Spurenansatz zugelassen werden können.

Zweitens führt der Fall vor Augen, dass sich die Diskussion um das „Beweismittelshopping“ einer neuen Realität stellen muss. Von Seiten der Polizeibehörden mag es logisch sein, dass aus Big-Data-Analysen aufgedeckte Straftaten auch zu verfolgen sind. Von juristischer Seite muss jedoch hinterfragt werden, welche Schutzstandards des nationalen Rechts für den Betroffenen dann noch gelten sollen, wenn das gewonnene Material im Ausland anderen Vorstellungen im Hinblick auf Grundrechtseingriffe und Verhältnismäßigkeit folgt. Jedenfalls dürfte fast sicher sein, dass sich mit diesen grundlegenden Fragen weitere Gerichte, insbesondere die deutschen Höchstgerichte, noch zu befassen haben. Es wird dann spannend sein, inwieweit der EncroChat-Fall Anlass zur Entwicklung neuer Leitlinien geben wird.

⁸³ Der Linie des OLG Bremen und des OLG Hamburg folgend: OLG Schleswig, Beschl. v. 29.4.2021 – 2 Ws 47/21, und OLG Rostock, Beschl. v. 11.5.2021 – 20 Ws 121/21. Anders nun offenbar LG Berlin (siehe *Diehl/Lehberger/Meyer-Heuer*, Spiegel Online v. 2.7.2021, abrufbar unter: <https://www.spiegel.de/panorama/justiz/berlin-landgericht-laesst-encrochat-daten-nicht-zu-a-6dd9be2e-f558-40fa-9995-2f8136581f8e>). Kritisch zum Ansatz der bisherigen oberlandesgerichtlichen Entscheidungen zu den EncroChat-Fällen aus Verteidigersicht *Sommer*, StV Spezial 2021, 67; *Stehr/Rackow*, StRR 2021, 6 (11).

⁸⁴ *Gleiß*, ZStW 125 (2013), 573 (581); *Hackner*, in: Schomburg/Lagodny (Fn. 19), IRG Vor § 68, Rn. 11e.

⁸⁵ *Gleiß* (Fn. 20), S. 120, 140; *dies.*, ZStW 125 (2013), 573 (580); *Heger*, ZIS 2007, 547 (552).