HRRS-Nummer: HRRS 2022 Nr. 1047
Bearbeiter: Karsten Gaede/Julia Heß
Zitiervorschlag: HRRS 2022 Nr. 1047, Rn. X

LG Berlin (525 KLs) 279 Js 30/22 (8/22) - Beschluss vom 19. Oktober 2022

EncroChat; Vorabentscheidungsverfahren; Telekommunikationsüberwachung (Quellen-TKÜ; kleine Online-Durchsuchung; Online-Durchsuchung; EncroChat); Richtlinie über die Europäische Ermittlungsanordnung in Strafsachen (EncroChat; Anordnungsbehörde: Auslegung, Zuständigkeit; materielle Anforderungen an eine Europäische Ermittlungsanordnung zur Beweisübermittlung: Erlass der EEA notwendig und verhältnismäßig, Verdachtsintensität, Wertungen hinsichtlich der Verhältnismäßigkeit der Vorratsdatenspeicherung, Recht auf ein faires Verfahren, Akteneinsicht, hypothetische Rechtmäßigkeitsprüfung nach innerstaatlichem Recht, noch zu vollstreckende Beweiserhebung, Transfer vorhandener Beweise, „Befugnisshopping"; Unterrichtung des Mitgliedstaats, in dem sich die Zielperson befindet: zuständige Behörde, Schutzrichtung, Verwertungsverbot; Rechtsfolgen einer unionsrechtswidrigen Beweiserlangung: Verfahrensautonomie, Beweisverwertungsverbot, Beweiswürdigung, Strafzumessung, Effektivitätsgrundsatz, Grundsatz der Äquivalenz, umfassende Interessenabwägung).

§ 100a StPO; § 100b StPO; § 100e StPO; § 91g IRG; Art. 267 AEUV; Art. 6 Richtlinie 2014/41; Art. 31 Richtlinie 2014/41; Art 6 Abs. 1 EMRK; Art. 8 EMRK; Art. 7 GRCh; Art. 47 Abs. 2 GRCh

Leitsätze des Bearbeiters

Zur Auslegung der Richtlinie 2014/41 (im Folgenden: RL EEA) im Zusammenhang mit „EncroChat" werden dem Gerichtshof der Europäischen Union im Wege des Vorabentscheidungsverfahren folgende Fragen vorgelegt:

1. Muss eine Europäische Ermittlungsanordnung (im Folgenden: EEA) zur Erlangung von Beweismitteln, die sich bereits im Vollstreckungsstaat (hier: Frankreich) befinden, von einem Richter erlassen werden, wenn nach dem Recht des Anordnungsstaats (hier: Deutschland) in einem vergleichbaren innerstaatlichen Fall die zugrunde liegende Beweiserhebung durch den Richter hätte angeordnet werden müssen?

2. Gilt dies hilfsweise zumindest dann, wenn der Vollstreckungsstaat die zugrunde liegende Maßnahme auf dem Hoheitsgebiet des Anordnungsstaats durchgeführt hat mit dem Ziel, die abgeschöpften Daten anschließend den an den Daten interessierten Ermittlungsbehörden im Anordnungsstaat zum Zweck der Strafverfolgung zur Verfügung zu stellen?

3. Muss eine EEA zur Erlangung von Beweismitteln unabhängig von den nationalen Zuständigkeitsregelungen des Anordnungsstaats immer dann von einem Richter (bzw. einer unabhängigen, nicht mit strafrechtlichen Ermittlungen befassten Stelle) erlassen werden, wenn die Maßnahme schwerwiegende Eingriffe in hochrangige Grundrechte betrifft?

4. Steht Art. 6 Abs. 1 lit. a) RL EEA einer EEA zur Übermittlung von im Vollstreckungsstaat (Frankreich) schon vorhandenen Daten aus einer Telekommunikationsüberwachung - insbesondere Verkehrs- und Standortdaten sowie Aufzeichnungen von Kommunikationsinhalten - entgegen, wenn die vom Vollstreckungsstaat durchgeführte Überwachung sich auf sämtliche Anschlussnutzer eines Kommunikationsdienstes erstreckte, mit der EEA die Übermittlung der Daten sämtlicher auf dem Hoheitsgebiet des Anordnungsstaates genutzten Anschlüsse begehrt wird und weder bei der Anordnung und Durchführung der Überwachungsmaßnahme noch bei Erlass der EEA konkrete Anhaltspunkte für die Begehung von schweren Straftaten durch diese individuellen Nutzer bestanden?

5. Steht Art. 6 Abs. 1 lit. a) RL EEA einer solchen EEA entgegen, wenn die Integrität der durch die Überwachungsmaßnahme abgeschöpften Daten wegen umfassender Geheimhaltung durch die Behörden im Vollstreckungsstaat nicht überprüft werden kann?

6. Steht Art. 6 Abs. 1 lit. b) RL EEA einer EEA zur Übermittlung von im Vollstreckungsstaat (Frankreich) schon vorhandenen Telekommunikationsdaten entgegen, wenn die der Datenerhebung zugrunde liegende Überwachungsmaßnahme des Vollstreckungsstaats nach dem Recht des Anordnungsstaats (Deutschland) in einem vergleichbaren innerstaatlichen Fall unzulässig gewesen wäre?

7. Hilfsweise: Gilt dies jedenfalls dann, wenn der Vollstreckungsstaat die Überwachung auf dem Hoheitsgebiet des Anordnungsstaats und in dessen Interesse durchgeführt hat?

8. Handelt es sich bei einer mit der Infiltration von Endgeräten verbundenen Maßnahme zur Abschöpfung von Verkehrs-, Standort- und Kommunikationsdaten eines internetbasierten Kommunikationsdienstes um eine Überwachung des Telekommunikationsverkehrs im Sinne von Art. 31 RL EEA?

9. Muss die Unterrichtung nach Art. 31 Abs. 1 RL EEA stets an einen Richter gerichtet werden oder gilt dies zumindest dann, wenn die vom überwachenden Staat (Frankreich) geplante Maßnahme nach dem Recht des unterrichteten Staats (Deutschland) in einem vergleichbaren innerstaatlichen Fall nur durch einen Richter angeordnet werden könnte?

10. Soweit Art. 31 RL EEA auch dem Individualschutz der betroffenen Telekommunikationsnutzer dient, erstreckt sich dieser auch auf die Verwendung der Daten zur Strafverfolgung im unterrichteten Staat (Deutschland) und ist gegebenenfalls dieser Zweck gleichwertig mit dem weiteren Zweck, die Souveränität des unterrichteten Mitgliedsstaats zu schützen?

11. Kann sich bei einer Beweismittelerlangung durch eine unionsrechtswidrige EEA unmittelbar aus dem unionsrechtlichen Effektivitätsgrundsatz ein Beweisverwertungsverbot ergeben?

12. Führt bei einer Beweismittelerlangung durch eine unionsrechtswidrige EEA der unionsrechtliche Äquivalenzgrundsatz zu einem Beweisverwertungsverbot, wenn die der Beweisgewinnung im Vollstreckungsstaat zugrunde liegende Maßnahme in einem vergleichbaren innerstaatlichen Fall im Anordnungsstaat nicht hätte angeordnet werden dürfen und die durch eine solche rechtswidrige innerstaatliche Maßnahme gewonnenen Beweise nach dem Recht des Anordnungsstaats nicht verwertbar wären?

13. Verstößt es gegen Unionsrecht, insbesondere den Grundsatz der Effektivität, wenn die strafprozessuale Verwertung von Beweismitteln, deren Erlangung gerade wegen eines fehlenden Tatverdachts unionsrechtswidrig war, im Rahmen einer Interessenabwägung mit der Schwere der erstmals durch die Auswertung der Beweismittel bekannt gewordenen Taten gerechtfertigt wird?

14. Hilfsweise: Ergibt sich aus dem Unionsrecht, insbesondere dem Grundsatz der Effektivität, dass Unionsrechtsverstöße bei der Beweismittelerlangung in einem nationalen Strafverfahren auch bei schweren Straftaten nicht vollständig ohne Folge bleiben dürfen und daher zumindest auf der Ebene der Beweiswürdigung oder der Strafzumessung zugunsten des Beschuldigten berücksichtigt werden müssen?

Entscheidungstenor

I. Dem Gerichtshof der Europäischen Union werden nach Art. 267 AEUV folgende Fragen zur Auslegung der Richtlinie 2014/41 (im Folgenden: RL EEA) vorgelegt:

1. Zur Auslegung des Merkmals „Anordnungsbehörde“ nach Art. 6 Abs. 1 i.V.m. Art. 2 lit. c) RL EEA

a) Muss eine Europäische Ermittlungsanordnung (im Folgenden: EEA) zur Erlangung von Beweismitteln, die sich bereits im Vollstreckungsstaat (hier: Frankreich) befinden, von einem Richter erlassen werden, wenn nach dem Recht des Anordnungsstaats (hier: Deutschland) in einem vergleichbaren innerstaatlichen Fall die zugrunde liegende Beweiserhebung durch den Richter hätte angeordnet werden müssen?

b) Gilt dies hilfsweise zumindest dann, wenn der Vollstreckungsstaat die zugrunde liegende Maßnahme auf dem Hoheitsgebiet des Anordnungsstaats durchgeführt hat mit dem Ziel, die abgeschöpften Daten anschließend den an den Daten interessierten Ermittlungsbehörden im Anordnungsstaat zum Zweck der Strafverfolgung zur Verfügung zu stellen?

c) Muss eine EEA zur Erlangung von Beweismitteln unabhängig von den nationalen Zuständigkeitsregelungen des Anordnungsstaats immer dann von einem Richter (bzw. einer unabhängigen, nicht mit strafrechtlichen Ermittlungen befassten Stelle) erlassen werden, wenn die Maßnahme schwerwiegende Eingriffe in hochrangige Grundrechte betrifft?

2. Zur Auslegung von Art. 6 Abs. 1 lit. a) RL EEA

a) Steht Art. 6 Abs. 1 lit. a) RL EEA einer EEA zur Übermittlung von im Vollstreckungsstaat (Frankreich) schon vorhandenen Daten aus einer Telekommunikationsüberwachung - insbesondere Verkehrs- und Standortdaten sowie Aufzeichnungen von Kommunikationsinhalten - entgegen, wenn die vom Vollstreckungsstaat durchgeführte Überwachung sich auf sämtliche Anschlussnutzer eines Kommunikationsdienstes erstreckte, mit der EEA die Übermittlung der Daten sämtlicher auf dem Hoheitsgebiet des Anordnungsstaates genutzten Anschlüsse begehrt wird und weder bei der Anordnung und Durchführung der Überwachungsmaßnahme noch bei Erlass der EEA konkrete Anhaltspunkte für die Begehung von schweren Straftaten durch diese individuellen Nutzer bestanden?

b) Steht Art. 6 Abs. 1 lit. a) RL EEA einer solchen EEA entgegen, wenn die Integrität der durch die

Überwachungsmaßnahme abgeschöpften Daten wegen umfassender Geheimhaltung durch die Behörden im Vollstreckungsstaat nicht überprüft werden kann?

3. Zur Auslegung von Art. 6 Abs. 1 lit. b) RL EEA

a) Steht Art. 6 Abs. 1 lit. b) RL EEA einer EEA zur Übermittlung von im Vollstreckungsstaat (Frankreich) schon vorhandenen Telekommunikationsdaten entgegen, wenn die der Datenerhebung zugrunde liegende Überwachungsmaßnahme des Vollstreckungsstaats nach dem Recht des Anordnungsstaats (Deutschland) in einem vergleichbaren innerstaatlichen Fall unzulässig gewesen wäre?

b) Hilfsweise: Gilt dies jedenfalls dann, wenn der Vollstreckungsstaat die Überwachung auf dem Hoheitsgebiet des Anordnungsstaats und in dessen Interesse durchgeführt hat?

4. Zur Auslegung von Art. 31 Abs. 1, Abs. 3 RL EEA

a) Handelt es sich bei einer mit der Infiltration von Endgeräten verbundenen Maßnahme zur Abschöpfung von Verkehrs-, Standort- und Kommunikationsdaten eines internetbasierten Kommunikationsdienstes um eine Überwachung des Telekommunikationsverkehrs im Sinne von Art. 31 RL EEA?

b) Muss die Unterrichtung nach Art. 31 Abs. 1 RL EEA stets an einen Richter gerichtet werden oder gilt dies zumindest dann, wenn die vom überwachenden Staat (Frankreich) geplante Maßnahme nach dem Recht des unterrichteten Staats (Deutschland) in einem vergleichbaren innerstaatlichen Fall nur durch einen Richter angeordnet werden könnte?

c) Soweit Art. 31 RL EEA auch dem Individualschutz der betroffenen Telekommunikationsnutzer dient, erstreckt sich dieser auch auf die Verwendung der Daten zur Strafverfolgung im unterrichteten Staat (Deutschland) und ist gegebenenfalls dieser Zweck gleichwertig mit dem weiteren Zweck, die Souveränität des unterrichteten Mitgliedsstaats zu schützen?

5. Rechtsfolgen einer unionsrechtswidrigen Beweiserlangung

a) Kann sich bei einer Beweismittelerlangung durch eine unionsrechtswidrige EEA unmittelbar aus dem unionsrechtlichen Effektivitätsgrundsatz ein Beweisverwertungsverbot ergeben?

b) Führt bei einer Beweismittelerlangung durch eine unionsrechtswidrige EEA der unionsrechtliche Äquivalenzgrundsatz zu einem Beweisverwertungsverbot, wenn die der Beweisgewinnung im Vollstreckungsstaat zugrunde liegende Maßnahme in einem vergleichbaren innerstaatlichen Fall im Anordnungsstaat nicht hätte angeordnet werden dürfen und die durch eine solche rechtswidrige innerstaatliche Maßnahme gewonnenen Beweise nach dem Recht des Anordnungsstaats nicht verwertbar wären?

c) Verstößt es gegen Unionsrecht, insbesondere den Grundsatz der Effektivität, wenn die strafprozessuale Verwertung von Beweismitteln, deren Erlangung gerade wegen eines fehlenden Tatverdachts unionsrechtswidrig war, im Rahmen einer Interessenabwägung mit der Schwere der erstmals durch die Auswertung der Beweismittel bekannt gewordenen Taten gerechtfertigt wird?

d) Hilfsweise: Ergibt sich aus dem Unionsrecht, insbesondere dem Grundsatz der Effektivität, dass Unionsrechtsverstöße bei der Beweismittelerlangung in einem nationalen Strafverfahren auch bei schweren Straftaten nicht vollständig ohne Folge bleiben dürfen und daher zumindest auf der Ebene der Beweiswürdigung oder der Strafzumessung zugunsten des Beschuldigten berücksichtigt werden müssen?

II. Es wird beantragt, über das Vorabentscheidungsersuchen im beschleunigten Verfahren, hilfsweise mit Vorrang zu entscheiden.

Gründe

A. Gegenstand und Sachverhalt des Ausgangsverfahrens

I. Verfahrensgegenstand und Erheblichkeit der Vorlagefragen

Die Staatsanwaltschaft Berlin legt dem Angeklagten vierzehn Fälle des unerlaubten Handeltreibens mit Betäubungsmittel in nicht geringer Menge sowie vier Fälle des unerlaubten Besitzes von Betäubungsmitteln in nicht geringer Menge in Deutschland zur Last. Zwischen dem 3. April 2020 und dem 27. Mai 2020 soll er im Berliner Stadtgebiet ca. 188 kg Marihuana und 3,25 kg Kokain gekauft, verkauft und verwahrt haben. Zur Abwicklung seiner Handelstätigkeiten soll er sich des als besonders abhörsicher beworbenen Kommunikationsdienstes „EncroChat“ bedient und darüber per Chat- und Bildnachrichten kommuniziert haben. 1

Die Kammer hat die Hauptverhandlung ausgesetzt, nachdem der Angeklagte sich zum Tatvorwurf nicht eingelassen und die Vorlage an den Gerichtshof der Europäischen Union angeregt hat. 2

Die Verurteilung des Angeklagten hängt maßgeblich von der Antwort des Gerichtshofs auf die Vorlagefragen ab. Die Anklagevorwürfe beruhen im Wesentlichen auf mutmaßlich von dem Angeklagten verfassten bzw. an ihn übermittelten Text- und Bildnachrichten, die nach Aktenlage mit hoher Wahrscheinlichkeit im Wesentlichen die in der Anklage beschriebenen Handelsgeschäfte zum Gegenstand haben und seine Identifizierung ermöglichen würden. Mit Hilfe des Vorabentscheidungsersuchens möchte die Kammer klären, ob die deutschen Ermittlungsbehörden bei der Erlangung der Daten gegen Regelungen der Richtlinie 2014/41 (im Folgenden: RL EEA) verstoßen haben und ob gegebenenfalls die Verstöße die Verwertung der Daten im Strafverfahren - mit der Folge eines Freispruchs - hindern bzw. sich auf andere Weise auf den Urteilsspruch auswirken müssen. 3

II. Sachverhalt

1. Gang der Ermittlungen

Auf der Grundlage der von den Ermittlungsbehörden übermittelten - allerdings unvollständigen - Akten, der von der Verteidigung eingereichten ergänzenden Unterlagen sowie der Beweisaufnahme in der ausgesetzten Hauptverhandlung stellt sich der für die Vorlagefragen entscheidungserhebliche Sachverhalt wie folgt dar: 4

a) Die französischen Ermittlungsbehörden stellten ab dem Jahr 2017 in mehreren Verfahren fest, dass Beschuldigte bei der Begehung von Straftaten, überwiegend aus dem Bereich der Betäubungsmittelkriminalität, Krypto-Handys des Anbieters „EncroChat“ nutzten. Diese Mobiltelefone ermöglichten mit einer speziellen Software und einer modifizierten Hardware über einen in Roubaix stationierten Server eine Ende-zu-Ende-verschlüsselte Kommunikation, die mit herkömmlichen Ermittlungsmethoden nicht zu überwachen war. 5

Mit richterlicher Genehmigung gelang es der französischen Polizei in den Jahren 2018 und 2019, Images der Serverdaten zu sichern. Auf der Grundlage der daraus gewonnenen Erkenntnisse wurde in Zusammenarbeit mit niederländischen Experten im Rahmen einer gemeinsamen Ermittlungsgruppe (Joint Investigation Team - im Folgenden: JIT) eine Trojaner-Software entwickelt, die mit Genehmigung des Strafgerichts Lille im Frühjahr 2020 auf den Server in Roubaix aufgespielt und von dort aus über ein simuliertes Update auf den Endgeräten installiert wurde. Insgesamt waren von der Maßnahme 32.477 Nutzer (von insgesamt 66.134 eingetragenen Nutzern) in 122 Ländern betroffen, darunter 380 Nutzer in Frankreich und ca. 4.600 Nutzer in Deutschland. 6

Zwischen dem 1. April 2020 und dem 28. Juni 2020 ermöglichte es die Trojaner-Software den französischen Behörden, die Gerätekennungen (IMEIs) der in den jeweiligen Ländern festgestellten Endgeräte, E-Mail-Adressen, Datum und Uhrzeit der Kommunikation, den Standort des Funkmastes, über den das Endgerät eingebucht war, sowie die in den laufenden Chats übermittelten Texte und Bilder abzufangen. Außerdem wurden die Gerätespeicher einschließlich der dort noch nicht gelöschten Chats aus der Zeit vor dem 1. April 2020 ausgelesen. 7

Soweit die Endgeräte sich im Ausland befanden, wurden die abgeschöpften Daten ab dem 3. April 2020 einer Reihe von nationalen Ermittlungsbehörden, u.a. dem deutschen Bundeskriminalamt (im Folgenden: BKA), laufend über einen Europol-Server zur Verfügung gestellt. 8

b) Das BKA hatte seit 2018 Erkenntnisse, dass in Deutschland EncroChat-Telefone bei der Begehung von schweren Straftaten insbesondere aus dem Betäubungsmittelbereich genutzt wurden. Ab Anfang des Jahres 2020 wurden Gespräche zwischen dem BKA und der Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) bei der Generalstaatsanwaltschaft Frankfurt am Main (im Folgenden: GStA Frankfurt) über die Möglichkeit von Ermittlungsmaßnahmen gegen die deutschen EncroChat-Nutzer geführt. 9

Am 9. März 2020 nahmen Vertreter des BKA und der GStA Frankfurt zusammen mit Vertretern französischer, niederländischer, britischer, europäischer und weiterer Behörden an einer Eurojust-Videokonferenz teil, auf der die französischen und niederländischen Vertreter die Vertreter der anderen Länder über die von der französischen Polizei geplante Überwachungsmaßnahme und die beabsichtigte Datenübermittlung an die anderen Länder informierten. Die deutschen Behördenvertreter signalisierten ihr Interesse an den Daten der deutschen Nutzer. 10

In einem Vermerk vom 13. März 2020 regte das BKA ein Ermittlungsverfahren gegen sämtliche unbekannten Nutzer des EncroChat-Dienstes wegen des Verdachts des bandenmäßigen Handeltreibens mit Betäubungsmitteln in nicht geringer Menge und der Bildung einer kriminellen Vereinigung an. Zur Begründung führte das BKA aus, die Nutzung eines EncroChat-Handys begründe einen Anfangsverdacht für die Begehung erheblicher Straftaten insbesondere des Betäubungsmittelhandels. Angesichts der konkreten Funktionen der Geräte und der hohen Kosten von 1.000 bis 2.000 € scheide eine legale Nutzung aus; dies werde durch die in früheren Strafverfahren festgestellte Nutzung von insgesamt ca. 300 EncroChat-Geräten bei der Begehung von Straftaten bestätigt. 11

Auf der Grundlage dieses Vermerks leitete die GStA Frankfurt am 20. März 2020 unter „Eilt“ ein entsprechendes Ermittlungsverfahren gegen Unbekannt (Az. 62 UJs 50005/20 - im Folgenden: UJs-Verfahren) ein. Ermittlungsmaßnahmen wurden zunächst nicht ergriffen oder beim Ermittlungsrichter beantragt. 12

Am 27. März 2020 erhielt das BKA über das europäische SIENA-Nachrichtensystem eine an die Polizeibehörden der an den EncroChat-Daten interessierten Länder gerichtete Nachricht des JIT in englischer Sprache. Darin wurden die zuständigen Behörden („competent authorities“) der an der Datenübermittlung interessierten Länder aufgefordert, schriftlich zu bestätigen, dass sie über die zur Datengewinnung von Geräten auf ihrem Staatsgebiet („from devices in their jurisdiction“) angewandten Methoden informiert worden seien. Zugleich sollte zugesichert werden, dass die grundsätzlich zunächst nur zu Auswertezwecken übermittelten Daten für laufende Ermittlungsverfahren nur nach Genehmigung durch die JIT-Länder verwendet würden. 13

In Absprache mit der GStA Frankfurt erteilte das BKA die in der Nachricht erbetenen Zustimmungen und Bestätigungen. Zu einer Unterrichtung durch die französischen Behörden nach Art. 31 Abs. 1 RL EEA, § 91 g IRG kam es nicht; von deutscher Seite wurde dies auch nicht beanstandet. 14

In der Zeit vom 3. April 2020 bis zum 28. Juni 2020 rief das BKA die täglich auf dem Europol-Server bereitgestellten Daten der in Deutschland genutzten Endgeräte ab. Nachdem die Datenauswertung einen konkreten Tatverdacht gegen einige Nutzer ergeben hatte, ersuchte das BKA die französische Staatsanwaltschaft mit Schreiben vom 13. Mai 2020 um die Genehmigung, noch während der laufenden Maßnahme einzelne Beschlüsse zur Identifizierung beim Ermittlungsrichter beantragen zu dürfen; es werde versucht werden, die Beschlüsse ohne jeglichen Hinweis auf den Gegenstand des französischen Verfahrens und die Art der Maßnahme zu erlangen, und im Fall einer Verfahrensabtrennung werde die Akte in dem neuen Ermittlungsverfahren gegen den einzelnen Nutzer mit einem richterlichen Beschluss beginnen, der keinen Rückschluss auf das französische Ermittlungsverfahren ermögliche. Nach Erteilung der erbetenen Genehmigung erwirkte die GStA Frankfurt sodann einzelne richterliche Beschlüsse für die Erhebung von Standortdaten und andere Ermittlungsmaßnahmen. 15

Am 2. Juni 2020 ersuchte die Generalstaatsanwaltschaft Frankfurt am Main im Rahmen des UJs-Verfahrens die französischen Behörden mittels EEA um die Genehmigung, die EncroChat-Daten unbeschränkt in Strafverfahren verwenden zu können. Zur Begründung wurde ausgeführt, das BKA sei über Europol informiert worden, dass in Deutschland eine Vielzahl schwerster Straftaten (insbesondere Einfuhr und Handeltreiben mit Betäubungsmitteln in nicht geringen Mengen) unter Nutzung von Mobiltelefonen mit der Verschlüsselungssoftware ‚EncroChat‘ begangen würden; es bestehe der Verdacht, dass bisher nicht identifizierte Personen in Deutschland unter Nutzung kryptierter Kommunikationsmittel schwerste Straftaten planten und begingen. Das Strafgericht Lille genehmigte daraufhin die Übermittlung und gerichtliche Verwendung der EncroChat-Daten der deutschen Nutzer. Ob es sodann zu einer erneuten Übermittlung von zuvor schon zu Auswertezwecken vom Europol-Server abgerufenen Daten kam, blieb bislang offen. Auf der Grundlage zweier ergänzender EEAs vom 9. September 2020 und 2. Juli 2021 wurden allerdings in der Folge zusätzliche Daten übermittelt. 16

In der Folgezeit trennte die GStA Frankfurt Verfahren gegen einzelne Nutzer, darunter auch den hiesigen Angeklagten, aus dem UJs-Vorgang ab und gab sie an lokale Staatsanwaltschaften ab. 17

c) Auch wenn die Datenabschöpfung maßgeblich von französischen Behörden und auf der Grundlage von französischen Gerichtsbeschlüssen durchgeführt wurde, handelte es sich von vornherein nicht um eine rein innerfranzösische Ermittlungsmaßnahme, sondern um ein europäisches Projekt. Dessen Ziel war es, den EncroChat-Dienst zu zerschlagen, dessen Betreiber zu verfolgen und eine Strafverfolgung aller europäischen Nutzer in deren jeweiligen Heimatländern zu ermöglichen. 18

Die Ermittlungen wurden bereits seit 2018 von den französischen und niederländischen Behörden gemeinsam geführt, von Eurojust im Rahmen einer Gemeinsamen Ermittlungsgruppe (JIT) koordiniert und von Europol umfangreich in technischer, organisatorischer und finanzieller Hinsicht unterstützt (vgl. die gemeinsame Pressemitteilung von Eurojust und Europol vom 2. Juli 2020, abrufbar unter https://www.eurojust.europa.eu/sites/default/files/Press/2020-07-02_joint-Eurojust-Europol-press-release_FR.pdf). 19

Die federführende Rolle der französischen Behörden ergab sich lediglich daraus, dass sich der EncroChat-Server, auf den im Laufe der Ermittlungen mehrfach zugegriffen werden musste, in Frankreich befand. Eine Strafverfolgung der Nutzer war von den französischen Behörden nur beabsichtigt, soweit die Nutzer sich in Frankreich befanden. Allein die Verfolgung der lediglich 380 französischen Nutzer hätte zudem den mit der Infiltrierung des Systems verbundenen immensen Aufwand nicht gerechtfertigt (vgl. den Bericht der englischen Ermittlungsführerin E. S. auf der CPS-/NCA-Besprechung vom 13. Februar 2020, Ziff. 8 des Protokolls); dieser lohnte sich nur vor dem Hintergrund, dass das Implantat zugleich auf die Geräte der Nutzer in anderen Mitgliedstaaten aufgebracht werden konnte. An den Daten dieser im Ausland ansässigen Nutzer hatten die französischen Behörden zu keinem Zeitpunkt ein eigenes Interesse. Vielmehr war von Anfang an beabsichtigt, diese Daten den jeweiligen Heimatländern zu überlassen, sofern sie vorab ihr Interesse bekundet und den Bedingungen des JIT zugestimmt hatten. Dabei war bereits die technisch aufwändige, länderübergreifend und mit Unterstützung von Europol realisierte Entwicklung der Trojaner-Software von der Erwartung getragen, dass ein erheblicher Teil der Mitgliedstaaten von der Möglichkeit des Datenabrufs Gebrauch machen würde. 20

Vor diesem Hintergrund kommt die Abschöpfung und Speicherung der EncroChat-Daten einer gemeinsamen Maßnahme 21

aller an den Daten interessierten Länder nahe. Deren Durchführung stellt sich hinsichtlich der nicht in Frankreich ansässigen Nutzer als eine Art „Geschäftsführung“ der französischen Behörden für die anderen Staaten dar, die von den französischen Behörden im Rahmen der Eurojust-Konferenz am 9. März 2020 und der nachfolgenden Kommunikation über das SIENA-System den anderen Staaten unter den in der SIENA-Nachricht vom 27. März 2020 niedergelegten Bedingungen angeboten wurde; mit ihrer Antwort auf die Nachricht haben die anderen Staaten der „Geschäftsführung“ zugestimmt und sich damit an der Maßnahme beteiligt.

d) Die Einleitung des deutschen UJs-Verfahrens durch die GStA Frankfurt stand in direktem Zusammenhang mit den französischen Ermittlungen und der von den französischen Behörden angebotenen „Geschäftsführung“. Sie geschah in der Hoffnung, zeitnah von dort Daten zu erhalten, und mit dem Ziel, einen rechtlichen Rahmen für die Entgegennahme dieser Daten zu schaffen. Dies wurde von der mit der Verfahrenseinleitung befassten Teamleiterin bei der GStA Frankfurt in der Hauptverhandlung so bekundet und wird bestätigt durch die zeitliche Nähe zu der Eurojust-Konferenz vom 9. März 2020 sowie den Umstand, dass trotz der Einleitung unter „Eilt!“ zunächst keine eigenen Ermittlungsmaßnahmen ergriffen wurden, sondern die Auswertung der französischen Daten abgewartet wurde. 22

e) Dass sich die Überwachungsmaßnahme nicht auf das französische Staatsgebiet beschränken würde, sondern Endgeräte auf deutschem Staatsgebiet infiltriert werden sollten, war den deutschen Ermittlungsbehörden von Anfang an entweder bekannt oder sie verschlossen vor dieser Möglichkeit und deren rechtlichen Konsequenzen die Augen. 23

Welche Informationen die französischen Behörden den deutschen vor Beginn der Maßnahme im Einzelnen übermittelten, lässt sich nicht feststellen, da die entsprechende Kommunikation nicht zur Verfahrensakte gelangte, das BKA die Herausgabe verweigert und auch im Übrigen von der GStA Frankfurt keine vollständigen Akten übermittelt wurden. Die Kammer ist daher auf die Auswertung der von der Verteidigung eingereichten Unterlagen verwiesen. Danach liegt es fern, dass die deutschen Ermittlungsbehörden irrtümlich von einer rein auf das französische Staatsgebiet beschränkten Maßnahme ohne Endgerätezugriff in Deutschland ausgegangen sein könnten. Soweit Ermittlungsbeamte in der Hauptverhandlung bekundet haben, sie hätten an eine „Server-Überwachung“ gedacht, blieben ihre Angaben, was genau sie darunter verstanden hätten und worauf sich ihre Einschätzung stütze, sehr vage und überzeugten nicht. 24

Dass der Zugriff auf die Kommunikationsinhalte ohne Infiltrierung der Endgeräte nicht möglich sein würde, drängte sich nach den mehrjährigen polizeilichen Erfahrungen mit den Problemen der Überwachung verschlüsselter Kommunikation auf. Für ein etwaiges Vertrauen darauf, dass ausgerechnet im Fall des auf ein besonders hohes Sicherheitsniveau ausgerichteten EncroChat-Dienstes eine Überwachung der Kommunikation ohne Endgerätezugriff allein auf französischem Staatsgebiet durchgeführt werden könnte, gab es keine Grundlage. 25

Der geplante Zugriff auf die Endgeräte ging zudem auch aus der dem BKA übermittelten und in Absprache mit der GStA Frankfurt von diesem beantworteten SIENA-Nachricht vom 27. März 2020 hervor. Darin wurden die zuständigen Behörden der beteiligten Länder aufgefordert zu bestätigen, dass sie über die zur Datengewinnung „from devices in their jurisdiction“, d.h. von Geräten auf ihrem Staatsgebiet, angewandten Methoden informiert worden seien. Bereits der Wortlaut der Nachricht wies unmissverständlich auf den Endgerätezugriff hin. Bei einer auf das französische Staatsgebiet beschränkten Maßnahme wäre zudem die Bedeutung, die das JIT der Information der Behörden der beteiligten Länder und deren Bestätigung durch diese beimaß, nicht nachvollziehbar gewesen. 26

Die Notizen der britischen Staatsanwaltschaft (NCA) zu einer Europol-Konferenz vom 19. bis 21. Februar 2020 belegen, dass der Zugriff auf die Endgeräte mittels einer Software auch gegenüber solchen Ländern offen kommuniziert wurde, die - wie Großbritannien - nicht Mitglied des JIT waren. Nach dem offiziellen Protokoll der Europol-Konferenz machten die Mitglieder des JIT die Datenübermittlung zudem davon abhängig, dass die teilnehmenden Länder den Zugriff auf die Daten aus ihren Staatsgebieten durch die nach nationalem Recht erforderlichen Genehmigungen rechtlich absicherten; in Großbritannien geschah dies Anfang März durch einen „Targeted Equipment Interception (TEI) Warrant“ (d.h. die Genehmigung zum Zugriff auf Geräte zur Ausspähung von Daten). Auch dies zeigt, dass die vollständige und wahrheitsgemäße Information der anderen Staaten im Interesse des JIT lag, und spricht dagegen, dass Informationen vor den deutschen Ermittlungsbehörden zurückgehalten wurden. 27

Sofern gleichwohl bei den deutschen Ermittlungsbehörden noch Unklarheiten über den Ort des Datenzugriffs bestanden hätten, wäre angesichts der offensichtlichen rechtlichen Relevanz dieser Frage zu erwarten gewesen, dass dies innerhalb der Behörden diskutiert worden und gegebenenfalls Nachfragen an das JIT gestellt worden wären. Solche Diskussionen und Nachfragen hat es jedoch nach Auskunft der in der Hauptverhandlung gehörten Ermittlungsbeamten nicht gegeben. 28

2. Geheimhaltung durch die beteiligten Behörden

Technische Einzelheiten zur Funktion der Trojaner-Software und der Speicherung, Zuordnung und Filterung der Daten durch die französischen Behörden bzw. Europol sind nicht bekannt. Die Funktionsweise der Trojaner-Software unterliegt grundsätzlich dem französischen Militärgeheimnis. Inwieweit Informationen, die nicht diesem Geheimnis unterfallen, an die deutschen Behörden weitergegeben wurden, ist nicht abschließend überprüfbar, weil das BKA, die Generalstaatsanwaltschaft und die europäischen Agenturen insoweit keine Akteneinsicht gewähren. 29

Aus der mindestens 1836 Seiten umfassenden UJs-Akte, aus der das Verfahren gegen den hiesigen Angeklagten abgetrennt wurde, wurde von der GStA Frankfurt bisher nur ein kleiner Teil von 122 Seiten übermittelt; dieser enthält zu internationalen Kontakten vor Beginn der Maßnahme keine Angaben. Die gesamte Kommunikation zwischen dem BKA und Europol bzw. Eurojust wurde ohnehin nicht zu den Akten genommen. Das BKA hält diese zurück mit der Begründung, es handele sich um polizeiinterne Vorgänge. Da Eurojust ebenfalls unter Berufung auf Geheimhaltungsinteressen keine Unterlagen zu Arbeitstreffen, insbesondere zu der Videokonferenz am 9. März 2020, übermittelt, lässt sich auch nicht verlässlich klären, welche Informationen den deutschen Behördenvertretern dort gegeben wurden. Auch die Frage, inwieweit die deutschen Ermittlungsbehörden schon vor der Eurojust-Konferenz am 9. März 2020 in die federführend von den französischen Behörden betriebene Überwachungsmaßnahme eingebunden waren, lässt sich auf diese Weise nicht abschließend beantworten. 30

Die Geheimhaltung der Kommunikation mit Europol und Eurojust führte dazu, dass zahlreiche mit Haftentscheidungen befasste deutsche Oberlandesgerichte unzutreffend davon ausgingen, die Daten seien an die deutschen Behörden „spontan“ und ohne deutsche Veranlassung bzw. Beteiligung an der Datenabschöpfung übermittelt worden (vgl. etwa OLG Bremen, Beschluss vom 18. Dezember 2020 - 1 Ws 166/20 -, juris Rn. 23, 27, 29; OLG Schleswig, Beschluss vom 29. April 2021 - 2 Ws 47/21 -, juris Rn. 22; OLG Brandenburg, Beschlüsse vom 9. August 2021 - 2 Ws 113/21 -, juris Rn. 14, und vom 16. Dezember 2021 - 2 Ws 197/21 -, juris Rn. 13). Die Einbindung der deutschen Behörden im Vorfeld und der Zusammenhang zwischen dem deutschen UJs-Verfahren und der in Frankreich geplanten Maßnahme waren den Gerichten nicht bekannt. Unterlagen dazu - wie etwa Konferenzprotokolle und SIENA-Nachrichten - wurden erst nachträglich von Verteidigern beschafft; sie konnten daher auch in der grundlegenden Entscheidung des Bundesgerichtshofs vom 2. März 2022 (5 StR 457/21 - juris Rn. 21 ff.) noch nicht berücksichtigt werden und werden weiterhin von den Staatsanwaltschaften bei Anklageerhebung nicht gemäß § 199 Abs. 2 S. 2 StPO mit den Verfahrensakten vorgelegt. 31

B. Vorlagefragen

I. Fragen zu 1.: Auslegung des Merkmals „Anordnungsbehörde“

Mit diesen Fragen soll die Zuständigkeit für den Erlass der EEAs vom 2. Juni 2020, 9. September 2020 und 2. Juli 2021 geklärt werden. 32

1. Nationales Recht 33

a) §§ 100 a ff. StPO regeln die Telekommunikationsüberwachung zum Zweck der Strafverfolgung. 34

§ 100 a Abs. 1 S. 1 StPO gestattet die Überwachung der laufenden Kommunikation in Form der „klassischen“ Telekommunikationsüberwachung. Ferner ist es zulässig, mittels Installation einer Spähsoftware auf den Endgeräten die laufende Kommunikation zu überwachen (sog. „Quellen-TKÜ“, § 100 a Abs. 1 S. 2 StPO), die im Anordnungszeitpunkt entstandenen bereits abgeschlossenen auf dem Gerät gespeicherten Kommunikationsvorgänge zu erfassen (sog. „kleine Online-Durchsuchung“, § 100 a Abs. 1 S. 3 StPO) sowie sämtliche auf dem Endgerät gespeicherten Daten auszulesen (sog. „Online-Durchsuchung“, § 100 b StPO). 35

Alle diese Maßnahmen setzen den konkreten Verdacht einer Straftat voraus, wobei der Kreis der Anlasstaten in §§ 100 a Abs. 2, 100 b Abs. 2 StPO auf bestimmte Katalogtatbestände eingeschränkt wird. Nach § 100 e Abs. 1 und Abs. 2 StPO dürfen die Maßnahmen nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden; die Online-Durchsuchung nach § 100 b StPO fällt dabei gemäß § 100 e Abs. 2 StPO i.V.m. § 74 a Abs. 4 GVG in die ausschließliche Zuständigkeit einer nicht mit Hauptverfahren in Strafsachen befassten Spezialkammer des Landgerichts. 36

Die französische Maßnahme gegen den EncroChat-Dienst und dessen Nutzer ähnelt nach den bisher dazu bekannt gewordenen Informationen im Wesentlichen einer Kombination aus einer Online-Durchsuchung i.S.d. § 100 b StPO und einer oder mehrerer der in § 100 a Abs. 1 StPO geregelten Maßnahmen (vgl. etwa OLG Hamburg, Beschluss vom 29. Januar 2021 - 1 Ws 2/21 -, juris Rn. 59, 93; KG, Beschluss vom 30. August 2021 - 2 Ws 79/21 -, juris Rn. 41; i.E. ähnlich BGH, Beschluss vom 2. März 2022 - 5 StR 457/21 -, juris Rn. 67). Gemäß § 100 e Abs. 2 StPO wäre für ihre Anordnung daher das Landgericht zuständig gewesen. 37

b) Das deutsche Gesetz über die internationale Rechtshilfe in Strafsachen (IRG) regelt nicht ausdrücklich, welche Behörde funktional für ausgehende EEAs zuständig ist. Nr. 114 Abs. 2 der Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten (RiVASt) sieht vor, dass die Anordnungsbehörde einen ausländischen Staat um eine nach deutschem Recht einem Richter vorbehaltene Maßnahme nur ersuchen darf, wenn sie zuvor eine richterliche Entscheidung über die Maßnahme eingeholt hat (vgl. Rackow in: Ambos/König/Rackow, Rechtshilferecht in Strafsachen, 2. Aufl. 2020, 1. Hauptteil Rn. 116f.; Böhm, NJW 2017, 1512, 1514). Daraus ergibt sich, dass es sich nach der Vorstellung des deutschen Gesetzgebers bei der Anordnungsbehörde selbst nicht zwingend um ein Gericht handeln muss. Nach den allgemeinen Regeln kann demnach eine EEA, mit der eine Telekommunikationsüberwachung im Ausland begehrt wird, im Ermittlungsverfahren vor Anklageerhebung von der ermittelnden Staatsanwaltschaft erlassen werden 38

(vgl. § 161 StPO).

Dementsprechend geht der 5. Senat des Bundesgerichtshofs in seiner Entscheidung vom 2. März 2022 (5 StR 457/21, juris Rn. 47) von einer Zuständigkeit der in dem UJs-Verfahren ermittelnden GStA Frankfurt für den Erlass der Beweistransfer-EEA aus. 39

2. Erläuterung der Fragen

Die Kammer hat Bedenken, ob der Erlass der EEAs vom 2. Juni 2020, 9. September 2020 und 2. Juli 2021 durch die GStA Frankfurt mit der RL EEA vereinbar ist. Es spricht einiges dafür, dass nach Art. 6 Abs. 1 i.V.m. Art 2 lit. c) RL EEA ein Gericht (örtlich und sachlich: das Landgericht Frankfurt am Main) zuständig gewesen wäre. 40

a) Nach dem Urteil des Gerichtshofs der Europäischen Union vom 16. Dezember 2021 (C-724/19, juris) muss eine EEA, mit der der Vollstreckungsstaat um eine Ermittlungsmaßnahme ersucht wird, von einem Richter erlassen werden, wenn in einem vergleichbaren innerstaatlichen Fall die Anordnung einer solchen Ermittlungsmaßnahme in die ausschließliche Zuständigkeit des Richters fällt. Zur Begründung verweist der Gerichtshof darauf, dass sowohl die Verhältnismäßigkeitsprüfung nach Art. 6 Abs. 1 lit. a) RL EEA als auch die Überprüfung der Maßnahme am Maßstab des nationalen Rechts nach Art. 6 Abs. 1 lit. b) RL EEA nur von derjenigen Behörde geleistet werden könne, die nach dem nationalen Recht des Anordnungsstaates für die Anordnung der Ermittlungsmaßnahme zuständig sei. Zudem würden unterschiedliche Zuständigkeiten für die Anordnung der Ermittlungsmaßnahme und den Erlass der EEA die mit der RL EEA bezweckte Einführung eines vereinfachten und wirksamen Systems gefährden (Gerichtshof aaO. Rn. 32ff.). 41

Diese Rechtsprechung könnte man übertragen auf den Fall, dass der Vollstreckungsstaat die Ermittlungsmaßnahme bereits durchgeführt hat und der Anordnungsstaat mit der EEA die Übermittlung der dadurch erlangten Daten bzw. die Erlaubnis für deren justizielle Verwendung begehrt. 42

aa) Der Wortlaut des Art. 2 lit. c) Ziff i) RL EEA (Zuständigkeit „in dem betreffenden Fall“) und des Art. 2 lit. c) Ziff. ii) RL EEA (Zuständigkeit „für die Anordnung der Erhebung von Beweismitteln“) enthält keinen Anhaltspunkt, dass für eine EEA zum Beweistransfer im Sinne des Art. 1 Abs. 1 S. 2 RL EEA andere Zuständigkeitsregeln gelten sollen als für eine EEA zur Durchführung der zugrunde liegenden Maßnahme. Auch insoweit würden unterschiedliche Zuständigkeiten im Widerspruch zu der ausweislich der Erwägungsgründe 5 bis 8 und 24 vom Richtliniengeber bezweckten Ausgestaltung der EEA als übergreifendes, wirksames, einheitliches und der Vereinfachung dienendes Instrument stehen. 43

bb) Die Entscheidung eines Richters scheint zudem geboten, um die ordnungsgemäße Durchführung der in Art. 6 Abs. 1 lit. a) und b) RL EEA vorgesehenen Prüfungsschritte zu gewährleisten. Auch in dieser Hinsicht lassen sich die Erwägungen des Gerichtshofs in seinem Urteil vom 16. Dezember 2021 (aaO. Rn. 32ff.) auf die Beweistransfer-EEA übertragen. 44

Die insoweit nach Art. 6 Abs. 1 lit. a) RL EEA vorzunehmenden Prüfungsschritte sind dieselben; insbesondere gibt es keinen Anhaltspunkt dafür, dass bei einer „nur“ auf die Übermittlung von Beweismitteln gerichteten EEA an die Prüfung geringere Anforderungen zu stellen wären. Die Konzeption der EEA als einheitliches Instrument spricht im Gegenteil für eine gleichermaßen umfangreiche und intensive Prüfung. Ob die Datenübermittlung notwendig und verhältnismäßig ist, lässt sich nicht trennen von der Frage der Notwendigkeit und Verhältnismäßigkeit der Maßnahme selbst. Vergleichbares gilt für den nach Art. 6 Abs. 1 lit. b) RL EEA gebotenen Vergleich mit einer entsprechenden innerstaatlichen Maßnahme. 45

b) Dass für die hier in Rede stehenden Beweistransfer-EEAs dieselben Zuständigkeitsregeln gelten müssen wie für eine EEA zur Durchführung der Maßnahme, erscheint gerade in der vorliegenden Fallgestaltung besonders geboten. Die später mit den EEAs erbetenen Daten stammten ausschließlich von Nutzern auf dem Hoheitsgebiet des Anordnungsstaates (Deutschland). Der Vollstreckungsstaat (Frankreich) hatte diese von vornherein nur mit dem Ziel erhoben und gespeichert, sie später dem Anordnungsstaat zum Zweck der dortigen Strafverfolgung zu übermitteln. Die deutschen Strafverfolgungsbehörden waren vor Beginn über die Überwachungsmaßnahme informiert. Durch das in der Antwort auf die SIENA-Nachricht vom 27. März 2020 erklärte Einverständnis und die darin gegebenen Zusagen, ohne die es nicht zur laufenden Bereitstellung der Daten zum Download auf dem Europol-Server gekommen wäre, haben sie sich die Maßnahme zu eigen gemacht. 46

Angesichts dessen hätte es für die deutschen Behörden nahegelegen, die französischen Behörden bereits vor Beginn der Maßnahme durch eine EEA mit der Durchführung der Maßnahme gegen die deutschen Nutzer zu beauftragen; für den Erlass dieser EEA wäre nach der Entscheidung des Gerichtshofs vom 16. Dezember 2021 ein deutsches Gericht (hier: das Landgericht Frankfurt am Main) zuständig gewesen. 47

Alternativ wären die französischen Behörden zu einer Unterrichtung nach Art. 31 RL EEA verpflichtet gewesen, die in Deutschland gemäß Art. 31 Abs. 3 RL EEA, § 91g Abs. 6 IRG ebenfalls zu einer vorherigen richterlichen Überprüfung der Maßnahme geführt hätte (zur Zuständigkeit insoweit vgl. unten zu Frage 4); dass diese Unterrichtung von den französischen Behörden versäumt worden war, war den deutschen Ermittlungsbehörden von Beginn an bekannt und wurde von ihnen nicht beanstandet. 48

Da die RL EEA nicht nur auf eine Vereinfachung des Systems der Zusammenarbeit, sondern auch auf die Sicherung nationaler Mindeststandards ausgerichtet ist, erscheint es bei dieser Sachlage geboten, die anschließende deutsche EEA zur Datenübermittlung denselben Zuständigkeitsregeln zu unterwerfen, die für eine EEA zur Durchführung der Überwachung gegolten hätten. In besonderem Maße gilt dies für die EEA vom 2. Juni 2020, bei deren Erlass die Überwachungsmaßnahme noch lief. Dass die Maßnahme in Frankreich von einem Richter angeordnet worden war, machte die Entscheidung des deutschen Gerichts nicht entbehrlich (vgl. - zur gerichtlichen Anerkennung der EEA im Vollstreckungsstaat - Urteil des Gerichtshofs vom 2. März 2021 - C-746/18 -, juris Rn. 53). 49

c) Aus dem Urteil des Gerichtshofs vom 2. März 2021 in der Rechtssache C-746/18 lässt sich nach Ansicht der Kammer darüber hinaus folgern, dass die EEAs hier auch unabhängig von den nationalen Zuständigkeitsvorschriften von einem Richter hätten erlassen werden müssen. Die Ausführungen des Gerichtshofs zur Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58 im Lichte der Grundrechte aus Art. 7, 8 und 11 der europäischen Grundrechte-Charta (GRCh) lassen sich auf die Auslegung des Art. 6 Abs. 1 lit. a) RL EEA übertragen. 50

Danach muss die Entscheidung über die Anforderung elektronischer Standort- und Verkehrsdaten zum Zweck der Strafverfolgung von einem Gericht oder einer unabhängigen Verwaltungsstelle getroffen werden. Art. 15 Abs. 1 der Richtlinie 2002/58 fordert eine Verhältnismäßigkeitsprüfung mit Erwägungen zum Tatverdacht und einer Abwägung der Belange der Strafverfolgung mit den Grundrechten auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten, die nach Ansicht des Gerichtshofs nicht von der mit den Ermittlungen befassten, am Datenzugang interessierten Stelle sichergestellt werden kann (Gerichtshof aaO. Rn. 51ff.). 51

Für die Auslegung von Art. 2 lit. c) RL EEA lässt sich daraus folgern, dass eine EEA zum Zweck der Strafverfolgung - unabhängig von den nationalen Zuständigkeitsregeln in einem vergleichbaren innerstaatlichen Fall - jedenfalls dann immer von einem nicht mit den konkreten Ermittlungsmaßnahmen befassten Richter erlassen werden muss, wenn die Verhältnismäßigkeitsprüfung nach Art. 6 Abs. 1 lit. a) RL EEA - wie hier - eine komplexe Abwägung zum Gegenstand hat und schwerwiegende Eingriffe in hochrangige Grundrechte betrifft. 52

Die hiesige Fallgestaltung weist zudem spezifische Parallelen zu der im Urteil vom 2. März 2021 behandelten Vorratsdatenspeicherung auf (vgl. dazu Frage Nr. 5 aus dem Fragenkatalog des EGMR vom 3. Januar 2022 - Verfahren Nr. 44715/20 und 47930/21 - in einem EncroChat betreffenden Beschwerdeverfahren) und geht hinsichtlich der Intensität des Grundrechtseingriffs noch über diese hinaus. Bei den EncroChat-Daten handelt es sich um eine große Datenmenge, die über einen längeren Zeitraum hinweg unterschiedslos von sämtlichen Nutzern eines Kommunikationsdienstes zum Zweck der Strafverfolgung, aber ohne konkreten Tatverdacht im Einzelfall erhoben und gespeichert wurde. Dabei wurden sogar nicht nur Verkehrs- und Standortdaten, sondern weitere Daten, insbesondere Kommunikationsinhalte, erfasst. 53

Bereits die Übermittlung von Verkehrs- oder Standortdaten an eine Behörde begründet nach der Rechtsprechung des Gerichtshofs einen schwerwiegenden Eingriff in die Grundrechte aus Art. 7 und 8 der Charta (vgl. Urteil vom 2. März 2021, aaO. Rn. 39; Urteil vom 6. Oktober 2020, La Quadrature du Net u.a. - C-511/18 u.a. -, juris Rn. 116). Durch die zusätzliche Übermittlung der vollständigen Kommunikationsinhalte eines mehrmonatigen Zeitraums wurde der Eingriff weiter intensiviert. Soweit es sich bei dem EncroChat-Dienst nicht um „klassische“ Telekommunikation im Sinne von Art. 2 S. 1 der Richtlinie 2002/58 i.V.m. Art. 2 lit. c) der Rahmenrichtlinie 2002/21 handelt, sondern um einen internetbasierten „Over-The-Top-Dienst“, rechtfertigt dies keine unterschiedliche Beurteilung, zumal nach der an die Stelle der Richtlinie 2002/21 getretenen Richtlinie 2018/1972 (vgl. dort etwa Erwägungsgrund 15) im Unionsrecht für die funktional vergleichbaren internetbasierten Kommunikationsformen ein gleichwertiger Schutz der Endnutzer gewährleistet werden soll. 54

Danach liegt es nahe, den Zugang der deutschen Strafverfolgungsbehörden zu den EncroChat-Daten im Wege der EEA vergleichbaren Kriterien zu unterwerfen wie den Zugang zu Vorratsdaten nach Maßgabe des Art. 15 Abs. 1 RL 2002/58. Dass die EncroChat-Daten nicht, wie bei den Vorratsdaten, auf behördliche Anordnung durch den Kommunikationsdienstleister gespeichert, sondern unmittelbar von den französischen Strafverfolgungsbehörden ausgeleitet wurden, rechtfertigt keine andere Beurteilung, sondern verstärkt noch den mit der Speicherung verbundenen Grundrechtseingriff und damit auch das Bedürfnis, den Zugang der deutschen Behörden an strenge Voraussetzungen zu binden und die Entscheidung darüber einem Richter zuzuweisen. 55

II. Fragen zu 2. und 3.: Zulässigkeit der EEAs nach Art. 6 Abs. 1 RL EEA

Die Fragen betreffen die materiellen Anforderungen an eine EEA zur Beweisübermittlung. 56

1. Nationales Recht

a) Zu den materiellen Anforderungen an eine ausgehende EEA enthalten die §§ 91 a ff. IRG keine Regelung. Insoweit ist ergänzend auf Art. 6 RL EEA zurückzugreifen (Böhm NJW 2017, 1512, 1514). 57

b) Eine heimliche Telekommunikationsüberwachung zum Zweck der Strafverfolgung setzt nach §§ 100 a, 100 b StPO den 58

Verdacht einer Straftat voraus. §§ 100 a, 100 b StPO schränken den Kreis der Anlasstaten - abgestuft nach der Schwere des Grundrechtseingriffs - auf bestimmte Katalogtaten ein, wobei sich der Tatverdacht jeweils auf „bestimmte Tatsachen“ gründen muss.

Der Gesetzgeber trägt damit den Vorgaben des Bundesverfassungsgerichts Rechnung, wonach bei einem heimlichen Zugriff auf personenbezogene Telekommunikationsdaten wegen der besonderen Schwere der damit verbundenen Eingriffe in das Fernmeldegeheimnis gem. Art. 10 GG bzw. in das Grundrecht auf IT-Sicherheit aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG erhöhte Anforderungen sowohl an die Bedeutung der aufzuklärenden Straftat als auch an den Verdachtsgrad zu stellen sind (vgl. etwa BVerfG, Beschluss vom 16. Juni 2009 - 2 BvR 902/06 -, „E-Mail-Beschlagnahme“, juris Rn. 75, 79; grundlegend zu der entsprechenden Frage im präventiven Bereich: BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07 -, „Online- Durchsuchung“, juris Rn. 250 f.). Die den Verdacht begründenden Tatsachen müssen jeweils so beschaffen sein, dass sie den Schluss nicht nur auf irgendein strafbares Verhalten, sondern auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen. Vage Anhaltspunkte, bloße Vermutungen oder allgemeine Erfahrungssätze reichen nicht (BVerfG, Urteil vom 27. Februar 2008 - 1 BvR 370/07 -, juris Rn. 250 f.). Gemäß § 100 e Abs. 2 Nr. 2 StPO muss zudem der konkrete Tatvorwurf in der Beschlussformel angegeben werden. 59

Die hier vor Beginn der Maßnahme gegebenen unspezifischen Verdachtsmomente und die Aufzählung diverser alternativ denkbarer Straftatbestände erfüllen diese Anforderungen nicht, so dass eine Überwachung sämtlicher EncroChat-Nutzer nach §§ 100 a ff., 100 e Abs. 3 Nr. 2 und 4 StPO nicht zulässig gewesen wäre (vgl. KG, Beschluss vom 30. August 2021 - 2 Ws 93/21 -, juris Rn. 39, 42; OLG Schleswig, Beschluss vom 29. April 2021 - 2 Ws 47/21 -, juris Rn. 35). 60

2. Erläuterung der Fragen zu 2.: Auslegung des Art. 6 Abs. 1 lit. a) RL EEA

Nach Art. 6 Abs. 1 lit. a) RL EEA muss der Erlass der EEA für die Zwecke des Verfahrens notwendig und verhältnismäßig sein. 61

a) Eine EEA, mit der der Zugriff auf Daten aus einer Telekommunikationsüberwachung zum Zweck der Strafverfolgung begehrt wird, erfüllt diese Voraussetzung nach Ansicht der Kammer nur, wenn gegen jede betroffene Person ein auf konkrete Tatsachen gestützter Verdacht der Beteiligung an einer schweren Straftat besteht. 62

Der 5. Senat des Bundesgerichtshofs hat in seinem Beschluss vom 2. März 2022 (5 StR 457/21, juris Rn. 55) die Auffassung vertreten, die von ihm selbst so bezeichnete „nicht spezifizierte Verdachtslage“ hinsichtlich der „in Frage kommenden vielfältigen Straftaten“ sei ausreichend gewesen, um nach Maßgabe des Art. 6 Abs. 1 lit. a) RL EEA die EEA zu erlassen. Dem möchte die Kammer nicht folgen. 63

aa) Bei den vom Bundesgerichtshof - in Übereinstimmung mit den Beschlüssen des Strafgerichts in Lille - beschriebenen Verdachtsmomenten handelte es sich zum einen um kriminalistische Erkenntnisse aus einer im Verhältnis zur Gesamtzahl der Nutzer sehr geringen Zahl früherer Strafverfahren ohne individuellen Bezug zu den von der EEA betroffenen Nutzern. Zum anderen legten Besonderheiten der Funktionen und Vertriebsmodalitäten der EncroChat-Telefone es nahe, dass diese für kriminelle Nutzer besonders attraktiv waren. Ermittlungen zu legalen Nutzungsmöglichkeiten für Personen mit einem ebenfalls überdurchschnittlichen Sicherungsbedürfnis waren dabei allerdings zu keinem Zeitpunkt angestellt worden. Konkrete strafbare Sachverhalte waren nicht einmal in groben Umrissen bekannt; sogar der Deliktstyp blieb offen. Soweit es Anhaltspunkte dafür gab, dass die EncroChat-Betreiber ihr System gezielt auf die Bedürfnisse von Kriminellen ausrichteten, erlaubte dies nur den ohnehin naheliegenden Schluss auf kriminelle Aktivitäten einiger, aber keinesfalls aller oder auch nur fast aller Nutzer. Hinweise darauf, dass es sich bei allen EncroChat-Nutzern um eine untereinander in Verbindung stehende kriminelle Gruppierung handelte, gab es nicht; angesichts der hohen Zahl an Nutzern (allein in Deutschland über 4.000, weltweit ca. 60.000) und deren Verteilung auf eine Vielzahl von Ländern lag dies auch fern. 64

Nach Ansicht der Kammer reichen diese Verdachtsmomente nicht aus, um den Erlass einer EEA zu rechtfertigen. Die hier im Rahmen des Art. 6 Abs. 1 lit. a) RL EEA an den Verdachtsgrad zu stellenden Anforderungen sollten den oben beschriebenen Anforderungen nach den §§ 100 a ff. StPO ähneln. Da die Ausgestaltung und Auslegung der §§ 100 a ff. StPO maßgeblich durch die Vorgaben der deutschen Verfassung geprägt ist und der unionsrechtliche Grundrechtsschutz gegen heimliche Abhörmaßnahmen vergleichbar stark ausgeprägt ist, liegt es nahe, auch im Rahmen des Art. 6 Abs. 1 lit. a) RL EEA vergleichbar starke und spezifische Verdachtsmomente zu fordern. 65

Würde man hier schon einen „nicht spezifizierten“ Verdacht ohne Einengung auf ein irgendwie konkretisiertes Geschehen als Tatverdacht im Sinne des Art. 6 Abs. 1 lit. a) RL EEA ausreichen lassen, würde das Erfordernis letztlich leerlaufen; für die von Art. 6 Abs. 1 lit. a) RL EEA geforderte einzelfallbezogene Verhältnismäßigkeitsprüfung würde es an einem wesentlichen Anknüpfungspunkt fehlen. 66

bb) Diese Auslegung des Art. 6 Abs. 1 lit. a) RL EEA wird gestützt durch die Rechtsprechung des Gerichtshofs zur Zulässigkeit der Vorratsdatenspeicherung. Die dort zur Verhältnismäßigkeit im Sinne von Art. 15 Abs. 1 der RL 2002/58 entwickelten Wertungen lassen sich auf die Verhältnismäßigkeit im Sinne von Art. 6 Abs. 1 lit. a) RL EEA übertragen. 67

Sowohl die Speicherung von Verkehrs- oder Standortdaten als auch der behördliche Zugang zu ihnen greifen in schwerwiegender Weise in die Grundrechte aus Art. 7 und 8 GRCh ein (Urteile des Gerichtshofs vom 2. März 2021, aaO. Rn. 39, und vom 5. April 2022 - C-540/20 -, juris Rn. 44). Ob dabei tatsächlich sensible Informationen über das Privatleben erlangt werden, ist für die Schwere des Eingriffs unerheblich. Ausreichend ist, dass dies ex ante möglich erscheint (Urteil des Gerichtshofs vom 2. März 2021, aaO. Rn. 40). Der Grundsatz der Verhältnismäßigkeit erfordert es, den Strafverfolgungsbehörden Zugriff nur auf Daten von solchen Personen zu gewähren, die im Verdacht stehen, eine schwere Straftat zu planen, zu begehen, begangen zu haben oder in eine solche verwickelt zu sein (aaO. Rn. 50). Dies spricht dafür, auch den Datenzugriff durch eine EEA von einem konkreten Verdacht abhängig zu machen. 68

Dem lässt sich nicht entgegenhalten, dass der Grundrechtsschutz der Betroffenen ausreichend im Rahmen des nationalen Strafverfahrens durch das nationale Strafprozessrecht gewährleistet werde (vgl. demgegenüber BGH, Beschluss vom 2. März 2022 - 5 StR 457/21 -, juris Rn. 41, 67ff.). Vor dem Hintergrund, dass die Speicherung der Daten und der Zugang zu ihnen zwei unterschiedliche Grundrechtseingriffe darstellen, hat der Gerichtshof entschieden, dass nationale Vorschriften über den Zugang zu Daten nicht geeignet sind, den mit der Speicherung verbundenen schwerwiegenden Eingriff zu beschränken oder zu beseitigen (Gerichtshof, Urteile vom 5. April 2022 - C-140/20 -, juris Rn. 47, und vom 20. September 2022, Spacenet u.a. - C-793/19 u.a. -, juris Rn. 91). Dies lässt sich übertragen auf die hier in Rede stehende Fragestellung. Bei der Verwertung der Daten im Strafverfahren handelt es sich um einen weiteren, zu den Eingriffen der Speicherung und des Zugriffs hinzutretenden selbständigen Grundrechtseingriff (vgl. BGH, Beschluss vom 2. März 2022, aaO. Rn. 67). Nur auf diesen Eingriff können sich die nationalen Vorschriften über die Datennutzung im Strafverfahren beziehen; den vorangegangenen Grundrechtseingriff, der mit dem durch die EEA ermöglichten behördlichen Zugriff auf die Daten verbunden ist, können sie hingegen weder beschränken noch beseitigen (vgl. auch Gerichtshof, Urteil vom 2. März 2021, aaO. Rn. 58, wonach eine Kontrolle im Rahmen der Verwendung die vorangehende Kontrolle des Zugangs zu den Daten nicht entbehrlich macht). 69

b) Weitere Bedenken gegen die Verhältnismäßigkeit der EEA ergeben sich mit Blick auf das Recht auf ein faires Verfahren (Art. 47 Abs. 2 GRCh, Art. 6 Abs. 1 EMRK). 70

Das Recht auf faires Verfahren fordert, dass der Beteiligte eines Gerichtsverfahrens eine echte Möglichkeit haben muss, zu einem Beweismittel Stellung zu nehmen. Das gilt besonders, wenn das Beweismittel aus einem technischen Bereich stammt, in dem das Gericht und der Verfahrensbeteiligte nicht über Sachkenntnis verfügen (Gerichtshof, Urteile vom 2. März 2021 - C-746/18 -, juris Rn. 44, vom 6. Oktober 2020, La Quadrature du Net u.a. - C-511/18 u.a. -, juris Rn. 226 f. und vom 10. April 2003, Steffensen - C-276/01 -, juris Rn. 77; EGMR, Entscheidung vom 18. März 1997, Mantovanelli/Frankreich § 36). 71

Um solche Beweismittel geht es auch hier. Die technischen Methoden, mit denen die EncroChat-Daten abgefangen, ausgeleitet, gespeichert und schließlich nach Ländern sortiert auf dem Europol-Server zum Download bereitgestellt wurden, werfen diverse komplexe Fragen insbesondere im Zusammenhang mit der Integrität der Daten (d.h. deren Korrektheit, Vollständigkeit und Konsistenz) auf. Die Möglichkeit, diese Fragen prüfen zu können, ist für eine wirksame Verteidigung von zentraler Bedeutung. Bei den EncroChat-Daten handelt es sich in fast allen Fällen - so auch hier - um das einzige Beweismittel. Da der hier (ebenso wie in der überwiegenden Zahl der deutschen Parallelverfahren) angeklagte Tatbestand des Betäubungsmittelhandels bereits durch das bloße ernsthafte Verhandeln über einen Betäubungsmittelverkauf erfüllt wird (vgl. beispielhaft die hiesigen Tatvorwürfe zu 2. und 3. der Anklageschrift), kommt es für die Verteidigung in besonderem Maße nicht nur auf die Auswertung einzelner Nachrichten, sondern auf den zeitlichen und inhaltlichen Bezug von gesendeten und empfangenen Nachrichten an. Technische Fehler und Unvollständigkeiten bergen damit in besonderem Maße die Gefahr, dass Chatverläufe auch unbeabsichtigt sinnentstellt werden, ohne dass dies beim Lesen der Auswerteprotokolle zu bemerken wäre. 72

Das Verständnis und die Beurteilung solcher möglicher Fehlerquellen erfordern eine erhebliche technische Sachkunde, über die in aller Regel nur ein IT-Sachverständiger verfügen wird. Die Veranlassung eines solchen Gutachtens ist der Verteidigung hier allerdings nicht möglich. Denn der Sachverständige würde diverse Informationen zu den technischen Grundlagen der Überwachungsmaßnahme und der Datenübertragung auf den Server von Europol benötigen, die aber von den französischen Behörden unter Berufung auf das Militärgeheimnis nicht mitgeteilt werden (vgl. zur Geheimhaltungsproblematik auch die Entscheidungen des französischen Cour de Cassation vom 11. Oktober 2022 - Nr. 21-85.148 - sowie - zu Sky ECC - des italienischen Corte Suprema di Cassazione vom 15. Juli 2022 - 12990/2022 -). Exemplarisch wird dies belegt durch eine SIENA-Nachricht vom 20. August 2020 an die am Datenabruf teilnehmenden Mitgliedstaaten, in der auf eine Vertauschung von Absender- und Empfängerkennungen in den Datensätzen hingewiesen wird, für die es wegen der Geheimhaltungsvorgaben keine technische Erklärung gebe. 73

Die Möglichkeit des Beschuldigten, weitere, noch nicht aktenkundige technische Fehler zu identifizieren und für seine Verteidigung zu nutzen, wird dadurch erheblich beschränkt (vgl. - ebenfalls zu einer Vereitelung der Begutachtung durch Vorenthaltung von tatsächlichen Grundlagen - Gerichtshof, Urteil vom 10. April 2003, Steffensen - C-276/01 -, juris Rn. 76ff.). 74

Aus Sicht der Kammer spricht einiges dafür, dass diese Einschränkung der Verteidigungsmöglichkeiten im späteren 75

Strafverfahren eine Vorwirkung auf die Verhältnismäßigkeitsprüfung nach Art. 6 Abs. 1 lit. a) RL EEA entfalten muss. In Betracht käme insoweit, dass Beweismittel der oben beschriebenen Art, gegen die der Beschuldigte sich in einem späteren Strafverfahren nicht wirksam wird verteidigen können, mit einer auf die Ermöglichung der Strafverfolgung abzielenden EEA nicht angefordert werden dürfen. Denn durch die in Art. 6 Abs. 1 lit. a) und b) RL EEA statuierten materiellen Voraussetzungen soll der Grundrechtsschutz gerade nicht allein dem späteren nationalen Verfahren überlassen werden (vgl. Art. 14 Abs. 7 S. 2 RL EEA), sondern schon auf die Ebene der Beweisgewinnung vorverlagert werden.

Für diese Auslegung sprechen auch die Wertungen des Art. 7 RL 2012/13. Nach Art. 7 Abs. 2 RL 2012/13 ist im Strafverfahren dem Beschuldigten zur Gewährleistung eines fairen Verfahrens umfassende und vollständige Akteneinsicht zu gewähren. Art. 7 Abs. 4 RL 2012/13 erlaubt eine Ausnahme, wenn ein wichtiges öffentliches Interesse des Staates, in dem das Strafverfahren stattfindet, dies erfordert. Danach erscheint es grundsätzlich denkbar, dass die Geheimhaltung der technischen Grundlagen durch die französischen Behörden in einem französischen Verfahren mit der RL 2012/13 vereinbar sein könnte. Die Beschränkung der Akteneinsicht in einem deutschen Strafverfahren lässt sich hingegen nach Art. 7 Abs. 4 RL 2012/13 mit französischen Interessen nicht rechtfertigen. Da andererseits im deutschen Strafverfahren eine Akteneinsicht in die von den französischen Behörden zurückgehaltenen Unterlagen aus tatsächlichen Gründen ausscheidet, erscheint es angemessen, der Wertung des Art. 7 Abs. 2 RL 2012/13 bereits bei der Anforderung der Daten mit einer auf die Ermöglichung der Strafverfolgung abzielenden EEA Rechnung zu tragen. 76

3. Erläuterung der Fragen zu 3.: Auslegung des Art. 6 Abs. 1 lit. b) RL EEA

a) Nach Art. 6 Abs. 1 lit. b) RL EEA muss die Anordnungsbehörde die in der EEA angegebene Maßnahme am Maßstab des innerstaatlichen Rechts überprüfen. Nach dem Verständnis der Kammer muss sich diese Prüfung bei einer Beweistransfer-EEA auf die der Beweiserhebung im Vollstreckungsstaat zugrunde liegende Ermittlungsmaßnahme (hier: die Telekommunikationsüberwachung) erstrecken: Wenn die Überwachungsmaßnahme in einem vergleichbaren innerstaatlichen Fall nicht hätte angeordnet werden dürfen, dürfen auch die aus einer solchen Maßnahme herrührenden Daten nicht mit einer EEA angefordert werden. Da die Voraussetzungen der §§ 100 a ff. StPO mangels konkreten Tatverdachts nicht vorlagen (s.o. 1.), hätten hier auch die EEAs nicht erlassen werden dürfen. 77

Der 5. Senat des Bundesgerichtshofs hat allerdings in seiner Entscheidung vom 2. März 2022 (5 StR 457/21, Rn. 47ff.) die Ansicht vertreten, Art. 6 Abs. 1 lit. b) RL EEA sei vorliegend nicht anwendbar. Die Norm erfasse nur eine EEA, mit der eine noch zu vollstreckende Beweiserhebung begehrt werde; auf eine EEA, die sich nur auf den Transfer schon vorhandener Beweise richte, sei sie nicht anwendbar und die Überprüfung der Maßnahme am Maßstab des innerstaatlichen Rechts daher entbehrlich. Auf der Ebene des Anordnungsstaats sei der Individualschutz allein durch die Prüfung nach Art. 6 Abs. 1 lit. a) RL EEA sowie durch die anschließende Prüfung der erhaltenen Beweismittel im nationalen Strafverfahren gemäß Art. 14 Abs. 7 S. 2 RL EEA zu gewährleisten. 78

Gegen diese Ansicht bestehen Bedenken. 79

aa) Dem Bundesgerichtshof ist zuzustimmen, dass die Beweisübermittlung als solche für die Prüfung, ob eine entsprechende Maßnahme in einem innerstaatlichen Fall angeordnet werden könnte, kein sinnvoller Bezugspunkt ist. Bei der Übermittlung von Beweisen aus einem Staat an einen anderen handelt es sich um einen originär internationalen Sachverhalt, für den es keine rein innerstaatliche Entsprechung gibt. Die in Art. 6 Abs. 1 lit. b) RL EEA angesprochene Frage nach der Sicherung von Mindeststandards angesichts unterschiedlicher nationaler Schutzniveaus stellt sich in dieser Form bei einem rein innerstaatlichen Sachverhalt - etwa der Weiterverwendung von Daten in einem anderen Strafverfahren nach §§ 100 e Abs. 6, 479 Abs. 2 StPO - nicht. 80

bb) Anders als der Bundesgerichtshof möchte die Kammer daraus aber nicht den Schluss ziehen, dass Art. 6 Abs. 1 lit. b) RL EEA auf eine auf einen Beweismitteltransfer gerichtete EEA unanwendbar ist. Vielmehr muss nach dem Verständnis der Kammer die Anordnungsbehörde in diesem Fall die Prüfung am Maßstab des innerstaatlichen Rechts auf die der Datenerhebung zugrundeliegende Ermittlungsmaßnahme beziehen: Sie darf im Vollstreckungsstaat bereits vorhandene Beweismittel nur dann durch EEA anfordern, wenn die Ermittlungsmaßnahme, durch die die Beweismittel im Vollstreckungsstaat gewonnen wurden, im Anordnungsstaat in einem vergleichbaren innerstaatlichen Fall zulässig gewesen wäre. 81

Die vom Bundesgerichtshof vorgenommene Einschränkung des Anwendungsbereichs ist mit dem Wortlaut der Norm zwar vereinbar, durch ihn aber keineswegs zwingend geboten. So hat sich die Prüfung am Maßstab des nationalen Rechts zwar auf die „in der EEA angegebene Ermittlungsmaßnahme“ zu beziehen. Die in der EEA „angegebene“ Maßnahme muss aber nicht zwingend die mit dieser EEA „angeordnete“ sein; zur Beschreibung der zu übermittelnden Daten ist es regelmäßig auch erforderlich, auf die Ursprungsmaßnahme Bezug zu nehmen und sie insofern „anzugeben“. 82

Auch die Systematik der Norm spricht gegen unterschiedliche Anwendungsbereiche von Art. 6 Abs. 1 lit. a) und lit. b) RL EEA. Beide Regelungen betreffen nach der einleitenden Formulierung in Absatz 1 ohne Differenzierung „eine EEA“. Art. 6 Abs. 2 und Abs. 3 RL EEA beziehen sich ebenfalls einschränkungslos auf beide Prüfungsschritte nach Absatz 1. In Absatz 2 heißt es ausdrücklich, die in Absatz 1 genannten Bedingungen - d.h. die Voraussetzungen nach lit. a) und lit. b) - würden „in jedem einzelnen Fall“ geprüft. 83

Die vom Bundesgerichtshof vertretene Unterscheidung steht zudem im Widerspruch zur Konzeption der EEA als einheitliches Instrument. Ferner würde durch den Wegfall der Prüfung nach Art. 6 Abs. 1 lit. b) RL EEA das von der Regelung verfolgte Ziel verfehlt, die Einhaltung individualschützender nationaler Mindeststandards zu gewährleisten und einem „Befugnisshopping“ vorzubeugen (vgl. dazu Knytel, Die Europäische Ermittlungsanordnung und ihre Umsetzung in die deutsche und französische Rechtsordnung, 2020, S. 85 m.w.N.). 84

b) Selbst wenn man demgegenüber Art. 6 Abs. 1 lit. b) RL EEA auf eine Beweistransfer-EEA grundsätzlich nicht anwenden würde, so sollte nach Ansicht der Kammer etwas anderes in der vorliegenden Konstellation gelten. 85

Die von den deutschen Behörden im eigenen Strafverfolgungsinteresse vorab befürwortete und von den französischen Behörden im Interesse der deutschen Behörden durchgeführte Überwachung der deutschen Nutzer kommt einer eigenen deutschen Ermittlungsmaßnahme nahe, deren Anordnung durch eine EEA nahegelegen hätte (vgl. dazu bereits oben unter I.2.b). Die Rechtmäßigkeit dieser EEA wäre gemäß Art. 6 Abs. 1 lit. b) RL EEA am deutschen Strafprozessrecht zu messen gewesen. Dass stattdessen zunächst auf informelle Formen der Zusammenarbeit zurückgegriffen wurde, lässt das in Art. 6 Abs. 1 lit. b) RL EEA angesprochene Schutzbedürfnis nicht entfallen. Dies gilt umso mehr, als die Unterrichtung nach Art. 31 Abs. 1 RL EEA, die ebenfalls eine von Verwertungsinteressen unabhängige Prüfung nach dem deutschen Recht bewirkt und damit einen ähnlichen Schutz gewährleistet hätte, unterlassen wurde, ohne dass dies durch die an den Daten interessierten deutschen Strafverfolgungsbehörden beanstandet worden wäre. All dies legt es nahe, die in Art. 6 Abs. 1 lit. b) RL EEA vorgesehene rechtliche Prüfung hier auf die nachfolgende EEA zur Beweiserlangung zu erstrecken. 86

III. Fragen zu 4.: Auslegung des Art. 31 RL EEA

1. Nationales Recht

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 RL EEA). Der zur Umsetzung dieser Regelung geschaffene § 91 g Abs. 6 IRG bestimmt, dass die deutsche Stelle die Durchführung der Maßnahme bzw. die Verwendung der Daten spätestens innerhalb von 96 Stunden untersagen oder die Verwendung an Bedingungen knüpfen muss, wenn die Maßnahme in einem vergleichbaren innerstaatlichen Fall nicht genehmigt würde. 87

Das Gesetz sagt nicht ausdrücklich, ob die Unterrichtung über die geplante Überwachungsmaßnahme an die Staatsanwaltschaft oder das Gericht zu richten ist. § 92 d IRG regelt lediglich die örtliche Zuständigkeit; nach § 92 d Abs. 1 Nr. 1 IRG ist für französische Ersuchen das „zuständige Gericht am Sitz der Landesregierung von Baden-Württemberg“ zuständig. Ob diese Regelung in funktionaler Hinsicht eine Zuständigkeit der Gerichte voraussetzt, wird in Rechtsprechung und Schrifttum unterschiedlich gesehen. Überwiegend wird eine gerichtliche Zuständigkeit angenommen (BGH, Beschluss vom 2. März 2022 - 5 StR 457/21 -, juris Rn. 40; Urteil vom 3. August 2022 - 5 StR 203/22 -, juris Rn. 19; OLG Bremen, Beschluss vom 18. Dezember 2020 - 1 Ws 166/20 -, juris Rn. 34). Andere gehen hingegen von einer Zuständigkeit der Staatsanwaltschaft aus (OLG Hamburg, Beschluss vom 29. Januar 2021 - 1 Ws 2/21 -, juris Rn. 104). In eine ähnliche Richtung dürften Stimmen gehen, wonach die Entgegennahme der EncroChat-Daten durch die deutschen Ermittlungsbehörden einer Heilung der Unterrichtung „gleich-“ bzw. „nahekomme“ (OLG Schleswig, Beschluss vom 29. April 2021 - 2 Ws 47/21 -, juris Rn. 25; KG, Beschluss vom 30. August 2021 - 2 Ws 93/21 -, juris Rn. 54): Eine Heilung durch die nachträgliche Zustimmung einer weisungsabhängigen Ermittlungsbehörde erscheint überhaupt nur denkbar, wenn auch die vorherige Erklärung von einer Ermittlungsbehörde (und nicht einem Gericht) hätte abgegeben werden müssen. 88

2. Erläuterung der Fragen

a) Der Bundesgerichtshof hat in seinem Beschluss vom 2. März 2022 (aaO. Rn. 41) in Zweifel gezogen, ob es sich bei der französischen Datenabschöpfungsmaßnahme um eine Überwachung des Telekommunikationsverkehrs im Sinne von Art. 31 Abs. 1 RL EEA handelte. Demgegenüber geht die Kammer davon aus, dass Art. 31 Abs. 1 RL EEA hier anwendbar ist und die französischen Behörden somit verpflichtet gewesen wären, vor Beginn der Maßnahme die zuständige deutsche Behörde (d.h. nach Ansicht der Kammer: das zuständige Gericht - s.u. b) über die geplante Infiltrierung der deutschen EncroChat-Endgeräte zu unterrichten. 89

Der Begriff des Telekommunikationsverkehrs dürfte - auch mit Blick auf die Zielsetzung der RL 2018/1979 einer einheitlichen Behandlung sämtlicher eingriffsintensiven elektronischen Kommunikationsformen (vgl. Erwägungsgrund 7) - in einem weiten Sinne zu verstehen und nicht auf „klassische“ Telekommunikation beschränkt sein. Auch der Begriff der Überwachung im Sinne des Art. 31 Abs. 1 RL EEA dürfte weit auszulegen sein und jede Abschöpfung von Daten aus der laufenden Kommunikation, insbesondere Verkehrsdaten, Standortdaten oder Inhalten, erfassen, und zwar auch durch Einsatz einer Schadsoftware auf den Endgeräten (Quellen-TKÜ). Soweit mit der Maßnahme darüber hinaus weitere Eingriffe verbunden waren, die sich nicht unter den Begriff der Telekommunikationsüberwachung fassen lassen, wurde die Unterrichtung nach Art. 31 Abs. 1 RL EEA dadurch nicht entbehrlich. 90

b) Art. 31 Abs. 1 RL EEA überlässt die Bestimmung der für die Entgegennahme der Unterrichtung „zuständigen Behörde“ 91

grundsätzlich dem Recht des von der Überwachung betroffenen Mitgliedstaates. Im Lichte der Grundrechte aus Art. 7, 8 und 11 GRCh und vor dem Hintergrund der oben zitierten Entscheidungen des Gerichtshofs vom 16. Dezember 2021 und vom 2. März 2021 neigt die Kammer aber zu der Auslegung, dass „zuständige Behörde“ im Sinne des Art. 31 Abs. 1 RL EEA nur eine weisungsunabhängige und nicht zu Ermittlungszwecken an den Daten interessierte Stelle - namentlich ein Gericht - sein kann.

Art. 31 Abs. 1 RL EEA und Art. 6 RL EEA haben eine einheitliche Schutzrichtung. Beide Vorschriften zielen darauf ab, bei der grenzüberschreitenden Telekommunikationsüberwachung die Einhaltung nationaler Mindestschutzstandards und die Beachtung der Grundrechte zu gewährleisten (vgl. Wörner in: Ambos/König/Rackow, Rechtshilferecht in Strafsachen, 2. Auflage 2020, 4. Hauptteil Rn. 439). Sowohl nach Art. 6 Abs. 1 lit. b) RL EEA als auch nach Art. 31 Abs. 3 RL EEA ist die Maßnahme am Maßstab des nationalen Rechts zu überprüfen. Die Überlegung des Gerichtshofs in seinem Urteil vom 16. Dezember 2021 (aaO. Rn. 34), eine solche Prüfung könne nur von einem Gericht geleistet werden, passt somit auch für Art. 31 RL EEA. Gleiches gilt für die Entscheidung des Gerichtshofs vom 2. März 2021 (aaO. Rn. 51 ff.), wonach die Abwägung zwischen dem staatlichen Strafverfolgungsinteresse und dem Grundrechtsschutz nicht den an den Daten interessierten Ermittlungsbehörden überlassen werden darf, sondern einem weisungsunabhängigen Gericht zugewiesen werden muss. 92

Dass die funktionale Zuständigkeit für die Entgegennahme der Unterrichtung nach Art. 31 Abs. 1 RL EEA nicht anders behandelt werden kann als diejenige für den Erlass einer EEA nach Art. 2 lit. c) RL EEA, wird gerade durch den vorliegenden Fall in besonderem Maße illustriert: Angesichts der Interessenlage vor Beginn der Maßnahme - die Überwachung der deutschen Nutzer geschah ausschließlich im deutschen Strafverfolgungsinteresse - hätte im März 2020 auch eine auf Durchführung der Maßnahme gerichtete EEA der deutschen Behörden an die französischen nahegelegen, die dann nach der Entscheidung des Gerichtshofs vom 16. Dezember 2021 von einem deutschen Gericht hätte erlassen werden müssen. Daran zeigt sich, dass bei grenzübergreifenden Maßnahmen, die auf europäischer Ebene angesiedelt sind und im gleichzeitigen Interesse mehrerer Staaten durchgeführt werden, die Rechtsinstitute der EEA und der Unterrichtung nach Art. 31 RL EEA weitgehend austauschbar sein können. Das spricht dafür, auch die Zuständigkeiten anzugleichen. 93

c) Art. 31 Abs. 1 RL EEA und der seiner Umsetzung dienende § 91 g IRG schützen zum einen die Souveränität des zu unterrichtenden Staates und sollen zum anderen der besonders hohen Grundrechtssensibilität eines heimlichen Zugriffs auf das gesprochene Wort Rechnung tragen (Wörner in: Ambos/König/Rackow, Rechtshilferecht in Strafsachen, 2. Auflage 2020, 4. Hauptteil Rn. 439). 94

Der Bundesgerichtshof (Beschluss vom 2. März 2022 - 5 StR 457/21 -, juris Rn. 41) vertritt dazu (mit Blick auf die Interessenabwägung zur Verwertbarkeit - vgl. dazu unten IV.) die Ansicht, der individuelle Grundrechtsschutz betreffe nur die Beweisverwertung im Ausland (hier: Frankreich), nicht hingegen im zu unterrichtenden Staat (Deutschland). Zudem handele es sich um einen dem Schutz der Staatssouveränität nachrangigen Normzweck. Die Kammer ist demgegenüber der Auffassung, dass nach der Konzeption des Art. 31 Abs. 1 und 3 RL EEA der Individualschutz der Betroffenen sich auf jede Beweisverwendung zur Strafverfolgung, gleich ob im In- oder Ausland, erstreckt (dazu aa) und im Verhältnis zum Souveränitätsschutz mindestens gleichwertig ist (dazu bb). 95

aa) Art. 31 RL EEA ergänzt die Regelungen über eine zu vollstreckende EEA und soll umfassend verhindern, dass nationale Schutzniveaus durch transnationale Telekommunikationsüberwachung unterlaufen werden. Für eine Erstreckung des Individualschutzes auf die Beweisverwertung im unterrichteten Staat spricht der Vergleich mit einer zu vollstreckenden EEA. Hätten die an den Daten der deutschen Nutzer interessierten deutschen Behörden vor Beginn der Maßnahme eine EEA zur Erstreckung der geplanten Maßnahme auf deutsches Staatsgebiet erlassen, wäre der Grundrechtsschutz der deutschen Nutzer über Art. 6 Abs. 1 RL EEA gewährleistet worden; dieser würde sich auch und gerade auf die Datenverwendung durch deutsche Strafverfolgungsbehörden beziehen. 96

Gerade bei grenzüberschreitenden Maßnahmen im gemeinsamen Interesse mehrerer Staaten sind eine zu vollstreckende EEA und die Unterrichtung nach Art. 31 RL EEA nicht trennscharf abzugrenzen, sondern können alternativ in Betracht kommen. Für die betroffenen Grundrechte und die Schwere des Eingriffs macht es zudem keinen grundsätzlichen Unterschied, in welchem Land bzw. welchen Ländern die Daten erhoben, gespeichert und verwendet werden. Danach muss Art. 31 RL EEA nach dem Verständnis der Kammer die Betroffenen jedenfalls vor einer Beweisverwendung in demjenigen Land schützen, in dessen Interesse die Daten erhoben werden (hier also Deutschland). 97

Dem lässt sich nicht entgegenhalten, der Schutz der Betroffenen vor einer Verwendung im deutschen Strafverfahren könne durch das deutsche Verfassungs- und Prozessrecht und insbesondere die Annahme eines Beweisverwendungs- oder Verwertungsverbots gewährleistet werden (so aber BGH, aaO. Rn. 41). Ein Verwertungsverbot setzt nach ständiger deutscher Rechtsprechung die Verletzung einer individualschützenden Vorschrift voraus und würde somit auf der Grundlage der Rechtsansicht des Bundesgerichtshofs ausscheiden. Zudem zielt Art. 31 RL EEA - ähnlich wie Art. 6 Abs. 1 RL EEA - darauf ab, den Grundrechtsschutz auf den Zeitpunkt der belastenden Maßnahme vorzuverlagern und nicht den nationalen Verfahrensordnungen in anschließenden Gerichtsverfahren zu überlassen. 98

bb) Die Annahme, es handele sich gegenüber dem Schutz der Staatssouveränität um einen nachgeordneten Zweck, überzeugt mit Blick auf das hohe Gewicht der betroffenen Grundrechte und die Schwere des Eingriffs ebenfalls nicht. 99

Gerade in Fällen wie dem vorliegenden, in denen es sich im Kern um eine gemeinsame europäische Maßnahme im Interesse mehrerer Mitgliedsstaaten handelt, treten Aspekte des Souveränitätsschutzes jedenfalls für die daran beteiligten Länder in den Hintergrund; umgekehrt kommt gerade mit Blick auf das gemeinsame Strafverfolgungsinteresse aller beteiligten Länder und die unterschiedlichen nationalen Schutzniveaus der Sicherung von Mindeststandards eine besondere Bedeutung zu. 100

IV. Fragen zu 5.: Rechtsfolgen

1. Nationales Recht

a) Die Strafprozessordnung enthält keine ausdrückliche Regelung zur Verwertung rechtswidrig erlangter Beweismittel. Nach ständiger Rechtsprechung des Bundesgerichtshofs setzt ein (ungeschriebenes) Verwertungsverbot voraus, dass die verletzte Vorschrift dem Individualschutz dient. Auch dann kommt es aber nur ausnahmsweise und auf der Grundlage einer umfassenden Abwägung in Betracht. In diese Abwägung einzustellen sind insbesondere die Bedeutung der betroffenen Rechtsgüter und die Schwere des Verstoßes (vgl. zu allem BVerfG NJW 2006, 2684, 2686 und NStZ 2006, 46, 47; BGH NJW 2007, 2269, 227). 101

Verfahrensverstöße bei Abhörmaßnahmen nach den §§ 100 a ff. StPO haben stets ein besonderes Gewicht. Bei einer ohne richterliche Anordnung durchgeführten Maßnahme liegt ein Beweisverwertungsverbot stets nahe (vgl. BGH NJW 1999, 959, 961 m.w.N.). Darüber hinaus ist mit Blick auf die Grundsätze eines rechtsstaatlichen Verfahrens ein Verwertungsverbot immer dann anzunehmen, wenn wesentliche sachliche Voraussetzungen für die Anordnung der Überwachungsmaßnahme fehlten. Das ist insbesondere dann der Fall, wenn der Verdacht einer Katalogtat des § 100 a StPO von vornherein nicht bestand. Bei der Prüfung eines auf bestimmte Tatsachen gestützten konkreten Tatverdachts gesteht der Bundesgerichtshof dem zur Entscheidung berufenen Gericht einen Beurteilungsspielraum zu. Als rechtsstaatswidrig - mit der Folge eines Verwertungsverbots - stellt sich die Anordnung der Überwachungsmaßnahme dar, wenn die Entscheidung diesen Spielraum überschreitet und daher nicht mehr vertretbar ist (BGH, Beschluss vom 1. August 2002 - 3 StR 122/02 -, juris Rn. 10 m.w.N.). Dieser Maßstab gilt auch für die Verwertung von aus anderen Verfahren stammenden sog. „Zufallserkenntnissen“ (BGH, Beschluss vom 7. März 2006 - 1 StR 316/05 -, juris Rn. 7 m.w.N.). 102

b) Nur in besonderen Ausnahmefällen kommt ein unmittelbar aus der Verfassung hergeleitetes Verwertungsverbot auch ohne Feststellung eines einfachgesetzlichen Rechtsverstoßes aufgrund allgemeiner Verhältnismäßigkeitserwägungen in Betracht (vgl. BGH, Beschluss vom 2. März 2022 - 5 StR 457/21 -, juris Rn. 65 ff.). 103

2. Erläuterung der Fragen

Die zu den EncroChat-Daten bisher ergangenen höchstrichterlichen und obergerichtlichen Entscheidungen gehen sämtlich von der Verwertbarkeit der EncroChat-Daten aus. Soweit Verstöße gegen Unionsrecht angenommen oder zumindest in Betracht gezogen werden, wird im Rahmen der Abwägung unter Hinweis auf die Schwere der anhand der EncroChat-Daten ermittelten Straftaten den Strafverfolgungsinteressen der Vorrang eingeräumt (zu Art. 31 RL EEA: BGH aaO. Rn. 44; vgl. auch - wohl zu Art. 6 RL EEA -: KG, Beschluss vom 30. August 2021 - juris Rn. 55). Auch eine Berücksichtigung an anderer Stelle - insbesondere der Beweiswürdigung oder der Strafzumessung - wird, soweit ersichtlich, den Tatgerichten nicht abverlangt; die strafmildernde Berücksichtigung des Verstoßes gegen Art. 31 RL EEA hat der Bundesgerichtshof sogar ausdrücklich als fehlerhaft beanstandet (BGH, Urteil vom 3. August 2022 - 5 StR 203/22 -, juris Rn. 19). 104

Die Kammer hat Zweifel, ob dies mit dem Unionsrecht vereinbar ist. 105

a) Nach ständiger Rechtsprechung des Europäischen Gerichtshofs ist es grundsätzlich Sache des nationalen Rechts, die Rechtsfolgen von Verstößen gegen Unionsrecht zu regeln. Die Verfahrensautonomie der Mitgliedstaaten wird jedoch begrenzt durch den Grundsatz der Effektivität (Gerichtshof, Urteil vom 2. März 2021 - C-746/18 -, juris Rn. 42 m.w.N.). Danach muss das nationale Recht Sorge dafür tragen, dass der Beschuldigte in einem Strafverfahren durch rechtswidrig erlangte Informationen und Beweise keine unangemessenen Nachteile erleidet (Gerichtshof aaO. Rn. 43). 106

Dies kann grundsätzlich nicht nur durch ein Beweisverwertungsverbot erreicht werden, sondern auch durch eine Berücksichtigung der Rechtsverstöße bei der Beweiswürdigung oder im Rahmen der Strafzumessung (Gerichtshof, Urteile vom 2. März 2021, aaO. Rn. 43, und vom 6. Oktober 2020, La Quadrature du Net u.a - C-511/18 u.a. -, juris Rn. 225). Gleichwohl kann nach der Rechtsprechung des Gerichtshofs der Effektivitätsgrundsatz im Einzelfall das nationale Gericht verpflichten, rechtswidrig erlangte Beweise vom Verfahren auszuschließen (Gerichtshof, Urteile vom 20. September 2022 - C-339/20 u.a. -, juris Rn. 106, vom 2. März 2021, aaO. Rn. 44 und vom 6. Oktober 2020, aaO. Rn. 226 f.; grundlegend Urteil vom 10. April 2003, Steffensen - C-276/01 -, juris Rn. 77 ff. im Anschluss an EGMR, Urteil vom 18. März 1997, Mantovanelli/Frankreich Tz. 36). Die Kammer versteht diese Rechtsprechung dahin, dass der Rechtsverstoß in einem solchen Fall qua Unionsrecht stets den Ausschluss der Beweise zur Folge haben muss und es auf eine Abwägung mit den nationalen Strafverfolgungsinteressen und insbesondere auf die Schwere der in Rede 107

stehenden Straftaten nicht mehr ankommt.

Es spricht einiges dafür, ein solches unmittelbar aus dem unionsrechtlichen Effektivitätsgrundsatz hergeleitetes Verwertungsverbot auch hier anzunehmen. Denn der Grundsatz des fairen Verfahrens ist in mehrerlei Hinsicht beeinträchtigt worden: 108

Bereits der Umstand, dass die mit der EEA angeforderten Daten wegen der französischen Geheimhaltung nicht durch einen technischen Sachverständigen überprüft werden können, dürfte die vom Gerichtshof in der Entscheidung vom 10. April 2003 (Steffensen) entwickelten Voraussetzungen erfüllen, unter denen das Gericht Beweise ausschließen muss. Hinzu kommen die oben zu I. bis III. angesprochenen mehrfachen Missachtungen formeller und materieller Sicherungsmechanismen nach Art. 31 und Art. 6 RL EEA, die entweder unmittelbar von den deutschen Strafverfolgungsbehörden zu verantworten sind oder vor denen sie zumindest die Augen verschlossen haben. Wären alle diese Vorgaben des Unionsrechts beachtet worden, wären die Daten der deutschen Nutzer weder erhoben noch bei Europol gespeichert und schon gar nicht an die deutschen Behörden zum Zweck der Strafverfolgung übermittelt worden. 109

Weiter hinzu tritt schließlich, dass die europäischen Agenturen und die deutschen Strafverfolgungsbehörden die Sachaufklärung und die Verteidigung durch die Verweigerung der Herausgabe von für die Verteidigung erheblichen Aktenbestandteilen und die Weigerung, verfahrensrelevante Dokumente überhaupt in die Akten aufzunehmen, im Nachgang weiter erschwert haben. Besonders gravierend wirkt sich dabei die Weigerung aus, die über das SIENA-System ausgetauschten Nachrichten zur Akte zu bringen (die wenigen im vorliegenden Verfahren bekannt gewordenen SIENA-Nachrichten wurden von der Verteidigung eingereicht und stammen mutmaßlich aus dem Ausland). Dadurch lässt sich etwa nicht überprüfen, ob es - was angesichts der SIENA-Nachricht vom 20. August 2020 naheliegt - Mitteilungen zu technischen Auffälligkeiten gab, die für die Bewertung der Chat-Nachrichten von Bedeutung sein könnten. Die ohnehin schon mit der französischen Geheimhaltung verbundene Beschränkung der Verteidigungsmöglichkeiten wurde dadurch weiter vertieft; ein von Art. 7 Abs. 4 RL 2012/13 gedeckter Rechtfertigungsgrund ist dafür nicht ersichtlich. Auch das in dem BKA-Schreiben vom 13. Mai 2020 angekündigte Verschweigen wesentlicher Informationen gegenüber dem Ermittlungsrichter passt in diesen Zusammenhang, da die aus dem Rechtsstaatsprinzip folgende Aufgabe des Ermittlungsrichters, die Ermittlungen eigenverantwortlich zu prüfen, unterlaufen wurde (vgl. zum Gebot der Aktenvollständigkeit im Ermittlungsverfahren BGH NStZ 2022, 561 f.). Insgesamt wurde damit in sämtlichen Verfahrensabschnitten eine unabhängige externe Überprüfung der Datengewinnung und -weiterverwendung verhindert. 110

All dies zusammen genommen dürfte in mehrfacher Hinsicht im Widerspruch zu den Wertungen der Art. 7 Abs. 2 RL 2012/13, Art. 47, 48 GRCh, Art. 6 Abs. 1 EMRK stehen und stellt die Fairness des Verfahrens in seiner Gesamtheit in Frage. 111

b) Die Autonomie der Mitgliedstaaten bei der Regelung der Rechtsfolgen von Verstößen gegen Unionsrecht wird weiter begrenzt durch den Grundsatz der Äquivalenz. Danach dürfen Verstöße gegen Unionsrecht nicht in geringerem Maße sanktioniert werden als vergleichbare Verstöße gegen innerstaatliches Recht (Urteil des Gerichtshofs vom 2. März 2021, aaO. Rn. 42). 112

Auch unter diesem Aspekt könnte man hier an ein zwingendes Verwertungsverbot denken. Denn nach dem deutschen Strafprozessrecht hätten bei einer Abhörmaßnahme sowohl der Verstoß gegen den Richtervorbehalt als auch der fehlende konkrete Verdacht einer Katalogtat jeweils die Unverwertbarkeit der Daten zur Folge. Es ist nicht ersichtlich, weshalb für vergleichbare Verstöße im Zusammenhang mit dem Erlass einer EEA etwas anderes gelten sollte. 113

c) Sofern sich demgegenüber aus dem Unionsrecht kein zwingendes Verwertungsverbot ergibt, kommt es nach dem deutschen Strafprozessrecht auf eine umfassende Interessenabwägung an. Der Bundesgerichtshof und die Obergerichte stellen maßgeblich auf das Gewicht der aufzuklärenden Straftaten ab und folgern daraus, dass das staatliche Strafverfolgungsinteresse gegenüber dem Individualschutz der betroffenen EncroChat-Nutzer den Vorrang genieße (vgl. BGH, Beschluss vom 2. März 2022, aaO. Rn. 36, 44, 57; OLG Karlsruhe, Beschluss vom 10. November 2021 - 2 Ws 261/21 -, juris Rn. 33). Die Kammer hat Zweifel, ob diese Argumentation mit dem Unionsrecht vereinbar ist. 114

Der Gerichtshof hat mehrfach entschieden, dass das Ziel, schwere Straftaten zu bekämpfen, eine allgemeine unterschiedslose Vorratsdatenspeicherung nicht rechtfertigen kann (Urteile vom 6. Oktober 2020, La Quadrature du Net, aaO. Rn. 141, vom 2. März 2021, aaO. Rn. 50 und vom 5. April 2022, aaO. Rn. 65). Solche rechtswidrig anlasslos gespeicherten Vorratsdaten sind dem anschließenden Zugriff der Strafverfolgungsbehörden auch dann entzogen, wenn sie im konkreten Fall der Aufklärung schwerer Taten dienen sollen. Dies gilt umso mehr, wenn - wie hier - mit einiger Wahrscheinlichkeit von der Datenabschöpfung auch Berufsgeheimnisträger - wie etwa Rechtsanwälte und Journalisten - betroffen sind (vgl. zu diesen Gesichtspunkt Gerichtshof, Urteil vom 20. September 2022, Spacenet u.a. - C-793/19 u.a. -, juris Rn. 82) und auch Kommunikationsinhalte erfasst werden. 115

Zu dieser Wertung und dem Grundsatz der Effektivität könnte es im Widerspruch stehen, wenn ein Rechtsverstoß, der unmittelbar an den fehlenden Tatverdacht anknüpft, unter Verweis auf nachträgliche Erkenntnisse aus den rechtswidrig erlangten Daten ohne Sanktion bleibt. Die Kammer neigt danach zu der Ansicht, dass bei der Abwägung, ob ohne ausreichenden Tatverdacht erlangte Daten trotz des Verstoßes gegen Art. 6 Abs. 1 lit. a) und b) RL EEA verwertbar sind, 116

das Gewicht der konkret in Rede stehenden Straftaten nur mit verringertem Gewicht berücksichtigt werden darf mit der Folge, dass bei einem Eingriff in hochrangige Grundrechte allein dieser Gesichtspunkt den Rechtsverstoß nicht aufwiegen und damit die Verwertung nicht rechtfertigen kann.

Vergleichbar lässt sich zu Art. 31 Abs. 1 RL EEA argumentieren: Die Schwere dieses Verstoßes ergibt sich maßgeblich daraus, dass das zuständige deutsche Gericht die Maßnahme wegen fehlenden Tatverdachts untersagt hätte. Auch hier erscheint es widersprüchlich und mit dem Grundsatz der Effektivität schwer zu vereinbaren, wenn bei der Abwägung dem Gewicht der nachträglich ermittelten Straftaten der Vorrang eingeräumt wird. 117

d) Hilfsweise entnimmt die Kammer den Entscheidungen des Gerichtshofs vom 10. April 2003 (Steffensen, aaO. Rn. Rn. 78 ff.), vom 2. März 2021 (aaO. Rn. 43) und vom 6. Oktober 2020 (La Quadrature du Net, aaO. Rn. 225) zumindest, dass ein grundrechtsrelevanter Verstoß gegen Unionsrecht nicht vollständig ohne Auswirkungen auf das nationale Strafverfahren bleiben darf. Danach gebietet es der Grundsatz der Effektivität nach dem Verständnis der Kammer jedenfalls, die Rechtsverstöße entweder bei der Beweiswürdigung oder als Milderungsgrund im Rahmen der Strafzumessung zu berücksichtigen. Mit Blick auf die Behinderung der Verteidigung durch die fehlende Überprüfbarkeit der Datengewinnung wäre dabei insbesondere an einen geminderten Beweiswert zu denken mit der Folge, dass allein auf die Daten eine Verurteilung nicht gestützt werden darf (vgl. - zur vorenthaltenen Befragung von Zeugen - EGMR, Urteil vom 23. April 1997, van Mechelen u.a. vs. Niederlande, Tz. 56 ff.; BVerfG, Beschluss vom 20. Dezember 2000 - 2 BvR 591/00 -, juris Rn. 44 m.w.N.). Auch die Ansicht des 5. Strafsenats des Bundesgerichtshofs (Urteil vom 3. August 2022 - 5 StR 203/22 -, juris Rn. 19), der Verstoß gegen Art. 31 RL EEA dürfe nicht strafmildernd berücksichtigt werden, erscheint mit Blick auf den Effektivitätsgrundsatz problematisch. 118

C. Eilbedürftigkeit

Der Europäische Gerichtshof wird gebeten, die Sache nach Art. 105 Abs. 1 der Verfahrensordnung im beschleunigten Verfahren bzw. hilfsweise mit Vorrang zu behandeln. 119

Es handelt sich um eine Haftsache, die einem besonderen Beschleunigungsgebot unterliegt, auch wenn der Haftbefehl aktuell nicht vollzogen wird. Eine dem Staat zuzurechnende vermeidbare Verfahrensverzögerung könnte dazu führen, dass der Haftbefehl aufzuheben wäre (BVerfG, Beschluss vom 29. November 2005 - 2 BvR 1737/05 -, juris Rn. 28 ff.). 120

Die Entscheidung des Gerichtshofs ist zudem für eine große Vielzahl noch offener gleichgelagerter Verfahren von Bedeutung. 121