

# EncroChat, Sky ECC, ANOM – Verteidigungsansätze vor dem Hintergrund der aktuellen Rechtsprechung

ONLINE FORUM STRAFVERTEIDIGUNG 2022

Rechtsanwalt Christian Lödden, LL.M.

Krefeld, 14.11.2022

*„Ersichtlich liegt zunächst kein Fall vor, bei dem deutsche Behörden durch ein planmäßiges Vorgehen zur Umgehung der maßgeblichen Vorschriften der Strafprozessordnung an der Datengewinnung im Ausland mitgewirkt hätten. Vielmehr war Deutschland an den von den französischen Ermittlungsbehörden geführten Operationen — soweit erkennbar — nicht beteiligt. Die ermittelten Daten sind anfänglich vielmehr ohne vorherige Absprache spontan an die deutsche Polizei übermittelt worden.“*

KG, Beschl. v. 30.08.2021 - 2 Ws 79/21

# Inhalt

Allgemeine  
Verteidigungs-  
ansätze

# 1

- Verwertbarkeit der Daten
- Datenintegrität und –authentizität (RA Daniel Scheibner)
- Identifikation des einzelnen Nutzers
- Konkretisierung der einzelnen Taten



# 2

- Datenerhebung
- Aktuelle Rechtsprechung

# Übersicht Kryptoverfahren 2019-2021



- Europol OTF EMMA seit März 2020 (Deutschland Mitglied)
- Deutschland Mitglied der OTF
- Datenerhebung 01. April - 30. Juni 2020 (Live-Phase)
- 32.477 Telefone in 121 Ländern (über 4.600 in Deutschland)

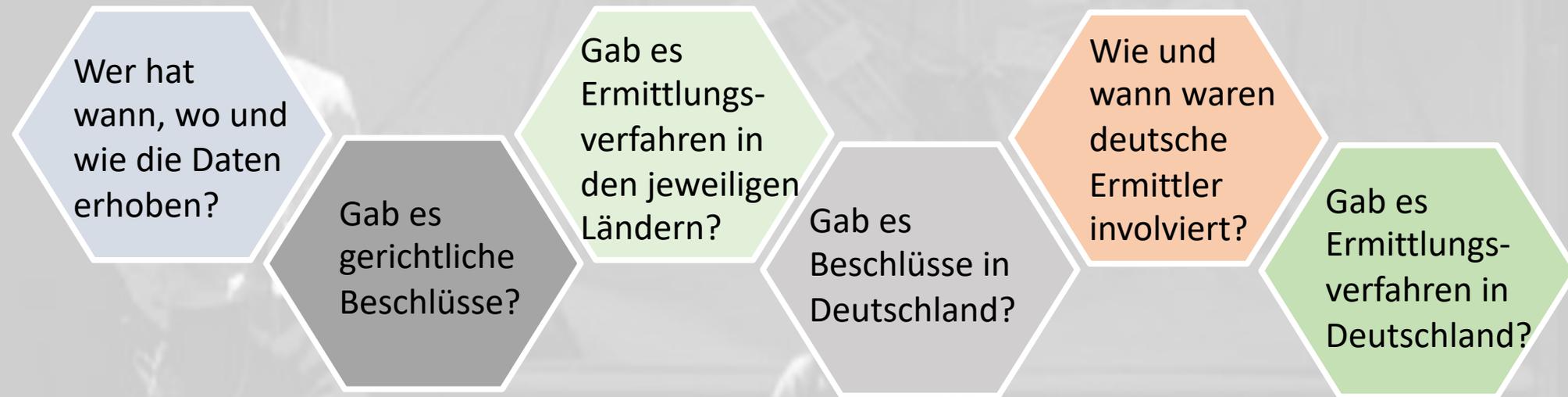


- Europol OTF Limit seit 2019
- Datenerhebung Dezember 2019 bis März 2021 (Live-Phase Mitte Februar 2021- 09. März 2021)
- Ca. 70.000 Telefone in der Live-Phase überwacht, insgesamt 170.000 Telefone

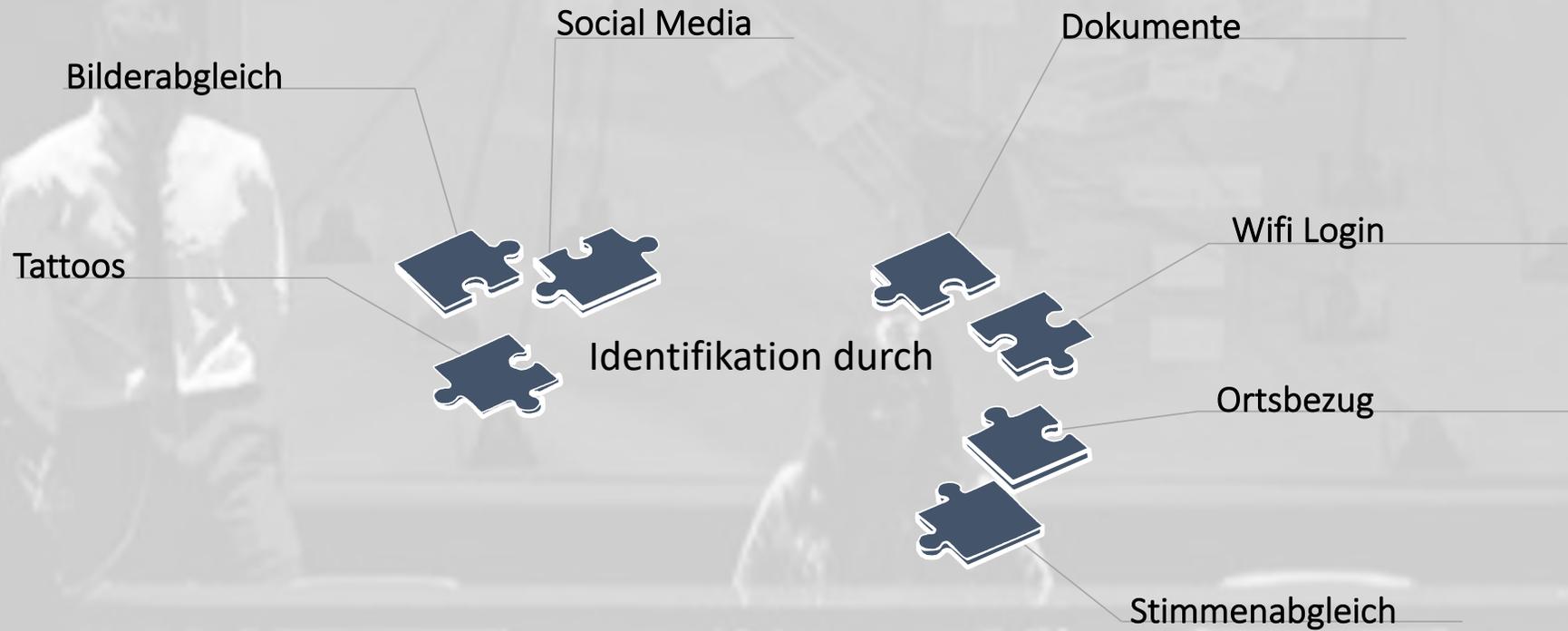


- Europol OTF Greenlight/Trojan Shield in Kooperation mit dem FBI seit dem 16.03.2020 (Deutschland Mitglied)
- Datenerhebung vom 07. Oktober 2019 bis 07. Juni 2021
- Mehr als 12.00 Telefone weltweit (die meisten davon in Deutschland)

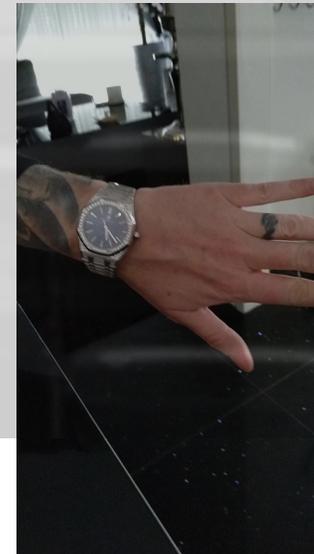
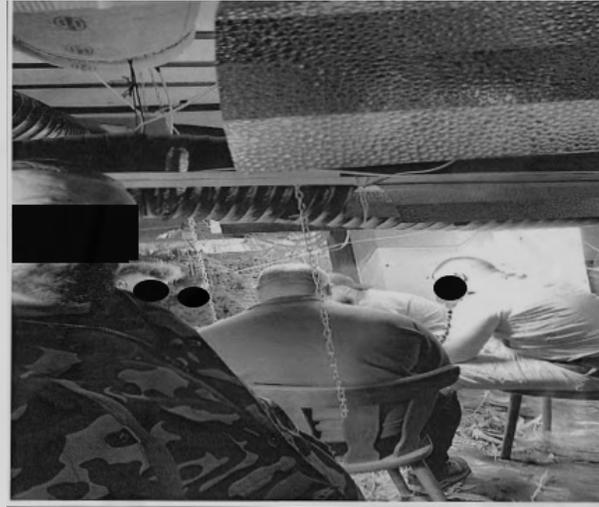
# Allgemeine Verteidigungsansätze – Verwertbarkeit der Daten



# Allgemeine Verteidigungsansätze – Identifikation des einzelnen Nutzers



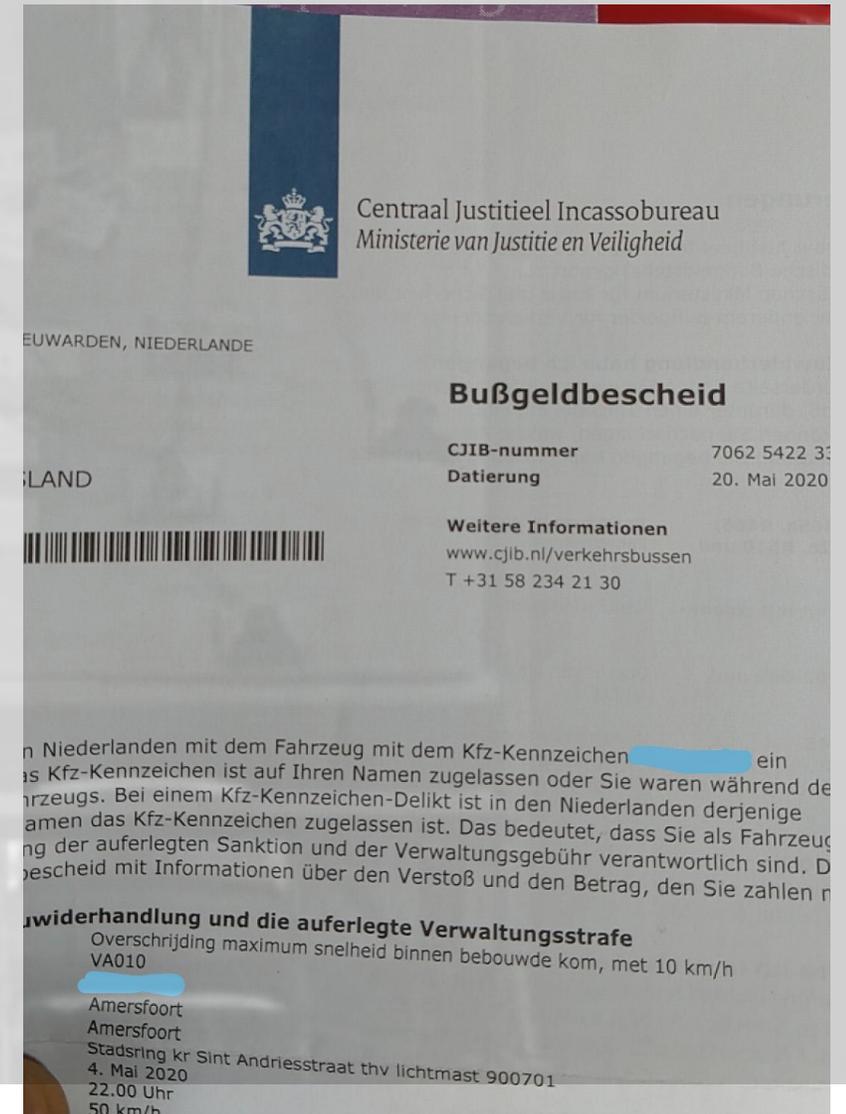
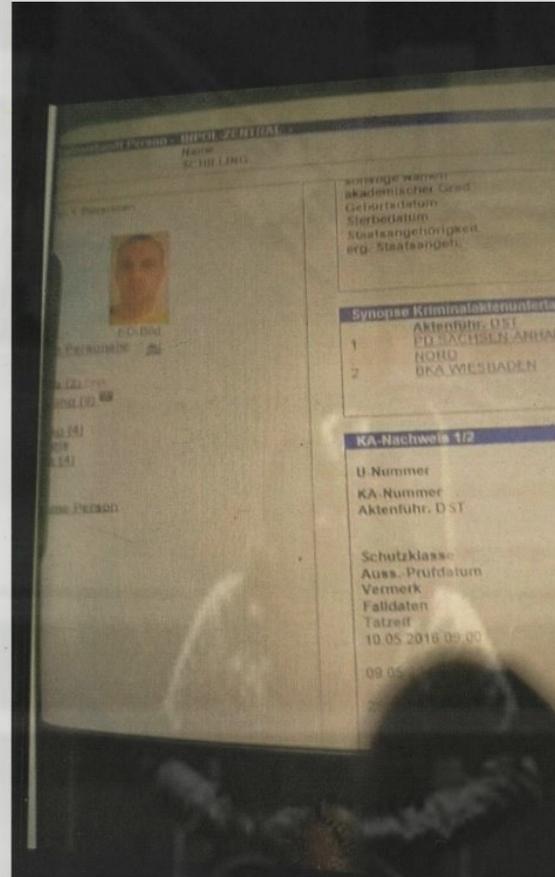
# Allgemeine Verteidigungsansätze – Identifikation des einzelnen Nutzers – Lichtbilder, Selfies, Tattoos etc.



# Allgemeine Verteidigungsansätze – Identifikation des einzelnen Nutzers- Fingerabdrücke



# Allgemeine Verteidigungsansätze – Identifikation des einzelnen Nutzers – sonstige Dokumente

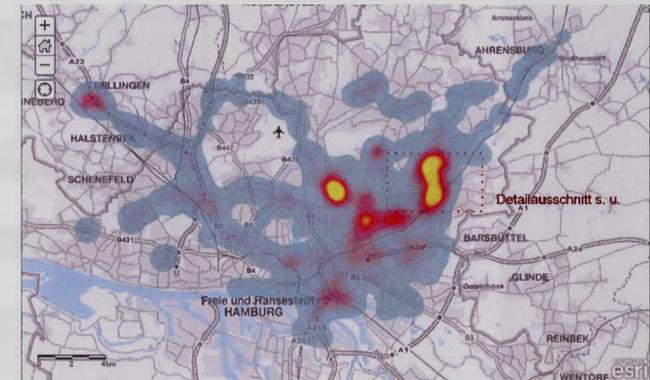


# Allgemeine Verteidigungsansätze – Identifikation des einzelnen Nutzers - Aufenthaltsorte

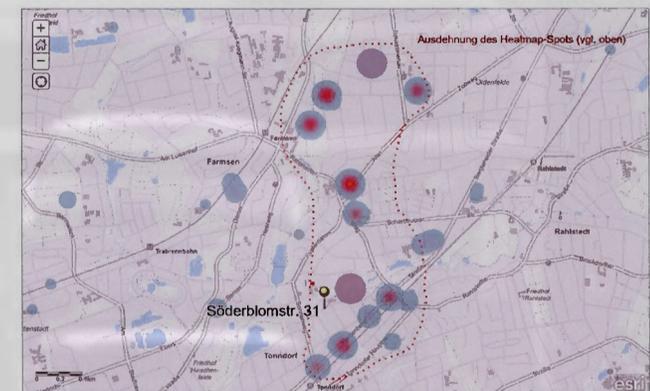
## 3.4 Standortdaten (Cell-IDs)

Es lagen zwar 2.478 Standortdaten vor, allerdings nur für die Tage vom 02. bis 09., und ohne den 05. April. Zudem gab es aus den Chats keine geeigneten Anhaltspunkte, so dass eine aussagekräftige Bewertung nicht möglich war. Es fielen durchaus Stichworte, die darauf schließen ließen, dass sich der beobachtete Nutzer in bestimmten Momenten an seiner Wohnanschrift aufhielt, allerdings lagen für diese Zeitpunkte keine Standortdaten vor.

Differenziert man die Standorte nach Häufigkeiten, zeichnet sich dagegen ein Schwerpunkt im Bereich der Stadtteile Farmsen-Berne/Rahlstedt ab, darin liegt die Wohnanschrift vor: Farmsen-Berne, Söderblomstraße 31:



Heatmap Gesamtansicht



Heatmap Detailausschnitt Farmsen-Berne/Rahlstedt

# Allgemeine Verteidigungsansätze – Identifikation des einzelnen Nutzers - Verteidigerkommunikation

Gem. vorliegendem Chat des **bjfighter** schickt dieser am 11.04.2020 ein Foto von einem Schreiben der Polizei Berlin, Abschnitt 11, vom 09. April 2020 um 20.34 Uhr an den Kontakt „navyarbor“.



Dazu schreibt **bjfighter** dem **navyarbor**: „Das ist gekommen zu diese freund wegen fahrerflucht“

Aus den vorliegenden Chatverläufen ergibt sich, dass der Account [navyarbor@encrochat.com](mailto:navyarbor@encrochat.com) von einem Rechtsanwalt der ir. .... insässigen Kanzlei „.....“ genutzt wird. Der Kontakt „navyarbor“ wird von der Gruppierung, insbesondere den Mitgliedern **imposingzone** und **bjfighter** jeweils zur Klärung rechtlicher Angelegenheiten kontaktiert. Das Schreiben der Polizei Berlin vom 09.04.2020 ist an .....

# Allgemeine Verteidigungsansätze – Konkretisierung der einzelnen Taten

## Gestaltungsmöglichkeit Einlassung

- Täterschaft/Teilnahme
- Verabredung zu einem Verbrechen/ Handeltreiben
- Verbalhandel (verbindliche, ernsthafte Angebote oder Verkaufsverhandlungen - BGH, Beschl. v. 17.6.2020 – 1 StR 110/20)
- (P) mittelbare Belastung von anderen Nutzern

## Allgemeine Fragen

- Bande/ Einkaufsgemeinschaft/Lieferant-Abnehmer/Risikoverteilung
- Tateinheit/Tatmehrheit – Bewertungseinheiten – z.B. spätere Bezahlung bei nächstem Geschäft
- Art, Menge, Beschaffenheit und Qualität der BtM (CBD z.B.), Waffen (Softair, Schreckschuss etc.)

# Datenerhebung



# Einleitungsvermerk 13.03.2020 von KHK Franzen (BKA)

Nach weitergehenden Prüfungen zur technischen Umsetzung der geplanten 100g-Maßnahmen mit dem Ziel einer möglichst ressourcenschonenden Bearbeitung der zu erwartenden Daten sowie Abstimmung des Einleitungsvermerks mit der GenStA Frankfurt am Main, ZIT wurde letzterer mit Datum vom 13.03.2020 finalisiert. Am 20.03.2020 wurde das UJs-Verfahren gegen die Nutzer von Encrochat unter dem Aktenzeichen 62 UJs 50005/20 bei der GenStA Frankfurt am Main, ZIT eingeleitet.



Herbst 2019

April 2020

# Einleitungsvermerk 13.03.2020 von KHK Franzen (BKA)

Bundeskriminalamt

Wiesbaden, 13.03.2020

- SO25 -

**Initiierung eines Ermittlungsverfahrens bei der GenStA Frankfurt am Main – ZIT gegen bisher unbekannte Nutzer von Krypto-Handys der Provider EncroChat und SkyECC wegen des Verdachts des bandenmäßigen Handelstreibens mit Betäubungsmitteln in nicht geringer Menge und der Bildung einer kriminellen Vereinigung**

## 1. Ausgangslage

Die kriminalpolizeilichen Ermittlungen, insbesondere im Bereich der Organisierten Kriminalität, belegen, dass sich kriminelle Gruppierungen im Bereich der eigenen Kommunikation immer mehr abschotten und den staatlichen Überwachungsmöglichkeiten und damit der möglichen Strafverfolgung nahezu vollständig entziehen. Zu diesem Zweck werden sogenannte Krypto-Handys genutzt, bei denen eine Überwachung der Inhaltsdaten durch die Strafverfolgungsbehörden nicht möglich ist.

Bei Krypto-Handys handelt es sich zunächst um handelsübliche Smartphones, bei denen die Kameras, Mikrofone und GPS-Sensoren ausgebaut oder deaktiviert werden und der Zugriff auf handelsübliche Messenger-Apps und Browser verwehrt wird. Anschließend werden die Geräte von den Providern mit einer gesonderten Software und SIM-Karten ausgestattet, sodass sich die Verwendung des Gerätes ausschließlich auf die vorinstallierte Software zum Datenaustausch beschränkt. Die zu sendenden Daten werden vor der Übertragung verschlüsselt und der Empfänger muss die gleiche Software auf einem speziell dafür eingerichteten Smartphone einsetzen, um die versendeten Daten auf seinem Gerät entschlüsseln zu können. Die Kommunikation mit anderen, handelsüblichen Geräten ist technisch nicht möglich, was im Sinne der Abschottung ist. Die Verschlüsselungssoftware ist zum Teil nur verdeckt über nicht erkennbare Apps zu öffnen, damit die eingesetzten Krypto-Handys als solche bei polizeilichen Maßnahmen nicht erkannt werden.

Der Preis eines solchen Smartphones mit der installierten Software liegt bei etwa 1.000 Euro bis 2.000 Euro bei einer Verwendungsdauer von drei bis sechs Monaten. Da die Funktionen der im Verhältnis sehr teuren Mobiltelefone massiv beschränkt sind und nur rudimentäre Kommunikation zwischen Geräten des gleichen Providers zulässt [nur Chat], ist ein legaler Zweck zur Nutzung der Krypto-Handys weder erkennbar noch bisher bekannt geworden.

## 5. Einleitung von Ermittlungen gegen die Nutzer der Geräte der Provider EncroChat und SkyECC

### a) Tatverdacht gegen die Nutzer der Geräte der Provider EncroChat und SkyECC

Das in Deutschland geplante Ermittlungsverfahren richtet sich gegen die aktuellen Nutzer der Geräte der Provider EncroChat und SkyECC, die sich während einer möglichen Datenerhebung in Deutschland aufhalten. Aufgrund der bisherigen Erkenntnislage besteht der Verdacht, dass die Nutzer von Krypto-Handys der Anbieter EncroChat oder SkyECC Straftaten von im Einzelfall erheblicher Bedeutung begehen, insbesondere banden- und gewerbsmäßig mit Betäubungsmitteln in nicht geringer Menge Handel treiben.

Die einzige Funktion von Krypto-Handys ist die von den Strafverfolgungsbehörden nicht zu überwachende, verschlüsselte Planung und Organisation schwerster Straftaten. Aufgrund der konkreten Ausgestaltung der Krypto-Handys wäre eine legale Nutzung sinnlos. Durch die Konfiguration der Geräte sind diese weder zum Telefonieren, noch für die Nutzung von Apps aus dem Play Store bzw. Apple Store geeignet. Eine Kommunikation ist ausschließlich über den installierten Chat und nur mit Nutzern von Krypto-Handys desselben Providers möglich. Die Krypto-Handys verfügen über keinen Internetzugang. Die Geräte sind daher nicht für Personengruppen mit dem Interesse der verschlüsselten Kommunikation zu legalen Zwecken, wie beispielsweise Journalisten, Abgeordnete oder Rechtsanwälte, geeignet. Eine legale Nutzung erscheint auch aufgrund der erheblichen Kosten von Krypto-Handys (ca. 1.500 Euro bis 1.900 Euro für sechs Monate) im Vergleich zu günstigen handelsüblichen Verschlüsselungsdiensten (ca. 10 Euro) abwegig.

# SIENA Nachricht vom 27.03.2020



Januar 2020

April 2020

Case nat. name Op. EMMA - Operational Meeting 19-21 February 2020.

Reference Sienna message 1514969-44-1

The competent authorities of each country that are willing to participate have to provide the JIT a written consent including that:

- they have been briefed about the methods that are being used to generate data from devices in their jurisdiction,
- they would like to receive the data as intelligence under the following conditions:

Europol Unclassified - BPL

## EURPOL SIENA Information Exchange message

Request 1514969-45-1 Received 27/03/2020 09:57 (UTC)

**From** Netherlands J-CAT;  
**Sender** [REDACTED]  
**Send date** 27/03/2020 09:57 (UTC)  
**To** [REDACTED] SOC - AP [REDACTED] France;  
[REDACTED] Cola;  
[REDACTED] UnitedKingdom;

**CC**

# SIENA Nachricht vom 27.03.2020

Dear colleagues,

Operational Task Force (OTF) EMMA provides the cooperation environment between the forthcoming JIT FR (Op. Emma) / NL (Op. 26LEMONT) and non-JIT countries engaged in similar cases.

The OTF includes the establishment of a Joint Operational Centre (JOC) at Europol, which will have the key objective of contributing to the identification of potential threats to life and limb affecting the participating countries.

The competent authorities of each country that are willing to participate have to provide the JIT a written consent including that:

- they have been briefed about the methods that are being used to generate data from devices in their jurisdiction,
- they would like to receive the data as intelligence under the following conditions:
  - o if a situation occurs when the data reveal an imminent threat to life or serious injury for a person (or persons). When that happens the joint investigation partners will decide ad hoc, in cooperation with Europol, about the way the competent authority will be briefed about this data and how this data may be used to combat the serious threat (handling code H0).
  - o Data can be supplied on intelligence basis. Europol will make an intel package for each participating country. France will try to supply Europol with packages already split up by countries. These packages can be distributed to countries not part of the joint investigation team after permission granted by the joint investigation parties. The receiving country will have to guarantee that the data will be analyzed by a small group of police officers and will be held strictly confidential. In no case this data may be used in an ongoing investigation, unless permission is granted by the joint investigation parties (handling code H1). The reason for this is to protect the operation. So there will be possibilities to use the information as intelligence in ongoing investigations in other countries.

but only if the interests of the operation of the JIT can be protected. Furthermore the countries that will use this intelligence based information express that they understand the legal basis for the deployment of this investigative method in France.

- they understand that the data can only be used in judicial procedures after following the applicable EIO or MLAT procedures.

# Aktuelle Rechtsprechung BGH



  
**BUNDESGERICHTSHOF**  
**BESCHLUSS**  
6 StR 639/21  
vom  
8. Februar 2022  
in der Strafsache  
gegen

Die aus den in der Antragschrift des Generalbundesanwalts genannten Gründen unzulässige Verfahrensrüge wäre auch unbegründet. Der Senat sieht im Ergebnis die aus der Überwachung der Kommunikation über den Krypto-Messengerdienst EncroChat durch französische Behörden gewonnenen Erkenntnisse im Einklang mit der obergerichtlichen Rechtsprechung als im Strafverfahren verwertbar an (vgl. etwa KG, NSIZ-RR 2021, 353 mwN).

  
**BUNDESGERICHTSHOF**  
**BESCHLUSS**  
5 StR 457/21  
vom  
2. März 2022  
in der Strafsache  
gegen

75 ee) Ob für den Fall eines zwecks bewusster Umgehung strengerer inländischer Anordnungsvoraussetzungen gestellten Rechtshilfeersuchens (im Sinne eines „Befugnis-Shoppings“, vgl. Roth, GSZ 2021, 238, 247; Labusga, NSIZ 2021, 702, 704) eine andere Bewertung vorzunehmen wäre, bedarf keiner Entscheidung (vgl. bereits BGH, Beschluss vom 21. November 2012 – 1 StR 310/12, BGHSt 58, 32 Rn. 37). Eine solche Konstellation ist weder dargelegt noch sonst ersichtlich (KG, Beschluss vom 30. August 2021 – 2 Ws 79/21 und 93/21, NSIZ-RR 2021, 353).

55 Angesichts der unter 2. b) geschilderten Verdachtslage und der über Europol dem Bundeskriminalamt übermittelten Erkenntnisse war die Einleitung eines Ermittlungsverfahrens gegen Unbekannt wegen des Verdachts schwerer Betäubungsmittelstraftaten im Sinne eines Anfangsverdachts plausibel. Auf dieser Grundlage durfte die Generalstaatsanwaltschaft gemäß § 161 Abs. 1 StPO eine Europäische Ermittlungsanordnung erlassen, die auf die umfassende Übermittlung sämtlicher Daten mit Bezug auf typischerweise im Rahmen organisierter Kriminalität begangene strafbare Handlungen im deutschen Staatsgebiet gerichtet war (aA Wahl, ZIS 2021, 452, 460; Sommer, StV Spezial 2021, 67, 69; Zimmermann, ZfISW 2022, 173, 180).

# Aktuelle Rechtsprechung

## Aufsätze und Besprechungen



- *Brodowski*, Anmerkung zu BGH, Beschluss vom 02.03.2022 -- 5 StR 457/21 = StV 2022, 353.
- *Cornelius*, Anmerkung zu BGH, Beschluss vom 02.03.2022 -- 5 StR 457/21 = StraFo 2022, 196.
- *Zeyer*, Anmerkung zu BGH, Beschluss vom 02.03.2022 -- 5 StR 457/21 = NZWiSt 2022, 236.
  
- *Ruppert*, Erheben ist Silber, Verwerten ist Gold? Verwendbarkeit und Verwertbarkeit von Daten ausländischer Ermittlungsbehörden im Lichte des Grundrechtsschutzes – EncroChat, NZWiSt 2022, 221.
  
- *Meyer-Mews*, Ein kritischer Blick auf den EncroChat-Beschluss des 5. Strafsenats des BGH, HRRS, S. 289 (Heft 9/2022)
  
- *Böse*, Der Auslandsbeweis im deutschen Strafprozess – die Encrochat- Entscheidung des BGH im Spiegel der Lehre von den strafprozessualen Verwertungsverboten, S. 1048-1056, JZ, Jahrgang 77 (2022) / Heft 21.



## Landgericht Berlin

### Beschluss

Geschäftsnummer: (525 KLs) 279 Js 30/22 (8/22)

Datum: 19.10.2022

In der Strafsache  
g e g e n  
M.N.,

Verteidiger  
Rechtsanwalt xxx

wegen Verstoßes gegen das Betäubungsmittelgesetz  
hat die 25. große Strafkammer des Landgerichts Berlin beschlossen:

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

#### II. Sachverhalt

##### 1. Gang der Ermittlungen

4 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:

13 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.

14 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.

# Aktuelle Rechtsprechung LG Berlin



20 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. Sweeting 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.

- 22 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.
- 23 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 bekannt oder sie verschlossen vor

**OStA Jana Ringwald,  
GenStA FFM - ZIT**

*„Ersichtlich liegt zunächst kein Fall vor, bei dem deutsche Behörden durch ein planmäßiges Vorgehen zur Umgehung der maßgeblichen Vorschriften der Strafprozessordnung an der Datengewinnung im Ausland mitgewirkt hätten. Vielmehr war Deutschland an den von den französischen Ermittlungsbehörden geführten Operationen — soweit erkennbar — nicht beteiligt. Die ermittelten Daten sind anfänglich vielmehr ohne vorherige Absprache spontan an die deutsche Polizei übermittelt worden.“*

KG, Beschl. v. 30.08.2021 - 2 Ws 79/21

# Aktuelle Rechtsprechung Reaktion GenStA FFM - ZIT



# Aktuelle Rechtsprechung Reaktionen LG Hamburg



## Beschluss

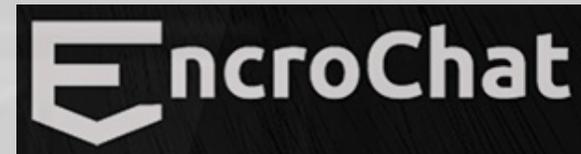
Die Gegenvorstellung gegen den Beschluss der Kammer vom 25. Oktober 2021 (Anl. 14 HV-Protokoll) wird zurückgewiesen und der Antrag auf Aussetzung des Verfahrens und Vorlage von „Fragestellungen“ an den EuGH zum Zwecke der Vorabentscheidung (Anl. 115 HV-Protokoll) wird abgelehnt.

## Gründe

Die ergänzende Begründung der Verteidigung zum Beweiserhebungs- und Beweisverwertungswiderspruch (vgl. Anl. 114 HV-Protokoll) und der Vorlagebeschluss des Landgerichts Berlin vom 19. Oktober 2022 (Az. 525 KLs 279 Js 30/21 (8/22)) geben der Kammer keinen Anlass für eine abweichende Beurteilung. Die Kammer des Landgerichts Berlin verfolgt ihre in der Rechtsprechung vereinzelt gebliebene Auffassung zur Nichtverwertbarkeit der EncroChat-Daten nunmehr vor dem Gerichtshof der Europäischen Union weiter. Letztlich legt das Landgericht Berlin seinem Vorbringen eine aus derzeitiger Sicht der Kammer unzutreffende Tatsachengrundlage und Rechtsauffassung zugrunde. Die Frage einer Verwertbarkeit der EncroChat-Daten ist allein nach nationalem Recht zu beurteilen. Dementsprechend besteht auch kein Anlass, dieses Verfahren auszusetzen und dem Gerichtshof der Europäischen Union Fragen zur Auslegung des Unionsrechts vorzulegen.

Auch ein Abwarten mit Blick auf beim Europäischen Gerichtshof für Menschenrechte anhängige Verfahren kommt nicht in Betracht (vgl. BGH, Beschluss vom 31. August 2022 – 5 StR 130/22, Rn. 3).

# Aktuelle Rechtsprechung Französischer Kassationsgerichtshof



N° E 21-85.763 FS-B

N° 01216

SL2  
25 OCTOBRE 2022

CASSATION PARTIELLE  
IRRECEVABILITE

M. BONNAL président,

R É P U B L I Q U E F R A N Ç A I S E

A U N O M D U P E U P L E F R A N Ç A I S

ARRÊT DE LA COUR DE CASSATION, CHAMBRE CRIMINELLE,  
DU 25 OCTOBRE 2022

MM. [L] [I], [V] [F], [S] [O], [P] [M], [G] [C] [E] et [Z] [D] ont formé des pourvois contre l'arrêt de la chambre de l'instruction de la cour d'appel de Nancy, en date du 9 septembre 2021, qui, dans l'information suivie contre eux des chefs, notamment, d'infractions à la législation sur les stupéfiants, association de malfaiteurs, importations de stupéfiants en bande organisée et blanchiment, a prononcé sur leurs demandes d'annulation d'actes de la procédure.

Zum ersten Teil des Rechtsmittelgrundes

21. Vom Kassationsgerichtshof mit einer vorrangigen Frage der Verfassungsmäßigkeit in Bezug auf Artikel 706-102-1 der Strafprozessordnung unter Bezugnahme auf Artikel 230-1 der Strafprozessordnung befasst, hat der Verfassungsrat mit Beschluss Nr. 2022-987, vom 8. April 2022, den zweiten Teil des zweiten Absatzes von Artikel 706-102-1 der Strafprozessordnung in seiner Fassung, die sich aus dem Gesetz Nr. 2019-222 vom 23. März 2019 zur Programmplanung 2018-2022 und der Justizreform ergibt, als verfassungskonform erklärt.

22. Daher wird die Klage, die auf die Verfassungswidrigkeit dieser Bestimmungen gestützt wird, abgewiesen.

Aber zum zweiten Teil des Rechtsmittelgrundes

Im Hinblick auf Artikel 230-3 und 593 der Strafprozessordnung:

23. Gemäß dem ersten dieser Artikel, vorbehaltlich der Verpflichtungen, die sich aus der Geheimhaltung der nationalen Verteidigung ergeben, werden den Ergebnissen die technischen Angaben beigefügt, die für das Verständnis und die Auswertung der Ergebnisse nützlich sind, sowie eine vom Verantwortlichen der technischen Stelle beglaubigte Bescheinigung, die die Richtigkeit der übermittelten Ergebnisse bescheinigt. Die so erhaltenen Kenntnisse sind Gegenstand eines Eingangsprotokolls und werden in die Verfahrensakte aufgenommen.

24. Gemäß dem zweiten Artikel muss jedes Urteil oder jeder Beschluss die Gründe enthalten, die die Entscheidung rechtfertigen, und auf die wesentlichen Gliederungen der Schriftsätze der Parteien eingehen.

25. Um den Grund für die Nichtigkeit von Computerdatenerfassungsvorgängen auszuschließen, die sich aus dem Fehlen der oben genannten Unterlagen im Verfahren ergeben, stellt das Urteil fest, dass die technischen Angaben zum Verständnis und zur Verwertung der Ergebnisse, sowie die vom Verantwortlichen der technischen Stelle beglaubigte Bescheinigung, die die Richtigkeit der übermittelten Ergebnisse bescheinigt, sind im Text nur „vorbehaltlich der sich aus dem nationalen Verteidigungsgeheimnis ergebenden Verpflichtungen“ vorgesehen.

26. Die Richter fügten hinzu, dass es konsequent sei, wenn sich das Zentrum zur Bekämpfung der digitalen Kriminalität in bestimmten Punkten, die sich auf die im Urteil formulierten Anträge auf technische Erklärungen beziehen, die Geheimhaltung der nationalen Verteidigung wendet, da andernfalls eine Verletzung der Geheimhaltung der nationalen Verteidigung festgestellt werden könnte.

27. Indem die Ermittlungskammer lediglich über das Fehlen technischer Angaben im Verfahren entschied, ohne auf die Schlussfolgerungen des Antragstellers einzugehen, der sich auf das Fehlen der beglaubigten Bescheinigung vom Verantwortlichen der technischen Stelle beruft, welche die Richtigkeit der übermittelten Ergebnisse bescheinigt, hat die Ermittlungskammer die gemäß Artikel 201 Strafprozessordnung für die Zulassung dieses Schriftstücks zum Verfahren zu ersuchen habe, ihre Entscheidung nicht begründet.

28. Daraus folgt, dass die Aufhebung in diesem Punkt gefördert wird.

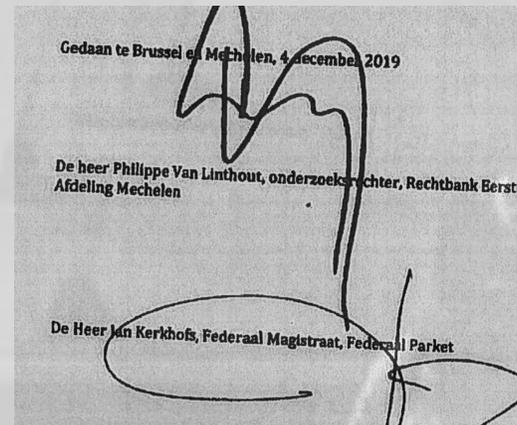
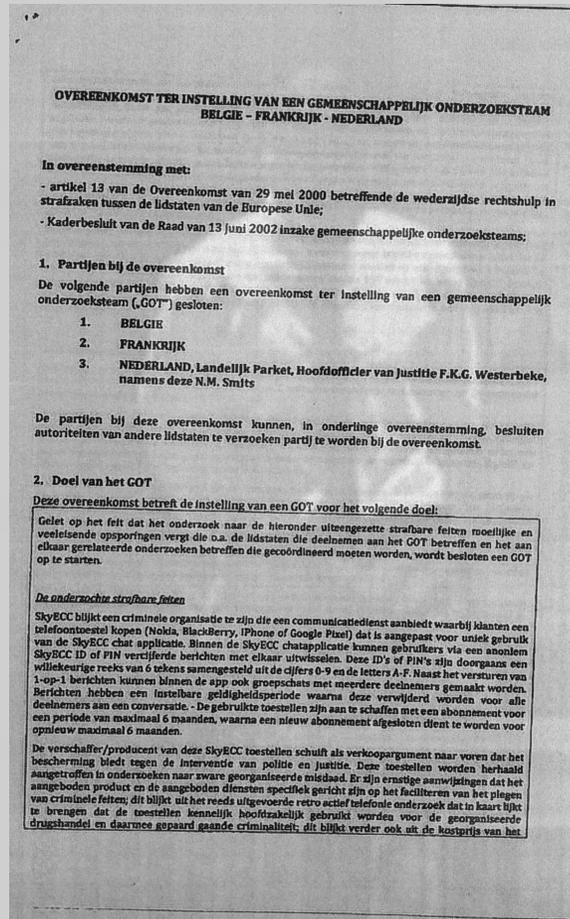
# Zeitstrahl

## An die Rechtsprechung angepasste Freigabe von Informationen



# Datenerhebung

SKYECC



Cour d'Appel de Paris  
Tribunal judiciaire de Paris

Cabinet de  
Brice HANSEMANN  
vice-président chargé de l'instruction

N° Parquet : 20342000697  
N° de dossier : JJ18252000010

**Ordonnance**

portant autorisation de mise en place d'un dispositif technique de captation de données informatiques

Nous, Brice HANSEMANN vice-président chargé de l'instruction, étant en notre cabinet au Tribunal judiciaire de Paris,

Vu l'information suivie contre : X

des chefs :

- 1) Association de malfaiteurs en vue de la préparation de crimes ou de délit puni de 10 années d'emprisonnement (crimes d'importations de produits stupéfiants commises en bande organisée, délits de trafic de produits stupéfiants)  
Faits prévus et réprimés par les articles 450-1, 450-3 et 450-5 du Code pénal (Natif 7188, 12214) ;
- 2) Fourniture de prestations de cryptologie visant à assurer des fonctions de confidentialité sans déclaration conforme ;  
Faits prévus et réprimés par les ART.35 §III et §IV ART.31 §I, ART.29 LOI 2004-575 DU 21/06/2004, ART.3,ART.4, ART.5, ART.8 DECRET 2007-663 DU 02/05/2007 (Natif 32529) ;
- 3) Fourniture d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sans déclaration préalable  
Faits prévus et réprimés par les ART.35 §I 1°, §IV ART.30 §III, ART.29 LOI 2004-575 DU 21/06/2004.  
ART.3,ART.4, ARTS DECRET 2007-663 DU 02/05/2007 (Natif 32537) ;

Attendu que dans le cadre de l'équipe commune d'enquête, les enquêteurs et techniciens néerlandais ont mis au point une technique susceptible de permettre d'obtenir les éléments cryptographiques stockés sur chaque téléphone utilisant l'application SkyECC ; que cette technique, basée sur l'installation d'un serveur jouant le rôle de « Man In The Middle » (serveur dit MITM) positionné sur la liaison externe du serveur 2 (ns6019808.ip-188-165-14.eu), consiste à recevoir tout le

Fait en notre cabinet, le 17 décembre 2020

Le vice-président chargé de l'instruction

# Aktuelle Rechtsprechung

## OLG Celle

SKYECC

OLG Celle, Beschluss vom 15.11.2021 - 2 HEs 24-30/21

Fundstelle openJur 2022, 5925 Rkr:   

Die von französischen Ermittlungsbehörden erhobenen Daten der mit Encrochat-Mobiltelefonen und der mittels SkyECC geführten Kommunikation sind in einem deutschen Strafverfahren gegen den Nutzer von Encrochat bzw. SkyEEC wegen Handeltreibens mit Betäubungsmitteln in nicht geringer Menge verwendbar und unterliegen keinem Beweisverwertungsverbot (Fortführung OLG Celle, Beschluss vom 12. August 2021 – 2 Ws 250/21 – NdsRpfl 2021, 410 – 415)

(3) Hinsichtlich der Angeschuldigten D. Y. und O. Y. beruht der dringende Tatverdacht auf der Auswertung der Textnachrichten, die unter den Nutzernamen „c.“ und „f.“ mittels verschlüsselter Mobiltelefone des Anbieters „Encrochat“ und unter den Nutzerkennungen ... und über den Anbieter „SkyECC“ versandt und empfangen wurden.

Zu den über „Encrochat“ versandten Daten hat der Senat bereits entschieden, dass diese gemäß § 100e Abs. 6 StPO in einem deutschen Strafverfahren gegen den Encrochat-Nutzer wegen Handeltreibens mit Betäubungsmitteln in nicht geringer Menge verwendbar und keinem Beweisverwertungsverbot unterliegen (Senat, Beschluss vom 12. August 2021, 2 Ws 250/21, juris). Dasselbe gilt für die mittels „SkyECC“ versandten Daten. Ebenso wie die Encrochat-Daten sind diese in einem französischen Ermittlungsverfahren erhoben worden und auch die wesentlichen Rahmenbedingungen stimmen zwischen den beiden Anbietern überein. Insbesondere befand sich – ausweislich der vorliegenden Beschlüsse des in beiden Fällen zuständigen Gerichts in Lille – bei beiden Anbietern der Server, über den die Kommunikation erfolgte, an einem Standort in R. und das Angebot sowohl von „Encrochat“ als auch von „SkyECC“ war dadurch gekennzeichnet, dass die Geräte nicht über legale Vertriebswege verkauft wurden und für die verschlüsselten Geräte ein außergewöhnlich hoher Preis – etwa 1.500 Euro für eine sechsmonatige Nutzung – zu zahlen war, obwohl die Geräte selbst nur über einen sehr eingeschränkten Funktionsumfang verfügten.

Es kann dahinstehen, ob darüber hinaus auch die über den Anbieter „An0m“ verschlüsselte Kommunikation im vorliegenden Strafverfahren verwertbar ist und den Tatverdacht gegen die Angeschuldigten stützt. Insbesondere bedarf es keiner näheren Prüfung, inwieweit die Verwertbarkeit der Daten ohne Kenntnis des Serverstandortes, der den Maßnahmen zugrundeliegenden gerichtlichen Beschlüsse und näherer Umstände zum Vertrieb der Geräte überhaupt beurteilt werden kann. Denn auf die Inhalte der mittels „An0m“ geführten Kommunikation kommt es für die Beurteilung des dringenden Tatverdachts nicht an, nachdem sich dieser bereits aus den vorgenannten Beweismitteln, namentlich der Kommunikation über „Encrochat“ und „SkyECC“ ergibt.

# Aktuelle Rechtsprechung Italienischer Kassationsgerichtshof

SKYECC

Penale Sent. Sez. 4 Num. 32915 Anno 2022

Presidente: CIAMPI FRANCESCO MARIA

Relatore: DI SALVO EMANUELE

Data Udiienza: 15/07/2022

## SENTENZA

sul ricorso proposto da:  
LORI ALESSIO nato a ROMA il 04/01/1991

avverso l'ordinanza del 03/02/2022 del TRIB. LIBERTA' di ROMA

udita la relazione svolta dal Consigliere EMANUELE DI SALVO;  
lette/sentite le conclusioni del PG MARIA FRANCESCA LOY  
Il Proc. Gen. conclude per il rigetto per entrambi i ricorsi.

E' presente l'avvocato MOIRAGHI ELEONORA NICLA del foro di ROMA in difesa di:

- Rückverweisung an das Instanzgericht, weil die Staatsanwaltschaft nicht mitgeteilt hat, wie die SkyECC-Daten von den französischen, niederländischen und belgischen Behörden erhoben worden sind
- Die Staatsanwaltschaft hat die zusammen mit den Daten von Europol übersandten Unterlagen über die Datenerhebung, mit Verweis auf Geheimhaltungspflichten von internationalem Polizeiaustausch, nicht zu den Verfahrensakten genommen.

# Aktuelle Rechtsprechung Entscheidung Italienisches Instanzgericht

SKYECC

  
**TRIBUNALE ORDINARIO DI ROMA**  
SEZIONE SPECIALE PER IL RIESAME DELLE MISURE CAUTELARI PERSONALI E REALI  
Tel. 06 38792324-2158 - Fax 2416 - PEC riesame.tribunale.roma@giustiziacert.it

NOTIFICAZIONE AI DIFENSORI ED ALLE PARTI PRIVATE DELL'AVVENUTO DEPOSITO  
IN CANCELLERIA DELL'ORDINANZA DEL TRIBUNALE DEL RIESAME EX ART. 128 C.P.P.

ROMA, 25/10/2022

**N. 1849/2022 R.G. LIBERTA'**  
A.C.R. da Cassazione, già T.L. n. 156/2022 R.G. LIBERTA'

R.G.N.R. 26389 / 2018 PROC. REP. ROMA  
R.G. G.I.P. 10494 / 2022 GIP c/o TRIB. ROMA -

**IL CANCELLIERE DEL TRIBUNALE DI ROMA  
AVVISA**

- PROCURA ROMA - SEDE

- LORI ALESSIO  
nato in data 04-01-1991 a ROMA  
AA.DD.-POGGIO MIRTETO (RI) - Via Ternana Km. 15,600 c/o Villa Ternana

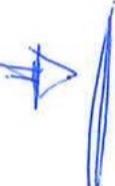
- AVV. MOIRAGHI ELEONORA NICLA  
ROMA - Via Giuseppe Palumbo 3 - PEC

- AVV. BRIZIARELLI GIADA  
PERUGIA - Largo Cacciatori delle Alpi 8 - PEC

che in data 24/10/2022 è stata DEPOSITATA in cancelleria l'ORDINANZA del Tribunale  
del Riesame, relativa all'impugnazione sopra emarginata, contenente il seguente dispositivo:  
P.Q.M.

Visto l'art 309 c.p.p.  
RIFORMA l'impugnata ordinanza e sostituisce nei confronti di Lori Alessio la misura cautelare della custodia in carcere con quella  
degli arresti domiciliari presso la struttura Villa Ternana sita in Poggio Mirteto, via Ternana km. 15,600, con i divieti di comunicazione  
di cui all'ordinanza del Gip del Tribunale di Roma del 9/6/2022 (sostituzione da non eseguirsi in quanto già disposta dal Gip nella  
predetta data del 9/6/2022).  
Nulla per le spese.  
Così deciso in Roma all'esito della camera di consiglio del 28/9/2022

L'Assistente Giudiziario  
dott. Ottavio Marco Barbieri

 Premesso che il procedimento pende allo stato nei confronti del Lori (e di altri coimputati) in sede di giudizio abbreviato, ammesso dal Gip all'udienza del 20.9.2022, va subito detto, sulla (unica) questione oggetto della pronuncia di annullamento, che la mancata realizzazione del richiesto contraddittorio – nei termini sopra indicati - preclude l'utilizzo, in questa sede, della documentazione acquisita tramite ordine europeo d'indagine dalla autorità giudiziaria francese, tanto in punto di gravi indizi, quanto in punto di esigenze cautelari, rendendo superfluo l'esame dei motivi in punto di utilizzabilità contenuti nelle memorie difensive.

- Die mit der EEA aus Frankreich übermittelten SkyECC-Daten werden als Beweise ausgeschlossen, da die Staatsanwaltschaft auch weiterhin nicht mitgeteilt hat, wie die Daten erhoben worden sind und damit die Verteidigung in die Lage versetzt, die Beweise zu prüfen und zu hinterfragen

**Vielen Dank für die Aufmerksamkeit!**

**Fragen?!**

**[cl@strafrecht-lb.de](mailto:cl@strafrecht-lb.de)**

**[www.strafrecht-lb.de](http://www.strafrecht-lb.de)**