# Praxisrubrik

*Lukas Theune**

## EncroChat

### – Begründet allein der Besitz eines sicheren Telefons einen hinreichenden Straftatverdacht, der den staatlichen Hack erlaubt?

Kammergericht, Beschluss vom 30.8.2021 – 2 Ws 79/21 gegen LG Berlin, Nichteröffnungsbeschluss vom 1.7.2021, (525 KLs) 254 Js 592/20 (10/21)

#### *I. Was ist EncroChat?*

Spektakuläre Bilder waren europaweit in den Medien zu sehen, nachdem französische und niederländische Behörden im Sommer 2020 nach und nach öffentlich gemacht hatten, welchen Datenschatz sie über die vergangenen vier Monate ausgebeutet hatten. „Folter-Container" in den Niederlanden, Bilder von großen Mengen illegalisierter Substanzen, Schusswaffen und anderem Verbotenem. Was war geschehen? Den französischen und niederländischen Ermittler*innen war es gelungen, über ein fingiertes Update, das in Wahrheit eine Schadsoftware enthielt, die Chats von Nutzer*innen eines sogenannten Kryptophones, also vermeintlich besonders gut gesicherter Mobiltelefone, live mitzulesen – inklusive sämtlicher geteilter Bilder. Freigiebig teilten sie den Schatz mit den anderen europäischen Ländern über einen Europol-Server, so auch mit der Bundesrepublik, je nachdem, wo die Nutzer*innen sich befanden; täglich übermittelte Europol die entsprechenden Daten an das Bundeskriminalamt.

Irgendwann fiel wohl einer Beamtin im Bundeskriminalamt auf, dass die Strafprozessordnung eigentlich Regeln für ein Strafverfahren vorsieht, zumal wenn es internationale Bezüge gibt. Im Juni, zwei Monate täglicher Lieferungen später, erließ die Generalstaatsanwaltschaft Frankfurt am Main eine Europäische Ermittlungsanordnung, auf die das Untersuchungsgericht in Lille die Genehmigung erteilte, die (längst erhaltenen) Daten nach Deutschland zu übersenden und in deutschen Strafverfahren zu verwenden. Vom Datenhub Frankfurt aus wurden die Nutzer*innen dann in sogenannten Trennverfahren selektiert und an die lokalen Staatsanwaltschaften weitergeleitet.

Dieses eher „hemdsärmelige" Vorgehen kollidiert vor allem mit zwei bürgerschützenden Regeln, einer europäischen und einer universalen, auch in der deutschen Strafprozessordnung verankerten. Zum einen ist dies die Richtlinie über die Europäische Ermitt-

* Rechtsanwalt und Strafverteidiger in Berlin.

DOI: 10.5771/0023-4834-2021-4-444

lungsanordnung (bzw. ihre Umsetzung im Gesetz über internationale Rechtshilfe – IRG) und zum anderen der Grundsatz, dass Ermittlungshandlungen einen Anfangsverdacht gegen die Betroffenen voraussetzen. Betroffen sind die Grundrechte des allgemeinen Persönlichkeitsrechts in seiner Ausprägung als Schutz der Vertraulichkeit und Integrität von informationstechnischen Systemen (im Folgenden: IT-Grundrecht) sowie das Telekommunikationsgeheimnis (Art. 10 GG).

Wie geht man um mit einem solchen Datenschatz, der so erlangt wurde?

## *II. Der Nichteröffnungsbeschluss des Landgerichts*

Die 25. Strafkammer des LG Berlin – Nichteröffnungsbeschluss vom 1.7.2021, (525 KLs) 254 Js 592/20 (10/21) – lehnte bereits die Eröffnung des Hauptverfahrens ab, hebt den Haftbefehl gegen einen Betroffenen auf und kommt sodann in den Gründen nach einer schulbuchmäßigen Prüfung zu dem einzigen aus rechtsstaatlicher Sicht vertretbaren Ergebnis: Es existiere keine „Strafverfolgung um jeden Preis."

### 1. Verstoß gegen die EEA-Richtlinie

> *„Wenn ein Mitgliedstaat den Telekommunikationsverkehr von Personen auf deutschem Hoheitsgebiet überwachen will, muss er die zuständige deutsche Stelle vor Beginn der Maßnahme (bzw. sobald ihm der Aufenthalt der Person bekannt wird) darüber unterrichten (Art. 31 Abs. 1 Richtlinie 2014/41/EU – im Folgenden: RiLi-EEA). Das dafür im Anhang C der Richtlinie vorgesehene Formblatt fordert unter anderem „alle erforderlichen Angaben, einschließlich einer Beschreibung des Falles (…), damit die unterrichtende Behörde bewerten kann, ob die Überwachung in einem ähnlichen innerstaatlichen Fall genehmigt würde und ob das dabei erlangte Material in einem Gerichtsverfahren verwendet werden kann". Kommt die deutsche Stelle auf der Grundlage dieser Angaben zu dem Ergebnis, dass die Maßnahme in einem vergleichbaren innerstaatlichen Fall nicht genehmigt würde, hat sie dieser binnen 96 Stunden zu widersprechen. Die ausländische Maßnahme kann dann nicht durchgeführt bzw. nicht fortgeführt werden; etwaige schon gesammelte Daten dürfen vom ersuchenden Staat nicht oder nur unter bestimmten Bedingungen verwendet werden (§ 91g Abs. 6, § 91c Abs. 2 Nr. 2 c) dd), § 59 Abs. 3 IRG; Art. 31 Abs. 3 RiLi EEA).*
>
> *Nach den bislang bekannt gewordenen Informationen ist davon auszugehen, dass es ein solches Ersuchen des französischen Staats und eine Überprüfung durch die zuständige deutsche Stelle hier nicht gegeben hat." (LG Berlin ebd., Rn. 25f.)*

Nun könnte man meinen, dass es sich hierbei um einen formalen Fehler handele, der – etwa durch die nachträgliche Korrespondenz zwischen Frankfurt und Lille oder einfach durch die Verwendung der Daten in den einzelnen Trennverfahren vor deutschen Gerichten – „geheilt" werden könnte. Doch das Landgericht erkennt in den Vorgaben der EEA-Richtlinie auch einen inhaltlichen Grund. Denn Deutschland etwa darf eine solche Überwachung von Personen auf deutschem Staatsgebiet nur dann überwachen, wenn es einen Anfangsverdacht gibt. Die flächendeckende Überwachung unzähliger Personen auf deutschem Staatsgebiet ist, gleich ob von deutschen oder ausländischen Polizeibehörden, mit dem Grundgesetz unvereinbar:

*„Die Prüfung nach Art. 31 RiLi-EEA, § 91g Abs. 6 IRG hätte hier ergeben, dass die Maßnahme mit den §§ 100a, 100b StPO nicht vereinbar ist. Der danach erforderliche qualifizierte Tatverdacht gegen die betroffenen deutschen Nutzer – einschließlich des hiesigen Angeschuldigten – lag nicht vor (…).*
*Dieser Umstand ist für die Frage der Verwertbarkeit auch unabhängig von dem formalen Verstoß gegen das Rechtshilferecht beachtlich. Die Überwachungsmaßnahme ist in vollem Umfang am Maßstab der deutschen Strafprozessordnung zu überprüfen." (LG Berlin, ebd., Rn. 28).*

2. Gab es einen hinreichenden Tatverdacht gegen den EncroChat-Nutzer?

Damit kommt das Gericht zum auch die Allgemeinheit interessierenden Kern der Auseinandersetzung. Der lässt sich im Wesentlichen in folgender Frage formulieren: Macht sich jemand allein dadurch verdächtig, dass er ein (vermeintlich) gut geschütztes Telefon zur Kommunikation erwirbt und nutzt?

Dies hatten das OLG Schleswig, das OLG Bremen, das OLG Rostock und das OLG Hamburg vor allem mit einer praktischerweise durch die französischen Behörden mitgelieferten Statistik bejaht. Demnach hatten sich bei rund zwei Drittel der von den französischen Behörden ausgewerteten Telefonen Hinweise auf kriminelle Nutzung (weiter differenziert wurde nicht) ergeben.

Das LG Berlin erteilt dem unter Hinweis auf den europäischen und deutschen Gesetzgeber eine Absage:

*„Die bloße Verwendung eines Krypto-Handys – auch eines solchen mit weit überdurchschnittlich hohem Sicherheitsstandard – lässt nicht nur keinen Schluss auf ein seiner Art nach und in zeitlicher Hinsicht zumindest in groben Zügen umrissenes strafbares Verhalten zu; sie trägt für sich gesehen (entgegen OLG Rostock (Beschlüsse vom 23. März 2021 – 20 Ws 70/21 –, juris Rn. 11 und vom 11. Mai 2021 – 20 Ws 121/21 –, BeckRS 2021, 11981 Rn. 14) sowie OLG Bremen (Beschluss vom 18. Dezember 2020 – 1 Ws 166/20 –, juris Rn. 16) nicht einmal den allgemeinen Schluss auf irgendeine Straftat.*
*Dass Straftäter häufig ein besonderes Interesse am Schutz ihrer Kommunikation gegen staatliche Zugriffe haben und deshalb schwer zu überwachende Kommunikationswege – etwa die VoIP-Telefonie über Messenger-Dienste oder den Tor-Browser – bevorzugen, ist allgemein bekannt. Ein genereller Schluss aus einem besonderen Sicherungsbedürfnis auf ein strafbares Verhalten wäre aber genauso unzulässig, wie etwa allein der Besitz von typischerweise bei Einbrüchen oder Fahrraddiebstählen genutzten Werkzeugen (Brechstangen, Bolzenschneider) nicht den für eine Durchsuchung nötigen Anfangsverdacht liefern kann.*
*Verschlüsselungstechnologien sind auch deshalb für sich gesehen kein tauglicher Anknüpfungspunkt für einen Tatverdacht, weil ihre Nutzung aus staatlicher Sicht nicht etwa unerwünscht ist, sondern im Gegenteil zum Schutz vertraulicher Daten vor den Zugriffen Dritter gestärkt werden soll. So heißt es in der Digitalen Agenda der Bundesregierung für 2014-2017 (S. 3), einfach zu nutzende Verschlüsselungsverfahren müssten gefördert werden, um „die wirtschaftlichen und gesellschaftlichen Potenziale des digitalen Wandels zu erschließen". Auf diese politischen Entscheidungen nimmt auch die Gesetzesbegründung zu §§ 100a, 100b StPO n.F. Bezug (BT-Drucksache 18/12785, S. 48).*

*Von der Möglichkeit, Anbieter derartiger Dienste zur Implementierung von „Hintertüren" (back doors) zu verpflichten, wollte der deutsche Gesetzgeber deshalb bewusst keinen Gebrauch machen (aaO., S. 48).*
*Allerdings drängt sich auf, dass (EncroChat) durch seine besonderen Sicherheitsvorrichtungen auch in besonderem Maße attraktiv für Kriminelle wurde; ein entscheidender Unterschied zu anderen verschlüsselten Diensten liegt darin aber nicht. Der besonders hohe Sicherheitsstandard machte (EncroChat) zudem gleichermaßen interessant für andere Personen mit ausgeprägtem Sicherungsbedürfnis – wie etwa Journalisten, politische Aktivisten, die eine staatliche Verfolgung oder die Beobachtung durch Geheimdienste fürchten, oder Mitarbeiter von Unternehmen, die sich vor Industriespionage schützen wollen. (…)*
*Die berechtigten Interessen der Nutzer ohne strafrechtlichen Hintergrund können so gewichtig gewesen sein, dass sie ohne Weiteres bereit waren, die vergleichsweise hohen, angesichts des technischen Aufwands aber auch nicht offensichtlich übersetzten Kosten für die Anschaffung und laufende Nutzung der...-Telefone zu akzeptieren. Auch unabhängig davon können die Preise der Telefone keinen Tatverdacht begründen. Diese liegen keinesfalls in einem typischerweise nur durch Straftaten zu erwirtschaftenden Bereich und entfernen sich nicht wesentlich von den Preisen für handelsübliche Mobiltelefone der Oberklasse, die ebenfalls weit über 1.000 € liegen können." (LG Berlin ebd., Rn. 41ff.).*

Und zuletzt widmet sich die 25. Strafkammer noch den angeführten Statistiken und Ermittlungserfolgen im Nachhinein:

*„Eine andere Beurteilung ist auch nicht mit Blick auf die durch die Maßnahme ermöglichten europaweiten Ermittlungserfolge geboten. Spätere Erkenntnisse, insbesondere solche aus der Überwachungsmaßnahme selbst, haben bei der Beurteilung des Tatverdachts außer Betracht zu bleiben; ob ein solcher begründet war, ist allein auf der Grundlage des Ermittlungsstandes zum Zeitpunkt der Anordnung zu beurteilen (BGH NStZ 1995, 510, 511). Zudem sind die Erfolge – so spektakulär etwa die großen sichergestellten Drogenmengen oder der in den Niederlanden entdeckte „Folter-Container" auch anmuten mögen – selbst rückblickend nicht geeignet, die Vermutung eines vollständig oder zumindest zum ganz überwiegenden Teil kriminellen Nutzerkreises zu bestätigen. Nach einer Mitteilung der Europäischen Kommission vom 14. April 2021 (COM/2021/170, abrufbar bei juris) waren bis zu diesem Zeitpunkt, d.h. fast ein Jahr nach Beendigung der Maßnahme, insgesamt nur 1500 Ermittlungsverfahren eingeleitet und 1800 Personen (entspricht 2,72% der Gesamtnutzer bzw. 5,54% der überwachten Nutzer) festgenommen worden." (LG Berlin, ebd., Rn. 54).*

### 3. Folge: Beweisverwertungsverbot

Damit ist klar, die Erhebung der Daten war unzulässig. Das Landgericht übergeht dann etwas überraschend die Frage nach der Verwendbarkeit der Daten in einem deutschen Strafverfahren.[1] Aber, weil von vornherein die sachlichen Voraussetzungen der Anordnung fehlten, folgt daraus jedenfalls ein Verwertungsverbot im Strafverfahren:

1 Vgl. dazu Derin/Singelnstein NStZ 2021, 449.

*„Im Fall der Telekommunikationsüberwachung sind ein Verwertungsverbot auslösende übergeordnete wichtige Gründe anzunehmen, wenn wesentliche sachliche Voraussetzungen für die Anordnung der Überwachungsmaßnahme fehlen (BGH, Beschlüsse vom 7. März 2006 – 1 StR 316/05 –, juris Rn. 7 m.w.N.; vom 1. August 2002 – 3 StR 122/02 –, juris Rn. 10). Das gilt erst recht, wenn es sich bei der Maßnahme um den besonders intensiven Eingriff der heimlichen Online-Durchsuchung bzw. Quellen-Telekommunikationsüberwachung handelt."* *(LG Berlin edd., Rn. 87).*

### *III. Kammergericht hebt Entscheidung des Landgerichts auf*

Mit Beschluss vom 30.8.2021 hat das Kammergericht indes die Entscheidung des Landgerichts wieder aufgehoben, und, weil die 25. Kammer sich „in einer Weise festgelegt (habe), die besorgen lässt, dass sie sich die Auffassung des Senats nicht innerlich zu eigen machen kann", das Verfahren bei einer anderen Kammer des Landgerichts eröffnet.

Die Argumente des Landgerichts überzeugen das Kammergericht nicht:

1. Es seien ja reine Zufallsfunde, keine bewussten Ermittlungsmaßnahmen gewesen:

Die Erkenntnisse gegen den Beschuldigten seien nämlich „Zufallsfunde" aus einem anderen Verfahren, weil ihnen kein förmliches Rechtshilfeersuchen deutscher Behörden vorausgegangen sei, sondern die Daten von sich aus von den französischen an die deutschen Behörden übermittelt worden seien. Von daher *„wäre es mit dem hinter dem Grundsatz der gegenseitigen Anerkennung stehenden Gedanken des gegenseitigen Vertrauens der Mitgliedstaaten der Europäischen Union nicht zu vereinbaren, eine in einem Mitgliedstaat ergangene, dort nicht aufgehobene gerichtliche Entscheidung in einem anderen Mitgliedstaat mit der Begründung als rechtswidrig zu bewerten, die Gerichte des Entscheidungsstaates hätten ihre eigene nationale Rechtsordnung nicht eingehalten."* (KG, ebd.)

2. Nun sind die Daten halt da:

Zwar gesteht auch das Kammergericht zu, dass *„die Anordnung der von den französischen Behörden durchgeführten Ermittlungsmaßnahmen nach bisherigem Erkenntnisstand nicht den Anforderungen zu genügen scheinen, die nach deutschem Recht an eine Überwachung des internetbasierten Datenaustausches und der Telekommunikation zu stellen wären."* Denn nach deutschem Recht ist *„eine verdachtslose Überwachung der Kommunikation dagegen grundsätzlich unzulässig"* (KG, ebd.).

Allerdings ist das Kind ja nun ohne deutsche Veranlassung in den Brunnen gefallen und die Daten sind da: *„Die ermittelten Daten sind anfänglich vielmehr ohne vorherige Absprache spontan an die deutsche Polizei übermittelt worden."* (KG, ebd.).

3. Außerdem: gute Verschlüsselung ist doch verdächtig

Das Kammergericht geht aber auch darüber hinaus und findet schon die Nutzung guter Verschlüsselungstechnik verdächtig genug: *„Schon die Nutzung der mit Verschlüsselungstechnik versehenen, hochpreisigen Endgeräte begründete im Übrigen jedenfalls vor dem Hintergrund der französischen Ermittlungsergebnisse in den Ausgangsverfahren wegen der Beteiligung am organisierten illegalen Betäubungsmittelhandel einen entsprechenden Anfangsverdacht gegen die Nutzer solcher — für eine konventionelle Kommunikation eher ungeeigneter — Geräte."*

4. Nichts gegen Frankreich, das Mutterland der Menschenrechte

Schließlich kommt dann noch ein Argument, dass die deutschen Gericht schon seit dem Reichsgericht gern heranziehen, wenn etwas „halt nicht sein kann": *„Die Nichtverwertung von legal durch Behörden der Republik Frankreich — nicht nur eines Gründungsmitgliedes der europäischen Union, sondern auch eines der Mutterländer des modernen Menschenrechtsverständnisses — beschaffter Informationen über derart schwerwiegende Straftaten, verstieße auch in erheblicher Weise gegen das allgemeine Gerechtigkeitsempfinden der rechtstreuen Bevölkerung."*

Damit offenbart der 2. Senat des Kammergerichts – im Übrigen im Einklang mit den Oberlandesgerichten Schleswig, Bremen, Hamburg und Rostock – en passant das gewichtigste Argument für die Verwendung und Verwertung des vergifteten Apfels, des Datenschatzes aus Frankreich: des Volkes Zorn, oftmals artikuliert durch Boulevardpresse und social media. Neben der von Burhoff aufgeworfenen Frage, ob diejenigen, die die Verwendung und Verwertung kritisch sehen, keine rechtstreuen Bürger*innen mehr seien,[2] handelt es sich bei dem Konstrukt der idealisierten „rechtstreuen Bevölkerung" (die es aus kriminologischer Sicht ohnehin nicht geben dürfte) um eine empirisch nicht belegte Größe, die auch und gerade in Deutschland vor historischen Hintergründen besonders kritisch betrachtet werden sollte.

Die Entscheidung des Kammergerichts ist, so erwartbar sie war, enttäuschend. Verschlüsselte Kommunikation ist erwünscht und nicht verdächtig. Die Begehrlichkeiten der Polizeien und Staatsanwaltschaften werden weiter auf verschlüsselte Kommunikation zielen; der Gesetzgeber hat dafür mittlerweile die sog. Online-Durchsuchung und die Quellen-TKÜ in den §§ 100a und 100b StPO normiert. Er hat dafür Voraussetzungen aufgestellt, die denen des LG Berlin entsprechen. Vor allem ist ein auf bestimmten Tatsachen begründeter Verdacht einer konkreten (schweren) Straftat erforderlich. Damit zeigt sich zugleich, dass allein die Nutzung verschlüsselter Kommunikation einen solchen Tatverdacht nicht begründet. Denn wenn dem so wäre, wären ja keine weiteren Voraussetzungen notwendig, um den staatlichen Angriff auf die verschlüsselten Systeme zu rechtfertigen.

Letztendlich wird EncroChat wohl noch das Bundesverfassungsgericht und wohl auch den Europäischen Gerichtshof für Menschenrechte beschäftigen.

2 https://blog.burhoff.de/2021/09/63718/.