Kommunikation & Recht

Betriebs-Berater für
● Medien ● Telekommunikation ● Multimedia

6
K&R

25. Jahrgang Juni 2022 Seiten 385 – 464

dfv Mediengruppe · Frankfurt am Main

RA Dr. Florian Deusch und Prof. Dr. Tobias Eggendorfer*

Generalverdacht durch Verschlüsselung?

Konsequenzen für IT-Nutzer aus der aktuellen EncroChat-Rechtsprechung

Kurz & Knapp

Der BGH hat ein Strafurteil gegen einen Drogendealer bestätigt. Die Tatnachweise beruhten auf der Überwachung von Kryptophones vom Typ „EncroPhone" durch französische Behörden. Diese Smartphones sind nach werbenden Angaben des Herstellers u. a. mit dem Ende-zu-Ende-verschlüsselten EncroChat-Messenger und weiteren Funktionen, die ein Abhören unmöglich machen sollen, ausgestattet. Die Verteidigung kritisierte die Beweiserhebung und -verwertung. Die Autoren diskutieren, ob dieses Urteil Konsequenzen für andere Verschlüsselungsdienste und deren Nutzer haben kann.

I. Der BGH-Beschluss und die Folgefragen für IT-Nutzer

Der BGH hat sich der „EncroChat-Rechtsprechung" zahlreicher Oberlandesgerichte angeschlossen und die Daten, die die französische Polizei mittels Quellen-TKÜ und Online-Durchsuchungen von infiltrierten Kryptohandys gesammelt hat, als verwertbares Beweismittel eingestuft.[1] Vorliegend stehen die IT-rechtlichen Folgefragen aus dieser Entscheidung für die Nutzung von Verschlüsselungstechnologien zur Diskussion.

1. Der BGH-Fall

In seinem Beschluss vom 2. 3. 2022 bestätigte der BGH das Strafurteil des LG Hamburg gegen einen Drogendealer. Wesentliche Beweismittel waren Nachrichten aus dem Ende-zu-Ende-verschlüsselten Messenger-Dienst EncroChat. Sie waren die Ergebnisse von Ermittlungen der französischen Polizei. Diese hatte festgestellt, dass ertappte Drogendealer für ihre Geschäfte sogenannte Kryptohandys nutzten. Sie waren mit dem Betriebssystem und Kommunikationssoftware des Anbieters EncroChat insbesondere für eine Ende-zu-Ende-Verschlüsselung ausgestattet nebst weiteren Funktionalitäten zur Wahrung der Anonymität. Auch die Vertriebskanäle waren auf Anonymität von Käufern und Verkäufern ausgerichtet. Auf Grundlage richterlicher Beschlüsse beschlagnahmten sodann die französischen Behörden Daten auf Servern von EncroChat und überwachten die Datenübertragungen von und zu diesen Servern, Telefonen und Systemen, soweit sie mit den EncroChat-Domainnamen in Verbindung standen.[2]

Etwas kryptisch formuliert der BGH in den Rn. 12 - 17, dass die Behörden auf den Servern und den hierüber identifizierten Mobiltelefonen mutmaßlich über ein Systemupdate eine Überwachungssoftware („Staatstrojaner"[3]) installiert und so die Inhalte der Nachrichten ermittelt haben. Die Software konnte die Daten lokal vor der Verschlüsselung abgreifen, soweit aus den Feststellungen zu erkennen ist,[4] ist die Verschlüsselung selbst nicht kompromittiert worden. Laut BGH-Beschluss waren 32 477 Telefone betroffen.[5] Die Verteidigung wendet sich gegen die Verwertung dieser Daten und hat dazu Verfassungsbeschwerde angekündigt.[6]

2. Argumentation der EncroChat-Rechtsprechung

Laut BGH erfüllt die Überwachung der infiltrierten Telefone und des Servers durch die französische Polizei alle gebotenen rechtsstaatlichen Anforderungen.[7] Folgende Kriterien schaffen für den BGH ausreichende Verdachtsmomente gegen die ermittelten EncroChat-Nutzer:[8]

– Die Encrochat-Geräte waren offiziell im Handel nicht erhältlich (allerdings laut Rn. 10 des BGH-Beschlusses auf der Internetplattform eBay).
– Die Geräte waren sehr teuer in Anschaffung und Betrieb.[9]
– Die Herstellerfirma war nicht ermittelbar.

---

* Strafprozessuale Fragen sind nicht Schwerpunkt dieser Abhandlung. Mehr über die Autoren erfahren Sie am Ende des Beitrags. Alle zitierten Internetquellen wurden zuletzt abgerufen am 5. 5. 2022.

1 BGH, 2. 3. 2022 – 5 StR 457/21 – juris = K&R 2022, 433, dort z. B. in Rn. 24 auch die Bezugnahmen auf die OLG-Entscheidungen, namentlich etwa Beschluss OLG Rostock, 23. 3. 2021 – 20 Ws 70/21, BeckRS 2021, 6824; ebenso OLG Bremen, 18. 12. 2020 – 1 Ws 166/20 und OLG Hamburg, 29. 1. 2021 — 1 Ws 2/21 und in Rn. 25 unter Zurückweisung der Kritik von *Deusch/Eggendorfer*, K&R 2021, 689, 695, Fn. 50.

2 Diese Angaben sind dem BGH, K&R 2022, 433 zu entnehmen und die Interpretation der Autoren aus den dortigen Angaben. Sie entsprechen auch den Informationen der Tagespresse zu dem Fall (https://www.zeit.de/digital/2022-03/bgh-entscheidung-encrochat-daten-kriminelle?utm_referrer=https%3A%2F%2Fwww.google.com%2F; https://www.faz.net/aktuell/gesellschaft/kriminalitaet/bgh-encrochat-daten-duerfen-bei-schwerenstraftaten-verwendet-werden-17908412.html).

3 In technischer Hinsicht ist die Bezeichnung „Staatstrojaner", wenn auch umgangssprachlich, kaum zutreffend: Hier wurde allen Angaben nach eine manipulierte Betriebssystem-Version über die vorgesehenen Updatekanäle verbreitet.

4 Siehe Nachweise in Fn. 2.

5 Presseberichte, die von bis zu 70 000 Telefonen und mehreren 10 000 Nutzern berichten, lassen sich nicht abschließend bestätigen, da die französischen Behörden die Ermittlungsdetails als Staatsgeheimnis behandeln (https://www.deutschlandfunkkultur.de/encro-chat-hack-ueberwachung-daten-100.html; https://netzpolitik.org/2022/encrochat-ermittlungen-strafverfahren-jenseits-des-rechtsstaats/).

6 Zuvor hatte der BGH durch Beschl. v. 8. 2. 2022 – 6 StR 639/21 ebenfalls die Verwertung von EncroChat-Daten bejaht; hiergegen wird in https://www.lto.de/recht/justiz/j/bverfg-encrochat-bgh-daten-kommunikation-deutschland-frankreich-krypto-verwertbarkeit-strafrecht/ von einer Verfassungsbeschwerde mit dem Aktenzeichen 2 BvR 558/22 berichtet, ebenso zur Verfassungsbeschwerde gegen den BGH-Beschluss gemäß Fn. 1.

7 In Deutschland richten sich diese Maßnahmen nach den §§ 100a, 100b StPO (QuellenTKÜ, Online-Durchsuchung), so LG Berlin, 1. 7. 2021 – (525 KLs) 254 Js 592/20 (10/21) – juris. Da die Beweise durch französische Behörden gewonnen wurden, prüft der BGH die dazu maßgeblichen Rechtshilfevorschriften, insbesondere RL 2014/41/EU (EEA) i. V. m. §§ 91a ff. IRG, die eine Prüfung der verfassungsrechtlichen Maßstäbe im Sinne des ordre public verlangen, siehe BGH, K&R 2022, 433, Rn. 26 - 31.

8 BGH, K&R 2022, 433, Rn. 35 - 37.

9 1610,00 € einschließlich Nutzerlizenz für 6 Monate, BGH, K&R 2022, 433, Rn. 35, ein Preis, der allerdings mit höherwertigen aktuellen Smartphones gut vergleichbar ist, ein iPhone 13 Pro 1 TB z. B. kostete am 1. 5. 2022 1829,00 €, https://www.apple.com/de/shop/buy-iphone/iphone-13-pro/6,7%22-display-1tb-silber.

– Die Geräte waren ausdrücklich damit beworben, dass man damit dem Zugriff der Polizei entgehen kann.[10]
– Laut Angaben von in Frankreich festgenommenen Beschuldigten[11] waren deren Kryptohandys ausschließlich für den Drogenhandel bestimmt. Der BGH nimmt dabei in Rn. 36 Bezug auf die „Analyse weiterer Nutzerdaten ab dem 1. 4. 2020", die laut Rn. 18 ergab, dass von 32 477 überwachten Telefonen 380 Geräte in Frankreich benutzt wurden und hiervon 63,7 % (242 Telefone) für kriminelle Zwecke, mehrheitlich von Drogenhändlern. Die übrigen 138 in Frankreich verwendeten Telefone seien inaktiv oder noch nicht ausgewertet.

Hieraus folgert der BGH, dass das EncroChat-Netzwerk von vornherein auf kriminelle Aktivitäten ausgerichtet sei. Jeder EncroChat-Nutzer sei der organisierten Kriminalität wie Drogen- und Waffenhandel oder Geldwäsche verdächtig. Ausdrücklich nimmt der BGH[12] auf obergerichtliche Entscheidungen Bezug wie z. B. den Beschluss des OLG Rostock v. 11. 5. 2021 (20 Ws 121/11, NJ 2021, 372, dort Leitsatz 1 und Rn. 17):

„Schon die Verwendung eines Krypto-Handys der Firma EncroChat deutet auf ein konspiratives Verhalten zur Begehung und Verdeckung von Straftaten hin."[13]

3. Folgefragen für die Nutzung von Verschlüsselungssystemen

Verschlüsselungssysteme sind in der IT-Sicherheit Stand der Technik und gängige Praxis in herkömmlichen IT-Anwendungen und Systemen. Sie schützen die Vertraulichkeit der verarbeiteten Daten. Im Finanz- und Gesundheitswesen z. B. ordnet der Gesetzgeber die Verschlüsselung ausdrücklich an, Art. 32 DSGVO benennt ausdrücklich die Verschlüsselung als Element des Datenschutzes. Auch Geschäftsgeheimnisse können Verschlüsselung gemäß § 2 Nr. 1 GeschGehG verlangen, ebenso Vertragspflichten in NDA oder Entwicklungsverträgen.[14] Darüber hinaus gibt es Situationen, in denen effektive Verschlüsselung – auch mit „EncroChat-vergleichbaren" Funktionen – sinnvoll und legitim sind (siehe unten Abschnitt II. Ziffer 5.). Die Verschlüsselungstechnik selbst unterscheidet aber nicht, ob die betroffenen Informationen kraft Gesetzes zu schützen sind, eine legitime oder moralische Rechtfertigung haben oder krimineller Natur sind. Somit stellt sich die Frage, ob die BGH-Kriterien aus Ziffer 2 passend sind, um eine kriminalitätsverdächtige Verschlüsselung abzugrenzen von legalen Verschlüsselungssituationen.

Aus diesem Grund stellt Abschnitt II. die „EncroChat-Technologie" im Vergleich zu anderen Verschlüsselungswerkzeugen dar.

II. Technischer Hintergrund

Die Anbieter von Kryptophones sowie der BGH suggerieren, dass nur Kryptophones eine verschlüsselte und damit vertrauliche Kommunikation ermöglichen, herkömmliche Smartphones jedoch nicht. Dieser Abschnitt untersucht die Unterschiede und gibt einen Überblick über Verschlüsselung, Angriffe auf Verschlüsselung und übliche Anwendungsgebiete.

1. Smartphone vs. Kryptophone

Smartphones mit den Betriebssystemen iOS und Android nutzen intensiv Verschlüsselungstechnologien: So verschlüsseln beide den persistenten Speicher,[15] Kommunikation erfolgt in der Regel verschlüsselt, so z. B. mit Webseiten über HTTPS, E-Mail nutzt zumindest soweit möglich für Teilstrecken bei der Übertragung TLS, sogar eine automatische Mail-Verschlüsselung mit S/MIME bieten die Systeme an.[16]

Kryptophones versuchen, durch zusätzliche Software eine erhöhte Sicherheit zu vermarkten. So sind Chat- oder Messengerprogramme so implementiert, dass sie im Idealfall die Daten lokal nur verschlüsselt ablegen und Ende-zu-Ende-verschlüsselt mit dem Gesprächspartner austauschen. Eine Funktion, die auch auf herkömmlichen Smartphones z. B. mit den Messengern Signal, Wire und Threema[17] gegeben ist.

Weiterhin bieten sie ein automatisches Löschen bei mehrfacher falscher PIN-Eingabe – iOS bietet das auch an, löscht allerdings nicht das Gerät selbst, sondern aus Effizienzgründen nur den verschlüsselten Entschlüsselungsschlüssel für den persistenten Speicher, wodurch sich dessen Inhalt nicht mehr rekonstruieren lässt.

Kryptophones bieten verschlüsselte Telefonate, in der Regel über Voice-Over-IP. Ebenfalls eine Funktion, die sich mit Signal, Wire und Threema problemlos nachbilden lässt.

So hat das von *Benner* untersuchte „Anophone",[18] ein dem Encrophone grob vergleichbares Produkt,[19] als wesentliche Vorteile eine in sich stimmige Konfiguration, die ein versehentliches Nutzen unverschlüsselter Anwendungen verhindert. Es bietet darüber hinaus den Vorteil, dass, einigen sich zwei Parteien auf den Einsatz des Anophones,

10 Die Funktionalitäten des Handys können in der Tat dazu eingesetzt werden, siehe Rn. 9, 23 des BGH-Beschlusses K&R 2022, 433.
11 Beachtenswert ist, dass in den gegenständlichen Verfahren überwiegend Drogendealer Beschuldigte waren, die zu ihrem Tatzweck Kryptophones gekauft haben. Aus der Befragung einer Subgruppe, egal ob Dealer oder auch sonstiger Straftaten Beschuldigter, auf die Grundgesamtheit aller Nutzer zu schließen, ist erkennbar unsinnig.
12 BGH, K&R 2022, 433, Rn. 37.
13 Die Verfasser haben derartige Formulierungen der obergerichtlichen Rechtsprechung in K&R 2021, 689, 695 kritisch bewertet, daher die Bezugnahme im BGH-Beschl. v. 2. 3. 2022 – 5 StR 457/21, K&R 2022, 433, Rn. 25.
14 Siehe unten Abschnitt II., zu den gängigen Verschlüsselungsverfahren *Deusch/Eggendorfer*, in: Taeger/Pohle (Hrsg.), Computerrechtshandbuch, 36. EL 2021, Kap. 50.1, Rn. 172 ff. (zum GeschGehG dort Rn. 421), zu den rechtlichen Pflichten zur Verschlüsselung z. B. *Voigt*, in: Voigt, IT-Sicherheitsrecht, 2. Aufl. 2021, Teil E Kap. IV, Rn. 193, 202, generell zu den einzelnen gesetzlichen und vertraglichen Pflichten vertraulicher und verschlüsselter Kommunikation *Deusch/Eggendorfer*, K&R 2015, 11, 15 ff.
15 Dauerhafter Speicher, im Gegensatz zum flüchtigen Arbeitsspeicher (RAM), der bei Verlust der Spannungsversorgung seine Daten verliert. Im Rechner ist dies vergleichbar zur Festplatte.
16 Beispielhaft für Apple iOS: https://support.apple.com/en-au/guide/security/sece3bee0835/web und https://developer.apple.com/documentation/safari-release-notes/safari-12_1-release-notes.
17 https://threema.ch/de, https://www.wire.com, https://www.signal.org.
18 *Benner*, Konzept für die Sicherheitsanalyse von verschlüsselten Smartphones am Beispiel AnoPhone, Masterarbeit, Hochschule Ravensburg-Weingarten, 2022.
19 Das „Anophone" (https://ano-phone.de/); ist nicht zu verwechseln mit dem in Rn. 24 des BGH-Beschlusses v. 2. 3. 2022 – 5 StR 457/21 genannten Krypto-Anbieter „Anom". Dass es in Rn. 24 des BGH-Beschlusses „Anon" heißt, ist offensichtlich einem Druckfehler geschuldet. Denn der BGH verweist ausdrücklich auf den „Anom"-Fall des OLG Frankfurt a. M., 22. 11. 2021 – 1 Hes 427/21, NJW 2022, 710. Die Vielzahl der Anbieter deutet sowohl an, dass der Aufwand, aus handelsüblichen Smartphones Kryptophones zu machen, überschaubar ist, als auch, dass es wohl einen großen Bedarf für solche Produkte gibt.

sie sich nicht mehr über Details, wie den Messenger oder das Telefonieprogramm verständigen müssen. Ansonsten zeigte sich das Anophone als relativ seriennahes, ursprünglich preisgünstiges (ca. 200 € laut *Benner*) Android-Smartphone, das fertig konfiguriert zum rund dreifachen Preis angeboten wurde.

Das Encrophone im BGH-Verfahren ist nicht wesentlich anders. Bemerkenswert ist dort der eigene, verschlüsselte Messenger-Dienst „EncroChat". Ob das nun ein Sicherheitsvorteil ist, ist fraglich. Denn gängige, sichere Messengerprotokolle sind von Dritten prüfbar, die Sicherheit basiert also nicht nur auf Herstellerangaben.

2. Arten der Verschlüsselung

Beim Thema Verschlüsselung taucht in der juristischen Literatur[20] regelmäßig die Unterscheidung zwischen „transportverschlüsselt" und „End-zu-End-verschlüsselt" (E2E) auf. Erstere ist ursprünglich dafür gedacht, dass während der Übertragung von einem Server zu einem anderen Dritten z. B. das Log-In-Passwort für den E-Mail-Account nicht mitlesen können, während zweitere auch sicherstellt, dass der Serverbetreiber keinen Einblick z. B. in die Mails erhält.

In der „Offline-Welt" ist Transportverschlüsselung einem Briefumschlag vergleichbar, der in jedem Postverteilzentrum entfernt und durch einen neuen ersetzt wird. Jeder in den Verteilzentren könnte damit den Brief lesen.

E2E-Verschlüsselung dagegen ist einem versiegelten Umschlag vergleichbar, den erst der Empfänger wieder entsiegeln kann. Naturgemäß stellt nur dieses Verfahren Vertraulichkeit tatsächlich sicher[21] – auch, wenn sich in der Diskussion immer wieder Klimmzüge finden, die eine Gegenmeinung verargumentieren wollen.

E2E-Verschlüsselung setzt voraus, dass die beiden Kommunikationspartner untereinander ihre Schlüssel tauschen. Dafür verfügen diverse Verschlüsselungsverfahren über eigene Vorgehensweisen. In den meisten Messenger-Diensten wie z. B. Wire, Threema, Signal sind entsprechende Funktionen implementiert. Threema z. B. bietet als weitere Option die Möglichkeit, einen QR-Code auf dem Telefon des Kommunikationspartners zu scannen und so den Schlüssel zu verifizieren.

3. Angriffe auf Verschlüsselung

Der Wunsch des ehemaligen Bundesinnenministers *Seehofer* nach einer staatlich gelieferten Verschlüsselung mit Hintertür für Ermittlungsbehörden („Sicherheit trotz und mit Verschlüsselung") lässt erkennen,[22] dass Verschlüsselung schwer anzugreifen ist. In der Mathematik und Informatik befasst sich die Kryptanalyse mit dem Knacken von Schlüsseln. In der Regel ist ein Angriff auf einen positiv evaluierten Algorithmus schwer, so gelten RSA, AES oder IDEA als schwer zu knacken. In der Praxis jedoch finden sich häufig Implementierungsfehler, die Angriffe ermöglichen – so sind vielleicht erforderliche Zufallswerte vorhersagbar, verwendete Primzahlen zu dicht nebeneinander oder anderweitig vorhersagbar.[23] Gelegentlich erlauben auch Hardwarebesonderheiten, wie die in den Sicherheitslücken Spectre und Meltdown ausgenutzten Effizienzsteigerungsverfahren von Prozessoren, Angriffe auf Schlüssel.[24] Genau diese Schwierigkeit, gute Verschlüsselung zu knacken, motivierte den ehemaligen Minister Seehofer zu seinem technisch unsinnigen Vorschlag.[25] In der Vergangenheit haben vorgesehene Lücken in Verschlüsselung immer schwere Folgen gehabt.[26]

4. Verschlüsselung in der IT

Verschlüsselte Kommunikation ist heutzutage in der IT eher als Standard, denn als Sonderfall anzusehen. So melden viele Browser beim Versuch, auf eine Webseite ohne verschlüsseltes HTTPS, also über offenes HTTP zuzugreifen, einen Fehler und zeigen die gewünschte Seite überhaupt nicht mehr an. Viele Mailprovider erzwingen für den Download von E-Mails in das eigene Mailprogramm und zur Übertragung für deren Versand eine Transportverschlüsselung.[27]

5. Gründe für den Einsatz von Encrophone, Anophone usw.

Verschlüsselung ist aus technischer Sicht ein notwendiger Sicherheitsstandard, der gegen eine Vielzahl von Angriffen auf die Vertraulichkeit der Kommunikation schützt. Nun mag man argumentieren, dass Verschlüsselung, soweit sie Standard ist, auch in Standard-Smartphones eingebaut ist, daher seien spezielle Kryptophones ungewöhnlich. Allerdings gibt es eine Vielzahl von Anwendungsfällen für sichere und fertig konfigurierte Verschlüsselung, wie sie die Kryptophones als wesentlichen Vorteil gegenüber Standardprodukten bieten:[28]

- Berufe, die der Schweigepflicht (§ 203 StGB) unterliegen, im Verhältnis zu ihren Mandanten, Klienten oder Patienten,[29]
- Journalisten, insbesondere investigative Journalisten, oder solche, die sich auf eine Berichterstattung aus ausländischen Staaten vorbereiten, die nicht über die EU-Standards zum Schutz der Privatheit und des Fernmeldegeheimnisses verfügen,

20 Siehe z. B. *Maseberg/Meyer/von Rahden/Schläger/Schmidt*, in: Schläger/Thode, Handbuch Datenschutz und IT-Sicherheit, 2. Aufl. 2021, Kap. 1, Rn. 108. Für diesen Aufsatz nicht relevant ist die kryptologisch wichtige Unterscheidung zwischen symmetrischer, asymmetrischer und hybrider Verschlüsselung, dazu mehr bei *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 14), Rn. 172 - 198.

21 *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 14), Rn. 172 - 198.

22 Entschließung des Rates zur Verschlüsselung – Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung v. 24. 11. 2020, Dokument-Nr. 13084/1/20 des Rates der EU, https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/de/pdf; dazu *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 14), Rn. 198, 280, kritisch ebenso *Taeger/Schiffner/Schmitz*, DSRITB 2021, 289 ff., 302.

23 Siehe u. a. *Inan*, Algorithm for a time efficient calculation of the statistical distribution of primes, Security & Management, 2019, *ders.*, Statistical analysis of prime number generators putting encryption at risk, Security & Management 2020.

24 Siehe z. B. *Percival*, Cache Missing for Fun and Profit, BSDCan, 2005; *Osvik/Shamir/Trome*, Cache Attacks and Countermeasures: the Case of AES (Extended Version), 2005; *Liu/Yarom/Ge/Heiser/Lee*, Last-Level Cache Side-Channel Attacks are Practical, IEEE Symposium on Security and Privacy, 2015; *Yarom/Genkin/Heninger*, CacheBleed: A Timing Attack on OpenSSL Constant Time RSA, 2016; *Kocher* et al., Spectre Attacks: Exploiting Speculative Execution, 2017; *Lipp* et al., Meltdown: Reading Kernel Memory from User Space, 2017.

25 Siehe Fn. 22.

26 So z. B. der FREAK-Angriff (https://freakattack.com/), siehe auch *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 14), Rn. 198.

27 Die werbewirksame Kampagne „E-Mail made in Germany" in Folge der Snowden-Enthüllungen war allerdings Augenwischerei, die NSA könnte transportverschlüsselte Mails auf den dazwischengeschalteten Servern abgreifen, auch in Deutschland sind Mailprovider zu einer entsprechenden Kooperation aus TKÜV verpflichtet.

28 Siehe dazu oben Abschnitt II. 1.

29 Dies soll nicht suggerieren, dass schweigepflichtige Berufsträger stets Kryptophones zur mandantenbezogenen Kommunikation verwenden (oder verwenden müssten); gleichwohl kann es sinnvolle Einsatzfälle dafür geben.

– Ermittler, unabhängig, ob behördlich oder privat,
– Dissidenten, Exilanten und andere politisch verfolgte Personengruppen, die Kontakte unterhalten müssen.
– Die Wissenschaft kann Bedarf nach Kryptophones haben, sei es zu Forschungszwecken oder zur Geheimhaltung spezifischer Forschungsergebnisse oder -vorhaben.
– Auch zum Schutz vor *Industriespionage* könnten die Schutzfunktionen von Kryptohandys fruchtbar gemacht werden. Das BMI rät insbesondere bei Auslandsreisen zu spezifischen Schutzmaßnahmen und zur Vorsorge gegen das Abhören von Handys, die zwar nicht den Einsatz eines Kryptohandys voraussetzen, sich aber damit durchaus umsetzen ließen.[30]
– Presseberichten zufolge haben die Mitglieder des NSA-Untersuchungsausschusses des Deutschen Bundestags Kryptohandys erhalten, um das Gremium gegen Ausforschung zu schützen.[31]
– In der Vergangenheit hat sich oft gezeigt, dass verschlüsselte Kommunikation in politisch schwierigen Situationen hilfreich war, um Veränderung zu bewirken, man denke an den arabischen Frühling oder die Demonstrationen in HongKong.

III. Nutzung von Verschlüsselung ohne Straftatverdacht?

Der BGH-Beschluss führt das rechtliche Risiko für Nutzer herbei, sich durch Verschlüsselung einem Straftatverdacht auszusetzen.

1. Problematik aus der kriminellen Nutzung von Kryptophones und der BGH-Rechtsprechung

Abschnitt I. hat gezeigt, dass Kryptohandys in der organisierten Kriminalität zur Organisation, Begehung und Verdeckung von schweren Straftaten eingesetzt und dort auch so beworben werden. Es gibt Täter, die diese Geräte aufgrund ihrer spezifischen Funktionalitäten ausschließlich für ihre kriminellen Zwecke einsetzen.

Abschnitt II. hat gezeigt, dass Verschlüsselung in der IT-Praxis eher die Regel ist als die Ausnahme. Weiter ist festzustellen, dass die Funktionalitäten der Kryptophones größtenteils bereits in herkömmlichen IT-Anwendungen verwendet werden (Abschnitt II. Ziffer 1. und 2.).

Weiter gibt es Situationen, in denen Krypto-Funktionalitäten, die mit den verfahrensgegenständlichen EncroChat-Phones vergleichbar sind, zu legitimen Zwecken eingesetzt werden (sogar von Bundestagsmitgliedern mit geheimhaltungsbedürftigen Aufgaben, siehe Abschnitt II. Ziffer 5.).

Ein weiteres Beispiel:

Der Geschäftsführer eines Unternehmens beabsichtigt eine Reise ins Ausland mit erhöhter Gefahr für Industriespionage. Er fragt seinen Datenschutzbeauftragten, ob ein Kryptophone geeignet ist, um die Kontaktdaten seiner Ansprechpartner i. S. v. Art. 32 DSGVO hinreichend vor unbefugter Kenntnisnahme zu schützen.

Anhand der BGH-Kriterien gemäß Abschnitt I. Ziffer 2. müsste der Datenschutzbeauftragte dem Geschäftsführer zum Einsatz eines Handys raten, das

– (zusammen mit der Kryptosoftware) weniger als € 1600,00 kostet,[32]
– über einen offiziellen Vertriebskanal verfügbar ist (wobei eBay hierfür nicht ausreichen würde),
– nicht zur Verdeckung von Straftaten beworben wird.
– Zudem darf der Anteil an kriminellen Nutzern dieses Handytyps nicht größer als 63 % sein.[33]

Dieses bewusst überzeichnete Fallbeispiel soll zeigen, dass ein Bedarf besteht, die kriminelle Nutzung von Verschlüsselung von der legalen Anwendung abzugrenzen. Die bisherigen BGH-Kriterien sind dazu nicht geeignet.

2. Unschuldsvermutung und Rechtsstaatlichkeit als Maßstäbe für die Abgrenzung zwischen Tatverdacht und unverdächtiger IT-Nutzung

Die Unschuldsvermutung gemäß Art. 6 Abs. 2 EMRK, 48 Abs. 1 EU-Grundrechtecharta i. V. m. mit dem Rechtsstaatsprinzip verlangt, den Strafanspruch in einem justizförmig geordneten Verfahren durchzusetzen, das eine wirksame Sicherung der Grundrechte des Beschuldigten gewährleistet. Dem Täter müssen Tat und Schuld nachgewiesen werden. Dabei steht eine Beweislastumkehr der Unschuldsvermutung entgegen.[34] Die Schlussfolgerung des BGH und die Formulierung zahlreicher OLG-Entscheidungen (EncroChat-Nutzer = Tatverdacht)[35] erscheinen nach diesem Maßstab eher unglücklich gewählt.

Die Unschuldsvermutung verhindert nicht, im Ermittlungsverfahren Entscheidungen zu Lasten des Beschuldigten zu treffen, um dessen Tatbeitrag und Schuld nachzuweisen, zum Beispiel durch Beschlagnahmen, Durchsuchungen, Abhörung der Kommunikation oder Online-Durchsuchungen. Allerdings setzen derartige Maßnahmen stets die Feststellung eines ggf. qualifizierten Tatverdachts voraus.[36]

Der Abschnitt II. und das Beispiel in Ziffer 1. zeigen, dass die BGH-Kriterien der EncroChat-Rechtsprechung (Abschnitt I. Ziffer 2.) auch rechtschaffene IT-Nutzer zu tatverdächtigen Beschuldigten machen können.

Ohne weitere Kriterien zur Abgrenzung des Tatverdachts vom legitimen Verschlüsselungseinsatz bleibt die Rechtsunsicherheit, sich von einem Tatverdacht entlasten zu müssen, den andere Teilnehmer eines Verschlüsselungsnetzwerks geschaffen haben.

30 So z. B. Seite 8 des BMI-Ratgebers „Leitfaden Wirtschaftsschutz“ (https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/leitfaden-wirtschaftsschutz.pdf?__blob=publicationFile&v=1).

31 https://www.golem.de/news/bsi-kryptohandys-kaum-anschluss-unter-dieser-nummer-1412-111290-2.html. https://www.sueddeutsche.de/politik/krypto-handy-nsa-ausschuss-wurde-womoeglich-opfer-von-spionage-angriff-12376857.

32 Stand zum BGH-Beschluss gemäß Fn. 1 am 2. 3. 2022; in künftigen Sachverhalten müsste die Inflation einberechnet werden. Das Apple iPhone 13 Pro 1 TB bot Apple am 1. 5. 2022 zum Neupreis in Höhe von € 1829,00 an (siehe Fn. 9).

33 BGH, K&R 2022, 433, Rn. 10.

34 BVerfG, 26. 3. 1987 – 2 BvR 589/79, 2 BvR 750/81, 2 BvR 284/85, BVerfGE 74, 358, 370; BVerfG, 29. 5. 1990 – 2 BvR 254/88, 2 BvR 1343/88, NJW 1990, 2741 (= BVerfGE 82, 106), BVerfG, 16. 5. 2002 – 1 BvR 2257/01, NJW 2002, 3231; *Frenz*, Europarecht, 3. Aufl. 2021, Kap. K, Rn. 1639 ff.; *Sommer*, in: Krekeler/Löffelmann/Sommer, Anwaltskommentar StPO, 2. Aufl. 2009, Art. 6 EMRK Rn. 69 - 75.

35 Siehe oben Abschnitt I. Ziffer 2. Ob diese Schlussfolgerung für die Bestätigung der Verurteilung überhaupt notwendig gewesen wäre, bleibt zweifelhaft. Denn laut BGH-Beschluss (K&R 2022, 433 dort Rn. 8, 11, 35) beruhten die französischen Ermittlungen zunächst auch auf dem Verdacht „unzulässiger Lieferung, Transfer und Import eines Verschlüsselungsmittels“. Sofern dies in Frankreich unter Strafe steht und sich bei diesen Ermittlungen Hinweise auf Delikte der organisierten Kriminalität ergeben haben, hätten diese möglicherweise als sogenannte „Zufallsfunde“ weiterverfolgt werden können (wenngleich für eine abschließende Beurteilung weitere Informationen zum Sacherhalt notwendig wären).

36 BVerfG, 16. 5. 2002 – 1 BvR 2257/01, NJW 1990, 2741 (= BVerfGE 82, 106), siehe auch Art. 104 Abs. 3 GG, Art. 5 Abs. 1 lit. c EMRK.

IV. Fazit

Die BGH-Entscheidung hat das Dilemma offengelegt, legalen Verschlüsselungseinsatz abzugrenzen von der Nutzung der Verschlüsselung zu kriminellen Zwecken. Der BGH hat diese Trennung in seinem Beschl. v. 2. 3. 2022 – 5 StR 457/21 danach getroffen, dass die Täter eine bestimmte Art von Kryptophones („EncroChat“) eingesetzt haben, die im kriminellen Milieu verbreitet war. Die Autoren halten die Kriterien, die der BGH dazu angelegt hat, nicht für geeignet, legale und unverdächtige IT-Nutzung von kriminellem bzw. verdächtigem Vorgehen abzuschichten. Vielmehr wären griffigere Kriterien anhand der Unschuldsvermutung und des Rechtsstaatsprinzips herauszuarbeiten.

Florian Deusch
ist als Rechtsanwalt und Fachanwalt für Informationstechnologierecht in der Anwaltskanzlei Dr. Gretter tätig und Lehrbeauftragter an der Hochschule Ravensburg-Weingarten. Er ist zudem als Datenschutzbeauftragter tätig.

Tobias Eggendorfer
ist Professor für IT-Sicherheit an der Hochschule Ravensburg-Weingarten und freiberuflicher IT-Berater. Er ist zudem als Datenschutzbeauftragter tätig.

RA Clemens Kochinke, MCL, Attorney at Law*

Länderreport USA

Kurz und Knapp

Obwohl Abgeordnete herbe Schlagworte über Redefreiheit, Zensur und von Medien und Internetkonzernen ausgehenden Missbrauch in die von ihnen gescholtenen Kommunikationswege schleudern, bringt der Kongress keine landesweiten Rechtsanpassungen zustande. Derweil setzt seine Bibliothek in ihrer Eigenschaft als Urheberrechtsamt einen besonderen Rechtsweg zur Verfolgung von Urheberrechtsverstößen um und die Gerichte werten in weitreichenden Entscheidungen nach geltendem Recht Eingriffe in die Redefreiheit und andere Kommunikationsrechte.

I. Redefreiheit

1. Hochschulbeiratszensur

Der Supreme Court der Vereinigten Staaten prüfte im Fall Houston Community College System v. Wilson[1] am 24. 3. 2022 die Redefreiheit nach dem Ersten Verfassungszusatz zur Bundesverfassung der USA.[2] Ein gewählter Hochschulbeirat klagte gegen seine vom College-Senat ausgesprochene Maßregelung. Diese sollte seine extreme Kritik im Senat und in den Medien rügen. Damit habe der Staat unzulässig in die dem Kläger als Bürger garantierte Redefreiheit eingegriffen.

Der Oberste Bundesgerichtshof der USA in Washington hielt eingangs fest, dass sich gewählte Amtsträger viel gefallen lassen müssten. Dieser Grundsatz gilt seit eh und je zum Beispiel bei Beleidigungen im Wahlkampf und in Parlamenten. Sie müssen eine dicke Haut besitzen. Eine verbale Maßregelung sei bei einer verbalen Auseinandersetzung unter Gleichen ein geeignetes Mittel ohne weitere Folgen. Ihr Verbot würde die Redefreiheit der anderen gewählten Amtsträger einschränken. Solche Ergebnisse wollten die Verfassungsväter vermeiden. Sie hätten vielmehr intensive verbale Redegefechte begrüßt und bewusst geschützt. Ein Eingriff stehe vor hohen Hürden. Prozesse seien das falsche Mittel, wenn Diskussionen nicht zum vom Redner gewünschten Erfolg führten.

2. Kunstfleischzensur

Ein Hersteller veganer Nahrungsmittel verklagte erfolgreich den Staat Louisiana wegen seines verfassungswidrigen Eingriffs in die gewerbliche Redefreiheit. Der angefochtene Truth in Labeling of Food Products Act verbietet als Verbraucherschutzmaßnahme die Erwähnung von Fleisch, Reis und Zucker in Ersatzprodukten. Im Fall Turtle Island Foods SPC v. Strain erkannte das erstinstanzliche Bundesgericht, dass bei drohender Durchsetzung des Gesetzes wegen der fleischerwähnenden Produktauszeichnungen die Aktivlegitimation vorliege, der Staat keine verbrauchergefährdende Irreführung belegt habe und die Klägerin durch Marktumfragen die von Verbrauchern bestätigte Verständlichkeit als fleischfreie Ware belegt habe.[3] Der Staat dürfe gewerbliche Rede regulieren, doch habe er das schwerere Mittel anstelle des nach der Bundesverfassung erforderlichen milderen gewählt. Damit verstoße das Gesetz gegen das First Amendment.[4]

II. Urheberrecht

1. Billiger Prozess

Gegen Urheberrechtsverletzungen können Rechtsinhaber nur dann gerichtlich vorgehen, wenn ihr Recht beim Copyright Office in Washington, DC, angemeldet und eingetragen ist, hatte der neben ihm angesiedelte Supreme Court in Fourth Estate Pub. Benefit Corp. v. Wall-Street.com ent-

* Mehr über den Autor erfahren Sie am Ende des Beitrags. Alle zitierten Internetquellen wurden zuletzt abgerufen am 27. 4. 2022.

1 United States Supreme Court, Washington, DC, 23. 3. 2022, https://www.supremecourt.gov/opinions/21pdf/20-804_j426.pdf.

2 First Amendment: Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances. https://constitution.congress.gov/constitution/amendment-1/.

3 Louisiana Rev. Stat. §§ 3:4741 - 4746.

4 United States District Court for the Middle District of Louisiana, Baton Rouge, 28. 3. 2022, https://www.leagle.com/decision/infdco20220404476.