Neues aus der Strafrechtswissenschaft:
Operation „Emma“ – Eine Europäische Erfolgsgeschichte?*

Von Dr. Marc-Oliver Sandner, Nürnberg**

Zum Geleit: Die (Straf-)Rechtswissenschaft ist ein stetig wachsendes Feld. Zum einen werden in einer immer komplexer werdenden Welt etwa durch gesetzgeberische und technische Entwicklungen stetig neue Forschungsgegenstände erschlossen, die auch strafrechtlicher Betrachtung bedürfen. Damit geht zum anderen aber auch einher, dass die Zahl der Personen, die sich diesen Fragestellungen widmen, beständig ansteigt.

Aus dieser Entwicklung ergibt sich ein Dilemma: Zwar entsteht einerseits eine Vielzahl wichtiger Untersuchungen – gedacht ist dabei insbesondere an Dissertationen und Habilitationsschriften –, die die strafrechtswissenschaftliche Forschung entscheidend voranbringen können. Andererseits werden viele solcher Arbeiten leider nicht im gebührenden Maße wahrgenommen, weil sie in der großen Menge der Publikationen untergehen und kaum noch jemand über die zeitlichen Ressourcen verfügt, Monographien aus bloßem Interesse heraus zu lesen.

Die Rubrik „Neues aus der Strafrechtswissenschaft“ will einen Beitrag dazu leisten, dieser Entwicklung gegenzusteuern. Sie bietet jungen Wissenschaftlerinnen und Wissenschaftlern aus der ganzen Welt die Möglichkeit, die zentralen Thesen ihrer Qualifikationsschrift in einem kompakten Aufsatz der internationalen Fachöffentlichkeit in deutscher, englischer oder spanischer Sprache vorzustellen. Auf diese Art und Weise haben interessierte Leserinnen und Leser die Möglichkeit, sich in zeiteffizienter Weise über den Inhalt und die Kernthesen des jeweiligen Buches zu informieren und auf dieser Grundlage entscheiden zu können, ob sie sich näher mit dem Werk beschäftigen mögen. So wird die Sichtbarkeit von herausragenden Arbeiten erhöht und der – insbesondere auch internationale – wissenschaftliche Austausch gefördert.

Herausgeber und Redaktion der ZfIStw

I. Vorspann

Dem „EncroChat-Komplex“ liegt folgender (verkürzter) Sachverhalt zugrunde:

Das Unternehmen EncroChat verkaufte sog. EncroChat-Smartphones oder auch Encrophones. Diese Geräte wurden mit dem Versprechen überwachungssicherer, vertraulicher Kommunikation bei gleichzeitiger Nutzeranonymität beworben. Die speziell in Hard- und Software modifizierten Geräte konnten über ein intervallisches, hochpreisiges Gebührenmodell[1] von sog. „Resellern“ erworben werden.

Nachdem französische Ermittlungsbehörden in den Jahren 2017 und 2018 im Rahmen mehrerer Ermittlungsverfahren Encrophones sichergestellt hatten, leiteten sie Vorermittlungen ein. Diese ergaben, dass keine legal existierende Gesellschaft namens „EncroChat“ existierte, es keine offiziellen Repräsentanten gab und angeblich auch kein Firmensitz bestand. Weiter konnte ermittelt werden, dass die Geräte mit einem herkömmlichen Android- und einem nur durch eine spezielle Tastenkombination aktivierbaren EncroChat-Betriebssystem versehen waren. Auf dem Android-Betriebssystem waren unter anderem folgende gängige Funktionen unterdrückt: Notruffunktion, Download von Fremdsoftware aus dem App-Store, „normale Telefonie“ und Nutzung der E-Mail-Anwendung. Angesichts dessen sowie des Preismodells, des Firmenversprechens der garantierten Anonymität und einiger Sicherheitsfeatures[2] der Geräte bestand der Verdacht, dass die Mobiltelefone im Bereich der organisierten Kriminalität genutzt würden.

Nach Erholung eines richterlichen Beschlusses erstellten die französischen Ermittler Kopien eines in Roubaix (Frankreich) bei dem Internetdienstleister OVH betriebenen Servers, der in Verbindung zu EncroChat stand. Anhand der Server-Kopien konnten die französischen Ermittler feststellen, dass ca. 39.000 Mobiltelefone den Messenger-Dienst von EncroChat nutzen würden. Entscheidend war zudem die teilweise Entschlüsselung von 3.477 chiffrierten, auf dem Server abgelegten Notizen. Diese hatten augenscheinlich Kokaingeschäfte im Kilogrammbereich mit überdurchschnittlich großem Aufwand unter Einsatz und Erzielung erheblicher finanzieller Mittel zum Gegenstand.

Diese Ermittlungsergebnisse und das Hindernis der weiterhin nicht dechiffrierbaren Chatnachrichten führten zur richterlich genehmigten Installation einer sog. Computerdaten-Abfangeinrichtung auf dem Server und den mit diesem verbundenen Endgeräten. Über ein stilles Update wurde verdeckt auf den EncroChat-Smartphones eine Trojaner-Schadsoftware installiert, die im Zeitraum vom 1.4.2020 bis zum 28.6.2020 heimlich Fotos, Chatnachrichten, Geräte-IMEI[3], Standorte der eingebuchten Funkmasten, E-Mail-Adressen und Benutzernamen, Adressbücher, Memos und Wifi-Login-Daten ausgelesen hat. Über 39.000 Mobiletelefone sollen hiervon betroffen gewesen sein (davon wohl 4.600 auf deutschem Hoheitsgebiet eingeloggte Geräte). Es sollen über

---

* Zusammenfassung der wesentlichen Thesen der Dissertation *Sandner*, Operation „Emma“ – Eine Europäische Erfolgsgeschichte? Eine Aufarbeitung der Infiltration des EncroChat-Netzwerks, Duncker Humblot, 2026.

** Der *Autor* ist Rechtsanwalt und Fachanwalt für Strafrecht in Nürnberg.

[1] Es kursieren unterschiedliche Angaben hierzu. Es sollen wohl 1.000 € Anschaffungspreis zzgl. einer monatlichen Nutzungsgebühr angefallen sein (bspw. ca. 1.500 € für eine sechs-monatige Nutzerlizenz).

[2] Etwa automatisiertes Löschen der Chatnachrichten, Entfernung von „überwachungsanfälligen“ Hardwarekomponenten wie USB-Port, GPS-Chip, Kamera und/oder Mikrofon, etc.

[3] International Mobile Equipment Identity: eine aus 15 Ziffern bestehende Nummer, die ein mit einem Mobilfunkchip versehenes technisches Gerät ihr weltweit eindeutig zuordnet; über die Tastenkombination „*#06#“ anzeigbar; siehe auch *Geschonneck*, Computer-Forensik, 6. Aufl. 2014, S. 293.

100 Millionen Chatnachrichten und Bilddateien ausgeleitet worden sein. Diese Daten werden umgangssprachlich auch als die „EncroChat-Protokolle“ bezeichnet. Die Funktionsweise des Trojaners sowie das Vorgehen bzgl. seiner Installation und der fortlaufenden Überwachung unterliegen dem französischen Militärgeheimnis.

Die ausgeleiteten Daten wurden über einen französischen Polizeiserver an EUROPOL und von dort an die Behörden der an der Operation teilnehmenden Partnerstaaten übermittelt. Die EncroChat-Daten durften in der Anfangsphase der Operation „Emma“[4] zunächst nur zu Auswertezwecken verwendet werden. Nach Übermittlung einer von der GenStA Frankfurt a.M. erlassenen Europäischen Ermittlungsanordnung (EEA) vom 2.6.2020 und deren Genehmigung durch ein französisches Gericht am 13.6.2020 wurde die uneingeschränkte Verwendung in Strafverfahren zugelassen. Auf diese Weise erlangten auch das BKA sowie die GenStA Frankfurt a.M. EncroChat-Daten, die zunächst in ein Unbekannt-Verfahren und nach Ermittlung individueller Nutzer in separate Ermittlungs- bzw. Strafverfahren flossen. Die EncroChat-Daten gelten als besonders wertvoll für Ermittler, da jedenfalls der kriminelle Nutzeranteil im Vertrauen auf die versprochene Vertraulichkeit erstaunlich offen[5] über teils schwere und schwerste Straftaten kommuniziert hat. Es konnten bislang noch nie dagewesene Einblicke in Rollenverteilungen, Organisationsstrukturen, modi operandi und Preisabsprachen krimineller Netzwerke erlangt werden.

II. Kernthesen der Dissertation

Die nachfolgenden Ausführungen sollen ausgewählte Punkte der Dissertation überblicksartig vorstellen. Eine ausführliche und tiefergehende Analyse erfolgte in der Dissertation.

1. Rechtstatsächlicher Sachverhalt

a) EncroChat-Smartphones

Wesentlicher Bestandteil der Dissertation ist eine Vorstellung des Unternehmens EncroChat sowie dessen Spezialgeräten, da die in den Medien und Gerichtsentscheidungen getroffenen Feststellungen hierzu teilweise unvollständig, unrichtig oder auch widersprüchlich waren. So kann beispielsweise festgehalten werden, dass entgegen der behördlich-justiziellen Darstellung durchaus zumindest zeitweise ein Geschäftssitz des Unternehmens mit einer Hauptfiliale in Amsterdam und zwei offiziellen „Reseller“-Stores in Leeuwarden und Rotterdam existiert haben sollen.[6] Offenzulegen ist dabei aber auch, dass es sich bei den letztgenannten Geschäften um eine Art Kiosk und einen Tabakwarenladen gehandelt haben soll.

Diesen Ausführungen folgt ein ausführlicher Vergleich zwischen herkömmlichen Smartphones und Encrophones. Hierbei wird festgestellt, dass herkömmliche Smartphones viele Sicherheitsfunktionen vorhalten, die so oder so ähnlich auch bei EncroChat-Geräten zu finden waren.[7] Gleichwohl können wesentliche Unterschiede benannt werden: Die Kommunikation über Encrophones war allein auf EncroChat-User beschränkt. Dagegen fungieren konventionelle Smartphones als Massenkommunikationsmittel, die auf die produktübergreifende Interaktion per Anruf oder SMS/MMS mit theoretisch unendlich vielen Personen ausgerichtet sind. Üblicherweise werden beim Kauf, spätestens bei der Inbetriebnahme herkömmlicher Smartphones personenbezogene Nutzerdaten erhoben, sodass keine absolute Anonymität des Nutzers besteht. EncroChat verwendete dagegen registrierungsfreie SIM-Karten und verlangte keine Nutzer-Registrierung. Die Verwaltungs-, Personal- und Vertriebsstruktur von EncroChat war – anders als bei gewöhnlichen Mobiltelefonherstellern – weitestgehend intransparent. Es existieren Berichte, wonach die Endgeräte nur an Interessenten verkauft wurden, nachdem diese auf ihre Vertrauenswürdigkeit überprüft worden waren. Ob dies ein generelles Vorgehen war, ist unklar. Die Produkte wurden jedenfalls auf verschiedenen frei zugänglichen Internetportalen (eBay, Facebook etc.) offen beworben, wohingegen die Übergabe konspirativ vollzogen wurde.

Insgesamt ist zu sehen, dass es sich bei den Encrophones um exklusive Hightech-Geräte handelte. Diese Endgeräte waren nicht für die breite Masse gedacht, sondern ganz bewusst auf eine konkrete Zielgruppe mit bestimmten Sicherheits- und Geheimhaltungsinteressen zugeschnitten. Diesen spezifischen Interessen trug EncroChat auf allen Ebenen von Verwaltung über Vertrieb und Produktkonzeption Rechnung und verschrieb sich voll und ganz der Anonymität. Gerichtlich bzw. medial erfolgte eine Einordnung von EncroChat-Smartphones als zur konventionellen Nutzung eingeschränkt oder gar nicht tauglichen Geräten, deren Nutzungsmöglichkeiten in keiner angemessenen Relation zum Kaufpreis stehen. Diese Sichtweise greift indes zu kurz, da sie sich am Maßstab gewöhnlicher Smartphones bzw. -nutzer orientiert. Dass EncroChat-Geräte auch für kriminelle Nutzer reizvoll waren, liegt auf der Hand. Die Inanspruchnahme von besonders sicherer, hochpreisiger Verschlüsselungstechnik stellt aber ein gem. Art. 10 Abs. 1, 2 Abs. 1 GG grundrechtlich geschütztes und gesetzlich erwünschtes[8] Verhalten dar und muss keines-

[4] Deckname der französischen Operation.

[5] So wurden etwa Fälle bekannt, in denen sich über Straftatvorbereitung bzw. -begehung unter Verwendung von Klarnamen oder Versendung von Dokumenten mit personenbezogenen Angaben ausgetauscht wurde, siehe bspw. KG Berlin, Beschl. v. 30.8.2021 – 2 Ws 79/21, 2 Ws 93/21 = openJur 2021, 26487 Rn. 9.

[6] Siehe https://encrophone.com/en/resellers/ (2.1.2026), nach vorübergehender Unerreichbarkeit im Zuge der EncroChat-Ermittlungen derzeit wieder erreichbar.

[7] Ende-zu-Ende-Verschlüsselung ist heutzutage Branchenstandard. Selbstlöschende Nachrichten werden bei Messenger-Diensten wie WhatsApp, Snapchat, Telegram etc. ermöglicht. „Gesperrte“ Chats können bei WhatsApp, Threma und Facebook-Messenger verwendet werden. Bei iOS-Betriebssystemen kann die Löschung des verschlüsselten Entschlüsselungskeys für den persistenten Speicher als Folge mehrfacher falscher PIN-Eingabe eingestellt werden.

[8] Schaffung vertraulicher Meldekanäle anlässlich der „Whistleblowing“-Richtlinie; Digitale Agenda der Bundesregierung für 2014–2017; Verschlüsselungsanforderungen der DSGVO;

wegs zwingend mit einem kriminellen Background verknüpft sein. Diversen Personengruppen und Branchen kann ein berechtigtes, „legales" Interesse an vertraulicher Kommunikation attestiert werden.[9] Ein Großteil dieser Personengruppen ist zudem willens und fähig, hohe Summen zur Anschaffung und Nutzung entsprechender Dienste zu bezahlen.

b) Eigentlicher Sachverhalt

In der Dissertation wird in einem zweiten Schritt der Gang der Ermittlungen chronologisch dargestellt. Ein Haupterkenntnisgewinn liegt darin, dass aufgezeigt wird, dass deutsche Ermittlungsbehörden die EncroChat-Daten – anders als stets behauptet – nicht ohne vorherige Absprache von den französischen Ermittlern bzw. EUROPOL erhalten haben. Der Erhalt der EncroChat-Daten war alles andere als überraschend: Bereits im Jahr 2018 gab es zumindest grobe Anhaltspunkte für ein französisches Vorgehen gegen EncroChat. Weiter kann nachvollziehbar gemacht werden, dass deutsche Vertreter an einer Eurojust-Videokonferenz am 9.3.2020 teilnahmen, in der durch französisch-niederländische Ermittler über den bevorstehenden Hack eines Kryptodienstes samt anschließender Datenverteilung informiert wurde. Die deutschen Vertreter hatten hierbei Interesse am Erhalt der angekündigten Daten bekundet. Ein damals anwesender BKA-Beamter soll als Zeuge in einem EncroChat-Verfahren bestätigt haben, dass hierbei – anders als zwischenzeitlich behauptet – ausdrücklich EncroChat genannt worden sein soll.

Von herausragender Bedeutung ist jedoch, dass das BKA am 27.3.2020 – also noch *vor* Beginn der Datenausleitungen ab 1.4.2020 – eine SIENA-Nachricht[10] erhalten hat. Darin wurden alle am Erhalt der EncroChat-Daten interessierten Sicherheitsbehörden adressiert und um eine schriftliche Bestätigung vor Beginn der Datenerhebungen aufgefordert. Die Bestätigung erfasste der Nachricht zufolge, dass man über die angewendeten Maßnahmen zur Datengewinnung von Geräten auf dem jeweiligen Hoheitsgebiet informiert wurde und etwa weiter, dass man die Daten unter Einwilligung in näher genannte Bedingungen erhalten möchte. Nach Rücksprache mit der GenStA Frankfurt a.M. erteilte das BKA die Bestätigung, ohne dass ein deutsches Gericht mit dem Sachverhalt betraut wurde.

Diese Geschehnisse konnten erst durch Verteidigertätigkeiten rekonstruiert werden. In den entsprechenden Verfahrensakten fanden sich zunächst weder Unterlagen, Vermerke noch sonst irgendwelche Hinweise darauf. Insbesondere die frühen ersten Gerichtsentscheidungen, aber auch Folgeentscheidungen, ergingen weitestgehend auf einer unvollständigen Tatsachengrundlage, da ihnen diese Umstände nicht bekannt gewesen sein dürften.

2. Verwendung

In rechtlicher Hinsicht ist sich zunächst zu vergegenwärtigen, dass sich die Verwendung und die Verwertung von Daten voneinander unterscheiden. Verwendung ist als Oberbegriff und die Verwertung als Unterfall zu sehen.[11] Da die Verwertung von Daten spezieller ist als die Verwendung, ist Letztere vorgelagert zu prüfen.[12]

a) Grundsätze

Im Kontext der Verwendung von Daten spielen die Grundsätze der Zweckbindung und -änderung eine zentrale Rolle. Nicht nur die Erhebung von Daten stellt einen Grundrechtseingriff dar. Auch jede weitere Datenverwendung lässt den ursprünglichen Grundrechtseingriff wieder aufleben.[13] Die Erhebung und weitere Verwendung von Daten ist dabei an einen konkreten Zweck gebunden.[14] Der Erhebungszweck limitiert die weitere Datenverwendung. Ist die Nutzung erhobener Daten zu anderen Zwecken als dem Erhebungszweck beabsichtigt, muss der damit verbundene selbstständige Grundrechtseingriff auf eine entsprechende Rechtsgrundlage gestützt werden können, die das Eingriffsgewicht der Datenerhebung auch im Rahmen der neuen Nutzung berücksichtigt.[15] Verfassungsrechtliches Erfordernis ist dabei eine Vorschrift mit hinreichend normenklarem und spezifischem Regelungsgehalt für die Verwendung von Daten.[16]

Der Gebrauch der EncroChat-Daten durch die deutschen Ermittlungsbehörden und das Heranziehen als Beweismittel in deutschen Strafverfahren stellen eine zweckändernde Verwendung dar. Die Zweckänderung liegt darin, dass die Daten nicht mehr im Kontext ihres ursprünglichen Zwecks eingesetzt werden (Erhebung für ein bestimmtes französisches

uneingeschränkte Unterstützung der Entwicklung, Umsetzung und Nutzung starker Verschlüsselung durch EU, Entschließung des Rates der Europäischen Union zur Verschlüsselung v. 24.11.2020 – 13084/1/20, S. 2; eIDAS-II-Verordnung.

[9] Ärzte, Anwälte, Journalisten, Aktivisten, politisch Verfolgte, Informanten, Aussteiger, Pharma-, Finanz- und Wirtschaftsbranche zum Schutz vor Spionage bzw. von Geschäftsgeheimnissen etc.

[10] SIENA: Secure Information Exchange Network Application, Kommunikationsplattform zum sicheren Nachrichtenaustausch innerhalb EUROPOL; veröffentlicht bspw. durch RA *Lödden* auf dessen LinkedIn-Profil: https://www.linkedin.com/pulse/encrochat-bgh-alles-klar-denkste-christian-l%C3%B6dden/ (2.1.2026).

[11] *Derin/Singelnstein*, StV 2022, 130 (130 f.).

[12] *Derin/Singelnstein*, StV 2022, 130 (130 f.).

[13] BVerfG, Beschl. v. 4.4.2006 – 1 BvR 518/02 = NJW 2006, 1939 (1946); *Derin/Singelnstein*, StV 2022, 130 (131); *dies*., NStZ 2021, 449 (450); *Ruppert*, NZWiSt 2022, 221 (223 f.).

[14] BVerfG, Urt. v. 14.7.1999 – 1 BvR 2226/94, 2420/95, 2437/95 = NJW 2000, 55 (57); BVerfG, Beschl. v. 13.6.2007 – 1 BvR 1550/03 u.a. = NJW 2007, 2464 (2466 f.); BVerfG, Urt. v. 11.3.2008 – 1 BvR 2074/05, 1 BvR 1254/07 = NJW 2008, 1505 (1509).

[15] *Zeyher*, ZWH 2022, 81 (84); *Derin/Singelnstein*, StV 2022, 130 (131); *dies*., NStZ 2021, 449 (450); BVerfG, Urt. v. 20.4. 2016 – 1 BvR 966/09, 1 BvR 1140/09 = NJW 2016, 1781 (1801); BVerfG, Beschl. v. 3.3.2004 – 1 BvF 3/92 = BVerfGE 110, 33 (69).

[16] BVerfG, Urt. v. 11.3.2008 – 1 BvR 2074/05, 1 BvR 1254/07 = NJW 2008, 1505 (1509); BVerfG, Urt. v. 14.7.1999 – 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95 = NJW 2000, 55 (57).

Verfahren), sondern nunmehr nach einem Datentransfer zum Gegenstand deutscher Ermittlungs- und Strafverfahren gemacht werden. Diese Zweckänderung bedarf einer tauglichen Rechtsgrundlage, um den in der Erhebung der Daten liegenden und durch die Verwendung neu auflebenden Grundrechtseingriff zu rechtfertigen. Die Rechtsgrundlage muss sich dabei an der Eingriffsintensität der Erhebungsmaßnahme orientieren, weshalb eine Einordnung der französischen Datenerhebungsmaßnahme vorgenommen wurde.

Nimmt man hierbei angesichts des einheitlichen Überwachungswillen das Eingriffsgewicht der Gesamtmaßnahme in den Blick und lehnt richtigerweise eine isolierte Betrachtung der individuellen Erfassung eines EncroChat-Nutzers ab, so zeigt sich eine massive Eingriffsintensität der Überwachungsmaßnahmen: Über 39.000 EncroChat-Nutzer in ca. 121 Ländern wurden heimlich fast drei Monate lang grundsätzlich fortlaufend[17] überwacht. Hierbei wurde sensibles Datenmaterial – bestehend unter anderem aus Standort- und Kommunikationsdaten sowie tagebuchartigen Notizen – ausgeleitet, das sich zur Erstellung von Bewegungs-, Verhaltens- und Persönlichkeitsprofilen eignet. Nachdem der Trojaner den EncroChat-Nutzern wohl auch vorspiegeln konnte, dass die „Wipe“-Funktion[18] erfolgreich war, obwohl dies tatsächlich nicht der Fall war, wurde auch mit täuschenden Elementen gearbeitet.

b) Denkbare Rechtsgrundlagen

Die StPO sieht ein dreistufiges System der Zweckänderung vor. Natur und Gewicht der Ausgangsmaßnahme werden darin berücksichtigt. Die Normen werden umso spezifischer und qualifizierter, je eingriffsintensiver die Ausgangsmaßnahme ist. Angesichts des vorstehend benannten erheblichen Eingriffsgewichts kommen für die Verwendung der EncroChat-Daten von vornherein allenfalls Verwendungsnormen der zweiten und dritten Stufe in Frage. Auf zweiter Stufe stehend wären dies insbesondere – die Anwendbarkeit auf den grenzüberschreitenden Kontext vorausgesetzt[19] – § 479 Abs. 2 S. 1 StPO bzw., auf dritter Stufe stehend, § 100e Abs. 6 Nr. 1 StPO, sofern man davon ausgehen wollte, dass die französischen Erhebungsmaßnahmen dem Bild einer § 100a StPO- respektive § 100b StPO-Maßnahme entsprechen.[20]

Das französische Ermittlungshandeln müsste sich hypothetisch als eine § 100a StPO bzw. § 100b StPO entsprechende Maßnahme darstellen. Untersucht man den Sachverhalt, so ist allerdings festzustellen, dass die französischen Überwachungsmaßnahmen schleppnetzartig auf eine möglichst weitreichende Überwachung möglichst vieler (unbekannter) Nutzer unter Ausleitung einer großen Datenvielfalt angelegt waren. Zum Anordnungszeitpunkt war weder klar, wer bzw. wie viele Nutzer/Geräte von der Überwachung konkret betroffen sein würden. Noch lagen konkrete Verdachtsmomente gegen bestimmte Personen wegen spezifischer strafbarer Sachverhalte vor. Es fehlt daher an den Charakteristika einer §§ 100a, 100b StPO hypothetisch entsprechenden Maßnahme, namentlich einem von individuellen Tatverdachtsmomenten getragenen, verhältnismäßigen, zielgerichteten und umgrenzten Einsatz der Überwachungssoftware gegen bestimmte Betroffene. Schutzvorkehrungen gegen das Miterfassen Dritter – wie sie prägend für §§ 100a, 100b StPO Maßnahmen sind – konnten so nicht getroffen werden. Die französischen Ermittlungsmaßnahmen würden das nach §§ 100a, 100b StPO zulässige Maß an Eingriffsintensität und -tiefe erheblich übersteigen. Die Maßnahmen entsprechen also im übertragenen Sinne nicht dem Bild einer Maßnahme nach § 100a bzw. § 100b StPO. Die französischen Überwachungsmaßnahmen finden in dieser Form keine Entsprechung in der StPO und sind daher als Maßnahme sui generis zu qualifizieren.[21] Für derartige Maßnahmen findet sich keine Verwendungsnorm in der StPO, sodass eine rechtsgrundlose Datenverwendung gegeben ist.

c) Rechtsprechung des BGH

Für die Verwendung der EncroChat-Daten als in der Hauptverhandlung erhobene Beweise zieht der BGH § 261 StPO und für die Verwendung im Ermittlungsverfahren § 161 StPO als Rechtsgrundlagen heran.[22] Zur Wahrung des Verhältnismäßigkeitsgrundsatzes wird zudem auf „die Grundgedanken der Verwendungsschranke mit dem höchsten Schutzniveau (§ 100e Abs. 6 StPO)“[23] verwiesen.

---

[17] Voraussetzung war anscheinend lediglich, dass ein EncroChat-Gerät eingeschaltet war.

[18] Löschung aller Gerätedaten nach Eingabe einer bestimmten PIN.

[19] Nach hier vertretener Ansicht sind §§ 479 Abs. 2 S. 1, 100e Abs. 6 Nr. 1 StPO weder direkt noch analog anwendbar. Bereits nach dem Wortlaut der Normen sind Maßnahmen der StPO vorausgesetzt. Gegen eine analoge Anwendung von § 100e Abs. 6 Nr. 1 StPO spricht außerdem der Zuschnitt auf den Datentransfer zwischen innerstaatlichen Strafverfahren sowie das Erfordernis einer spezifischen und normenklaren Rechtsgrundlage für die Verwendung von Daten aus eingriffsintensiven Maßnahmen. Letzteres darf nicht durch eine entsprechende Anwendung ausgehebelt werden.

[20] In der Dissertation werden mit §§ 100e Abs. 6 Nr. 3, 161 Abs. 3, 244 Abs. 2 StPO, §§ 91j Abs. 3 Nr. 2, 92b IRG weitere Verwendungsnormen diskutiert und als untauglich verworfen. Der Übersichtlichkeit halber wird sich auf die die rechtliche Diskussion prägendsten Verwendungsnormen konzentriert.

[21] *Derin/Singelnstein*, NStZ 2021, 449 (452, 454); *dies.*, StV 2022, 130 (132, 134), *Schmidt*, ZStW 134 (2022), 982 (994); *Zühlke*, StV-Spezial 2022, 165 (166); vgl. *Strate*, HRRS 2022, 15 (16); ähnl. wohl *Wahl*, ZIS 2021, 452 (453); *Ruppert*, NZWiSt 2022, 221 (226); offengelassen *Brodowski*, StV 2022, 364 (364 f.); vgl. *Petersen*, StV 2022, 679 (680); vgl. *Lenk*, EuR 2024, 51 (73).

[22] BGH, Beschl. v. 2.3.2022 – 5 StR 457/21 = BeckRS 2022, 5306 Rn. 61, 64; BGH, Beschl. v. 5.7.2022 – 4 StR 61/22 = BeckRS 2022, 22161 Rn. 8; BGH, Beschl. v. 6.7.2022 – 4 StR 63/22 = BeckRS 2022, 18570; BGH, Beschl. v. 16.2. 2023 – 4 StR 93/22 = openJur 2023, 4234 Rn. 17; BGH, Urt. v. 7.12.2023 – 5 StR 168/23 = BeckRS 2023, 42174 Rn. 8.

[23] BGH, Beschl. v. 2.3. 2022 – 5 StR 457/21 = BeckRS 2022, 5306 Rn. 68.

Nach hiesiger Ansicht handelt es sich jedoch bei §§ 261, 161 StPO um keine tauglichen Rechtsgrundlagen für die Verwendung der EncroChat-Daten. Als Generalklausel kann § 261 StPO gerade nicht der Gefahr einer uferlosen Weiterverwendung erhobener Daten begegnen. Die Norm berücksichtigt nicht das Eingriffsgewicht der Erhebungsmaßnahme und stellt keine spezifischen Anforderungen an die Verwendung daraus resultierender Daten. Das verfassungsrechtliche Erfordernis einer gesetzlichen, normenklaren und spezifischen Rechtsgrundlage kann auch nicht dadurch umgangen werden, dass gesetzliche Verwendungsbeschränkungen dem Grundgedanken nach angewendet werden.[24] Der Verhältnismäßigkeitsgrundsatz kann das Erfordernis einer entsprechenden Rechtsgrundlage nicht ersetzen, sondern nur gesetzliche Eingriffsbefugnisse beschränken.[25] Diese Argumente kommen hinsichtlich § 161 Abs. 1 StPO erneut zum Tragen, da auf die Ermittlungsgeneralklausel keine erheblichen Grundrechtseingriffe gestützt werden können. Im Übrigen wurde dargelegt, dass die französischen Ermittlungshandlungen nicht mit den Charakteristika einer Maßnahme gem. § 100a StPO oder § 100b StPO vereinbar sind und deren Eingriffsintensität deutlich übersteigen, sodass sie keine Entsprechung im übertragenen Sinne in §§ 100e Abs. 6 Nr. 1, 100b StPO finden können. Die Anwendung der Grundgedanken dieser Normen ist daher abzulehnen.

d) Zwischenfazit

Nach hiesiger Auffassung findet sich keine taugliche Rechtsgrundlage für die Verwendung der EncroChat-Daten in deutschen Verfahren. Der Gesetzgeber hat über Verwendungsregelungen klar und präzise festgelegt, wann eine Weiterverwendung erhobener Daten zulässig ist – und wann nicht. Hierin ist zugleich der Wille zu erkennen, einer rechtsgrundlosen Verwendung von erhobenen Daten den Boden zu entziehen. Die EncroChat-Daten unterliegen daher einem totalen Nutzungsverbot.

3. Verwertung

Die Dissertation befasst sich mit verschiedenen möglichen Verwertungsverboten, wobei im Folgenden zwei Verwertungsverbote näher thematisiert werden sollen.

a) Verstöße gegen allgemein rechtsstaatliche Grundsätze

Zunächst ist zu konstatieren, dass nach Rechtsprechung des BGH[26] keine Rechtmäßigkeitskontrolle des Handelns französischer Ermittlungsbehörden am Maßstab des französischen oder deutschen Rechts durch deutsche Gerichte erfolgen darf. Vielmehr wird allein eine eingeschränkte Kontrolle ausländischer Entscheidungen und Urteile dahingehend für zulässig erachtet, ob allgemein rechtsstaatliche Grundsätze (ordre-public-Grundsatz) oder völkerrechtlich verbindliche, individualschützende Normen verletzt seien.[27]

Nach hiesiger Ansicht ist ein dreifacher Verstoß gegen Kernprinzipien des Rechtsstaatsprinzips zu bejahen. Zum einen wurden über 39.000 EncroChat-Nutzer heimlich mehrere Monate überwacht. Im Anordnungszeitpunkt fehlte es an konkreten Verdachtsmomenten in Bezug auf bestimmte strafbare Lebenssachverhalte konkreter Nutzer. Es wurden gewaltige Datenbestände einer erheblichen Datenvielfalt aufgezeichnet. Auf „gut Glück" wurden alle Geräte, die mit dem Server verbunden waren, überwacht. Wie viele Geräte dies betreffen würde, war im Vorfeld nicht annähernd eingegrenzt, sondern war letztlich dem Zufall überlassen. Derart streubreite, unterschiedslose Überwachungsmaßnahmen – mithin überschießende Datenzugriffe – sind mit dem Verhältnismäßigkeitsgrundsatz nicht in Einklang zu bringen.

Zum anderen sind allgemein rechtsstaatliche Grundsätze auch hinsichtlich des Missbrauchs- und Willkürverbots verletzt: Strafprozessuale Zwangsmaßnahmen dürfen nicht für die gezielte Suche nach Zufallsfunden zweckentfremdet werden, da andernfalls das staatliche Gewaltmonopol missbraucht würde. Letztlich ist aber im EncroChat-Komplex genau dies eingetreten. Ganz gleich, ob die französischen Ermittlungen vorrangig den Betreibern EncroChats gegolten haben – was abwegig erscheint – oder letztlich die Nutzer verfolgt werden sollen, in beiden Fällen war die Operation „Emma" auf die systematische Gewinnung möglichst vieler Daten ausgerichtet, um aus dem gesammelten Datenmaterial nachgelagert individuelle Verdachtsmomente generieren zu können. Fernab der vagen Vermutung einer kriminellen Zwecksetzung des EncroChat-Netzwerks fehlte es an einem konkreten Tatverdacht gegen bestimmte User wegen bestimmter Sachverhalte oder Straftaten. Es war noch nicht einmal klar, gegen wie viele Encrophones sich die Maßnahmen richten würden. Mit den grundlegenden Aspekten allgemein rechtsstaatlicher Grundsätze ist nicht vereinbar, derart eingriffsintensivste Ermittlungsmaßnahmen nach „Gutdünken" zu führen.

Schließlich folgt aus diesen Erwägungen zugleich ein weiterer Verstoß gegen allgemein rechtsstaatliche Grundsätze, da strafprozessuale Zwangsmaßnahmen nach deutschem Verständnis an das Vorliegen einer tatsachenbasierten Verdachtslage gekoppelt sind. Dies erfordert konsequenterweise gewisse Vorkenntnisse zu einem potentiell strafbaren Sachverhalt bzw. einer verdächtigen Person.

Aus diesen Verstößen folgt ein Beweisverwertungsverbot. Zwar sind in den EncroChat-Daten teils schwere und schwerste Straftaten dokumentiert, sodass das Verwertungsinteresse entsprechend gewichtig ist. Allerdings widerspricht es den zentralen Wertvorstellungen der deutschen Rechtsordnung, wenn Beweismittel durch Erhebungsmaßnahmen gewonnen werden, die losgelöst von individuellen Verdachtsmomenten oder Verhältnismäßigkeitserwägungen angeordnet werden. Für die Anerkennung von Beweismitteln, die mit Erhebungsmaßnahmen gewonnen werden, die in Konzeption

[24] *Ruppert*, NZWiSt 2022, 221 (225).
[25] *Cornelius*, NJW 2022, 1546 (1547).
[26] BGH, Beschl. v. 21.11.2012 – 1 StR 310/12 = BeckRS 2013, 4113 Rn. 34.
[27] BGH, Beschl. v. 21.11.2012 – 1 StR 310/12 = BeckRS 2013, 4113 Rn. 38 f.

und Eingriffsintensität noch über die eingriffsintensivsten Maßnahmen der StPO hinausgehen, besteht kein Raum.

b) Verletzung des Unterrichtungsverfahrens gem. Art. 31 Abs. 1 RL-EEA

Nach derzeitigem Kenntnisstand ist zudem davon auszugehen, dass die gem. Art. 31 Abs. 1 RL-EEA[28] erforderliche Unterrichtung von der Überwachung von Zielpersonen auf deutschem Hoheitsgebiet durch die Behörden Frankreichs nicht erfolgt ist. Gem. § 92d Abs. 1 Nr. 1 IRG ist das Amtsgericht Stuttgart örtlich zuständige deutsche Stelle für französische Überwachungsmaßnahmen. Die eigentlich vorgesehene Unterrichtung löst die fristgebundene Widerspruchsmöglichkeit gem. Art. 31 Abs. 3 RL-EEA – in § 91g Abs. 6 IRG richtlinienüberschießend zur Widerspruchspflicht ausgestaltet – aus, wenn die Überwachung in einem vergleichbaren innerstaatlichen Fall nicht genehmigt würde. Es wurde bereits skizziert, dass derartige Überwachungsmaßnahmen bereits ihrer Konzeption nach nicht mit der deutschen Rechtsordnung vereinbar sind. Die Maßnahmen wären in einem hypothetisch innerstaatlichen Fall keinesfalls genehmigt worden, da es im Anordnungszeitpunkt an konkreten, tatsachenbasierten Verdachtsmomenten bzgl. bestimmter Beschuldigter wegen spezifischer strafrechtlich relevanter Lebenssachverhalte fehlte und eine derartig streubreite Überwachung zahlloser Unbekannter nicht verhältnismäßig ist.

In der Rechtsprechung wird bisweilen vertreten, dass in dem Erlass einer EEA durch die GenStA Frankfurt a.M., die auf die Verwendung der übermittelten EncroChat-Daten in deutschen Strafverfahren gerichtet war, und der tatsächlichen Verwendung der Daten eine Heilung des Unterrichtungsverstoßes zu sehen ist. Diese Ansicht ist indes abzulehnen, da sie das Unterrichtungsverfahren und die (deutsche) Widerspruchspflicht ad absurdum führen würde. Sinn und Zweck ist gerade, dass die unterrichteten Behörden durch die Notifikation die hypothetisch innerstaatliche Genehmigungsfähigkeit der Überwachung prüfen und rechtzeitig widersprechen können, bevor es überhaupt zu einer rechtswidrigen Überwachung kommt. Des Weiteren steht deutschen Behörden jedenfalls dann, wenn – wie hier bejaht – eine Widerspruchspflicht gem. § 91g Abs. 6 IRG bestünde, gar keine Dispositionsbefugnis hinsichtlich der Geltendmachung des Unterrichtungsverstoßes zu.[29]

Der Verstoß gegen die rechtshilferechtlichen Normen des Unterrichtungsverfahrens kann aber nur dann ein Verwertungsverbot nach sich ziehen, wenn die verletzte Vorschrift zumindest reflexartig individualschützenden Charakter aufweist.[30] Wurde ein solcher individualschützender Charakter der Norm seitens des BGH[31] noch kritisch gesehen, ist dies – im Einklang mit dem EuGH[32] – mit Blick auf Sinn und Zweck zu bejahen. Das Unterrichtungs- und Widerspruchsverfahren schützt einerseits die staatliche Souveränität. Andererseits dient das Verfahren angesichts seiner grundrechtssichernden Funktion klar dem Individualschutz.[33] Die richtlinienüberschießende Normierung einer Widerspruchspflicht in § 91g Abs. 6 IRG ergibt nur dann Sinn, wenn neben dem Souveränitätsinteresse zumindest auch gleichrangig Grundrechtsschutz deutscher Staatsbürger verfolgt werden soll.[34]

Tritt man sodann in die gebotene Abwägung ein, ist – neben den bereits ausgeführten Argumenten (s.o.) – anzuführen, dass es sich beim Notifikationsverfahren um keine bloße Lappalie, sondern einen wesentlichen Verfahrensschritt handelt. Die beteiligten Akteure haben enorme Anstrengungen zur Aufrechterhaltung der Geheimhaltung der Operation betrieben. Es liegt der Verdacht nahe, dass die ohne Weiteres mögliche Unterrichtung bewusst unterblieben ist, um die geheime Operation nicht zu kompromittieren. Insgesamt wird daher auch hier vertreten, dass aus dem Verfahrensverstoß ein Verwertungsverbot erwächst.

III. Fazit

Die Arbeit zeigt auf, dass es sich bei den EncroChat-Geräten um Hightech-Geräte handelte, die nicht am Maßstab gewöhnlicher Smartphones gemessen werden können. Werden die Geräte als zur konventionellen Nutzung nicht (gänzlich) tauglich eingeordnet und wird auf eine fehlende Relation von Kaufpreis zu Nutzungsmöglichkeiten abgestellt, greift dies zu kurz. Die Inanspruchnahme von derartiger Verschlüsselungstechnik ist grundrechtlich geschützt. Diverse Personengruppen haben ein berechtigtes Interesse an ihrer Nutzung und verfügen über die notwendigen finanziellen Mittel, ohne dass sie pauschal mit dem Vorwurf krimineller Gebrauchsabsichten überzogen werden können.

Die Arbeit konnte ferner den rechtstatsächlichen Sachverhalt näher beleuchten. Hier ist insbesondere von Bedeutung, dass ein Großteil der EncroChat-Entscheidungen auf einem unvollständigen Sachverhalt beruht.

[28] Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates v. 3.4.2014 über die Europäische Ermittlungsanordnung in Strafsachen.

[29] Ähnl. *Rückert*, in: Kudlich (Hrsg.), Münchener Kommentar zur Strafprozessordnung, StPO, Bd. 1, 2. Aufl. 2023, § 100a Rn. 51e; *Schmidt*, ZStW 134 (2022), 982 (1001).

[30] BGH, Beschl. v. 21.11.2012 – 1 StR 310/12 = BeckRS 2013, 4113 Rn. 25.

[31] BGH, Beschl. v. 2.3.2022 – 5 StR 457/21 = BeckRS 2022, 5306 Rn. 40 f.; BGH, Beschl. v. 5.7.2022 – 4 StR 61/22 = BeckRS 2022, 22161 Rn. 15; BGH, Urt. v. 7.12.2023 – 5 StR 168/23 = BeckRS 2023, 42174 Rn. 8.

[32] EuGH, Urt. v. 30.4.2024 – C-670/22 = NJW 2024, 1723 (1731 Rn. 124 f.).

[33] *Roth*, GSZ 2021, 238 (244); *Rückert*, NStZ 2022, 446; *Petersen*, StV 2022, 679 (681 f.); *Meyer-Mews*, HRRS 2022, 289 (289, 295 f.); *Zimmermann*, ZfIStw 2/2022, 173 (178); *Rückert* (Fn. 29), § 100a Rn. 51b, 51h; *Schmidt*, ZStW 134 (2022), 982 (1000 f.).

[34] *Rückert*, NStZ 2022, 446; *Petersen*, StV 2022, 679 (681); so letztlich auch BT Drs. 18/9757, S. 75; LG Berlin, Beschl. v. 1.7.2021 – (525 KLs) 254 Js 592/20 (10/21) = openJur 2021, 21800 Rn. 92; *Weiss*, ZfIStw 6/2022, 427 (431); *Zimmermann*, ZfIStw 2/2022, 173 (178); *Rückert* (Fn. 29), § 100a Rn. 51h; *Lenk*, EuR 2024, 51 (70 Fn. 91).

In rechtlicher Hinsicht ist festzuhalten, dass keine taugliche Verwendungsnorm für die Verwendung der EncroChat-Daten in hiesigen Ermittlungs- und Strafverfahren existiert. Die Daten unterliegen daher einem totalen Nutzungsverbot. Des Weiteren werden Beweisverwertungsverbote wegen Verstößen gegen allgemein rechtsstaatliche Grundsätze sowie der Verletzung des Unterrichtungsverfahrens gem. Art. 31 Abs. 1 RL-EEA angenommen.