EncroChat – ein Kapitel in der Geschichte des zerbröselnden europäischen Strafprozesses

Rechtsanwalt Prof. Dr. Ulrich Sommer, Köln

Artikel 7 der Charta der Grundrechte der Europäischen Union (GrCh): »*Jede Person hat das Recht auf Achtung [...] ihrer Kommunikation.*«

EncroChat und die rechtliche Problematik des heimlichen staatlichen Datenzugriffs auf einen kompletten Kommunikationsserver im Ausland beginnt die deutschen Gerichtssäle zu überfluten. Zur Orientierung ein erster – von Wissenschaftlichkeit weit entfernter – Überblick aus Verteidigersicht:

A. Das Phänomen EncroChat

EncroChat war eines der größten weltweit agierenden Unternehmen, das eine weitgehend verschlüsselte Kommunikation anbot. Das Unternehmen hatte weltweit mehr als 60.000 Kunden. Es handelte sich um ein niederländisches Unternehmen, der von diesem Unternehmen betriebene Zentralserver befand sich in Roubaix/Frankreich.

EncroChat warb offiziell auf seiner Homepage mit einer Garantie der Anonymität. Ein Erwerb der Endgeräte war über die offizielle Webseite nicht möglich, auf der Verkaufsplattform eBay oder durch andere Wiederverkäufer wurden derartige verschlüsselte Geräte für ca. 1.000 € (und mehr) angeboten, wobei dieser Preis eine Nutzerlizenz für die Dauer von 6 Monaten beinhaltete.

Der über eine vorinstallierte App gesicherte verschlüsselte Kontakt konnte nur zwischen Kunden der Firma EncroChat erfolgen. Insoweit orientierte sich das Unternehmen an bereits bestehenden Konzepten anderer Anbieter für verschlüsselte Daten, wie beispielsweise des schweizerischen Unternehmens »Threema« (www.threema.ch »Sicherheit und Privatspäre«). Die weitergehenden Funktionen auf der speziellen Hardware ermöglichten es dem jeweiligen Benutzer auch, individuelle Einstellungen zum Löschen seiner Nachricht einzurichten. Durch Anwendung eines besonderen Passwortes konnte der gesamte Datenbestand des Gerätes unmittelbar gelöscht werden. Weitere Mechanismen wurden angeboten, um eine Manipulation der jeweiligen Geräte von außen auszuschließen.

Namen und Motivationen der Nutzer sind und waren unbekannt. Die besonderen Sicherungsmechanismen dürften trotz erhöhter Kosten Personen zu deren Nutzung veranlasst haben, denen es in besonderer Weise auf die Gewährleistung ihrer Privatsphäre ankam. Hierzu gehörten mutmaßlich zum einen Nutzer, die verbotene Liebesaffären nicht an die Öffentlichkeit dringen lassen wollten, zum anderen aber auch Personen, die einem Beruf nachgehen, der ihnen in ausdrücklicher gesetzlicher Vorgabe Geheimhaltungen auferlegt (zahlreiche Anwälte sollen über ein solches Gerät verfügt haben), letztlich auch politisch Oppositionelle im Exil, die den digitalen Nachstellungen der diktatorischen Heimat entgehen wollten, ebenso wie Whistleblower, die sich vor der wirtschaftlichen Stärke ihres bisherigen Arbeitgebers schützen wollten.

Dass diese Kommunikationsmöglichkeit auch von kriminellen Banden genutzt wurde, ist selbstverständliche kriminologisch belegbare Folge. Nicht festgestellt werden konnte bislang, dass ein Großteil oder sogar die Mehrheit der Nutzer die Kommunikationsmöglichkeit für Straftaten nutzte. Ebenso wenig konnte festgestellt werden, dass die Betreiber des Servers gerade derartige kriminelle Aktivitäten ermöglichen oder unterstützen wollten.

B. Dekryptieren durch die französische Justiz

Die französischen Strafverfolgungsbehörden haben nach monatelanger Ermittlung einen Zugriff auf die Kommunikationsdaten erreicht. Durch Infiltration des Servers und der mobilen Endgeräte gelang es ihnen, über 3 Monate (April bis Juni 2020) den kompletten Kommunikationsverkehr aller Nutzer zu erfassen und abzuspeichern.

Anlass für die umfassende »Datenerfassung« waren 7 (!) laufende Ermittlungsverfahren in Frankreich gegen gemutmaßte Drogenhändler, bei denen die Ermittlungsbehörden davon ausgingen, dass diese zur Durchführung ihrer – bereits aufgeklärten – Taten sich der EncroChat-Geräte bedienten. Die französischen Behörden ermittelten daraufhin allgemein wegen des Verdachts der Bildung einer kriminellen Vereinigung sowie wegen angeblicher Delikte im Zusammenhang mit dem Transfer und dem Import von Verschlüsselungsmitteln (Art 13 Décret n°2007–663 vom 02.05.2007), denen in Deutschland kein vergleichbarer Tatbestand entspricht.

Unter Berufung auf Art. 706-102-1 des Code de procédure pénal wurde durch Beschluss vom 20.03.2020 die »Genehmigung des Einsatzes einer Computerdaten-Abfangeinrichtung« vom *Untersuchungsrichter* in *Lille* erteilt. Die Maßnahme war gegen keinen konkreten oder konkretisierbaren Beschuldigten gerichtet, weder die Verdächtigen der 7 Ausgangsverfahren noch andere Personen – wie möglicherweise die Betreiber der Plattform – waren in den richterlichen Anordnungen benannt.

Das Ergebnis: Den französischen Ermittlungsbehörden gelang ein unmittelbarer und geheimer Zugriff auf sämtliche Daten. Entscheidend war offensichtlich die »Injektion« einer Schadsoftware auf jedes einzelne Mobiltelefon der Nutzer, wodurch noch vor der Chiffrierung der eingegebenen Nachricht die Daten an staatliche Behörden umgeleitet wurden; Details sind unbekannt, weil sie angeblich ein »militärisches Geheimnis« darstellen. Über 3 Monate wurde damit die Kommunikation von – wie die französische Polizei in ihrem Erfahrungsbericht anführt – mehr als 30.000 Nutzern mit mehr als 100 Millionen Datensätzen ungefiltert gesammelt, gelesen und ausgewertet. Der Zugriff endete erst, als die Betreiber die Infiltration bemerkten, die Nutzer informierten und den Server abschalteten.

C. Transfer der Daten an die deutsche Justiz

Ergebnisse dieses Zugriffs sind in Händen der deutschen Ermittlungsbehörden. Tausendfache Chats, die auf einen kriminellen Hintergrund schließen ließen und bei denen die ebenfalls sichergestellten Standortdaten auf einen Aufenthalt des Nutzers in Deutschland hinwiesen, wurden unter anderem unter Vermittlung von Europol dem BKA zur Verfügung gestellt. Andere

Selektionen gingen als gesonderte Pakete in andere Länder. Das BKA war früh – wahrscheinlich schon in der Planungsphase – in die Absicht der Infiltrierung des Servers eingebunden. Jedenfalls erhielt die Behörde parallel zur Erhebung der Daten aus Frankreich tägliche Datenlieferungen von Europol, die man dort zum Anlass für weitere individualisierende Ermittlungen nahm.

Selektion und Transfer der Daten sind intransparent. Die Hash-Algorithmen zum Verschlüsseln digitaler Signaturen, die die EU-Verordnung Nr. 910/2014 des Europäischen Parlamentes und des Rates vom 23.07.2014 als vertrauenswürdiges elektronisches Identifizierungsmittel voraussetzt, sind auf dem langen Weg von Roubaix auf den Schreibtisch eines deutschen Strafrichters jedenfalls nicht respektiert worden. Die Authentizität der Beweisergebnisse steht schon deswegen in Frage.

Begleitet wurden die polizeilichen Ermittlungen durch die Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) bei der Generalstaatsanwaltschaft Frankfurt am Main. Dort wurde noch vor der Infiltration des Servers ein Verfahren gegen Unbekannt eingeleitet, das in der Folgezeit als justizielles Vehikel zur Einschleusung der Beweisergebnisse in deutsche Strafverfahren diente. Auf Antrag aus diesem Verfahren erließ das *AG Frankfurt/M.* bereits im Mai 2020 erste Beschlüsse, wonach Überwachungsmaßnahmen gegen unbekannte Nutzer bestimmter Telefone, deren Identifikationsdaten zuvor die französischen Behörden übermittelt hatten, gemäß §§ 163f, 100g, 100i StPO angeordnet wurden.

Am 02.06.2020 verfasste die Generalstaatsanwaltschaft Frankfurt eine Europäische Ermittlungsanordnung (EEA) an die französische Justiz mit dem Ziel, die Übersendung derjenigen Erkenntnisse zu genehmigen, die das BKA längst hatte und nutzte. Mit dem 06.07.2020 genehmigte der *Untersuchungsrichter* in *Lille* die Übersendung der durch die Infiltrierung gewonnenen Ergebnisse an die Generalstaatsanwaltschaft Frankfurt.

Wenn das BKA meinte, ausreichende Identifizierungen vorgenommen zu haben, legte die Generalstaatsanwaltschaft Frankfurt aus ihrem Verfahren gegen Unbekannt der jeweils örtlich zuständigen Staatsanwaltschaft die selektierten Ermittlungsergebnisse mit der Bitte vor, gegen den jeweils konkretisierten Verdächtigen ein Ermittlungsverfahren einzuleiten. Bundesweit sind mittlerweile Hunderte von Ermittlungsverfahren eingeleitet und zahllose Haftbefehle ausgebracht worden, die sich in ihrer Beweiswürdigung ausschließlich auf die Kommunikation von EncroChat beziehen.

D. Akzeptanz der Ergebnisse durch die deutsche Justiz

Die Deutlichkeit mancher Chats, in denen angesichts gefühlter Sicherheit der Kommunizierenden insbesondere Drogendeals unschwer rekonstruierbar erscheinen, fasziniert Ermittler. Strafrichter sind erleichtert, wenn sie bei der Interpretation digitaler Kommunikation nicht mehr – wie bislang regelmäßig – die Grenze des Erträglichen der freien richterlichen Beweiswürdigung auszuloten haben, sondern sich auf Klartext berufen können.

Es gibt offensichtlich aktuell keine einzige gerichtliche Entscheidung, die die Verwertbarkeit dieser Beweisergebnisse in einem deutschen Strafverfahren bezweifeln würde. Einwände der Verteidigung in laufenden Hauptverhandlungen werden zurückgewiesen. Mehrere Oberlandesgerichte haben sich in bestätigenden Haftentscheidungen allein oder maßgeblich auf EncroChat gestützt. Eine erste Beschwerde hat das *BVerfG* ohne weitere Begründung nicht zur Entscheidung angenommen.

Der Argumentationsduktus wiederholt sich mittlerweile: Es gäbe keine Anhaltspunkte für die Verletzung französischer Rechtsnormen, die Beweisergebnisse seien durch richterlichen Beschluss daher ordnungsgemäß gewonnen. Der Vertrauensgrundsatz innerhalb der EU gebiete Respekt vor dieser Entscheidung, die von einem deutschen Richter grundsätzlich nicht zu hinterfragen sei. Aus dieser Distanz gebe es jedenfalls keine Veranlassung, die Maßnahme der Verbrechensbekämpfung in Frankreich als unverhältnismäßig zu qualifizieren. Die EEA sei formell ordnungsgemäß beantragt und erlassen. Die französische Polizei und Europol hätten sogar eine Verpflichtung, ihre Kenntnis von Straftaten den deutschen Behörden zu übermitteln. Eine Vorlage an den *EuGH* wird konsequent verweigert. Einig ist sich die Justiz bundesweit, dass selbst bei Zweifeln an der Rechtmäßigkeit der Infiltrierung des Servers die so gewonnenen Daten keinem Beweisverwertungsverbot unterliegen; die überragende Bedeutung der Aufklärung insbesondere schwerster Drogenkriminalität lasse in der vom *BGH* konstituierten und vom *BVerfG* abgesegneten Abwägungslehre jegliche prozessuale Fehlerhaftigkeit verblassen. Ein Beweisverwertungsverbot müsse die prozessuale Ausnahme sein, für die es hier keine ausreichenden Anhaltspunkte gäbe.

Die Sicherheit, mit der eine bestehende juristische Lösung der Problematik in diesen Entscheidungen suggeriert wird, ist irreführend. Das Konglomerat unterschiedlichster EU-Rechtsnormen, ungeklärte nationale Rechtsprobleme im Rechtshilfeverkehr in Verbindung mit der Vagheit einer Dogmatik von Beweisverwertungsverboten lassen die EncroChat-Konstellation als vorbildlos erscheinen. Sie hat vielmehr die Potenz für eine Weichenstellung des zukünftigen europäischen Strafprozesses.

E. Rechtshilfe zwischen staatlicher Souveränität und individuellem Grundrechtsschutz

Die Sicherung der bürgerlichen Grundrechte gegen forschen Ermittlungs- und Verurteilungseifer ist ein wesentliches Ziel strafprozessualer Gesetze. Wird in nationalen Strafprozessordnungen die Subjektstellung des betroffenen Bürgers hochgehalten, so wird er traditionell im Rechtshilfeverfahren zum Objekt staatlicher Souveränitäten und Eifersüchteleien degradiert. Die Europäische Union wollte das ändern und den subjektiven Rechten auch im transnationalen Strafverfahren Geltung verschaffen. Verzicht auf Teilaspekte staatlicher Souveränität und damit die Erleichterung des Rechtshilfeverkehrs in der EU sollten einhergehen mit der Betonung transnationaler Rechte auch im Strafverfahren.

Die EncroChat-Problematik dokumentiert, dass dies Vorhaben offensichtlich misslungen ist. Kein einziger deutscher Beschuldigter hatte und hat jemals die Chance, durch ein EU-weites Rechtsmittel den gesamten Vorgang oder einzelne juristische Schritte anzugreifen. Für Rechtsbehelfe in Frankreich gibt es keinen Ansatz, in Deutschland soll die EEA unanfechtbar sein, jedenfalls verweigert das *AG Frankfurt /M.* die Entscheidung über Beschwerden der EEA und lässt sie allenfalls an die mit konkreten Anklagen befassten Strafkammern nachsenden. Selbst eine Akteneinsicht in das Grund-

lagenverfahren der Generalstaatsanwaltschaft Frankfurt wird verweigert, es richte sich schließlich nicht gegen Hunderte von Beschuldigten, sondern »gegen Unbekannt«. Niemand soll wissen, welcher Staatsanwalt wann und wie in das Geschehen involviert war.

Rechtshilfe nach EU-Recht ist nach Ansicht der deutschen Justiz letztlich eine Erweiterung staatlicher Machtbefugnisse. Der bescheiden daherkommende Grundsatz des gegenseitigen Vertrauens nationaler staatlicher Machtapparate verschleiert, dass sich aus Sicht eines beschuldigten Bürgers die Potenz der auf Machtausübung fixierten Justiz und Polizei vervielfacht hat. Der prozessuale Grundrechtsschutz hat durch die EU-Vereinfachungen gelitten.

F. EU-weiter Informationsaustausch

Die rechtliche Bewertung unterliegt einem begrifflichen Verwirrspiel der deutschen Justiz. Es gehe doch nur – so der Ansatz vieler Entscheidungen – um »Informationen«. Was kann bedenklich sein an simplen Informationen? Suggeriert wird, es handele sich um einen weitgehend grundrechtsirrelevanten Aufklärungsvorgang, vergleichbar mit dem schlichten Auskunftsersuchen des § 163 StPO. Es wird sogar die Behauptung aufgestellt, bezüglich EncroChat handele es sich um einen nach dem Rahmenbeschluss 2006/960/JI legitimierten und notwendigen spontanen Informationsaustausch zwischen den Strafverfolgungsbehörden der Mitgliedstaaten. Die EEA vom 02.06.2020 enthalte daher auch nicht das Ersuchen um einen Grundrechtseingriff in Frankreich, sondern lediglich die harmlose Bitte um Übersendung bereits vorliegender Daten.

Der Weg zur organisierten Verantwortungslosigkeit ist mit der Reduktion auf schlichte Daten geebnet. Wird ein durch Folter erwirktes Geständnis eingeschmolzen auf äußere Buchstaben, Bits und Bytes, kann der Blick auf das Informationssubstrat umso leichter von dem maßgeblich zu beurteilenden prozessualen Lebenssachverhalt abgewandt werden.

G. Die Europäische Ermittlungsanordnung (EEA)

Antrag und Genehmigung der EEA begegnen vielfältigen Bedenken. Die EEA dient nicht allgemeiner Information, sondern konkreten strafrechtlichen Ermittlungszwecken. Art. 6 RL 2014/41/EU fordert unter Berücksichtigung der Rechte der verdächtigen oder beschuldigten Person die Einhaltung des Maßstabes der Notwendigkeit und Angemessenheit. Damit wird eine Ermittlung wegen einer konkreten Tat gegen einen konkreten möglichen Täter vorausgesetzt. Ein Verfahren ohne Bezug auf eine Tat oder einen möglichen Verdächtigen kann für den Erlass der EEA keine Grundlage sein. Die formale Hülle des Verfahrens der Generalstaatsanwaltschaft Frankfurt »gegen Unbekannt« kann keine taugliche Basis für den erbetenen Beweistransfer sein.

Nach Art. 6 RL 2014/41/EU kann die EEA nur ergehen, wenn die Ermittlungsmaßnahme in einem vergleichbaren innerstaatlichen Fall unter denselben Bedingungen hätte angeordnet werden können. Dass in Deutschland die Infiltrierung von mehr als 60.000 Mobiltelefonen unverdächtiger Bürger angeordnet werden könnte, darf als ausgeschlossen gelten. Eine maßgebliche Hürde für eine innerstaatliche grundrechtstangierende Ermittlungsmaßnahme ist nach der StPO der Anfangsverdacht. Hier wusste die Staatsanwaltschaft niemals, weswegen und gegen wen sie ermittelte. Sie war aufgrund kriminalistischer Hypothesen lediglich auf der Suche nach Informationen, um möglicherweise erstmals einen Anfangsverdacht formulieren zu können. Die Generalstaatsanwaltschaft Frankfurt stocherte im strafprozessualen Nebel, ohne die Idee einer Tat oder eines Täters.

Auch eine Online-Durchsuchung nach § 100b StPO (Staatstrojaner) setzt einen qualifizierten Anfangsverdacht voraus und unterliegt darüber hinaus dem Richtervorbehalt. Schon aus diesen Gründen wäre die EEA hier der Kompetenz der Staatsanwaltschaft entzogen.

H. Die Überprüfungsintensität ausländischer Beweisgewinnung durch deutsche Strafgerichte

Nicht Beschuldigtenrechte, sondern Arbeitserleichterungen für die Justiz stehen im Mittelpunkt der Entwicklung einer Rechtsprechung des *BGH*, die die Lähmung des aufklärungswilligen Strafrichters propagiert, wenn es allgemein bei der Verwertung von im Ausland gewonnenen Beweisen darum geht, deren Rechtmäßigkeit zu überprüfen. Das Vertrauen eines deutschen Beschuldigten, wonach der deutsche Strafrichter Garant für die Einhaltung eines fairen Verfahrens ist, soll berechtigterweise enttäuscht werden dürfen, wenn das die Verurteilung tragende Beweismittel im Ausland gewonnen wurde. Der *BGH* tarnt die Propagierung der Passivität mit einem pseudohöflichen Respekt gegenüber der ausländischen Staatsgewalt: Man wolle nicht den Eindruck erwecken, das ausländische Recht besser zu verstehen als die Behörden und Gerichte des Ermittlungsstaates.

EncroChat sollte Anlass für einen Wendepunkt in diesem Denken bieten. Nicht die Höflichkeit gegenüber einem französischen Ermittlungsrichter muss im deutschen Strafverfahren im Mittelpunkt stehen, sondern der Respekt vor den (Prozess-) Grundrechten eines Beschuldigten. Der Beschuldigte hat auch im Ausland einen Anspruch auf Einhaltung der Gesetze durch die Ermittlungsbehörden. Gerade im Zusammenhang mit Haftbedingungen im EU-Ausland haben sowohl das *BVerfG* als auch der *EuGH* zuletzt deutlich gemacht, dass der Blick über die Grenzen zur Wahrung der Bürgerrechte unabdingbar ist. Der deutsche Strafrichter hat jedenfalls dann Zurückhaltung gegenüber ausländischen Beweisermittlungen zu üben, wenn für ihn sehr deutlich ist, dass diese nur unter Verletzung tragender rechtsstaatlicher Verfahrensprinzipien erfolgten.

I. Forum shopping

Aktuell nutzen deutsche Gerichte ein internationales Pingpongspiel unterschiedlicher Zuständigkeiten, um das illusionäre Bild eines fairen Gesamtverfahrens zu skizzieren. In einer nahezu Palmström'schen Volte will beispielsweise das *OLG Hamburg* die Legitimation für Verurteilungen deutscher Angeklagter daraus ableiten, dass *nach* Vorliegen der EncroChat-Protokolle auch nach deutschem Recht eine Infiltration nach § 100b StPO möglich gewesen wäre.[1] Man setzt also mit dem rechtfertigenden Denken erst zu einem Zeitpunkt an, nachdem bereits ein – nach deutschem Recht unzulässiger – Informationsstand produziert worden ist.

Im Vorfeld der Regelung der EEA war befürchtet worden, dass internationale Ermittlungen das Niveau des fairen Prozesses massiv absenken. Wenn das Konzept einer nationalen Rechts-

1 OLG Hamburg, Beschl. v. 29.01.2021 – 1 Ws 2/21.

ordnung zur Wahrung der Grundrechte bestimmte einzelne Ermittlungsmaßnahmen untersagt, würden sich die Ermittler möglicherweise die gewünschten Ergebnisse über Ermittler anderer Staaten besorgen, bei denen unterschiedliche Gesetzesstrukturen exakt diese singuläre Maßnahme zulassen. Noch die deutsche Gesetzesbegründung zur Umsetzung der EEA-Richtlinie schwor, dass die EEA keinesfalls zur Kompetenzerweiterung der nationalen Ermittlungsbehörden führen dürfe.

Der Gesetzgeber hat den unbedingten Verfolgungswillen und den mangelnden Respekt der Ermittlungsbehörden vor den Menschenrechten seiner Bürger falsch eingeschätzt.

Das polizeiliche Vorgehen bei EncroChat dürfte alle Befürchtungen von Juristen übertreffen. Auch wenn die Beteiligten intensiv an Vertuschung arbeiten, steht fest, dass die deutschen Behörden die unzulässige Beweisgewinnung begleitet, unterstützt und womöglich mit initiiert haben. Europol vermittelte. Im Ergebnis wurden mit Kenntnis der deutschen Behörden zehntausende von Mobiltelefonen unverdächtiger Bürger auf deutschem Boden von den französischen Behörden überwacht. Die Ergebnisse trafen mit geringfügiger zeitlicher Verspätung auf den Schreibtischen der deutschen Ermittler ein. Wo ein polizeilicher Wille ist, ist auch ein Weg.

J. Beweisverwertungsverbot

Keine der bislang bekannt gewordenen gerichtlichen Entscheidungen in Deutschland begnügt sich mit dem Lob polizeilicher Effektivität. Dass die Ermittler bindende Rechtsnormen verletzt haben könnten, will kaum ein Richter ausschließen. Unisono will man hieraus allerdings keine Konsequenzen ziehen. Dass Gesetze dazu gedacht sind, eingehalten zu werden, erkennt der Strafrichter bei den vor ihm sitzenden Angeklagten, nicht jedoch bei Ermittlern.

Aus dem ursprünglich vom *BVerfG* formulierten Grundsatz, dass aus prozessualen Gesetzesverstößen »nicht ohne weiteres« auch ein Beweisverwertungsverbot entsteht, hat die strafrichterliche Rechtsprechung in Umkehrung rechtsstaatlicher Grundsätze die Behauptung entwickelt, die Nichtverwendung müsse regelmäßig die – wohlbegründete – Ausnahme sein. Eine solche Ausnahme sieht aktuell kein deutscher Strafrichter. Unter Ausblendung des gescheiterten gesetzgeberischen Konzepts, Drogenhandel und Drogenkonsum durch Strafrecht zu unterbinden, reicht manchen Landgerichten die herausragende Bedeutung der letztendlich verfolgten Drogendelikte, um dahinter alle anderen denkbaren Abwägungsfaktoren verblassen zu lassen.

Wenn erkannt wird, dass auch bei der – so der *BGH* – schier unendlichen Weite der strafrichterlichen Akzeptanz von illegalen Ermittlungsergebnissen die Bewahrung von grundsätzlichen Gewährleistungen des Rechtsstaatsprinzips eine unüberwindliche Hürde für die Verwertung bilden könnte, finden sich nur Solidaritätsbekundungen mit den französischen Richtern. Diese hätten anständig, zielgerichtet und rechtskonform gehandelt.

Das Gegenteil ist der Fall.

Die bereits bekannten Fakten machen deutlich, dass die Behörden als unübersteigbar geltende Grenzen von Menschenrechten und Grundrechten überschritten haben. Freiheit in einem Rechtsstaat bedeutet die Freiheit vor der Kontrolle jeglicher Kommunikation des Bürgers. Das Post- und Fernmeldegeheimnis in Art. 10 GG hat dies exemplarisch und prominent herausgestrichen. Art. 8 der Europäischen Menschenrechtskonvention fordert vom Staat die unbedingte Achtung des Privatlebens seines Bürgers und seiner Korrespondenz. Art. 17 IPBR stellt weltweit die Forderung auf, dass niemand willkürlichen staatlichen Eingriffen in seinen Schriftverkehr ausgesetzt werden darf. Modern und lakonisch heißt es in Art. 7 der EU-Grundrechtecharta: *»Jede Person hat das Recht auf Achtung […] ihrer Kommunikation.«*

Nichts dergleichen hat die staatliche Autorität geachtet. In der ebenso unbewiesenen wie unsubstantiierten Hoffnung auf Aufdeckung einiger krimineller Taten hat die Staatsgewalt Millionen kommunikativer Datensätze ihrer Bürger mitgelesen und kontrolliert. Dieser massenhafte Eingriff in die Privatheit der Bürger ist unter keinem einzigen legitimierenden Kriterium denkbar, das der *EGMR* oder das *BVerfG* in der Vergangenheit aufgestellt haben. Abseits von der Überlegung des eingriffshindernden Anfangsverdachts ist das Prinzip der Verhältnismäßigkeit nie gewahrt.

Bereits bei der Beurteilung der anlasslosen Vorratsdatenspeicherung hatte der *EuGH* deutlich gemacht, dass das blinde Abgreifen von Kommunikationsdaten niemals gerechtfertigt sein kann, wenn es nicht ausnahmsweise um existenzielle staatliche Belange geht. Was für inhaltslose Kommunikationsdaten des digitalen Austausches gilt, muss erst recht für Maßnahmen gelten, die den Inhalt der privaten Kommunikation betreffen.

Fazit: Der staatliche Datenraub von Roubaix verletzt den Kerngehalt grundgesetzlicher und menschenrechtlicher Garantien. Seine bewusste Missachtung kann nur das Verbot einer strafprozessualen Verwertung der Ergebnisse zur Folge haben.

K. Ausblick in den Orwell'schen Abgrund

EncroChat beleuchtet grell symptomatische Entwicklungen sowohl der Justiz als auch der Gesellschaft:

Die angesprochenen juristischen Problembereiche sollten zumindest diskutabel sein. Die Justiz will allerdings nicht diskutieren. In einer bemerkenswerten Einheitlichkeit wehren sich die deutschen Strafrichter mit Verve dagegen, dass ihnen ein geschätztes Beweismittel wieder aus der Hand genommen wird. Das mag psychologische Gründe haben: Neurowissenschaftler haben belegt, dass das menschliche Gehirn nicht in der Lage ist, einen einmal wahrgenommenen und positiv eingeschätzten Sachverhalt aus einer späteren Entscheidung auszublenden. Letztlich verlangt das Gesetz mit der Dogmatik der Beweisverwertungsverbote übermenschliches und traut Richtern einen solchen Kraftakt zu. Ein solches Vertrauen wird täglich in Gerichtssälen enttäuscht, die Totalität der EncroChat-Lösung in der Richterschaft zeigt schlaglichtartig die Dominanz dieses Phänomens beim Richten in unserer Zeit.

Symptomatisch ist auch die Enttäuschung des Bürgers, der noch an die Wahrung seiner Grundrechte durch die dritte Gewalt glaubt. In der besonderen gesellschaftlichen Position der Unabhängigkeit war Richtern die Aufgabe anvertraut, Bürger vor den willkürlichen Eingriffen der Exekutive – und hier insbesondere von Ermittlern – zu schützen. Stattdessen nehmen Verteidiger schon seit vielen Jahren wahr, dass sich Richter in der Rolle des solidarischen verlängerten Arms der polizeilichen Verbrechensjäger wohlfühlen. Die Rechtfertigungen der EncroChat-Ergebnisse verdeutlichen dies exemplarisch. So wird beispielsweise die Verwertbarkeit der Daten von einem *Senat* damit gerechtfertigt, dass das Ermittlungsziel der Be-

hörden (leider) ohne Zugriff auf die Daten nicht zu erreichen gewesen war. Oder: Was polizeilich sein muss, muss sein.

Merkwürdig ist in der aktuellen gesellschaftlichen Diskussion die Reaktion der Presse. Selbst staatskritische Medien begnügen sich zumeist damit, die durch EncroChat erzielten Erfolge der Kriminalitätsaufdeckung abzufeiern, und decken das millionenfache Mitlesen privatester Korrespondenz mit dem Mantel des Schweigens zu. Die fehlende Kritik von Justiz und Presse befeuert die Ermittler darin, noch weiter in das Privatleben von Bürgern einzudringen. EncroChat war erst der Anfang. Bereits Mitte März wurde bekannt, dass seit längerer Zeit ein noch viel größeres Kommunikationsunternehmen – Sky ECC – infiltriert worden sein soll. »WhatsApp«, »Signal«, Telekom und Vodafone könnten die nächsten sein, die unfreiwillig und fern der Gesetze – über andere Staaten – ihre Kommunikationsdaten dem Überwachungsstaat ausliefern.

Verteidigung scheint derzeit die einzige gesellschaftliche Kraft zu sein, die zu einem Umdenken beitragen könnte.

Der »BAMF-Skandal« – Strafverfolgung zwischen Politik und Medien

Prof. Dr. Henning Ernst Müller, Regensburg

Im April begann[1] die Hauptverhandlung über Vorwürfe, die vor fast drei Jahren die unter dem Namen »BAMF-Skandal« bekannt gewordene Affäre begründeten. Grundlage dieser Hauptverhandlung ist das seit Jahrzehnten aufwändigste Ermittlungsverfahren der Bremer Staatsanwaltschaft, jedenfalls bearbeitet von der »bislang größte[n] Ermittlungsgruppe in der Geschichte der Polizei Bremen«.[2] Von den Tatvorwürfen der Anklage sind nach dem Eröffnungsbeschluss des *LG Bremen*[3] jedoch nur wenige zum Hauptverfahren zugelassen worden. Über den Kern des »Skandals«, der im Jahr 2018 monatelang die Öffentlichkeit beschäftigte, wird also nicht mehr strafrechtlich geurteilt werden, weil das *LG Bremen* insofern schon den hinreichenden Tatverdacht verneinte (§ 203 StPO). Das auch insoweit erstaunliche Verfahren ist eines, dessen juristische und nichtjuristische Zusammenhänge und Wirkungen schon zuvor eine Vielzahl von problematischen Aspekten der Strafverfolgung unter den Bedingungen der Mediengesellschaft sichtbar gemacht haben. Die folgenden Ausführungen sollen diese Zusammenhänge verdeutlichen. Zudem sollen einige Anmerkungen zum Eröffnungsbeschluss des *LG Bremen* gemacht werden.

A. Aufdeckung des »Skandals«

Am 20.04.2018 berichteten Presse- und Rundfunkorgane übereinstimmend, die ehemalige Leiterin der BAMF-Außenstelle in Bremen werde verdächtigt, in kollusivem Zusammenwirken mit einigen Rechtsanwälten in etwa 2000 Fällen in Asyl- bzw. Aufenthaltsverfahren rechtswidrig zugunsten von Asylsuchenden entschieden zu haben.[4]

Verantwortlich für diese Berichterstattung war ein Recherchenetzwerk des NDR, der Süddeutschen Zeitung und Radio Bremen. Diese Meldungen waren aber nicht Ergebnis investigativ-journalistischer Recherche im engeren Sinne. Die Staatsanwaltschaft ermittelte zu diesem Zeitpunkt bereits fünf Monate lang[5] und die Hauptbeschuldigte war bereits Mitte 2016 von ihrem Leitungsposten versetzt worden.[6]

Insbesondere die in der seriösen Presse und im öffentlich-rechtlichen Rundfunk berichteten Einzelheiten sowie die umgehende Bestätigung der Bremer Staatsanwaltschaft, ein Ermittlungsverfahren inklusive Durchsuchungen und Beschlagnahmen finde bereits statt,[7] überzeugten einen großen Teil der Öffentlichkeit davon, dass die Vorwürfe auf tatsächlichen Grundlagen beruhten und nur noch Details der »kriminellen Machenschaften« zur Debatte stünden. Geschildert wurde eine Anzahl von 1200 bzw. 2000[8] rechtswidrig beschiedenen Fällen im Zeitraum von 2013 bis 2017, mutmaßlich unter gewerbsmäßigen Bedingungen. Konkret wurde behauptet, die Bremer Außenstelle sei nur für einen Bruchteil dieser Fälle überhaupt zuständig gewesen.[9] Die beschuldigten Rechtsanwälte hätten zur Durchführung der Asylverfahren im (unzuständigen) Bremen sogar Busse organisiert, um ihre Mandanten zur Anhörung nach Bremen zu transportieren.[10] Schließlich seien auch Vorteile an die beschuldigte Beamtin geflossen, wobei (»zumindest«) von Restauranteinladungen und Hotelübernachtungen die Rede war.[11]

Es ist nicht völlig geklärt, auf welchem Wege die Informationen über die Tatvorwürfe und das Ermittlungsverfahren an die Presse gelangten. Einerseits wurde nachträglich über eine schon frühere Befassung eines Journalisten von Radio Bremen mit Korruptionsgerüchten berichtet; dieser habe auch schon mit der Bremer Staatsanwaltschaft in Kontakt gestanden.[12] Einen größeren Anteil an der Publikation der Affäre im April und Mai 2018 hatte aber wohl eine Beamtin des BAMF, die zwischenzeitlich anstelle der 2016 suspendierten

1 Das Verfahren gegen die Hauptangeklagte wurde inzwischen gem. § 153a StPO gegen eine Geldauflage vorläufig eingestellt.
2 StA Bremen, Staatsanwaltschaft erhebt Anklage im »BAMF-Verfahren«, Pressemitteilung 7/2019 v. 19.09.2019, S. 2.
3 LG Bremen StV-S 2021, 45 (in diesem Heft).
4 *Richter/Strozyk*, Verdacht auf weitreichenden Skandal im Bamf, SZ 20.04.2018.
5 *Adelhardt*, BAMF-Affäre: Angaben vom Hörensagen, NDR-Presseportal 08.06.2018.
6 *Adelhardt/Stalinski/Stempfle*, Chronologie der BAMF-Affäre: Was passierte wirklich?, tagesschau 20.08.2018.
7 StA Bremen, Ermittlungsverfahren wegen Verleitung zum Asylmissbrauch, Pressemitteilung 3/2018 v. 20.04.2018.
8 *Richter/Strozyk* (Fn. 4) korrigieren ihre Angabe von 1200 Fällen noch am selben Tag auf 2000 Fälle.
9 *Richter/Strozyk* (Fn. 4) schreiben, nur für 98 Fälle sei die Außenstelle Bremen zuständig gewesen.
10 *Richter/Strozyk* (Fn. 4).
11 *Richter/Strozyk* (Fn. 4).
12 *Adelhardt* (Fn. 5); *Schirrmeister*, Der eigentliche »Bamf-Skandal«: die Berichterstattung der Medien, Übermedien 13.09.2019.