Faculty of Law,
Economics
and Finance

Law Working Paper Series
Paper number 2021-010

Wenn Sicherheitsinteressen kollidieren

Technische und rechtliche Implikationen einer verpflichtenden Zugriffmöglichkeit auf verschlüsselte Daten durch Behörden

Sandra Schmitz, University of Luxembourg
sandra.schmitz@uni.lu

Stefan Schiffner, University of Luxembourg
Stefan.Schiffner@uni.lu

02/11/2021

UNIVERSITÉ DU LUXEMBOURG

Wenn Sicherheitsinteressen kollidieren – Technische und rechtliche Implikationen einer verpflichtenden Zugriffsmöglichkeit auf verschlüsselte Daten durch Behörden[1]

Stefan Schiffner/Sandra Schmitz

Interdisciplinary Centre for Security, Reliability and Trust (SnT)/Université du Luxembourg
stefan.schiffner@uni.lu/sandra.schmitz@uni.lu

Im November 2020 verabschiedete der Rat der Europäischen Union seine Entschließung zur Verschlüsselung[2], in welcher die Notwendigkeit der Sicherheit durch Verschlüsselung und der Sicherheit trotz Verschlüsselung hervorgehoben wird. Hintergrund der Entschließung ist die Annahme, dass der Zugang zu verschlüsselten Inhalten für zuständige Behörden im Bereich Sicherheit und Strafjustiz bei u.a. der Bekämpfung von Terrorismus und organisierter Kriminalität zunehmend an Bedeutung gewinne. Die Idee einer außergewöhnlichen Zugriffsmöglichkeit auf verschlüsselte Daten wird auch von der Europäischen Kommission in Mitteilungen wie z.B. der Counter-Terrorism Agenda[3] und anderen EU-Gesetzesinitiativen wie dem Entwurf für eine NIS-Richtlinie 2.0[4] aufgegriffen. Während die anvisierte Förderung und teilweise auch Verpflichtung von Diensteanbietern zur Ende-zu Ende-Verschlüsselung einen Schritt vorwärts zu mehr Datensicherheit bedeutet, stellt eine verpflichtende Zugriffsmöglichkeit auf verschlüsselte Daten für Sicherheits- und Strafverfolgungsbehörden genau für diese begehrte Datensicherheit einen Rückschritt dar. Eine solche Zugriffsmöglichkeit, die keine Hintertür ist, ist zum einen technisch vermutlich nicht darstellbar und stellt darüber hinaus immer eine Schwachstelle für die IT-Sicherheit dar.

[1] Dieser Aufsatz basiert auf einem Vortrag bei der 22. Herbstakademie 2021 der Deutschen Stiftung für Recht und Informatik „Im Fokus der Rechtsentwicklung – Die Digitalisierung der Welt“, welche virtuell im September 2021 stattfand. Eine Kurzversion des Vortrags mit dem Titel „Ein Schritt vor, zwei Schritte zurück? Technische und rechtliche Implikationen einer verpflichtenden Zugriffsmöglichkeit auf verschlüsselte Daten“ findet sich im Tagungsband, Jürgen Taeger (Hrsg.), Im Fokus der Rechtsentwicklung -Die Digitalisierung der Welt, S. 289 – 304.

[2] *Rat der Europäischen Union,* Entschließung, 13084/1/20 REV 1.

[3] *Europäische Kommission,* A Counter-Terrorism Agenda for the EU, COM(2020) 795 final.

[4] *Europäische Kommission,* Proposal for a NIS 2.0 Directive, COM(2020) 823 final.

Inhalt

I. Einleitung: Politischer Wille zu außergewöhnlichen, aber rechtmäßigen Zugriffsmöglichkeiten auf verschlüsselte Daten

Unstrittig hat die Digitalisierung inzwischen alle Lebensbereiche erreicht. Dabei ist (Tele-) Kommunikation noch immer der Lebensbereich, der am stärksten digitalisiert ist. Bis auf wenige Ausnahmen findet heute jegliche Art von Kommunikation ganz oder teilweise digital statt. Digitale Kommunikation ist schneller, zuverlässiger und vor allem billiger. So ist es nicht überraschend, dass leicht zugängliche „Verschlüsselungslösungen, die für rechtmäßige Zwecke konzipiert sind“ auch von Straftätern „für ihre Vorgehensweisen“ genutzt werden können.[5] Während der Zugriff auf elektronische Beweismittel für Sicherheits- und die Strafverfolgungsbehörden in diesem Zusammenhang immer bedeutender

[5] *Rat der Europäischen Union,* Entschließung, 13084/1/20 REV 1, S. 3.

wird, erschwert aber eben gerade der einfache Zugang zu Verschlüsselung zunehmend den Zugang zu Daten.

Eine Entschließung zur „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“ des Rates soll nun den Rahmen für „außergewöhnliche, aber rechtmäßige“ Zugriffsmöglichkeiten setzen. Kurz vor Ende der Ratspräsidentschaft der Bundesrepublik Deutschland hat der Rat die von der Bundesregierung ausgearbeitete Entschließung verabschiedet. Mit dem sperrigen Titel soll zum Ausdruck gebracht werden, dass man bei der Schaffung eines Rahmens für rechtmäßige behördliche Zugriffe die Cybersicherheit und die Förderung einer starken Verschlüsselung nicht außer Acht lässt; vielmehr soll beides in Einklang gebracht werden. Entsprechend bezieht sich der Begriff der *Sicherheit durch Verschlüsselung* offensichtlich auf IT-Sicherheit, der Begriff der *Sicherheit trotz Verschlüsselung* aber ebenso offensichtlich auf die öffentliche Sicherheit, anders ließe sich das vermeintliche Paradoxon auch nicht auflösen. Der Text der Entschließung macht dies dann auch unmissverständlich deutlich: Der Rat hebt einerseits seine Unterstützung für die Entwicklung, Umsetzung und Nutzung starker Verschlüsselung als ein notwendiges Mittel zum Schutz von Grundrechten und der digitalen Sicherheit der Bürgerinnen und Bürger sowie von Regierungen, Industrie und Gesellschaft hervor.[6] Andererseits soll sichergestellt werden, dass die zuständigen Behörden im Bereich Sicherheit und Strafjustiz, ihre gesetzlichen Befugnisse zum Schutz der Gesellschaften und Bürger durch Zugriff auf verschlüsselte Daten ausüben können.

Dieser Gedanke wird im Übrigen unter anderem auch in der Counter-Terrorism Agenda der EU, sowie bspw. der Richtline (EU) 2018/1972 (sog. EECC)[7] und dem Vorschlag für eine NIS 2.0 Richtlinie aufgegriffen. So heißt es im Erwägungsgrund 96 des EECC, dass die Verschlüsselung gefördert werden sollte und erforderlichenfalls mittels datenschutzfreundlicher Voreinstellungen und Technikgestaltung vorgeschrieben werden. Gleichzeitig sollen dadurch aber nicht „die Befugnisse der Mitgliedstaaten, den Schutz ihrer wesentlichen Sicherheitsinteressen und der öffentlichen Sicherheit zu gewährleisten und die Ermittlung, Aufklärung und Verfolgung von Straftaten zu ermöglichen“ berührt werden. Der Entwurf für eine NIS 2.0 Richtlinie, welche ebenfalls die Förderung von insbesondere Ende-zu-Ende Verschlüsselung vorsieht, spezifiziert letzteres dahingehend, dass die Nutzung von Ende-zu-Ende Verschlüsselung mit den zuvor genannten Befugnissen der Mitgliedsstaaten in Einklang zu bringen ist.[8] Ähnlich wie die Entschließung des Rates zur Verschlüsselung und auch die Counter-Terrorism Agenda, hebt der der Vorschlag für eine NIS 2.0 Richtlinie hervor, dass „Lösungen für den rechtmäßigen Zugang zu Informationen in End-zu-End-verschlüsselter Kommunikation […] die Wirksamkeit der Verschlüsselung beim Schutz der Privatsphäre und der Sicherheit der Kommunikation aufrechterhalten und zugleich eine wirksame Reaktion auf Straftaten gewährleisten“ sollten.

[6] Ebenda, S. 2.

[7] Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation, Abl. L 321/36 vom 17.12.2018.

[8] (n4) Erwägungsgrund 54.

Befasst man sich mit der Funktionsweise von Verschlüsselung, so stellt sich zwangsläufig die Frage, wie die nunmehr allseits beschworenen Ziele - (i) Sicherheit durch Verschlüsselung und (ii) Sicherheit trotz Verschlüsselung - in Einklang gebracht werden können. In diesem Sinne hinterfragt dieser Beitrag, ob es grundsätzlich möglich ist behördliche Zugriffsmöglichkeiten auf verschlüsselte Daten (zur Sicherheit *trotz* Verschlüsselung) so zu gestalten, dass Sicherheit *durch* Verschlüsselung weiterhin gewährleistet sein kann. Zunächst wird hierzu die Funktionsweise und der derzeitige Stand der Technik bei Verschlüsselung grob skizziert, bevor allgemein Sinn und Zweck von Verschlüsselung erläutert werden. Auch wird kurz historisch beleuchtet, dass vertrauliche Kommunikation im Internet schon immer Begehrlichkeiten bei staatlichen Stellen weckte. Am Beispiel des Datenschutzes und der IT-Sicherheit wird schließlich aufgezeigt, welche Bedeutung der europäische Gesetzgeber wiederum der Verschlüsselung beimisst, bevor kritisch verpflichtende Zugriffsmöglichkeiten eruiert werden. Da offensichtlich ist, dass Zugangsmöglichkeiten „im vollen Einklang mit einem ordnungsgemäßen Verfahren und anderen Garantien sowie Grundrechten“ [9] zu stehen haben, wird im Anschluss die in der Erklärung außen vor gelassene technische Seite in den Fokus gerückt.

II. Hintergrund: Der Zugriff auf verschlüsselte Daten

1. Historischer Kontext

a. Rückblick: Die frühen „Crypto Wars“

Die gegenwärtige Diskussion um die Entschließung kann nicht ohne einen Rückblick auf frühe Bestrebungen der US-amerikanischen Regierung, die Verschlüsselung außerhalb der militärischen Nutzung zu unterbinden erfolgen. Tatsächlich diente Verschlüsselung zu Anfang dazu den Zugriff Dritter auf staatliche, vertrauliche Kommunikation technisch und rechtlich zu erschweren. Dabei waren Dritte oft andere Staaten bzw. deren Geheimdienste. Entsprechend galt Verschlüsselungstechnologie als Produkt der Rüstungsindustrie, welches entsprechenden Exportbeschränkungen unterfiel. Mit der Digitalisierung des zivilen Raums wuchs auch das Schutzbedürfnis, insbesondere, da das Internet und digitale Dienste zunehmend als kommerzielles Spielfeld für innovative Produkte wahrgenommen wurden. Somit wurden Produkte, die kryptografische Verfahren beinhalteten, zu „Dual-Use-Technologie“.[10] Insbesondere in den USA führte das zu einer starken Regulierung des Marktes, wiederum mit Exportbeschränkungen für Produkte mit starker Kryptografie.[11] In Konsequenz mussten Softwarehersteller Exportversionen ihrer Software anbieten, die entsprechend schlechter geschützt war. Dies erwies sich bald als Standortnachteil und führte zum Urkrieg der sog. „Crypto-Wars“. Dieser fand erst

[9] *Rat der Europäischen Union,* Entschließung, 13084/1/20 REV 1, S. 4.

[10] Siehe auch die entsprechenden Auflistungen zu Kryptografie im Wassenaar Abkommen, abrufbar unter https://www.wassenaar.org/ (abgerufen 30.06.2021).

[11] *Schwartzbeck*, The Evolution of US Government Restrictions on Using and Exporting Encryption Technologies, https://www.cia.gov/readingroom/docs/DOC_0006231614.pdf (abgerufen 30.06.2021).

sein Ende als Anfang der 2000er Jahre die damalige Clinton-Administration diese Exportbeschränkungen weitestgehend aufhob,[12] wenn auch weiterhin Beschränkungen bestehen. Trotz der damaligen klaren Kosten-Nutzen-Abwägung zu Gunsten starker und frei verfügbarer Kryptoprodukte, kehrt dieses Thema in kurz-frequenter Regelmäßigkeit zurück.

b. Voraussetzung für gegenwärtige Diskussion: Sicherheit durch Verschlüsselung in allen Lebensbereichen

Der Urkrieg der Crypto-Wars zeigt sich nun in neuem Gewand. Ob öffentlich oder privat, in allen Lebensbereichen findet Verschlüsselung in der heutigen Zeit Anwendung. Während Verschlüsselung in den Anfängen besonders dem sicheren Austausch vertraulicher Inhalte des Staates diente, wird eine Verschlüsselung von Kommunikation heute von vielen Internetnutzern quasi vorausgesetzt: Schließlich bewegt man sich bei der Kommunikation im Internet in einem öffentlichen Netz, der Kommunikationsweg ist also alles andere als sicher. Über genau dieses Netz tauscht die Privatperson genauso gerne sensible Informationen aus, wie ein Unternehmen Geschäftsgeheimnisse. Verschlüsselung hat als solche nun einen deutlich größeren Anwenderkreis, gerade auch weil die Nutzung verschlüsselter Dienste keine besonderen IT-Kenntnisse mehr erfordert.

Denkt man bei Verschlüsselung nur an den Schutz vertraulicher Inhalte, so lässt dies die weiteren Aspekte der Schutzziel-Trias der IT-Sicherheit außen vor. IT-Sicherheit erfordert Vertraulichkeit, Integrität und Verfügbarkeit von Daten, im Englischen auch als CIA (confidentiality, integrity and availability) der IT-Sicherheit bekannt. Neben des ersten Schutzziels, der Vertraulichkeit, wird auch das zweite Schutzziel, die Integrität, durch die Anwendung von Kryptografie gewährleistet. Verschlüsselung schützt Daten während des Übertragungsvorgangs oder der Speicherung vor dem unberechtigten Zugriff Dritter. Mit den gleichen mathematischen Mitteln schützen kryptographische Prüfsummen und elektronische Signaturen Daten vor der unberechtigter Manipulation Dritter. Verfügbarkeit lässt sich nicht durch Kryptografie sicherstellen und wird im Allgemeinen durch Redundanz, d.h. Daten- und Funktionalitätsreplikation, gesichert. Es lässt sich aber zeigen, dass der Verlust einer Schutzdimension zur Unbrauchbarkeit des Systems führt. In Konsequenz wird die Schutzziel-Trias immer als Einheit betrachtet. Die mathematische Verwobenheit von Vertraulichkeit und Integrität hat zur Konsequenz, dass erfolgreiche Angriffe[13] auf eine der beiden Dimensionen oft übertragbar ist auf die andere. Auch ist es so, dass in der Praxis beide Schutzziele im Wege der sog. Authenticated Encryption (AE) oft zu-

[12] *Spiegel online,* USA lockern Exportbeschränkungen, v. 16.01.2000, https://www.spiegel.de/netzwelt/web/kryptographie-usa-lockern-exportbeschraenkungen-a-59981.html (abgerufen 30.06.2021).

[13] Angriffe meint in diesem Kontext Manipulationen des Systems durch Dritte (Angreifer) mit dem Ziel ein oder mehrere Schutzziele zu brechen.

sammen implementiert werden, da dies eine geringere Anfälligkeit für Programmierfehler gewährleistet. Dieses Vorgehen ist in der Praxis soweit anerkannt, dass z.B. die neuste Version des weit verbreiteten TLS-Protokolls (1.3)[14] nur noch AE zulässt.

2. Was bedeutet Verschlüsselung aus technologischer Sicht?

Um die verschiedenen Ansatzpunkte für einen Zugriff auf verschlüsselte Daten zu analysieren, bedarf es zunächst einer Erläuterung, was Verschlüsselung eigentlich bedeutet und wie diese technisch funktioniert.

a. Kryptografische Technologien

Zunächst kann zwischen symmetrischer und asymmetrischer Kryptografie (auch Public Key-Kryptografie) unterschieden werden. Die Verfahren unterscheiden sich in der Art der Schlüssel[15]. Kommen symmetrische Verfahren zur Anwendung, dann können alle Kommunikationspartner alle kryptografischen Operationen ausführen, d.h. jeder im Besitz des Schlüssels kann ver- und entschlüsseln oder kryptografische Prüfsummen erzeugen. Asymmetrische Verfahren zeichnen sich durch Schlüsselpaare aus, wobei ein Teil öffentlich sein kann, während der andre Teil typischerweise nur einer Partei bekannt ist. So kann der öffentliche Schlüssel von jedem zum Verschlüsseln benutzt werden, aber nur der Besitzer des geheimen Schlüssels kann auch entschlüsseln. Erst die Erfindung asymmetrischer Kryptografie erlaubte die weit verbreitete Anwendung sicherer elektronischer Kommunikation, da sie erlaubt (öffentliche) Schlüssel über unsichere Kommunikationswege auszutauschen, während sie gleichzeitig die Zahl der nötigen Schlüssel reduziert. Außerdem ermöglicht asymmetrische Kryptografie sichere Kommunikation zwischen Kommunikationspartnern, die sich nicht uneingeschränkt vertrauen. Anwendungsfälle reichen von Verträgen und Attesten (elektronische Signaturen) bis hin zur Durchsetzung von Verwertungsrechten (digitale Wasserzeichen).

Da asymmetrische Verfahren in der Regel mathematisch komplexer sind (längere Rechenzeiten, erhebliche Nachrichtenexpansion, die zu Verteuerung bei der Übertragung führen) werden beide Verfahren in der Praxis immer in Kombination verwendet. Für Verschlüsselung heißt das, ein typischerweise kurzer und nur für den aktuellen Kontext gültiger symmetrischer Schlüssel (Session-Key) wird mittels asymmetrischer Verfahren ausgetauscht und dann für die eigentliche Kommunikation verwendet. In sogenannten nicht-interaktiven Verfahren wird dabei der mit dem asymmetrischen Verfahren

[14] *Rescorla*, Internet Request for Comments (RfC) 8446, The Transport Layer Security (TLS) Protocol 1.3, DOI: 10.17487/RFC8446.

[15] In der modernen Kryptografie ist ein Schlüssel eine Information, die es dem Besitzer erlaubt eine kryptografische Operation auszuführen, z.B. zu verschlüsseln oder zu signieren. Hinweis: der Schlüssel ist das einzige Geheimnis in der modernen Kryptografie (Kerhofsprinzip).

verschlüsselte Session-Key[16] direkt an die Nachricht angehängt, während bei interaktiven-Verfahren vor jeder Session ein Schlüsselaustausch-Protokoll durchgeführt wird.

Ähnlich wird für eine elektronische Signatur das zu signierende Dokument mittels einer kryptografisch sicheren Streuwertfunktion auf einem kurzen (für das Dokument repräsentativen) Streuwert[17] abgebildet und dieser Streuwert wird dann signiert. Im klassischen Anwendungsfall wie oben beschrieben, hat dieses Vorgehen Nachteile. Zum einen wird das Gesamtsystem komplexer, was die Angriffsfläche der Implementierung vergrößert, zum anderen reicht ein erfolgreicher Angriff entweder des symmetrischen oder des asymmetrischen Teils aus, um die Sicherheit des Systems zu kompromittieren. Dabei ist aber zu erwähnen, dass bei Systemen, die perfekte vorwärtsgerichtete Geheimhaltung[18] bieten, durch einen erfolgreicher Angriff auf den asymmetrischen Teil nur zukünftig ausgetauschte Schlüssel kompromittiert werden.

b. Differenzierung zwischen Ende-zu-Ende-Verschlüsselung und Kanalverschlüsselung

Neben den oben aufgeführten grundsätzlich verschiedenen kryptografischen Technologien, unterscheidet man weiterhin zwischen Ende-zu-Ende-Verschlüsselung (im Folgenden: E2E-Verschlüsselung) und Kanalverschlüsselung. Diese Unterscheidung ist unabhängig davon welche kryptografische Technologie zum Einsatz kommt; es wird vielmehr unterschieden welche Partei welche Schlüssel kennt. Dabei wird von E2E-Verschlüsselung gesprochen, wenn nur der tatsächliche Empfänger das nötige Schlüsselmaterial hat, um eine Nachricht zu entschlüsseln, und von Kanalverschlüsselung, wenn auch (u.U. ausgewählte) Zwischenstationen, wie zum Beispiel Server des Internetdiensteanbieters, Nachrichten entschlüsseln können. Ein typisches Beispiel von Kanalverschlüsselung sind Web-Mail-Dienste: die Kommunikation vom Nutzer zum Server ist zwar verschlüsselt, aber die Nachrichten sind beim Dienstanbieter im Klartext und werden (im besten Fall) auf dessen Server mit einem anderen Schlüssel gegen Zugriff durch unberechtigte Dritte geschützt. Möchte nun der Empfänger auf diese Email zugreifen, wird der Dienstanbieter die Nachricht erst entschlüsseln um sie dann mit dem Kanalschlüssel des Empfängers verschlüsselt an den Empfänger zu senden.

c. Konsequenzen von hybriden Verfahren für den Zugriff durch Ermittlungsbehörden

Die in der Praxis übliche Verwendung hybrider Verschlüsselung hat technische Konsequenzen wie ein Zugriff von Ermittlungs- oder Sicherheitsbehörden auf verschlüsselte Inhalte im Rahmen eines Ermittlungsverfahrens implementiert werden kann. Im Fall, dass E2E-Verschlüsselung verwendet wurde, kann die Ermittlung nur über eine Art Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) erfolgen. Dabei ist es wichtig, dass im Verlauf der Überwachung erzeugte Session-Keys gespeichert werden,

[16] Korrekter: das notwendige Schlüsselmaterial, das es dem Kommunikationspartner in Kombination mit seinem geheimen Schlüssel erlaubt ein gemeinsames Geheimnis zu erzeugen, welches dann verwendet wird, um den eigentlichen Session-Key zu erzeugen.

[17] Englisch: cryptographic hash funktion, hash.

[18] Englisch: perfect forward secrecy.

da diese letztlich nötig sind um verschlüsselte Nachrichten, die während der Überwachung entstanden sind, zu entschlüsseln. Das Vorhalten von Langzeit-Schlüsseln der asymmetrischen Verfahren kann das nicht unter allen Umständen leisten (siehe perfekte vorwärtsgerichtete Geheimhaltung). Aus dem gleichen Grund, ist die Möglichkeit der Entschlüsselung von Berichten aus der Vergangenheit bei diesem Vorgehen nicht garantiert.

Im Fall von kanalverschlüsselter Kommunikation könnten Behörden auf die Kooperation von Diensteanbietern setzen: auch hier wäre es allerdings nötig alle Session-Keys des Überwachungsziels im Überwachungszeitraum vorzuhalten. Eine nachträgliche Rekonstruktion von Session-Keys ist u.U. nicht möglich, sodass nicht auf Inhalte in der Vergangenheit zugegriffen werden kann, sondern nur eine Echtzeit-TKÜ garantiert ist.

3. Technologischer Fortschritt: ein ständiger Wettlauf mit der Zeit

Auch wenn in jüngster Zeit die Halbleiterindustrie nicht mehr in der Lage war das mooresche Gesetz[19] zu erfüllen, bedroht der fortlaufende Erkenntnisgewinn, sei es durch Ressourcen-Verbilligung, neue mathematische Erkenntnisse oder neue Technologien, die Sicherheit von bestehenden Systemen. Gerade für asymmetrische Verfahren stellen sog. Brute-Force Angriffe, also Angriffe, die darauf basieren, dass der gesamte potentielle Nachrichtenraum (Suchraum) aufgezählt und mit dem öffentlichen Schlüssel verschlüsselt wird bis sich zufällig die verschlüsselte Nachricht ergibt, eine systematische Bedrohung dar. Schlüssellängen und Parameter stehen dabei im direkten Zusammenhang wie groß der Suchraum für den Angriff ist und damit wie lang ein erfolgreicher Angriff auf einem gegebenen System dauert. Für asymmetrische Kryptografie werden gegenwärtig 80 bit effektive Schlüssellänge als sicher betrachtet, das heißt für einen erfolgreichen Angriff muss ein Angreifer durchschnittlich mehr als $6*10^{23}$ Verschlüsselungen durchführen. Dies ist ein beachtlicher Aufwand, aber, dank der größeren Effizienz symmetrischer Verfahren, ist es üblich symmetrische Schlüssel zu wählen, die den Suchraum auf das mehr als 10^{14} (100 Billionen) fache anwachsen lassen.

Deswegen spielen Stand der Technik, Schlüssellängen und Parameter eine zentrale Rolle bei der praktischen Nutzung von Kryptografie. Entsprechend erstellen Wissenschaftler und nationale und internationale Behörden regelmäßig Prognosen über die Sicherheit einzelner Verfahren auf und empfehlen maximale Nutzungszeiträume und Übergangsphasen für potentiell unsichere kryptografische Verfahren. Basis dieser Empfehlungen sind (je nach Sicherheitsniveau) immer Annahmen über Angreiferresourcen, z.B. wird oft angenommen, dass ein Angreifer nicht bereit ist einen Supercomputer im Wert von einer Millionen Euro für ein Jahr rechnen zu lassen. Konkret seien hier exemplarisch die BSI Technische Richtlinie TR-02102-1 und die NIST „Recommendation for Key Management, Special Publication 800-57 Part 1 Rev. 5“, die regelmäßig aktualisiert werden, genannt. Des Weiteren liefert auch

[19] Die Komplexität integrierter Schaltkreise verdoppelt sich alle 18-24 Monate bei gleichbleibenden Kosten.

die Forschergemeinschaft innovative Ansätze, die Zukunftssicherheit kryptografischer Verfahren abzuschätzen, [20] die aber unter der kurzen Laufzeit projektfinanzierter Forschung leiden. Die Initative BlueKrypt[21] dokumentiert die diversen Ansätze auf ihrer Website.

In jüngster Zeit fällt in Bezug auf die Zukunftssicherheit kryptografischer Verfahren gehäuft das Schlagwort Sicherheitsbedrohungen durch Quanten-Computing. Grundsätzlich sind weite Teile der klassischen asymmetrischen Kryptografie durch einen hinreichend großen und billigen Quanten-Computer bedroht, da die gängigen Sicherheitsannahmen (wie zum Beispiel: „das Faktorisieren großer Zahlen ist schwer") nicht mehr gültig sind. Als Lösung wird Quantum-Safe-Kryptografie (manchmal weniger zutreffend auch Post-Quanten-Kryptografie) angeboten: moderne kryptografische Verfahren, deren Sicherheitsannahmen auch gelten, wenn dem Angreifer ein Quantencomputer zur Verfügung steht. In Bezug auf Innovation, werden heute fast ausschließlich Quantum-Safe-Algorithmen erforscht. Wie schon im klassischen Angreifermodell, versuchen Wissenschaftler den ökonomischen und innovativen Aufwand abzuschätzen, der nötig wäre, einen praktikablen Quanten-Computer zu realisieren. [22]

III. Sicherheit *durch* Verschlüsselung

a. Grundrechtsrelevanz von Verschlüsselung

Unbestritten ist Verschlüsselung wichtig zum Schutz in die Vertraulichkeit informationstechnischer Systeme. Allerdings ist unklar, ob und in welchem Umfang die Grundrechte eine verfassungsrechtliche Schutzpflicht des Staates zur IT-Sicherheit vermitteln[23] und somit dem Staat aufgeben zur Ausfüllung der Schutzpflicht rechtliche Maßstäbe zu setzen.

Wenn allerdings gesetzliche Regelungen die Möglichkeit zur Verschlüsselung von Kommunikationsinhalten einschränken oder feststeht, dass ein Zugriff trotz Verschlüsselung möglich ist, so werden verschiedene Grundrechte tangiert. Aus deutscher Sicht greift der Zugriff auf verschlüsselte Kommunikationsinhalte in den Schutzbereich des Art. 10 GG ein,[24] dies jedenfalls vom Zeitpunkt des Absendens einer Information bis zu deren Eingang oder Übergabe. Das Recht auf informationelle Selbstbestimmung gewährt subsidiären Schutz, wo Art. 10 GG tatbestandlich nicht zum Tragen kommt,[25] also

---

[20] ECRYPT, ECRYPT II, ECRYPT CSA.

[21] Abrufbar unter https://www.keylength.com/en/ (abgerufen 30.06.2021).

[22] *BSI,* Entwicklungsstand Quantencomputer, zuletzt aktualisiert 2020, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/P283_QC_Studie-V_1_2.pdf (abgerufen 30.06.2021).

[23] *Deusch/Eggendorfer*, in: Taeger/Pohle, Computerrechts-Handbuch, Rn. 388.

[24] Nicht so aber ein Verbot der Verschlüsselung, vgl. *Durner,* in: Maunz/Dürig, Grundgesetz, Art. 10, Rn. 71. Hier wird als Beispiel aufgeführt, dass dem Staat zwar das Öffnen von Briefen durch Art. 10 GG untersagt ist, nicht aber das Verschließen ebendieser zu verbieten.

[25] Ebenda, Rn. 78.

z.b. dort, wo der Übertragungsvorgang bereits beendet war.[26] Entscheidend ist bei der Abgrenzung nicht der Zeitpunkt des staatlichen Eingriffs, sondern der Zeitpunkt des Datenanfalls. Der durch das Telekommunikationsgeheimnis bewirkte Schutz besteht nicht, wenn eine staatliche Stelle die Nutzung eines informationstechnischen Systems als solches überwacht oder die Speichermedien des Systems durchsucht.[27] Das Schutzniveau beider Rechte ist weitgehend identisch.[28]

Verschlüsselung schützt auch die Kommunikationsgrundrechte des Art. 5 GG. Die Gewissheit, dass die Kommunikationsinhalte vor Dritten auf dem Übertragungsweg geschützt sind, gewährt dem sich Äußernden Schutz: Derjenige, der weiß, dass Inhalte geschützt sind, vermag sich anders äußern als derjenige, der jederzeit damit rechnen muss, dass Dritte auf die Inhalte zugreifen. Daneben kann auch der grundrechtliche Schutz der Familie (Art. 6 GG), die Unverletzlichkeit der Wohnung (Art. 13 GG), die Religionsausübungsfreiheit (Art. 4 Abs. 2 GG), etc. betroffen sein. Wird der Schutz nicht bereits durch andere Grundrechte gewährt, so kommt als Auffangrecht das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (sog. IT-Grundrecht) zum Tragen. Letzteres greift vor allem dort, wo Informationen außerhalb eines laufenden Kommunikationsvorgangs ermittelt werden.[29] Welche Grundrechte inwiefern bei einem staatlichen Zugriff auf verschlüsselte Daten betroffen sind, hängt somit unter anderem vom Zeitpunkt des Datenzugriffs und des Inhalts der Daten ab. Auf jeden Fall hat jeglicher Zugriff Grundrechtsrelevanz.

b. Einfachgesetzliche Anforderungen: Datenschutz

Der Unionsgesetzgeber stuft die Verschlüsselung in der DS-GVO als eine der prioritären Sicherheitsmaßnahmen zum Schutz personenbezogener Daten ein.[30]

So benennt Art. 32 Abs. 1 Hs. 2 lit. a DS-GVO mit Pseudonymisierung und Verschlüsselung zwei konkrete technische Maßnahmen zur Sicherheit der Verarbeitung personenbezogener Daten. Ergibt die Datenschutz-Folgenabschätzung ein Risiko für die Datenverarbeitung, so nennt auch Erwägungsgrund 83 DS-GVO die Verschlüsselung als eine Maßnahme zur Eindämmung eines Risikos. Abhängig vom Risikograd kann somit Verschlüsselung zum Schutz personenbezogener Daten gesetzlich geboten sein.

Die Verschlüsselung von Daten kann für den Verantwortlichen auch sonstige Vorteile haben. So kann der Verantwortliche von seiner Verpflichtung, die von einem Datenschutzverstoß betroffenen

[26] Strafprozessuale Konsequenz: Während der Übermittlung auf dem Telekommunikationswege kann eine Überwachung von Kommunikation daher nur nach den Voraussetzungen des § 100a StPO zulässig sein, während außerhalb des Übertragungsvorgangs z.B. E-Mails nach §§ 94, 98 StPO beschlagnahmt werden können.

[27] BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07 und 1 BvR 595/07, NJW 2008, 822, 825.

[28] *Durner,* in: Maunz/Dürig, Grundgesetz, Art. 10, Rn. 79.

[29] Ebenda, Rn. 81.

[30] *Martini,* in: Paal/Pauly, DS-GVO BDSG, Art. 32 DS-GVO, Rn. 34.

Personen zu informieren, gemäß Art. 34 Abs. 3 lit a DS-GVO frei werden. Grund hierfür ist die Annahme, dass der Zugriff auf Inhalte bei Verschlüsselung ohne entsprechenden Schlüssel nicht möglich ist. Kryptografische Verfahren bei der Verschlüsselung müssen den Stand der Technik berücksichtigen.[31]

Das Beispiel der DS-GVO zeigt, dass Verschlüsselung gesetzlich geboten sein kann, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Bedeutung erlangt die Verschlüsselung insbesondere auch bei der Übertragung von personenbezogenen Daten in Drittstaaten außerhalb der EU. Eine solche Datenübermittlung ist zulässig, wenn im Zielstaat ein im Wesentlichen gleichwertiges Schutzniveau existiert.[32] Kapitel V der DS-GVO unterwirft die Übermittlung personenbezogener Daten in Drittstaaten bestimmten Regeln: so kann eine solche Übermittlung u.a. auf der Grundlage eine Angemessenheitsbeschlusses (Art. 45) oder vorbehaltlich geeigneter Garantien erfolgen (Art. 46) z.B. EU Standard-Vertragsklauseln. Bei Letzteren obliegt es den Datenexporteuren zu verifizieren, ob die Standarddatenschutzklauseln in dem Drittland eingehalten werden. Nach Art. 58 Abs. 2 lit. f und j DS-GVO ist die Aufsichtsbehörde verpflichtet, eine Übermittlung personenbezogener Daten auszusetzen oder zu verbieten, wenn sie im Licht aller Umstände der Auffassung ist, dass die Standarddatenschutzklauseln in dem Drittland nicht eingehalten werden oder nicht eingehalten werden können und dass der nach dem Unionsrecht erforderliche Schutz der übermittelten Daten nicht durch andere Mittel gewährleistet werden kann.[33] Angesichts der Tatsache, dass Standarddatenschutzklauseln nicht die Zugriffsbefugnisse staatlicher Stellen im Drittstaat aushebeln können und diese Zugriffe und die Rechtsbehelfe gegen diese nicht europäischen Datenschutzniveau entsprechen müssen, fordert der Europäische Datenschutzausschuss zusätzliche Schutzmaßnahmen beim Datentransfer. Solche „supplementary measures“ können insbesondere technische Maßnahmen wie eine starke E2E-Verschlüsselung sein.[34] E2E-Verschlüsselung wird zuerkannt, eine der wenigen Möglichkeiten zu sein, um den Zugriff auf personenbezogene Daten durch staatliche Stellen zu verhindern.[35]

Somit gewinnt die Verschlüsselung zum Schutz von Daten auch auf sekundärer Ebene an Bedeutung, nämlich z.B. dann, wenn es um die zulässige Gestaltung des internationalen Datentransfers in der Post-Schrems II-Ära geht.

[31] Siehe Art. 32 Abs. 1 S. 1 DS-GVO.

[32] EuGH, Urt. v. 06.10.2015 - C-362/14 (Schrems), ECLI:EU:C:2015:650, Rn. 73.

[33] EuGH, Urt. v. 6.07.2020 – C-311/18 (Schrems II), ECLI:EU:C:2020:559, Rn. 113.

[34] Siehe *EDPB*, Recommendations 01/2020, Annex 2, S. 22.

[35] Ebenda.

c. Einfachgesetzliche Anforderungen: IT-Sicherheit

Der Schutzauftrag zur IT-Sicherheit wird inhaltlich durch den Schutzbereich des IT-Grundrechts definiert. Allerdings finden sich in einfachgesetzlichen Normen, wie z.B. dem BSI-Gesetz keine Anforderungen hinsichtlich Verschlüsselung. Auch die NIS Richtline 2016/48[36], welche für Betreiber wesentlicher Dienste und bestimmte Anbieter digitaler Dienste Sicherheitsanforderungen und Meldepflichten eingeführt hat, benennt als geeignete und verhältnismäßige technische und organisatorische Maßnahmen zum Schutz der Netz- und Informationssysteme nicht die Verschlüsselung. Anders sieht dies jedoch im eingangs erwähnten Vorschlag für eine NIS 2.0 Richtlinie aus dem Dezember 2020 aus. Der NIS 2.0 Vorschlag weist im Hinblick auf Cybergefahren daraufhin, dass die Anbieter von Netz- und Informationssystemen ihre Nutzer auf den Schutz ihrer Kommunikation z.B. durch Verschlüsselung hinweisen sollten.[37] Um die Sicherheit dieser Netzwerke und Dienste zu gewährleisten, soll der Einsatz von Verschlüsselung, insbesondere von E2E-Verschlüsselung gefördert werden, und wo notwendig, verpflichtend für die Anbieter sein - dies im Einklang mit Sicherheitsgrundsätzen und privacy by default und by design.[38]

Gemäß Art. 18 NIS 2.0 Vorschlag, überschrieben mit „Cybersecurity risk management measures", sollen angemessene und verhältnismäßige technische und organisatorische Maßnahmen zur Risikobewältigung unter Berücksichtigung des Stands der Technik ein dem Risiko angemessenes Sicherheitsniveau der Netz- und Informationssysteme gewährleisten. Beispielhaft wird im selben Artikel die Nutzung von Kryptografie und Verschlüsselung als geeignete Maßnahmen genannt.

Allerdings ist auch hier das „Kleingedruckte" nämlich die Erwägungsgründe mitzulesen. Erwägungsgrund 54 stellt klar, dass die Verwendung einer E2E-Verschlüsselung mit den Befugnissen der Mitgliedsstaaten in Einklang gebracht werden sollte, den Schutz ihrer wesentlichen Sicherheitsinteressen und öffentlichen Sicherheit zu gewährleisten und die Ermittlung, Aufdeckung und Verfolgung von Straftaten im Einklang mit Unionsrecht zu ermöglichen. Im Folgenden wird klargestellt, was dies bedeuten soll: es sollen Lösungen für den rechtmäßigen Zugang zu Informationen bei E2E-verschlüsselter Kommunikation geschaffen werden. Somit greift auch der NIS 2.0 Vorschlag den Grundgedanken der Entschließung zur Verschlüsselung auf. Ebenso wird zuerkannt, dass die Effektivität von Verschlüsselung zum Schutz der Privatsphäre und der Sicherheit der Kommunikation aufrecht zu erhalten ist, gleichzeitig soll aber trotz Verschlüsselung Sicherheitsbehörden eine wirksame Reaktionsmöglichkeit zur Kriminalitätsbekämpfung geboten werden.

[36] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 06.07.2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, Abl. L 194/1.

[37] Erwägungsgrund 53 NIS 2.0 Vorschlag.

[38] Erwägungsgrund 54 NIS 2.0 Vorschlag.

IV. Sicherheit trotz Verschlüsselung: Der Zugriff auf verschlüsselte Daten

1. Zugriffsmöglichkeiten auf verschlüsselte Daten

Deutlich wird sowohl aus der Entschließung als auch dem NIS 2.0 Vorschlag, dass staatliche Zugriffsmöglichkeiten auf verschlüsselte Daten kein Wunschdenken mehr sein sollen. Bevor die gesetzlichen Voraussetzungen hierfür geschaffen werden können, bedarf es aber grundsätzlich einer Auseinandersetzung mit der Frage, wie denn ein solcher Zugriff technisch möglich sein könnte.

Wie zuvor erörtert bedeutet E2E-Verschlüsselung, dass ausschließlich die Kommunikationspartner mitlesen können und gerade niemand Drittes. Dieses Prinzip muss gebrochen werden, wenn Dritten, und hierzu zählen Sicherheits- und Ermittlungsbehörden, Zugriff gewährt werden soll. Dabei kann man zwei grundsätzliche Zugriffswege unterscheiden: (i) die Umgehung des Schutzmechanismuses oder (ii) den Bruch des Schutzmechanismuses. Bei (i) wird entweder das Endgerät des Senders oder des Empfängers so manipuliert, dass der Klartext der Nachricht oder entsprechendes Schlüsselmaterial abgegriffen wird und damit Dritten zur Verfügung steht; dies gleicht den unterschiedlichen Varianten der Quellen-TKÜ oder Keyescrow-Systemen wie dem Clipper Chip[39]. Angesetzt wird hier schon außerhalb des Übertragungsvorgangs. Im Gegensatz hierzu wird bei (ii) davon ausgegangen, dass z.B. Ermittlungsbehörden über Ressourcen oder Wissen verfügen, die es erlauben Kryptogramme zu öffnen, so z.B. wie zu Zeiten der Exportbeschränkungen von Produkten mit kryptografischen Mechanismen und damit einhergehender Einschränkung der erlaubten Schlüssellänge, sodass für entsprechend ausgestattete Behörden Brute-Force-Angriffe möglich waren.

Dass die Zugriffsmechanismen begrenzt sind, zeigt auch ein im Dezember 2020 geleaktes Diskussionspapier der Europäischen Kommission, welches sich mit technischen Lösungen zur Aufspürung von kinderpornographischen Inhalten in E2E-verschlüsselter Kommunikation befasst.[40] Dieses Papier zeigt verschiedene Verfahren des Zugangs auf, wobei hier nach geräte-, server- und verschlüsselungsbezogenen Ansätzen unterschieden wird. Die gerätebezogenen Ansätze sind dabei nicht viel anderes als die zuvor genannte Quellen-TKÜ. Bei den aufgeführten Lösungen ist zudem von Bedeutung, dass es primär um einen Abgleich der Hashwerte der übermittelten Daten mit einer Datenbank bekannt illegaler Inhalte geht. Ziel der Maßnahme ist mithin das Auffinden von Kopien bereits bekannter Inhalte und nicht um einen Zugriff auf verschlüsselte Kommunikation mit unbekanntem Inhalt.[41] Bei solchen

[39] Der Clipper Chip war ein Versuch der US-Regierung in den 90er Jahren ein client-seitiges Keyescrow-System staatlich zu mandatieren. Computerhersteller sollten dazu verpflichtet werden, den sog. Clipper Chip in Telefone, Faxgeräte und Computer einzubauen, welcher Datenaustausch veschlüsseln sollte. Zwei Teilschlüssel sollten bei verschiedenen Behörden hinterlegt werden und auf richterlicher Anordnung zum Zugang freigegeben werden. Zum Hintergrund siehe *Levy*, Battle of the Clipper Chip, v. 12.06.1994, https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html (abgerufen 30.06.2021).

[40] Technical solutions to detect child sexual abuse in end-to-end encrypted communications, abrufbar unter https://www.politico.eu/wp-content/uploads/2020/09/SKM_C45820090717470-1_new.pdf (abgerufen 30.06.2021).

[41] Wenn auch schon die Möglichkeit des Rückschlusses auf den Inhalt übermittelter Daten als Aufweichen von echter E2E-Verschlüsselung betrachtet wird, so *Figas/Olbrich,* Ende-zu-ende-Verschlüsselung mit Hintertür –

Datenbankabgleichen über das Endgerät des Nutzers ist zu berücksichtigen, dass die für die Überwachung nötigen Berechnungen (von teils erheblichem Aufwand) unter Verwendung der Nutzerresourcen durchgeführt werden und dies einen Schwachpunkt bei der Verdecktheit der Maßnahme darstellt. Deutlich macht das Dokument, dass selbst bei einem Datenbankabgleich von Inhalten verschlüsselungsbezogene Ansätze aktuell als kaum machbar eingestuft werden.[42] Mithin ist vollkommen offen, wie ein Zugriff auf verschlüsselte Daten außerhalb bereits existierender Verfahren ablaufen soll.

2. Rechtliche Fragestellungen im Zusammenhang mit behördlichem Zugriff

Auch wenn stets darauf hingewiesen wird, dass die Zugriffsmöglichkeiten im Einklang mit einem ordnungsgemäßen Verfahren und anderen Garantien sowie Grundrechten stehen sollen, so muss die Frage gestellt werden, von welchem Zugriff man hier spricht. Aus den Diskussionen um den Zugang zu verschlüsselten Daten wird deutlich, dass es hierbei nicht um den Einsatz von Spionagesoftware geht, welche beispielsweise Daten schon im Rechner des Absenders abgreift, noch ehe diese für den Transport verschlüsselt werden. Dies wäre, wie zuvor ausgeführt, nichts anderes als Quellen-TKÜ als technische Sonderform der TKÜ, welche z.B. für Ermittlungsbehörden im Strafverfahren in Deutschland in § 100a Abs. 1 S. 2 und 3 StPO geregelt ist.

Vielmehr geht es in der Entschließung um den Zugriff auf bereits verschlüsselte Inhalte. Aus Metadaten zu verschlüsselten Chats lassen sich Erkenntnisse ableiten, welche den Inhalt für Ermittlungs- oder Sicherheitsbehörden interessant machen. Regelmäßig werden die Behörden im Besitz der zugehörigen Kryptogramme sein, auf deren Inhalte aber kein Zugriff möglich ist. Dies wirft die Frage auf, ob der europäische Gesetzgeber zur Realisierung des Zugangs letztlich Diensteanbieter verpflichten müsste, Schlüssel zu speichern. Ein solches Speichern wäre aber technisch nur bei der Methode der Kanalverschlüsselung möglich, da bei der E2E-Verschlüsselung sich die Session-Keys nur in Händen der Kommunikationspartner befinden, die Diensteanbieter so keinen Zugriff auf diese Schlüssel haben.

Bei einer Verpflichtung zur Speicherung von Session-Keys bei der Kanalverschlüsselung wäre zu differenzieren, ob Session-Keys generell gespeichert werden sollen oder ob bspw. nach einer behördlichen Anordnung neu generierte Session-Keys durch die Diensteanbieter übermittelt werden sollen, um Zugang zu Echtzeit-Kommunikation gewähren. So wäre es den Behörden möglich Kenntnis der Kommunikationsinhalte während des Übermittlungsvorgangs zu erhalten wie es schon bei der klassischen Echtzeit-Überwachung von Telekommunikation der Fall ist.

Eine generelle Speicherpflicht stößt auf weitreichende Bedenken, da sich hier dieselben Problemfelder wie bei der anlasslosen Vorratsdatenspeicherung durch Internetdiensteanbieter auftuen; dies allerdings mit dem Unterschied, dass die Vorratsdatenspeicherung nunmehr sogar erweitert werden würde auf Kommunikationsinhalte: denn die Speicherung von Schlüsseln bedeutet nichts anders als

die Pläne der EU, v. 02.03.2021, https://www.boxcryptor.com/de/blog/post/e2ee-weakening-eu/, zuletzt (abgerufen 28.06.2021).

[42] Technical solutions to detect child sexual abuse in end-to-end encrypted communications, S. 20.

die Speicherung von Inhalten. Anknüpfend an seine Grundsatzentscheidung[43] zur Vorratsdatenspeicherung,[44] hat der EuGH zuletzt im Oktober 2020[45] sowie März 2021[46] klargestellt, dass zwar eine anlasslose Vorratsdatenspeicherung und -sammlung unzulässig ist, es von diesem grundsätzlichen Verbot aber Ausnahmen geben kann. So können Mitgliedsstaaten durchaus eine zeitlich befristete Vorratsdatenspeicherung einführen, wenn eine ernsthafte Bedrohung der nationalen Sicherheit vorliegt, die sich als tatsächliche und gegenwärtige oder vorhersehbare Gefahr erweise oder der Bekämpfung schwerer Straftaten und der Abwehr schwerwiegender Bedrohungen der öffentlichen Sicherheit diene.

Die Vorratsdatenspeicherung kann somit nur in engen Grenzen angeordnet werden, ist aber nicht in Gänze unzulässig. Auf eine mögliche Verpflichtung von Diensteanbietern zur Speicherung von Schlüsseln übertragen bedeutet dies zunächst, dass eine generelle Verpflichtung zur Speicherung unzulässig wäre. Aufgrund der Schwere des Eingriffs in Grundrechte könnte durch einen Mitgliedsstaat allerdings anlassbezogen eine solche Verpflichtung eingeführt werden, was bedeutet, dass grundsätzlich nur auf Daten ab einer Überwachungsanordnung zugegriffen werden könnte. Jedenfalls ist jetzt schon abzusehen, dass der Rahmen für eine anlassbezogene Speicherung ebenfalls sehr eng gesteckt werden müsste.

Wie bereits angerissen funktioniert dieser Ansatz bei E2E-Verschlüsselung nicht, da sich hier die Session-Keys allein in Händen der Kommunikationspartner befinden. Ein Zugriff auf E2E-verschlüsselte Inhalte ist nur möglich über eine Schwächung der zugrundeliegenden Kryptografie. Es wird davon ausgegangen, dass aktuelle Standards z.B. vom BND nicht zu durchbrechen sind.[47] Anders wäre dies, wenn eine Einschränkung der Verschlüsselungsverfahren durch den Gesetzgeber erfolgen würde, man also die Diensteanbieter verpflichten würde, die E2E-Verschlüsselungsstärke einzuschränken oder Keyescrow-Mechanismen verpflichtend zu implementieren. Dies setzt weiter voraus, dass die angebotenen Dienste auf proprietären Protokollen beruhen, so dass der Diensteanbieter Kontrolle über die verwendete Client-Software hat; in einem offenen System stünde es dem Nutzer sonst zur Wahl

[43] EuGH, Urt. v. 21.12.2016 – Verbundene Rechtssachen C-203/15 und C-698/15 (Tele2 Sverige et al), ECLI:EU:C2016:970.

[44] Mitgliedsstaaten dürfen u.a. Rechtsvorschriften die zur Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten Zugang zu den von Betreibern elektronischer Kommunikationsdiensten gespeicherten Verkehrs- und Standortdaten gewähren und somit die in der Richtlinie vorgesehenen Rechte und Pflichten, namentlich die Pflicht zur Gewährleistung der Vertraulichkeit der Kommunikation und der Verkehrsdaten beschränken, nur erlassen, wenn die Rechtsvorschriften die allgemeinen Grundsätze des Unionsrechts beachten

[45] EuGH, Urt. v. 06.10.2020 – Verbundene Rechtssachen C-511/18, C-512/18 und C-520/18 (La Quadrature du Net et al), ECLI:EU:C:2020:791, Rn. 166-169, sowie Urt. v. 06.10.2020 - C-623/17 (Privacy International), ECLI:EU:C:2020:790.

[46] EuGH, Urt. v. 02.03.2021 - C-746/18 (Strafverfahren gegen H.K.), ECLI:EU:C:2021:152.

[47] So z.B. *Hoppenstedt/Wiedmann-Schmidt,* So überwacht der BND das Internet, v. 19.05.2020, https://www.spiegel.de/netzwelt/netzpolitik/bundesnachrichtendienst-so-ueberwacht-der-bnd-das-internet-a-216ebe9a-6f22-4883-b1c9-ac5d1442497a (abgerufen 30.06.2021).

eigene Clientsoftware ohne eingeschränkte Kryptografie oder Keyescrow zu verwenden. Im Falle der eingeschränkten Kryptografie würde es den Ermittlungs- und Sicherheitsbehörden möglich gemacht sich bspw. durch eine Brute-Force-Attacke Zugang zu verschlüsselten Inhalten zu schaffen. Dieser Ansatz entspricht dem Ansatz der USA im Zeitalter der Exportbeschränkungen und somit zu Anfang der Crypto-Wars. Eine solche Schwächung der Verschlüsselung birgt allerdings auch zwangsläufig das Risiko, dass nicht nur den genannten Behörden das „Hacking" erleichtert wird. Beide Methoden würden auch bei der Kanalverschlüsselung eine Speicherung von Session-Keys obsolet machen.

Die Entschließung zur Verschlüsselung lässt offen, wann, wie und wo der Zugriff erfolgen soll, gerade weil es dem Wortlaut der Entschließung entsprechend noch „keine Patentlösung"[48] gibt. Grundlegende Idee ist primär, die Diensteanbieter mit in die Pflicht zu nehmen. Dies lässt natürlich Raum für Spekulationen und läuft aufgrund der Begrenztheit der aufgezeigten technischen Möglichkeiten bei der E2E-Verschlüsselung offensichtlich auf eine staatliche angeordnete Schwächung von Kryptografie hinaus.

V. Ausblick

Verschlüsselung lebt davon, dass sie nicht gebrochen werden soll und ist nicht nur ein Instrumentarium für Kriminelle, um ihre Kommunikation geheim zu halten. Vielmehr durchzieht Verschlüsselung alle Lebensbereiche und gewinnt gerade mit einem gestiegenen Datenschutzniveau in der EU immer mehr an Bedeutung, u.a. im Rahmen der Datenübermittlung in Drittstaaten. Hier sollen die Daten gerade vor dem Zugriff staatlicher ausländischer Stellen wie der NSA geschützt sein. Der Einsatz von starken und verlässlichen Verfahren der Kryptografie ist essentiell für die Netz- und Informationssicherheit.

Allerdings zeigt der nun eingeschlagene Weg verschiedener Organe der EU ganz klar auf, dass politisch nicht länger hingenommen wird, dass Ermittlungs- und Sicherheitsbehörden nicht mit den ihnen zur Verfügung stehenden Mitteln auf verschlüsselte Kommunikationsinhalte zugreifen können.

Kritiker der Entschließung sprechen oftmals von „Hintertüren" und „Nachschlüsseln",[49] die der europäische Gesetzgeber einbauen wolle. Wie technisch „Hintertüren" implementiert werden könnten, bleibt dabei offen. Nachschlüssel, was nicht mehr bedeuten kann also eine Speicherpflicht, sind angesichts der Rspr. zur Vorratsdatenspeicherung als generelle Speicherpflicht wohl nicht durchsetzbar. Somit besteht die Gefahr der Verpflichtung zu Nachschlüsseln, die Türen öffnen, wo eigentlich keine sein sollten und zum Missbrauch einladen, nicht im prognostizierten Maße.

Ein technisch machbarer Weg des Zugriffs auf E2E-verschlüsselte Daten stellt wie zuvor aufgezeigt die Aufweichung von Verschlüsselung dar. Ein Absenken des Niveaus der Kryptografie bedeutet aber

[48] *Rat der Europäischen Union,* Entschließung, 13084/1/20 REV 1, S. 5.

[49] Z.B. *Kurz*, Von jahrelangen Debatten über Hintertüren unbeeindruckt, v. 09.11.2020, https://netzpolitik.org/2020/it-sicherheit-von-jahrelangen-debatten-ueber-hintertueren-unbeeindruckt/ (abgerufen 30.06.2021),

auch, dass Netzwerke generell unsicher werden – denn die Möglichkeit des Brechens der Kryptografie kann nicht lokal auf Ermittlungs- und Sicherheitsbehörden in der EU beschränkt werden. Ebenso wie die zuvor erwähnte Hintertür lädt eine Schwächung der Kryptografie zum Missbrauch ein. Die größte Gefahr ist der Zugriff unberechtigter Dritter und damit wird auch dieser wichtige Aspekt der IT-Sicherheit konterkariert. Letztlich wird auch die offensichtlich anvisierte Schwächung der Verschlüsselung und somit aktive Gefährdung der Schutz-Trias informationstechnischer Systeme diejenigen, auf die sie abzielt, am wenigsten treffen:

Kriminelle können ihre eigenen verschlüsselten Netzwerke aufbauen oder auf sich nicht dem Recht der EU unterwerfende Unternehmen ausweichen.

Der Fall des Kommunikationsdienstes ANOM hat kürzlich nochmals deutlich gemacht, dass der Faktor Mensch selbst eine vielversprechende Schwachstelle bleibt: Eine vom FBI in Zusammenarbeit mit australischen Ermittlungsbehörden aufgesetzte App zur verschlüsselten Kommunikation erfreute sich in der organisierten Kriminalität großer Beliebtheit, wobei keinem der Nutzer bewusst war, dass die Ermittlungsbehörden mitlasen.[50] Ganz ähnlich lasen die Ermittlungsbehörden auch eine ganze Weile beim als besonders abhörsicher beworbenen niederländischen Krypto-Kommunikationsdienst EncroChat mit, nachdem auf in Frankreich befindlichen Servern des Unternehmens durch französische Ermittlungsbehörden ein Trojaner aufgespielt worden war. Auf diese Weise wurden monatelang mehr als 32.000 Endgeräte in über 120 Ländern überwacht – darunter auch solche auf deutschem Hoheitsgebiet; letztlich wurden mehr als 100 Millionen Nachrichten mitgelesen.[51] Zumindest in Deutschland wird die Verwendung und Verwertung der gewonnenen Daten kontrovers diskutiert.[52] Die ersten Gerichte kommen inzwischen zu dem Ergebnis, dass bezüglich der Daten ein Beweisverwertungsverbot besteht, da die Datenabschöpfung bei den EncroChat-Nutzern durch ausländische Ermittlungsbehörden auf deutschem Staatsgebiet unter Missachtung individualschützender Rechtshilfevorschriften erfolgte und dies auch ohne den erforderlichen konkreten Tatverdacht.[53]

Angesichts der Probleme, die sich bei der Zulässigkeit der Verwertung im Strafprozess stellen, erscheint es geradezu paradox, dass sich nun auf politischer Ebene mit augenscheinlich darüber hinaus-

[50] *Flade/Strunz,* Polizei trickste Kriminelle mit App aus, v. 09.06.2021, https://www.tagesschau.de/investigativ/organisierte-kriminalitaet-anom-101.html (abgerufen 30.06.2021).

[51] *Derin/Singelnstein,* NStZ 2021, 449.

[52] *Derin/Singelnstein,* NStZ 2021, 449ff; *Pauli*, NStZ 2021, 146ff; *Sommer*, StV Spezial 2021, 67 . Für eine Verwertbarkeit: OLG Hamburg (1. Strafsenat), Beschluss vom 29.01.2021 – 1 Ws 2/21; OLG Rostock (1. Strafsenat), Beschluss vom 11.05.2021 – 20 Ws 121/21; OLG Schleswig, Beschluss vom 29.04.2021 – 2 Ws 47/21; gegen eine Verwertbarkeit: LG Berlin, Beschluss vom 01.07.2021 – (525 KLs) 254 Js 592/20 (10/21) (inzwischen aufgehoben durch das KG Berlin, Beschluss vom 30.08.2021 – 2 Ws 79/21).

[53] LG Berlin, Beschluss vom 01.07.2021 – (525 KLs) 254 Js 592/20 (10/21). Konkret war in diesem Fall der Eingriff in das T-Grundrecht und Telekommunikationsgeheimnis nicht gerechtfertigt, da die Daten nach Auffassung des Gerichts unter Verstoß gegen Art. 31 RL 2014/41/EU über die Europäische Ermittlungsanordnung (i.V.m. § 91g Abs 6 IRG) erlangt worden seien und der bei Anordnung und Durchführung der Maßnahme der nach §§ 100a, 100b StPO erforderliche qualifizierte Tatverdacht nicht vorlag.

gehendem Zugriff, beschäftigt wird. Auch zeigt der EncroChat-Fall, dass es in manchen Mitgliedsstaaten schon sehr weitreichende Zugriffsmöglichkeiten gibt, nämlich dann, wenn allein aufgrund der Vermutung, dass ein Kommunikationsdienst von vielen kriminellen Akteuren genutzt wird ohne individualisierten Tatverdacht, eine verdeckte Ermittlungsmaßnahme eingeleitet werden kann. Hier wird schon gezielt gegen geschützte, sichere Kommunikation vorgegangen – wenn es dies ist, was die politischen Akteure sich wünschen, so ist schon jetzt absehbar, dass dies jedenfalls als strafprozessuale Maßnahme aufgrund der Eingriffsintensität in Grundrechte in Deutschland rechtlich nicht möglich sein wird.

Literatur

Derin/Singelnstein, Verwendung und Verwertung von Daten aus massenhaften Eingriffen in informationstechnische Systeme aus dem Ausland (Encrochat), NStZ 2021, 449-454.

European Data Protection Board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (10.11.2020).

Europäische Kommission, A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond, COM(2020) 795 final.

Europäische Kommission, Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union. Repealing Directive (EU) 2016/1148, COM(2020) 823 final.

Hagemeier, Heike: Kryptografie – heute und zukünftig, DuD 2019, 631-635.

Maunz, Theodor/Dürig, Günter/ u.a. (Hrsg.): Grundgesetz, Kommentar, Loseblattsammlung München, Stand: Oktober 2020 (93. EL).

Paal, Boris/Pauly, Daniel (Hrsg.): Datenschutz-Grundverordnung Bundesdatenschutzgesetz (DS-GVO BDSG), Kommentar, 3. Aufl. München 2021.

Pauli, Zur Verwertbarkeit der Erkenntnisse ausländischer Ermittlungsbehörden – EncroChat, NStZ 2021, 146-149.

Rat der Europäischen Union, Entschließung des Rates zur Verschlüsselung – Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung, 13084/1/20 REV 1.

Sommer, EncroChat – ein Kapitel in der Geschichte des zerbröselnden europäischen Strafprozesses, StV Spezial 2021, 67.

Taeger, Jürgen/Pohle, Jan (Hrsg.): Computerrechts-Handbuch, Informationstechnologie in der Rechts- und Wirtschaftspraxis, Loseblattsammlung München, Stand: Februar 2021 (36. EL).

The research for this article was funded by the Luxembourg National Research Fund (FNR) C18/IS/12639666/EnCaViBS/Cole, https://www.fnr.lu/projects/the-eu-nis-directive-enhancing-cybersecurity-across-vital-business-sectors-encavibs/.