Bundeskriminalamt

Anhörung des Vizepräsidenten des Bundeskriminalamtes

Peter Henzler

im Ausschuss für Recht und Verbraucherschutz
des Deutschen Bundestages am 31. Mai 2017

zum Entwurf eines Gesetzes zur Änderung
des Strafgesetzbuchs, des Jugendgerichtsgesetzes,
der Strafprozessordnung und weiterer Gesetze

hier: zum Thema Quellen-TKÜ und Online-Durchsuchung in der StPO gem. Formulierungshilfe der BReg

(Drs. 18/11272, *18(6)/334 Formulierungshilfe*)

Telekommunikation ist der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen (§ 3 Nr. 22 TKG). Durch die Entwicklungen im Bereich der Informations- und Kommunikationstechnologien, insbesondere in den Bereichen Anonymisierung und Kryptierung, läuft die „klassische“ Telekommunikationsüberwachung durch Ermittlungsbehörden im Rahmen ihrer gesetzlichen Befugnisse mittels Ausleitung der Daten durch den Telekommunikationsanbieter zunehmend ins Leere. Das liegt daran, dass der Ursprung der Telekommunikation in Form des genutzten physikalischen Anschlusses bzw. des Urhebers häufig nicht mehr ermittelt werden kann (Folge der Anonymisierung) und ein zunehmend hoher Anteil der Telekommunikation nicht mehr überwach- bzw. auswertbar ist (Folge der Verschlüsselung).

Dabei ist darauf hinzuweisen, dass verschlüsselte Kommunikation mittlerweile in vielen Fällen keine willentliche Nutzung einer Kryptierungssoftware voraussetzt, sondern zunehmend von den gängigen elektronischen Kommunikationsanbietern wie z. B. deutschen E-Mail-Anbietern als technischer Standard verwendet wird. Darüber hinaus integrieren die Anbieter der gängigsten (mobilen) IuK-Plattformen (z.B. Apple, Google) inzwischen Ende-zu-Ende-Verschlüsselungsverfahren in ihre Systeme, die die Kommunikation automatisch verschlüsseln. Insofern ist inzwischen ein signifikanter Teil der Kommunikation über allgemein gebräuchliche Anbieter aufgrund ihrer Verschlüsselung als nicht mehr auswertbar durch die Ermittlungsbehörden anzusehen.

Selbst wenn nicht bereits die Verschlüsselung die Überwachbarkeit der Kommunikation verhindert, ist dies häufig bei mobiler Nutzung von IT-Systemen der Fall, wenn sich der Nutzer nicht über den ihm zugeordneten Mobilfunk- oder Festnetzanschluss, sondern über freie WLAN anonym ins Internet einwählt (sog. nomadische Nutzung). Auch in diesen Fällen kann nur eine Quellen-TKÜ die Überwachung der Kommunikation gewährleisten.

Jenseits der Konstellation der Überwachung laufender kryptierter Telekommunikation stellt die Kryptierung bzw. Verschlüsselung von Daten seitens der Täter (z. B. bei Verschlüsselung eines Bereichs der Festplatte eines Computers oder einer externen Festplatte) die Sicherheitsbehörden zunehmend vor technische Probleme. Um im Einzelfall verschlüsselte Daten als Spurenansätze bzw. Beweismittel auswerten zu können, wäre mangels anderer Möglichkeiten das Ermittlungsinstrument der Online-Durchsuchung erfolgversprechend. Insbesondere bei schweren Delikten, Serientaten, Strukturermittlungen bei Organisierter Kriminalität und Terrorismus sind diese Daten aber aus polizeilicher Sicht unerlässlich.

Leider fehlen entsprechende Befugnisnormen für die Quellen-TKÜ und die Onlinedurchsuchung in der StPO bisher.

Dabei ist darauf hinzuweisen, dass das BVerfG in seiner Entscheidung zur Online-Durchsuchung (im LfV-Gesetz NRW) schon 2008 deutlich gemacht hat, dass eine Online-Durchsuchung in der StPO zur Verfolgung von schweren Straftaten durchaus denkbar wäre. In seiner Entscheidung 2016 zum BKAG hat das BVerfG zudem die

Wertigkeit von Wohnraumüberwachung und Online-Durchsuchung (im Gefahrenabwehrrecht) bezüglich der Eingriffstiefe (in unterschiedliche Grundrechte) auf eine Stufe gestellt. Zudem hat es in dieser Entscheidung grundsätzlich die im BKAG zur Prüfung angestandenen Befugnisnormen im Aufgabenfeld des BKA nach § 4a BKAG im Kern als verfassungskonform anerkannt.

Die nun vorgesehenen Änderungen in der StPO stellen zweifellos einen deutlichen Mehrwert für eine effiziente wie effektive Strafverfolgung aus Sicht des Bundeskriminalamtes dar. Bei der sogenannten Quellen-TKÜ wird die gebotene Rechts- und Handlungssicherheit geschaffen, bei der Online-Durchsuchung wird der seit Jahren vom Bundeskriminalamt begründeten Forderung zur Schaffung einer solchen konstitutiven Regelung – über das BKAG hinaus – auch zur Strafverfolgung nachgekommen.

Im Folgenden möchte ich noch einmal die Hauptargumente für den Bedarf an den geforderten Regelungen sowohl in rechtlicher als auch in polizeifachlicher Hinsicht darstellen:

1. Quellen-TKÜ

a. Polizeifachlicher Bedarf

Telekommunikationsüberwachung ist ein unverzichtbarer Bestandteil der Ermittlungsarbeit. Der Erfolgswert dieser Maßnahme wird bedroht durch die Nutzung kryptierter Telekommunikationswege und -dienste, die mit einer konventionellen TKÜ-Maßnahme nicht überwachbar sind. Damit durch die Nutzung von Kommunikationsverschlüsselung kein strafverfolgungsfreier Raum entsteht, benötigen die Ermittlungsbehörden Ausgleichsmaßnahmen, um die wachsenden Lücken bei der klassischen Telekommunikationsüberwachung zu schließen. Hier muss das derzeit erfolgversprechendste Ermittlungsinstrument, die Quellen-TKÜ, genutzt werden. Dieses verfolgt den Lösungsansatz, die Kommunikationsdaten vor der Verschlüsselung bzw. nach Entschlüsselung aufzuzeichnen und an die Ermittlungsbehörden zu übertragen (sog. Quellen-Telekommunikationsüberwachung). Die Verschlüsselung kann so umgangen werden. Hierzu ist erforderlich, eine spezielle Software auf das zur Kommunikation genutzte Endgerät aufzubringen. Die verdeckte Aufbringung der Software auf das Endgerät stellt für die Sicherheitsbehörden eine besondere technische Herausforderung dar und ist regelmäßig mit hohem Aufwand verbunden.

Hinsichtlich des polizeifachlichen Bedarfs an der Überwachung und Auswertung verschlüsselter Telekommunikationsinhalte wird auf die Ergebnisse einer vom BKA durchgeführten Bund-/Ländererhebung hingewiesen. Im Erhebungszeitraum 01.01.2012 bis 31.12.2013 wurden knapp 300 Sachverhalte mit dem Ergebnis ausgewertet, dass die nicht auswertbaren Telekommunikationsinhalte zu teils erheblichen Überwachungslücken führten und damit zu unvollständigen Ermittlungsergebnissen, einer mangelhaften Beweislage oder gar zum Scheitern der Ermittlungen. Insbesondere die Aufklärung der Kommunikations- und Organisationsstrukturen der Tatverdächtigen, sowie Planung und Durchführung von (Begleit-) Ermittlungsmaßnahmen werden in erheblichem Maße erschwert. Gleichzeitig gehen Versuche, die Ermittlungsdefizite auch nur im Ansatz auszugleichen, in der Regel mit deutlich intensiveren Grundrechtseingriffen bei den Betroffenen einher.

Keineswegs verwundert daher, dass sich dieser Trend fortsetzt. Im Rahmen einer Datenanalyse bezogen auf die im BKA durchgeführten TKÜ-Maßnahmen mit IP-Datenverkehr aus dem Jahr 2016 zeichnet sich aktuell folgendes Bild – allein bezogen auf die Kommunikation per Messengerdiensten ab:
In 67% der im BKA durchgeführten TKÜ-Maßnahmen mit IP-Datenverkehr war Messengerkommunikation enthalten. Die am häufigsten genutzten Messenger waren Facebook-Messenger (65%), WhatsApp (56%) und Viber (28%).

b. Rechtsrahmen und Bedarf an der Schaffung einer Befugnisnorm für die Quellen-TKÜ in der StPO

Das BKA begrüßt ausdrücklich, dass die Quellen-TKÜ nun (klarstellend) in der StPO geregelt werden soll, die tatbestandlichen Voraussetzungen (insbesondere Straftaten-Katalog) der „normalen" TKÜ entsprechen und die Schutzregelungen sich an die Regelung in §§ 4a, 20l BKAG anlehnen.
Bisher ist eine explizite Befugnisnorm zur Durchführung von Quellen-TKÜ in der StPO nicht enthalten. Im Rahmen der präventivpolizeilichen Aufgaben des BKA zur Abwehr von Gefahren des internationalen Terrorismus ist die Quellen-TKÜ, neben der TKÜ, für das BKA jedoch bereits explizit in § 20l Abs. 2 BKAG als zulässige Eingriffsmaßnahme vorgesehen.
Dabei ist es aus Sicht des BKA nicht ausreichend, diese Software ausschließlich im Bereich der Gefahrenabwehr zum Einsatz zu bringen. Vielmehr soll die mit hohem personellem und finanziellem Aufwand entwickelte Software auch bei der Strafverfolgung als Einsatzmittel zur Verfügung stehen. Um aber auch für Ermittlungsverfahren das Instrument der Quellen-TKÜ als Option zu erhalten und aus Gründen der einheitlichen Handlungs- und Rechtssicherheit in Bund und Ländern sieht es das BKA als geboten an, eine klarstellende Regelung in die StPO aufzunehmen.

Diese Forderung hatte auch Eingang in den Koalitionsvertrag für die 18. Wahlperiode gefunden. Zudem wurde mit Beschluss des 69. Deutschen Juristentages vom 20.09.2012 der fachliche Bedarf bestätigt und der Gesetzgeber aufgefordert, eine (klarstellende) Regelung zum Einsatz von Quellen-TKÜ im Rahmen der Strafverfolgung zu schaffen.

2. Online-Durchsuchung

a. Polizeifachlicher Bedarf

Neben kryptierter Telekommunikation (siehe Quellen-TKÜ) stellt die Kryptierung bzw. Verschlüsselung von Daten durch die Täter (z. B. bei Verschlüsselung eines Bereichs der Festplatte eines Computers oder einer externen Festplatte) sowie die von den Herstellern von Hardware zunehmend ab Werk voreingestellte Verschlüsselung (insbesondere von Handys) als „Standard-Sicherheitsfeature“ die Sicherheitsbehörden zunehmend vor technische Probleme. Um im Einzelfall verschlüsselte Daten als Spurenansätze bzw. Beweismittel auswerten zu können, wäre mangels anderer Möglichkeiten auch hier das Ermittlungsinstrument der Online-Durchsuchung erfolgversprechend. Jedoch fehlt eine Befugnisnorm in der StPO. In bestimmten Fallkonstellationen können im Ermittlungsverfahren mit einer Online-Durchsuchung Dateien erlangt werden, die auf dem Zielsystem nur für kurze Zeit klartextlich vorliegen, oder es können mittels Keylogging oder Screen-/Applicationshots Passwörter und Zugangscodes erlangt werden, die bei einer Beschlagnahme von verschlüsselten Datenträgern eine spätere Datenauswertung überhaupt erst ermöglichen.

Neben den klassischen Konstellationen der Online-Durchsuchung, die auf dem Rechner eines Endkunden stattfindet, ist auch der Zugriff auf Serversysteme oder auf mobile Devices (Smartphones/Tablets) notwendig. Zudem sollte es neben der reinen Erhebung von Daten auf dem Rechner möglich sein, den RAM des durchsuchten Gerätes auszulesen/zu sichern.

Fallbeispiele:

Folgende Fälle aus Ermittlungsverfahren und sonstige typische Konstellationen werden zur Veranschaulichung der Problematik beispielhaft aufgeführt:

- Terrorismus

Erkenntnisse über die Ausreise deutscher Staatsangehöriger im Frühjahr 2012 mit dem Ziel, sich im nordafrikanischen Raum für die Teilnahme am gewaltsamen Jihad terroristisch ausbilden zu lassen, führten im September 2012 zur Einleitung eines Ermittlungsverfahrens des GBA wegen des Verdachts der Unterstützung einer terroristischen Vereinigung im Ausland gemäß §§ 129a, 129b StGB gegen zunächst fünf Beschuldigte. Derzeit werden beim BKA dreizehn Ermittlungsverfahren und zwei Strafverfahren

wegen des Verdachts der Unterstützung einer terroristischen Vereinigung im Ausland sowie wegen des Verdachts der Mitgliedschaft in einer terroristischen Vereinigung im Ausland (AQM, ISIG, JaN, Junud Al Sham) mit insgesamt sechszehn Beschuldigten und fünf Angeklagten im Auftrag des GBA bearbeitet. Die Beschuldigten/Angeklagten stehen im Verdacht, sich an Kampfhandlungen radikaler Islamisten gegen das Assad-Regime in Syrien zu beteiligen, beteiligt zu haben oder die jihadistischen Kämpfer im Ausland oder aus Deutschland heraus zu unterstützen. Es wurden über 200 TKÜ-Maßnahmen geschaltet. Neben Mobiltelefonen, DSL- und Festnetzanschlüssen sowie E-Mail Adressen wurden auch zahlreiche Auslandskopf-und IMEI-Überwachungen durchgeführt. Etwa 10% der Maßnahmen sind derzeit noch aktiv. Trotz des Maßnahmenpakets kann weiterhin ein Großteil der geführten Kommunikation nicht festgestellt werden, da die Betroffenen regelmäßig bewusst kryptierte Kommunikationswege nutzen (z.B. Telegram, WhatsApp, Ask.fm, Skype, Tango), die technisch und/oder rechtlich nicht überwacht werden können. Regelmäßige verfahrensrelevante Kommunikation wird verbal oder schriftlich bewusst über die genannten verschlüsselten Dienste geführt. Konkrete Verabredungen, um auf verschlüsselte Kommunikationswege auszuweichen,
können regelmäßig auf den vorhandenen TKÜ-Maßnahmen festgestellt werden. Da in hiesigen Ermittlungsverfahren vor allem schriftliche Kommunikation über kryptierte Kommunikationswege geführt wird, würde die Möglichkeit der Online-Durchsuchung ein profundes Ermittlungsinstrument darstellen (Stichwort: Screenshots von geführter schriftlicher verschlüsselter Kommunikation), um an verschlüsselte und verfahrensrelevante Kommunikationsinhalte zu gelangen, die eine hohe Verfahrensrelevanz aufweisen dürften.

- PMK links

In einem Ermittlungsverfahren wurden 125 elektronische Datenträger (PC, USB-Sticks etc.) sichergestellt. Auf 29 Datenträgern (entspricht 23%) befinden sich verschlüsselte Daten, die nicht entschlüsselt werden konnten. Lediglich auf einem Datenträger konnten kryptierte Daten entschlüsselt werden (Entschlüsselung erfolgte durch Eingabe des sich aus der Asservatenauswertung ergebenden Passwortes); d.h., lediglich 3% der verschlüsselten Datenträger konnten entschlüsselt werden. Zur Verschlüsselung wurden u.a. folgende Programme verwendet: TrueCrypt, LUKS/dm-crypt, ecryptfs.

Das Verschlüsseln von E-Mailverkehr, Dateien oder ganzen Festplatten ist mittlerweile gängige Praxis im Phänomenbereich PMK -links-. Dabei werden täterseitig verschiedene Verschlüsselungsprogramme verwendet. Selbstverständlich wäre das Instrument der Onlinedurchsuchung in diesem Zusammenhang hilfreich, da z.B. die Erstellung von Selbstbezichtigungsschreiben, Dokumenten zur Ausspähung von Anschlagszielen und Vorbereitung von Straftaten auf Rechnern der Beschuldigten vor einer möglichen Verschlüsselung gesichtet und gesichert werden könnten. Ebenso ist denkbar, dass Verschlüsselungscodes, die innerhalb der Tätergruppe versandt werden, festgestellt werden.

Die Online-Durchsuchung wäre neben der Quellen-TKÜ wahrscheinlich das einzige zweckmäßige Überwachungsinstrument, wenn die Täter bspw. über offene WLAN-Netze kommunizieren. Die Online-Durchsuchung wäre neben der Quellen-TKÜ auch dann das einzige erfolgversprechende Mittel zur Erlangung aktueller IT-Erkenntnisse (Täterkontakte, Informationswege, Beweisdateien etc.), wenn der Beschuldigte über VPN kommuniziert.

- Kinderpornographie

In einem Ermittlungsverfahren wegen des Verdachts der Verbreitung kinderpornografischer Schriften verschlüsselt der Beschuldigte seine Festplatte. Eine offene Durchsuchung (inkl. Sicherstellung der Datenträger) ist nicht erfolgsversprechend, da der Beschuldigte das Passwort nicht preisgibt und eine Entschlüsselung der Festplatte aus technischen Gründen nicht möglich ist.

Eine Online-Durchsuchung auf dem Zielsystem des Beschuldigten ermöglicht die Sicherstellung von beweiserheblichem Material, während der Beschuldigte seinen Computer nutzt und mit dem Internet verbunden ist.

- Online-Betrug

In einem Ermittlungsverfahren wegen des Verdachts des gewerbsmäßigen Betrugs verschlüsselt der Beschuldigte seine Festplatte. Eine offene Durchsuchung ist aus den oben genannten Gründen nicht möglich.

Eine Online-Durchsuchung auf dem Zielsystem ermöglicht das Auslesen (die Sicherstellung) möglicher Zugangskennungen, die der Beschuldigte bei der Begehung der Straftaten benutzt hat. Mithilfe der Zugangskennungen ist ein detaillierter Tatnachweis in der offenen Ermittlungsphase möglich.

- Auslesen von Zugangskennungen

In einem Ermittlungsverfahren verschlüsselt der Beschuldigte seine Festplatte. Eine Entschlüsselung der Festplatte ist aus technischen Gründen nicht möglich.
Eine Online-Durchsuchung auf dem Zielsystem des Beschuldigten ermöglicht das Auslesen von im Arbeitsspeicher temporär hinterlegten Passwörtern/Verschlüsselungscodes. Mithilfe dieser Passwörter kann ein bei einer offenen Durchsuchung sichergestelltes Zielsystem entschlüsselt werden.

b. Rechtsrahmen und Bedarf an der Schaffung einer Rechtsgrundlage für Online-Durchsuchung in der StPO

Das BKA begrüßt ferner grundsätzlich, dass auch eine Online-Durchsuchungs-Regelung vorgesehen ist.
Die vorgenannten Beschlüsse des 69. Deutschen Juristentages zur Anerkennung des fachlichen Bedarfs und zur Aufforderung des Gesetzgebers zur Schaffung einer Rechtsgrundlage beziehen sich im Übrigen neben der Quellen-TKÜ auch auf die Online-Durchsuchung.

Der für die Online-Durchsuchung vorgeschlagene Straftatenkatalog lehnt sich nun nach hiesigem Verständnis an den der Wohnraumüberwachung und der Regelung der „Vorratsdatenspeicherung“ an, was vor dem Hintergrund der Eingriffsintensität der Maßnahme durchaus nachvollziehbar erscheint.

Das Verbot der Anordnung der Maßnahmen nach § 100b und § 100c StPO-E (ODS und WRÜ) erstreckt sich im Entwurf auf ALLE Berufsgeheimnisträger. Systematisch sollte aber ein solches pauschales Verbot nur auf die absolut geschützten und damit privilegierten Berufsgeheimnisträger (Parlamentarier, Geistliche, Verteidiger, Rechtsanwälte) beschränkt sein, gegen die relativ geschützten Berufsgruppen könnten die Maßnahmen bei Vorliegen der überwiegenden hoheitlichen Interessen im Einzelfall an der Durchführung der Maßnahme vorbehalten werden.

Die Regelung in § 100e Abs. 2 StPO-E, dass die Anordnung bei den Maßnahmen ODS und WRÜ einem Kollegialgericht vorbehalten ist, erscheint aus hiesiger Sicht schlüs-

sig, da bereits jetzt die WRÜ unter Kammervorbehalt des Landgerichts nach GVG steht.

In § 100e Abs. 6 Nr.1 StPO-E wird der vom BVerfG in seiner Entscheidung vom 20.04.2016 entworfene Grundsatz der Verwendung von Daten aus eingriffsintensiven Maßnahmen und ihre Möglichkeit der Umwidmung für andere Zwecke (Hypothetische Datenneuerhebung) aufgegriffen und in modifizierter Form in der StPO verankert.

In § 100e Abs. 6 Nr.2 StPO-E wird die Möglichkeit der Umwidmung der Informationen zum Zweck der Gefahrenabwehr an bestimmte Rechtsgüter geknüpft. Es fehlt hier das Rechtsgut „*Bestand des Staates*“, wohingegen die im Entwurf vorzufindenden Formulierungen „*im Einzelfall bestehende Lebensgefahr*“ und „*dringende Gefahr für Leib …*“ letztlich redundant sind.

Die Statistik- und Berichtspflichten nach § 101b StPO-E fordern grundsätzlich die Justiz, nicht die Polizei. Allerdings betrachtet das BKA mit Sorge, dass einige der auffällig extensiven Statistikpflichten faktisch auf die Polizei abgewälzt werden und einen hohen Mehraufwand fordern. Die Erfassungspflichten gehen über die ohnehin schon vorgesehenen (siehe etwa § 88 BKAG-E) Erfassungen durch das BKA hinaus.