KriPoZ Kriminalpolitische Zeitschrift JuP

„Junges Publizieren“

Seminararbeit von

Paula Benedict

WhatsApp-Nachrichten als Beweismittel

Inhaltsverzeichnis

I. Einleitung

Die rasante technische Entwicklung hat einen großen Einfluss auf die Gesellschaft und verändert so auch die Kommunikation. Mithin werden technische Geräte und die mit ihnen verarbeiteten Daten auch immer relevanter für das Recht. In Bezug auf das Strafprozessrecht stellen diese Daten enormes Potential dar, da sie viel Aufschluss über das Leben von Tätern und Straftaten geben können. Vor allem Nachrichten über Messengerdienste wie WhatsApp spielen eine große Rolle. Sie sind oft so persönlich wie ein privates Telefongespräch, werden jedoch im Unterschied zu diesen ohne Weiteres auf den Endgeräten gespeichert. Täter teilen möglicherweise Motive, Abläufe und Standorte mit ihren Kommunikationspartnern. Die Nachrichten können folglich eine hohe Beweiskraft haben. Allerdings kann eine Verwendung im Strafverfahren einen starken Eingriff in die Privatsphäre darstellen. In dieser Arbeit werden WhatsApp-Nachrichten als Beweismittel näher betrachtet. Zunächst wird das Beweisrecht vorgestellt, um in diesem Kontext die WhatsApp-Nachrichten als Beweismittel einordnen zu können. Dabei wird sowohl auf den Zugriff auf diese im Ermittlungsverfahren als auch auf die Einführung als Beweismittel in die Hauptverhandlung eingegangen.

II. WhatsApp-Nachrichten als Beweismittel

1. WhatsApp-Nachrichten

WhatsApp ist ein Instant-Messaging-Dienst, mit dem Nutzer Textnachrichten, Ton-Dateien, Dokumente, Standort und Kontaktinformationen verschicken sowie internetbasiert telefonieren können.[1] Die Nachrichten werden seit 2016 von WhatsApp in Echtzeit mittels einer sogenannten „End-to-End-Verschlüsselung“ gesichert.[2] Dies gilt sowohl für Nachrichten zwischen zwei Personen als auch für solche, die in „WhatsApp-Gruppen“, also an mehrere Teilnehmer, versendet werden.[3] WhatsApp als Unternehmen speichert nur nicht-zugestellte Nachrichten auf seinen Servern, jedoch auch das nur verschlüsselt und kann selbst nicht auf diese zugreifen.[4]

a) Telekommunikationsvorgang

WhatsApp-Nachrichten fallen unter den Begriff der Inhaltsdaten des Telekommunikationsvorgangs. Telekommunikation umfasst alle Formen der Nachrichtenübermittlung unter Raumüberwindung in nichtkörperlicher Weise mittels technischer Einrichtungen.[5] Als „wesentliche Orientierungshilfe“ wird zur Definition des Begriffs § 3 Nr. 22 TKG herangezogen, welcher Telekommunikation als den technischen Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen bezeichnet.[6] Inhaltsdaten sind dabei alle Daten, die den tatsächlichen Nachrichteninhalt umfassen.[7]

---

1 *Graf*, in: BeckOK-StPO, 28. Edition, § 100a Rn. 71.
2 WhatsApp Encryption Overview, Technical White Paper, 2017, abrufbar unter: https://scontent.whatsapp.net/v/t61.22868-34/68135620_760356657751682_6212997528851833559_n.pdf/WhatsApp-Security-Whitepaper.pdf?_nc_sid=41cc27&_nc_ohc=e-uwISyWn80AX9WAcN-&_nc_ht=scontent.whatsapp.net&oh=60952870742ce73726838cb700385350&oe=5ED81153 (zuletzt abgerufen am 27.5.2020).
3 WhatsApp Encryption Overview, Technical White Paper.
4 https://www.WhatsApp.com/security/ (zuletzt abgerufen am 8.1.2018).
5 *Bruns,* in: KK-StPO, 7. Aufl. (2013), § 100a Rn. 4; *BGH*, NStZ 1997, 247.
6 *BGH,* NJW 2001, 1587.
7 Graf, in: BeckOK-StPO, § 100a Rn. 39.

b) Ermittlungsverfahren

Fraglich ist, auf welche Art und Weise die Strafverfolgungsbehörden im Ermittlungsverfahren Zugriff auf die in den Inhaltsdaten verschlüsselten Nachrichten erlangen können.

aa) Telekommunikationsüberwachung eines laufenden Vorgangs § 100a StPO

Ein Zugriff auf die Nachrichten während des laufenden Telekommunikationsvorgangs kann in bestimmten Fällen über die richterlich angeordnete Telekommunikationsüberwachung nach § 100a StPO erfolgen. Diese kann auch ohne das Wissen des Betroffenen stattfinden (verdeckte Ermittlungsmaßnahme). Zunächst muss es sich dafür um Telekommunikation handeln, die überwacht werden soll.[8] Weiterhin muss ein auf bestimmten Tatsachen beruhender, ausreichender Tatverdacht vorliegen. Das Vorliegen dessen liegt im Beurteilungsspielraum des anordnenden Ermittlungsrichters.[9] Der Tatverdacht muss sich auf eine der in § 100a Abs. 2 StPO benannten Katalogtaten beziehen. Ausreichend ist dabei auch der bloße Versuch einer solchen oder eine Vorbereitungstat.[10] Zudem sind die Strafverfolgungsbehörden nach § 100a Abs. 1 Nr. 2 StPO zu einer Einzelfallprüfung verpflichtet, bei der sie jede Tat darauf prüfen müssen, ob sie in diesem konkreten Fall besonders schwer wiegt.[11] Eine Telekommunikationsüberwachung darf ferner nach § 100a Abs. 1 Nr. 3 StPO nur angeordnet werden, wenn die Sachverhaltserforschung auf andere Weise aussichtslos oder wesentlich erschwert wäre. Weiterhin muss auch diese immer dem Verhältnismäßigkeitsgrundsatz entsprechen.

Auch während der Nachrichtenübermittlung, also vor Empfang auf dem Gerät des Adressaten, kann eine Telekommunikationsüberwachung der Inhaltsdaten auf § 100a StPO gestützt werden.[12] Eine solche Telekommunikationsüberwachung kann durch den Anbieter der Telekommunikationsdienste erfolgen, in diesem Fall WhatsApp Inc. Dieser müsste den Strafverfolgungsbehörden eine Kopie der zu überwachenden Telekommunikationsinhalte bzw. –daten zur Verfügung stellen. Problematisch erscheint hierbei, dass WhatsApp aufgrund der „End-to-End"-Verschlüsselung der Nachrichten selbst nicht auf diese zugreifen kann. Daher können die Behörden selber die Überwachung durchführen. Bei der Quellen-Telekommunikationsüberwachung werden technische Vorkehrungen getroffen, die Kommunikationsdaten noch vor ihrer Verschlüsselung bzw. nach ihrer Entschlüsselung auf dem Gerät abfängt.[13] Diese ist jedoch nur verfassungsgemäß, sofern sie sich ausschließlich auf Daten aus dem laufenden Telekommunikationsvorgang beschränkt, was technisch sichergestellt sein muss.[14] Im Falle der WhatsApp-Nachrichten wird aber auch dies kaum möglich sein, da die Daten, selbst wenn sie noch nicht beim Empfänger angelangt sind, auf Servern von WhatsApp verschlüsselt gespeichert sind,[15] der Vorgang also bereits abgeschlossen ist. § 100a StPO kann mithin in Bezug auf WhatsApp-Nachrichten keine Anwendung finden.

8 Zur Begriffsdefinition s. oben.
9 *BGH*, NJW 1995, 1974 ff.; *Günther,* in: MüKo-StPO, 2014, § 100a Rn. 74 f.
10 *Bruns*, in: KK-StPO, § 100a Rn. 31.
11 BT-Drs. 16/5846, S. 40.
12 *Bär*, TK-Überwachung, 2009, § 100a Rn. 12.
13 *Bruns*, in: KK-StPO, § 100a Rn. 27.
14 *BVerfG*, NJW 2008, 822.
15 Siehe oben.

bb) Nach Abschluss des Telekommunikationsvorgangs

(1) Sicherstellung bzw. Beschlagnahme nach § 94 StPO

Nach Abschluss des Kommunikationsvorgangs könnte ein Zugriff auf die auf einem Endgerät oder Server gespeicherten Daten zunächst über die Sicherstellung bzw. Beschlagnahme nach § 94 Abs. 1, 2 StPO erfolgen. Diese stellt typischerweise eine offene Ermittlungsmaßnahme dar. Dabei wird (bei Fehlen einer Einwilligung) aufgrund einer richterlichen Anordnung (§§ 94 Abs. 2, 98 StPO) ein Gegenstand in Verwahrung genommen oder in anderer Weise sichergestellt. Objekt der Sicherstellung kann dabei jeder Gegenstand sein, der einen Beweiswert haben und für die Untersuchung von Bedeutung sein kann.[16] Die Untersuchung beinhaltet das gesamte Strafverfahren von der Einleitung bis zum rechtskräftigen Abschluss.[17] Der Gegenstand muss als Beweismittel in Frage kommen. Beweismittel ist jeder Gegenstand, der unmittelbar oder mittelbar in der Lage ist, für die Tat oder die Umstände ihrer Begehung Beweis zu erbringen oder für den Straffolgenausspruch Beweisbedeutung hat.[18] Um als potentielles Beweismittel angesehen werden zu können, genügt es, wenn in einer ex ante Betrachtung nicht ausgeschlossen werden kann, dass der Gegenstand im weiteren Verfahren zu Beweiszwecken verwendet wird.[19] Zur Ermächtigung der Strafverfolgungsbehörden genügt ein einfacher Anfangsverdacht i.S.v. § 152 Abs. 2 StPO, d.h. konkrete Tatsachen müssen die Annahme belegen, dass eine verfolgbare Straftat begangen wurde.[20] Zudem muss die Sicherstellung bzw. Beschlagnahme auch verhältnismäßig sein. Die Anordnung einer Beschlagnahme i.S.v. § 94 Abs. 2 StPO bei Fehlen der Freiwilligkeit liegt also grundsätzlich im Ermessen des Ermittlungsrichters.

Der weite Begriff des „Gegenstands" i.S.v. § 94 StPO erlaubt auch die Beschlagnahmefähigkeit nicht körperlicher Gegenstände. Daher sind auch Inhaltsdaten nach Abschluss des Telekommunikationsvorgangs von § 94 StPO erfasst.[21] Der Zugriff auf die Daten kann durch Sicherstellung bzw. Beschlagnahme von Ausdrucken oder Datenträgern selbst erfolgen. Es entspricht jedoch regelmäßig der Verhältnismäßigkeit, nicht den Datenträger selbst zu beschlagnahmen, sondern eine Durchsuchung bzw. Durchsicht i.S.v. §§ 102 i.V.m. 110 Abs. 3 StPO des Datensatzes vorzunehmen, da betroffene Datenträger oft Informationen über unbeteiligte Dritte enthalten.[22] Die Behörden können also eine Spiegelung des Mobiltelefons oder Computers, auf dem die WhatsApp-Nachrichten gespeichert sind, vornehmen und diese auswerten.

Weiterhin können die Nachrichten, sofern sie auf einem Server des Providers zwischen- oder endgespeichert sind, bei dem Provider beschlagnahmt werden.[23] Aufgrund der „End-to-End"-Verschlüsselung liegen die Nachrichten jedoch nicht im Herrschaftsbereich von WhatsApp und das Unternehmen kann diese nicht herausgeben. Anders sieht es aus, wenn der Teilnehmer ein Backup der Nachrichten unverschlüsselt in einer sogenannten „Cloud" gespeichert hat. In diesem Fall könnten die Behörden dieses Backup auch vom jeweiligen Betreiber der Cloud beschlagnahmen.[24]

16 *BVerfG*, NJW 2005, 1917 (1920).
17 *Hauschild*, in: MüKo-StPO, § 94 Rn. 16.
18 *OLG München*, NJW 1978, 601.
19 *BVerfG*, NJW 1988, 890 (894).
20 *Wohlers/Greco*, in: SK-StPO, 5. Aufl. (2016), § 94 Rn. 15.
21 *Gerhold*, in: BeckOK-StPO, § 94 Rn. 4.
22 *Joecks*, in: Radtke/Hohmann, StPO, 2011, § 94 Rn. 25.
23 *BVerfG*, NJW 2009, 2431.
24 *Dalby*, CR 2013, 361 (367).

(2) Erhebung von Bestandsdaten § 100j StPO

Bei Speicherung auf einem Endgerät oder Server kann sich den Ermittlungsbehörden das Hindernis der Zugangssicherungscodes, die sogenannte Bestandsdaten i.S.v. §§ 95, 111 TKG sind, stellen. Zugangssicherungscodes können z.B. PIN, PUK oder Passwörter sein.[25] Daher normiert der 2013 in Kraft getretene § 100j Abs. 1 S. 2 StPO eine Auskunftspflicht über diese Codes für die Telekommunikationsunternehmen. Diese Auskunftspflicht muss gem. § 100j Abs. 3 StPO auf Ersuchen der Staatsanwaltschaft von einem Richter angeordnet werden. Voraussetzung für die Anordnung ist die Erforderlichkeit der Auskunft zur Sachverhaltserforschung.[26] Außerdem müssen auch die gesetzlichen Voraussetzungen für den Zugriff auf die durch die Codes gesicherten Daten vorliegen (z.B. Beschlagnahme nach § 94 StPO), da nur dann die Erforderlichkeit der Auskunft über die Zugangsdaten vorliegen wird.[27] Sind die WhatsApp-Nachrichten demnach auf einem Handy, PC oder in einer Cloud gespeichert, muss entweder der Telefonanbieter, der Anbieter des Betriebssystems oder der Provider der Cloud den zu dem Nutzer gehörigen Zugangscode unverzüglich (Abs. 4) an die Ermittlungsbehörden übermitteln.

(3) Online-Durchsuchung § 100b StPO

Der im August 2017 in Kraft getretene § 100b StPO ermächtigt die Behörden zu einer Online-Durchsuchung. Diese Maßnahme war 10 Jahre lang umstritten. Die Beschlagnahme eines PCs mit komplettem Datenbestand und die anschließende Durchsuchung war zwar schon lange nach §§ 94, 102, 110 Abs. 3 StPO möglich,[28] die heimliche Durchsuchung eines solchen war jedoch nicht von diesen Vorschriften umfasst.[29] § 100b StPO ermöglicht nun den heimlichen Zugriff auf sämtliche informationstechnische Systeme und die auf ihnen gespeicherten Inhalte.[30] Die Online-Durchsuchung erfolgt über einen Remote-Zugriff über die Datenleitung durch eine unbemerkt installierte Software, mit der das Gerät ohne das Wissen des Benutzers kontrolliert werden kann und auf darauf gespeicherte Inhalte (wie z.B. WhatsApp-Nachrichten) zugegriffen werden kann.[31] Die Voraussetzungen für die Anordnung decken sich mit denen des § 100a StPO, bloß der Anlasstatenkatalog bezieht sich bei § 100b StPO auf besonders schwere Straftaten.

c) Hauptverhandlung und Revision

Wie oben bereits ausgeführt, ist es nach § 244 Abs. 2 StPO dem Gericht überlassen, wie es Erkenntnisse in die Hauptverhandlung einführt, verwertet und würdigt. Hauptsächlich können die Daten durch Augenscheinsbeweis in die Verhandlung eingeführt werden, indem sie für die Beteiligten sichtbar gemacht werden.[32] Weiterhin können die (ausgedruckten) Nachrichten aber auch durch Urkundenbeweis eingeführt bzw. einem der Kommunikationspartner bei seiner Aussage vorgehalten werden. Urkunden- und Augenscheinsbeweis können aber nur als authentisches Beweismittel in Betracht kommen, wenn der Prozess der Sichtbarmachung technisch einwandfrei ablief, was eventuell durch Heranziehung der dafür zuständigen Person zu beweisen ist.[33] Es kommt auch die Zeugenvernehmung des zuständigen Auswertungsbeamten über die festgestellten Erkenntnisse in Betracht, was aber den

25 *Graf*, in: BeckOK-StPO, § 100j Rn. 8.
26 *Bär*, MMR 2013, 700 (702).
27 *BVerfG*, NJW 2012, 1419.
28 *BVerfG*, NJW 2006, 976.
29 *BGH*, NJW 2007, 930.
30 *Graf*, in: BeckOK-StPO, § 100b Rn. 1.
31 *Graf*, in: BeckOK-StPO, § 100b Rn. 7-10.
32 *BGH*, NStZ 2001, 493.
33 *Momsen*, in: FS Beulke, 2015, S. 871 (878).

Beweiswert verringert.[34] Grundsätzlich kann eine Revision auf Grundlage von §§ 94, 100a, 100b, 100g StPO darauf gestützt werden, dass das Urteil auf unverwertbaren Erkenntnissen beruht, wenn auf die WhatsApp-Nachrichten nicht hätte zugegriffen werden dürfen.

2. Beispiel

In einem vor dem *Landgericht Frankfurt am Main* verhandelten Fall[35] war der Beschuldigte wegen Mordes an seiner Ehefrau angeklagt. Der Angeklagte war angeklagt, mehrfach mit einem Hammerbeil auf den Kopf seiner Ehefrau eingeschlagen und sie anschließend bis zur Bewusstlosigkeit gewürgt zu haben. Die Verletzungen und der anschließende Blutverlust führten schließlich zum Tod der Frau. In der Hauptverhandlung war vor allem umstritten, ob es sich hierbei um eine Affekthandlung handelte oder ob der Angeklagte die Tat schon länger geplant hatte, um sich am Opfer für die Trennung zu rächen. Im Zentrum der Hauptverhandlung stand daher ein forensisch-psychiatrisches Sachverständigengutachten, das zu dem Ergebnis gelangte, dass der Angeklagte zum Tatzeitpunkt zum einen unter einer schweren seelischen Störung litt, zum anderen, dass für das unmittelbare Tatgeschehen ein höchstgradiger Affekt wahrscheinlich ist. Damit lägen die Voraussetzungen der Anwendung des § 21 StGB aufgrund einer erheblich verminderten Steuerungsfähigkeit bei erhaltender Einsicht vor. In der Beweismittelliste sowie der Anklageschrift befanden sich unter anderem Ausdrucke von vier WhatsApp-Nachrichten des Angeklagten, die er vier Tage vor der Tat an verschiedene Freunde sendete. In diesen äußerte er sich positiv zu Fällen bei denen Familienväter ihre Frauen und Kinder töteten/ermordeten.

Die Beweisrelevanz dieser Nachrichten ergibt sich wie folgt. Sie zeigen, dass die Rachegedanken des Angeklagten, die er schon in einem „Abschiedsbrief" zwei Monate vor der Tat beschrieb, bereits vier Tage vor der Tat wieder aufflammten und er die Tötung als Form zum Ausleben dieser auch in Betracht zog bzw. bei anderen Männern in seiner Position bewunderte. In seiner Einlassung hatte er ausgesagt, die Gedanken seien wieder verschwunden. Die Nachrichten tauchen nicht im Verhandlungsprotokoll auf, nur eine der vier wurde im Urteil erwähnt. Dies deutet darauf hin, dass die Nachrichten nicht als Urkundenbeweis in die Verhandlung eingeführt wurden, sondern wenn überhaupt, durch Vorhalt Teil der Hauptverhandlung wurden. Problematisch bei der Einführung als Urkundenbeweis könnte gewesen sein, dass die Nachrichten hauptsächlich auf Französisch verfasst wurden und eine Verlesung dieser gegen § 184 GVG (Deutsch als Gerichtssprache) verstoßen würde, sofern kein Sachverständiger als Dolmetscher hinzugezogen würde.[36] Das *Landgericht* entschied zugunsten einer Affekthandlung und verurteilte den Angeklagten wegen Totschlags gem. § 212 StGB zu einer Haftstrafe von sieben Jahren.

3. Bedeutung von WhatsApp-Nachrichten als Beweismittel

Anhand dieses Falles lässt sich erkennen, welchen Wert WhatsApp-Nachrichten für die Beweisführung haben können. Sie weisen hier auf den längerfristig vorhandenen Tatvorsatz des Angeklagten hin und hätten bei ordnungsgemäßer Würdigung das Urteil vom Totschlag zum Mord umschwenken lassen können oder müssen. Als problematisch kann gesehen werden, dass die von WhatsApp Inc. 2016 eingeführte „End-to-End"-Verschlüsse-

34 BGHSt 43, 36 (38).
35 *LG Frankfurt a.M.*, Az 5/21 Ks – 3590 Js 244545/16 (6/17).
36 *BGH*, NJW 1965, 643; NStZ 1985, 466.

lung auch die Möglichkeiten der Strafverfolgungsbehörden beschränkt und daher extrem beweisrelevantes Material zum Beispiel im Falle von Verlust oder Zerstörung der Endgeräte für immer verloren gehen kann. Dies steigert aber gerade das Vertrauen der Teilnehmer in die Vertraulichkeit ihrer Nachrichten. Dass der Angeklagte in diesem Fall solch persönliche Gedankengänge an seine Freunde verschickt, zeigt gerade, wie sicher er sich der Vertraulichkeit der Kommunikation war.

Problematisch ist also insbesondere das Spannungsverhältnis zwischen dem extrem hohen Beweiswert bzw. der Beweisrelevanz in der Hauptverhandlung und dem Eingriff in die Privatsphäre bzw. die Vertraulichkeit der Kommunikation bei Erhebung im Ermittlungsverfahren. Bei der Verwertung von persönlichen Daten und zwischenmenschlichen Kommunikation muss sich immer die Frage stellen, inwiefern der Staat zu einem solchen Eingriff ermächtigt werden kann und welche Grundrechte dabei vielleicht verletzt werden könnten. Bei einer Telekommunikationsüberwachung eines laufenden Vorgangs nach § 100a StPO ist immer das Post- und Fernmeldegeheimnis des Art. 10 Abs. 1 GG betroffen. Dieses umfasst auch das Telekommunikationsgeheimnis, also die „unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs“ unabhängig von der Übermittlungsart oder der Inhalte an sich.[37] Geschützt wird die Vertraulichkeit der Kommunikation, nicht aber das Vertrauen der Teilnehmer untereinander.[38] Bei einer heimlichen Online-Durchsuchung informationstechnischer Systeme nach § 100b StPO hingegen findet stets ein Eingriff in das „Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme“ als eine eigenständige Ausprägung des Rechts auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG statt.[39] Bei allen anderen oben beschriebenen Maßnahmen ist ebenfalls das Grundrecht auf informationelle Selbstbestimmung betroffen.

Eine Rolle spielt auch der sogenannte Kernbereich privater Lebensgestaltung. Der Kernbereich umfasst Inhalte höchstpersönlichen Charakters, die in einer Einzelfallbetrachtung bewertet werden.[40] Dies beinhaltet auch „innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art“.[41] Dieser wird für §§ 100a – 100c StPO durch § 100d StPO seit August 2017 verstärkt geschützt, der wie § 100a StPO a.F. den verfassungsrechtlichen Vorgaben entspricht.[42] So sind gem. §100d Abs. 1 StPO Maßnahmen unzulässig, durch die allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung gewonnen werden. Darüber hinaus besteht gem. § 100d Abs. 2 StPO ein Verwertungsverbot für Erkenntnisse aus dem Kernbereich privater Lebensgestaltung. Zudem wird vorgeschrieben, dass solche Erkenntnisse unverzüglich zu löschen sind. § 100d StPO ist also eine wichtige Norm, um den Kernbereich privater Lebensgestaltung und die jeweils betroffenen Grundrechte zu schützen. Die Begrenzungen des § 100d StPO beziehen sich jedoch nur auf die Maßnahmen der §§ 100 a-c StPO. Durch die Speicherung der Kommunikationsdaten auf Endgeräten und die mögliche Sicherstellung bzw. Beschlagnahme nach § 94 StPO kann jedoch in vergleichbarem Maße in den Kernbereich privater Lebensgestaltung eingegriffen werden. Dabei ändert das Wissen des Betroffenen nichts an der Eingriffsintensität. Es kann also mit Recht die Frage aufgeworfen werden, ob zum Schutz der Privatsphäre in diesem Bereich noch Handlungsbedarf für den Gesetzgeber besteht.

37 BVerfGE 67, 157 (172); 100, 313 (358); NJW 2008, 822 (825).
38 BVerfGE 85, 386 (399).
39 BVerfGE 120, 274.
40 BVerfGE 80, 367 (374).
41 *Hegmann*, in: BeckOK-StPO, § 100d Rn 6.
42 *BVerfG*, NJW 2012, 833 ff.

Natürlich sind bei den Maßnahmen richterliche Anordnungen unter Beachtung des Subsidiaritätsprinzips erforderlich (§§ 98, 100e StPO und § 100j Abs. 3 StPO). Diese sind jedoch den unterschiedlichsten Anforderungen unterworfen. So ist bei einer Beschlagnahme nach § 94 Abs. 2 StPO lediglich ein einfacher Anfangsverdacht jeglicher verfolgbaren Straftat erforderlich, während bei einer Telekommunikationsüberwachung nach § 100a StPO ein Tatverdacht auf schwere Straftaten, die im Einzelfall erheblich sein müssen, vorliegen muss. § 100a StPO richtet sich (aufgrund der Unanwendbarkeit auf WhatsApp, s. oben) wohl eher auf Telefongespräche. WhatsApp-Nachrichten haben jedoch mittlerweile für viele Menschen Telefongespräche abgelöst, vor allem in jüngeren Generationen. Es werden tiefste Gefühle und private Erlebnisse mit den Telekommunikationspartnern geteilt, immer in dem Vertrauen darauf, dass niemand diese liest, von dem man dies nicht möchte. Sie genießen diesbezüglich auch einen weitaus persönlicheren Stellenwert als zum Beispiel E-Mails, die mittlerweile hauptsächlich für geschäftliche oder professionelle Zwecke genutzt werden. Deshalb muss sich die Frage stellen, warum die Anordnung einer offenen Beschlagnahme der genauso persönlichen Nachrichten geringere Anforderungen erfüllen muss als das Abhören eines Telefongespräches. Zwar stellt das Unwissen des Betroffenen bei heimlichen Maßnahmen eine gewisse Schutzlosigkeit dar, trotzdem muss meiner Meinung nach eine sensiblere und an die hohe Persönlichkeit der Nachrichten angepasste Lösung möglich sein.

Auf der anderen Seite kann argumentiert werden, dass die Nachrichten einen extrem hohen Beweiswert haben. Bei einer möglichst weitreichenden Ermächtigung der Behörden zum Zugriff könnten offensichtlich Straftaten viel effizienter und möglicherweise korrekter aufgeklärt und mit dem richtigen Strafmaß bemessen werden, was wiederum die verfassungsrechtlichen Grundlagen des Verfahrens (faires Verfahren, Schuldprinzip) absichert. Trotzdem sollte der Staat WhatsApp-Nachrichten mit größter Vorsicht behandeln. Die Informationen über die Person und ihre Kommunikationspartner betreffen in den meisten Fällen den Kernbereich privater Lebensgestaltung oder zumindest das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Problematisch ist darüber hinaus, dass WhatsApp dem Nutzer (und somit auch dem Überwachendem) die Option zur Verfügung stellt, auf Nachrichten zuzugreifen, die weit in der Vergangenheit liegen und somit den Behörden Informationen als Beweismittel vorliegen, die vielleicht nicht mehr dem aktuellen Stand entsprechen. Die Anforderungen an einen Eingriff sollten hoch sein und die Ermittlungsbehörden trotz des hohen Beweiswertes nur in seltenen Fällen dazu ermächtigen auf die Nachrichten zuzugreifen. Möglicherweise kann die technische Durchführungsweise so erweitert werden, dass bloß Nachrichten, die tatsächlich Beweiswert haben, betroffen sind und nicht solche, die andere Menschen oder Sachverhalte betreffen.

III. Fazit

Das Thema ist sowohl technisch als auch rechtlich höchst komplex und betrifft höchstpersönliche Informationen. Daher ist wichtig, dass es stets im öffentlichen und politischen Diskurs bleibt und sensibel damit umgegangen wird. WhatsApp-Nachrichten (sowie die anderer Messenger-Dienste) umfassen mittlerweile nicht mehr lediglich die Gespräche selbst. Sie beinhalten häufig auch die Übersendung von Fotos, Videos, Dokumenten und Standorten, bei WhatsApp ist sogar die Übersendung eines Live-Standorts über mehrere Stunden möglich. Zudem gehört WhatsApp zu einem Unternehmen, welches auch die Social-Media-Dienste wie Facebook und Instagram betreibt. Die Menge an Daten, die mithin über Nutzer angesammelt wird, ist folglich enorm und sollte von staatlicher Seite mit großer Vorsicht behandelt werden. Natürlich ist es möglich, WhatsApp-Nachrichten nicht nur repressiv als

Beweismittel, sondern auch präventiv als Möglichkeit der (häufig vermutlich effektiveren) Gefahrenabwehr zu verwenden. Daten könnten von den Beteiligten oder den Anbietern an die Polizei- und Ordnungsbehörden (freiwillig oder unfreiwillig) übergeben werden, um so Gefahren für die öffentliche Sicherheit & Ordnung abzuwenden.

Ähnliches wird aktuell in der Diskussion um die Eindämmung der COVID-19-Pandemie überlegt. Zum einen geht es dabei um die Übermittlung von Verkehrsdaten und den daraus gezogenen Bewegungsprofilen von den Telekommunikationsanbietern (z.B. die Telekom) an die Gesundheitsämter. Diese kann vor dem Hintergrund des Allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG aber nur anonymisiert und (von den Anbietern) freiwillig erfolgen. Eine Verpflichtung der Anbieter ist ohne ausdrücklich gesetzliche Grundlage nicht möglich. Zum anderen ist die Entwicklung einer sogenannten „Corona-Tracing-App“ geplant. Diese soll über Bluetooth von Smartphone zu Smartphone den Standort austauschen, sodass Infizierte sich eintragen können und die in dem für die Infektion kritischen Abstand von 1,5 – 2 Metern bekommen eine Benachrichtigung und können so entsprechende Quarantäne-Maßnahmen vornehmen. Eine Eindämmung der Infektionszahlen erscheint auf diesem Wege sehr vielversprechend, ist aber rechtlich nur auf rein anonymer und freiwilliger Basis (auch bezüglich der Installation) akzeptabel, um den Datenschutz und somit Schutz des Allgemeinen Persönlichkeitsrechts zu ermöglichen.

Diese Grundsätze lassen sich aber nur bedingt auf WhatsApp-Nachrichten übertragen. Zunächst handelt es sich bei COVID-19 voraussichtlich um eine zeitlich begrenzte Gefahr für die Allgemeinheit, die es schnell zu bekämpfen gilt, um die Gesundheit selbst, das Gesundheitssystem und mittelbar auch die Wirtschaft zu schützen. Darüber hinaus geht die Gefahr nicht von einer Person aus. WhatsApp-Nachrichten werden wohl kaum „freiwillig“ von Personen, die aus wie auch immer gearteten Gründen eine Gefahr darstellen oder verursachen, herausgegeben werden. Und auch WhatsApp Inc. selbst wird sich wohl nicht dazu überreden lassen, dauerhaft bzw. wiederholt freiwillig Daten über seine User herauszugeben, da sie diese dann vermutlich verlieren würden (zudem sind sie dazu technisch ja auch gar nicht in der Lage, s. oben). Auch das Erheben von anonymen Daten wird wohl bei der „alltäglichen“ Gefahrenabwehr kaum bzw. in wenigen Spezialfällen sinnvoll sein, da meist gerade die Information über eine spezifische Person benötigt wird. Fraglich ist auch, wie anonym etwas noch sein kann, wenn Inhalte von Gesprächen analysiert werden. Eine Verpflichtung zur Übergabe von WhatsApp-Nachrichten kann daher auch im präventiven Bereich nur unter Wahrung des Kernbereichs der Privatsphäre und der Verhältnismäßigkeit erfolgen. Eine richterliche Anordnung und eine dringende Gefahr sollten stets vorliegen, ebenso wie im repressiven Bereich ein zumindest hinreichender, wenn nicht sogar dringender Tatverdacht.

Zusammenfassend kann man sagen, dass das letzte Wort zum Thema WhatsApp-Nachrichten als Beweismittel wohl aufgrund der immer weiterlaufenden technischen Entwicklung und der sich daran anzupassen versuchenden Rechtsentwicklung noch nicht gesprochen ist oder vielleicht nie gesprochen sein wird.