Januar 2019

RUHR UNIVERSITÄT BOCHUM

RUB

MASTER KRIMINOLOGIE KRIMINALISTIK UND POLIZEIWISSENSCHAFT

Masterarbeit zum Thema:

Die Telekommunikationsüberwachung als zeitgemäße Ermittlungsmethode der deutschen Strafverfolgungs- und Gefahrenabwehrbehörden?

Eine kritische Reflexion in Zeiten von verschlüsselten Datenverbindungen und Datenschutzinteresse.

Erstgutachter:	Herr Staatsanwalt Daniel Garabett
Zweitgutachter:	Herr Ltd. KD Rainer Kasecker

Vorgelegt von:

Julian Twenning

Matrikelnummer: 108115203000

E-Mail: Julian.Twenning@ruhr-uni-bochum.de

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

AES	**Advanced Encryption Standard**
BfDI	**Bundesbeauftragte für den Datenschutz und die Informationsfreiheit**
BfJ	**Bundesamt für Justiz**
BGH	**Bundesgerichtshof**
BKA	**Bundeskriminalamt**
BMBF	**Bundesministerium für Bildung und Forschung**
BMI	**Bundesministerium des Innern, für Bau und Heimat**
BMVg	**Bundesministerium für Verteidigung**
BNetzA	**Bundesnetzagentur**
BRD	**Bundesrepublik Deutschland**
BSI	**Bundesamt für Sicherheit in der Informationstechnik**
BVerfG	**Bundesverfassungsgericht**
CCC	**Chaos Computer Club**
Cell-ID	**Cell Identity (Funkzellenidentität)**
DDR	**Deutsche Demokratische Republik**
DSL	**Digital Subscriber Line**
E2E	**End-to-End**
EFF	**Electronic Frontier Foundation**
EuGH	**Europäischer Gerichtshof**
GFF	**Gesellschaft für Freiheitsrechte**
GrCH	**Charta der Grundrechte der Europäischen Union**
GSM	**Global System for Mobile Communications**
ID	**Identifikationsnummer**

IMSI	**International Mobile Subscriber Identity**
IP	**Internet Protocol**
ISDN	**Integrated Services Dial Network**
MfS	**Ministerium für Staatssicherheit**
P2P	**Peer-to-Peer**
PLMN	**Public Land Mobile Network**
RCIS	**Remote Communication Interception Software**
RSS	**Radio Subsystem**
SINA	**Sichere Inter-Netzwerk Architektur**
SMS	**Short-Messaging-Service**
TKÜ	**Telekommunikationsüberwachung**
TR	**Technische Richtlinie**
UFED	**Universal Forensic Extraction Device**
VoIP	**Voice-over-IP**
VPN	**Virtual Private Network**
VS	**Verschlusssache**
ZITiS	**Zentrale Stelle für Informationstechnik im Sicherheitsbereich**

1 Einleitung

Das geheime Abhören von Telefonaten und Datenverbindungen durch staatliche Behörden erregt in hohem Maße das Interesse der Öffentlichkeit. Seit Jahren findet eine hitzige Diskussion im Spannungsfeld zwischen dem Sicherheitsinteresse der Bevölkerung und dem Schutz des höchstpersönlichen Lebensbereichs des Einzelnen statt. Es verwundert daher nicht, dass auch seitens der Politik die Thematik regelmäßig aufgegriffen und diskutiert wird. Letztlich scheiden sich die Geister an der Frage, wie umfangreich der Staat in die Grundrechte der einzelnen Bürger eingreifen darf und auch muss, um im Zeitalter neuer Gefahren und zur Erfüllung der Strafverfolgungsaufgabe, seinen hoheitlichen Verpflichtungen nachkommen zu können.

1.1 Ausgangslage und Themendarstellung

Die vorliegende Masterarbeit widmet sich eben dieser Thematik. Abstrakt scheint die Lösung auf der Hand zu liegen. So fand die allgemeine situationsbeschreibende und appellierende Rede des damaligen Bundesinnenministers *Thomas de Maizière (CDU)* anlässlich der Abschlusspressekonferenz der Innenministerkonferenz in Dresden am 14.06.2017 breite Zustimmung:

> „[...] Es kann nicht sein, dass es für die Verfolgung von Straftaten faktisch rechtsfreie Räume gibt, in denen Straftäter sich im Internet bewegen. [...] Das bedeutet zum Beispiel, dass man die Behörden rechtlich und technisch in den Stand versetzen muss – unter den gleichen Bedingungen wie man ein Telefon oder eine SMS abhört – auch Informationen und Nachrichten auf Messangerdiensten abgreifen zu können. [...]“[1]

Es wird im Rahmen dieser Arbeit jedoch eingehender zu beleuchten sein, welche Schwierigkeiten sich über diesen Gemeinsatz hinaus nicht nur rechtlich stellen. Vor allem werden daher auch die Schwierigkeiten behandelt, die sich aufgrund der technisch veränderten Realität im Bereich der Telekommunikation ergeben.

[1] *Phönix* 2017.

Kommunikationsdienste, wie beispielsweise WhatsApp, Viber, Skype und Co., die Daten und Kommunikation verschlüsselt zwischen den Teilnehmern übertragen, stellen eine enorme Herausforderung für Strafverfolgungs- und Gefahrenabwehrbehörden dar. In kürzester Zeit lassen sich durch derartige Anwendungen große Mengen von Daten weltweit übertragen. Dass diese auch für illegale Machenschaften und zur Planung von Operationen terroristischer Organisationen und durch Einzeltäter genutzt werden können, ist dabei evident. Dabei nutzen derartige Täter ganz gezielt bestimmte Kommunikationswege, um sich der Überwachung staatlicher Sicherheitsbehörden zu entziehen. So sollen beispielsweise die Täter der Anschläge von Paris im November 2015 im Vorfeld mittels Videospielen und Spielekonsolen kommuniziert haben, um die Anschläge zu planen, ohne von Sicherheitsbehörden überwacht zu werden.[2]

Doch gibt es auch Stimmen, die eine eklatante Beschneidung der Grundrechte des einzelnen Bürgers und den damit einhergehenden „Überwachungsstaat" befürchten. So argumentieren Datenschutzaktivisten des Vereins Digitalcourage, der gegen die rechtliche Möglichkeit zur Überwachung verschlüsselter Telekommunikation mithilfe einer Abhörsoftware („Staatstrojaner") Verfassungsbeschwerde eingelegt hat, wie folgt:

> „Der Staatstrojaner ist ein maßloser Übergriff auf das Privatleben aller Menschen. In Zukunft reicht es schon aus, WhatsApp installiert zu haben und mit jemandem befreundet zu sein, der Mitglied im Hanfverband ist, um von staatlichen Überwachern gehackt zu werden. Die Auswirkung [sic!] auf Demokratie und Meinungsfreiheit sind zum Fürchten – mit solchen Gesetzen ebnet die Große Koalition den Weg in einen autoritären Überwachungsstaat."[3]

Um den Gefahren, die mittels der modernen Telekommunikation entstehen, technisch und rechtlich begegnen zu können und gleichzeitig nur in einem gewissen Rahmen in die Persönlichkeitsrechte des Einzelnen einzugreifen, bewegen sich die Eingriffsbefugnisse deutscher Strafverfolgungs- und Gefahrenabwehrbehörden in einem gesetzlichen Rahmen. Ob in diesem ge-

---

[2] Vgl. *Fröhlich* 2016.

[3] *Demuth / Friedemann* 2017.

schaffenen Rahmen überhaupt noch effektiv Strafverfolgung und Gefahrenabwehr betrieben werden kann, oder ob dieser die Grundrechte des einzelnen Bürgers derart beschneidet, dass ein „Überwachungsstaat“ befürchtet werden muss, ist Gegenstand dieser Masterarbeit. Dabei widmet sich diese Arbeit schwerpunktmäßig den Besonderheiten und Problematiken, die sich bei der Überwachung verschlüsselter Telekommunikation ergeben.

1.2 Einordnung des Themas in die Kriminalistik

> „Die Kriminalistik ist die Wissenschaft von der Aufdeckung, Untersuchung und Verhütung von Straftaten und kriminalistisch relevanten Sachverhalten. Ihr Gegenstand sind die Gesetzmäßigkeiten und Erscheinungen des Entstehens von Informationen (Spuren/Beweisen) bei der Straftatenbegehung sowie die Methoden ihres Auffindens, Sicherns und Bewertens für Ermittlungs- und Beweiszwecke. Ihre Aufgabe ist, Ereignisse mit strafrechtlicher und kriminalistischer Relevanz aufzudecken, deren Ablauf zu untersuchen, den Täter zu ermitteln und mit hinreichender Sicherheit zu überführen (Repression). Sie entwickelt aus Erkenntnissen zur Straftatenuntersuchung Verfahren zur Verhütung künftiger Straftaten (Prävention) und gibt kriminalstrategische Empfehlungen zur Kriminalitätskontrolle und Bekämpfung von Straftaten.“[4]

Basierend auf dieser Definition der Kriminalistik, unterteilen *Ackermann / Clages / Roll* sie in sechs Teildisziplinen: Theorie und Methodologie, Kriminaltaktik, Kriminaltechnik, spezielle Kriminalistik, kriminalistische Psychologie und Kriminalstrategie.[5]

Andere Stimmen in der Wissenschaft nehmen eine unterschiedliche Unterteilung vor. So unterteilen *Kube / Schreiber* beispielsweise die Kriminalistik lediglich in drei Teildisziplinen: Kriminalstrategie, Kriminaltaktik und Kriminaltechnik.[6]

---

[4] *Ackermann / Clages / Roll* 2011, S. 13.

[5] Vgl. *Ackermann / Clages / Roll* 2011, S. 17.

[6] Vgl. *Kube / Schreiber* 1992, S. 2 f.

Da es sich bereits bei der Telekommunikation an sich um einen technischen Prozess handelt, wird auch für das Mithören und Aufzeichnen dieser Telekommunikation Technik benötigt.

Jedoch subsummieren sowohl *Ackermann / Clages / Roll* als auch *Kube / Schreiber* die TKÜ nicht explizit unter den Begriff der Kriminaltechnik. Die Schwierigkeit der Einordnung von TKÜ in die Kriminaltechnik dürfte darin begründet sein, dass es sich hierbei um eine spezielle Ermittlungsmethode handelt, die nur deliktsspezifisch Anwendung findet und hohen rechtlichen Voraussetzungen unterliegt. So führen *Ackermann / Clages / Roll* in ihren Ausführungen zur speziellen Kriminalistik u. a. ausgewählte kriminalphänomenologische Erscheinungen an, bei denen die spezielle Kriminalistik Anwendung findet. Herauszugreifen sind hier die Organisierte Kriminalität und die politisch motivierte Kriminalität.[7] Bei diesen speziellen Phänomenen bedarf es daher auch spezieller technischer Mittel um auf diese reagieren zu können.

Da es sich bei der TKÜ um eine technische Maßnahme handelt, die nur bei ausgewählten kriminalphänomenologischen Erscheinungen zum Einsatz kommt, lässt sie sich daher am ehesten in den Bereich der speziellen Kriminalistik eingruppieren. *Ackermann / Clages / Roll* verdeutlichen diese Einordnung mit ihrer Definition zur speziellen Kriminalistik:

> „Bezogen auf ausgewählte kriminalphänomenologische Erscheinungen der Kriminalität befasst sich die spezielle Kriminalistik mit Methoden und Verfahrensweisen zu ihrer Aufdeckung, Untersuchung, Vorbeugung einschließlich von strategischen Entscheidungen zur Verhinderung bzw. Einflussnahme auf Entwicklung dieser Erscheinungsformen.“[8]

1.3 Aufbau der Arbeit

Diese Masterarbeit beginnt mit einer kurzen Darstellung des geschichtlichen Hintergrunds der TKÜ in der Bundesrepublik Deutschland. Hiermit soll ver-

[7] Vgl. *Ackermann / Clages / Roll* 2011, S. 27.
[8] *Ackermann / Clages / Roll* 2011, S. 28.

deutlicht werden, dass die Überwachung von Telekommunikation nicht erst in der heutigen Zeit Aktualität erlangte, sondern bereits seit Jahrzehnten durch Strafverfolgungs- und Sicherheitsbehörden eingesetzt wird.

Im Anschluss werden zunächst die klassischen Formen der Telekommunikation, sowie die technischen und rechtlichen Grundlagen der Überwachung beschrieben, bevor die aktuelle Problematik der Überwachung verschlüsselter Telekommunikation betrachtet wird. Hierzu wird eine Auswahl der relevantesten verschlüsselten Sprachkommunikationsdienste und Messengeranwendungen betrachtet, wobei die besonderen rechtlichen und technischen Herausforderungen für die deutschen Strafverfolgungs- und Gefahrenabwehrbehörden problembasiert thematisiert werden.

Schwerpunktmäßig beschäftigt sich diese Masterarbeit mit der Problematisierung des Einsatzes von Telekommunikationsüberwachung bei verschlüsselter Telekommunikation und der Erarbeitung von Lösungsansätzen, mit denen dieser neuen Herausforderung begegnet werden kann. Hierzu erfolgt eine kritische Gegenüberstellung von Eingriffsbefugnissen seitens des Staates und den Persönlichkeitsrechten der einzelnen Bürgerinnen und Bürger. Es werden neue technische Entwicklungen und deren rechtliche Grundlagen thematisiert, sowie deren Effektivität und technische Durchsetzbarkeit diskutiert.

In einem abschließenden Fazit wird ein Resümee der zuvor dargestellten thematischen Schwerpunkte gezogen. Es werden die erarbeiteten Lösungsansätze zusammenfassend dargestellt und es wird versucht, die Ausgangsfrage: „Ist die Telekommunikationsüberwachung eine zeitgemäße Ermittlungsmethode der deutschen Strafverfolgungs- und Gefahrenabwehrbehörden?“ im Lichte der vorangegangenen Ausarbeitung zu beantworten.

2 Geschichtlicher Hintergrund der Telekommunikationsüberwachung in der BRD

Der Ursprung der Telefonie datiert vom 26. Oktober 1861 *Philipp Reis (1834 – 1874)* präsentierte im Physikalischen Verein zu Frankfurt am Main ein Gerät, das Gespräche mit der Hilfe von elektrischem Strom mit einem in der

Ferne befindlichen Zweitgerät ermöglichte. Diese Geräte benannte er „Telephon“. 15 Jahre nach dieser damals, aufgrund ihrer schlechten Sprachqualität unterschätzten Erfindung, meldete der Brite *Alexander Graham Bell (1847 – 1922)* in den USA das erste Patent für ein Telefon an.[9] Damit setzte er den Grundstein für eine völlig andere und neue Art der Kommunikation. Welchen Stellenwert die Telekommunikation allein bis zum Ende des Zweiten Weltkriegs eingenommen hatte zeigt sich daran, dass *General Dwight D. Eisenhower (1890 – 1969)* nach dem Einmarsch der alliierten Truppen in Deutschland als eines der ersten Gesetze ein Zensurgesetz erließ. Durch dieses wurde zunächst jegliche Form der Telekommunikation in der Besatzungszone verboten bzw. unterbunden und die Wiederaufnahme des Telefonverkehrs strikten Zensurbestimmungen unterworfen.[10] Das dem zugrundeliegende sog. MRG-Gesetz Nr. 76 trat am 29. Januar 1945 in Kraft und kann als das erste Gesetz zur Überwachung des Post- und Telefonverkehrs in der deutschen Nachkriegszeit bezeichnet werden.[11]

Mit der Verabschiedung des Grundgesetzes im Jahre 1949 wurde in Artikel 10 das Brief-, Post und Fernmeldegeheimnis eingeführt. Bereits dort wurde ein einfacher Gesetzesvorbehalt implementiert, der einen Eingriff aufgrund eines Gesetzes zulässt.[12]

Im Rahmen der Notstandsgesetzgebung im Jahre 1968 wurde – systemwidrig – auch eine Änderung des Artikels 10 verabschiedet, in der die sog. „Staatsschutzklausel“ in Art. 10 Abs. 2 S. 2 GG aufgenommen wurde.[13] Das dem zugrundeliegende G10-Gesetz markierte einen Meilenstein in der deutschen Nachkriegsgeschichte. Es konnte als eine Art Befreiung von den letzten durch die Besatzungsmächte verhängten Restriktionen gesehen werden, da es das bis dahin gültige und im Deutschlandvertrag von 1952 festgeschriebene Vorbehaltsrecht der Besatzungsmächte hinsichtlich der Überwa-

[9] Vgl. *Blume* 2011.
[10] Vgl. *Foschepoth* 2017, S. 48.
[11] Vgl. *Foschepoth* 2017, S. 50.
[12] Vgl. *Bundesgesetzblatt Nr. 1* 1949, S. 178; BGBl I 1949, S. 178.
[13] Vgl. *Foschepoth* 2017, S. 178.

chung des Post- und Fernmeldeverkehrs ablöste und den deutschen Sicherheitsbehörden erstmals diese Kompetenzen übertrug.[14]

Die öffentliche und politische Debatte um die Einführung des G10-Gesetzes und den damit verbundenen eklatanten Eingriff in Artikel 10 führte in dieser Zeit in eine politische und gesellschaftliche verfassungsrechtliche Kontroverse. Obwohl mit dem G10-Gesetz auch die §§ 100a, b StPO in die Strafprozessordnung aufgenommen wurden, fand dies in der geführten Kontroverse kaum Beachtung.[15]

In den 70er Jahren gewannen die §§ 100a, b StPO und die damit einhergehende repressive TKÜ jedoch aufgrund des aufkeimenden Linksterrorismus maßgeblich an Bedeutung.[16]

In den 80er Jahren wurde es in der Öffentlichkeit relativ ruhig um das Thema der Überwachungsmaßnahmen, bevor in den 90er Jahren eine Zunahme der dokumentierten verdeckten Ermittlungsmaßnahmen zu verzeichnen war.[17] Dies dürfte insbesondere mit der Erweiterung der Strafprozessordnung und des Strafgesetzbuchs durch das im Jahre 1992 verabschiedete „Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität“ (OrgKG) sowie dem damit einhergehenden Bedeutungsgewinn der Organisierten Kriminalität zusammenhängen.

Bis in die 2000er Jahre wurde der Straftatenkatalog des § 100a StPO seit seiner Entstehung mehrfach Änderungen unterzogen. Er wurde um 20 Straftatbestände ergänzt.[18]

Im Jahr 2001 erfolgte durch ein Gesetz zur Änderung der Strafprozessordnung zudem auch die Einführung der §§ 100g, h StPO,[19] die die Telekommunikationsdienstanbieter unter gewissen Voraussetzungen dazu verpflichten, den Ermittlungsbehörden Telekommunikationsverbindungsdaten zur Verfügung zu stellen. Ein Jahr später folgte die Einführung des

---

[14] Vgl. *Foschepoth* 2015, S. 29 – 30.
[15] Vgl. *Welp* 2001, S. 289.
[16] Vgl. *Albrecht / Dorsch / Krüpe* 2013, S. 7.
[17] Vgl. *Kühne* 2015, Rn. 519.
[18] Vgl. *Paeffgen* 2001, S. 1300.
[19] BGBl. I 2001, S. 3879.

§ 100i StPO,[20] der den repressiven Einsatz von sog. IMSI-Catchern ermöglichte. Die Einführung dieser Normen war dem fortwährenden technischen Fortschritt im Bereich der mobilen Telefonie geschuldet. Eben dieser technische Fortschritt im Bereich der Telekommunikation zwingt den Gesetzgeber dazu, auch die Eingriffsbefugnisse fortwährend anzupassen. So erfolgte zuletzt im Jahre 2017 eine Erweiterung der §§ 100a, b StPO,[21] die es den Ermittlungsbehörden u. a. ermöglicht, die sog. Quellen-TKÜ einzusetzen.

3 Telekommunikation und Telekommunikationsüberwachung

Der Begriff der Telekommunikation ist jedem Menschen in der modernen Gesellschaft geläufig und wird häufig mit Telefonie gleichgesetzt. Der Gesetzgeber stellt eine klare Definition hierzu auf. In § 3 Nr. 22 TKG stellt er fest, dass Telekommunikation den „[...] technischen Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen [...]“ bedeutet. Doch welche vielseitigen Möglichkeiten sich hinter dieser Definition verbergen, wird erst deutlicher, wenn man die in § 3 Nr. 23 TKG befindliche Definition der Telekommunikationsanlagen näher betrachtet:

„Telekommunikationsanlagen [sind] technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können.“

Hier wird klar, dass es sich bei Telekommunikation keinesfalls zwingend um ein einfaches Gespräch zwischen zwei verbundenen Telefongeräten handelt. Vor dem Hintergrund moderner Medien zeigt sich vielmehr, dass Telekommunikation auf vielen verschiedenen Ebenen und in den unterschiedlichsten Formen stattfinden kann.

Um die Hintergründe der im Rahmen dieser Arbeit dargelegten Problematiken im Bereich der TKÜ im Hinblick auf den unaufhaltsamen technischen

[20] BGBl. I 2002, S. 3018.
[21] BGBl. I 2017, S. 3203 - 3204.

Fortschritt der Telekommunikationsmedien besser verstehen zu können, wird nachfolgend ein Überblick über verschiedene Telekommunikationsmöglichkeiten, deren technische Hintergründe sowie die technischen und rechtlichen Aspekte der Überwachung selbiger gewährt.

Die Ausführungen werden sowohl jene zur Überwachung des Gesprächs- bzw. SMS-Inhalts, als auch die Möglichkeit der Erhebung von Verkehrs- und Standortdaten umfassen. Hinsichtlich der repressiven Erlangung von Standortdaten wird im Rahmen dessen eine aktuelle rechtliche und tatsächliche Problematik bei der Beantragung und Beschaffung von retrograden Standortdaten erläutert, bevor auf die Besonderheiten der verschlüsselten Telekommunikation eingegangen wird.

3.1 Unverschlüsselte Telefonie

„Das [Festnetz-]Telefon prägt unser Leben. Die Technik des Telefons und damit das Telefonieren wird für uns immer interessanter.“[22] Dieses Zitat aus einem Sachbuch über Telefontechnik aus dem Jahre 1995 war seinerzeit sicher zutreffend, erscheint in Zeiten von Messengerdiensten und VoIP-Telefonie jedoch nicht mehr ganz aktuell. Statistiken belegen, dass die Nachfrage nach Festnetztelefonanschlüssen deutlich rückläufig ist. So bestanden im Jahr 2005 noch 54.791.000 Festnetztelefonanschlüsse in der Bundesrepublik Deutschland. Bis in das Jahr 2017 ging diese Zahl um fast 19% auf 44.400.000 Anschlüsse zurück.[23] Die Anzahl der Mobilfunkanschlüsse entwickelt sich jedoch gegenläufig. Im Jahr 2000 konnten in der Bundesrepublik Deutschland insgesamt 48.202.000 Mobilfunkanschlüsse registriert werden. Im Jahr 2017 umfasst die Gesamtzahl der Mobilfunkanschlüsse in der BRD bereits unglaubliche 106.000.000.[24] Die enorme Steigerung der Anzahl von Mobilfunkanschlüssen in der BRD dürfte verschiedene Gründe haben. Ein wichtiger Grund ist jedoch ohne Zweifel, dass in Zeiten von Smartphones als alltägliche Begleiter, das Mobiltelefon nicht ausschließlich für Telefongesprä-

[22] *Frey / Schönfeld* 1995, S. 11.
[23] Vgl. *International Telecommunication Union* 2018.
[24] Vgl. *International Telecommunication Union* 2018.

che, sondern vielmehr als multimedialer Alleskönner mit dauerhafter Internetverbindung genutzt wird.

Nichtsdestotrotz zeigt die zwar rückläufige, aber dennoch hohe Zahl an Festnetztelefonanschlüssen und auch die enorme Zahl der Mobilfunkanschlüsse, dass die herkömmliche Telefonie auch in Zeiten von Messengerdiensten, softwarebasierter VoIP-Telefonie und mobilen Datenverbindungen nicht vernachlässigt werden sollte. Unter der herkömmlichen unverschlüsselten Telefonie wird in der Folge die analoge und digitale Festnetztelefonie, sowie die über das mobile Telefonnetz geführte, nicht internetbasierte Mobilfunktelefonie verstanden.

3.1.1 Technische Grundlagen

Festnetztelefonie

Die herkömmliche unverschlüsselte Festnetztelefonie kann zunächst in analoge und digitale Telefonie untergliedert werden. Der analoge Telefonanschluss zeichnet sich dadurch aus, dass der Nutzer nur über eine einzige Telefondose als Netzabschluss verfügt. Er kann deshalb nur eine fest definierte Rufnummer nutzen.[25] Die digitale Festnetztelefonie wurde mit der Einführung des sog. Integrated Services Dial Network (ISDN) ermöglicht. Durch die damals fortschreitende Digitalisierung der Fernmelde-Ortsnetze entstand das „Universalnetz“ ISDN, das dem Teilnehmer – neben der Telefonie – weitere Dienste wie z. B. Datenübermittlung über mehrere Kanäle zur Verfügung stellte.[26]

Die Nachfolge des ISDN trat die sog. Digital Subscriber Line (DSL) an. Auch dieses System kann auf der Grundlage der bereits vorhandenen Telefonkabel installiert und genutzt werden. Durch den Einsatz eines sog. Splitters ermöglicht der DSL-Anschluss das parallele Betreiben einer analogen oder digitalen (ISDN) Telefonleitung.[27] Der Unterschied des DSL-Netzes zum ISDN und dem analogen Telefonnetz ist, dass sich die beiden Letztgenannten stets mit einer fest zugeteilten Rufnummer einwählen müssen. Das DSL-

[25] Vgl. *Telefon 24 Blog* 2015.
[26] Vgl. *Frey / Schönfeld* 1995, S. 49.
[27] Vgl. *Schemberg / Linten* 2006, S. 79.

Netz stellt dagegen IP-basiert eine Datenverbindung her.[28] Eine zugeteilte Rufnummer ist hierzu nicht mehr notwendig.

Bis 2018 beabsichtigt der größte deutsche Netzbetreiber die Abschaltung sämtlicher analoger und ISDN-basierter Festnetzanschlüsse, sodass das Telefonieren ausschließlich über die bereits beschriebene VoIP-Verbindung möglich sein wird.[29]

Mobilfunktelefonie

Das Telefonieren mit dem Mobiltelefon birgt einige Besonderheiten im Vergleich zur Festnetztelefonie.

Es entstanden seit 1958 immer neue Mobilfunkstandards, welche die mobile Telefonie und das mobile Surfen komfortabler und nutzerfreundlicher gestalteten. Die 1. Generation des Mobilfunks (1G) umfasste das A-Netz (1958), das B-Netz (1972) und das C-Netz (1986). Die Sprachübertragung erfolgte analog. Ab der 2. Generation (2G, 1992) wurde die digitale Sprachübertragung im D-Netz eingeführt und der internationale GSM-Standard etabliert. Im 2.5G-Netz (2001) wurde die Technik durch die digitale Datenübertragung ergänzt. Die nachfolgenden Generationen erhöhten stets den Funktionsumfang und die Bandbreiten der Datenströme. So wurde im Jahr 2004 das UMTS eingeführt (3G), dessen Bandbreite im Jahr 2006 erweitert (HSPA, 3.5G; EDGE 2.75G) und im Jahre 2010 das auf dem UMTS-Standard basierende LTE (4G) angeboten. Die zukünftige Mobilfunkgeneration (5G) wird im Jahre 2020 erwartet.[30]

In Deutschland gibt es im Jahre 2018 drei große Mobilfunkbetreiber, welche die benötigte Infrastruktur zur Verfügung stellen. Hierbei handelt es sich um die Deutsche Telekom, Vodafone und Telefonica.

Das Mobilfunknetz ist zellular aufgebaut. Das bedeutet, dass eine Vielzahl von Funkzellen z. B. auf dem Gebiet der Bundesrepublik Deutschland verteilt sind. In diese wählt sich das Mobiltelefon des Nutzers ein. Über die Mobilfunkzellen wird so dem Nutzer ermöglicht, eine Verbindung zu anderen Mo-

[28] Vgl. *Schemberg / Linten* 2006, S. 80.
[29] Vgl. *Verbraucherzentrale* 2018.
[30] Vgl. *Hessische/Niedersächsische Allgemeine* 2017.

biltelefonen oder in das Festnetz aufzubauen bzw. Datenverbindungen unterwegs zu nutzen."[31]

Das heutzutage im GSM-Standard genutzte Public Land Mobile Network (PLMN) besteht aus den Mobilstationen (MS), Basisstationen (BS), Mobilvermittlungseinrichtungen (MSC) und Aufenthaltsregistern (LR).[32] Das innerhalb des PLMN genutzte Radio Subsystem (RSS) dient als Ankopplung der Mobilfunkteilnehmer an das Festnetz. Das RSS beinhaltet die Mobilstationen (mobile Endgeräte) und die Basisstationen samt Steuerung.[33] An die Basisstationen sind die einzelnen Funkzellen angeschlossen. Diese stellen den kleinsten geografischen Funkversorgungsbereich dar, sind im Idealfall wabenförmig aufgebaut und können im GSM-900-System eine Fläche von bis zu 35 km abdecken. Jede Funkzelle verfügt zudem über eine eigene Identität und kann anhand der Cell-ID identifiziert werden.[34] Somit ist es u. a. möglich, den Standort der Funkzelle und die in ihr eingewählten Mobilstationen in Erfahrung zu bringen.

Überwachung und Übermittlung von TKÜ-Daten

§ 110 Abs. 1 Nr. 1 des Telekommunikationsgesetzes (TKG) verpflichtet denjenigen, der „[...] eine Telekommunikationsanlage betreibt, mit der öffentlich zugängliche Telekommunikationsdienste erbracht werden, [...] ab dem Zeitpunkt der Betriebsaufnahme auf eigene Kosten technische Einrichtungen zur Umsetzung gesetzlich vorgesehener Maßnahmen zur Überwachung der Telekommunikation vorzuhalten und organisatorische Vorkehrungen für deren unverzügliche Umsetzung zu treffen [...]." § 110 Abs. 3 TKG berechtigt zudem die Bundesnetzagentur (BNetzA) die technischen „[...] Einzelheiten, die zur Sicherstellung einer vollständigen Erfassung der zu überwachenden Telekommunikation und zur Auskunftserteilung sowie zur Gestaltung des Übergabepunktes zu den berechtigten Stellen erforderlich sind, in einem Benehmen mit den berechtigten Stellen und unter Beteiligung der Verbände und der Hersteller [...]" in einer technischen Richtlinie (TR) festzulegen.

---

[31] Vgl. *Duque-Antón* 2002, S. 2.
[32] Vgl. *Biala* 1995, S. 57.
[33] Vgl. *Biala* 1995, S. 58.
[34] Vgl. *Biala* 1995, S. 59.

Gem. § 7 Abs. 2 S. 1 TKÜV hat der Verpflichtete jede Überwachungskopie unter der von der berechtigten Stelle vorgegebenen Referenznummer an diese zu übermitteln. Diese Referenznummer beginnt mit der Identifikationsnummer (ID) der jeweiligen berechtigten Stelle.

In Deutschland existieren insgesamt 41 berechtigte Stellen. Hierzu zählen das Bundesamt und die Landesämter für Verfassungsschutz, das Zollkriminalamt sowie die Zollfahndungsämter, das Bundeskriminalamt, sämtliche Landeskriminalämter, die Bundespolizei, der Militärische Abschirmdienst und vereinzelte Innenministerien.[35]

Die Übermittlung der Daten zwischen den Telekommunikationsunternehmen und den berechtigten Stellen erfolgt bilateral. Das heißt, dass sowohl Daten von den berechtigten Stellen an die Unternehmen (z. B. digitale Kopien von TKÜ-Anordnungen) als auch von den Unternehmen an die berechtigten Stellen gesendet werden.

Die nachfolgende Abbildung stellt – am Beispiel eines Auskunftsersuchens und der zugehörigen Auskunft über Verkehrsdaten – den Datenaustausch zwischen der berechtigten Stelle und dem Unternehmen dar.

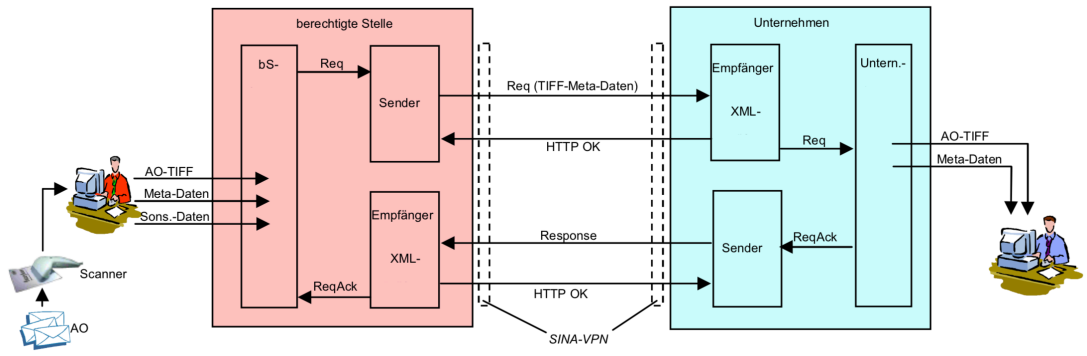

Abbildung 1: Datenübermittlung zwischen berechtigter Stelle und Unternehmen[36]

Abbildung 1 zeigt, dass die an sich bereits verschlüsselten Daten (hier: XML-verschlüsselte Dokumenten- oder Audiodateien) zwischen dem Netzwerk

[35] Vgl. *Bundesnetzagentur für Elektrizität, Gas, Telekommunikation und Eisenbahnen,* o. D.

[36] *Bundesnetzagentur für Elektrizität, Gas, Telekommunikation und Eisenbahnen* 2017, S. 126.

des Telekommunikationsunternehmens und dem Netzwerk der berechtigten Stelle ausgetauscht werden. Dieser Austausch erfolgt über das herkömmliche Internet, in dem mittels eines ebenfalls verschlüsselten Virtual Private Network (VPN) die Datenübermittlung zusätzlich abgesichert wird.

Die BNetzA schreibt vor, dass für diese zusätzliche Absicherung sog. SINA-Boxen (Sichere Inter-Netzwerk Architektur) des Herstellers Secunet zu benutzen sind. Eine SINA-Box ist am einfachsten damit zu beschreiben, dass sie von außen einem herkömmlichen DSL-Router ähnelt. Die IT-Infrastruktur des Telekommunikationsunternehmens und der berechtigten Stelle sind jedoch erst über die SINA-Boxen, die das o. g. VPN aufbauen, mit dem Internet verbunden. In der SINA-Box des Absenders werden die Daten verschlüsselt und erst in der zweiten SINA-Box des jeweiligen Adressaten werden diese wieder entschlüsselt.

Die kryptographische Verschlüsselung der SINA-Box (Modell L3) ist durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) bis zum Geheimhaltungsgrad *Verschlusssache (VS) – GEHEIM* zugelassen.[37]

Hier zeigt sich, dass seitens der Behörden großes Augenmerk auf die Sicherheit der Übermittlung von TKÜ-relevanten Daten gelegt wird. Durch das TKG, die TKÜV und die TR TKÜV der BNetzA liegen zudem klare Vorgaben für Telekommunikationsanbieter vor, wie die TKÜ-relevanten Daten an die berechtigten Stellen zu übermitteln sind.

3.1.2 Rechtliche Grundlagen

Nachfolgend werden die rechtlichen Grundlagen zur Überwachung der unverschlüsselten Telefonie dargestellt und erläutert. Die Ausführungen umfassen sowohl die Rechtsgrundlagen zur Inhaltsüberwachung als auch zu den Verbindungs- und Standortdaten. Im Rahmen der Ausführungen zu den Eingriffsbefugnissen hinsichtlich der Erlangung von Verbindungs- und Standortdaten, wird ein aktuelles rechtliches und tatsächliches Problem im Bereich der Strafverfolgung betrachtet, welches dazu führt, dass aktuell ein repressi-

[37] Vgl. *Bundesamt für Sicherheit in der Informationstechnik* 2016, S. 30.

ver Zugriff auf retrograde Standortdaten seitens der Ermittlungsbehörden faktisch nicht möglich ist.

3.1.2.1 Repressive Rechtsgrundlagen

Inhaltsüberwachung

Die repressive Rechtsgrundlage der Telekommunikationsüberwachung findet sich in den §§ 100a, 100e StPO. Die Anordnung einer Telekommunikationsüberwachung gem. § 100a Abs. 1 StPO kann demnach erfolgen, „[...], wenn es sich bei dem zu kontrollierenden Kommunikationsvorgang um eine Form der Telekommunikation [...] handelt, die einer Überwachung und Aufzeichnung [...] zugänglich ist, sofern als eigentliche Voraussetzungen ein bestimmter Tatverdacht für eine Katalogtat [...], die auch im Einzelfall schwer wiegt [...], vorliegt und der Subsidiaritätsgrundsatz [...] einer solchen Zwangsmaßnahme nicht entgegen steht."[38] Unter dem Begriff der Telekommunikation werden, neben den hier zurede stehenden Nachrichten- oder Gesprächsinhalten, ebenso sämtliche „[...] mit dem Aussenden, Übermitteln oder Empfangen verbundene Vorgänge [...]"[39] subsummiert. Ebenso umfasst der Begriff der Telekommunikation i. S. d. § 100a Abs. 1 StPO „[...] alle modernen Formen der Datenkommunikation [...]."[40] Die seit dem 01.01.2008 in den § 100a Abs. 1 S. 1 StPO aufgenommene Formulierung „auch ohne Wissen des Betroffenen" verdeutlicht die Heimlichkeit der Maßnahme. Ab dem Jahre 1989 wurde zudem die Formulierung „Aufnahme auf einem Tonträger" schlicht durch „überwacht und aufgezeichnet" ersetzt, was die Speicherung der überwachten Telekommunikation auf sämtlichen aktuellen und ggf. in Zukunft verfügbaren Datenträgern ermöglichte.[41] § 100a Abs. 1 Nr. 1 StPO schreibt einen durch bestimmte Tatsachen konkretisierten Tatverdacht für das Vorliegen einer in Abs. 2 bezeichneten Katalogtat vor. Mit der ebenfalls am 01.01.2008 aufgenommenen Formulierung „schwere Straftat" hinsichtlich der Katalogtat, wurde eine Abgrenzung des § 100a StPO zum einen zu dem eingriffsintensiveren „Großen Lauschangriff" gem. § 100c StPO vorgenom-

[38] *Bär* 2010, Rn. 8.
[39] *Bär* 2010, Rn. 10.
[40] *Bär* 2010, Rn 11.
[41] Vgl. *Bär* 2010, Rn. 15.

men, in dem eine „besonders schwere Straftat“ gefordert wird. Zum anderen wurde eine Abgrenzung zu der weniger eingriffsintensiven Verkehrsdatenerhebung gem. § 100g Abs. 1 S. 1 Nr. 1 StPO vorgenommen, in der nur eine „Straftat von erheblicher Bedeutung“ gefordert wird.[42]

Bei dem für die Anordnung einer Maßnahme nach § 100a StPO erforderlichen Tatverdacht hinsichtlich der in Abs. 2 bezeichneten schweren Straftat handelt es sich weder um einen dringenden Tatverdacht i. S. d. § 112 StPO, noch um einen hinreichenden Tatverdacht i. S. d. § 203 StPO. Es genügt vielmehr ein einfacher Tatverdacht, der auf bestimmten Tatsachen beruhen muss.[43] Bei diesen Tatsachen handelt es sich um schlüssige Aspekte der inneren und äußeren Geschehenswelt. Sie dürfen nicht auf bloßen Vermutungen beruhen. Jedoch kann die kriminalistische Erfahrung ausreichend sein. Der hinsichtlich dieser Tatsachen vorliegende Verdacht muss zudem nicht unerheblich sein.[44] Im Vergleich zu den sonstigen Verdachtsformen der StPO stellt der Gesetzgeber demnach keine qualifizierten Anforderungen an die notwendige Verdachtsform der TKÜ, sondern beschränkt die Möglichkeit der Durchführung der Überwachung auf das Vorliegen von Verdachtsmomenten hinsichtlich bestimmter, besonders gravierender Taten.

Gem. § 100a Abs. 1 Nr. 2 StPO muss die in Abs. 2 bezeichnete Katalogtat auch im Einzelfall schwer wiegen. Hiermit soll sichergestellt werden, dass solche Fälle ausgeschieden werden, in denen zwar eine Katalogstraftat vorliegt, diese jedoch mangels hinreichender Schwere im konkreten Einzelfall einen Eingriff in das Fernmeldegeheimnis durch TKÜ-Maßnahmen nicht zu rechtfertigen vermag.[45]

In § 100a Abs. 1 Nr. 3 StPO findet sich zudem noch die sog. Subsidiaritätsklausel. Diese besagt, dass die Ermittlung des Sachverhalts oder des Aufenthaltsorts des Beschuldigten auf andere Art und Weise aussichtslos oder wesentlich erschwert sein müsste. Das bedeutet, dass andere Ermittlungsmethoden weniger erfolgversprechend sein müssen, als der Einsatz einer

---

[42] Vgl. *Bär* 2010, Rn. 16.

[43] Vgl. OLG Hamm, NStZ 2003, 279.

[44] Vgl. *Krüpe-Gescher* 2005, S. 21; BGHSt 41,30, 33.

[45] Vgl. BT-Drs. 16/5846, S. 40.

TKÜ. Demnach muss der Eingriff in die Inhalte der Telekommunikation das „letzte Mittel“ sein.[46]

Im Jahre 2017 wurde – wie bereits zu Beginn dieser Arbeit kurz skizziert – der § 100a Abs. 1 StPO durch die Sätze 2 und 3 ergänzt. Hierdurch wurde eine Rechtsgrundlage für den Einsatz der Quellen-TKÜ und die damit einhergehende Möglichkeit zur Überwachung verschlüsselter Telekommunikation geschaffen, die im weiteren Verlauf dieser Arbeit näher betrachtet wird.

Mit dem Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 23.08.2017 und der damit ebenso verbundenen Implementierung der sog. Online-Durchsuchung in § 100b StPO, wurde die Anordnungsbefugnis für TKÜ-Maßnahmen nach § 100a StPO nun in § 100e StPO geregelt.[47] § 100e Abs. 1 StPO schreibt vor, dass die Anordnung von TKÜ-Maßnahmen nur durch ein Gericht auf Antrag der Staatsanwaltschaft erfolgen darf. Bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft erfolgen. In diesem Fall muss die Anordnung binnen drei Werktagen durch ein Gericht bestätigt werden um nicht außer Kraft zu treten. Der sog. Richtervorbehalt hat nach Ansicht des Bundesverfassungsgerichts (BVerfG) den Nutzen “[...], dass Richter aufgrund ihrer persönlichen und sachlichen Unabhängigkeit und ihrer strikten Unterwerfung unter das Gesetz (Art. 97 GG) die Rechte der Betroffenen am besten und sichersten wahren könnten. Eine vorherige richterliche Mitwirkung sei insbesondere dann sinnvoll oder geboten, wenn Grundrechtseingriffe ohne vorherige Anhörung des Betroffenen stattfänden.“[48] Weiterhin schreibt § 100e StPO in den Abs. 3 und 4 die formellen Voraussetzungen der Anordnung von TKÜ-Maßnahmen vor.

Um den Schutz der Grundrechte der Betroffenen abzusichern, sieht die StPO weitere Regelungen vor. So sind gem. § 100d Abs. 1 StPO TKÜ-Maßnahmen unzulässig, durch die allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung des Betroffenen erlangt werden würden. Die Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die im Rahmen von TKÜ-Maßnahmen erlangt werden, dürfen gem. § 100d Abs. 2 StPO nicht

[46] Vgl. *Bär* 2010, Rn. 24.
[47] BGBl. I 2017, S. 3202 – 3207.
[48] *Gusy* 2003, S. 275.

verwertet werden und sind unverzüglich zu löschen. Kernbereichsrelevante Inhalte können demnach beispielsweise Äußerungen sein, die das Intimleben betreffen oder Ausdrucksformen der Sexualität. Auch Gespräche mit engen Vertrauenspersonen über existentielle Fragen oder private Angelegenheiten werden ebenso wie Seelsorgegespräche oder Beratungsgespräche in Bezug auf Krankheiten unter dem Kernbereich privater Lebensgestaltung subsummiert.[49] Dem Schutz trägt auch § 160a StPO Rechnung, der entsprechend gilt. Die mittels TKÜ aufgezeichneten Gespräche mit in § 53 StPO genannten Personen sind unverzüglich zu löschen. In der Praxis sind hier oft Gespräche des von TKÜ-Maßnahmen Betroffenen mit dessen Rechtsanwalt von Relevanz. Verfügt der Rechtsanwalt gem. § 53 Abs. 1 S. 1 Nr. 2 StPO über ein Zeugnisverweigerungsrecht bezüglich seines Mandanten, sind dahingehend aufgezeichnete Telefongespräche nicht verwertbar und unverzüglich zu löschen.[50]

§ 101 StPO regelt die Unterrichtung des Betroffenen über bei ihm durchgeführte TKÜ-Maßnahmen. Demnach sind die Betroffenen grundsätzlich über bei ihnen durchgeführte TKÜ-Maßnahmen zu benachrichtigen, sobald dies den Untersuchungszweck nicht mehr gefährdet. Von dieser Benachrichtigung kann unter Umständen abgesehen werden. Wenn länger als zwölf Monate von der Benachrichtigung der Betroffenen abgesehen werden soll, muss ein Gericht über die weitere Dauer des Absehens von der Benachrichtigung entscheiden. Durch die Benachrichtigung erhält der Betroffene die Möglichkeit, die bei ihm durchgeführten TKÜ-Maßnahmen nachträglich auf ihre Rechtmäßigkeit hin überprüfen zu lassen.

Gem. § 101b Abs. 1 StPO haben die Länder und der Generalbundesanwalt zudem dem Bundesamt für Justiz (BfJ) über durchgeführte Maßnahmen gem. § 100a StPO zu berichten. Eine aufgrund dieser Daten erstellte Statistik wird jährlich durch das BfJ auf dessen Internetpräsenz veröffentlicht.

---

[49] Vgl. *Keller / Braun / Hoppe* 2015, S. 37.

[50] BGH, NJW 2014, 1314 – 1316.

Verkehrs- und Standortdaten gem. § 100g StPO

§ 96 Abs. 1 TKG bestimmt, dass der Telekommunikationsdiensteanbieter die folgenden Verkehrsdaten speichern darf, sofern dies für Abrechnungszwecke oder zur Aufrechterhaltung der Telekommunikation notwendig ist. Hierzu zählen die Nummer oder Kennung der beteiligten Anschlüsse, personenbezogene Berechtigungskennungen, Kartennummern von Kundenkarten und bei mobilen Anschlüssen auch die Standortdaten. Außerdem zählen Beginn und Ende der jeweiligen Daten- oder Telefonverbindung nach Datum und Uhrzeit, sowie der vom Nutzer in Anspruch genommene Telekommunikationsdienst und sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation notwendige Daten zu den Verkehrsdaten.

Im Gegensatz zu diesen freiwillig und zu Geschäftszwecken gespeicherten Daten verpflichtet § 113b TKG die Diensteanbieter klar definierte Verkehrs- und Standortdaten für einen vorgegebenen Zeitraum zu speichern. Demnach müssen die Anschlusskennungen der Teilnehmer, Datum und Uhrzeit des Gesprächsbeginns und -endes, Angaben zum genutzten Dienst, bei mobilen Telefondiensten die internationale Kennung der beteiligten Anschlüsse und Endgeräte, das Datum und die Uhrzeit der Aktivierung des genutzten Dienstes, sowie bei Internet-Telefondiensten die IP-Adressen der beteiligten Anschlüsse für zehn Wochen gespeichert werden. Auch die Versende- und Empfangszeit von Kurz-, Multimedia- oder ähnlichen Nachrichten, Anwahlversuche und – im Falle von Internetzugangsdiensten – die dem Teilnehmer zugewiesene IP-Adresse, die eindeutige Benutzerkennung des Anschlusses, sowie Datum und Uhrzeit des Beginns und des Endes der Internetnutzung sind für zehn Wochen zu speichern.

§ 113b Abs. 4 TKG schreibt dem Diensteanbieter zudem vor, dass – bei mobiler Telefonie oder Internetnutzung – die genaue Bezeichnung der genutzten Funkzelle, deren geografische Position und die Hauptstrahlrichtungen der Funkantennen in der jeweiligen Funkzelle gespeichert werden müssen. Die Speicherung dieser sog. Standortdaten muss gem. § 113b Abs. 1 Nr. 2 TKG für vier Wochen erfolgen.

Aufgrund der deutlich unterschiedlich gewichteten Eingriffe in die Rechte der Betroffenen (§ 96 TKG: freiwillige Möglichkeit zur Speicherung von Daten zu

Geschäftszwecken durch die Dienstenanbieter; § 113b TKG: Verpflichtung der Diensteanbieter zur Speicherung klar definierter Verbindungs- und Standortdaten für einen vorgegebenen Zeitraum) wurde die sog. Vorratsdatenspeicherung in mehreren höchstrichterlichen Entscheidungen auf Bundes- und Europaebene thematisiert. So hat der Europäische Gerichtshof (EuGH) in einem Urteil vom 08.04.2014 die Ungültigkeit der Richtlinie zur Vorratsdatenspeicherung festgestellt.[51] Die durch den EuGH gestellten Anforderungen an eine europarechtskonforme Auslegung zur Vorratsdatenspeicherung decken sich weitestgehend mit der Argumentation des BVerfG in seinem Urteil vom 02.03.2010.[52]

Um weiterhin die Möglichkeiten der Vorratsdatenspeicherung bei einer effektiven und effizienten Strafverfolgung nutzen zu können, war der Gesetzgeber aus o. g. Gründen nun gezwungen, den § 100g StPO in der bis dahin gültigen Fassung grundlegend zu ändern. Dies erfolgte sodann am 10.12.2015 mit dem Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten.[53] Beachtlich ist, dass es sich nun jeweils bei § 100g Abs. 1, 2 und 3 um eigenständige Normen mit einer vollkommen unterschiedlichen Zielrichtung handelt.

§ 100g Abs. 1 StPO zielt nun auf die Erlangung der zu Geschäftszwecken gespeicherten Verkehrsdaten (§ 96 TKG) ab. Wie in der vorherigen Fassung des § 100g StPO wird hier ein aufgrund bestimmter Tatsachen vorliegender Verdacht hinsichtlich einer Straftat von erheblicher Bedeutung gefordert. Wie in den Ausführungen zu § 100a StPO bereits dargelegt, sind Straftaten von erheblicher Bedeutung niederschwelliger anzusetzen als die in § 100a StPO geforderten schweren Straftaten. Der erforderliche Grad des Tatverdachts korrespondiert jedoch mit dem in den Ausführungen zu § 100a StPO dargestellten Tatverdacht. Gem. § 100g Abs. 1 S. 1 Nr. 2 StPO reicht es jedoch ebenfalls aus, dass der genannte Tatverdacht hinsichtlich einer mittels Telekommunikation begangen Straftat vorliegt. Diese muss – der Formulierung folgend – nicht von erheblicher Bedeutung sein.

---

[51] EuGH, NJW 2014, 2169.

[52] BVerfG, NJW 2010, 833; vgl. *Graf* 2018, S. 493 – 494, Rn. 1.

[53] BGBl. I 2015, S. 2218 – 2228.

§ 100g Abs. 1 StPO erlaubt demnach nur auf die in § 96 TKG genannten, zu Geschäftszwecken durch die Diensteanbieter gespeicherten, Daten zuzugreifen. S. 3 schränkt zudem den Zugriff auf die Standortdaten der Betroffenen weiter ein. Es wird nur der Zugriff auf künftig anfallende oder in Echtzeit abgerufene Standortdaten erlaubt. Die Erlangung von retrograden, nach § 96 TKG gespeicherten, Standortdaten ist damit rechtlich mit dieser Ermächtigungsgrundlage nicht mehr möglich.

Bei Maßnahmen nach § 100g Abs. 1 S. 1 Nr. 2 StPO wurde in S. 3 eine verschärfte Subsidiaritätsklausel integriert, die analog der in den Ausführungen zu § 100a StPO dargestellten Subsidiaritätsklausel zu verstehen ist.

Der Adressat einer derartigen Maßnahme findet sich nun in § 101a StPO. Abs. 1 verweist auf § 100a Abs. 3 StPO, der vorgibt, dass sich auch Maßnahmen nach § 100g StPO nur gegen Beschuldigte und Nachrichtenmittler richten dürfen.

§ 100g Abs. 2 StPO legt nun fest, unter welchen Voraussetzungen die nach § 113b TKG gespeicherten Verkehrs- und Standortdaten erhoben werden dürfen. Vor allem mit der Einführung dieser Norm setzt der Gesetzgeber die bereits erwähnten Vorgaben hinsichtlich der Vorratsdatenspeicherung des EuGH und des BVerfG um.[54]

Um seitens der Ermittlungsbehörden Zugriff auf die nach § 113b TKG gespeicherten Verbindungs- und Standortdaten zu erhalten ist nunmehr ein aufgrund bestimmter Tatsachen bestehender Verdacht hinsichtlich einer „besonders schweren Straftat“ erforderlich. Diese besonders schweren Straftaten sind abschließend in dem ebenfalls in § 100g Abs. 2 StPO befindlichen Straftatenkatalog aufgeführt. Beachtlich erscheint in diesem Zusammenhang, dass Abs. 1 lediglich eine Straftat von erheblicher Bedeutung fordert, wohingegen Abs. 2 nicht nur eine schwere Straftat, sondern nunmehr eine besonders schwere Katalogtat fordert. Der Straftatenkatalog des § 100g Abs. 2 StPO und die geforderte Schwere der zugrundeliegenden Straftat orientieren sich damit an der sehr eingriffsintensiven Maßnahme der akustischen Wohnraumüberwachung gem. § 100c StPO[55], was vor diesem Hinter-

[54] Vgl. *Graf* 2018, S. 503 – 504, Rn. 27.

[55] Vgl. *Graf* 2018, S. 504, Rn. 31.

grund beachtlich erscheint und die durch den Gesetzgeber angenommene Eingriffsintensität von Maßnahmen nach § 100g Abs. 2 StPO aufzeigt.

§ 100g Abs. 3 StPO bestimmt, unter welchen Voraussetzungen eine Funkzellenabfrage durchgeführt werden darf. Eine Funkzellenabfrage ist dabei von der Abfrage von Standortdaten abzugrenzen.

Bei der Funkzellenabfrage geht es darum, sämtliche Verkehrsdaten, die innerhalb eines bestimmten Zeitraums in einer festgelegten Funkzelle angefallen sind, festzustellen und somit in Erfahrung zu bringen, welche Mobiltelefone sich zu diesem Zeitpunkt im Wirkungsbereich der Funkzelle befunden haben.[56]

Für eine derartige Funkzellenabfrage bedarf es nach § 100g Abs. 3 StPO drei Eingriffsvoraussetzungen. Diese müssen kumulativ vorliegen. Zunächst muss gem. Nr. 1 – wie in § 100g Abs. 1 StPO – eine Straftat von erheblicher Bedeutung vorliegen. Gem. Nr. 2 muss die Verhältnismäßigkeit gewahrt bleiben. Nr. 3 stellt erneut eine an § 100a StPO angelehnte Subsidiaritätsklausel dar. Dem Gesetzeswortlaut nicht zu entnehmen – dennoch nötig – ist es, dass zudem tatsächliche Anhaltspunkte dafür vorliegen müssen, dass sich der Beschuldigte oder Nachrichtenmittler in der abgefragten Funkzelle zum Abfragezeitpunkt aufgehalten hat.[57]

Da durch eine derartige Maßnahme selbstverständlich nicht nur die Verbindungsdaten der Beschuldigten oder Nachrichtenmittler in der entsprechenden Funkzelle übermittelt werden, sondern vielmehr die Daten aller Teilnehmer, die zum abgefragten Zeitpunkt in eben dieser Funkzelle eingeloggt waren, wird bei der Anordnung dieser Maßnahme ein erhöhtes Augenmerk auf die Verhältnismäßigkeit gelegt. Demgemäß fordert auch § 101a Abs. 1 S. 3 StPO, dass bei Funkzellenabfragen „eine räumlich und zeitlich eng begrenzte und hinreichend bestimmte Bezeichnung der Telekommunikation“ stattzufinden hat.

Gem. § 100g Abs. 4 StPO sind – analog zu den obigen Ausführungen zu § 100a StPO – Verkehrsdaten, die Erkenntnisse erbringen würden, über die

---

[56] Vgl. *Graf* 2018, S. 507, Rn. 39.

[57] LG Dortmund Beschl. v. 23.02.2016 – 36 Qs-121 UJs 60/16-25/16; AG Dortmund Beschl. v. 06.01.2016 – 701 Gs 18/16, 701 Gs – 520 Js 1/16 – 18/16; vgl. *Graf* 2018, S. 508, Rn. 42.

eine zeugnisverweigerungsberechtigte Person (§ 53 Abs. 1 S. 1 Nr. 1 - 5 StPO) das Zeugnis verweigern dürfte, nicht verwertbar (z. B. Verkehrsdaten zu Gesprächen mit bestelltem Verteidiger).

§ 100g Abs. 5 StPO stellt klar, dass nach Abschluss des Kommunikationsvorgangs die Regelungen des § 100g StPO keine Anwendung mehr finden. Vielmehr richten sich die Sicherung von Kommunikationsdaten nach abgeschlossener Telekommunikation nach den §§ 94 ff. StPO. In der Regel dürfte es sich hierbei um Verbindungsdaten auf zur Beweissicherung sichergestellten oder beschlagnahmten Mobiltelefonen handeln.[58]

Die Anordnung von Maßnahmen nach § 100g StPO ist gem. § 101a Abs. 1 StPO in § 100e StPO geregelt. Demnach erfolgt die Anordnung analog zu Maßnahmen nach § 100a StPO. § 101a Abs. 1 S. 2 StPO beinhaltet jedoch zudem die Besonderheit, dass Maßnahmen nach § 100g Abs. 2 und 3 StPO (Vorratsdatenspeicherung) auch bei Gefahr im Verzug nicht durch die Staatsanwaltschaft angeordnet werden dürfen.

§ 101a StPO beinhaltet weitere Regelungen zur Verwendung, Weitergabe und Löschung der erlangten Daten. Gem. § 101a Abs. 6 StPO ist die von einer Maßnahme nach § 100g StPO betroffene Person von der Maßnahme zu unterrichten. Die Unterrichtung des Betroffenen kann nur unter bestimmten Umständen durch das Gericht zurückgestellt werden.

Durch die Reform des § 100g StPO hat der Gesetzgeber die ursprüngliche Konzeption der Verkehrs- und Verbindungsdatenabfrage damit dahingehend geändert, dass es sich nun nicht mehr um eine verdeckte Maßnahme handelt. Dies führt dazu, dass der Betroffene grundsätzlich unverzüglich über die Maßnahme unterrichtet wird. Die durch ein Gericht angeordnete Zurückstellung der Unterrichtung ist – im Gegensatz zur alten Fassung der Norm – nur noch in begründeten Ausnahmefällen möglich.

Rechtliche Problematik: retrograde Standortdaten

Auch wenn der Gesetzgeber hinsichtlich einer europarechtskonformen Auslegung der Vorratsdatenspeicherung tätig geworden ist und § 100g StPO

[58] Vgl. *Graf* 2018, S. 511, Rn. 51.

grundsätzlich neu geregelt hat, besteht aktuell ein schwerwiegendes rechtliches Problem hinsichtlich der repressiven Erlangung retrograder Standortdaten.

Gem. § 150 Abs. 1 S. 1 TKG sind die Diensteanbieter seit dem 01.07.2017 dazu verpflichtet, die Telekommunikationsdaten nach Maßgabe der §§ 113b bis 113e und 113g zu speichern und bereitzustellen. Jedoch bestehen auch nach der Neuregelung des § 100g StPO und des § 113b TKG weiterhin Zweifel an der Rechtmäßigkeit der Vorratsdatenspeicherung in dieser neuen Form. Der EuGH sieht in der Vorratsdatenspeicherung einen schwerwiegenden Eingriff in die in Art. 7 und 8 der in der Charta der Grundrechte der Europäischen Union (GrCH) verankerten Grundrechte auf Achtung des Privat- und Familienlebens und dem Schutz personenbezogener Daten der Unions-Bürger. In Anbetracht dessen erlaube nur der Zweck der Bekämpfung schwerer Kriminalität einen derartigen Eingriff zu rechtfertigen.[59] Die Speicherung sämtlicher anfallender Verkehrsdaten und die damit einhergehende unterschiedslose Vorratsdatenspeicherung der Verkehrs- und Standortdaten aller Telekommunikationsteilnehmer, auch wenn diese nicht im Entferntesten einen Bezug zur schweren Kriminalität aufweisen, vermöge auch die genannte Zielsetzung (Bekämpfung schwerer Kriminalität) jedoch nicht zu rechtfertigen. Eine pauschale Speicherung sämtlicher Verkehrsdaten, die keinerlei Differenzierung, Einschränkung oder Ausnahme hinsichtlich des verfolgten Ziels vorsieht, sei damit unzulässig.[60] Dieser Sichtweise hat sich das OVG Münster in seinem Beschluss vom 22.06.2017[61] angeschlossen. Da § 113b TKG keinen Zusammenhang sämtlicher gespeicherter Vorratsdaten zu dem durch das Gesetz verfolgten Zweck (Bekämpfung der schweren Kriminalität) erkennen lasse, sondern die Pflicht der Provider, sämtliche dort aufgelistete Telekommunikationsdaten von ausnahmslos jedem Telekommunikationsteilnehmer zu speichern beinhalte, genüge das Gesetz nicht den Anforderungen des EuGH. Demnach müsse der Personenkreis, der von der

[59] EuGH NJW 2017, 717, Rn. 102; vgl. *Scheurle / Mayen* 2018, S. 1168, Rn. 8.
[60] EuGH NJW 2017, 717, Rn. 103, 105, 107; vgl. *Scheurle / Mayen* 2018, S. 1168, Rn. 8.
[61] OVG Münster, Beschl. v. 30.06.2017 – 13 B 238/17.

Vorratsdatenspeicherung betroffenen Personen, einen zumindest mittelbaren Zusammenhang zu schweren Straftaten erkennen lassen.[62]

Durch das BVerfG wurde bereits angekündigt, dieser Thematik im Rahmen des Hauptsacheverfahrens gegen die §§ 113a ff TKG nachzugehen.[63] Die Aussetzung des Vollzugs der §§ 113a und 113b TKG sowie der §§ 100g, 101a und 101b StPO verneinte das BVerfG jedoch mit der Begründung, dass nicht die Speicherung, sondern erst das Abrufen der gespeicherten Daten zu einer irreparablen Grundrechtsbeeinträchtigung führen könne.[64] Trotzdem wird in dem bereits benannten Verfahren des OVG Münster[65] festgestellt, dass die Antragstellerin (ein IT-Unternehmen, das Internetzugangsleistungen für rund 1200 Geschäftskunden aus der EU erbringt) nicht verpflichtet ist, Verkehrsdaten nach Maßgabe des § 113b Abs. 3 TKG zu speichern, bis ein rechtskräftiger Abschluss des dies betreffenden Hauptsacheverfahrens vor dem OVG Münster stattgefunden hat. Diese Entscheidung steht bis dato noch aus.

Obwohl die Regelungen des § 113b TKG zum Teil bußgeldbewehrt sind und gem. § 149 Abs. 1 Nr. 36 TKG derjenige (Diensteanbieter) ordnungswidrig handelt, der nicht sicherstellt, dass die in § 113b Abs. 1 i. V. m. § 113a Abs.1 S. 2 TKG genannten Daten gespeichert werden oder nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig mitgeteilt werden und eine derartige Ordnungswidrigkeit gem. § 149 Abs. 2 Nr. 1 TKG mit einer Geldbuße von bis zu 500.000 Euro durch die Bundesnetzagentur (BNetzA) geahndet werden kann, setzte diese aufgrund des Urteils des OVG Münster die Umsetzung der Vorratsdatenspeicherung i. S. d. § 113b TKG aus.[66] Die Aussetzung der Regelungen zur Vorratsdatenspeicherung soll zudem bis zum rechtskräftigen Abschluss des Hauptsacheverfahrens Bestand haben.[67] Damit besteht die unbefriedigende Lage, dass eine gesetzliche Speicherfrist für die TK-Diensteanbieter besteht, die übergeordnete Behörde (BNetzA) – aufgrund der Bedenken des OVG Münster – im Rahmen ihres Ermessensspiel-

---

[62] Vgl. *Scheurle / Mayen* 2018, S. 1169, Rn. 14.
[63] BVerfG NVwZ 2016, 1240, Rn. 26.
[64] BVerfG NVwZ 2016, 1240, Rn. 18, 26; vgl. *Scheurle / Mayen* 2018, S. 1169, Rn. 15.
[65] OVG Münster, Beschl. v. 30.06.2017 – 13 B 238/17.
[66] Vgl. *Greis* 2017.
[67] Vgl. *Greis* 2017.

raums von der bußgeldbewehrten Ahndung von Verstößen absieht, weshalb sich die TK-Diensteanbieter nicht gehalten fühlen, die Speicherung und Übermittlung der Daten vorzunehmen.

Diese Entscheidung hat für die Ermittlungsbehörden in Deutschland weitreichende Folgen. Aufgrund des § 100g Abs. 1 S. 3 StPO ist die Übermittlung von gespeicherten retrograden Standortdaten i. S. d. § 96 Abs. 1 TKG an die Ermittlungsbehörden rechtlich nicht möglich. Durch die Entscheidung der BNetzA, die Regelungen zur Vorratsdatenspeicherung bis auf weiteres auszusetzen, ist es somit ebenfalls nicht möglich, nach Maßgabe des § 100g Abs. 2 StPO, gespeicherte Standortdaten zu erhalten. Folglich besteht seitens der Ermittlungsbehörden im Strafverfahren aktuell keine Möglichkeit, Zugriff auf retrograde Standortdaten der Mobiltelefone von Beschuldigten zu erhalten. Gerade in Zeiten gesteigerter Terrorgefahr erscheint dies höchst problematisch.

Ein derartiger Zustand wird auf Dauer dem grundrechtlichen Anspruch der Bürger auf effektive Strafverfolgung seitens des Staates nicht Genüge tun können. Auch wenn die EU-Kommission bereits für 2017 Leitlinien für die Vorratsdatenspeicherung ankündigte, jedoch diese nicht veröffentlichte, bleibt zu hoffen, dass dies – wie im Arbeitsprogramm der EU-Kommission für 2018 vorgesehen – noch im Jahr 2018 oder zumindest Anfang 2019 passieren wird.[68] Nur so können europarechtskonform sowohl der Grundrechteschutz als auch eine effektive Strafverfolgung in Einklang gebracht werden.

3.1.2.2 Präventive Rechtsgrundlage

Die Bundes- und Landesgesetzgebung beherbergt eine Vielzahl präventiver Rechtsgrundlagen, die die Überwachung der Telekommunikation ermöglichen. Zu nennen wären hier beispielsweise die §§ 23a ff. des Zollfahndungsdienstgesetzes (ZFdG), §§ 8 ff. des Bundesverfassungsschutzgesetzes (BVerfG) und die §§ 1, 3 und 5 des Artikel-10-Gesetzes (G10-Gesetz).

Der Übersicht und des Umfangs halber werden diese Rechtsgrundlagen jedoch in den folgenden Ausführungen nicht berücksichtigt. Die Ausführungen

[68] Vgl. *Wildt* 2018, S. 182.

werden sich auf die präventive TKÜ nach dem hessischen Polizeigesetz (HSOG) beschränken.

Die gefahrenabwehrrechtliche Eingriffsbefugnis zur Überwachung der Telekommunikation und zur Erhebung von Verkehrsdaten wird im Bundesland Hessen in § 15a des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) geregelt. Die Norm weist im Vergleich mit den korrespondierenden repressiven Ermächtigungsgrundlagen gem. §§ 100a, 100g StPO zahlreiche Parallelen hinsichtlich der Möglichkeiten und Voraussetzungen, jedoch auch einige Unterschiede auf.

Gem. § 15a Abs. 1 HSOG können die Polizeibehörden von dem Telekommunikationsdiensteanbieter verlangen, dass dieser ihnen die Kenntnisnahme des Inhalts der Telekommunikation ermöglicht, sowie die näheren Umstände der Telekommunikation einschließlich des Standorts eingeschalteter mobiler Endgeräte übermittelt. Voraussetzung hierfür ist, dass dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person unerlässlich ist. Eine gegenwärtige Gefahr liegt vor, wenn die Einwirkung des schädigenden Ereignisses bereits begonnen hat oder unmittelbar bevorsteht. Eine Gefahr für Leib, Leben oder Freiheit ist eine Gefahr, bei der eine nicht nur leichte Körperverletzung, der Tod oder der Verlust der Freiheit zu befürchten ist.[69] Bei der geforderten Gefahr handelt es sich zudem um eine konkrete Gefahr. Eine konkrete Gefahr liegt dann vor, wenn im konkreten Einzelfall mit hinreichender Wahrscheinlichkeit in naher Zukunft mit dem Schadenseintritt gerechnet werden kann.[70]

Bei dem der präventiven TKÜ zugrundeliegenden Gefahrenbegriff handelt es sich um einen hochrangigen gegenwärtigen Gefahrenbegriff. Nur wenn hohe Rechtsgüter konkret und akut gefährdet werden, ist die Anordnung einer TKÜ nach § 15a HSOG möglich.

§ 15a Abs. 1 S. 2 HSOG verweist zudem auf § 15 Abs. 4 S. 2 bis 5 HSOG. In diesem ist analog zu § 100d Abs. 1 StPO der Schutz des Kernbereichs privater Lebensführung geregelt. Eine präventive TKÜ, durch die ausschließlich kernbereichsrelevante Erkenntnisse erlangt werden würden, ist demnach

[69] Vgl. *Meixner / Fredrich* 2016, S. 55.
[70] Vgl. *Meixner / Fredrich* 2016, S. 53.

nicht zulässig. Im Vergleich zu § 100d Abs. 2 StPO, in dem festgelegt ist, dass diese Maßnahmen nicht verwertbar und unverzüglich zu löschen sind, schreibt § 15 Abs. 4 S. 8 HSOG jedoch vor, dass eine Datenerhebung – bei Zweifeln hinsichtlich der Kernbereichsrelevanz – ausschließlich durch eine automatische (Fortsetzung der) Aufzeichnung durchgeführt werden darf. Diese automatische Aufzeichnung kann damit so lange erfolgen, bis eine Entscheidung über die Kernbereichsrelevanz der Inhalte getroffen wurde.

§ 15a Abs. 2 HSOG lässt unter denselben Voraussetzungen, unter denen eine präventive TKÜ durchgeführt werden kann, auch die präventive Erhebung von beim Provider gespeicherten Verkehrsdaten zu. Durch das Gesetz zur Änderung des HSOG und anderer Gesetze vom 14.12.2009[71] wurde § 15a Abs. 2 HSOG an § 100g Abs. 1 StPO angepasst.[72] So ist nach der präventiven Eingriffsbefugnis ebenfalls nur ein Zugriff auf Verkehrsdaten gem. § 96 Abs. 1 TKG (beim Diensteanbieter zu Geschäftszwecken gespeicherte Daten) zulässig. Entgegen § 100g Abs. 1 S. 3 StPO verbietet § 15a Abs. 2 HSOG jedoch nicht ausdrücklich den Zugriff auf retrograde Standortdaten i. S. d. § 96 Abs. 1 S. 1 Nr. 1 TKG, sodass diese seitens des Diensteanbieters ebenfalls herausgegeben werden müssen.

Ein in einer vorherigen Fassung des HSOG geregelter Zugriff auf Verkehrsdaten, die gem. § 113b TKG (Vorratsdatenspeicherung) durch die Diensteanbieter verpflichtend gespeichert und herausgegeben werden mussten, wurde im Rahmen der bereits thematisierten Verfassungswidrigkeit dieser Vorgehensweise mit dem Gesetz zur Änderung des HSOG und des LfV-Gesetzes vom 27.06.2013[73] gestrichen.

Mit der bereits thematisierten Neuregelung des § 100g StPO durch das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10.12.2015[74] und der erneuten bundesgesetzlichen Regelung zur Vorratsdatenspeicherung ist auch auf der gefahrenabwehrrechtlichen Seite jedoch aktuell ebenfalls kein Zugriff auf im Rahmen der Vorratsdatenspeicherung erhobene Verkehrsdaten möglich. Dies ist der Fall, da

---

[71] LT-Drs. 18/861 und 18/1604.

[72] Vgl. *Meixner / Fredrich* 2016, S. 46.

[73] LT-Drs. 18/7137 und 18/7553.

[74] BGBl. I 2015, S. 2218 – 2228.

gem. § 113c Abs. 1 Nr. 2 TKG für eine Übermittlung der Daten an die Gefahrenabwehrbehörden der Länder eine gesetzliche Bestimmung verlangt wird. In der aktuellen Fassung verfügt das HSOG über eine solche jedoch nicht.

§ 15a Abs. 2 HSOG regelt zudem die präventive Bestandsdatenauskunft analog zu § 100j StPO i. V. m. § 113 TKG was an dieser Stelle – aufgrund des begrenzten Umfangs dieser Arbeit und weil es sich bei diesen Daten nicht um Daten handelt, die einem konkreten Telekommunikationsvorgang zugeordnet werden können – nicht weiter thematisiert wird. Auch auf § 15a Abs. 3 HSOG, bei dem es sich um die präventive Rechtsgrundlage zum Einsatz eines IMSI-Catchers (analog § 100i StPO) handelt, wird aus den genannten Gründen nicht näher eingegangen.

Eine Besonderheit stellt § 15a Abs. 4 HSOG dar. Dieser gestattet den Polizeibehörden unter den genannten Voraussetzungen den Eingriff in die Telekommunikation in der Form, dass er die Unterbrechung einer Telekommunikationsverbindung mit eigenen technischen Mitteln erlaubt. In der Praxis kann die Störung einer Funkfrequenz beispielsweise dazu verwendet werden, die Zündung von Sprengstoff mittels eines Mobiltelefons zu verhindern.[75] Eine Inanspruchnahme des Diensteanbieters zu dem genannten Zweck sieht die Norm jedoch nicht vor.

Die Anordnungsbefugnis für Maßnahmen nach den genannten Absätzen 1 bis 4 ergibt sich aus § 15a Abs. 5 HSOG. Demnach ist für die Anordnung dieser Maßnahmen das Amtsgericht zuständig, in dessen Bezirk die ersuchende Polizeibehörde ihren Sitz hat. Aufgrund der Verweisungen gelten zudem die Voraussetzungen der §§ 39 Abs. 1 und 15 Abs. 5 HSOG. Diese beinhalten die Formvorschriften für die Anordnung (schriftlich, genaue Bezeichnung des Adressaten der Maßnahme und Anordnungsdauer). Die Polizeibehörde kann bei Gefahr im Verzug die o. g. Maßnahmen selbst anordnen. In diesem Fall muss jedoch unverzüglich eine richterliche Bestätigung dieser Anordnung erfolgen.

Eine Verwertung von präventiv durch TKÜ-Maßnahmen oder Verkehrsdaten erlangten Erkenntnissen zu repressiven Zwecken ist grundsätzlich möglich.

[75] Vgl. *Meixner / Fredrich* 2016, S. 165.

§ 15a Abs. 6 HSOG verweist dazu auf § 163 StPO und andere bundesrechtliche Übermittlungspflichten.

Die speziellere Norm findet sich bezüglich präventiv erlangter TKÜ-Erkenntnisse in § 161 Abs. 2 S. 1 StPO. Die präventiv erlangten Daten können demnach nur zur Aufklärung einer in § 100a Abs. 2 StPO aufgeführten Katalogstraftat herangezogen werden.[76] Auch für die Verwertung präventiv erlangter Verkehrsdaten nach Maßgabe des § 96 Abs. 1 TKG wird auf § 161 Abs. 2 S. 1 StPO zurückgegriffen.[77]

Eine Verwendung präventiv erlangter Verkehrsdaten nach Maßgabe des § 113b TKG richtet sich nach § 101a Abs. 5 StPO. Im vorliegenden Fall ist dies – wie bereits beschrieben – aufgrund der diesbezüglich fehlenden Regelungen im HSOG jedoch hinfällig.

3.2 Verschlüsselte Telekommunikation

Nachdem nun die repressiven und am Beispiel Hessens die nach dem Hessischen Sicherheits- und Ordnungsgesetz geltenden präventiven Rechtsgrundlagen der Telekommunikationsüberwachung dargestellt und problematisiert wurden, werden in diesem Abschnitt moderne internetbasierte Telekommunikationsformen detailliert betrachtet.

In der Vergangenheit stellte vor allem die Überwachung der mobilen Telekommunikation ein Problem für die Strafverfolgungs- und Gefahrenabwehrbehörden dar. Das Problem bestand weniger darin, die Inhalte der Telekommunikation mittels Mobiltelefons zu überwachen. Vielmehr wurden die Ermittlungen dadurch erschwert, dass es in Deutschland keine Ausweispflicht beim Erwerb von im Voraus bezahlten Mobilfunkdienstleistungen gab. Hierdurch war es faktisch jedem möglich, anonym sog. Prepaid-Karten (im Voraus bezahlte SIM-Karten) zu erwerben. Die Ermittlung des Anschlussnutzers war damit in erheblichem Maße erschwert. So war es auch Kriminellen bis dato möglich, eine SIM-Karte anonym zu erwerben, mit dieser einen Anruf zu tätigen und sich dann der SIM-Karte zu entledigen. Aufsehen erregt

[76] Vgl. *Graf* 2018, S. 423 – 424, Rn. 188.
[77] Vgl. *Graf* 2018, S. 555 – 556, Rn. 22.

hat diesbezüglich ein Fall, in dem auf den Namen eines obdachlosen Ungarn 200.000 SIM-Karten gekauft und registriert wurden. Diese SIM-Karten konnten teilweise bei den erschossenen Terroristen nach den Anschlägen von Paris und Brüssel in den Jahren 2015 und 2016 aufgefunden werden.[78]

Mit dem Erlass des Gesetzes zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus[79] am 29.07.2016 reagierte der Gesetzgeber auf diesen Umstand: In § 111 TKG wurde die Pflicht zur Vorlage und Überprüfung eines Ausweisdokuments zur Freischaltung von im Voraus bezahlten Mobilfunkdiensten implementiert.[80] Auch wenn diese Regelung die Weitergabe von SIM-Karten nicht unterbinden wird, bleibt zu hoffen, dass die Ermittlungen hinsichtlich entsprechender Anschlussnutzer hierdurch in Zukunft erleichtert werden.

In jedem Fall bleibt festzuhalten, dass hier durch den Gesetzgeber – wenn auch reichlich spät (entsprechende Vorschriften wurden in der Schweiz bereits im Jahre 2004 erlassen) – eine Problematik erkannt und auf diese reagiert wurde. Eine ähnliche, wenn auch deutlich schwerwiegendere Problematik, ist Gegenstand der nachfolgenden Ausführungen.

Im Nachgang der terroristischen Anschläge von Paris konnte in unmittelbarer Nähe des Tatorts Bataclan in einem Mülleimer ein weißes Samsung-Smartphone aufgefunden werden, das zweifelsfrei den Attentätern zugeordnet werden konnte. Die ausgelesenen Daten gaben den Ermittlern viele Hinweise auf die Vorgehensweise der Terroristen. So konnte festgestellt werden, dass etwa sieben Stunden vor den Anschlägen die App „Telegram“ auf dem Smartphone installiert wurde.[81] Telegram wird auf der Website des Herstellers[82] mit den Worten „Telegram is a cloud-based mobile and desktop messaging app with a focus on security and speed” beworben. Dieser Slogan zeigt, dass der Fokus der App vorwiegend auf der Sicherheit der übermittelten Kommunikation liegt. Die Website des Herstellers enthält weiterhin

[78] Vgl. *Kuhn* 2017.
[79] BGBl. I 2016, S. 1818.
[80] Vgl. *Scheurle / Mayen* 2018, S. 1157, Rn. 14ff.
[81] Vgl. *Flade* 2016.
[82] *https://core.telegram.org* (besucht am 31.10.2018).

detaillierte Informationen zu der von Telegram genutzten Ende-zu-Ende-Verschlüsselung.

Eben diese Verschlüsselung stellt die Sicherheitsbehörden vor eine große Herausforderung. Hierdurch ist – wie bei den anonym erworbenen SIM-Karten – zum einen der Absender der Nachricht anonym. Zum anderen – und das ist das wesentlich schwerwiegendere Problem – lässt sich auch der Inhalt der Nachrichten nicht ohne weiteres überwachen.

3.2.1 Begriffserklärungen

Als Grundlage für die weiteren Betrachtungen, werden zunächst zwei essentielle Begriffe im Zusammenhang mit der verschlüsselten Telekommunikation erläutert.

3.2.1.1 Voice-over-IP-Telefonie

Der Begriff der Voice-over-IP-Telefonie (VoIP-Telefonie) wird häufig synonym zu den Begriffen IP-Telefonie und Internettelefonie gebraucht.[83] Im Gegensatz zur herkömmlichen Telefonie, die durch ein Endgerät akustische in elektronische Signale umwandelt und diese mithilfe einer leitungsvermittelten, stehenden Verbindung zwischen den Gesprächspartnern herstellt, funktioniert die Voice-over-IP-Telefonie paketbasiert.[84] Das bedeutet, dass die gesprochene Information in viele einzelne Datenpakete aufgeteilt und über das Internet oder ein Netzwerk vom Sender zum Empfänger übertragen wird.[85] Aufgrund von Latenzzeiten (unterschiedlich lange Übertragungsdauer der einzelnen Pakete vom Sender zum Empfänger) erfolgt zunächst eine Zwischenspeicherung, bevor die Datenpakete in der richtigen Reihenfolge auf dem Endgerät des Empfängers wieder zusammengesetzt und als akustische Signale ausgegeben werden.[86] Diese Form der internetbasierten Sprachtelefonie kann sowohl über mit dem Internet verbundene Festnetztele-

[83] Vgl. *Klöppner* 2007, S. 2.
[84] Vgl. *Klöppner* 2007, S. 11 – 12.
[85] Vgl. *Klöppner 2007,* S. 12.
[86] Vgl. *Liebig* 2005, S. 124.

fone, als auch über Computer und Smartphones erfolgen.[87] Dieser Aspekt zeigt auch den großen Vorteil der VoIP-Telefonie für den Nutzer. Der Nutzer muss sich – im Gegensatz zur herkömmlichen drahtgebundenen bzw. analogen Telefonie – nicht an seinem Wohnort aufhalten. Er kann sich an jedem Punkt in der Welt befinden, an dem eine Verbindung mit dem Internet hergestellt werden kann, und ist trotzdem über eine normale deutsche Festnetztelefonnummer erreichbar.[88]

3.2.1.2 Messengerdienste

Neben der internetbasierten Sprachtelekommunikation existiert eine weitere zentrale Art der Telekommunikation in der modernen Gesellschaft. Mit dem Versenden der ersten SMS im Jahre 1992 zog die handyvermittelte schriftliche Telekommunikation in den Alltag der Gesellschaft ein.[89] Das Versenden und Empfangen mobiler Kurznachrichten nimmt vor allem bei Nutzern von Mobiltelefonen eine zentrale Rolle ein. Durch den technischen Fortschritt und die weite Verbreitung internetfähiger Smartphones wurde die textbasierte Telekommunikation jedoch stets erweitert. Mit modernen Messengerdiensten wie Telegram, Threema, Viber, WhatsApp und co. ist es heutzutage nicht nur möglich, mobil Textnachrichten zu versenden. Diese Dienste bieten darüber hinaus eine Vielzahl an weiteren Möglichkeiten zur Telekommunikation. So ist es möglich, Gruppenchats einzurichten, sowie Bilder, Videos und Audiodateien zu versenden.[90] Darüber hinaus wurden einige Messengerdienste erweitert, sodass diese ebenfalls Funktionen zur internetbasierten Audio- und Videotelefonie bieten. Dieser Aspekt lässt die Grenzen zwischen der Internettelefonie und den Messangerdienste weiter verschwimmen.

[87] Vgl. *Liebig* 2005, S. 124.
[88] Vgl. *Klöppner* 2007, S. 26.
[89] Vgl. *König / Bahlo* 2014, S. 1.
[90] Vgl. *König / Bahlo* 2014, S. 1.

3.2.2 Darstellung der Funktionsweise an Beispielen

In Zeiten der modernen keyboard-to-screen-Kommunikation[91] eröffnen sich immer neue Möglichkeiten der internetbasierten Telekommunikation. Mittels Apps wie Telegram, Threema, Viber, WhatsApp und co. wird die Telekommunikation paketbasiert über das Internet übertragen. Die einzelnen Paketdaten, die die Kommunikation enthalten, werden zunächst in der Anwendung des Absenders verschlüsselt. In dieser verschlüsselten Form werden sie nun mittels Internet zum Empfänger transportiert. Die Entschlüsselung der Daten erfolgt dann erst auf dem Gerät des Empfängers, sodass die Kommunikation stattfinden kann. Das alles passiert in Bruchteilen von Sekunden. Ein Zugriff auf die übermittelten Daten während des Kommunikationsvorgangs gestaltet sich deshalb schwierig.

Neben dem bereits genannten Messenger-Dienst „Telegramm“ existieren eine Vielzahl weiterer entsprechender Anwendungen. Der Funktionsumfang dieser Anwendungen ist unterschiedlicher Natur. Bei einigen ist lediglich die Kommunikation in Textform, bei anderen lediglich die sprach- bzw. videobasierte Telekommunikation möglich. Daneben wird der Funktionsumfang der einzelnen Anwendung ständig erweitert. So wurde im Laufe der Zeit in Anwendungen, die zunächst nur die textbasierte Kommunikation beherrschten, nach und nach Funktionen zur sprach- und videobasierten Telekommunikation implementiert. Die Verwendung der meisten dieser Anwendungen kann sowohl stationär an einem Computer als auch mobil mittels Tablets, Laptops und Smartphones erfolgen.

Um den Umfang und die Verbreitung internetbasierter Telekommunikationsanwendungen zu veranschaulichen, werden am Beispiel von WhatsApp und Skype die Entstehung, die Nutzerzahlen und die Funktionsweise dieser Dienste dargestellt. Bei WhatsApp und Skype handelt es sich um die bekanntesten und weit verbreitetsten Anwendungen. Diese wurden nicht nur aufgrund ihrer Popularität und der damit ebenfalls einhergehenden Nutzung durch Straftäter, sondern auch aufgrund ihrer unterschiedlichen Funktionsweise in Bezug auf deren Anwendungsbereiche sowie der unterschiedlichen Verschlüsselungsformen ausgewählt.

---

[91] Vgl. *Jucker / Dürscheid* 2012.

3.2.2.1 WhatsApp

Bei dem Messenger-Dienst WhatsApp handelte es sich zunächst um eine Anwendung, die nur die textbasierte Telekommunikation ermöglichte. Im Laufe der Jahre wurde WhatsApp jedoch um ergänzende Funktionen erweitert. So wurde es nach und nach möglich, Bild- und Videodateien zu empfangen und zu senden, Sprach- und Videoanrufe zu tätigen, Statusnachrichten zu erstellen und bereits gesendete Nachrichten im Nachhinein zu löschen.[92]

WhatsApp wurde im Jahr 2009 gegründet. Im Jahre 2014 wurde es für die Rekordsumme von umgerechnet 14 Milliarden Euro an Facebook verkauft. Mit Stand Januar 2018 nutzen ca. 1,5 Milliarden Menschen weltweit WhatsApp.[93]

WhatsApp steht vor allem seit seiner Übernahme durch Facebook immer wieder in der Kritik. Grund hierfür ist der Datenschutz.[94] Dadurch, dass WhatsApp während der Installation die gesamte Kontaktliste des Nutzers einliest und diese Informationen ohne die Zustimmung der jeweiligen Kontakte nutzt, verarbeitet und u. a. an Facebook weitergibt, verstößt die Nutzung des Dienstes in Unternehmen gegen Art. 6 der Datenschutzgrundverordnung (DSGVO). Bei Art. 6 DSGVO handelt es sich um ein „generelles Verbot der Datenweitergabe mit Erlaubnisvorbehalt“[95], das durch diese Praktiken von WhatsApp berührt wird.

Trotzdem erfreut sich der Messenging-Dienst WhatsApp steigender Beliebtheit. Dies wird anhand des nachfolgenden Diagramms anschaulich verdeutlicht.

---

[92] Vgl. *Mühlroth* 2018.

[93] Vgl. *Albers-Heinemann / Friedrich* 2018, S. 89.

[94] Vgl. *Mormann* 2018.

[95] *Plath* 2018, S. 71, Rn. 2.

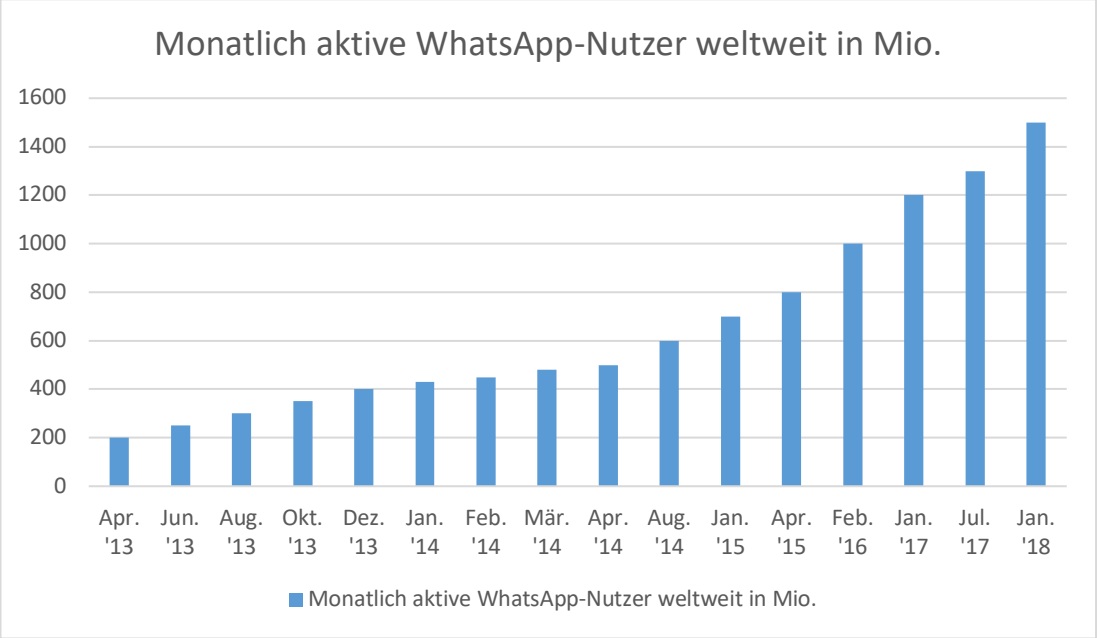

Abbildung 2: Anzahl der monatlich aktiven Nutzer von WhatsApp weltweit in ausgesuchten Monaten von April 2013 bis Januar 2018 (in Millionen) [96]

Das Diagramm zeigt deutlich auf, in welch kurzem Zeitraum die Anzahl der monatlichen Nutzer von WhatsApp weltweit exorbitant gestiegen ist. Dies verdeutlicht, weshalb WhatsApp in der heutigen Zeit eine derart große Bedeutung im Hinblick auf Telekommunikation innehat.

Im Jahre 2016 wurde WhatsApp mittels einer Ende-zu-Ende-Verschlüsselung abgesichert. Sämtliche Inhalte (Texte, Fotos, Videos und Anrufe) wurden damit nur noch in verschlüsselter Form übertragen, was diese nur noch für die beteiligten Nutzer sichtbar machte. Selbst das Unternehmen Facebook, als Eigentümer von WhatsApp, hat damit nicht mehr die Möglichkeit Nachrichteninhalte einzusehen. Folglich können diese auch nicht mehr auf Verlangen an Sicherheitsbehörden herausgegeben werden.[97] Durch diesen Schritt wurde WhatsApp durch die Electronic Frontier Foundation (EFF) in die Liste der sog. Krypto-Messenger aufgenommen.[98] Unter einem Krypto-Messenger versteht man eine Messenger-Anwendung, welche die übertragene Kommunikation auf unterschiedlichste Weisen verschlüsselt. Die bei WhatsApp verwendete Ende-zu-Ende-Verschlüsselung basiert auf

[96] Vgl. *Statista* 2018.

[97] Vgl. *Spiegel Online* 2016.

[98] Vgl. *Petrlic / Sorge* 2017, S. 103; *https://www.eff.org/de/node/82654* (besucht am 02.11.2018).

dem Signal-Protokoll.[99] Diese wurde ursprünglich für den gleichnamigen Signal-Messenger entwickelt und kann als „Goldstandard in der Kryptoszene“ bezeichnet werden.[100]

3.2.2.2 Skype

Die zweite betrachtete Messenger-Anwendung trägt den Namen Skype. Ursprünglich stellte Skype eine Alternative zur normalen Telefonie dar. Es war hiermit möglich, internetbasiert mittels VoIP-Telefonie zwischen zwei Geräten eine sprachbasierte Telekommunikation stattfinden zu lassen. Doch auch die Entwickler von Skype erweiterten den Umfang der Funktionen fortwährend. So ist es mittels Skype mittlerweile auch möglich, textbasierte Nachrichten auszutauschen, Videotelefonie und sogar Videokonferenzen mit bis zu 25 Teilnehmern abzuhalten, sowie Sprachanrufe ins herkömmliche Fest- oder Mobilfunknetz durchzuführen.[101]

Skype wurde im Jahre 2003 durch die Programmierer *Niklas Zennström* und *Janus Friis* gegründet. Nachdem der Dienst im Jahre 2005 durch die Gründer für 2,6 – 3,1 Milliarden Dollar an eBay verkauft wurde, verkaufte eBay ihn im Jahre 2011 für 8,5 Milliarden Dollar an Microsoft.[102]

Im März 2013 vermeldete Skype, dass die Nutzer des Videotelefonie-Dienstes insgesamt mehr als zwei Millionen Minuten pro Tag diesen Dienst in Anspruch nahmen.[103]

Der Name „Skype“ entstand aus einer Notlösung. Ursprünglich sollte die Anwendung den Namen „Skyper“ tragen. „Skyper“ sollte synonym für die Funktionsweise des Dienstes stehen: „Sky peer-to-peer“. Da jedoch die Webadressen für „Skyper“ schon vergeben waren, entschieden sich die Gründer dafür, den Namen „Skype“ zu nutzen.[104]

---

[99] Vgl. *Petrlic / Sorge* 2017, S. 104.
[100] Vgl. *Mobilsicher* 2018.
[101] Vgl. *Welling* 2018.
[102] Vgl. *Sander* 2013.
[103] Vgl. *Sander* 2013.
[104] Vgl. *Sander* 2013.

Neben dem kostenlosen Angebot für private Anwender bietet Skype auch eine kostenpflichtige Alternative für Unternehmen an. „Skype for Business“ ermöglicht es diesen – vernetzt mit den gängigen Office-Anwendungen – Besprechungen, Videokonferenzen und interaktive Vorträge weltweit durchzuführen.[105]

Auch Skype erfreute sich über die Jahre steigender Beliebtheit als internetbasiertes Telekommunikationsmittel. Wie der nachfolgenden Grafik zu entnehmen ist, stieg die Zahl der weltweit registrierten Skype-Nutzer bis ins Jahr 2017 stetig auf 1,3 Milliarden Menschen an.

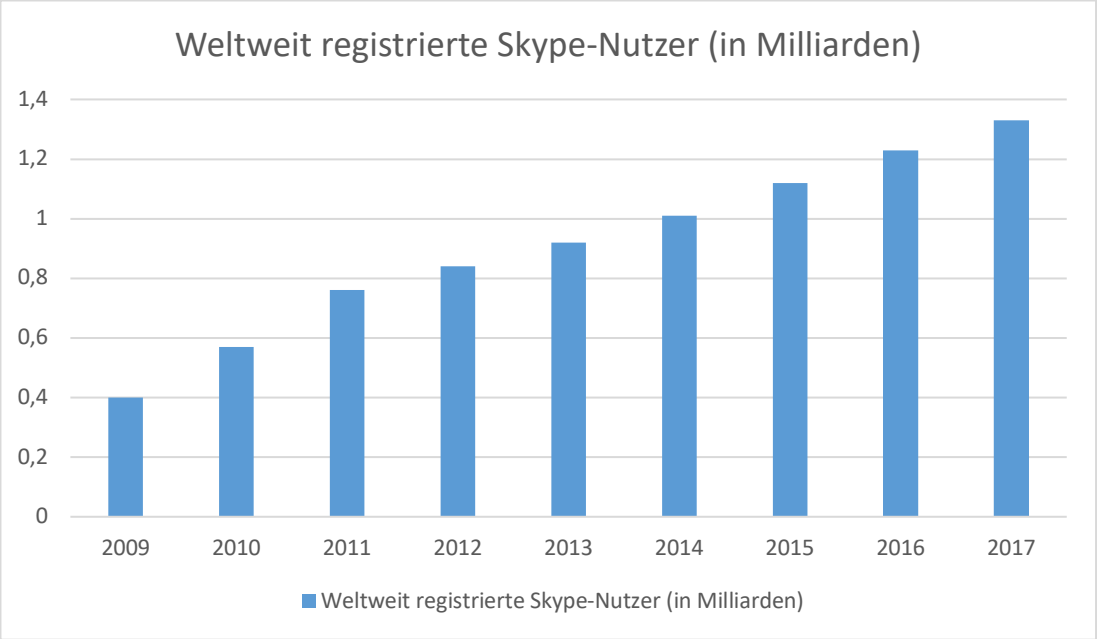

Abbildung 3: Schätzung zur Anzahl der weltweit registrierten Skype-Nutzer in den Jahren 2009 bis 2017[106]

Die bei Skype genutzte Peer-to-Peer-Verbindung führt dazu, dass die einzelnen Skype-Anwendungen in einem direkten Austausch stehen und nicht über einen zentralen Server kommunizieren. Das einzige zentrale Element in der Telekommunikationsverbindung ist der Login-Server, auf dem sich die Skype-Nutzer mit ihren Zugangsdaten einloggen.[107]

---

[105] Vgl. *https://www.skype.com/de/business/* (besucht am 02.11.2018).
[106] Vgl. *Statista* 2018a.
[107] Vgl. *Asi* 2008, S. 212 – 213.

Die Verschlüsselung der P2P-Telekommunikation in Skype geschieht in der Form, dass beide Klienten zunächst automatisiert einen digitalen 128-Bit-Schlüssel generieren. Dieser wird mit Hilfe des Public-Key-Kryptosystems RSA in der Folge zwischen beiden Klienten ausgetauscht und kombiniert. Hierdurch entsteht letztendlich eine 256-Bit-Verschlüsselung der direkt stattfindenden Kommunikation via Skype.[108]

Doch findet – im Gegensatz zu WhatsApp oder anderen Ende-zu-Ende-verschlüsselten und serverbasierten Diensten – nicht zwangsläufig jede Kommunikation via Skype verschlüsselt statt. Skype beinhaltet jedoch auch die Möglichkeit, eine internetbasierte Telekommunikationsverbindung in das herkömmliche Telefonnetz herzustellen. Die mit dem Fest- oder Mobilfunknetz stattfindende Telekommunikation wird in dem Teil, das im öffentlichen Telefonnetz stattfindet, nicht verschlüsselt.[109] Ein derartiges Telefonat ließe sich folglich mit den herkömmlichen Mitteln der Telekommunikationsüberwachung durch Strafverfolgungs- und Gefahrenabwehrbehörden mithören und aufzeichnen.

3.2.3 Technische Grundlagen

Im Nachfolgenden wird nun der technische Hintergrund des Betreibens und Überwachens von verschlüsselter Telekommunikation anhand der genannten Anwendungen dargestellt.

Betrieb verschlüsselter Telekommunikationsdienste

Verschlüsselte Telekommunikation erfolgt heutzutage maßgeblich über das Medium Internet. Durch die zunehmende Anbindung verschiedenster stationärer und mobiler Endgeräte sind laut einer aktuellen Onlinestudie der ARD und des ZDF 90,3% aller Menschen über 14 Jahren in Deutschland online.[110] In der Altersgruppe der 14- bis 29-jährigen nutzen 70% der Bundesbürger

[108] Vgl. *Asi* 2008, S. 214.

[109] Vgl. *https://support.skype.com/de/faq/FA31/verwendet-skype-verschlusselung* (besucht am 02.11.2018).

[110] Vgl. *Frees / Koch* 2018, S. 398.

zudem täglich den mobilen Internetzugang.[111] Insgesamt werden in dieser Altersgruppe, laut der benannten Studie, täglich deutlich über zwei Stunden damit verbracht, mittels Messengern wie WhatsApp etc. zu kommunizieren.[112] Diese Zahlen zeigen, welche Wichtigkeit die internetbasierte Telekommunikation aufweist.

Doch gibt es auf der technischen Seite unterschiedliche Standards, nach denen eine internetbasierte Telekommunikationsverbindung aufgebaut werden kann. Zwei maßgeblich verschiedene Formen werden auf der Grundlage der bereits dargestellten Messenger-Anwendungen WhatsApp und Skype hier näher erläutert.

Wie bereits angesprochen basiert der VoIP-Dienst Skype auf sog. Peer-to-Peer Verbindungen. „Mit dem Begriff Peer-to-Peer ist die Vorstellung verbunden, dass in einem Verbund Gleichberechtigter („Peers“), die sich wechselseitig Ressourcen wie Informationen, CPU-Laufzeiten, Speicher und Bandbreite zugänglich machen, kollaborative Prozesse unter Verzicht auf zentrale Koordinationsinstanzen durchgeführt werden.“[113] In einfachen Worten bedeutet dies, dass kein zentraler Server für die Übermittlung der Daten (in diesem Fall der Kommunikation) genutzt wird. Skype nutzt, wie bereits beschrieben, lediglich für die Login-Informationen einen eigenen Server. Die gesamte weitere Korrespondenz besteht fortan nur zwischen den einzelnen Peers (Skype-Klienten). Dadurch, dass keine zentrale Zwischenspeicherung auf einem unternehmenseigenen Server stattfindet, ist eine Kommunikation nur mit Klienten möglich, deren Endgerät im selben Moment mit dem Internet verbunden ist. Die Verschlüsselung der übermittelten Nachrichten/Kommunikation erfolgt auf dem Transportweg – wie bereits beschrieben – in einem kooperativen Prozess zwischen den Anwendungen beider Gesprächsteilnehmer. Skype setzt zur Verschlüsselung der Gespräche den 256-Bit-Verschlüsselungsstandard AES (Advanced Encryption Standard) ein.[114]

---

[111] Vgl. *Frees / Koch* 2018, S. 401.

[112] Vgl. *Frees / Koch* 2018, S. 406.

[113] *Schoder* 2002, S. 3.

[114] Vgl. https://support.skype.com/de/faq/FA31/verwendet-skype-verschlusselung (besucht am 03.11.2018).

Bei anderen Instant-Messaging-Diensten wie WhatsApp wird die Kommunikation über zentrale Server vermittelt. Das bedeutet, dass versandte Nachrichten zunächst von einem Server (zwischen)gespeichert werden, bis der Empfänger der Nachricht diese abruft. Der Standort der hierfür benötigten WhatsApp-Server befindet sich im US-Bundesstaat Kalifornien.[115] Laut WhatsApp werden sämtliche Nachrichten bei Abruf von dem firmeneigenen Server gelöscht. Sollten die Nachrichten nicht abgerufen werden, erfolgt die Löschung nach 30 Tagen.[116] Bevor die Daten an den Server übertragen werden, erfolgt die Verschlüsselung selbiger mit der bereits benannten Ende-zu-Ende-Verschlüsselung. Nur durch den Empfänger der Daten können deren Inhalte somit wieder lesbar gemacht werden. Für die Verschlüsselung der Nachrichten vor dem Versand nutzt WhatsApp ebenso den 256-Bit-Verschlüsselungsstandard AES.[117] Jedoch werden durch die Ende-zu-Ende-Verschlüsselung nur die jeweiligen Kommunikationsinhalte gesichert. Andere Meta-Daten wie Zeit- und Datenstempel, sowie die IP-Adresse der beteiligten Kommunikationsteilnehmer werden unverschlüsselt übertragen.[118]

Überwachung verschlüsselter Telekommunikation

Strafverfolgungs- und Gefahrenabwehrbehörden haben unter gewissen rechtlichen Voraussetzungen (§ 100a Abs. 1 S. 2, 3 StPO bzw. § 15b HSOG), die im weiteren Verlauf dieser Arbeit noch thematisiert werden, die theoretische Möglichkeit, verschlüsselte Telekommunikation mit Hilfe eines Eingriffs in das informationstechnische System des Betroffenen abzuhören und aufzuzeichnen. Diese Maßnahme wird auch als Quellen-TKÜ bezeichnet.[119]

Während bei der „herkömmlichen“ TKÜ gem. § 100a Abs. 1 S. 1 StPO bzw. gem. § 15a HSOG die Diensteanbieter gem. § 110 Abs. 1 TKG dazu verpflichtet sind, die notwendigen Maßnahmen für die Umsetzung der Überwachung leitungsvermittelter Telekommunikation zu treffen, stellt sich die Situa-

[115] Vgl. *Belschner* 2016.
[116] Vgl. *o. V.* 2015.
[117] Vgl. *Petrlic / Sorge* 2017, S. 105.
[118] Vgl. *Witte* 2018.
[119] Vgl. *Keller / Braun / Hoppe* 2015, S. 44.

tion bei der Überwachung verschlüsselter, mittels Internet geführter, Telekommunikation anders dar. Die Herstellung einer Telekommunikationsverbindung erfolgt – im Gegensatz zur leitungsvermittelten Telekommunikation – nicht mittels einer stehenden Verbindung. Peer-to-Peer und auch Serververmittelte Telekommunikation senden die Inhaltsdaten in einzelnen Datenpaketen, die beim Empfänger sodann wieder zum gesamten Inhalt zusammengesetzt werden.[120] Die einzelnen Datenpakete werden, wie bereits dargestellt, vor dem Versand der Nachricht (Ende-zu-Ende-Verschlüsselung) oder während des Telekommunikationsvorgangs (Peer-to-Peer-Verbindung) durch die meisten internetbasierten Telekommunikationsanwendungen verschlüsselt. Eine Ausleitung der Daten durch die Diensteanbieter i. S. der „herkömmlichen" TKÜ ist daher zwar möglich, der Inhalt der Daten ist aufgrund der Verschlüsselung jedoch durch die Sicherheitsbehörden nicht les- bzw. hörbar und dadurch zu großen Teilen wertlos.[121] Die Entschlüsselung der sowohl durch WhatsApp als auch Skype genutzten 256-Bit-AES-Verschlüsselung ist aktuell technisch nahezu ausgeschlossen. Ein Versuch der Entschlüsselung würde jedenfalls eine nicht vertretbar lange Zeit bis zur Erlangung der Gesprächsinhalte in Anspruch nehmen.[122]

Aus diesem Grund kann eine Überwachung verschlüsselter internetbasierter Telekommunikation nicht erst auf dem „Transportweg" erfolgen. Wie der Name „Quellen-TKÜ" bereits suggeriert, muss es den Sicherheitsbehörden daher gelingen, die zu überwachende Telekommunikation bereits an ihrem Ursprung aufzuzeichnen. Dies kann sowohl vor einer Verschlüsselung der Daten beim Absender, als auch nach der Entschlüsselung beim Empfänger erfolgen.[123]

Diese Vorgehensweise macht es erforderlich, dass ein Eingriff in das informationstechnische System des Betroffenen erfolgt. Üblicherweise geschieht dies, indem eine Software auf das Endgerät des Betroffenen aufgespielt wird. Dies kann sowohl „virusgleich" über das Internet erfolgen, als auch di-

[120] Vgl. *Liebig* 2015, S. 123.
[121] Vgl. *Liebig* 2015, S. 126.
[122] Vgl. *Liebig* 2015, S. 126; vgl. *Weis* 2016, S. 65 – 66.
[123] Vgl. *Bratke* 2013, S. 44 – 45.

rekt am Endgerät des Betroffenen.[124] Auch besteht die Möglichkeit der Nutzung sog. Zero-Day-Exploits, um die Software in das Zielsystem einzubringen. Hierbei handelt es sich um Schwachstellen von bereits auf dem Zielsystem installierter Software, die sowohl durch Cyberkriminelle als auch durch Geheimdienste genutzt werden, um Hackerangriffe durchzuführen.[125]

Bisher wurden unter anderem die Programme Digitask[126] und FinSpy/Finfisher[127] als für diese Zwecke genutzte Software bekannt. In der öffentlichen Berichterstattung wird derartige Software gemeinhin als Staats- oder Bundestrojaner bezeichnet.[128] Mit dieser Software ist es beispielsweise möglich, den Tastendruck am Gerät des Betroffenen (sog. Keylogger) oder die Aktivität des Mikrofons bei der VoIP-Telefonie zu überwachen und aufzuzeichnen.[129] Auch ermöglichen die Programme, Abbilder des auf dem Bildschirm des betroffenen Endgeräts angezeigten Inhalts (Screengrabber) zu fertigen.[130] Eine Mitwirkung der betroffenen Anbieter von Instant-Messaging- oder VoIP-Diensten ist durch den Einsatz der Software somit nicht erforderlich.

Jedoch gibt es auch eine weitere Möglichkeit seitens der Sicherheitsbehörden Zugriff auf verschlüsselte Telekommunikationsinhalte zu erhalten: Bei sog. „Backdoors“ (Hintertüren) handelt es sich um Sicherheitslücken, die der Entwickler der entsprechenden Kommunikationssoftware unter Umständen absichtlich in das Programm integriert hat. Durch diese hat zumindest der Anbieter der Software selbst die Möglichkeit, die Kommunikation in unverschlüsselter Form einzusehen und ggf. an Strafverfolgungs- oder Gefahrenabwehrbehörden auszuleiten. Im Jahre 2008 verdichteten sich beispielsweise die Hinweise, dass Skype durch derartige Backdoors dem amerikanischen Geheimdienst NSA Zugriff auf Gesprächsinhaltsdaten ermöglicht hat.[131] Fraglich erscheint jedoch, ob „Backdoors“ als adäquate Opti-

[124] Vgl. *Dalby* 2016, S. 138.
[125] Vgl. *Flade* 2017.
[126] Vgl. BT-Drs. 17/7760, S. 2ff.
[127] Vgl. *Meister* 2013.
[128] Vgl. *Neumann* 2018.
[129] Vgl. *Dalby* 2016, S. 138.
[130] Vgl. *Flade* 2017.
[131] Vgl. *Liebig* 2015, S. 127.

on für eine rechtmäßige Überwachung der verschlüsselten Telekommunikation sinnvoll sind. Auch Unberechtigte könnten sich über diese Sicherheitslücken Zugriff zur Telekommunikation von VoIP- oder Messengerdienstnutzern verschaffen und vertrauliche Gespräche mithören und aufzeichnen.

3.2.4 Rechtliche Grundlagen

Ergänzend zu den bereits dargestellten Rechtsgrundlagen zur Überwachung unverschlüsselter Telekommunikation wurden die repressiven und präventiven Rechtsgrundlagen in jüngerer Vergangenheit dahingehend erweitert, dass ebenfalls die Überwachung verschlüsselter Telekommunikation rechtlich möglich wurde.

3.2.4.1 Repressive Rechtsgrundlage

Im Jahre 2017 wurde – wie bereits zu Beginn dieser Arbeit kurz skizziert – der § 100a Abs. 1 StPO durch die Sätze 2 und 3 ergänzt. Im Rahmen des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens wurde die Rechtsgrundlage für die sog. Quellen-TKÜ hinzugefügt.[132] § 100a Abs. 1 S. 2 und 3 StPO lauten nun:

> „Die Überwachung und Aufzeichnung der Telekommunikation darf auch in der Weise erfolgen, dass mit technischen Mitteln in von dem Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen. Auf dem informationstechnischen System des Betroffenen gespeicherte Inhalte und Umstände der Kommunikation dürfen überwacht und aufgezeichnet werden, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können."

Die Überwachungserweiterung war notwendig, da in der modernen Zeit große Teile der Kommunikation verschlüsselt über das Internet übertragen werden. Die Strafverfolgungsbehörden erhalten so die Möglichkeit, direkt in das

[132] BGBl. I 2017, S. 3203 - 3204.

informationstechnische System einzugreifen, um Kommunikation bereits vor ihrer Verschlüsselung zu überwachen und aufzuzeichnen. Gem. § 100a Abs. 5 StPO ist hierbei technisch sicherzustellen, dass ausschließlich die laufende Kommunikation oder Inhalte und Umstände der Kommunikation nach dem Zeitpunkt der Anordnung entsprechender Maßnahmen überwacht und aufgezeichnet werden. Hiermit soll sichergestellt werden, dass mittels der Abhörsoftware keine über die Kommunikationsdaten herausgehenden Daten auf dem informationstechnischen System eingesehen werden (vgl. Online-Durchsuchung). Außerdem schreibt § 100a Abs. 5 StPO vor, dass das informationstechnische System nur soweit verändert werden darf, wie es für die Datenerhebung unerlässlich ist. Weiterhin müssen diese Änderungen nach Beendigung der Maßnahme rückgängig gemacht werden. Auch beinhaltet die Vorschrift den Passus, dass die genutzte Abhörsoftware gegen die unbefugte Nutzung zu schützen ist.

Auf die hiermit einhergehenden rechtlichen und tatsächlichen Schwierigkeiten und die Diskussion um den sog. „Bundestrojaner“ wurde bzw. wird im Verlauf dieser Thesis eingegangen. An dieser Stelle sei jedoch darauf hingewiesen, dass die in S. 2 und 3 geregelte Quellen-TKÜ expressis verbis „notwendig“ sein muss, also sie nur eingesetzt werden darf, sofern mit der herkömmlichen TKÜ keine ausreichenden Ermittlungsergebnisse erzielt werden können.[133]

3.2.4.2 Präventive Rechtsgrundlage

Anders als in S. 2 und 3 der repressiven Eingriffsnorm § 100a Abs. 1 StPO, wurde im HSOG der Eingriff in informationstechnische Systeme zur Telekommunikationsüberwachung (Quellen-TKÜ) in einer gesonderten Norm – dem § 15b HSOG – geregelt. Der Wortlaut der Norm orientiert sich stark an § 100a Abs. 1 S. 2 und 3, Abs. 5 StPO. Für eine Maßnahme nach § 15b HSOG gelten dieselben gefahrenabwehrrechtlichen Voraussetzungen wie für die präventive Überwachung unverschlüsselter Kommunikation gem. § 15a HSOG.

[133] Vgl. *Freiling / Safferling / Rückert* 2018, S. 11.

4 Rechtliche und tatsächliche Probleme der Überwachung verschlüsselter Telekommunikation

Dieses Kapitel widmet sich den rechtlichen und tatsächlichen Problemen im Hinblick auf die Durchführung von Telekommunikationsüberwachungsmaßnahmen. Wie bereits im Verlauf dieser Arbeit ausführlich dargestellt wurde, handelt es sich bei der „herkömmlichen“ TKÜ um eine etablierte und seit vielen Jahren angewandte Ermittlungsmethode der Strafverfolgungs- und Gefahrenabwehrbehörden. Diese kann unter klaren rechtlichen Voraussetzungen und unter Inanspruchnahme der inländischen Telekommunikationsdiensteanbieter durchgeführt werden. Mit im Jahre 2016 in der BRD insgesamt erlassenen 21.355 Erst- und Verlängerungsanordnungen[134] von Maßnahmen nach § 100a StPO (zeitlich vor der Implementierung der Quellen-TKÜ in die Sätze 2 und 3), belegen die aktuellen Zahlen des Bundesamts für Justiz, dass die TKÜ eine Standardmaßnahme zur Strafverfolgung geworden ist.

Im Hinblick auf die Überwachung verschlüsselter Telekommunikation ergeben sich, trotz höchstrichterlicher Rechtsprechungen und in jüngerer Vergangenheit geschaffener repressiver und präventiver Rechtsgrundlagen, jedoch noch immer Probleme bei der Durchführung entsprechender Maßnahmen. Nachfolgend werden einige dieser Probleme beleuchtet und problemorientiert erörtert.

4.1 Verschlüsselungsverbot gem. § 8 Abs. 3 TKÜV

§ 8 Abs. 3 der Telekommunikations-Überwachungsverordnung (TKÜV) gibt vor, dass, wenn der Verpflichtete die ihm zur Übermittlung (an die berechtigte Stelle) anvertraute Telekommunikation netzseitig durch technische Maßnahmen gegen unbefugte Kenntnisnahme schützt, er diese Schutzvorkehrung bei der am Übergabepunkt bereitzustellenden Überwachungskopie aufzuheben hat.

[134] *Bundesamt für Justiz* 2017.

Diese Vorschrift kann, laut *Pernice*, als „verstecktes Verschlüsselungsverbot“ angesehen werden.[135] Fraglich erscheint nun, weshalb Dienste wie WhatsApp oder Skype trotz dieser Vorschrift die übermittelte Telekommunikation nicht in unverschlüsselter Form an staatliche Stellen ausleiten. Zur Beantwortung dieser Frage muss zunächst geklärt werden, wer „Verpflichteter“ i. S. der TKÜV ist. Gem. § 2 S. 1 Nr. 16 TKÜV ist Verpflichteter jeder, der nach den Vorschriften der TKÜV technische und organisatorische Vorkehrungen zur Umsetzung von Anordnungen zu treffen hat. Weiterhin wird der Kreis der Verpflichteten danach definiert, wer Betreiber einer Telekommunikationsanlage ist.[136] Betreiber einer Telekommunikationsanlage ist gem. § 2 S. 1 Nr. 4 TKÜV das Unternehmen, das tatsächlich die Kontrolle über die Funktionen einer Telekommunikationsanlage ausübt.

Um die Frage zu beantworten, ob WhatsApp oder Skype nun Verpflichtete i. S. der TKÜV bzw. nach dem TKG sind, müssen zunächst die Vorschriften des Telemediengesetzes (TMG) näher in Augenschein genommen werden. Gem. § 1 Abs. 1 TMG gelten die Vorschriften des TMG für alle Informations- und Kommunikationsdienste, soweit es sich bei diesen nicht um Telekommunikationsdienste nach § 3 Nr. 24 TKG, telekommunikationsgestützte Dienste nach § 3 Nr. 25 TKG oder Rundfunk nach § 2 des Rundfunkvertrags handelt. Gem. § 3 Nr. 24 TKG sind Telekommunikationsdienste in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen.

Nach mancher Meinung handelt es sich demnach bei VoIP-Diensten (z. B. Skype) um Telekommunikationsdienste, da rein äußerlich kein Unterschied zur herkömmlichen leitungsgebundenen Telefonie zu erkennen ist.[137] Andere Quellen beziehen sich darauf, dass es auf die technische Ausgestaltung des einzelnen zu beurteilenden Dienstes ankommt, ob dieser ganz oder überwiegend aus der Übertragung von Signalen über Telekommunikationsnetze besteht.[138] Diese Übertragung der Signale wird von wieder anderen Quellen

---

[135] Vgl. *Pernice* 2002, S. 211.

[136] Vgl. *Abel* 2011, S. 300.

[137] Vgl. *Abel* 2011, S. 14.

[138] Vgl. *Deutscher Bundestag* 2016, S. 8.

eher im Zuständigkeitsbereich des Internetanbieters und nicht bei den Betreibern der Messenger- bzw. VoIP-Dienste gesehen, weshalb diese eher unter die Regelungen des TMG fallen würden.[139]

Wie sich gezeigt hat, ist die Einordnung der VoIP- und Messengerdienste als Telekommunikationsdienst i. S. d. TKG oder als sonstiger Informations- und Kommunikationsdienst i. S. d. TMG eine noch immer umstrittene Frage, die intensiv diskutiert wird.[140] Doch ist sie elementar dafür, ob selbige unter die Regelungen der TKÜV fallen. Denn nur wenn VoIP- und Messengerdienste als Telekommunikationsdienste i. S. des TKG einzustufen sind, wäre die TKÜV auf diese grundsätzlich anwendbar. Da *Gorgass* offensichtlich die Auffassung teilt, dass es sich zumindest bei VoIP-Diensten um Telekommunikationsdienste i. S. des TKG handelt, zeigt er eine Möglichkeit auf, nach der z. B. Skype dem „Verschlüsselungsverbot" i. S. d. § 8 Abs. 3 TKÜV nachkommen und die Telekommunikationsinhalte unverschlüsselt an die berechtigten Stellen ausleiten müsste. Technisch wäre das über einen sog. Zwangs-Proxy(-server) möglich.[141]

Die Übertragung des Kommunikationsinhalts würde in diesem Fall zunächst verschlüsselt von dem Anrufenden an den Zwangs-Proxy stattfinden. Dort würde die Verschlüsselung für einen kurzen Zeitraum aufgehoben werden, bevor die Kommunikation erneut verschlüsselt an den Angerufenen gesichert übertragen werden würde. Die somit im Zwangs-Proxy vorliegenden unverschlüsselten Daten könnten dann im Bedarfsfall an die berechtigten Stellen ausgeleitet werden.[142]

Gorgass äußert jedoch auch Sicherheitsbedenken hinsichtlich dieser Vorgehensweise, da auch durch die nur kurzzeitige Aufhebung der Verschlüsselung ein zusätzliches Sicherheitsrisiko geschaffen werde, das auch unberechtigten Dritten die Möglichkeit der Nutzung dieser Schwachstelle bietet, um so Kenntnis vom Inhalt der per VoIP geführten Telekommunikation zu erlangen.[143] Eine derartige Vorgehensweise ließe sich jedoch nur bei Ver-

[139] Vgl. *Ulbricht* 2018, S. 282.
[140] Vgl. *Ulbricht* 2018, S. 282.
[141] Vgl. *Gorgass* 2011, S. 107.
[142] Vgl. *Gorgass* 2011, S. 107.
[143] Vgl. *Gorgass* 2011, S. 106 – 107.

schlüsselungsformen anwenden, die während des Übertragungsvorgangs der Daten aufgebaut werden. Wie bereits beschrieben, nutzt Skype eine solche Verschlüsselung.

Um an den Kommunikationsinhalt von Ende-zu-Ende-verschlüsselten Messengerdiensten wie WhatsApp zu gelangen, ist eine derartige Vorgehensweise nutzlos, da die Verschlüsselung – wie ebenfalls bereits thematisiert – bereits vor dem Versand der Kommunikationsdaten erfolgt und ein zwischengeschalteter Proxy-Server somit auch nicht in der Lage wäre, die übermittelten Daten zu entschlüsseln.[144]

Um einen VoIP-Anbieter wie Skype zur Ausleitung der Daten in der von *Gorgass* beschriebenen Form zu verpflichten, müssten die Vorschriften des TKG und der TKÜV jedoch auch örtlich anwendbar sein. Skype, als Tochterunternehmen von Microsoft, unterhält seinen Firmenhauptsitz in Luxemburg.[145] Damit liegt dieser nicht im Geltungsbereich des in Deutschland gültigen TKG bzw. der TKÜV. Eine ähnliche Problematik wurde im Rahmen dieser Arbeit bereits hinsichtlich des Standorts der WhatsApp-Server im US-Bundesstaat Kalifornien thematisiert. Bereits aufgrund der mangelnden örtlichen Anwendbarkeit scheidet eine entsprechende Pflicht daher bereits aus. Der Umstand, dass die Dienste auch in Deutschland erbracht werden, reicht für die Anwendbarkeit indes nicht aus.

4.2 Infiltration von Abhörsoftware

Für die Überwachung verschlüsselter Telekommunikation ist es auch deshalb erforderlich bereits vor der Verschlüsselung des Telekommunikationsinhalts durch Messenger- oder VoIP-Dienste wie WhatsApp oder Skype, diesen in unverschlüsselter Form auf dem jeweiligen Endgerät aufzuzeichnen und an die Strafverfolgungs- bzw. Gefahrenabwehrbehörden auszuleiten. Die hierfür benötigten rechtlichen Grundlagen (§ 100a Abs. S. 2 und 3 StPO und § 15b HSOG) wurden im Verlauf dieser Arbeit bereits ausführlich thematisiert und dargestellt. Welche Möglichkeiten in der Praxis nun bestehen, die hierfür benötigte Abhörsoftware auf dem betreffenden Endgerät (Zielsystem)

[144] Vgl. *Gorgass* 2011, S. 107.

[145] Vgl. https://www.skype.com/de/about/ (besucht am 07.11.2018).

zu installieren, welche weiteren Vorgehensweisen hierfür möglich wären und welche Probleme damit einhergehen, ist Gegenstand der nachfolgenden Ausführungen.

Zunächst muss festgehalten werden, dass zwei Möglichkeiten zur Infiltration des Zielsystems bestehen. Zum einen ist das Einbringen über das Internet und zum anderen das Einbringen unter Ausnutzung des physischen Zugriffs auf das entsprechende Zielsystem zu nennen. Fest steht, dass ein Betreten der Wohnung des Betroffenen zum Zwecke der Infiltration des Zielsystems nicht von der jeweiligen Rechtsgrundlage umfasst ist.[146] Dieses Problem lässt sich nicht nur durch den hiermit verbundenen zusätzlichen Eingriff in Art. 13 Abs. 1 GG begründen. Bei TKÜ-Maßnahmen handelt es sich grundsätzlich um verdeckte Ermittlungsmethoden bzw. heimliche Maßnahmen. Das heimliche Eindringen in die Wohnung des Betroffenen durch Mitarbeiter der Sicherheitsbehörden unterliegt besonders strengen rechtlichen Voraussetzungen. So bemisst sich die Rechtfertigung heimlicher repressiver Maßnahmen, die mittels Zutritt zur Wohnung des Betroffenen durchgeführt werden, nach dem Gewicht der verfolgten Straftat.[147] Gem. Art. 13 Abs. 2 GG ist dies nur bei Vorliegen einer besonders schweren Straftat (siehe auch § 100c StPO) möglich. Für die Anordnung von Maßnahmen nach § 100a StPO ist jedoch „nur“ das Vorliegen einer schweren Straftat erforderlich, was mithin nicht zum heimlichen Betreten der Wohnung berechtigt.

Dieses Problem scheint jedoch bereits durch die Politik erkannt worden zu sein. Im Bayrischen Polizeiaufgabengesetz (BayPAG) wurde bereits am 01.08.2008 mit Art. 34e BayPAG ein heimliches Betretungs- und Durchsuchungsrecht im präventiven Bereich eingeführt. Dies wurde jedoch genau ein Jahr später, aufgrund der Entscheidung des BVerfG zur Online-Durchsuchung,[148] wieder entfernt.[149] Zehn Jahre später unternehmen die Justizminister der Bundesländer Rheinland-Pfalz, Bayern, Hessen und Mecklenburg-Vorpommern auf der 89. Konferenz der Justizministerinnen und Justizminister am 06. und 07.06.2018 in Thüringen einen neuen Versuch, ein

---

[146] Vgl. *Graf* 2018, S. 408, Rn. 109; Vgl. BT-Drs. 18/11272.
[147] Vgl. *Sodan* 2018, S. 189, Rn. 11.
[148] BVerfG NJW 2008, 822.
[149] LT-Drs. 16/1271; vgl. *Bratke* 2013, S. 472.

entsprechendes Betretungsrecht zu etablieren. Sie fassten den Beschluss, dass ein gesetzliches Betretungsrecht zum Zwecke der Aufbringung von Abhörsoftware unter Berücksichtigung der verfassungsrechtlichen Implikationen der Bundesministerin der Justiz und für Verbraucherschutz vorgelegt werden soll.[150] Ob dies unter verfassungsrechtlichen Gesichtspunkten erfolgreich sein wird, bleibt abzuwarten.

Diese Problematik dürfte sich jedoch maßgeblich auf das Aufbringen der Abhörsoftware auf stationären Computersystemen beziehen. Hinsichtlich mobiler Endgeräte bestehen weitere Möglichkeiten unter Ausnutzung des physischen Zugriffs auf das entsprechende Endgerät. Unter der Maßgabe „[...], dass ein Zugriff auf ein informationstechnisches System des Betroffenen zum Zweck der Aufbringung der Überwachungssoftware grds. nur auf technischem Wege oder mittels kriminalistischer List erfolgen darf, [...]“[151] bieten sich eine Vielzahl von polizeilichen Maßnahmen an, die eine Infiltration des Endgeräts ermöglichen.

Eine interessante Möglichkeit ergibt sich beispielsweise im Rahmen von Kontrollmaßnahmen zum Nachteil des Betroffenen. In einem Urteil vom 26.04.2017 befand der BGH in bestimmten Konstellationen die bis dahin (und auch heute noch) umstrittenen sog. „legendierten Kontrollen“ für rechtmäßig.[152] Demnach wäre es bei einer präventiv-repressiven Gemengelage grds. möglich, den Beschuldigten im Strafverfahren einer Verkehrskontrolle nach Gefahrenabwehrrecht zu unterziehen, sein Fahrzeug und seine Person präventiv nach dem zu infiltrierenden Endgerät zu durchsuchen, die Abhörsoftware aufzuspielen und den Beschuldigten in Unkenntnis der tatsächlichen Hintergründe samt des infiltrierten Endgeräts aus der Maßnahme zu entlassen.

Auch andere offene Maßnahmen, die weniger die Aufmerksamkeit des Betroffenen erwecken dürften, könnten dazu dienen, die Abhörsoftware auf dem physisch zugänglichen Gerät zu installieren. *Bratke* führt hierzu beispielhaft offene Durchsuchungsmaßnahmen nach § 102 ff. StPO, zollrechtli-

---

[150] Vgl. *89. Konferenz der Justizministerinnen und Justizminister* 2018, S. 1 – 2.
[151] *Graf* 2018, S. 408, Rn. 109.
[152] Vgl. BGH NJW 2017, 3173.

che Kontrollen am Flughafen sowie das Ausnutzen von Situationen, in denen sich das Gerät beispielsweise bei einer Reparatur befindet, an.[153]

Neben der Infiltration von physisch zugänglichen Endgeräten, handelt es sich bei einer online aus der Ferne durchgeführten Installation der Abhörsoftware ebenfalls um eine gangbare Vorgehensweise in der Praxis.[154] Hierzu ist es jedoch in vielen Fällen erforderlich, den Nutzer des zu infiltrierenden Geräts mittels einer Täuschung zu einer unbewussten Mitwirkungshandlung zu veranlassen.[155]

Bratke führt hierzu einige weitere Beispiele zu der Möglichkeit der Online-Infiltration von informationstechnischen Systemen an. So könnte beispielsweise eine fingierte Internetseite eingerichtet werden, die auf die Lebensumstände des Betroffenen zugeschnitten ist. Sollte der Betroffene diese Seite dann aufrufen, könnte das Abhörprogramm so in das entsprechende Endgerät implementiert werden (Drive-by-Download).[156]

Als weitere Möglichkeit könnte auch eine E-Mail unter dem Namen einer anderen Behörde versandt werden, die im Rahmen des sog. E-Governments durch den Betroffenen nicht als unüblich bzw. verdächtig eingestuft werde. Diese enthielte dann einen zu öffnenden Anhang, der die Abhörsoftware auf dem Zielsystem installiert.[157] Ein Problem hierbei dürfte jedoch sein, dass durch das Bekanntwerden einer derartigen Vorgehensweise das Vertrauen der Bürger in staatliche Stellen nachhaltig geschädigt werden könnte.[158]

Eine andere Form der online durchgeführten Infiltration des Zielsystems mittels „Zero-Day-Exploits“ und absichtlich in die VoIP- oder Messengersoftware eingebauten „Backdoors“ wurde im Rahmen dieser Arbeit bereits thematisiert. Wie bereits dargestellt, handelt es sich bei diesen um Schwachstellen,

[153] Vgl. *Bratke* 2013, S. 99 – 100.
[154] Vgl. *Bratke* 2013, S. 96.
[155] Vgl. *Bratke* 2013, S. 96.
[156] Vgl. *Bratke* 2013, S. 97; vgl. *Liebig* 2015, S. 131.
[157] Vgl. *Bratke* 2013, S. 97; vgl. *Liebig* 2015, S. 131.
[158] Vgl. *Bratke* 2013, S. 97.

die durch den Hersteller der Software nicht bedacht wurden[159] bzw. um solche, die vorsätzlich durch den Hersteller in die Software integriert wurden.[160]

Ein nicht zu unterschätzendes Problem hierbei dürfte allerdings das hierdurch entstehende Sicherheitsrisiko für die Gesamtheit der Nutzer der betreffenden Telekommunikationssoftware sein. Eine staatliche Stelle, die einen Zero-Day-Exploit in einer Software feststellt, stünde damit in einem Konflikt zwischen der Nutzung des Exploits, um Abhörsoftware in das Zielsystem einzubringen, und der möglichen Pflicht zur Mitteilung der Sicherheitslücke an den betroffenen Softwarehersteller, um eine Gefahr für die Gesamtheit der Nutzer abzuwehren.

Diese Pflicht ergibt sich unter anderem aus § 3 Abs. 1 S. 1 des BSI-Gesetzes. Demnach hat das BSI die Pflicht, die Sicherheit in der Informationstechnik zu fördern. Ein Ausnutzen dieser Sicherheitslücken zur Strafverfolgung stünde somit im direkten Gegensatz hierzu.[161] Aus Sicht des Autors dürfte jedoch in diesen Fällen – abhängig vom konkreten Einzelfall – die Pflicht zur Gefahrenabwehr für eine Vielzahl von Nutzern dem staatlichen Interesse der Strafverfolgung eines einzelnen Nutzers überwiegen.

Auch vorsätzlich durch den Hersteller in die Telekommunikationssoftware integrierte Backdoors dürften ähnliche Sicherheitsproblematiken aufweisen. Sollte es unberechtigten Dritten (z. B. Hackern) gelingen, Zugriff auf ein solches Backdoor zu erhalten, besteht auch hier eine Gefahr für die Gesamtheit der Nutzer der entsprechenden Software. Fraglich erscheint zudem, ob VoIP- und Messengerdiensteanbieter auf die Integration dieser Backdoors in ihre angebotene Software einließen.[162] Ein Hauptaugenmerk von WhatsApp und Skype, sowie der gesamten Industrie der sog. Krypto-Messenger, liegt eben auf der Sicherheit und Verschlüsselung der über sie geführten Kommunikation. So wirbt WhatsApp, nach der Integration der Ende-zu-Ende-Verschlüsselung, offensiv damit, dass niemand mehr in die betreffenden Nachrichten schauen kann.[163]

---

[159] Vgl. *Siller* 2017.
[160] Vgl. *Siller* 2018.
[161] Vgl. *Roggan* 2018, S. 39; vgl. *Roggan* 2017, S. 829.
[162] Vgl. *Liebig* 2015, S. 131 – 132.
[163] Vgl. *Spiegel Online* 2016.

Nicht nur die Installation, sondern auch die grundsätzlich geforderte Deinstallation der Abhörsoftware[164] könnte ein Problem für Strafverfolgungs- und Gefahrenabwehrbehörden darstellen. *Bratke* führt hierzu drei Möglichkeiten auf.

Ähnlich wie bei der Infiltration des Zielsystems, ließe sich die Abhörsoftware bei einem direkten Zugriff auf das Endgerät sowie online aus der Ferne wieder deinstallieren.[165] Die dritte Möglichkeit besteht darin, die Abhörsoftware nach klar definierten Voraussetzungen automatisiert zu löschen. Hierzu könnte ein Zeitpunkt in die Software integriert werden, zu dem sie sich selbst deinstalliert. Aber auch die Löschung bei Nicht-Erreichbarkeit der Software (z. B. wegen einer nachträglich auf dem Endgerät installierten Firewall) käme in Betracht.[166] § 100a Abs. 5 S 1 Nr. 3 StPO präferiert diese Möglichkeit und schreibt hierzu sinngemäß vor, dass die Löschung der Abhörsoftware grundsätzlich automatisiert zu erfolgen hat.

Auch wenn die nicht durchgeführte Löschung der Abhörsoftware nicht zu einer Unverwertbarkeit der strafprozessualen TKÜ führt,[167] sollte es im Interesse der Sicherheitsbehörden liegen, diese trotzdem durchzuführen. Dadurch, dass nach Offenlegung der Verfahrensakten sowohl dem Betroffenen selbst, als auch dessen Rechtsanwälten die Durchführung einer Quellen-TKÜ bekannt wird, gilt es umso mehr, die taktischen Vorgehensweisen und die genaue Funktion im Hinblick auf den künftigen Einsatz der Software geheim zu halten.

Der Chaos Computer Club (CCC) gelangte beispielsweise im Jahre 2011 an eine aktuelle Version des dort so bezeichneten „Staatstrojaners“ und analysierte dessen Quellcode.[168] In den dazu getätigten Ausführungen forderte der CCC unter anderem die „zukünftige automatische Offenlegung von Quellcode, Binary und Protokollen des Trojaners nach jedem Einsatz.“[169] Diese Forderung erscheint im Hinblick auf eine zukünftige effektive Strafverfolgung und Gefahrenabwehr unter Einsatz der Abhörsoftware wenig sinnvoll. Die hierdurch erlangten Daten könnten durch Kriminelle genutzt werden,

---

[164] Vgl. *Bratke* 2013, S. 94.
[165] Vgl. *Bratke* 2013, S. 102 – 103.
[166] Vgl. *Bratke* 2013, S. 103.
[167] Vgl. *Graf* 2018, S. 411, Rn. 126.
[168] Vgl. *Chaos Computer Club* 2011.
[169] *Chaos Computer Club* 2011.

um ihre Endgeräte gegen den Einsatz der Abhörsoftware abzusichern. Die Sicherheitsbehörden müssten in diesem Fall ständig den Quellcode der Software verändern und erneuern, um deren Einsatz trotz Firewalls und Antivirensoftware zu garantieren. Dies würde einen enormen – aus Sicht des Autors – nicht vertretbaren Mehraufwand im Bereich der Softwareentwicklung bedeuten. Auch wenn die Umsetzung der Forderung nach automatisierter Offenlegung des Quellcodes der Abhörsoftware nach jedem Einsatz aus nachvollziehbaren Gründen eher nicht stattfinden wird, zeigt dies umso mehr, welche Relevanz die restlose Löschung der Software vom Zielsystem nach einer durchgeführten Quellen-TKÜ hat.

4.3 Funktionsumfang der Abhörsoftware

Neben der Installation und Deinstallation der Abhörsoftware auf dem Zielsystem birgt auch deren Betrieb einige Probleme. Der Betrieb der Software muss beispielsweise so gestaltet sein, dass es keinem Dritten möglich ist, die Kontrolle über das Abhörprogramm zu erlangen. Nachdem der CCC am 08.10.2011 eine ältere Version der von Digitask entwickelten Abhörsoftware analysiert und unter anderem festgestellt hatte, dass keine ausreichende Verschlüsselung der Übertragungsstrecke der Abhörsoftware zu den Servern der Ermittler vorhanden war, gelang es dem CCC die Kontrolle über die Software zu übernehmen und sämtliche Funktionen zu nutzen.[170] Auch aus diesem Grund wurde der damalige Präsident des Bundeskriminalamts (BKA) *Jörg Ziercke* am 19.10.2011 vor dem Innenausschuss des Deutschen Bundestags zu den Vorwürfen des CCC befragt. Hier stellte *Ziercke* klar, dass die durch den CCC analysierte Software eine alte, nicht zum Einsatz gekommene, Version sei. Die zu diesem Zeitpunkt eingesetzte Version nutze einen gemeinsamen Schlüssel, der die Verschlüsselung zwischen Einsatzserver und der Abhörsoftware sicherstelle und sich somit ein unberechtigter Dritter, in Unkenntnis des Schlüssels, nicht als Kommunikationspartner der Abhörsoftware legitimieren könne.[171]

---

[170] Vgl. *Chaos Computer Club* 2011a.

[171] Vgl. *Deutscher Bundestag* 2011, S. 9.

Bereits am 26.10.2011 veröffentlichte der CCC eine weitere Analyse der nun zu diesem Zeitpunkt aktuellen Version der Abhörsoftware. Im Hinblick auf die Angaben *Zierckes* zu der bidirektionalen Verschlüsselung des Weges zwischen Einsatzserver und Abhörsoftware stellte der CCC klar: „Der CCC konnte sein selbstgeschriebenes Trojaner-Steuerprogramm in nur wenigen Stunden anpassen, die Schadsoftware weiterhin steuern und Code auf den Opfer-Rechnern nachladen."[172]

Anhand dieser Vorfälle zeigt sich deutlich, dass nicht nur das Überwinden von Verschlüsselungsvorkehrungen im Rahmen des Einsatzes einer Quellen-TKÜ von vorrangigem Interesse ist. Die Absicherung des Datenstroms zwischen den Servern der Ermittler und der auf dem Zielsystem eingebrachten Software sollte mindestens gleich großes Augenmerk erfahren. Da derartige Maßnahmen sich unter Umständen auch gegen informationstechnische Systeme richten könnten, die sich innerhalb der IT-Infrastruktur finanzkräftiger und innovativer Unternehmen befinden, sollte in Zeiten von internationaler Wirtschaftsspionage und Hackerangriffen[173] ein durch Sicherheitsbehörden eingebrachtes Sicherheitsrisiko in das Zielsystem unter allen Umständen vermieden werden.

Neben der Verhinderung selbstgeschaffener Sicherheitsrisiken muss ein zentrales Augenmerk der Sicherheitsbehörden auf dem Funktionsumfang der in das Zielsystem eingebrachten Abhörsoftware liegen. Die im Jahre 2016 zum Einsatz freigegebene und durch das BKA selbst programmierte Quellen-TKÜ-Software RCIS (Remote Communication Interception Software) in der Version 1.0 beschränkte sich auf die Möglichkeit des Abhörens von Skype-Gesprächen an Windows-Desktop-Computern.[174] Ein derart spezifischer Funktionsumfang ist in Zeiten von unterschiedlichsten verschlüsselten VoIP- und Messengerdiensten zur effektiven Strafverfolgung und Gefahrenabwehr definitiv nicht ausreichend.

Aus diesem Grund wurde bereits im Jahre 2017 RCIS in der Version 2.0 programmiert und anschließend für den Einsatz freigegeben. Diese Software soll nun in der Lage sein, vor allem in mobile Endgeräte wie Smartphones

---

[172] *Chaos Computer Club* 2011.

[173] Vgl. *Könen* 2017, S. 46; vgl. *Schwarzer* 2018, S. 492.

[174] Vgl. *Meister* 2018.

und Tablets implementiert zu werden, um Nachrichten in verschlüsselten Messengerdiensten überwachen zu können.[175] Welchen Funktionsumfang RCIS 2.0 genau aufweist, kann bis dato keiner offenen Quelle entnommen werden. Durch das BKA wird großer Wert auf die Geheimhaltung der Funktionsweisen von RCIS 2.0 gelegt. So wurde im April 2018 ein zu diesem Thema geplantes Interview der Süddeutschen Zeitung mit einem TÜV-Informationstechniker, dessen Arbeitgeber im Vorfeld der Freigabe an der Prüfung der Software beteiligt war, kurzfristig auf Drängen des BKA abgesagt.[176]

Neben den Eigenentwicklungen nutzt das BKA aktuell zusätzlich die bereits thematisierte kommerziell programmierte Software FinFisher/Finspy der Firma Gamma.[177] Diese wurde nach der oben beschriebenen Enttarnung durch den CCC und der damit verbundenen Einstellung von Digitask[178] bereits im Jahre 2012 erworben.[179] Die Genehmigung für den Einsatz von FinFisher/Finspy erfolgte durch das BMI im Januar 2018.[180] Bei FinFisher/Finspy handelt es sich um eine Software, die – zumindest in früheren Versionen – u. a. Funktionen wie Keylogger, sowie die Überwachung des Mikrofons und einer Webcam ermöglichte.[181] Diese Funktionsweisen führen zu einem weiteren Problem beim Einsatz von Abhörsoftware.

Im Gegensatz zu der zu geringen Funktionalität von RCIS 1.0, wies nun diese Version von FinFisher/Finspy einen zu großen Funktionsumfang auf. Denn „[...], [d]ass [bei einer Quellen-TKÜ] grds. nur eine **laufende,** also gerade stattfindende, **Telekommunikation** überwacht werden darf, versteht sich aus den Grundsätzen der Überwachungsmaßnahmen nach § 100a quasi von selbst, weil ansonsten nur eine unter den strengeren Voraussetzungen des § 100b zulässige Online-Durchsuchung durchgeführt werden dürfte.“[182]

---

[175] Vgl. *Meister* 2018.
[176] Vgl. *Tanriverdi* 2018.
[177] Vgl. *Meister* 2018.
[178] Vgl. *Deutscher Bundestag* 2011, S. 9.
[179] Vgl. *Meister* 2017.
[180] Vgl. *Flade* 2018; vgl. *Meister* 2018.
[181] Vgl. *Meister* 2014; vgl. https://netzpolitik.org/wp-upload/Gamma-2011-Finfisher.pdf (besucht am 10.11.2018).
[182] *Graf* 2018, S. 410, Rn. 122, Hervorh. im Original.

4.4 Beschränkung von Freiheitsrechten

Die Durchführung von TKÜ-Maßnahmen und insbesondere Quellen-TKÜ-Maßnahmen stellt einen schwerwiegenden Eingriff in die Persönlichkeits- und Freiheitsrechte der Betroffenen dar. Ein Kommentar in der Süddeutschen Zeitung, nach der Implementierung der Quellen-TKÜ und der Online-Durchsuchung in die StPO, bezeichnet diese Maßnahmen als „Skandal“ und „[k]eine[n] Eingriff in die Privatsphäre, sondern ein[en] Einbruch.“[183] Auch Politiker der Oppositionsparteien sehen den Einsatz skeptisch. Die stellvertretende Vorsitzende der Partei „Die Linke“ bezeichnete diesen als „[...] ungebremsten Angriff auf Privatsphäre und Bürgerrechte.“[184]

Durch die Gesellschaft für Freiheitsrechte (GFF) wurde zudem am 22.08.2018 vor dem BVerfG Verfassungsbeschwerde gegen die Implementierung der Quellen-TKÜ und der Online-Durchsuchung in die StPO im Rahmen der Verabschiedung des Gesetzes zur effektiveren und praxistaglicheren Ausgestaltung des Strafverfahrens vom 23.08.2017[185] eingelegt.[186] Auch andere Vereine und Verbände wie der Bundesverband IT-Sicherheit (TeleTrusT), aber auch die Oppositionspartei FDP legten Verfassungsbeschwerde ein.[187]

Inwiefern der Einsatz einer Quellen-TKÜ in die Persönlichkeits- und Freiheitsrechte der Bürger eingreift und welche Problematiken dadurch entstehen, ist Gegenstand der nachfolgenden Ausführungen.

4.4.1 Fernmeldegeheimnis gem. Art. 10 Abs. 1 GG

„Das Fernmeldegeheimnis, auch Telekommunikationsgeheimnis genannt, schützt die unkörperliche Übermittlung von Informationen durch elektrische, elektromagnetische, optische, funktechnische digitale oder analoge Signale an individuelle Empfänger vor staatlicher Kenntniserlangung.“[188]

---

[183] *Prantl* 2017.
[184] *Renner* 2018.
[185] BGBl. I 2017, S. 3202 – 3213.
[186] Vgl. *Strate* 2018.
[187] Vgl. *Beuth* 2018.
[188] *Liebig* 2015, S. 134; Vgl. BVerfG NJW 2010, 833, 835; 2012, 1419, 1421.

Die am Telekommunikationsverkehr beteiligten Personen sollen hierdurch dasselbe Recht auf Vertraulichkeit des gesprochenen Wortes erlangen, wie bei der direkten Konversation von Anwesenden.[189] Neben den konkreten Gesprächsinhalten sind auch Verkehrs- und Standortdaten vom Schutzbereich des Art. 10 GG umfasst.[190]

Auch im Hinblick auf die Überwachung verschlüsselter internetbasierter Telekommunikation mittels Infiltration eines informationstechnischen Systems ist Art. 10 Abs. 1 GG berührt. Hierzu führt das BVerfG aus, dass es unerheblich sei, „[...] ob die Maßnahme technisch auf der Übertragungsstrecke oder am Endgerät der Telekommunikation ansetzt."[191] Jedoch führt das BVerfG hierzu in seinem Urteil zur Online-Durchsuchung vom 27.02.2008[192] weiter aus, dass der Schutzbereich des Art. 10 Abs. 1 GG unter Umständen nicht ausreichend für den Persönlichkeitsschutz ist, wenn der Staat mittels Quellen-TKÜ in ein informationstechnisches System eingreift. Durch das Einbringen der Überwachungssoftware in das Endgerät des Betroffenen sei demnach die technische Hürde überwunden, um nicht nur Zugriff auf die Telekommunikation, sondern auf die gesamten Daten auf dem infiltriertem Endgerät des Betroffenen zu erhalten.[193] „Dadurch entstehe stets das Risiko einer weit über die Telekommunikationsdaten hinausgehenden Informationserhebung, welches bei der herkömmlichen netzbasierten Telekommunikationsüberwachung nicht bestehe."[194] Art. 10 Abs. 1 GG kann demnach bei einer Quellen-TKÜ nur alleine betroffen sein, wenn durch technische und rechtliche Vorgaben eine Beschränkung auf die Übermittlung von Kommunikationsdaten vorgenommen wird.[195]

4.4.2 Unverletzlichkeit der Wohnung gem. Art. 13 Abs. 1 GG

Als weiteres, durch TKÜ-Maßnahmen betroffenes Grundrecht käme Art. 13 Abs. 1 GG in Betracht. In den Fällen, in denen mittels Quellen-TKÜ ein in der

---

[189] Vgl. *Liebig* 2015, S. 134; vgl. BVerfG NJW 2006, 641.
[190] Vgl. BVerfG NJW 2008, 822.
[191] BVerfG NJW 2002, 3619.
[192] BVerfG NJW 2008, 822.
[193] Vgl. BVerfG NJW 2008, 822, 825.
[194] *Liebig* 2015, S. 135.
[195] Vgl. BVerfG NJW 2008, 822, 827.

Wohnung des Betroffenen befindliches Endgerät infiltriert wird, könnte ein Eingriff in das Grundrecht auf Unverletzlichkeit der Wohnung vorliegen.

Entsprechend der vorliegenden Ausführungen liegt unzweifelhaft ein derartiger Eingriff vor, wenn Mitarbeiter der Sicherheitsbehörden sich Zutritt zur Wohnung des Betroffenen verschaffen, um vor Ort Software zur Durchführung einer Quellen-TKÜ auf das betreffende Gerät aufzuspielen.

Doch auch der Eingriff in den Schutzbereich des Art. 13 Abs. 1 GG mittels technischer Mittel von außerhalb der Wohnung ist möglich. In Bezug auf § 100c StPO (akustische Innenraumüberwachung von Wohnungen; „Großer Lauschangriff“) stellte das BVerfG klar, dass hierbei ein Eingriff in den Schutzbereich des Art. 13 Abs. 1 GG vorliegt.[196] Im Hinblick auf die Quellen-TKÜ herrschen hierzu in der Rechtsprechung unterschiedliche Ansichten.

Das LG Hamburg setzt in seinem Beschluss vom 01.10.2007[197] die von außerhalb der Wohnung durchgeführte heimliche Installation eines „Spionageprogramms“ auf dem in der Wohnung befindlichen Endgerät des Betroffenen einem körperlichen Eindringen in die Wohnung gleich.[198] Dem entgegen begründet das BVerfG, dass es für die Ermittlungen irrelevant sei, ob sich das infiltrierte informationstechnische System innerhalb oder außerhalb der Wohnung des Betroffenen befinde. Sollte das Einbringen der Überwachungssoftware also von außerhalb der Wohnung des Betroffenen erfolgen (z. B. mittels E-Mail-Anhang), sei nicht klar bestimmbar, ob sich das zu infiltrierende Endgerät ständig, nur zeitweise oder überhaupt nicht in der Wohnung des Betroffenen befindet. Der raumbezogene Schutz des Art. 13 Abs. 1 GG sei demnach nicht in der Lage, die spezifische Gefährdung des informationstechnischen Systems abzuwenden.[199]

Laut *Böckenförde* kann die Betroffenheit des Schutzbereichs des Art. 13 Abs. 1 GG davon abhängig gemacht werden, ob „[...] die eine Wohnung umgebenden räumlichen Barrieren [...]“[200] physisch überwunden werden.[201]

---

[196] Vgl. BVerfG NJW 2004, 999, 1001.
[197] LG Hamburg Beschl. v. 01.10.2007 – 629 Qs 29/07.
[198] Vgl. *Liebig* 2015, S. 137.
[199] Vgl. BVerfG NJW 2008, 822, 826; Vgl. *Liebig* 2015, S. 137.
[200] *Böckenförde* 2008, S. 926.
[201] Vgl. *Liebig* 2015, S. 138.

Diese Rechtsauffassung erscheint fraglich, weil – wie bereits beschrieben – Programme wie FinSpy oder Digitask theoretisch ebenfalls über Funktionen verfügen, die beispielsweise die Ansteuerung und die Offenschaltung eines mit einem in der Wohnung des Betroffenen befindlichen informationstechnischen System verbundenen Mikrofons ermöglichen. Aus diesem Grund erscheint die Auffassung des BVerfG, dass, wenn der Schutz vor einer Überwachung der Wohnung durch technische Mittel, auch wenn diese von außerhalb der Wohnung eingesetzt werden würden, nicht unter den Schutzbereich des Art. 13 Abs. 1 GG fallen würde, dies dem Schutzzweck der Norm nicht entspräche, zutreffend.[202]

Eine Quellen-Telekommunikationsüberwachung, die nur auf die durch das überwachte Endgerät übermittelte Telekomunikation Zugriff erlangt, stellt aus der Sicht des Autors jedoch keinen Eingriff in Art. 13 Abs. 1 GG dar. Sollte dies von Teilen der Literatur gegensätzlich gesehen werden, müsste konsequenterweise auch die „herkömmliche“ Telekommunikationsüberwachung unter den Gesichtspunkten des Art. 13 Abs. 1 GG betrachtet werden, sofern das überwachte Gespräch aus einer Wohnung heraus geführt wird. Eine derart weite Auslegung des Schutzbereichs des Art. 13 GG wird jedoch wiederum nicht vertreten.

4.4.3 Recht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Das Grundrecht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i. V. m. Art. 1 GG ist eine Ausprägung des allgemeinen Persönlichkeitsrechts. Es ermöglicht dem Betroffenen grundsätzlich selbst zu entscheiden, ob, wann und wie er seine persönlichen Lebenssachverhalte offenbart.[203] Durch das Grundrecht werden persönliche und personenbezogene Daten geschützt. Der Schutzumfang des Rechts auf informationelle Selbstbestimmung umfasst sowohl sensible Daten als auch solche, die nur einen geringen Informationsgehalt aufweisen.[204] Jede Kenntnisnahme, Erhebung,

[202] Vgl. BVerfG NJW 2004, 999; vgl. *Sodan* 2018, S. 189, Rn. 12.
[203] Vgl. BVerfG NJW 2013, 1335; vgl. *Sodan* 2018, S. 45, Rn. 6b.
[204] Vgl. BVerfG NJW 2007, 2464, 2466; vgl. *Liebig* 2015, S. 138.

Speicherung, Veröffentlichung, Weitergabe und sonstige Verwendung der geschützten Daten stellt demnach einen Eingriff in das Grundrecht dar.[205]

Gegen staatliche Überwachungsmaßnahmen – auch durch den Eingriff in ein informationstechnisches System – bietet das Recht auf informationelle Selbstbestimmung allerdings keinen ausreichenden Schutz. So stellt das BVerfG klar, dass das Grundrecht auf informationelle Selbstbestimmung dem Einzelnen das Recht einräumt, über seine persönlichen Daten (z. B. Namen, Adresse, Geburtsdatum, usw.) selbst zu bestimmen. Dies trägt dem besonderen Schutzbedürfnis des Nutzers eines informationstechnischen Systems jedoch nicht vollständig Rechnung.[206] Dadurch, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf informationstechnische Systeme angewiesen ist, gibt er allein durch deren Nutzung einen wesentlich größeren Datenumfang preis. Ein Dritter, der sich Zugang zu diesen Daten verschafft, hat somit die Möglichkeit, ohne die Nutzung weiterer Datenerhebungsverfahren, einen tiefen Einblick in die Persönlichkeit des Betroffenen zu erlangen.[207] Um diesem Umstand zu begegnen entwickelte die Rechtsprechung das spezifischere Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

4.4.4 Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Bei dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG handelt es sich um ein recht junges Grundrecht. In seiner Grundsatzentscheidung zu den Regelungen der Online-Durchsuchung im Verfassungsschutzgesetz des Landes Nordrhein-Westfalen vom 27.02.2008[208] leitete das BVerfG dieses aus dem allgemeinen Persönlichkeitsrecht ab.

---

[205] Vgl. BVerfG NJW 1984, 419.
[206] Vgl. BVerfG NJW 2008, 822, 826f.
[207] Vgl. BVerfG NJW 2008, 822, 827.
[208] BVerfG NJW 2008, 822.

Der durchaus komplizierte Name des neuen Grundrechts fand sich in der öffentlichen Berichterstattung seitdem vermehrt in vereinfachter Form als „Computer-Grundrecht“[209] oder „IT-Grundrecht“[210] wieder.

Das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme tritt demnach zu den Grundrechten nach Art. 10 Abs. 1 GG, Art. 13 Abs. 1 GG und dem Recht auf informationelle Selbstbestimmung hinzu, „[...]soweit diese keinen oder keinen hinreichenden Schutz gewähren.“[211] Durch die Nutzung von moderner Informationstechnik erhält der Einzelne neue Möglichkeiten, seine Persönlichkeit zu entfalten.

Hierdurch entstehen jedoch auch neuartige Gefährdungen für die Persönlichkeit.[212] Diese neuen Gefährdungen für die Persönlichkeit entstehen dadurch, dass der Einzelne auf die Nutzung von informationstechnischen Systemen angewiesen ist und diesen seine persönlichen Daten anvertraut.

Die Brisanz der durch komplexe informationstechnische Systeme erfassten Daten, ergibt sich daraus, dass es sich bei diesen sowohl um bewusst angelegte als auch um durch das System selbständig generierte Daten handelt. Solche Daten beinhalten die Möglichkeit, dass sie Rückschlüsse auf Verhaltensweisen, persönliche Verhältnisse und Eigenschaften des Nutzers zulassen und sie sich dadurch mitunter bis zur Persönlichkeitsprofilbildung auswerten lassen.[213]

Ein staatlicher Eingriff zur Erlangung dieser Daten gehe demnach in seinem „[...] Gewicht für die Persönlichkeit des Betroffenen über einzelne Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützt, weit hinaus.“[214] Ein Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme liegt grundsätzlich dann vor, wenn „[...] die Integrität des geschützten informationstechnischen Systems angetastet wird, indem so auf das System zugegrif-

---

[209] Vgl. *Hipp* 2008.
[210] Vgl. *Beckedahl* 2013; vgl. *Baum / Kurz / Schantz* 2013.
[211] BVerfG NJW 2008, 822, 824.
[212] Vgl. BVerfG NJW 2008, 822, 827.
[213] Vgl. BVerfG NJW 2008, 822, 827; vgl. *Bratke* 2013, S. 121.
[214] BVerfG NJW 2008, 822, 827; vgl. *Sodan* 2018, S. 45, Rn. 6c.

fen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können."[215]

Jedoch erstreckt sich der Schutzbereich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme lediglich auf den heimlichen Zugriff im Rahmen verdeckter Maßnahmen. Offene Datenerhebung durch die Sicherstellung von informationstechnischen Systemen, beispielsweise im Rahmen von Durchsuchungsmaßnahmen, werden nicht unter den Schutzbereich des Grundrechts subsummiert. Dies ergibt sich maßgeblich aus den Leitsätzen des Urteils, sowie aus den Ausführungen zur Verhältnismäßigkeit, die sich nur auf heimliche Maßnahmen beziehen.[216]

Zur Quellen-TKÜ führt das BVerfG aus, dass mit dem Einbringen der benötigten Software in das Zielsystem „[...] die entscheidende Hürde genommen [ist], um das System insgesamt auszuspähen."[217] Allerdings ist Art. 10 Abs. 1 GG „[...] der alleinige grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zu einer „Quellen-Telekommunikationsüberwachung", wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt. Dies muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein."[218]

Dies zeigt die Wichtigkeit der Beschränkung der Funktionalität von Software wie FinSpy/FinFisher bzw. RCIS im Rahmen einer Quellen-TKÜ und die notwendige Abgrenzung der Quellen-TKÜ zur eingriffsintensiveren Online-Durchsuchung. Wenn demnach sichergestellt werden kann, dass die in das informationstechnische System eingebrachte Software „lediglich" auf Daten eines laufenden Telekommunikationsvorgangs zugreift und diese ausleitet, liegt kein Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme vor.[219]

---

[215] BVerfG NJW 2008, 822, 827; vgl. *Liebig* 2015, S. 141.
[216] Vgl. *Liebig* S. 141.
[217] BVerfG NJW 2008, 822, 825.
[218] BVerfG NJW 2008, 822, 826; vgl. *Roggan* 2017, S. 821.
[219] Vgl. *Roggan* 2017, S. 822.

4.4.5 Verfassungsrechtliche Bedenken des Gesetzgebungsverfahrens

Für besonderes Unverständnis bei einigen Oppositionspolitikern, Datenschützern und Teilen der Fachöffentlichkeit sorgte auch die Art und Weise, wie das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 23.08.2017[220] letztendlich im Bundestag beschlossen wurde.

Um das Gesetz noch in der letzten Wahlperiode zu beschließen, brachte die Koalition die neuen Überwachungsbefugnisse in einem Änderungsantrag zu einem Gesetzesentwurf unter, der beispielsweise Neuerungen zu strafrechtlichen Fahrverboten enthielt. Dadurch, dass die Änderungen in ein laufendes Verfahren eingeführt wurden, wurde sowohl die erste Beteiligung des Bundesrats als auch die vorgesehenen drei Lesungen der Änderungen vermieden. Eine Beteiligung der Bundesdatenschutzbeauftragten fand ebenfalls nicht statt.[221]

Diese Art und Weise der Gesetzgebung erweckt den Eindruck, dass die Verabschiedung eines Gesetzes zu einem derart grundrechtsintensiven Eingriff, wie der Infiltration eines informationstechnischen Systems mit Abhörsoftware, durch staatliche Stellen ohne besondere Prüfung und öffentliches Interesse stattfinden sollte.

Rubbert spricht beispielsweise von einem „Taschenspielertrick“ und merkt an, dass der Gesetzgeber in einem „[...] verfassungsrechtlich fragwürdigen Verfahren [eine] verfassungsrechtlich fragwürdige Ermächtigungsgrundlage in die StPO eingeführt [hat] – unter Vermeidung jeder gesellschaftlichen Auseinandersetzung, einer Anhörung der Fachverbände oder auch nur der Bundesdatenschutzbeauftragten.“[222]

Als Begründung für diese Vorgehensweise gab die stellvertretende Vorsitzende der SPD-Bundestagsfraktion *Eva Högl* an, dass angesichts der ständigen Terrorgefahr Grund zur Eile bestanden habe.[223] Diese Begründung erscheint eher fragwürdig. So stellt auch *Rubbert* fest, dass diese Eile nach

[220] BGBl. I 2017, S. 3202 – 3213.
[221] Vgl. *Grunert* 2017.
[222] *Rubbert* 2017, S. I.
[223] Vgl. *Grunert* 2017.

näherer Überprüfung weder geboten noch angebracht war.[224] Schließlich ginge es nicht „[...] um die Abwehr von drohenden Gefahren für überragend wichtige Rechtsgüter, sondern um Einsätze im Bereich der Strafverfolgung.“[225]

Diese Vorgehensweise öffnete somit Tür und Tor für die eingangs erwähnten Verfassungsbeschwerden. Fraglich ist, ob ein bedachteres und reflektierteres – ggf. verfassungskonformes – Gesetzgebungsverfahren zur gesetzeskonformen Etablierung der Quellen-TKÜ als mächtige Maßnahme der Strafprozessordnung nicht die bessere Alternative gewesen wäre. Inwiefern sich das BVerfG mit den im Rahmen der Verfassungsbeschwerden vorgetragenen Bedenken befasst und welche Konsequenzen diese in Zukunft für eine effektive Strafverfolgung haben werden, ist zum jetzigen Zeitpunkt nicht absehbar.

5 Lösungsansätze

Nachdem sich der vorangegangene Teil v. a. mit den rechtlichen und tatsächlichen Problemen der Überwachung verschlüsselter Telekommunikation befasst hat, befasst sich das folgende Kapitel mit der Erarbeitung von Lösungsansätzen. Es wird erarbeitet, inwiefern eine Anpassung sowohl der Rechtsgrundlagen als auch der Gefahrenabwehr- und Strafverfolgungsbehörden selbst an die technisch veränderte Realität vonstatten gehen könnte. Weiterhin wird umgrenzt, inwiefern eine Erweiterung der Eingriffsbefugnisse und die damit einhergehende Beschränkung von Freiheitsrechten durch die Bevölkerung Akzeptanz erfahren könnte und welcher Ausgleich hierfür in Betracht käme.

[224] Vgl. *Rubbert* 2017, S. I.
[225] *Rubbert* 2017, S. I.

5.1 Anpassung der Gefahrenabwehr- und Strafverfolgungsbehörden an technisch veränderte Realität

Bereits in den 1990er Jahren versuchte die Regierung der Vereinigten Staaten von Amerika die Hersteller von Computerchips dazu zu verpflichten, Hintertüren („Backdoors“) zu integrieren, damit staatlichen Stellen die Überwachung verschlüsselter Kommunikation ermöglicht werde.[226] Der darauffolgende Widerstand der Zivilgesellschaft und technische Probleme führten dazu, dass Verschlüsselungsstandards die digitale Welt sicherer gemacht haben.[227] In Zeiten des internationalen Terrorismus scheint dieser Trend sich jedoch in die entgegengesetzte Richtung zu entwickeln. Das BMI gibt in seiner Cyber-Sicherheitsstrategie für das Jahr 2016 neben dem Ansatz „Sicherheit durch Verschlüsselung“ auch den Ansatz „Sicherheit trotz Verschlüsselung“ als seine Strategie vor und fordert die technischen Fähigkeiten der Strafverfolgungs- und Sicherheitsbehörden analog dem technischen Stand in Sachen Verschlüsselung zu verbessern.[228] Fraglich ist, welche technischen Maßnahmen hierzu nötig wären. Aktuelle Zahlen im Hinblick auf die Häufigkeit des repressiven Einsatzes von Abhörsoftware (Quellen-TKÜ) liegen zum jetzigen Zeitpunkt noch nicht vor.

Obwohl § 101b Abs. 1 StPO darauf verweist, dass diese Zahlen auf der Website des Bundesamts für Justiz veröffentlicht werden müssen, stammen die letzten Zahlen hinsichtlich des Einsatzes von TKÜ aus dem Jahr 2016 und somit aus der Zeit vor der Novellierung der §§ 100a ff. StPO.[229]

Auch durch das BKA wurde bis dato keine diesbezügliche Statistik veröffentlicht. Vielmehr verweist der Internetauftritt zur Quellen-TKÜ und Online-Durchsuchung des BKA darauf, dass „[...] [d]as BKA [...] aus einsatztaktischen Gründen keine Auskünfte darüber erteilen [kann], wie oft die Software bereits zum Einsatz gekommen ist.“[230] Die Häufigkeit des Einsatzes dürfte

[226] Vgl. *Schulze* 2017, S. 1.
[227] Vgl. *Schulze* 2017, S. 1.
[228] Vgl. *Bundesministerium des Innern* 2016, S. 15.
[229] Vgl. *Bundesamt für Justiz* 2017.
[230] *Bundeskriminalamt* o. D.

sich jedoch aktuell noch in Grenzen halten. So gebe es beispielsweise noch Probleme bei der Infiltration der Zielgeräte.[231]

Für den höchstkomplexen Einsatz der Abhörprogramme im Rahmen der Quellen-TKÜ und die stetige Befassung mit der Weiterentwicklung informationstechnischer Systeme und deren Verschlüsselungsmechanismen erscheint es somit erforderlich, dass eine gewisse Expertise im IT-Bereich den Strafverfolgungs- und Gefahrenabwehrbehörden an die Hand gegeben wird.

Hierzu beschloss die Bundesregierung in ihrer Cyber-Sicherheitsstrategie des Jahres 2016 die Gründung einer neuen Behörde. Diese wurde „Zentrale Stelle für Informationstechnik im Sicherheitsbereich“ (ZITiS) genannt und im Geschäftsbereich des Bundesministeriums des Innern eingerichtet.[232] Dass die ZITiS vor allem auch zur Behebung von Problemen im Zusammenhang mit der Verschlüsselung von Telekommunikation gegründet wurde, zeigt die Beschreibung des Arbeitsfelds „Telekommunikationsüberwachung“ auf der Website: „Der ständige Wandel der Telekommunikationswelt führt dazu, dass die TKÜ ständig an die technologische Entwicklung angepasst werden muss. ZITiS unterstützt deshalb, in enger Abstimmung mit den Bedarfsträgern, die Forschung und Entwicklung neuer Methoden und Strategien zur nachhaltigen Sicherung der TKÜ-Fähigkeiten des Bundeskriminalamts, der Bundespolizei und des Bundesamts für Verfassungsschutz.“[233] Weiterhin verfügt ZITiS über das Arbeitsfeld „Kryptoanalyse“, das „[...] insbesondere Projekte in der Digitalforensik und Telekommunikationsüberwachung, in denen der Umgang mit Verschlüsselung eine große Rolle spielt [unterstützt].“[234]

Die Einrichtung einer derartigen Behörde, die unterstützende Tätigkeiten in einem hoch komplexen Bereich innehat, erscheint vor dem Hintergrund der effektiven Strafverfolgung und Gefahrenabwehr äußerst sinnvoll. Auch wenn es Mitte 2018, etwa ein Jahr nach der Gründung von ZiTIS, noch an geeignetem sach- und fachkundigem Personal mangelt und nur 56 der 120 Perso-

[231] Vgl. *Flade* 2018a.
[232] Vgl. *Könen* 2017, S. 59; vgl. *Bundesministerium des Innern* 2016.
[233] *Zentrale Stelle für Informationstechnik im Sicherheitsbereich* o. D.
[234] *Zentrale Stelle für Informationstechnik im Sicherheitsbereich* o. D.a.

nalstellen besetzt werden konnten,[235] wurden doch vielversprechende Projekte publik.

So wurde im Rahmenprogramm der Bundesregierung und des Bundesministeriums für Bildung und Forschung (BMBF) zur Quantentechnologie aus September 2018 bekannt, dass die ZITiS an ihrem Standort der Bundeswehrakademie in München, gemeinsam mit dem Bundesministerium für Verteidigung (BMVg), die Nutzung eines Quantencomputers u. a. zur erfolgreichen Entschlüsselung verschlüsselter Daten plant.[236]

Die weitere personelle und finanzielle Aufstockung entsprechender Stellen dürfte Voraussetzung für eine effektive Gefahrenabwehr und Strafverfolgung im technologisierten Zeitalter sein.

Neben der technologischen Aufrüstung hinsichtlich der Möglichkeiten einer Entschlüsselung von modernen Kommunikationsverschlüsselungsstandards könnte beispielsweise mit Hilfe der Expertise der sachkundigen Mitarbeiter der ZITiS eine weitere Möglichkeit des Umgehens von Verschlüsselungsmechanismen geprüft werden.

Die Nutzung der bereits beschriebenen „Exploits“[237] für VoIP- und Messengerdienste würde die Möglichkeit bieten, auch ohne aufwendige Entschlüsselungsverfahren und Quantencomputer an den über sie geführten Kommunikationsinhalt zu gelangen. Diese Schadprogramme, die in der entsprechenden Software entdeckte Sicherheitslücken ausnutzen, könnten durch die Sicherheitsbehörden angekauft werden. Dieser Ankauf würde jedoch nicht in einem ordentlichen Vergabeverfahren stattfinden. Vor allem im Darknet fluoriert der Handel mit Exploits. Für die exklusive Kenntnis einer Sicherheitslücke im Apple-Betriebssystem iOS werden Preise von ca. 500.000 Euro verlangt.[238]

Fraglich erscheint, ob eine derartige Vorgehensweise rechtsstaatlich und faktisch sinnvoll ist. Der Staat würde finanzielle Mittel an dubiose „Geschäftspartner“ transferieren, um das Wissen über entsprechende Sicher-

---

[235] Vgl. *Pinkert / Strozyk / Tanriverdi* 2018.
[236] Vgl. *Bundesministerium für Bildung und Forschung* 2018, S. 25.
[237] Vgl. *Siller* 2017.
[238] Vgl. *Schieb* 2016.

heitslücken zu erwerben. Hierbei wäre weder die Exklusivität dieser Informationen, noch die Nutzungsdauer des Exploits absehbar. Der bereits thematisierte Konflikt zwischen der Nutzung des Exploits und der gefahrenabwehrenden Mitteilung über selbigen an den Anbieter der betreffenden Software, wird im weiteren Verlauf dieser Arbeit im Zusammenhang mit der sog. „Kryptodebatte“[239] noch lösungsorientiert problematisiert.

In der Gesamtschau erscheint eine derartige Vorgehensweise durch Sicherheitsbehörden jedoch nicht zielführend und vor allem unter rechtsstaatlichen Gesichtspunkten äußerst bedenklich.

Neben der Etablierung eigener staatlicher Stellen könnte auch die IT-Expertise externer etablierter Unternehmen in Anspruch genommen werden, um Zugriff auf verschlüsselte Telekommunikation zu erhalten. Im Bereich der Entschlüsselung von physisch verfügbaren Endgeräten kann exemplarisch in diesem Zusammenhang die israelische Firma Cellebrite Forensics[240] Erwähnung finden.

Aus der Antwort einer kleinen Anfrage der Partei DIE LINKE an den sächsischen Landtag vom 02.09.2015 hinsichtlich der Auswertung mehrerer im Rahmen einer Demonstration beschlagnahmter IT-Gegenstände geht hervor, dass die Auswertung dieser mittels des von Cellebrite Forensics angebotenen „Universal Forensic Extraction Device“ (UFED) stattgefunden hat.[241] Auch das BKA zeigt mit dem bereits thematisierten Erwerb der Abhörsoftware FinSpy/Finfisher, dass ein Rückgriff auf die Expertise privater Unternehmen eine erfolgversprechende Alternative zu Eigenentwicklungen darstellen kann. Es gilt jedoch zu beachten, dass die Beauftragung privater Unternehmen mit der Entwicklung einer Software für derart grundrechtsintensive Eingriffe wie die Quellen-TKÜ stets ein gewisses Risiko birgt. Vor allem die Beauftragung ausländischer Unternehmen könnte Sicherheitsrisiken in einem derart sensiblen Bereich bergen.

---

[239] Vgl. *Schallbruch* 2018, S. 79ff.

[240] https://www.cellebrite.com/de/startseite/ (besucht am 13.11.2018).

[241] Vgl. LT-Drs. 6/2408.

5.2 Anpassung der Rechtsgrundlagen an technisch veränderte Realität

Neben technischen und organisatorischen Lösungsansätzen im Bereich der Strafverfolgungs- und Gefahrenabwehrbehörden käme auch die Anpassung der Rechtsgrundlagen zur sachgerechteren und problemfreieren Überwachung verschlüsselter Telekommunikation in Betracht.

Andere Staaten haben in diesem Zusammenhang bereits weitgreifende Regelungen getroffen. In Russland wurde beispielsweise bereits im Jahre 2016 ein Gesetz geschaffen, das Firmen verpflichtet, staatliche Hintertüren in Kommunikationssoftware zu implementieren. China führte im Januar 2017 eine Lizensierungspflicht für VPN-Clients ein. Hiermit soll vermieden werden, dass die Chinesen mithilfe westlicher VPN-Dienste die staatliche Internetzensur umgehen. Verstöße hiergegen sind mit hohen Strafen bewehrt.[242]

Derartige Bemühungen sind jedoch nicht nur in autoritären Regimen gegenwärtig. Auch die Geheimdienstpartnerschaft „Five Eyes“ unter Beteiligung der USA, Kanada, Großbritannien, Australien und Neuseeland betreibt eine fortwährende Initiative, staatliche Vorgaben hinsichtlich einer Auflockerung von Verschlüsselungsstandards zu schaffen.

So wurde im Jahr 2016 in Großbritannien die Investigatory Power Bill verabschiedet. Durch dieses Gesetz können Internetdienstleister dazu verpflichtet werden auf Anordnung Verschlüsselungen aufzuheben. Weiterhin ermöglicht sie, Firmen zu verpflichten, Backdoors in ihre Software zu integrieren oder Sicherheitsupdates zu blockieren, damit staatliche Stellen Zugriff auf die Telekommunikation erhalten.[243] In den USA wurde im Jahr 2016 die sog. Burr-Feinstein Encryption Bill entwickelt, die vorsieht, Unternehmen zu verpflichten, die Sicherheit ihrer Produkte absichtlich zu senken und die Firmen bei Vorliegen eines Gerichtsbeschlusses zu verpflichten, die Verschlüsselung der Kommunikation aufzuheben.[244] Dieser Gesetzentwurf wurde jedoch bis dato nicht verabschiedet.[245]

---

[242] Vgl. *Schulze* 2017, S. 2.
[243] Vgl. *Schulze* 2017, S. 2.
[244] Vgl. *Conger* 2016.
[245] Vgl. *Schulze* 2017, S. 2.

Fraglich erscheint in diesem Zusammenhang, welchen Nutzen derartige Gesetzesänderungen in Deutschland hätten und ob diese überhaupt durchführbar wären. Vor allem die gesetzliche Pflicht zur Aufhebung von Verschlüsselungsmechanismen dürfte auf breiten öffentlichen Widerstand stoßen.

Wie bereits im Rahmen dieser Arbeit thematisiert, stellt nicht nur die Umgehung der Verschlüsselung zur Strafverfolgung und Gefahrenabwehr eine wichtige Säule der inneren Sicherheit dar. Die Verschlüsselung von Telekommunikationsdaten muss ebenfalls hohe Priorität haben. Welche Gefahren bei nicht vorhandener oder unzureichender Verschlüsselung entstehen, zeigte der CCC – wie bereits thematisiert – im Jahre 2011, als es ihm zweimal innerhalb kürzester Zeit gelang, die Kontrolle über die damals durch das BKA eingesetzte Abhörsoftware des Herstellers Digitask zu erlangen.[246]

Die im Jahre 2016 durch das BMI vorgegebenen Strategieansätze „Sicherheit durch Verschlüsselung“ und gleichermaßen „Sicherheit trotz Verschlüsselung“[247] zeigen auf, in welchem Dilemma sich der Gesetzgeber hierzulande hinsichtlich der Findung von Rechtsgrundlagen befindet, die Verschlüsselungsmechanismen zu Strafverfolgungs- oder Gefahrenabwehrzwecken außerkraftsetzen oder schwächen sollen.

So schreibt auch *Roggan* von einem Zielkonflikt zwischen Strafverfolgung und IT-Sicherheit, der größer kaum vorstellbar ist.[248] Die gegensätzlichen Strategieansätze des BMI und die Diskussion um den hierdurch entstehenden Zielkonflikt bezeichnet *Schallbruch* als „Kryptodebatte“.[249]

Bereits Anfang der 1990er Jahre hatte sich der damalige Bundesinnenminister *Manfred Kanther* (CDU) für eine gesetzliche Beschränkung der Kryptografie aus Sicherheitsgründen stark gemacht. Ende der 1990er Jahre wurde das Thema durch die rot-grüne Regierung unter *Gerhard Schröder* (SPD) wieder aufgegriffen, bevor sich die Bundesregierung 1999 in ihren „Eckpunkten der deutschen Kryptopolitik“[250] für eine freie Kryptografie aussprach.[251]

---

[246] Vgl. *Chaos Computer Club* 2011; vgl. *Chaos Computer Club* 2011a.
[247] Vgl. *Bundesministerium des Innern* 2016, S. 15.
[248] Vgl. *Roggan* 2018, S. 39.
[249] Vgl. *Schallbruch* 2018, S. 85.
[250] Vgl. *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* 1999.
[251] Vgl. *Schallbruch* 2018, S. 87.

Bis heute gelten dieser Kabinettsbeschluss und die darin festgelegten Eckpunkte fort. Unter anderem wurde die „[...] [a]ktive Förderung des Einsatzes von Verschlüsselungstechniken in der Verwaltung, bei Privatpersonen und in Wirtschaftsunternehmen, [...][die] Erbringung von Serviceleistungen, die den Gebrauch von effektiven Verschlüsselungsprogrammen für jedermann erleichtern, [...] Maßnahmen zum besonderen Schutz der Telekommunikation von Berufsgruppen, die besondere Verschwiegenheitspflichten unterliegen [...], Unterstützung von Wirtschaftsunternehmen beim Schutz ihrer geschäftlichen Telekommunikation [...]“[252] und einige Eckpunkte mehr beschlossen.

Auch die „[...] Trennung von ‚Code Maker[n]‘ und ‚Code Breaker[n]‘“[253] im Rahmen der Konstruktion des Bundesamts für Sicherheit in der Informationstechnik als Cyber-Sicherheitsbehörde und der ZITiS als ermittlungsunterstützende Zentralstelle zeigt, dass die Änderung gesetzlicher Grundlagen, die die Reduzierung der Sicherheit verschlüsselter Kommunikation hervorrufen, in Deutschland eher keine Alternative sind. Der Cyber-Sicherheit wird folglich ein ebenso hoher Stellenwert wie der effektiven Gefahrenabwehr und Strafverfolgung eingeräumt.

Freiling / Safferling / Rückert stellen jedoch noch eine weitere interessante Alternative zur Überwachung verschlüsselter Telekommunikation vor. So zeigen sie auf, dass es nach der Infiltration des Zielsystems technisch durchaus möglich wäre, den verwendeten Schlüssel der Ende-zu-Ende-Verschlüsselung aus dem Arbeitsspeicher des infiltrierten Systems auszulesen und ihn an die Ermittlungsbehörden weiterzuleiten. Dies würde es den Ermittlungsbehörden ermöglichen, mithilfe der herkömmlichen TKÜ, die Daten abzufangen und unter Zuhilfenahme des ausgelesenen Schlüssels lesbar zu machen, sodass eine Änderung der Rechtsgrundlage und eine damit einhergehende Schwächung der digitalen Sicherheitsarchitektur der BRD nicht notwendig wäre.[254]

Eine einfachere Möglichkeit Zugriff auf den benötigten Schlüssel zu erhalten, wäre jedoch eine Kooperation mit den Anbietern entsprechender verschlüsselter VoIP- und Messengerdienste wie Skype oder WhatsApp. Fraglich er-

---

[252] *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* 1999.

[253] *Schönbohm* 2018, S. 431.

[254] Vgl. *Freiling / Safferling / Rückert* 2018, S. 18; vgl. *Taubmann et al.* 2016, S. 114 – 123.

scheint jedoch, wie bereits dargestellt, ob diese Anbieter einer derartigen Kooperation zustimmen würden.[255] Da dies aus den bereits genannten Gründen eher unwahrscheinlich erscheint, ist weiter fraglich, ob auch die Möglichkeit der Verpflichtung dieser Dienste bestehen würde.

Die Problematik hinsichtlich der Subsumtion von VoIP- und Messengerdiensten unter die Legaldefinition der „Telekommunikationsdienste“ i. S. d. § 3 S. 1 Nr. 24 TKG wurde bereits im Rahmen dieser Arbeit thematisiert. Auch aus dem Grund, dass sich der Firmensitz von Diensten wie Skype und WhatsApp nicht in Deutschland befindet und diese somit nicht in den Wirkungsbereich des TKG fallen, erscheint eine übernationale Lösung an dieser Stelle als durchaus zielführender. Eine internationale Gesetzesgrundlage zur Verpflichtung der VoIP- und Messengerdiensteanbieter zur Herausgabe der verwendeten Schlüssel, um staatlichen Stellen die Überwachung der Telekommunikation zu ermöglichen, erscheint jedoch unrealistisch, zumal auch antidemokratische Regime von derartigen Regelungen profitieren könnten und es fraglich ist, welche Institution die Diensteanbieter international dazu verpflichten sollte.

Jedoch wäre eine Implementierung der Verpflichtung von derartigen Diensteanbietern hinsichtlich der Herausgabe der Schlüssel in europäisches Recht zumindest ein erster Schritt in die richtige Richtung.

Im Bereich der IT-Sicherheit existieren derartige Modelle bereits. Im Jahre 2013 schlug die Europäische Kommission eine Cyber-Securtiy-Strategy vor, die im August 2016 in die Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie) umgesetzt wurde.[256] Deutschland überführte diese mit dem „Gesetz zur Umsetzung der NIS-Richtlinie“ als einer der ersten EU-Mitgliedstaaten am 29.06.2017 in nationales Recht.[257]

Eine derartige Regelung hinsichtlich der Herausgabe von Schlüsseln durch VoIP- und Messengerdiensteanbieter sollte jedoch auf einer rechtlich ein-

[255] Vgl. *Freiling / Safferling / Rückert* 2018, S. 18.
[256] Vgl. *Schönbohm* 2018, S. 433 – 434.
[257] Vgl. *Schönbohm* 2018, S. 434.

wandfreien Grundlage erfolgen, um eine derart heftige Kontroverse wie um die europäische Richtlinie zur Vorratsdatenspeicherung[258] zu vermeiden.

Eine europäische Regelung böte jedenfalls die Möglichkeit, in einem nächsten Schritt auf Augenhöhe mit Verbündeten (beispielsweise den USA) über eine gemeinsame Vorgehensweise i. S. der Sicherheit beider Partner zu debattieren, um auch Dienste, die ihren Firmensitz bzw. Serverstandort dort unterhalten (beispielsweise WhatsApp), in entsprechende Regelungen mit einzubeziehen.

Die Verabschiedung eines übernationalen, auch transatlantischen Abkommens hinsichtlich der Zusammenarbeit bei Telekommunikationsmaßnahmen erscheint zumindest denkbar. Bereits im Jahre 2009 wurde das „Gesetz zur Umsetzung des Abkommens zwischen der Bundesrepublik Deutschland und der Regierung der Vereinigten Staaten von Amerika vom 1. Oktober 2008 über die Vertiefung der Zusammenarbeit zur Verhinderung und Bekämpfung schwerwiegender Kriminalität“ beschlossen.[259] Dieses regelt unter anderem den bilateralen Austausch und Abgleich von gespeicherten DNA-Profilen oder daktyloskopischen Daten. Nach einigen Schwierigkeiten, zu denen unter anderem datenschutzrechtliche Bedenken der Oppositionsparteien gehörten, wurde das Inkrafttreten des Gesetzes (mit Ausnahme des bilateralen Austauschs von DNA-Profilen) am 04.04.2012 bekanntgemacht.[260]

Auch wenn derartige Regelungen zunächst keine Lösung im Hinblick auf die IT-Sicherheit (Implementierung von „Backdoors“) erzielen würden, wäre eine erste Hürde auf dem Weg zu einer effektiven Gefahrenabwehr und Strafverfolgung in Zeiten von verschlüsselten Telekommunikationsverbindungen genommen.

---

[258] RL 2006/24/EG.

[259] BGBl. II 2009, S. 1010.

[260] BGBl. II 2012, S. 499a.

5.3 Spannungsfeld Freiheitsrechte vs. Gefahrenabwehr / Strafverfolgung

Vor allem in der Bundesrepublik Deutschland führt die Ausweitung von Befugnissen der Sicherheitsbehörden, insbesondere beim Thema Überwachungsmaßnahmen, regelmäßig in einen breiten öffentlichen Diskurs.

Unter dem Motto „Freiheit statt Angst“[261] finden diesbezüglich seit dem Jahr 2006 bis heute regelmäßige Demonstrationen in deutschen Großstädten statt, die sich vor allem gegen die Ausweitung von polizeilichen Eingriffsbefugnissen richten. Ein weiteres in diesem Zusammenhang gebrauchtes politisches Schlagwort entstand im Jahre 2007 und richtete sich gegen den damaligen Bundesinnenminister *Wolfgang Schäuble* (CDU) und dessen Pläne zur Vorratsdatenspeicherung: „Stasi 2.0“.[262]

Es handelt sich hierbei um eine Wortschöpfung aus dem Begriff „Web 2.0“[263], mit dem eine veränderte modernere Nutzung des Internets beschrieben wird, und des Kurzworts des berüchtigten und in der Deutschen Demokratischen Republik (DDR) als Nachrichtendienst und Geheimpolizei eingesetzten Ministeriums für Staatssicherheit (MfS).

Diese dem Internet entspringende Wortschöpfung zeigt somit auch, dass die öffentliche Empörung eines Teiles der deutschen Bevölkerung im Zusammenhang mit der Erweiterung der polizeilichen Eingriffsbefugnisse und insbesondere der Befugnisse zur Überwachung vor allem in der Geschichte Deutschlands zu suchen sind. Unzweifelhaft ist, dass die auf öffentlichkeitswirksamen Demonstrationen vertretene Meinung nicht zwingend mit einer Mehrheitsmeinung in der Bevölkerung gleichzusetzen ist. Es ist jedoch auch Aufgabe der Politik, sich dieser Meinung anzunehmen und den Ängsten der Menschen zu begegnen.

Fraglich erscheint daher, ob die Schaffung eines öffentlich breit akzeptierten Ausgleichs in Bezug auf die Erweiterung polizeilicher und strafprozessualer Eingriffsbefugnisse möglich ist.

---

[261] Vgl. https://freiheitstattangst.de/ (besucht am 15.11.2018).

[262] Vgl. *Vongehlen* 2007.

[263] Vgl. *Lackes* o. D.

Aktuell existieren bereits einige Vorschriften, die dem Schutz der Privatsphäre des Einzelnen gewidmet sind. So wurden bereits die strengen rechtlichen Voraussetzungen für die Anordnung von TKÜ-Maßnahmen im Rahmen dieser Arbeit thematisiert. Beginnend bei dem Richtervorbehalt der Anordnung von TKÜ-Maßnahmen – ganz gleich ob diese repressiver oder präventiver Natur sind – über den Schutz höchstpersönlicher Lebensbereiche (Kernbereich) bis hin zu Benachrichtigungs-, Speicher- und Löschfristen zeigt der Gesetzgeber, dass er sich der Intensität des Eingriffs in die Persönlichkeitsrechte des Einzelnen durch TKÜ-Maßnahmen durchaus bewusst ist.

Man kann sich dennoch die Frage stellen, ob die bereits dargestellten rechtlichen Hürden für den Einsatz der TKÜ ausreichend sind, um dem Schutz der Persönlichkeit des Einzelnen vollumfänglich gerecht zu werden.

Unzweifelhaft ist, dass der Staat in Zeiten von z. B. terroristischen Bedrohungen Möglichkeiten zum Schutz seiner Bevölkerung eingeräumt bekommen muss. Um diesen Schutz zu gewährleisten ist es essentiell, dass etwaige Gefahren bereits im Vorfeld – beispielsweise durch TKÜ-Maßnahmen – identifiziert werden können.

Doch muss kritisch hinterfragt werden, ob die Gefahr besteht, dass diese Möglichkeiten für andere staatliche Maßnahmen oder rein zur Überwachung der Bevölkerung missbraucht werden könnten.

Derartige Befürchtungen werden in Deutschland stets dann vermehrt geäußert bzw. medial thematisiert, wenn neue oder erweiterte Rechtsgrundlagen beschlossen und verabschiedet werden, die vor allem die Überwachung von Telekommunikation oder sonstige verdeckte Maßnahmen betreffen.

So wurde, wie bereits thematisiert, durch verschiedene Parteien und politische Interessenverbände gegen die Einführung der Eingriffsbefugnisse zur Quellen-TKÜ und Online-Durchsuchung Verfassungsbeschwerde eingelegt.[264]

Hinsichtlich der Vorratsdatenspeicherung musste der Gesetzgeber ebenfalls reagieren, da hier der EuGH diese in der vorherigen Form als nicht europa-

[264] Vgl. *Beuth* 2018.

rechtskonform angesehen hatte.[265] Durch die Änderung des § 100g StPO und die Implementierung von Speicherfristen in § 113b TKG reagierte der Gesetzgeber hierauf. Doch auch die dargestellten Änderungen und vor allem die Pflicht der Provider zur Speicherung sämtlicher Verbindungsdaten führten dazu, dass noch immer rechtliche Bedenken bestehen und ein Abruf von retrograden Standortdaten zu repressiven Zwecken aktuell nicht stattfinden kann, bis eine Entscheidung im Hauptsacheverfahren des OVG Münster[266] gefunden wird.

Hinsichtlich der Pflicht zur Vorratsdatenspeicherung lässt sich jedoch auch eine gegensätzliche Meinung vertreten. Selbst wenn die Vorratsdatenspeicherung in der nun gültigen Form auch tatsächlich umgesetzt werden würde, würden beispielsweise die Standortdaten gem. § 113b Abs. 1 Nr. 2 TKG nur für vier Wochen gespeichert werden. Dieser kurze Zeitraum wurde mit dem Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten[267] eingeführt und gewählt, um seitens des Gesetzgebers einen Ausgleich für den durch diese Maßnahme stattfindenden sehr intensiven Grundrechtseingriff zu schaffen.[268] Es erscheint jedoch zweifelhaft, ob eine Speicherung für nur vier Wochen einer effektiven und praxistauglichen Strafverfolgung Genüge tut.

An diesem Beispiel zeigt sich, dass der Gesetzgeber stets bemüht ist, einen entsprechenden Ausgleich zu schaffen. Jedoch zeigt sich auch, dass dieser nicht immer auf breite Akzeptanz stößt. So lässt sich festhalten, dass im gewählten Beispiel der gefundene Ausgleich weder im Sinne einer effektiven Strafverfolgung, noch im Sinne eines angemessenen Schutzes der Persönlichkeit des Einzelnen geeignet erscheint.

Im Sinne einer bürgernahen und transparenten Politik erscheint jedoch die Implementierung von Ausgleichen für die Einführung eingriffsintensiverer Rechtsgrundlagen, insbesondere hinsichtlich Überwachungsmaßnahmen, als notwendiges Instrumentarium, um auch in der Bevölkerung Akzeptanz für diese Maßnahmen zu schaffen.

---

[265] EuGH, NJW 2014, 2169.
[266] OVG Münster, Beschl. v. 30.06.2017 – 13 B 238/17.
[267] BGBl. I 2015, S. 2218 – 2228.
[268] Vgl. *o. V.* 2015a.

Die Art und Weise, wie die Einführung der Quellen-TKÜ und der Online-Durchsuchung mithilfe der Verabschiedung des derer zugrundeliegenden Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 23.08.2017[269] stattgefunden hat, trägt jedenfalls nicht zu einer breiteren Akzeptanz dieser Eingriffsbefugnisse bei.

6 Fazit

Die vorliegende kriminalistische Masterarbeit zeigte im Kontext des Themas Telekommunikationsüberwachung in Zeiten verschlüsselter Datenverbindungen und gesteigertem Datenschutzinteresse auf, dass – vor dem Hintergrund der forschungsleitenden Fragestellung: „Ist die TKÜ noch eine zeitgemäße Ermittlungsmethode der deutschen Strafverfolgungs- und Gefahrenabwehrbehörden?“ – eine kritische Reflexion dieser Thematik einige aktuelle rechtliche und tatsächliche Probleme beim Einsatz selbiger zu Tage führte. Doch existieren bereits umgesetzte, als auch neue, zu überdenkende Lösungsansätze, entsprechend der vorliegenden Darstellungen.

Die Telekommunikationsüberwachung wurde zunächst in das Themengebiet der Kriminalistik eingeordnet und es wurde festgestellt, dass sie am ehesten der speziellen Kriminalistik zugeordnet werden kann, wenn auch die zur Überwachung verwendete Technik einige Bezugspunkte zu dem Themengebiet der Kriminaltechnik aufweist.

Es erfolgte sodann eine historische Einordnung der Telefonie und der Telekommunikationsüberwachung. Diese verdeutlichte, dass der Telekommunikationsüberwachung bereits kurz nach Ende des zweiten Weltkriegs seitens der Besatzungsmächte eine enorme taktische Bedeutung zur Kontrolle der Besatzungszone zugeschrieben wurde. Auch wurde deutlich, dass sich sowohl die Rechtsgrundlagen als auch die technischen Voraussetzungen der Telekommunikationsüberwachung stetig der aktuellen Kriminalitätslage sowie dem sich rasant entwickelnden technischen Fortschritt anpassen mussten.

[269] BGBl. I 2017, S. 3202 – 3213.

Im Anschluss wurde eine Unterteilung in zwei große Themengebiete vorgenommen: Zum einen wurde die herkömmliche unverschlüsselte Telefonie und zum anderen die verschlüsselte internetbasierte Telekommunikation beleuchtet. Im Themengebiet der unverschlüsselten Telefonie erfolgte eine detaillierte Darstellung der Eingriffsbefugnisse und der technischen Grundlagen der diesbezüglichen herkömmlichen Telefonüberwachung.

Auch erfolgte ein Exkurs in eine aktuelle rechtliche Problematik im Hinblick auf die Erlangung retrograder Standortdaten von Mobiltelefonen. Es konnte aufgezeigt werden, dass aufgrund von europarechtlichen Bedenken aktuell die Erlangung dieser Daten durch Strafverfolgungsbehörden nicht möglich ist.

Diese Betrachtungen dienten als Basis für die weiteren Ausführungen zur verschlüsselten Telekommunikation. Hierauf Bezug nehmend erfolgte zunächst eine Erklärung der grundlegenden Begriffe, die zugleich die beiden zentralen, weil meist genutzten, Standards der verschlüsselten Telekommunikation erläuterten. Betreffend der Voice-Over-IP-Telefonie wurde sodann deren Funktionsweise anhand der Anwendung Skype verdeutlicht. Die Beschreibung der Funktionsweise von Messengerdiensten erfolgte am Beispiel der sehr beliebten Instant-Messaging-App WhatsApp. Auch die Bedeutung der beiden Dienste im Hinblick auf ihre enorme Nutzeranzahl und die damit ebenso einhergehende Relevanz im Bereich der Strafverfolgung und Gefahrenabwehr wurde herausgestellt.

Aufbauend auf den Ausführungen zur unverschlüsselten Telefonie und deren Überwachungsmöglichkeiten erfolgten sodann Erläuterungen zu den technischen Besonderheiten der Überwachung verschlüsselter Telekommunikation. Es wurde insbesondere herausgestellt, dass aktuell nur die Quellen-TKÜ adäquate Möglichkeiten zur Überwachung verschlüsselter Telekommunikation bietet. Die der jüngsten Vergangenheit entspringenden Ergänzungen der repressiven und präventiven Rechtsgrundlagen zur Telekommunikationsüberwachung wurden im Anschluss dementsprechend zum Ende des deskriptiven Teils dieser Masterarbeit beleuchtet.

Im weiteren Verlauf erfolgte, aufbauend auf den zuvor dargestellten Grundlagen, die Erarbeitung rechtlicher und technischer Probleme beim Einsatz der Quellen-TKÜ.

So konnte zunächst festgestellt werden, dass § 8 Abs. 3 TKÜV vorschreibt, dass der Verpflichtete verschlüsselte Telekommunikation vor ihrer Ausleitung an die berechtigte Stelle zu entschlüsseln hat. Die Anwendung dieser Vorschrift ist jedoch nur möglich, wenn der angebotene Telekommunikationsdienst des Verpflichteten zum einen unter die Vorschriften des TKG fällt und zum anderen deutsches Recht auf diesen anwendbar ist. Bezugnehmend auf WhatsApp und Skype steht derzeit jedoch weder fest, ob diese Dienste unter das TMG oder das TKG fallen, noch befinden sich die Firmensitze im Anwendungsbereich deutschen Rechts.

Weitere Probleme beim Einsatz der Quellen-TKÜ wurden in der Folge erarbeitet. So wurden zunächst Möglichkeiten zur Infiltration der Abhörsoftware in das entsprechende Zielsystem beleuchtet. Im Hinblick auf die problematische Einschleusung der Software sowohl mittels Internet, als auch mittels direktem Zugriff auf das Gerät, zeigte sich zum einen, dass durch Maßnahmen wie getarnte E-Mails von anderen Behörden mit infiziertem Anhang ein Vertrauensverlust der Bevölkerung in den Staat evident ist. Zum anderen wurde eine fehlende Rechtsgrundlage zum heimlichen Zutritt zur Wohnung des Betroffenen thematisiert, um dort z. B. das Zielsystem zu infiltrieren. Ob eine solche Rechtsgrundlage entsprechend der Forderung im Rahmen der 89. Konferenz der Justizministerinnen und Justizminister jedoch auch unter verfassungsrechtlichen Gesichtspunkten rechtlich etabliert werden wird, erscheint eher fraglich.

Auch der Funktionsumfang der Abhörsoftware bedurfte einer näheren Betrachtung. Es konnte gezeigt werden, dass sowohl ein zu geringer, als auch ein zu umfangreicher Funktionsumfang zu eklatanten Problemen beim Einsatz der Quellen-TKÜ führt. So konnte erarbeitet werden, dass der Funktionsumfang von RCIS 1.0, der nur das Abhören von Skype auf stationären Windows-PCs ermöglichte, nicht den aktuellen Ansprüchen an eine effektive Strafverfolgung genügt.

Im Gegensatz hierzu erfolgte eine kritische Betrachtung der kommerziellen und durch das BKA eingesetzten Abhörsoftware FinFisher / FinSpy. Es zeigte sich, dass diese über einen sehr viel größeren Funktionsumfang verfügt, der weit über die erlaubte Eingriffsintensität in die Persönlichkeitsrechte der Betroffenen hinaus geht. So ist es mit dieser Software beispielsweise auch möglich, das Mikrofon und die Webcam des infiltrierten Zielsystems fernzusteuern, sofern sie mit ihrem gesamten Funktionsumfang eingesetzt wird. Es wurde gezeigt, dass eine derartige Anwendung der Software zum Teil nur unter wesentlich strengeren rechtlichen Voraussetzungen möglich und nicht von den Eingriffsbefugnissen zur Quellen-TKÜ umfasst ist. So ist die Ansteuerung der Webcam in der Wohnung des Betroffenen dahingegen verfassungsrechtlich höchst problematisch.

Anschließend erfolgte hierauf aufbauend eine Problematisierung der durch die Quellen-TKÜ betroffenen Grundrechte. Vor allem wurde aufgezeigt, dass der Eingriff in informationstechnische Systeme und die damit einhergehende Datenveränderung nicht mit dem Grundrechtseingriff, der durch herkömmliche TKÜ-Maßnahmen verwirklicht wird, vergleichbar ist. Durch den Funktionsumfang der Abhörsoftware kommen weitere Grundrechtseingriffe in Betracht. Es wurde daher geprüft, ob neben dem Eingriff in das Fernmeldegeheimnis nach Art. 10 Abs. 1 GG auch ein Eingriff in Art 13 Abs. 1 GG oder in das Recht auf informationelle Selbstbestimmung durch den Einsatz von Abhörsoftware verwirklicht wird und es wurden sowohl dafürsprechende als auch dagegen-stimmende Meinungen gegenübergestellt.

In diesem Zusammenhang wurde auch das sog. Computer-Grundrecht, das im Jahre 2009 durch das BVerfG aufgrund der dargestellten Problematiken kreiert wurde, einer näheren problemorientierten Betrachtung unterzogen.

Zum Abschluss dieses Kapitels erfolgte eine kritische Betrachtung des der Quellen-TKÜ zugrundeliegenden Gesetzgebungsverfahrens. Dieses erweckte im Ergebnis den Eindruck, dass eine breite öffentliche Diskussion seitens der Großen Koalition verhindert werden sollte, um die entsprechenden Rechtsgrundlagen kurz vor Ende der Legislaturperiode im „Eilverfahren“ zu beschließen.

Um die Beantwortung der forschungsleitenden Fragestellung zu ermöglichen, wurden sodann im letzten Kapitel dieser Masterarbeit Lösungsansätze zum adäquaten Einsatz der Quellen-TKÜ sowohl unter technischen, als auch unter rechtlichen Gesichtspunkten erarbeitet. So wurden zunächst Möglichkeiten untersucht, wie die Strafverfolgungs- und Gefahrenabwehrbehörden technisch den zuvor betrachteten Problemen begegnen können. Hier konnte festgestellt werden, dass u. a. durch die Einrichtung der ZITiS bereits ein großer Schritt in Richtung der Etablierung technischen Know-Hows bei Strafverfolgung- und Gefahrenabwehrbehörden erfolgt ist.

Anschließend wurde untersucht, inwiefern durch die Anpassung von Rechtsgrundlagen den Problemen beim Einsatz der Quellen-TKÜ entgegengetreten werden könnte. Vor allem das Dilemma um den Zielkonflikt zwischen den Leitsätzen „Sicherheit durch Verschlüsselung“ und gleichermaßen „Sicherheit trotz Verschlüsselung“ wurde herausgearbeitet. Eine umfassende Lösung für dieses Problem scheint jedoch noch immer in weiter Ferne zu liegen.

Zum Abschluss der vorliegenden Masterarbeit wurden die Ängste von Teilen der Bevölkerung im Hinblick auf die Beschränkung von Freiheitsrechten durch die Einführung weiterer und tiefgreifender Rechtsgrundlagen zur Telekommunikationsüberwachung beleuchtet und problematisiert. Es konnte im Ergebnis festgestellt werden, dass maßgeblich durch die Implementierung von verfassungsrechtlichen Ausgleichen die Schaffung von Akzeptanz für derartige Maßnahmen erreicht werden kann. Doch darf auch hierbei seitens des Gesetzgebers nicht die Effektivität der Maßnahmen aus den Augen verloren werden.

Im Rahmen der Bearbeitung dieser Masterarbeit zeigte sich, dass die TKÜ mit der Etablierung neuer internetbasierter und verschlüsselter Telekommunikationsdienste in ihrer ursprünglichen Form nicht mehr den aktuellen Anforderungen gewachsen ist. Es konnte festgestellt werden, dass die im TKG vorgeschriebene Verpflichtung der Diensteanbieter bei verschlüsselten internetbasierten und im Ausland ansässigen Diensten ins Leere läuft. Daraus resultierend konnte die Einführung von Rechtsgrundlagen für die Quellen-TKÜ und deren Einsatz auf den ersten Blick als angemessene Antwort auf

dieses Problem identifiziert werden. Doch zeigte sich auch, dass mit dem Einsatz der Quellen-TKÜ vielfältige neue rechtliche und technische Probleme auf Seiten der Strafverfolgungs- und Gefahrenabwehrbehörden entstanden sind.

Für einige dieser Probleme konnten Lösungsvorschläge unterbreitet werden. Für andere Probleme konnte auch im Rahmen dieser Masterarbeit keine adäquate Lösung gefunden werden. Es bleibt jedoch festzustellen, dass die Telekommunikation im digitalen Zeitalter einen Bedeutungszugewinn erfährt. Gleichzeitig stellt der technische Fortschritt in diesem Bereich die Ermittlungsbehörden vor zahlreiche Probleme. Es gilt daher umso mehr, den noch immer vorhandenen Herausforderungen bei der Durchführung von TKÜ-Maßnahmen zu begegnen. Nur so kann es gelingen, dass in Zeiten terroristischer und extremistischer Gefahren und grenzüberschreitender organisierter Kriminalität ein angemessenes Maß an Sicherheit bei gleichzeitiger Wahrung der Freiheitsrechte sämtlicher Bürger gewährleistet werden kann und die Strafverfolgung und Gefahrenabwehr nicht hinter der Lebenswirklichkeit zurückbleibt.

Literatur- und Quellenverzeichnis

89. Konferenz der Justizministerinnen und Justizminister (2018): Frühjahrskonferenz. 6. Und 7. Juni 2018. Beschluss. TOP II.8. Ergänzung der Regelungen zur Quellen-TKÜ und zur Online-Durchsuchung um ein Betretungsrecht. URL: http://www.jm.nrw.de/JM/jumiko/beschluesse/2018/Fruehjahrskonferenz_2018/II-8-RP---Ergaenzung-der-Regelungen-zur-Quellen-TKUe-und-zur-Online-Durchsuchung-um-ein-Betretungsrecht.pdf (besucht am 08.11.2018).

Abel, Horst (2011): Praxiskommentare Telemediengesetz, Telekommunikationsgesetz und TKÜV. Datenschutz im TMG, TKG und in der TKÜV. Für den Praktiker leicht verständlich erläutert. Kissing.

Ackermann, Rolf / Clages, Horst / Roll, Holger (2011): Handbuch der Kriminalistik. Kriminaltaktik für Praxis und Ausbildung. 4. Aufl. Stuttgart.

Albers-Heinemann, Tobias / Friedrich, Björn (2018): Das Elternbuch zu WhatsApp, YouTube, Instagram & Co. 2. Aufl. Heidelberg.

Albrecht, Hans-Jörg / Dorsch, Claudia / Krüpe, Christiane (2013): Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen. Abschlussbericht. Freiburg. URL: https://www.mpicc.de/files/pdf1/k115.pdf (besucht am 15.09.2018).

Asi, Dennis (2008): VoIP- und Skype-Sicherheit. In: *Dudek, Denise et al.:* Netzsicherheit und Hackerabwehr. Seminar WS07/08. Karlsruhe. S. 209 – 225. URL: http://doc.tm.uka.de/tr/TM-2008-3.pdf#page=212 (besucht am 01.11.2018).

Bär, Wolfgang (2010): TK-Überwachung. §§ 100a-101 StPO mit Nebengesetzen. Kommentar. Köln und München.

Baum, Gerhart / Kurz, Constanze / Schantz, Peter (2013): Das vergessene Grundrecht. Frankfurt am Main. URL: http://www.faz.net/aktuell/feuilleton/debatten/datenschutz-das-vergessene-grundrecht-12095331.html (besucht am 06.11.2018).

Beckedahl, Markus (2013): Fünf Jahre IT-Grundrecht. Berlin. URL: https://netzpolitik.org/2013/funf-jahre-it-grundrecht/ (besucht am 06.11.2018).

Belschner, Mike (2016): WhatsApp versus Threema. Messenger im Vergleich. Hamburg. URL: https://www.netzwelt.de/whatsapp/whatsapp-alternativen/150402_3-whatsapp-versus-threema-messenger-vergleich.html (besucht am 03.11.2018).

Beuth, Patrick (2018): Auch die FDP will Staatstrojaner bremsen. Hamburg. URL: http://www.spiegel.de/netzwelt/netzpolitik/staatstrojaner-verfassungsbeschwerde-auch-die-fdp-will-spaehsoftware-bremsen-a-1224037.html (besucht am 10.11.2018).

Biala, Jacek (1995): Mobilfunk und intelligente Netze. Grundlagen und Realisierung mobiler Kommunikation. 2., neubearb. Aufl. Braunschweig und Wiesbaden.

Blume, Dorlis (2011): Die Erfindung des Telefons. URL: http://www.dhm.de/lemo/rueckblick/oktober-1861-die-erfindung-des-telefons.html (besucht am 13.09.2018).

Böckenförde, Thomas (2008): Auf dem Weg zur elektronischen Privatsphäre. Zugleich Besprechung von BVerfG, Urteil v. 27.2.2008 – „Online-Durchsuchung". In: Juristen Zeitung, 63. Jahrg., Nr. 19 (3. Oktober 2008) *Hrsg. von Hilgendorf, Eric et al.* Tübingen, S. 925 – 939.

Born, Günther (2018): Skype im Niedergang. Wer hat's kaputt gemacht? Kelkheim. URL: https://www.borncity.com/blog/2018/05/13/skype-im-niedergang-wer-hats-kaputt-gemacht/ (besucht am 02.11.2018).

Bratke, Bastian (2013): Die Quellen-Telekommunikationsüberwachung im Strafverfahren. Grundlagen, Dogmatik, Lösungsmodelle. Berlin.

Bundesamt für Justiz (2017): Übersicht Telekommunikationsüberwachung (Maßnahmen nach § 100a StPO) für 2016. Berlin. URL: https://www.bundesjustizamt.de/DE/SharedDocs/Publikationen/Justizstatistik/Uebersicht_TKUE_2016.pdf?__blob=publicationFile&v=2 (besucht am 07.11.2018).

Bundesamt für Sicherheit in der Informationstechnik (2016): Sichere Inter-Netzwerk Architektur. SINA. Bonn. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/SINA.pdf?__blob=publicationFile&v=8 (besucht am 07.10.2018).

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (1999): 58. Konferenz vom 7./8. Oktober 1999. Eckpunkte der deutschen Kryptopolitik. Ein Schritt in die richtige Richtung. URL: https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/58DSK-EckpunkteDerDeutschenKryptopolitik-EinSchrittInDieRichtigeRichtung.html (besucht am 14.11.2018).

Bundesgesetzblatt Nr. 1 (1949): Grundgesetz für die Bundesrepublik Deutschland. Vom 23. Mai 1949. In: Amtliches Organ zur Verkündung von Rechtsverordnungen der Zentralverwaltungen Nr. 28. Hrsg. von *Zentral-Justizamt für die Britische Zone.* Hamburg, S. 176 ff.

Bundeskriminalamt (o. D.): Quellen-TKÜ und Online-Durchsuchung. Notwendigkeit, Sachstand und Rahmenbedingungen. Wiesbaden. URL: https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html (besucht am 13.11.2018).

Bundesministerium des Innern (2016): Cyber-Sicherheitsstrategie für Deutschland 2016. Berlin. URL: https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (besucht am 12.11.2018).

Bundesministerium für Bildung und Forschung (2018): Quantentechnologien. Von den Grundlagen zum Markt. Rahmenprogramm der Bundesregierung. Berlin. URL: https://www.bmbf.de/pub/Quantentechnologien.pdf (besucht am 13.11.2018).

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation und Eisenbahnen (2017): Technische Richtlinie zur Überwachung der Telekommunikation, Erteilung von Auskünften (TR TKÜV). Ausgabe 7.0. Stand 14. Juni 2017. Mainz. URL: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/TechnUmsetzung110/Downloads/TR%20TKU EV%20Version %207.0%20pdf%20 deutsch.pdf?__blob=publicationFile&v=1 (besucht am 03.10.2018).

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation und Eisenbahnen (o. D.): Technische Umsetzung von Überwachungsmaßnahmen. Informationen zur Vergabe von IDs für eindeutige Referenznummern. Mainz. URL: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/TechnUmsetzung110/ Downloads/16TKUE_EMail_VergabeIDspdf.pdf?__blob=publicationFile&v=7 (besucht am 07.10.2018).

Chaos Computer Club (2011): Chaos Computer Club analysiert aktuelle Version des Staatstrojaners. Hamburg. URL: https://www.ccc.de/de/updates/2011/analysiert-aktueller-staatstrojaner (besucht am 08.11.2018).

Chaos Computer Club (2011a): Chaos Computer Club analysiert Staatstrojaner. Hamburg. URL: https://www.ccc.de/updates/2011/staatstrojaner (besucht am 09.11.2018).

Conger, Kate (2016): Burr-Feinstein encryption bill is officially here in all its scary glory. Dublin. URL: https://techcrunch.com/2016/04/13/burr-feinstein-encryption-bill-is-officially-here-in-all-its-scary-glory/?guccounter=1 (besucht am 12.11.2018).

Dalby, Jakob (2016): Grundlagen der Strafverfolgung im Internet und in der Cloud. Möglichkeiten, Herausforderungen und Chancen. Wiesbaden.

Demuth, Kerstin / Friedemann, Ebelt (2017): Wir klagen gegen die Staatstrojaner – Verfassungsbeschwerde unterstützen! URL: https://digitalcourage.de/index.php/blog/2017/wir-klagen-gegen-den-staatstrojaner-verfassungsbeschwerde-jetzt-unterstuetzen (besucht am 06.09.2018).

Deutscher Bundestag (2011): Innenausschuss. Ausschussdrucksache 17(4)366. Berlin. URL: https://netzpolitik.org/wp-upload/174366-Bericht-BKA-Prasident-Ziercke_TOP-24a-24c_53.-InnenA-Sitzug.pdf (besucht am 09.11.2018).

Deutscher Bundestag (2016): Regulierung von Messengerdiensten. Datenportabilität und Interoperabilität. Wissenschaftliche Dienste. Fachbereich WD 10: Kultur, Medien und Sport. Az.: WD 10 – 3000 – 060/16. Berlin. URL: https://www.bundestag.de/blob/491792/477b164f ff61393d41e605fd4cf39bef/wd-10-060-16-pdf-data.pdf (besucht am 07.11.2018).

Duque-Antón, Manuel (2002): Mobilfunknetze. Grundlagen, Dienste und Protokolle. 1. Aufl. Hrsg. von *Mildenberger, Otto.* Wiesbaden.

Flade, Florian (2016): So lassen Islamisten Terrorfahnder ins Leere laufen. Berlin. URL: https://www.welt.de/politik/deutschland/article154518365 /so-lassen-Islamisten-Terrorfahnder-ins-Leere-laufen.html (besucht am 31.10.2018).

Flade, Florian (2017): Der Bundestrojaner. Das kann er, und das nicht. Berlin. URL: https://investigativ.welt.de/2017/07/26/der-bundestrojaner-das-kann-er-und-das-nicht/ (besucht am 05.11.2018).

Flade, Florian (2018): Ministerium gibt Bundestrojaner für den Einsatz frei. Berlin. URL: https://www.welt.de/politik/deutschland/article173121473 /Verdeckte-Ueberwachung-Ministerium-gibt-neuen-Bundestrojaner-fuer-den-Einsatz-frei.html (besucht am 09.11.2018).

Flade, Florian (2018a): Bundestrojaner. Kein Einsatz trotz Genehmigung. Berlin. URL: https://investigativ.welt.de/2018/02/23/bundestrojaner-kein-einsatz-trotz-genehmigung/ (besucht am 13.11.2018).

Foschepoth, Josef (2015): Verfassung und Wirklichkeit: Die Überwachung des Fernmeldeverkehrs in der Geschichte der Bundesrepublik Deutschland. In: Datenschutz – aktuelle Fragen und Antworten. Atzelsberger Gespräche 2014. Hrsg. von *Neuhaus, Helmut*. Erlangen, S. 11 – 44.

Foschepoth, Josef (2017): Überwachtes Deutschland. Post- und Telefonüberwachung in der alten Bundesrepublik. 5., durchgesehene Aufl. Göttingen.

Frees, Beate / Koch, Wolfgang (2018): Ergebnisse aus der Studienreihe „Medien und ihr Publikum“ (MiP). ARD/ZDF-Onlinestudie 2018. Zuwachs bei medialer Internetnutzung und Kommunikation. In: *Krupp, Mannfred* (Hrsg.): Media Perspektiven 9/2018. Frankfurt am Main, S. 398 – 413.

Freiling, Felix / Safferling, Christoph / Rückert, Christian (2018): Quellen-TKÜ und Online-Durchsuchung als neue Maßnahmen für die Strafverfolgung. Rechtliche und technische Herausforderungen. In: *Olzen, Dirk / Schäfer, Gerhard* (Hrsg.): Juristische Rundschau (JR), Heft 1/2018. Berlin, S. 9 – 22.

Frey, Horst / Schönfeld, Detlef (1995): Mehr über das Telefon und seine Zusatzgeräte. Technik, analog und digital, ISDN, Dosen, Stecker und Schalter, Anschaltbedingungen und Installation. 3., verb. Aufl. Poing.

Fröhlich, Christoph (2016): Wie Terroristen über die Playstation 4 kommunizieren. URL: https://www.stern.de/digital/online/paris--warum-terroristen-anschlaege-mit-der-playstation-4-planen-6558062.html (besucht am 27.08.2018).

Graf, Jürgen Peter (2018): Strafprozessordnung. Mit Gerichtsverfassungsgesetz und Nebengesetzen. Kommentar. 3. Aufl. München.

Greis, Friedhelm (2017): Bundesnetzagentur setzt Vorratsdatenspeicherung aus. München. URL: https://www.sueddeutsche.de/digital/nach-urteil-bundesnetzagentur-setzt-vorratsdatenspeicherung-aus-1.3564204 (besucht am 01.11.2018).

Grunert, Marlene (2017): Durch die Hintertür zur Online-Überwachung. Frankfurt am Main. URL: http://www.faz.net/aktuell/politik/online-durchsuchung-quellen-tkue-bundestrojaner-wird-gesetz-15071053.html (besucht am 10.11.2018).

Gusy, Christoph (2003): Überwachung der Telekommunikation unter Richtervorbehalt. Effektiver Grundrechtsschutz oder Alibi? In: Zeitschrift für Rechtspolitik, 36. Jahrg., H. 8 (August 2003). Frankfurt am Main, S. 275 – 278.

Hessische/Niedersächsische Allgemeine (2017): Von 1G bis 5G. Die Generationen der Mobilfunkstandards. Kassel. URL: https://www.hna.de/netzwelt/von-1g-bis-5g-generationen-mobilfunk standards-zr-8485449.html (besucht am 27.09.2018).

Hipp, Dietmar (2008): Online-Durchsuchungen. Richter erfinden das Computer-Grundrecht. Hamburg. URL: http://www.spiegel.de/politik/deutschland/online-durchsuchungen-richter-erfinden-das-computer-grundrecht-a-538238.html (besucht am 06.11.2018).

International Telecommunication Union (2018): Country ICT Data (Until 2017). Genf. URL: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx (besucht am 25.09.2018).

Jelica, Albert (2018): Skype. Wie Microsoft es geschafft hat, die Marke zu zerstören. Hamburg. URL: https://windowsarea.de/2018/05/skype-wie-microsoft-es-geschafft-hat-die-marke-zu-zerstoeren/ (besucht am 02.11.2018).

Jucker, Andreas / Dürscheid, Christa (2012): The linguistics of keyboard-to-screen communication. A new terminological framework. In: Linguistik Online, 56(6/12). Zürich. S. 1 – 26. URL: https://www.zora.uzh.ch/id/eprint/67310/1/Jucker_Duerscheid_2012_KSC.pdf (besucht am 31.10.2018).

Keller, Christoph / Braun, Frank / Hoppe, Rene (2015): Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen. 2. erw. Aufl. Stuttgart u. a.

Klöppner, Carsten (2007): Rechtsprobleme der IP-Telefonie. Zugl.: Konstanz, Univ., Diss., 2007. Berlin, Münster.

Könen, Andreas (2017): Gefahren für die innere Sicherheit aus dem Cyber-Raum – Wie kann Deutschland sich schützen? In: *Sensburg, Patrick* (Hrsg.): Sicherheit in einer digitalen Welt. Baden-Baden, S. 45 – 60.

König, Katharina / Bahlo, Nils Uwe (2014): SMS, WhatsApp & Co. Gattungsanalytische, kontrastive und variationslinguistische Perspektiven zur Analyse mobiler Kommunikation. In: Wissenschaftliche Schriften der WWU Münster. Reihe XII, Band 12. Münster.

Krüper-Gescher, Christiane (2005): Die Überwachung der Telekommunikation nach den §§ 100a, 100b StPO in der Rechtspraxis. In: Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht. Kriminologische Forschungsberichte. Hrsg. von *Albrecht, Hans-Jörg / Kaiser, Günther*. Bd. K 127. Freiburg i. Br.

Kube, Edwin / Schreiber, Manfred (1992): Theoretische Kriminalistik. In: Kriminalistik. Hrsg. von *Kube, Edwin / Störzer, Hans Udo / Timm, Klaus Jürgen*. Stuttgart u. a., S. 1 – 17.

Kuhn, Violetta (2017): Wegwerf-SIMs für Terroristen. Was tun gegen den Prepaid-Missbrauch? Hannover. URL: https://heise.de/-3596708 (besucht am 31.10.2018).

Kühne, Hans-Heiner (2015): Strafprozessrecht. Eine systematische Darstellung des deutschen und europäischen Strafverfahrensrechts. 9., völlig neu bearb. und erw. Aufl. Heidelberg.

Lackes, Richard (o. D.): Web 2.0. Definition. Wiesbaden. URL: https://wirtschaftslexikon.gabler.de/definition/web-20-51842 (besucht am 15.11.2018).

Liebig, Britta (2015): Der Zugriff auf Computerinhaltsdaten im Ermittlungsverfahren. Cloud computing, E-Mail und IP-Telefonie als neue rechtliche und technische Herausforderung für die Strafverfolger. Zugl.: Trier, Univ., Diss., 2015. Hamburg.

Meister, Andre (2013): Geheimes Dokument. Bundeskriminalamt kauft international bekannte Staatstrojaner FinFisher/FinSpy von Gamma (Updates). Berlin. URL: https://netzpolitik.org/2013/geheimes-dokument-bundeskriminalamt-kauft-international-bekannten-staatstrojaner-finfisherfinspy-von-gamma/ (besucht am 05.11.2018).

Meister, Andre (2014): Geheimes Dokument: Bundeskriminalamt darf Fin Fisher/Finspy nicht einsetzen, versucht einfach neue Version noch mal. Berlin. URL: https://netzpolitik.org/2014/geheimes-dokument-bundeskriminalamt-darf-finfisherfinspy-nicht-einsetzen-versucht-einfach-neue-version-nochmal/ (besucht am 09.11.2018).

Meister, Andre (2017): Geheimes Dokument: Das BKA will schon dieses Jahr Messenger-Apps wie WhatsApp hacken. Berlin. URL: https://netzpolitik.org/2017/geheimes-dokument-das-bka-will-schon-dieses-jahr-messenger-apps-wie-whatsapp-hacken/ (besucht am 09.11.2018).

Meister, Andre (2018): Geheime Dokumente: Das Bundeskriminalamt kann jetzt drei Staatstrojaner einsetzen. Berlin. URL: https:// netzpoltik.org /2018/geheime-dokumente-das-bundeskriminalamt-kann-jetzt-drei-staatstrojaner-einsetzen/ (besucht am 09.11.2018).

Meixner, Kurt / Fredrich, Dirk (2016): Hessisches Gesetz über die öffentliche Sicherheit und Ordnung. HSOG. Mit Erläuterungen und ergänzenden Vorschriften. 12. vollst. überarb. Aufl. Stuttgart u. a.

Mobilsicher (2018): Messenger-App Signal kurz vorgestellt. Berlin. URL: https://mobilsicher.de/kategorie/whatsapp-und-messenger/ messenger-app-signal-kurz-vorgestellt (besucht am 02.11.2018).

Mormann, Hauke (2018): WhatsApp verschlüsselt. Kritik am Datenschutz bleibt. Düsseldorf. URL: https://www.checked4you.de/handy-telefon/ messenger/whatsapp-verschlüsselt-kritik-am-datenschutz-bleibt-351587 (besucht am 03.11.2018).

Mühlroth, Adrian (2018): Diese Funktionen gibt es bei WhatsApp. Berlin. URL: https://www.techbook.de/apps/messenger/funktionen-whatsapp (besucht am 31.10.2018).

Neumann, Dana (2018): Der Staatstrojaner für Smartphones ist im Einsatz. Berlin. URL: https://www.futurezone.de/netzpolitik/article213267959/ Der-Staatstrojaner-fuer-Smartphones-ist-im-Einsatz.html (besucht am 05.11.2018).

o. V. (2015): WhatsApp und Datenschutz. Antworten auf die wichtigsten Fragen. Hamburg u. a. URL: https://www.datenschutzbeauftragter-info.de/whatsapp-und-datenschutz-antworten-auf-die-wichtigsten-fragen/ (besucht am 03.11.2018).

o. V. (2015a): Vorratsdatenspeicherung. Mit einem Gesetzentwurf schlägt Bundesregierung die Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vor. Köln. URL: https://www. bundesanzeiger-verlag.de/gesetze/nachrichten/detail/artikel/vorrats datenspeicherung-16366.html (besucht am 08.12.2018).

Paeffgen, Hans-Ullrich (2001): Überlegungen zu einer Reform der Überwachung der Telekommunikation. In: *Schünemann, Bernd* (Hrsg.): Festschrift für Claus Roxin zum 70. Geburtstag am 15. Mai 2001. Berlin, New York, S. 1299 – 1318.

Pernice, Ina (2002): Die Telekommunikations-Überwachungsverordnung (TKÜV). In: Datenschutz und Datensicherheit 26(4) (2002). Wiesbaden, S. 207 – 211.

Petrlic, Ronald / Sorge, Christoph (2017): Datenschutz. Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie. Wiesbaden.

Phoenix (2017): Pressekonferenz zur Innenministerkonferenz am 14.06.2017. Youtube, 14.06.2017. URL: https://www.youtube.com/ watch?v=wmXAzI5KHfM, 08:02 Minuten (besucht am 06.09.2018).

Pinkert, Reiko / Strozyk, Jan / Tanriverdi, Hakan (2018): Staatliche Hacker dringend gesucht. München. URL: https://www.sueddeutsche.de/digital/it-sicherheitsbehoerde-zitis-staatliche-hacker-dringend-gesucht-1.4017900 (besucht am 13.11.2018).

Plath, Kai-Uwe (2018): DSGVO/BDSG. Kommentar zu DSGVO, BDSG und den Datenschutzbestimmungen von TMG und TKG. 3. Aufl. Köln.

Prantl, Heribert (2017): Der Staatstrojaner ist ein Einbruch ins Grundrecht. Kommentar. München. URL: https://www.sueddeutsche.de/digital/ueberwachung-der-staatstrojaner-ist-ein-einbruch-ins-grundgesetz-1.3555917 (besucht am 10.11.2018).

Renner, Martina (2018): Angriff auf Bürgerrechte. Linksfraktion unterstützt Klage gegen Staatstrojaner. Pressemitteilung. Berlin. URL: https://www.linksfraktion.de/presse/pressemitteilungen/detail/angriff-auf-buergerrechte-linksfraktion-unterstuetzt-klage-gegen-staatstrojaner-1/ (besucht am 10.11.2018).

Roggan, Frederik (2017): Die strafprozessuale Quellen-TKÜ und Online-Durchsuchung: Elektronische Überwachungsmaßnahmen mit Risiken für Beschuldigte und Allgemeinheit. In: *Gercke, Björn / Jahn, Matthias / Pollähne, Helmut* (Hrsg.): Strafverteidiger (StV), Heft 12/2017. Köln, S. 821 – 829.

Roggan, Frederik (2018): Quellen-TKÜ und Online-Durchsuchung zur Strafverfolgung. In: *Müller-Heidelberg, Till et al.* (Hrsg.): Grundrechte-Report 2018. Zur Lage der Bürger- und Menschenrechte in Deutschland. Frankfurt am Main, S. 38 – 41.

Rubbert, Martin (2017): George Orwell 2017 – Online-Durchsuchung und Quellen-TKÜ im Schnellverfahren in die StPO eingeführt. Editorial. In: *Gercke, Björn / Jahn, Matthias / Pollähne, Helmut* (Hrsg.): Strafverteidiger (StV), Heft 9/2017. Köln, S. I.

Sander, Ralf (2013): Zehn Fakten zu Skype. Hamburg. URL: https://www.stern.de/digital/smartphones/zehnjaehriges-jubilaeum-zehn-fakten-zu-skype-3210416.html (besucht am 02.11.2018).

Schallbruch, Martin (2018): Schwacher Staat im Netz. Wie die Digitalisierung den Staat in Frage stellt. Wiesbaden.

Schemberg, Axel / Linten, Martin (2006): PC-Netzwerke. 3., aktualisierte und erw. Aufl. Bonn.

Scheurle, Klaus-Dieter / Mayen, Thomas (2018): Telekommunikationsgesetz. Kommentar. 3. Aufl. München.

Schieb, Jörg (2016): Handel mit Sicherheits-Lücken: Exploit-Handel. Meerbusch. URL: https://www.schieb.de/746083/746083 (besucht am 13.11.2018).

Schoder, Detlef (2002): Peer-to-Peer. Ökonomische, technologische und juristische Perspektiven. Berlin, Heidelberg.

Schönbohm Arne (2018): Flexibilität und Unabhängigkeit. Rahmenbedingungen für eine gesellschaftliche Cyber-Sicherheit. In: *Bär, Christian / Grädler, Thomas / Mayr, Robert* (Hrsg.): Digitalisierung im Spannungsfeld von Politik, Wirtschaft, Wissenschaft und Recht. Berlin, S. 429 – 439.

Schulze, Matthias (2017): Verschlüsselung in Gefahr: weltweit schwächen Staaten die Cyber-Sicherheit – Deutschland sollte dagegenhalten. In: Stiftung Wissenschaft und Politik. SWP-Aktuell 56, August 2017. Berlin, S. 1 – 4. URL: https://www.ssoar.info/ssoar/handle/document/53647 (besucht am 12.11.2018).

Schwarzer, Eckhard (2018) Das Dilemma der Politik in der digitalen Welt. In: *Bär, Christian / Grädler, Thomas / Mayr, Robert* (Hrsg.): Digitalisierung im Spannungsfeld von Politik, Wirtschaft, Wissenschaft und Recht. Berlin, S. 487 – 504.

Siller, Helmut (2017): Exploit. Wiesbaden URL: https://wirtschaftslexikon.gabler.de/definition/exploit-53419/version-200916 (besucht am 08.11.2018).

Siller, Helmut (2018): Backdoor. Wiesbaden. URL: https://wirtschaftslexikon.gabler.de/definition/backdoor-53418/version-276510 (besucht am 08.11.2018).

Sodan, Helge (2018): Beck'sche Kompakt-Kommentare. Grundgesetz. München u. a.

Spiegel Online (2016): Neuer Sicherheitsstandard. WhatsApp verschlüsselt Kommunikation vollständig. Hamburg. URL: http://www.spiegel.de/netzwelt/apps/whatsapp-messenger-fuehrt-ende-zu-ende-verschluesselung-ein-a-1085636.html (besucht am 02.11.2018).

Statista (2018): Anzahl der aktiven Nutzer von WhatsApp weltweit in ausgewählten Monaten von April 2013 bis Januar 2018 (in Millionen). Hamburg. URL: https://de.statista.com/statistik/daten/studie/285230/umfrage/aktive-nutzer-von-whatsapp-weltweit/ (besucht am 31.10.2018).

Statista (2018a): Schätzung zur Anzahl der weltweit registrierten Skype-Nutzer in den Jahren 2009 bis 2024 (in Milliarden) Hamburg. URL: https://de.statista.com/statistik/daten/studie/185958/umfrage/registrierte-und-zahlende-skype-nutzer-seit-2007/ (besucht am 02.11.2018).

Strate, Gerhard (2018): Verfassungsbeschwerde gegen § 100a Abs. 1 Satz 2 und 3, Abs. 3 und 5, § 100b, §100d Abs. 5 Satz 2 und 3 der Strafprozessordnung (StPO) in der Fassung des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017 (BGBl. I S. 3202). Hamburg. URL: https://freiheitsrechte.org/home/wp-content/uploads/2018/08/GFF_Verfassungsbeschwerde_Staatstrojaner_anonym.pdf (besucht am 10.11.2018).

Tanriverdi, Hakan (2018): BKA verpasst Staatstrojaner-Testern Maulkorb. München. URL: https://www.sueddeutsche.de/digital/it-sicherheit-bka-verpasst-staatstrojaner-testern-maulkorb-1.3942712 (besucht am 09.11.2018).

Taubmann, Benjamin et al. (2016): TLSkex. Harnessing virtual machine introspection for decrypting TLS communivation. In: *Roussev, Vassil* (Hrsg.): DFRWS 2016 Europe. Ausgabe 16/2016. Passau, S. 114 – 123.

Telefon24 Blog (2015): ISDN oder Analog – Was macht den Unterschied? Glasgow. URL: https://www.telefon24.de/blog/isdn-oder-analog-macht-den-unterschied/ (besucht am 27.09.2018).

Ulbricht, Carsten (2018): Praxishandbuch Social Media und Recht. Rechtssichere Kommunikation und Werbung in sozialen Netzwerken. Freiburg i. Br.

Verbraucherzentrale (2018): Telekom kündigt alte Festnetzanschlüsse. Düsseldorf. URL: https://www.verbraucherzentrale.de/wissen/digitale-welt/mobilfunk-und-festnetz/telekom-kuendigt-alte-festnetz anschluesse-11780 (besucht am 27.09.2018).

Vongehlen, Dirk (2007): Stasi 2.0. Widerstand mit Schäublone gegen den Bundesinnenminister. München. URL: https://www.jetzt.de/ueberwachung/stasi-2-0-widerstand-mit-schaeublone-gegen-den-bundesinnenminister-378419 (besucht am 15.11.2018).

Weis, Rüdiger (2016): Technische Sicherung der Digitalen Souveränität. In: *Friedrichsen, Mike / Bisa, Peter (Hrsg.)*: Digitale Souveränität. Vertrauen in die Netzwerkgesellschaft. Wiesbaden, S. 53 – 66.

Welling, Kira (2018): Wie funktioniert Skype? München. URL: https://praxistipps.chip.de/wie-funktioniert-skype_17258 (besucht am 31.10.2018).

Welp, Jürgen (2001): Überwachung als System. Die Entwicklung der Fernmeldeüberwachung in der Bundesrepublik Deutschland. In: Verteidigung und Überwachung. 1. Aufl. Baden-Baden, S. 278 – 312.

Wildt, Dorothee (2018): Vorratsdatenspeicherung im Jahr 2017 – kein Ende in Sicht. Ein Trauerspiel in (zu) vielen Akten. In: *Müller-Heidelberg, Till et al.* (Hrsg.): Grundrechte-Report 2018. Zur Lage der Bürger- und Menschenrechte in Deutschland. Frankfurt am Main, S. 179 – 182.

Witte, Katharina (2018): Ende-zu-Ende-Verschlüsselung. Was genau ist das? Hannover. URL: https://www.heise.de/tipps-tricks/Ende-zu-Ende-Verschluesselung-was-genau-ist-das-4007116.html (besucht am 03.11.2018).

Zentrale Stelle für Informationstechnik im Sicherheitsbereich (o. D.): Arbeitsfelder. Telekommunikationsüberwachung. München. URL: https://www.zitis.bund.de/DE/Arbeitsfelder/Ueberwachung/ueberwachung_node.html (besucht am 13.11.2018).

Zentrale Stelle für Informationstechnik im Sicherheitsbereich (o. D.a): Arbeitsfelder. Kryptoanalyse. München. URL: https://www.zitis.bund.de/DE/Arbeitsfelder/Kryptoanalyse/kryptoanalyse_node.html (besucht am 13.11.2018).

Eigenständigkeitserklärung

Hiermit versichere ich, dass ich die vorliegende Arbeit selbständig angefertigt habe. Ich habe außer den im Literatur- und Quellenverzeichnis und im Text genannten Hilfsmitteln keine weiteren verwendet und alle Stellen der Arbeit, die anderen Werken dem Wortlaut oder dem Sinn nach entnommen sind, unter Angabe der Quellen als Entlehnung kenntlich gemacht.

Julian Twenning	22.01.2019
(Vorname, Name)	(Datum)