Masterstudiengang Kriminologie, Kriminalistik und Polizeiwissenschaft

MA Krim 12

Erstgutachter: Herr Dr. Andreas Ruch

Zweitgutachter: Herr Ulf Küch

Masterarbeit

Die Telekommunikationsüberwachung als Strafverfolgungsmaßnahme im digitalen Zeitalter

vorgelegt von:

Nandy Hielscher

Inhaltsverzeichnis

1. Einleitung

Im Zeitalter der Digitalisierung befinden sich die Telekommunikation und die Nutzungsgewohnheiten ihrer Anwender im stetigen Wandel. Der rasante Fortschritt moderner Kommunikationstechnologien beeinflusst das Kommunikationsverhalten der Menschen in grundlegender Weise.[1] Der moderne Bürger des 21. Jahrhunderts verfügt über ein buntes Potpourri an Möglichkeiten, mittels technischer, mobiler sowie stationärer Anlagen miteinander zu kommunizieren sowie Informationen auszutauschen, während die vergangenen Jahrzehnte von Analogietelefonie und Fernmeldeeinrichtungen geprägt waren.[2] Darüber hinaus hat sich auch das Internet zu einem Multikommunikationsmedium entwickelt. Es erfüllt mit seinem technischen Potential, bezogen auf die Aufbau- und Leistungsfähigkeit, die Anforderungen, welche die heutige Gesellschaft an weltweit erreichbare, individuell ausgestaltete und 24-Stunden verfügbare Telekommunikationsdienste stellt.[3] Begriffe wie Industrie 4.0, Internet der Dinge, neue Medien und soziale Netzwerke stehen sinnbildlich für den Wandel der Gesellschaft, der sich weg von direkter, persönlicher Kommunikation hin zu einem stetig zunehmenden Nachrichtenaustausch mittels komplexer, multifunktionaler informationstechnischer Einrichtungen und Systeme bewegt. Dieser Wandel trifft immer mehr Bereiche des alltäglichen beruflichen, sozialen und privaten Lebens.[4]

Gemäß des Statistischen Bundesamts verfügen 90 Prozent aller privaten Haushalte in Deutschland über einen Personal Computer und 91 Prozent über einen Internetanschluss. Über ein Telefon verfügen 100 Prozent der Haushalte. Davon nutzen 90 Prozent ein herkömmliches Festnetztelefon und 95 Prozent ein Mobiltelefon, wie Handy oder Smartphone.[5] Aufgrund der gestiegenen Verbreitung leistungsfähiger Personal Computer in den Privathaushalten in Deutschland sowie des Internets in vielen Teilen der täglichen Lebensgestaltung[6], gewinnt die Technik der Internettelefonie bzw. die sogenannte

[1] Bratke, 2013, S. 15.
[2] Vgl. Bratke, 2013, S. 15.
[3] Vgl. Bratke, 2013, S. 15.
[4] Vgl. Bratke, 2013, S. 15.
[5] Vgl. Statistisches Bundesamt, Ausstattung privater Haushalte mit Informations- und Kommunikationstechnik – Deutschland, 2017.
[6] Vgl. Bratke, 2013, S. 16.

Voice-over-IP-Kommunikation (VoIP) auf dem Telekommunikationsmarkt an Bedeutung. Diese wirkt sich entsprechend auf das Kommunikationsverhalten großer Teile der Bevölkerung aus. Funktional ist die Internettelefonie mit der klassischen Festnetz- oder Mobilfunktelefonie vergleichbar. Der Unterschied zur klassischen leitungsvermittelten Festnetztelefonie besteht darin, dass bei der paketvermittelten Internettelefonie die Kommunikation nicht im Rahmen einer festen Verbindung über speziell vorgesehene Leitungen stattfindet, sondern digitalisiert und in einzelne Datenpakete aufgeteilt über das weltweite Datennetz mittels Internetprotokoll transportiert wird.[7] Erfolgt die VoIP-Kommunikation über den Computer, das Handy oder Smartphone mit spezieller Software, nimmt die VoIP-Software automatisch eine Verschlüsselung der Daten während der Übermittlung im Datennetz vor.[8]

Vor diesem Hintergrund bleibt die zunehmende Digitalisierung und Verschlüsselung von Kommunikation über das Internet und Smartphone nicht ohne Auswirkung auf die Arbeit staatlicher Stellen bei der Aufklärung, Bekämpfung, Verfolgung und Verhütung von Straftaten. Moderne Internetdienste werden nicht nur zur Begehung von computerspezifischen Delikten genutzt, sondern darüber hinaus zur Kommunikation und Absprache zwischen Straftätern bei unterschiedlichen Deliktsarten, auch aus dem Bereich der organisierten Kriminalität.[9] Die zunehmende Verbreitung verschlüsselter Kommunikation stellt die Ermittlungsbehörden bei der Überwachung der Telekommunikation vor gesteigerte technische und rechtliche Schwierigkeiten.[10] Während die Telekommunikationsüberwachung den Behörden bislang meist einen problemlosen Einblick in die Kommunikationsinhalte ermöglichte, liefert die herkömmliche Aufzeichnung und Überwachung verschlüsselter VoIP-Kommunikation auf dem Transportweg im Datennetz nur kryptierte Daten. Diese können weder mit einfachen Mitteln noch in angemessener Zeit von den Strafverfolgungsbehörden entschlüsselt werden. Diese Umstände machen es erforderlich, die VoIP-Kommunikation bereits vor deren Verschlüsselung abzugreifen. Zu Beginn steht deshalb die Frage: Wie gelingt es Ermittlern i.S.d. § 100 a StPO laufende und

[7] Vgl. Bratke, 2013, S. 16.
[8] Vgl. Bratke, 2013, S. 16.
[9] Vgl. Bratke, 2013, S. 16.
[10] Vgl. Bratke, 2013, S. 482.

zum Teil verschlüsselte Kommunikation abzuhören? Schwerpunktmäßig wird dabei die Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) behandelt, welche als angepasstes Ermittlungsinstrument im Bereich der Strafverfolgung gilt.[11] In den vergangenen Jahren fand sie wiederholt im Zusammenhang mit der Gefahrenabwehr, insbesondere zur Terrorismusbekämpfung in den Fachkreisen und Medien Erwähnung. Das Bundesverfassungsgericht befasste sich in mindestens zwei Urteilen, nämlich zu den Online-Durchsuchungen 2008 und zum Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten 2016, mit der Quellen-TKÜ. In die Strafprozessordnung wurde sie im August 2017 aufgenommen, nachdem u.a. die Innenminister der Länder eine gesetzliche Regelung für die strafprozessuale Quellen-TKÜ forderten.[12] Die Große Koalition von CDU/CSU und SPD reagierte auf die Forderung mit einem Eilverfahren im Zusammenhang mit den Änderungen an dem Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens. Sie verabschiedete die gesetzliche Grundlage zur Regelung der Quellen-TKÜ in wenigen Wochen. Mit dieser Eingriffsbefugnis soll es Ermittlern gelingen, den laufenden Kommunikationsverkehr bereits „an der Quelle“, also dem Absender, vor der Verschlüsselung des Anbieters abzufangen und an die Strafverfolgungsbehörden weiterzuleiten.[13] Hierzu ist es erforderlich, das von dem Straftäter genutzte Zielgerät zuvor unbemerkt mit einer Abhörsoftware zu versehen, die in den Medien als sogenannter Staatstrojaner bekannt wurde.[14] Da die grundrechtlichen Freiheiten im modernen Zeitalter der Informationsgesellschaft vehemente Verteidigung erfahren, ist gerade die stattfindende heimliche Infiltration eines informationstechnischen Systems mit einer staatlich kontrollierten Fremdsoftware, welche das Abfangen und Ausleiten verschlüsselt geführter Telekommunikation an der Quelle möglich macht, höchst umstritten.[15]

[11] Vgl. Bratke, 2013, S. 44.
[12] Vgl. Guld, Durchbruch bei der Innenministerkonferenz in Dresden. Die Chance nutzen, 2017.
[13] Liebig, 2015, S. 128.
[14] Vgl. Dalby, 2016, S. 137.
[15] Vgl. Bratke, 2013, S. 18.

Während die Anfänge der Quellen-TKÜ auf das Jahr 2006 zurückgehen[16], gewinnt das Thema Abhörung von verschlüsselter (Tele-) Kommunikation zunehmend an Bedeutung. Zur Entwicklung rechtskonformer Staatstrojaner verfügt beispielsweise das Bundeskriminalamt über eine eigene Fachabteilung. Im September 2017 wurde in München zu diesem Zweck die „Zentrale Stelle für Informationstechnik im Sicherheitsbereich“ (ZITiS) eröffnet. In den nächsten Jahren werden sich Bundesländer zu einem „Gemeinsamen Kompetenz- und Dienstleistungszentrum“ (GKDZ) zusammenschließen, um den Bereich der verschlüsselten Telekommunikationsüberwachung voranzubringen und gleichzeitig im Einzelnen Kosten zu sparen. Diese neu geschaffenen Abteilungen bringen sowohl die Aktualität sowie Relevanz des Themas zum Ausdruck.

Das Ziel dieser Arbeit ist es, die Brisanz um die Abhörung verschlüsselter Kommunikation aufzugreifen und darzustellen, wie es Strafverfolgungsbehörden i.S.d. § 100 a StPO gelingt, laufende und zum Teil verschlüsselte Kommunikation abzuhören. Während die zwei Formen der Telekommunikationsüberwachung abgebildet werden, sollen die rechtlichen und technischen Probleme im Zusammenhang mit der Quellen-TKÜ Berücksichtigung finden und die Frage nach der Notwendigkeit der Ermittlungsmaßnahme beantwortet werden.

Die Themenerarbeitung erfolgt literaturtheoretisch. Neben einschlägiger Fachliteratur werden Urteile des Bundesverfassungsgerichts und Pressemittleilungen einbezogen. Im Zentrum der Arbeit stehen drei Themengebiete: Die Quellen-TKÜ als neue Ermittlungsgrundlage in der Strafprozessordnung, daraus entstehende rechtliche und technische Probleme sowie der Diskurs um die Notwendigkeit der Maßnahme.

Jedes Kapitel beginnt mit einem Ausblick auf dessen Inhalte.

Im zweiten Kapitel werden die allgemeinen sowie technischen Grundlagen der Quellen-TKÜ deskriptiv dargestellt und eine Abgrenzung zur herkömmlichen Telekommunikationsüberwachung sowie zur Online-Durchsuchung vorgenommen.

[16] Vgl. O.V., Staatstrojaner - was ist das und wie funktioniert er?, 2017.

Dem folgend befasst sich das dritte Kapitel analytisch mit den verfassungsrechtlichen Grundlagen und Problemen, die im Zusammenhang mit der Quellen-TKÜ entstehen. Aus diesem Grund werden erst hierin die einschlägigen Grundrechte, die den Bürger vor einem staatlichen Eingriff, wie der Quellen-TKÜ schützen sowie die Rechtsgrundlage, die die Strafverfolgungsbehörden zu einer Quellen-TKÜ ermächtigt, behandelt. Am Ende des Kapitels wird der beschleunigte Gesetzgebungsprozess thematisiert, den die Große Koalition zur Verabschiedung des § 100 a StPO wählte.

Das vierte Kapitel stellt einen Exkurs dar, welcher die technischen Schwierigkeiten aufzeigt, die in Bezug auf die Quellen-TKÜ auftreten können, von der Entwicklung der Staatstrojaner im Bundeskriminalamt bis hin zu den Gefahren, die bei einer Infiltration entstehen können.

Das fünfte Kapitel liefert eine Diskussion um die Notwendigkeit der Quellen-TKÜ. Das Hauptaugenmerk liegt auf den befürwortenden und ablehnenden Stimmen, die inhaltlich nicht weiter auseinandergehen könnten.

Die Arbeit schließt mit einem Fazit, welches die Ergebnisse der Kapitel sowie die Antworten auf die Ausgangsfrage zusammenfassend darstellt und einen Ausblick auf die Quellen-TKÜ und ihre Bedeutung für die Zukunft gibt.

2. Der Einsatz der Telekommunikationsüberwachung in der Strafverfolgung

Das Kapitel greift die Fragestellung auf, wie es Ermittlern i.S.d. § 100 a StPO gelingt, laufende, zum Teil verschlüsselte Kommunikation abzuhören. Einführend wird die Telekommunikationsüberwachung (TKÜ) als heimliche Ermittlungsmaßnahme im Bereich der Strafverfolgung vorgestellt und der Begriff der Telekommunikation erläutert. Zahlen zu der Häufigkeit der Anwendung in Deutschland belegen, dass die Telekommunikationsüberwachung als Ermittlungsinstrument in den vergangenen Jahren gesteigert eingesetzt wurde und der Fokus insbesondere auf der Überwachung von Internet- sowie Mobilfunkanschlüssen liegt. Da es sich bei der Überwachung der herkömmlichen Telekommunikation um automatische, standardisierte IT-Verfahren handelt, bei denen die Betreiber öffentlicher Telefonnetze die geforderten Verbindungen

für die Strafverfolgungsbehörden aufschalten, finden das Telekommunikationsgesetz sowie die Telekommunikations-Überwachungsverordnung Erwähnung. Diese enthalten entscheidende Regelungen zur Telekommunikationsüberwachung in Deutschland. Die herkömmliche Telekommunikationsüberwachung stößt an ihre technischen Grenzen, wenn der betroffene Nutzer zur (Tele-) Kommunikation einen Voice-over-IP-Anbieter wählt, der die Telefonie oder Messenger-Nachrichten Ende-zu-Ende verschlüsselt. Diese spezielle Form sorgt für eine verschlüsselte Direktübertragung zwischen den miteinander verbundenen Gesprächspartnern vom Absenden der Daten bis zu deren Eingang beim Zielsystem.[17] Mit der herkömmlichen Telekommunikationsüberwachung kann der Datenstrom bei dem Anbieter zwar mitgeschnitten und der VoIP-Datenstrom daraus isoliert werden, die Audiodateien sind jedoch so kryptiert, dass sie für den Ermittler nicht hörbar sind.[18] Strafverfolgungsbehörden streben deshalb die Quellen-TKÜ als technisch angepasstes Ermittlungsinstrument an. Das Ziel der Quellen-TKÜ besteht darin, eine Überwachung von verschlüsselter Telekommunikation gesichert durchzuführen, in dem die Gesprächsinhalte bereits vor ihrer Verschlüsselung an dem beteiligten Endgerät aufgezeichnet und an die Ermittler weitergeleitet werden. Hierunter fällt die Infiltration des betroffenen Endgeräts durch (fern-) installierte Software zum Abfangen und Ausleiten von Kommunikationsdaten zum Zeitpunkt des Aussendens.[19] Zur Quellen-TKÜ werden die technischen Grundlagen erläutert und die Begriffe der herkömmlichen-TKÜ, Quellen-TKÜ und Online-Durchsuchung voneinander unterschieden.

2.1. Allgemeines zur Telekommunikationsüberwachung (TKÜ)

Während der Informationsaustausch zwischen Straftätern viele Jahre über das Festnetz- und Mobiltelefon erfolgte, werden dazu heute weitestgehend moderne Kommunikationsmittel eingesetzt. Zu diesen zählen Smartphones, Chat- und SMS- Dienste, E-Mail-Verkehr oder Voice-Over-IP Telefonie.[20] Die Strafverfolgungsbehörden sind deshalb zur Aufklärung von Straftaten auf Er-

[17] Vgl. Bratke, 2013, S. 31 ff.
[18] Vgl. Liebig, 2015, S. 126.
[19] Vgl. Dalby, 2016, S. 137.
[20] Vgl. Keller et al., 2015, S. 19.

mittlungsbefugnisse angewiesen, die die Inhalte und Umstände von Telekommunikationsvorgängen festhalten. Hierfür hält der Gesetzgeber eine sogenannte heimliche Ermittlungsbefugnis bereit, bei welcher die Betroffenen zunächst keine Kenntnis davon haben, dass sie durch den Staat abgehört werden.[21] Die Rede ist von der Telekommunikationsüberwachung. Sie ist für den Bereich der Strafverfolgung in § 100 a StPO geregelt und ermöglicht den Zugriff auf die Inhalte der laufenden Telekommunikation.[22] Telekommunikation beschreibt den technischen Vorgang der Nachrichtenübermittlung vom Absenden der Signale bis zu deren Empfang beim Adressaten.[23] Ermittler dürfen mit Hilfe dieser Abhörmethode das eigentliche Gespräch, Hintergrundgespräche und Aufzeichnungen erheben und verwerten, „die während des Wählvorgangs oder beim Ertönen des Freizeichens gemacht werden."[24] Gleiches gilt, wenn der Betroffene versehentlich eine von ihm hergestellte Telekommunikationsverbindung nicht beendet hat.[25] § 100 a StPO gestattet ferner den Zugriff auf Standort- und Verkehrsdaten eines Mobiltelefons, die zu Ermittlungszwecken herangezogen werden dürfen.[26] Das Bundesamt für Justiz liefert jährlich Zahlen zur Häufigkeit der Telekommunikationsüberwachung in den einzelnen Bundesländern sowie in Deutschland. Hiernach wurden 2016 bundesweit 5738 Verfahren i.S.d. § 100 a Abs. 1 StPO geführt, bei welchen es insgesamt 17510 Erstanordnungen gab. Zu den Zahlen ist anzuführen, dass in einem Verfahren mehrere Anordnungen sowie Verlängerungsanordnungen ergehen können. Mit Blick auf die Anzahl der Überwachungsanordnungen unterschieden nach der Art der zu überwachenden Kommunikation, fällt die hohe Zahl der abgehörten Mobilfunktelekommunikation mit 21236 neben der Festnetztelekommunikation mit 3856 Überwachungsanordnungen auf. Auch das staatliche Abhören der Internettelekommunikation mit 10606 Überwachungsanordnungen gewährt einen Einblick darin, dass die Verständigung über moderne Kommunikationswege zugenommen hat.[27] *Meister* berichtet, dass 2016 in

[21] Vgl. ebd.
[22] Vgl. ebd. S. 27.
[23] Vgl. Liebig, 2015, S. 122.
[24] Keller et al., 2015, S. 27.
[25] Vgl. BGH NStZ 2003, 668.
[26] Vgl. Keller et al., 2015, S. 28.
[27] Vgl. Bundesamt für Justiz, 2016, S. 1 ff.

Berlin über 1,3 Millionen Telefonate abgehört wurden. Ein Drittel der Anordnungen betraf das Betäubungsmittelgesetz. In den letzten Jahren ist die Zahl der Telekommunikationsüberwachungen gestiegen. Die Überwachung von Internet- und Mobilfunkanschlüssen erreicht einen neuen Rekord.[28] Sich dem anschließend, bezeichnen *Keller*, *Braun* und *Hoppe* die strafprozessuale Telekommunikationsüberwachung als Massenermittlungsmethode, die im Zeitalter der Digitalisierung nicht mehr für alle Formen der Kommunikation zielführend Anwendung findet.[29]

2.2. Die herkömmliche Telekommunikationsüberwachung

Noch immer werden Telefongespräche über den Festnetzanschluss und Mobilfunkgeräte geführt, obwohl eine Zunahme der Telekommunikation über Smartphones und das Internet zu verzeichnen sind.[30] Die herkömmliche Telekommunikation funktioniert mithilfe eines Telefons als Endgerät, welches akustische in elektronische Signale umwandelt und umgekehrt. Die umgewandelten elektronischen Signale werden über ein drahtgebundenes Telefonnetz, meistens durch Kupferkabel, weitergeleitet. Es handelt sich bei einem herkömmlichen Telefongespräch um eine leitungsvermittelte, sogenannte stehende Verbindung zwischen den Gesprächsteilnehmern, da ein Teil des Telefonnetzes für die Dauer des Telefonats für dieses Gespräch reserviert wird.[31] Das staatliche Abhören funktioniert hierbei durch automatische, standardisierte IT-Verfahren, bei denen die Betreiber öffentlicher Telefonnetze die geforderten Verbindungen für die Strafverfolgungsbehörden aufschalten. Diesen wird es hierdurch ermöglicht, den laufenden Kommunikationsverkehr abzuhören.[32] Das Telekommunikationsgesetz (TKG) enthält nach § 110 Abs. 1 Nr. 1 TKG die für die Telekommunikationsüberwachung zentrale Verpflichtung, technische Einrichtungen zur Umsetzung gesetzlich vorgesehener Maßnahmen zur Überwachung der Telekommunikation vorzuhalten. Durch das TKG werden zwei Überwachungsarten und Verfahren geregelt: Die vollständige Überwachung des Kommunikationsinhaltes und der Verkehrsdaten nach §

[28] Vgl. Meister, Telefonüberwachung: Berliner Polizei hat letztes Jahr zwei Telefongespräche pro Minute abgehört, 2017.
[29] Vgl. Keller et al., 2015, S. 24.
[30] Vgl. Liebig, 2015, S. 122 ff.
[31] Vgl. Liebig, 2015, S. 124.
[32] Vgl. Keller et al., 2015, S. 44.

110 TKG sowie das automatisierte Auskunftsverfahren der Sicherheitsbehörden in Bezug auf Bestandsdaten wie Anschrift, Name und Rufnummer des Kunden nach §§ 111, 112, 113 TKG.[33] Bei den Verkehrsdaten handelt es sich um die technischen Informationen in der Telekommunikation, die bei der Nutzung eines Telekommunikationsdienstes beim jeweiligen Telekommunikationsanbieter anfallen und von diesem erhoben, gespeichert, genutzt und übermittelt werden. Die im TKG festgelegten Anforderungen sind durch die Betreiber von Telekommunikationsplattformen auf eigene Kosten zu erbringen.[34] Die Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation, kurz Telekommunikations-Überwachungsverordnung (TKÜV) bestimmt, wie die Anforderungen z.B. aus dem Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG), des Zollfahndungsdienstgesetzes (ZFdG), der Strafprozessordnung (StPO) und den landesgesetzlichen Vorschriften umzusetzen sind.[35] Insbesondere geht es darum, inwieweit die Telekommunikationsanbieter eine Überwachungsstruktur und Abhörschnittstellen zu implementieren und vorzuhalten haben.[36]

2.3. Die Quellen-Telekommunikationsüberwachung

Aufgrund der Zunahme von modernen Kommunikationsmitteln in der Telekommunikation, stellt die Quellen-TKÜ ein modernes Ermittlungsinstrument dar, welches in direkter Weise mit der fortschreitenden technischen Entwicklung auf dem Telekommunikationsmarkt und der damit verbundenen Erschwernis in Bezug auf strafprozessuale Ermittlungsarbeit korreliert.[37] Die Quellen-TKÜ ist die Antwort auf die zunehmende Verbreitung softwarebasierter VoIP-Kommunikation, bei welcher in technischer Hinsicht eine automatisierte und um-

[33] Vgl. Gorgass, 2011, S. 54 ff.
[34] Vgl. Gorgass, 2011, S. 54.
[35] Vgl. Bundesministerium der Justiz und für Verbraucherschutz, Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation, 2017.
[36] Vgl. Gorgass, 2011, S. 67 ff.
[37] Vgl. Bratke, 2013, S. 44.

fassende Ende-zu-Ende-Verschlüsselung stattfindet, weshalb bei dieser Kommunikationsform eine klassische Telekommunikationsüberwachung wenig erfolgsversprechend ist.[38]

Seit den Enthüllungen von *Snowden* zu den weltweiten Abhör- und Spionagepraktiken von Geheimdiensten 2013[39] gibt es zunehmend Telefon- und Messenger-Dienste, die dem Nutzer eine verschlüsselte (Tele-) Kommunikation und damit mehr Sicherheit anbieten. Wurden zuvor Bilder, Nachrichten, Videos und Telefonie weitgehend ungesichert über das Internet verschickt, so dass es Dritten mit geringem Aufwand möglich war, mitzulesen oder mitzuhören[40], basiert die noch recht junge Technologie der IP-Telefonie auf Internet-Protokollen und erfolgt über paketvermittelte Netze. Ein solches Netz stellt das Internet dar. Aus technischer Sicht wird die Sprachinformation in IP-Pakete aufgeteilt, die unabhängig voneinander durch das Netzwerk zum Ziel gelangen und dort wieder zu einem Audiodatenpaket zusammengesetzt werden. Bei der Internet-Telefonie dient meist ein an das Internet angeschlossener Computer als Endgerät, auf dem eine entsprechende Kommunikationssoftware installiert ist.[41] Die Anbieter von IP-Telefonie, auch Voice-over-IP (VoIP) genannt, stellen eine direkt verbundene Kommunikation von Computer zu Computer (peer-to-peer/P2P) kostenlos zur Verfügung und gewinnen auf diese Weise weiter an Beliebtheit.[42] Wie *Google-Talk*, *Skype*, *QuteCom* u. a. zeigen, hält das Internet eine Bandbreite der speziellen VoIP-Software zum Download bereit. Die bekannteste und mit rund 560 Millionen Nutzern weltweit am weitesten verbreitete VoIP-Software war viele Jahre die des Anbieters *Skype*. Neben der Kostenfreiheit und der weltweiten Verfügbarkeit des Dienstes, bietet die automatische Ende-zu-Ende-Verschlüsselung der Kommunikationsinhalte während der Übermittlung einen Anreiz für den Nutzer.[43] Alle *Skype*-internen Audio- und Videogespräche, die von Computer zu Computer geführt werden, werden laut Unternehmensangaben automatisch durch einen sicheren Ver-

[38] Vgl. Bratke, 2013, S. 44.
[39] Vgl. Beuth, Alles Wichtige zum NSA-Skandal, 2013.
[40] Vgl. Hesseling, Verschlüsselte Messenger: Threema, Signal, Telegram, WhatsApp, 2015.
[41] Vgl. Liebig, 2015, S. 124.
[42] Vgl. Bratke, 2013, S. 29 ff.
[43] Vgl. Bratke, 2013, S. 30 ff.

schlüsselungsalgorithmus vor unbefugten Zugriffen Dritter geschützt. Die spezielle Ende-zu-Ende-Verschlüsselung sorgt hierbei für eine verschlüsselte Direktübertragung zwischen den miteinander verbundenen Gesprächspartnern vom Absenden der Daten bis zu deren Eingang beim Zielsystem.[44] Von der *Skype*-Software erfolgt die Verschlüsselung automatisch gesteuert, lokal auf dem Computer des jeweiligen Absenders der Kommunikationsdaten, während die Entschlüsselung erst auf dem Computer des Empfängers stattfindet. Neben dem kostenlosen softwarebasierten P2P-VoIP-Dienst bietet das Unternehmen *Skype* als einen zusätzlichen VoIP-Dienst auch das Führen von Telefonaten von Computern und Anschlüssen im öffentlichen Telefonnetz an. Bei Gesprächen unter Beteiligung des öffentlichen Telefonnetzes können die Signale technisch bedingt nicht Ende-zu-Ende-verschlüsselt übertragen werden. Die Verschlüsselung findet hier bis zu bzw. ab den Gateways statt, den Schnittstellen zwischen dem Internet und dem Fest-/Mobilfunknetz. Seit 2010 ist nunmehr auch die *Skype*-Software zur mobilen Nutzung des Dienstes, insbesondere für Mobiltelefone, Smartphones und Tablets mit einer Ende-zu-Ende-Verschlüsselung erhältlich.[45]

Die drei genannten Formen von VoIP, die das Unternehmen *Skype* u.a. anbietet, geben einen Einblick in die unterschiedlichen Erscheinungsformen von IP-Kommunikation.[46] Telefoniert ein Verdächtiger nicht auf herkömmlichem Wege, sondern über das Internet oder Smartphone mittels VoIP-Software, sind die Gesprächsdaten verschlüsselt. Das bedeutet, dass sich bei dem Internetanbieter zwar der Datenstrom mitschneiden und der VoIP-Datenstrom daraus isolieren lässt, die Audiodateien jedoch kryptiert, also für den Strafverfolger nicht hörbar und somit faktisch wertlos sind.[47] Die herkömmliche Telekommunikationsüberwachung ist hierbei nicht mehr erfolgsversprechend. Zudem hat der Ermittler mit seinen bisherigen Werkzeugen technisch kaum Möglichkeiten die Kommunikationsdaten zu entschlüsseln. „Der VoIP-Software-Anbieter *Skype* etwa setzt nach eigenen Angaben die maximale Verschlüsselung von 256 Bit ein.“[48] Diese zu entschlüsseln würde für die Ermittler eine

[44] Vgl. Bratke, 2013, S. 31 ff.
[45] Vgl. Bratke, 2013, S. 34.
[46] Vgl. Bratke, 2013, S. 40.
[47] Vgl. Liebig, 2015, S. 126.
[48] Vgl. Liebig, 2015, S. 126.

unzumutbar lange Zeit in Anspruch nehmen, bis die Gesprächsinhalte offen lägen.[49] Obwohl eine Entschlüsselung der kryptierten Gesprächsdaten durch die Strafverfolger nahezu ausgeschlossen ist, stellen sogenannte Backdoors (Hintertüren) eine generelle Entschlüsselungsmöglichkeit dar. Hierbei handelt es sich um Sicherheitslücken, die Software-Entwickler teilweise absichtlich in ihre Programme einbauen, um sich oder Dritten im Nachhinein versteckt Zugang zu den Gesprächsinhalten zu verschaffen.[50] Die Nutzung einer technischen Hintertür wäre mit einer herkömmlichen Telekommunikationsüberwachung vergleichbar.[51] Da eine solche Hintertür den Strafverfolgungsbehörden im Allgemeinen nicht zur Entschlüsselung der Telekommunikation zur Verfügung steht, streben diese, neben der hier nicht zielführenden herkömmlichen Telekommunikationsüberwachung die Quellen-TKÜ als technisch angepasstes Ermittlungsinstrument an. Hierunter fällt die Infiltration des betroffenen Endgeräts durch (fern-) installierte Software zum Abfangen und Ausleiten von Kommunikationsdaten zum Zeitpunkt des Aussendens.[52] Das Ziel der Quellen-TKÜ besteht darin, eine Überwachung von verschlüsselter Telekommunikation, wie VoIP-Telefonie und Messenger-Diensten, gesichert durchzuführen, in dem „die Gesprächsinhalte bereits vor ihrer Verschlüsselung an dem beteiligten Endgerät aufgezeichnet und an die Ermittler weitergeleitet werden. Die Daten müssen praktisch ‚an der Quelle′ abgegriffen werden“[53], woraus sich der Name dieser Maßnahme ableitet.[54] Zusammenfassend soll mit der Quellen-TKÜ ein Zugriff auf Daten eines Telekommunikationsvorgangs in unverschlüsselter, also einsehbarer Form, und letztlich die Erlangung von beweisverwertbaren Erkenntnissen zur Verfolgung und Aufklärung von Straftaten gewährleistet werden.[55] Wesentlicher Gegenstand der Ermittlungsmaßnahme sind dabei im Regelfall die Inhalte der geführten VoIP-Kommunikation. Wie bei der herkömmlichen Telekommunikationsüberwachung können neben der

[49] Vgl. Liebig, 2015, S. 126.
[50] Vgl. Liebig, 2015, S. 127.
[51] Vgl. Keller et al., 2015, S. 44.
[52] Vgl. Dalby, 2016, S. 137.
[53] Liebig, 2015, S. 128.
[54] Vgl. Bratke, 2013, S. 41.
[55] Vgl. Bratke, 2013, S. 45.

Quellen-TKÜ auch die näheren Umstände der Telekommunikation, wie z.B. die Erhebung von Verkehrsdaten im Fokus der Überwachung stehen.[56]

2.3.1. Das Verschlüsselungsverbot nach § 8 Abs. 3 TKÜV und die Übertragung der Telekommunikationsinhalte an die Strafverfolgungsbehörden

Notwendig wäre die Quellen-TKÜ insbesondere dann nicht, wenn die Telekommunikationsanbieter ihre Verschlüsselung zum Zwecke der Strafverfolgung aufheben würden. Als ‚verstecktes Verschlüsselungsverbot' wird § 8 Abs. 3 TKÜV angesehen, für welches nur ein enger verfassungsrechtlicher Rahmen besteht. Aus diesem geht hervor, dass bei der Ausleitung der Nutzinformation, genauer den Nutzdaten, die Verschlüsselung durch den Telekommunikationsanbieter aufzuheben ist.[57] Es ist zu beachten, dass die Pflicht zur Schlüsselherausgabe oder unverschlüsselten Ausleitung nur gegenüber den Telekommunikationsbetreibern besteht, die eine eigene netzseitige Verschlüsselung anbieten. Wird die Verschlüsselungstechnik von einem Drittanbieter übernommen oder von dem Endkunden selbst eingesetzt, so zählen diese nicht zum Adressatenkreis der TKÜV und müssen keine Vorkehrungen zur Entschlüsselung vornehmen.[58] *Gorgass* weist auf eine mögliche Ungleichbehandlung zwischen Telekommunikationsanbietern und solchen von reiner Verschlüsselungssoftware hin. Denn der Telekommunikationsanbieter, der durch die TKÜV angesprochen wird, ist gesetzlich gezwungen, ein weniger effektives und sicheres Angebot zu erbringen als der Anbieter der reinen Verschlüsselungssoftware.[59] Das Verschlüsselungsverbot hilft den Strafverfolgungsbehörden an dieser Stelle nur bedingt weiter. Ebenfalls zu beachten ist, dass mit der Entschlüsselung bzw. kurzzeitigen Aufhebung der Verschlüsselung bei dem Anbieter ein zusätzliches Risiko geschaffen wird, dass auch ein unberechtigter Dritter diese Schwachstelle nutzt. Um den Strafverfolgungsbehörden den Ge-

[56] Vgl. Bratke, 2013, S. 46.
[57] Vgl. Gorgass, 2011, S. 106.
[58] Vgl. Gorgass, 2011, S. 106.
[59] Vgl. Gorgass, 2011, S. 106.

sprächsinhalt in unverschlüsselter Form zur Verfügung zu stellen, ist der Einsatz eines sogenannten „Zwangs-Proxy-Servers“ notwendig.[60] Allgemein fungiert ein Proxy-Server als ein Vermittler in einem Netzwerk. Er nimmt Anfragen entgegen und leitet sie stellvertretend weiter. Mit einem Proxy-Server gelingt es, die Kommunikation zwischen einem lokalen Client, also dem Anwender- bzw. dem Computerprogramm und einem Webserver abzusichern, zu beschleunigen und zu verschleiern.[61] Er wird in diesem Verfahren gezwungenermaßen dazwischengeschaltet. Der Telekommunikationsinhalt verläuft hierbei zwischen dem Anrufenden (A-Teilnehmer) und dem eingesetzten Zwangs-Proxy-Server verschlüsselt. An diesem wird die Verschlüsselung für einen minimalen Zeitraum aufgehoben, so dass die Inhalte nach einer erneuten Verschlüsselung zwischen dem Zwangs-Proxy-Server und dem Angerufenen (B-Teilnehmer) gesichert übertragen werden. Auf diese Art ist es möglich, das Gespräch an dem eingesetzten Zwangs-Proxy-Server im Bedarfsfall unverschlüsselt an die berechtigten Stellen weiterzuleiten.[62]

2.3.2. Der technische Hintergrund der Quellen-TKÜ

Bei einer Quellen-TKÜ handelt es sich aus technischer Sicht um den Einsatz einer Spionagesoftware, die auf einem informationstechnischen System möglichst ohne Wissen des Nutzers unbemerkt verdeckte Funktionen ausführt.[63] Diese Software hat die Funktionsweise eines sogenannten Trojaners und muss zunächst auf dem Endgerät installiert werden. Als Beispiele für solche Trojaner werden hier die vom Bundeskriminalamt (BKA) programmierte Remote Communication Interception Software (*RCIS*) und die Spionagesoftware *FinSpy*[64] genannt, die von der britisch-deutschen Firma FinFisher GmbH entwickelt und vom BKA gekauft wurde. Die Spionagesoftware dient insbesondere der Aufzeichnung sowie Weiterleitung unverschlüsselter Telekommunikationsdaten an die Ermittler[65] und wird allgemein als Staatstrojaner bezeichnet.[66] Wie er beschaffen sein kann, zeigt ausschnittsweise die Analyse des

[60] Vgl. Gorgass, 2011, S. 107.
[61] Vgl. Donner, Was ist ein Proxy Server?, 2017.
[62] Vgl. Gorgass, 2011, S. 107.
[63] Vgl. Kurz et al., 2016, S. 3.
[64] Vgl. Reuter, Nordrhein-Westfalen will den Staatstrojaner nutzen, 2017.
[65] Vgl. Liebig, 2015, S. 129.
[66] Buermeyer, 2017, S. 20.

Chaos Computer Clubs (CCC), der 2011 den von dem privaten Softwareunternehmen *DigiTask* programmierten Trojaner untersuchte, welcher zum staatlichen Abhören der Telekommunikation eingesetzt wurde. Der Trojaner verfügte über die Funktionen Bildschirmfotos, sogenannte Screenshots, anzufertigen, *Skype* und andere VoIP-Gespräche abzuhören und beliebige „Schad-Module“ nachzuladen.[67] Durch Schad-Module wäre es technisch denkbar, die Funktionalität des Trojaners dahingehend zu erweitern, dass auch das Durchsuchen, Schreiben, Lesen und Manipulieren von Dateien ermöglicht wäre. Des Weiteren wäre ein Zugriff auf das Mikrofon, die Kamera und Tastatur vorstellbar, was grundsätzlich einem digitalen großen Lauschangriff nahekäme. Unter diesem wird umgangssprachlich die akustische Wohnraumüberwachung verstanden, die das Aufzeichnen des nicht öffentlich gesprochenen Wortes mit technischen Mitteln vorsieht.[68] Bei dem Trojaner sei der Versuch damals nicht unternommen worden, technisch sicherzustellen, dass die Datenerfassung auf die Telekommunikationsdaten beschränkt bliebe.[69] Wie die Untersuchung des CCC zeigte, gelang es bereits 2011 mit der Software nicht nur eine Quellen-TKÜ durchzuführen, um verschlüsselte VoIP-Telekommunikation abzuhören, sondern nahezu das gesamte infiltrierte Computersystem zu überwachen.[70]

2.3.3. Möglichkeiten zur Infiltration von Abhörsoftware

Für die Durchführung einer Überwachung und Aufzeichnung der über das Zielsystem geführten verschlüsselten Telekommunikation, im Sinne einer Quellen-TKÜ, ist die vorherige Installation eines entsprechenden Staatstrojaners erforderlich.[71] Dieser muss dem Endgerät heimlich bzw. verdeckt zugeführt werden.

In der Praxis hat sich eine Vielzahl von Vorgehensweisen entwickelt, wie die Überwachungssoftware unbemerkt in das Zielsystem gebracht und auf diesem installiert werden kann. Die Auswahl hängt sowohl von den technischen Gegebenheiten als auch von den Gewohnheiten sowie dem individuellen Nutzungsverhalten der Zielperson im konkreten Fall ab.[72] Eine kriminalistische

[67] Vgl. Liebig, 2015, S. 129 ff.
[68] Vgl. Bundeszentrale für politische Bildung, Lauschangriff, 2017.
[69] Vgl. Liebig, 2015, S. 130.
[70] Vgl. Liebig, 2015, S. 130.
[71] Vgl. Bratke, 2013, S. 94.
[72] Vgl. Bratke, 2013, S. 95.

Kreativität der durchführenden Behörde sei bei der Bandbreite der Einzelkonstellationen unerlässlich, wobei allen Vorgehensweisen die Heimlichkeit gleich ist. Nachfolgend sollen die in Frage kommenden Vorgehensweisen zum Einbringen der Spähsoftware auf das Zielsystem dargestellt werden.

Die Online-Infiltration zählt als gangbare Vorgehensweise, den Trojaner aus der Ferne verdeckt und ohne direkten physischen Zugriff auf das Gerät zu bringen. Hierbei wird von Remote-Installation gesprochen. Mit dieser Vorgehensweise ist eine gewisse Täuschung des Nutzers verbunden, um diesen zu einer Mitwirkungshandlung zu veranlassen. Dies lässt sich in der Praxis beispielsweise durch eine zugesandte E-Mail realisieren.[73] Dabei wird eine präparierte E-Mail durch die Überwachungsbehörde an den Betroffenen versandt, welche die Abhörsoftware versteckt enthält. Denkbar wäre ebenfalls eine Datei, welche der E-Mail als Anhang mitgeschickt wird. Durch das Herunterladen und anschließende Öffnen der Datei durch die Zielperson installiert sich der Trojaner im Hintergrund, ohne dass weitere Zwischenschritte notwendig werden.[74] Damit der Betroffene die Spähsoftware nicht erkennt und deren Installation durch sein Mitwirken unbewusst veranlasst, werden die E-Mails und Dateien in der Regel unter einer bestimmten Legende, wie einem Namen oder einem bestimmten Betreff versandt. Hierdurch soll der Empfänger über eine gewisse Vertrauenswürdigkeit getäuscht werden. Alternativ könnte eine solche E-Mail auch als offizielles Schreiben unter dem Namen einer anderen Behörde versendet werden, was sich jedoch aufgrund der Akzeptanz und des Vertrauens in elektronische Angebote und Schreiben staatlicher Stellen auf begründete Ausnahmefälle beschränken sollte.[75] In Erwägung ziehen ließe sich auch das Einrichten einer manipulierten fingierten Internetseite, die bei Downloads oder dem bloßen Aufrufen der Webseite durch den Betroffenen die Überwachungssoftware heimlich überträgt. Bei dem Vorgang wird von sogenannten Drive-By-Downloads gesprochen.[76] Als weitere erfolgsversprechende Vorgehensweise soll der Einsatz von manipulierten Datenträgern, wie CDs, DVDs und USB-Sticks vorgestellt werden. Diese können der Zielperson

[73] Vgl. Bratke, 2013, S. 96.
[74] Vgl. Bratke, 2013, S. 96.
[75] Vgl. Bratke, 2013, S. 97.
[76] Vgl. Bratke, 2013, S. 97.

unter einer Legende, wie einer Vorteilsaktion, zugespielt werden. Die Datenträger können den Staatstrojaner selbst enthalten, welcher sich dann beim Anschließen auf dem Zielsystem installiert oder ein Programm enthalten, welches eine Hintertür in das Zielsystem öffnet, um die Software von außen einspielen zu können.[77] Neben den vorgestellten Alternativen kann eine heimliche Infiltration des Trojaners auch ohne eine Mitwirkungshandlung des Betroffenen erfolgen. Hierzu zählt vor allem das Ausnutzen bestehender Sicherheitslücken oder Fehlfunktionen in Anwendungsprogrammen oder Betriebssystemen genutzter Systeme. Mit Hilfe virtueller Werkzeuge (sogenannter Exploits) nutzen die Ermittlungsbehörden derartige Lücken als Einfallstor in das Zielsystem für das Einbringen der Abhörsoftware. Ein Exploit stellt ein kleines Schadprogramm bzw. eine Befehlsfolge dar, die Sicherheitslücken und Fehlfunktionen von Anwendungs- und Hilfsprogrammen ausnutzt, um sich programmtechnisch Möglichkeiten zur Manipulation von PC-Aktivitäten zu verschaffen.[78] Wie die Exploits stellen auch Backdoors die Möglichkeit zur heimlichen Softwareinstallation ohne Mitwirkung des Betroffenen dar.[79]

Neben dem dargestellten Fernzugriff dient das manuelle Einwirken als Kompromiss, um den Staatstrojaner auf das Zielsystem zu spielen. Hiermit ist der physische Zugriff auf den Computer gemeint. Auch dieses Vorgehen ist regelmäßig mit einer gewissen Täuschungshandlung gegenüber dem Nutzer verbunden.[80] Hoheitsträger können die Spähsoftware eigenständig durch kurzzeitiges Verschaffen des direkten Zugriffs auf das Zielgerät heraufbringen[81], etwa bei einer Grenz- oder Personenkontrolle, einer Durchsuchungsmaßnahme oder während sich das Gerät bei einer Reparatur befindet.[82] Dieses Vorgehen erfordert regelmäßig eine gewisse kriminalistische bzw. kriminaltaktische Kreativität, sowie eine intensive Ermittlungsarbeit im Vorfeld, um die Gewohnheiten und das soziale Umfeld der betroffenen Person zu kennen und eine erfolgversprechende Option zu wählen.[83] Dieser Möglichkeit schließt sich

[77] Vgl. Bratke, 2013, S. 98.
[78] Vgl. Siller, Exploit, 2017.
[79] Vgl. Bratke, 2013, S. 99.
[80] Vgl. Bratke, 2013, S. 99.
[81] Vgl. Liebig, 2015, S. 131.
[82] Vgl. Bratke, 2013, S. 100.
[83] Vgl. Bratke, 2013, S. 100.

die Methode an, dass sich die Strafverfolgungsbehörden heimlich Zugang zu den Räumlichkeiten des Betroffenen verschaffen, in denen sich das Zielsystem befindet. In den Wohn-, Betriebs- und Geschäftsräumen könnten zunächst die Systemparameter in Erfahrung gebracht werden, um dann über die verfügbaren Systeminformationen einen auf das Zielsystem zugeschnittenen Trojaner zu entwerfen und diesen in einem nächsten Schritt auf dem Endgerät zu infiltrieren. Der direkte Zugriff bietet die unmittelbare Möglichkeit, sicherzustellen, dass die Software auf das richtige Gerät gelangt.[84] Dieses Vorgehen unterliegt insbesondere dann einer rechtlichen Prüfung, sobald es zu einem heimlichen Betreten von Wohnräumen und sonstigen durch Art. 13 Abs. 1 Grundgesetz (GG) geschützten Räumlichkeiten des Betroffenen kommt. Für das heimliche Sich-Zugang-Verschaffen zu dem Gerät wäre zur Rechtfertigung des Eingriffs in Art. 13 Abs. 1 GG ein Betretungsrecht erforderlich. Ein solches findet für Maßnahmen der Telekommunikationsüberwachung weder eine verfassungsrechtliche Grundlage in Art. 13 Abs. 1 GG, noch geht es aus der einfachgesetzlichen Rechtsgrundlage des § 100 a StPO hervor.[85] Für die Praxis ist deshalb entscheidend, wo sich das Zielgerät befindet und ob es gegebenenfalls frei zugänglich ist. In öffentlich zugänglichen Räumen oder auch in Räumen Dritter mit deren Einverständnis ist der direkte Zugriff durch Ermittlungspersonen auf Zielgeräte im Gegensatz zu nach Art. 13 Abs. 1 GG geschützten Räumlichkeiten unproblematisch.[86] Bei der genannten Untersuchung des *DigiTask*-Trojaners durch den CCC konnte nicht festgestellt werden, auf welche Art und Weise dieser auf den Zielrechnern installiert wurde.[87]

Nach Abschluss der Telekommunikationsüberwachung ist die Abhörsoftware wieder von dem Endgerät zu entfernen. Auch das Entfernen gilt wie das Installieren als Begleitmaßnahme der Quellen-TKÜ. Unter der Deinstallation des Trojaners wird das vollständige Entfernen aller installierten Softwarekompo-

[84] Vgl. Bratke, 2013, S. 101.
[85] Vgl. Bratke, 2013, S. 101.
[86] Vgl. Bratke, 2013, S. 101.
[87] Vgl. Liebig, 2015, S. 132.

nenten sowie getätigten Konfigurationen vom überwachten informationstechnischen System verstanden. Das Zielgerät muss anschließend wieder in einem Zustand, wie vor der technischen Infiltration, gebracht werden.[88]

Hinsichtlich der Abwehrmöglichkeiten seitens des Nutzers gilt, dass eine Verhinderung oder zumindest eine Erschwerung einer Infiltration des Systems trotz aller technischen Finesse der Angriffsprogramme möglich ist. Hierfür sind allerdings ein nicht unerheblicher Aufwand sowie ein gewisses Fachwissen von Nöten. Nutzer können neben den üblichen Sicherheitsvorkehrungen, wie der Anwendung einer Personal Firewall oder eines Virenscanners auch ausgefallenere Varianten wählen. Darunter wird beispielsweise die regelmäßige Neuinstallation des Betriebssystems oder der ständige Wechsel des Internet-Zugangs verstanden.[89]

2.3.4. Abgrenzung der Quellen-TKÜ zur herkömmlichen Telekommunikationsüberwachung

Nachdem die Quellen-TKÜ für den Bereich der Strafverfolgung viele Jahre keine rechtliche Verankerung in der Strafprozessordnung fand, wurde im Juni 2017 eine Änderung des § 100 a StPO durch den Bundestag verabschiedet. Mit dem Gesetz zur effektiveren und praxistauglichen Ausgestaltung des Strafverfahrens vom August 2017 trat der geänderte § 100 a StPO in Kraft, welcher erstmalig die Quellen-TKÜ für den Bereich der Strafverfolgung regelt.[90] § 100 a Abs. 1 S. 1 StPO erlaubt weiterhin die herkömmliche TKÜ, die Quellen-TKÜ findet ihre Rechtsgrundlage in § 100 Abs. 1 S. 2 und 3 StPO. Zwar ähnelt diese von ihrem Namen einer herkömmlichen Telekommunikationsüberwachung, ist aber technisch nicht mit dem Abhören von Telekommunikation auf dem Leitungsweg zu vergleichen. Der technische Aufwand und die möglichen Gefahren werden bei der Quellen- gegenüber der herkömmlichen Telekommunikationsüberwachung für deutlich höher befunden, da dem bloßen Aufschalten der Telekommunikationsanbieter eine Spähsoftware gegenübersteht, die zunächst auf das Zielgerät gebracht werden muss. Mit der neuen Überwachungsmaßnahme sieht der CCC einen heimlichen digitalen Einbruch in ein

[88] Vgl. Bratke, 2013, S. 94.
[89] Vgl. Hermann, 2010, S. 29.
[90] Vgl. O.V., Änderungen an der Strafprozeßordnung, 2017.

informationstechnisches System verbunden. Erfasst die Überwachungssoftware neben der laufenden Kommunikation auch andere Informationen des infiltrierten Systems, ist sie als Online-Durchsuchung zu werten.[91]

2.3.5. Abgrenzung der Quellen-TKÜ zur Online-Durchsuchung

An dieser Stelle soll auf die inhaltliche Abgrenzung zu dem Begriff der Online-Durchsuchung eingegangen werden. Sowohl bei der Quellen-TKÜ als auch der Online-Durchsuchung werden fremde Computersysteme heimlich mit einem Staatstrojaner überwacht. Die Online-Durchsuchung zielt auf alle gespeicherten Daten ab, die sich auf dem Endgerät befinden, während sich die Quellen-TKÜ auf laufende Kommunikationsdaten beschränken soll.[92] Funktional ist die Quellen-TKÜ nur in Hinsicht auf die nach der Infiltration auszuführenden Befehle abzugrenzen. Das technische Vorgehen ist nahezu identisch. Bei beiden Strafverfolgungsmaßnahmen müssen während der Infektion Dateien ausgelesen, geändert und geschrieben, Programme ausgeführt, Sicherheitsmechanismen umgangen und Systembestandteile verändert werden.[93]

2.3.6. Zusammenfassung der Telekommunikationsüberwachung in der Strafverfolgung

Zur Beantwortung der gestellten Frage, wie es Ermittlern gelingt, laufende und teils verschlüsselte Kommunikation abzuhören, kann festgehalten werden, dass die Strafverfolgungsbehörden nach § 100 a StPO rechtlich dazu befugt sind, die herkömmliche laufende Telekommunikation via Festnetzanschluss und Mobiltelefon sowie die verschlüsselte (Tele-) Kommunikation via IP-Telefonie und Messenger-Diensten abzuhören. Bei der herkömmlichen TKÜ sind die Netzbetreiber angehalten, die geforderte Telefonverbindung aufzuschalten, so dass die Ermittler die gewünschte Telekommunikationsleitung mithören können. Bei der Quellen-TKÜ muss zunächst von den Strafverfolgern eine Abhörsoftware auf dem Zielgerät infiltriert und installiert werden, um die noch unverschlüsselte Telekommunikation vor dem Absenden abzufangen und den Ermittlern weiterzuleiten. Nach *Bratke* habe die Kommunikation via Internet-

[91] Vgl. Kurz et al., 2016, S. 4.
[92] Vgl. Liebig, 2015, S. 129.
[93] Vgl. Kurz et al., 2016, S. 5.

protokoll das technische und wirtschaftliche Potential, die herkömmliche Festnetztelefonie durch Internettelefonie im Zeitalter der Digitalisierung abzulösen[94], weshalb die Quellen-TKÜ für die Strafverfolgungsbehörden im digitalen Zeitalter an Bedeutung gewinnt.

3. Rechtliche Probleme im Zusammenhang mit der Quellen-TKÜ

Mit einer Ermittlungsbefugnis wie der Quellen-TKÜ nach § 100 a Abs. 1 S. 2 und 3 StPO wird bei Anwendung in Grundrechte von Betroffenen eingegriffen. Das Bundesverfassungsgericht stellte bereits 1958 in seiner „Lüth-Entscheidung“ fest, dass Grundrechte in erster Linie dazu bestimmt sind, die Freiheitssphäre des Einzelnen vor Eingriffen der öffentlichen Gewalt zu sichern.[95] Das Verfassungsrecht soll in diesem Kapitel bei der Beantwortung der Frage einbezogen werden, in welche Grundrechte mit der Quellen-TKÜ und deren Begleitmaßnahmen eingegriffen wird.

Anschließend wird der reformierte § 100 a StPO behandelt, welcher mit der vorherigen Fassung des Gesetzestextes verglichen wird. Während Ausführungen hinsichtlich des erforderlichen Tatverdachts sowie des vorgegebenen Straftatenkatalogs der (Quellen-) Telekommunikationsüberwachung gemacht werden, folgen die Regelungen zu den Adressaten, der Anordnungskompetenz und dem Kernbereichsschutz. Schließlich werden §§ 100 a ff. StPO dahingehend untersucht, in wie weit bei einer Quellen-TKÜ die technischen Komponenten sichergestellt und protokolliert werden müssen.

Der Staat gerät im Zusammenhang mit der Infiltration der Staatstrojaner in einen Interessenskonflikt. Bei der Variante des Fernzugriffs müssen Strafverfolgungsbehörden Schwachstellen bzw. Sicherheitslücken nutzen, die Softwarebetreiber entweder selbst eingepflegt oder aber noch nicht festgestellt haben, um darüber Zugriff auf das Zielsystem zu erhalten. Dieses Vorgehen birgt die Gefahr, dass auch andere Personen, wie beispielsweise Cyberkriminelle solche Wege ausnutzen. Der Staat kommt in den Konflikt, zum einen die Sicherheitslücken selbst nutzen zu wollen, zum anderen der Pflicht nachzugehen, diese über die Softwareanbieter schließen zu lassen, um eine Vielzahl von

[94] Vgl. Bratke, 2013, S. 483.
[95] Vgl. BVerfGE 7, 198, Leitsatz 1; Rn. 58.

Softwarenutzern vor heimlichen Angriffen zu schützen. Dem folgen aufgeworfene rechtliche und technische Bedenken hinsichtlich der Abgrenzung zwischen der Quellen-TKÜ und Online-Durchsuchung. Kritiker halten eine technische Abgrenzung beider Maßnahmen mit Blick auf die Staatstrojaner für unwahrscheinlich und sehen in der Quellen-TKÜ eine versteckte Online-Durchsuchung. Nach dieser Ansicht münde jede Quellen-TKÜ letztlich in einer Online-Durchsuchung.[96] Anschließend wird der beschleunigte Gesetzgebungsprozess dargestellt, der es ermöglicht hat, den Einsatz von Staatstrojanern binnen weniger Wochen vom Deutschen Bundestag zu verabschieden.

3.1. Verfassungsrecht – Durch die Quellen-TKÜ betroffene Grundrechte

Zunächst soll das Verfassungsrecht einen Überblick gewähren, in welche Grundrechte durch das heimliche staatliche Abhören von Telekommunikation mittels Spionagesoftware eingegriffen werden könnte. In Frage kommen das Fernmeldegeheimnis sowie das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, welche in Bezug auf informationstechnische Systeme eng nebeneinanderstehen. Beide Grundrechte werden miteinander verglichen und voneinander abgegrenzt. Ihnen folgt das Recht auf informationelle Selbstbestimmung und die Meinungsfreiheit. Nachdem das Bundesverfassungsgericht in seinen Urteilen der letzten Jahre wiederholt zum Ausdruck gebracht hat, dass heimlich durchgeführte staatliche Maßnahmen den unantastbaren Kernbereich privater Lebensgestaltung zu wahren haben[97], wird dieser in seinen Grundzügen betrachtet.

3.1.1. Das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG

Das Bundesverfassungsgericht (BVerfG) beschreibt die Quellen-TKÜ in seinem Urteil zu Online-Durchsuchungen 2008 als einen staatlichen Vorgang, bei dem ein komplexes informationstechnisches System zum Zweck der Telekommunikationsüberwachung technisch infiltriert wird.[98] Des Weiteren führt der Erste Senat dazu aus, dass sobald sich eine Ermächtigung auf eine staatliche Maßnahme beschränkt, durch welche die Inhalte und Umstände der laufenden Telekommunikation im Rechnernetz erhoben oder darauf bezogene Daten

[96] Vgl. Buermeyer, 2017, S. 9.
[97] Vgl. BVerfGE 6, 32, Rn. 15 ff.
[98] Vgl. BVerfG 120, 274, S. 21.

ausgewertet werden, ein Eingriff allein an Art. 10 Abs. 1 GG zu messen sei.[99] Der Schutzbereich dieses Grundrechts ist unabhängig davon betroffen, „ob die Maßnahme technisch auf der Übertragungsstrecke oder am Endgerät der Telekommunikation ansetzt.“[100]

Gemäß dieser Rechtsprechung soll in Bezug auf die Quellen-TKÜ der Schutzbereich des Fernmeldegeheimnisses vorgestellt werden. Nach Art. 10 Abs. 1 GG schützt das Fernmeldegeheimnis die unkörperliche Übermittlung von Informationen durch elektrische, elektromagnetische, optische, funktechnische, digitale oder analoge Signale an individuelle Empfänger vor staatlicher Kenntniserlangung.[101] Der Schutz des Art. 10 Abs. 1 GG erfasst Telekommunikation in Hinblick auf die Übermittlungsart, wie analoge und digitale Vermittlung sowie die Ausdrucksform, wie Bilder, Töne oder Zeichen.[102] Deshalb wird beim Art. 10 Abs. 1 GG auch vom Telekommunikationsgeheimnis gesprochen. Der Schutzbereich erstreckt sich ferner auf die Kommunikationsdienste des Internets.[103] Neben den Inhalten der Telekommunikation sind auch dessen Umstände, wie Verbindungsdaten und die Standortkennung vor einer staatlichen Kenntnisnahme geschützt.[104] Die Vielzahl der im Rahmen der modernen Telekommunikation erfassbaren Daten führe zu einer besonderen Intensität des mit der Überwachungsmaßnahme verbundenen Eingriffs in das Fernmeldegeheimnis.[105] In den Schutzbereich falle zudem die Erlangung der Kenntnis, „ob, wann, wie oft und zwischen welchen Personen Telekommunikation stattgefunden hat oder versucht worden ist.“[106] Das Fernmeldegeheimnis ziele darauf ab, dass die an dem Telekommunikationsverkehr beteiligten Personen ihre Meinungen und Informationen austauschen können ohne permanent damit rechnen zu müssen, dass der Staat sich heimlich in die Kommunikationsübertragung einschaltet.[107] Da das Fernmeldegeheimnis die Vertraulichkeit von

[99] Vgl. BVerfGE 120, 274, S. 1.
[100] BVerfGE 106, 28, Rn. 37.
[101] Vgl. BVerfGE 67, 157, Rn. 54 ff.; Liebig, 2015, S. 86.
[102] Vgl. BVerfGE 106, 28, Rn. 36.
[103] Vgl. BVerfGE 113, 348, Rn. 383.
[104] Vgl. BVerfGE 120, 274, S. 20.
[105] Vgl. BVerfGE 113, 348, S. 11.
[106] BVerfGE 113, 348, S. 10.
[107] Vgl. Liebig, 2015, S. 86 ff.; Epping, 2017, S. 346 ff.

Mitteilungen beim Kommunikationsvorgang schützt, gilt es in zeitlicher Hinsicht nur während des Kommunikationsvorgangs. Nur in dieser Zeit sind Teilnehmer des Kommunikationsvorgangs den Gefahren ausgesetzt, die sich aus der Verwundbarkeit des Kommunikationsvorgangs ergeben und vor denen das Fernmeldegeheimnis schützen soll.[108]

Nach dem modernen Verständnis handelt es sich bei einem Eingriff um „jedes staatliche Handeln, das dem Einzelnen ein Verhalten, das in den Schutzbereich eines Grundrechts fällt, ganz oder teilweise unmöglich macht, gleichgültig, ob diese Wirkung final oder unbeabsichtigt, unmittelbar oder mittelbar, rechtlich oder tatsächlich, mit oder ohne Befehl und Zwang erfolgt.“[109] Dabei muss die Beeinträchtigung von einem zurechenbaren Verhalten der öffentlichen Gewalt erkennbar sein.[110] Die Richter erläutern in dem Urteil zu Online-Durchsuchungen, dass bei einer Datenerhebung, die Aufschluss über die Kommunikation des Betroffenen mit Dritten gibt, der Bürger in seiner Möglichkeit beschränkt werde, an einer unbeobachteten Fernkommunikation teilzunehmen.[111] Hierdurch werde die Freiheit der Bürger mittelbar beeinträchtigt, da eine Furcht vor Überwachung eine unbefangene Individualkommunikation verhindern könne.[112] Ein Eingriff werde dadurch intensiver, dass die Betroffenen den Überwachungsmaßnahmen in einer Situation vermeintlicher Vertrautheit ausgesetzt werden.[113] Die staatliche Wahrnehmung von Inhalten der Telekommunikation sei immer dann am Art. 10 Abs. 1 GG zu messen, wenn eine staatliche Stelle eine Telekommunikationsbeziehung von außen überwacht, ohne dabei selbst Kommunikationsadressat und ohne durch Kommunikationsbeteiligte autorisiert zu sein.[114] Im Falle der beschriebenen Nichtautorisierung kann ein Eingriff in Art. 10 Abs. 1 GG bejaht werden. Als typischer Eingriff in das Fernmeldegeheimnis gilt das staatliche Überwachen der persönlichen Telekommunikation wie E-Mail, SMS, Telefax und Telefonie.[115] Sofern einer von mehreren Beteiligten der staatlichen Überwachung freiwillig zustimmt, gilt die

[108] Vgl. Epping, 2017, S. 348 ff.
[109] Bleckmann et al., 1988, S. 373.
[110] Vgl. Hermann, 2010, S. 134.
[111] Vgl. BVerfGE 115, 166, Rn. 118 ff.
[112] Vgl. BVerfGE 113, 348, Rn. 81.
[113] Vgl. BVerfGE 34, 238, Rn. 43 ff.
[114] Vgl. BVerfGE 120, 274, S. 40.
[115] Vgl. Epping, 2017, S. 348 ff.

staatliche Stelle als autorisiert. Ebenfalls liegt kein Eingriff in Art. 10 Abs. 1 GG vor, wenn ein Teilnehmer eines geschlossenen Chats einer staatlichen Stelle seinen Zugang freiwillig zur Verfügung stellt und eine Strafverfolgungsbehörde diesen nutzt.[116] Zusammenfassend halten die Richter in ihrem Urteil fest, dass Art. 10 Abs. 1 GG die freie Entfaltung der Persönlichkeit durch einen privaten, vor der Öffentlichkeit verborgenen Austausch von Kommunikation gewährleistet und damit zugleich die Würde des Menschen schützt.[117]

In Abgrenzung zu Online-Durchsuchungen weist der Erste Senat in seinem Urteil 2008 darauf hin, dass Art. 10 Abs. 1 GG nur dann als alleiniger grundrechtlicher Maßstab für den Zugriff auf Internettelefonie dienen könne, wenn sich die Überwachungsmaßnahme, genauer die Quellen-TKÜ, ausschließlich auf Daten aus einem laufenden Kommunikationsvorgang beschränke.[118] Die Beschränkung „muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein.“[119] Solange die Gefahr besteht, dass durch die Infiltration einer Spionagesoftware neben den Kommunikationsdaten weitere sensible Daten auf dem betroffenen informationstechnischen System erhoben werden können, biete das Fernmeldegeheimnis keinen ausreichenden Schutz.[120]

In dem Urteil aus dem Jahr 2016 – 1 BvR 966/09 – richteten sich die Verfassungsbeschwerden gegen die Regelungen des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG), die in einem Unterabschnitt durch das Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt eingefügt wurden. Die Beschwerde beinhaltete neben weiteren Ermittlungsbefugnissen sowohl § 20 k BKAG, in welchem es um die Zugriffe auf informationstechnische Systeme geht, als auch § 20 l BKAG, der zur Überwachung der laufenden Telekommunikation befugt. Beide Regelungen hielten die Richter mit den Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1, Art. 10 Abs. 1, Art. 13 Abs. 1 und 3, Art. 1 Abs. 1 und Art. 19 Abs. 4 GG nicht vereinbar und

[116] Vgl. BVerfGE 120, 274, S. 40.
[117] Vgl. BVerfGE 67, 157, Rn. 54.
[118] Vgl. BVerfGE 120, 274, S. 21 ff.
[119] BVerfGE 120, 274, S. 22.
[120] Vgl. BVerfGE 120, 274, S. 21.

entschieden über eine Neuregelung des Gesetzes, spätestens bis zum Juni 2018.[121]

Der Erste Senat des BVerfG wiederholt seine Ausführungen aus 2008, indem er festhält, dass sowohl die herkömmliche Telekommunikationsüberwachung, als auch die Quellen-TKÜ nach § 20 l BKAG an Art. 10 Abs. 1 GG zu messen seien. § 20 l Abs. 2 BKAG erlaube ausschließlich Überwachungen, die sich auf den laufenden Telekommunikationsvorgang beschränken. Die Vorschrift habe lediglich die Aufgabe, den technischen Entwicklungen der Informationstechnik zu folgen und ohne Zugriff auf weitere inhaltliche Information des informationstechnischen Systems eine Telekommunikationsüberwachung dort zu ermöglichen.[122] Sofern durch technische Maßnahmen sichergestellt sei, dass ausschließlich laufende Telekommunikation erfasst werde, seien die Vorschriften an dem Fernmeldegeheimnis aus Art. 10 Abs. 1 GG und nicht an dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG zu messen. Letzteres sei bei der Online-Durchsuchung betroffen.[123] Des Weiteren führen die Richter zur Quellen-TKÜ nach § 20 l Abs. 2 BKAG an, dass das Ob oder Wie sich durch technische Maßnahmen sicherstellen lasse, dass ausschließlich die laufende Telekommunikation überwacht und aufgezeichnet werde, die Anwendung der Norm, nicht jedoch ihre Gültigkeit betreffe. Das Gesetz lasse keinen Zweifel, dass die Quellen-TKÜ nur bei einer technisch sichergestellten Begrenzung der Überwachung auf die laufende Telekommunikation erlaubt sei. Maßgeblich hierfür sei, ob das Programm für die Durchführung einer Quellen-TKÜ so ausgestaltet ist, dass es Mitarbeiterinnen und Mitarbeitern des Bundeskriminalamts inhaltlich eine ausschließlich auf die laufenden Kommunikationsinhalte begrenzte Kenntnisnahme ermöglicht.[124] Sollten solche Anforderungen nicht erfüllbar sein, liefe diese Vorschrift leer. Dennoch mache sie dies nicht widersprüchlich und verfassungswidrig.[125] Gemäß dieses Urteils nicht mit der Verfassung zu vereinbaren, war die nicht näher eingeschränkte Erstreckung der Telekommunikationsüberwachung nach § 20 l Abs. 1 Nr. 2

[121] Vgl. 1 BvR 966/09, 1 BvR 1140/09, Urteil.
[122] Vgl. 1 BvR 966/09, 1 BvR 1140/09, Rn. 228.
[123] Vgl. 1 BvR 966/09, 1 BvR 1140/09, Rn. 228.
[124] Vgl. 1 BvR 966/09, 1 BvR 1140/09, Rn. 234.
[125] Vgl. 1 BvR 966/09, 1 BvR 1140/09, Rn. 234.

BKAG auf Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie terroristische Straftaten vorbereiten. Diese Vorschrift verstoße gegen den Bestimmtheitsgrundsatz und sei unverhältnismäßig weit gefasst. Da sich § 20 l Abs. 2 BKAG auf diese Vorschrift bezieht, könne hierfür nichts Anderes gelten.[126] Ausgenommen war in diesem Urteil die Regelung der Quellen-TKÜ für den Bereich der Strafverfolgung.[127]

3.1.2. Das „Computer-Grundrecht“ aus Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme („Computer Grundrecht“) leitete das BVerfG 2008 in seinem Urteil - 1 BvR 370, 595/07 - aus der Menschenwürde des Art. 1 Abs. 1 GG sowie dem allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1 GG ab.[128] Gegenstand der Verfassungsbeschwerden waren Vorschriften des Verfassungsschutzgesetzes Nordrhein-Westfalen (VSG NRW), welche verschiedene Datenerhebungen, insbesondere in Bezug auf informationstechnische Systeme beinhalteten. § 5 Abs. 2 Nr. 11 VSG NRW ermächtigte die Verfassungsschutzbehörde zu zwei Arten von Ermittlungsmaßnahmen: Zum einen zum heimlichen Beobachten und sonstigen Aufklären des Internets (Alt. 1), zum anderen zum heimlichen Zugriff auf informationstechnische Systeme (Alt. 2). Der Erste Senat erklärte § 5 Abs. 2 Nr. 11 VSG NRW mit Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, Art. 10 Abs. 1 GG und Art. 19 Abs. 1 S. 2 GG für unvereinbar und nichtig.[129] In den Leitsätzen zu dem Urteil hielten die Richter fest, dass die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können nur dann verfassungsrechtlich zulässig ist, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig seien Leib, Leben und Freiheit der Person, sowie Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder solche der Existenz der Menschen berührt.[130] Weiter führt das Gericht aus, dass eine staatliche Ermächtigung, die

[126] Vgl. 1 BvR 966/09, 1 BvR 1140/09, Rn. 232.
[127] Vgl. 1 BvR 966/09, 1 BvR 1140/09, Rn. 45.
[128] Vgl. BVerfGE 120, 274, S. 18.
[129] Vgl. BVerfGE 120, 274, S. 2.
[130] Vgl. BVerfGE 120, 274, S. 1.

darauf abzielt, die Inhalte und Umstände der laufenden Telekommunikation im Rechnernetz zu erheben oder darauf bezogene Daten auszuwerten, den Eingriff an Art. 10 Abs. 1 GG zu messen hat.[131]

Wegweisend ist der Leitsatz, aus dem hervorgeht, dass das allgemeine Persönlichkeitsrecht das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst.[132] Wie alle Grundrechte mit Ausnahme der Menschenwürde gelte dieses zwar nicht schrankenlos, das BVerfG gehe jedoch von einem außerordentlichen Gewicht aller Eingriffe in das „Computer-Grundrecht“ aus.[133] Hierzu führen die Richter näher aus, dass das allgemeine Persönlichkeitsrecht Elemente der Persönlichkeit gewährleiste, die nicht Gegenstand der besonderen Freiheitsgarantien des Grundgesetzes seien, diesen aber in ihrer konstituierenden Bedeutung für die Persönlichkeit nicht nachstehen.[134] Einer lückenschließenden Gewährleistung bedarf es insbesondere, um neuartigen Gefährdungen zu begegnen, zu denen es im Zuge gewandelter Lebensverhältnisse und wissenschaftlich-technischer Fortschritte kommen kann. So habe die Nutzung der Informationstechnik für die Persönlichkeit und Entfaltung des Einzelnen eine früher nicht absehbare Bedeutung erlangt. Die Informationstechnik eröffne dem Einzelnen neue Möglichkeiten, berge jedoch auch neuartige Gefahren für die Persönlichkeit in sich.[135] Informationstechnische Systeme seien mittlerweile allgegenwärtig. Ihre Nutzung sei für die Lebensführung vieler Bürger von zentraler Bedeutung. Dies werde darin deutlich, dass eine deutliche Mehrheit der Haushalte in der Bundesrepublik Deutschland über einen Personal Computer verfüge. Sowohl der Personal Computer mit seiner Leistungsfähigkeit, der Kapazität der eingebauten Arbeitsspeicher und damit verbundene Speichermedien werden stetig weiterentwickelt und steigen in ihrem Umfang an.[136] Personal Computer dienen unterschiedlichen Zwecken: Der Verwaltung und Archivierung der eigenen persönlichen und geschäftlichen Angelegenheiten, der digitalen Bibliothek und

[131] Vgl. BVerfGE 120, 274, S. 1.
[132] Vgl. BVerfGE 120, 274, S. 1.
[133] Vgl. Buermeyer, 2017, S. 7.
[134] Vgl. BVerfGE 99, 185, Rn. 51 ff.
[135] Vgl. BVerfGE 54, 148, Rn. 14 ff.
[136] Vgl. BVerfGE 120, 274, S. 18.

Unterhaltung.[137] Dementsprechend sei die Bedeutung von Personal Computern für die Persönlichkeitsentfaltung erheblich gestiegen.[138] Daneben beinhalten zahlreiche Gegenstände informationstechnische Komponenten, mit denen große Teile der Bevölkerung täglich umgehen, beispielsweise Telekommunikationsgeräte, Geräte in Wohnungen oder Kraftfahrzeugen.[139] Sowohl der Leistungsumfang als auch ihre Bedeutung für die Persönlichkeitsentfaltung nehmen noch zu, wenn solche Systeme miteinander vernetzt werden. Das werde zunehmend zum Normalfall, denn die Vernetzung informationstechnischer Systeme ermögliche es, Aufgaben auf die Systeme zu verteilen und insgesamt die Rechenleistung zu erhöhen.[140] Auch das Internet als komplexer Verbund von Rechnernetzen stelle dem Einzelnen zahlreiche neuartige Kommunikationsdienste zur Verfügung, die es z.B. ermöglichen, soziale Verbindungen aufzubauen und zu pflegen. Technische Konvergenzeffekte führen dazu, dass herkömmliche Formen der Fernkommunikation in weitem Umfang auf das Internet verlagert werden können.[141]

Neben den vorangegangenen Möglichkeiten für die Persönlichkeitsentfaltung gehen die Richter in ihrem Urteil auf damit verbundene Persönlichkeitsgefährdungen ein. So erzeugen informationstechnische Systeme im Rahmen des Datenverarbeitungsprozesses selbstständig weitere Daten, die neben den vom Nutzer gespeicherten Daten, in Hinblick auf seine Eigenschaften und sein Verhalten ausgewertet werden können. Aus dem Arbeitsspeicher und anderen Speichermedien gehen eine Vielzahl von Daten mit Bezug zu den persönlichen Verhältnissen, den sozialen Kontakten und den ausgeübten Tätigkeiten hervor.[142] Sofern diese Daten durch Dritte erhoben und ausgewertet werden, sei es ihnen möglich, weitreichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung zu ziehen.[143] Bei vernetzten Systemen werden diese Gefährdungen vertieft. Zum einen erhöhe sich die Anzahl der vorhandenen erzeugten und gespeicherten Daten, die ausgewertet werden

[137] Vgl. BVerfGE 120, 274, S. 18.
[138] BVerfGE 120, 274, S. 18.
[139] Vgl. BVerfGE 120, 274, S. 19.
[140] Vgl. BVerfGE 120, 274, S. 19.
[141] Vgl. BVerfGE 120, 274, S. 19.
[142] Vgl. BVerfGE 120, 274, S. 19.
[143] Vgl. BVerfGE 65, 1, Rn. 153.

können, zum anderen eröffne die Vernetzung von Systemen Dritten eine technische Zugriffsmöglichkeit, um Daten auszuspähen oder zu manipulieren. Der Einzelne könne solche Zugriffe teilweise gar nicht wahrnehmen bzw. solche nur begrenzt abwehren.[144] So könne ein technischer Selbstschutz durch das Verschlüsseln oder Verschleiern sensibler Daten, den durchschnittlichen Nutzer überfordern und einen hohen Aufwand, auch mit Funktionseinbußen des geschützten Systems, mit sich bringen. Der Selbstschutz werde überdies wirkungslos, sofern Dritten eine Infiltration einmal gelungen ist.[145]

Aus der Bedeutung der Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung und der Persönlichkeitsgefährdungen folgt ein grundrechtlich erhebliches Schutzbedürfnis. So sei der Einzelne nach Meinung des BVerfG darauf angewiesen, dass der Staat die Erwartungen an die Integrität und Vertraulichkeit derartiger Systeme achtet. Die grundrechtlichen Gewährleistungen der Art. 10 und Art. 13 GG sowie den entwickelten Ausprägungen des allgemeinen Persönlichkeitsrechts tragen dem durch die Entwicklung der Informationstechnik entstandenen Schutzbedürfnis nicht hinreichend Rechnung.[146] Hinsichtlich der Quellen-TKÜ machen die Richter in ihrem Urteil folgende Ausführungen: Der Art. 10 Abs. 1 GG schützt die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs, nicht aber die Vertraulichkeit und Integrität von informationstechnischen Systemen.[147] Soweit der heimliche Zugriff auf ein informationstechnisches System dazu dient, neben der laufenden Telekommunikation, Daten auch insoweit zu erheben, als Art. 10 Abs. 1 GG nicht vor einem Zugriff schützt, bleibt eine Schutzlücke vorhanden, die durch das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Schutz der Vertraulichkeit und Integrität von informationstechnischen Systemen geschlossen werde.[148] Der Erste Senat verdeutlicht, dass Art. 10 Abs. 1 GG der alleinige grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zu einer Quellen-TKÜ sei, sofern sich

[144] Vgl. BVerfGE 120, 274, S. 20.
[145] Vgl. BVerfGE 120, 274, S. 20.
[146] Vgl. BVerfGE 120, 274, S. 20.
[147] Vgl. BVerfGE 120, 274, S. 21.
[148] Vgl. BVerfGE 120, 274, S. 21.

die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt. Dies müsse durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein.[149]

Das Gericht geht in seinem Urteil zu Online-Durchsuchungen von einer veränderten grundrechtlichen Gefährdungslage aus und erkennt einen deutlich gesteigerten Schutzbedarf gegen staatliche Zugriffe auf informationstechnische Systeme.[150] Hierfür liefern die Richter zwei Anhaltspunkte: Der Staat kann sich erstens durch einen Online-Zugriff einen potentiell äußerst großen Datenbestand beschaffen, welcher zweitens höchstpersönliche und damit äußerst sensible Daten enthalten kann. Somit ginge es dem Gericht um den Schutz vor Ausforschung der Persönlichkeit des Betroffenen[151], insbesondere dem Schutz der Vertraulichkeit und Integrität. Der Nutzer rechne damit, dass seine Vertraulichkeitserwartung an das System und die darin enthaltenen Daten durch andere respektiert werde. Genau dieses Vertrauen soll durch die Entscheidung des BVerfG geschützt werden.[152] Diesem Punkt schließt sich die richterliche Entscheidung zum niedergelegten Schutz des Systems vor Manipulation oder Schäden an. In Folge eines Zugriffs auf den Rechner können beispielsweise Daten verändert werden oder verloren gehen. Der aufgestellte Integritätsschutz trägt dazu bei, die Rechte des Betroffenen zu wahren und dient darüber hinaus dem Schutz der Persönlichkeit und der Persönlichkeitsentwicklung.[153] Zusammenfassend bietet das „Computer-Grundrecht“ immer dann Schutz, „wenn die Eingriffsermächtigung Systeme erfasst, die allein oder in ihren technischen Voraussetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten.“[154] Das Grundrecht schützt das Interesse

[149] Vgl. BVerfGE 120, 274, S. 22.
[150] Vgl. Hermann, 2010, S. 114.
[151] Vgl. BVerfGE 120, 274, S. 24.
[152] Vgl. Hermann, 2010, S. 115.
[153] Vgl. Hermann, 2010, S. 115 ff.
[154] BVerfGE 120, 274, S. 24.

des Nutzers, dass die von einem vom Schutzbereich erfassten System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben.[155]

Ein Eingriff liegt dann vor, wenn die Integrität des geschützten informationstechnischen Systems angetastet wird, indem auf die Weise auf das System zugegriffen wird, dass dessen Funktionen, Leistungen und Speicherinhalte durch Dritte genutzt werden können.[156] Aus der Gesamtschau des Urteils ergibt sich, dass nur der heimliche Zugriff, nicht hingegen eine offene Durchsuchungsmaßnahme am Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gemessen werden soll.[157] Das BVerfG lässt das neue Grundrecht nur dann zur Anwendung kommen, wenn kein oder kein hinreichender Schutz durch andere Grundrechte, wie insbesondere durch Art. 10 Abs. 1, Art. 13 Abs. 1 GG und das Recht auf informationelle Selbstbestimmung gewährleistet ist.[158] Das „Computer-Grundrecht“ gelangt demnach subsidiär zur Anwendung, was bedeutet, dass bei einem Verhältnis von Vorschriften mit sich überschneidenden Anwendungsbereichen, das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme durch die vorrangige Regelung verdrängt wird.[159] Im Gegensatz zu Art. 10 Abs. 1 GG verfüge das „Computer-Grundrecht“ über den prozedural stärkeren Schutz in Form des grundsätzlichen Richtervorbehalts, der weder bei Art. 10 GG noch bei G 10 vorgesehen ist.[160] Sind bei einem Zugriff auf informationstechnische Systeme laufende Kommunikationsvorgänge betroffen, ist die Maßnahme aufgrund der Spezialitätsannahme weiterhin ausschließlich an Art. 10 Abs. 1 GG zu messen, obwohl die Überwachung eines Systems bei laufender Kommunikation im Ergebnis zu einem geringeren grundrechtlichen Schutz des Betroffenen führe.[161] Diese Betrachtung über-

[155] Vgl. Liebig, 2015, S. 141.
[156] Vgl. BVerfG NJW 2008, 822, 827, Rn. 204.
[157] Vgl. Liebig, 2015, S. 141.
[158] Vgl. Hermann, 2010, S. 110.
[159] Vgl. Hermann, 2010, S. 110.
[160] Vgl. Hermann, 2010, S. 110.
[161] Vgl. Hermann, 2010, S. 110.

sieht, dass bezüglich des Art. 10 Abs. 1 GG der Richtervorbehalt ungeschrieben über den Grundsatz der Verhältnismäßigkeit gilt. Somit ist der Grundrechtsschutz nicht geringer, was den Richtervorbehalt betrifft.[162]

3.1.3. Fernmeldegeheimnis vs. „Computer-Grundrecht“ bei der Quellen-TKÜ

Nachdem das Fernmeldegeheimnis sowie das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme vorgestellt wurden, soll eine mögliche Abgrenzungsmethode nach *Hermann* herangezogen werden, um die Grundrechte leichter zu unterscheiden. Ein Abgrenzungsproblem ergibt sich nicht, wenn offensichtlich nur eines der beiden Grundrechte tatbestandlich anwendbar ist, wie z.B. bei der Überwachung eines analogen Telefons. Hier liegt eindeutig kein Zugriff auf ein informationstechnisches System vor, so dass ausschließlich Art. 10 Abs. 1 GG Anwendung findet. Schwierigkeiten ergeben sich dann, wenn mit einem informationstechnischen System kommuniziert wird.[163] *Hermann* versucht aus dem BVerfG-Urteil 2008 eine fallgruppenorientierte Abgrenzung zu konstruieren. So werden vom Ersten Senat der E-Mail-Verkehr und die Sprachtelefonie der Telekommunikation zugeordnet. Gleiches sollte für die Videotelefonie und andere Formen der direkten Kommunikation, wie Chats gelten. Im Umkehrschluss sind die sonstige Überwachung der Nutzung bzw. der Inhalte eines Systems, sowie gespeicherte Verbindungsdaten eines zurückliegenden Kommunikationsvorgangs nicht als Eingriff in die Telekommunikationsfreiheit zu werten.[164] Wird außerhalb laufender Kommunikationsvorgänge auf Daten zugegriffen, muss zweifelsfrei das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme Anwendung finden. Werden unautorisiert die Daten eines laufenden Kommunikationsvorgangs auf dem technisch dafür vorgesehenen Weg erhoben, muss die Maßnahme an Art. 10 Abs. 1 GG gemessen werden.[165] Ein weiteres problematisches Feld tut sich auf, wenn Ermittler auf die laufende Kommunikation zugreifen und dazu einen technisch nicht vorgesehenen Weg wählen. Als Beispiele hierfür werden die Quellen-

[162] Vgl. Hermann, 2010, S. 111.
[163] Vgl. Hermann, 2010, S. 132.
[164] Vgl. Hermann, 2010, S. 132.
[165] Vgl. Hermann, 2010, S. 133.

TKÜ und Online-Überwachung angeführt. Beide Maßnahmen setzen die Infiltration des Zielsystems voraus, unterscheiden sich aber, da sie auf unterschiedliche Arten von Daten zugreifen. Da im Rahmen der Quellen-TKÜ ausschließlich auf Daten laufender Kommunikation zugegriffen werden soll, liegt hier vorerst nur ein Eingriff in das Fernmeldegeheimnis vor. Das „Computer-Grundrecht“ tritt hinter der spezielleren Gewährleistung des Art. 10 Abs. 1 GG zurück. Somit gelten für die Quellen-TKÜ geringere Eingriffsvoraussetzungen.[166] Da mit der Infiltration des Systems die entscheidende Hürde zur Ausspähung des gesamten Systems genommen ist, hat das Bundesverfassungsgericht 2008 deutlich gemacht, dass es den Schutzbereich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme dann nicht als Maßstab ansieht, wenn „durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt“[167] ist, dass ausschließlich Daten des laufenden Telekommunikationsvorgangs erhoben werden. In diesem Fall gilt der Schutzbereich des Fernmeldegeheimnisses als eröffnet.[168] Sofern der Nutzer, der zum Zwecke der Quellen-TKÜ eingesetzten Software, auch in der Lage ist, weitere Daten aus dem infiltrierten System einzusehen, zu übermitteln und zu verändern, muss neben dem Art. 10 Abs. 1 GG von der Eröffnung des Schutzbereiches des „Computer-Grundrechts“ ausgegangen werden.[169]

3.1.4. Der Kernbereichsschutz privater Lebensgestaltung

„Der verfassungsrechtliche Schutz des Kernbereichs privater Lebensgestaltung gewährleistet dem Individuum einen Bereich höchstpersönlicher Privatheit gegenüber Überwachung.“[170] Er schützt einen dem Staat nicht verfügbaren Menschenwürdekern und wurzelt in den von den jeweiligen Überwachungsmaßnahmen betroffenen Grundrechten, die in Verbindung mit Art. 1 Abs. 1 GG stehen.[171] Einen Eingriff in diesen absolut geschützten Bereich pri-

[166] Vgl. Hermann, 2010, S. 133.
[167] BVerfGE 120, 274, S. 22.
[168] Vgl. Liebig, 2015, S. 142.
[169] Vgl. Liebig, 2015, S. 142.
[170] 1 BvR 966/09, 1 BvR 1140/09, S. 3.
[171] Vgl. 1 BvR 966/09, 1 BvR 1140/09, S. 33.

vater Lebensgestaltung können selbst überragende Interessen der Allgemeinheit nicht rechtfertigen.[172] Zur Entfaltung der Persönlichkeit gehört die Möglichkeit, innere Vorgänge, wie Ansichten, Empfindungen und Gefühle höchstpersönlicher Art zum Ausdruck zu bringen. Somit schützt der Kernbereich privater Lebensgestaltung die nichtöffentliche Kommunikation mit Personen des höchstpersönlichen Vertrauens, die in der Annahme geführt wird, nicht überwacht zu werden. Ein Beispiel für eine solche Kommunikation sind Gespräche im Bereich der Wohnung. Zu den Personen zählt das BVerfG insbesondere Ehe- und Lebenspartner sowie Geschwister und Verwandte in gerader Linie. Ebenso können auch enge persönliche Freunde, Ärzte und Strafverteidiger solche Personen darstellen.[173] Der Schutz des Kernbereichs privater Lebensgestaltung ist strikt, weshalb die Verfassung für die Ausgestaltung der Überwachungsbefugnisse die Achtung des Kernbereichs als eine strikte Grenze sieht.[174] Dem Kernbereichsschutz soll auf zwei Ebenen bei der Durchführung von Überwachungsmaßnahmen Rechnung getragen werden: Der Erhebungs- und der Durchsichtebene.[175] Bei der Datenerhebung sollen Vorkehrungen getroffen werden, um eine unbeabsichtigte Miterfassung von Kernbereichsinformationen auszuschließen. Im Zuge der nachgelagerten Auswertung und Verwertung sollen die Folgen eines nicht vermiedenen Eindringens in den Kernbereich privater Lebensgestaltung minimiert werden.[176] „Zentrales Element des vom BVerfG aufgestellten zweistufen Schutzkonzepts ist die möglichst wenig eingriffsintensive Sichtung der erlangten Daten.“[177] Das Gericht verdeutlicht mit dem Hinweis auf diesen verfassungsrechtlichen Schutz, dass eine gesetzliche Ermächtigung zu einer Überwachungsmaßnahme, die den Kernbereich privater Lebensgestaltung berühren kann, sicherstellen soll, dass Daten mit Kernbereichsbezug nicht erhoben werden.[178] In jedem Fall ist der Abbruch der Maßnahme vorzusehen, wenn erkennbar ist, dass eine Überwachung in den Kernbereich privater Lebensgestaltung eindringt.[179] Ist es, wie

[172] Vgl. BVerfGE 109, 279, Rn. 278 ff.
[173] Vgl. BVerfGE 109, 279, Rn. 278 ff.
[174] Vgl. 1 BvR 966/09, 1 BvR 1140/09, S. 34.
[175] Vgl. Hermann, 2010, S. 79.
[176] Vgl. BVerfGE 120, 274, S. 38 ff.
[177] Hermann, 2010, S. 80.
[178] Vgl. BVerfGE 120, 274, S. 37.
[179] Vgl. 1 BvR 966/09, 1 BvR 1140/09, S. 35.

bei der Quellen-TKÜ, praktisch unvermeidbar Informationen zu erlangen, bevor ihr Kernbereichsbezug bewertet werden kann, „muss für hinreichenden Schutz in der Auswertungsphase gesorgt sein.“[180] Daten, die dem Kernbereich zugeordnet werden können, sind unverzüglich zu löschen. Eine Verwertung dieser Daten ist ausgeschlossen.[181]

3.1.5. Das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG und die Meinungsfreiheit aus Art 5. Abs. 1 GG

Ebenfalls könnten in Bezug auf die Quellen-TKÜ das Recht auf informationelle Selbstbestimmung (RIS) nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG sowie die Meinungsfreiheit aus Art. 5 Abs. 1 GG Anwendung finden. Beide werden nachfolgend vorgestellt. Das Recht auf informationelle Selbstbestimmung gewährt dem Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[182] Durch jede Erhebung, Kenntnisnahme, Speicherung und Verwendung geschützter Daten gilt der Schutzbereich des Rechts auf informationelle Selbstbestimmung als eröffnet. Ein Eingriff in das Grundrecht liegt durch diese Maßnahmen vor.[183] Bei einer heimlichen Ermittlungsmaßnahme, wie der Quellen-TKÜ ist das RIS ebenfalls berührt, da der Betroffene zunächst keine Kenntnis darüber hat, dass er abgehört wird und dadurch nicht über die Preisgabe und Verwendung seiner persönlichen Daten entscheiden kann. Der Erste Senat erklärt in seinem Urteil aus dem Jahr 2005 – 1 BvR 668/04 -, in dem es um die vorbeugende Telekommunikationsüberwachung geht, dass das Recht auf informationelle Selbstbestimmung hinter der spezielleren Gewährleistung aus Art. 10 Abs. 1 GG zurücktritt, soweit sich die Schutzbereiche überschneiden.[184] „Gleiches gilt für die Gewährleistung der freien Meinungsäußerung aus Art. 5 Abs. 1 GG, soweit der Eingriff in der staatlichen Wahrnehmung und gegebenenfalls Verarbeitung der mit Mitteln der Telekommunikation geäußerten Meinungen liegt.“[185] Art. 5 Abs. 1 GG gewährleistet das Äußern sowie das Verbreiten einer Meinung in Wort,

[180] BVerfGE 120, 274, S. 37.
[181] Vgl. BverfGE 120, 274, S. 37.
[182] Vgl. BVerfGE 65, 1, Rn. 152.
[183] Vgl. Liebig, 2015, S. 11.
[184] Vgl. BVerfGE 113, 348, S. 10.
[185] BVerfGE 113, 348, S. 10.

Schrift und Bild. Diese drei Begriffe sind dabei weit auszulegen. Jede Form der Meinungskundgabe, soweit sie sich auf eine geistige Auseinandersetzung beschränkt, ist von diesem Grundrecht geschützt. Dem Schutzbereich der Meinungsfreiheit sind exemplarisch das gesprochene und gesungene Wort, Aufkleber, Plaketten und Tonträger zuzuordnen.[186]

3.1.6. Zusammenfassung der betroffenen Grundrechte

Nachdem die vier Grundrechte mit ihren jeweiligen Schutzbereichen vorgestellt wurden, um zu prüfen, welches Grundrecht in Hinblick auf die Quellen-TKÜ zur Anwendung kommt, soll das BVerfG erneut zitiert werden. Es hält in einem Urteil fest, dass das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG bei der Quellen-TKÜ das spezielle Grundrecht darstellt und sein Schutzbereich als eröffnet gilt, wenn „durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt“[187] ist, dass ausschließlich Daten des laufenden Telekommunikationsvorgangs erhoben werden. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, das Recht auf informationelle Selbstbestimmung und die Meinungsfreiheit sind ebenfalls einschlägig, treten aber neben dem speziellen Fernmeldegeheimnis zurück.

3.2. Vorstellung des § 100 a StPO nach der Reform der Strafprozessordnung - Ein Vergleich mit der vorherigen Norm

Durch eine Reform der Strafprozessordnung wurde die Quellen-TKÜ 2017 bundesweit für den Bereich der Strafverfolgung geregelt. Hierzu ergänzte der Gesetzgeber den bereits bestehenden § 100 a StPO, der bislang die herkömmliche Telekommunikationsüberwachung erlaubte. Diese findet ihre Grundlage in § 100 a Abs. 1 S. 1 StPO, während die tatbestandlichen Anforderungen an eine Telekommunikationsüberwachung in § 100 a Abs. 1 S. 1 Nr. 1 bis 3 StPO aufgeführt werden. Dieser Satz blieb unverändert. § 100 a Abs. 1 S. 2 bis 3 StPO beziehen sich auf die neu aufgenommene Quellen-TKÜ. In § 100 a Abs. 1 S. 2 StPO heißt es, „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

[186] Vgl. Epping, 2017, S. 104 ff.
[187] BVerfGE 120, 274, S. 22.

insbesondere in unverschlüsselter Form zu ermöglichen.“ Des Weiteren dürfen nach § 100 a Abs. 1 S. 3 StPO auf dem informationstechnischen System des Betroffenen gespeicherte Inhalte und Umstände der Kommunikation überwacht und aufgezeichnet werden, „wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können.“ Dieser dritte Satz betrifft vor allem die verschlüsselte Kommunikation über Messenger-Dienste wie *WhatsApp*.[188]

3.2.1. Tatverdacht und Straftatenkatalog

In § 100 a Abs. 1 Nr. 1 StPO wird der erforderliche Tatverdacht festgelegt, welcher einer durch bestimmte Tatsachen erhärteten Verdachtslage bedarf.[189] Hierbei ist weder ein dringender Tatverdacht i.S.d. § 112 StPO noch ein hinreichender Tatverdacht i.S.d. § 203 StPO gefordert. Vielmehr genügt ein einfacher Tatverdacht, der sich jedoch auf bestimmte Tatsachen stützen lässt[190], die den Verdacht einer Katalogstraftat nach § 100 a Abs. 2 StPO begründen und ein gewisses Maß an Konkretisierung erreicht haben. Dabei können auch kriminalistische Erfahrungen Berücksichtigung finden.[191] Dem Verhältnismäßigkeitsgrundsatz trägt der Gesetzgeber u.a. mit dem in § 100 a Abs. 2 StPO festgehaltenen Katalog von schweren Straftaten Rechnung. Es handelt sich um solche, die zwischen besonders schweren Straftaten i.S.d. Art. 13 Abs. 3 GG und Straftaten von erheblicher Bedeutung i.S.d. § 110 a Abs. 1 S. 1 StPO angesiedelt sind.[192] Es werden auch Fälle mittlerer Kriminalität aufgeführt, die sich auf Eigentums-, Vermögens- und wirtschaftsstrafrechtliche Delikte mit erhöhtem Strafrahmen beziehen, zumeist in gewerbs- und bandenmäßigen Begehungsformen.[193] Die Tat muss jedoch nach § 100 a Abs. 1 S. 1 Nr. 2 StPO im Einzelfall schwer wiegen. Es sollen die Fälle ausgeschlossen werden, die zwar eine Katalogtat darstellen, aber mangels hinreichender Schwere den mit

[188] Vgl. O.V., StPO-Reform 2017: Änderungen im Ermittlungsverfahren, 2017.
[189] Vgl. Keller et al., 2015, S. 28.
[190] Vgl. OLG Hamm, 2 Ss 906/02, Rn. 10.
[191] Vgl. Keller et al., 2015, S. 28.
[192] Vgl. Keller et al., 2015, S. 28.
[193] Vgl. Keller et al., 2015, S. 28.

einer TKÜ verbundenen Eingriff in das Fernmeldegeheimnis nicht zu rechtfertigen vermögen.[194] Zwischen der herkömmlichen und der Quellen-TKÜ werden im § 100 a Abs. 2 StPO keine Unterschiede gemacht. Beide Abhörmaßnahmen können bei Ermittlungen u.a. wegen Mordes und Totschlags, bei Geld- und Wertzeichenfälschung oder gewerbsmäßiger Hehlerei durchgeführt werden. § 100 a Abs. 1 S. 1 Nr. 3 StPO fordert zudem, dass die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise, als die Telekommunikationsüberwachung, wesentlich erschwert oder aussichtslos wäre.

3.2.2. Adressaten

§ 100 a Abs. 3 StPO bestimmt, gegen welche Adressaten sich die Telekommunikationsüberwachung richten darf. Die Maßnahme kann sich gegen den Beschuldigten, dessen Identität noch nicht feststehen muss sowie gegen Nichtverdächtige richten.[195] Bei Nichtverdächtigen spricht der Gesetzestext von „Personen, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss oder ihr informationstechnisches System benutzt.“ Hier fügte der Gesetzgeber den Passus „oder ihr informationstechnisches System benutzt“ hinzu. Mit der Alternative „dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben“ ist der sogenannte Nachrichtenmittler gemeint.

3.2.3. Anordnungskompetenz und Kernbereichsschutz

Die Anordnungskompetenz für eine Telekommunikationsüberwachung war vor der Reform in § 100 b Abs. 1 S. 1 StPO und ist nunmehr in § 100 e Abs. 1 StPO geregelt. Heimliche Abhörmaßnahmen i.S.d. Telekommunikationsüberwachung dürfen nach § 100 e Abs. 1 S. 1 StPO nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden. Hierbei ist das Gericht am Sitz der Staatsanwaltschaft zuständig. Bei Gefahr im Verzug kann die Anordnung auch nach § 100 e Abs. 1 S. 2 StPO durch die Staatsanwaltschaft ge-

[194] Vgl. Keller et al., 2015, S. 28.
[195] Vgl. Keller et al., 2015, S. 29.

troffen werden. Diese muss nach § 100 e Abs. 1 S. 3 StPO binnen drei Werktagen von dem Gericht bestätigt werden, anderenfalls tritt sie außer Kraft. Gefahr im Verzug liegt vor, „wenn der Erfolg der Maßnahme durch die Verzögerung, die die Erwirkung der richterlichen Entscheidung mit sich bringen würde, gefährdet wäre.“[196] Eine Eilzuständigkeit der Polizei besteht nicht.[197]

Den bereits vorgestellten Schutz des Kernbereichs privater Lebensgestaltung hat der Gesetzgeber aus dem ehemaligen § 100 a Abs. 4 StPO in den jetzigen § 100 d Abs. 1 und 2 StPO transferiert. Nach § 100 d Abs. 1 StPO darf eine Telekommunikationsüberwachung nicht angeordnet werden bzw. gilt als unzulässig, wenn zu prognostizieren ist, dass durch die Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung zu erwarten sind. § 100 d Abs. 2 StPO legt für die Fälle der Erlangung von Erkenntnissen aus dem Kernbereichsschutz i.S.d. § 100 a StPO fest, dass diese nicht verwertet werden dürfen. Aufzeichnungen über solche Erkenntnisse sind nach § 100 d Abs. 2 S. 2 StPO unverzüglich zu löschen. Die Tatsache über die Erlangung und Löschung sind nach § 100 d Abs. 2 S. 3 StPO zu dokumentieren.

3.2.4. Technische Sicherstellung und Protokollierung

In § 100 a Abs. 5 S. 1 Nr. 1 a StPO wurde die Rechtsprechung des BVerfG aus seinem Urteil aus 2016 zum Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten berücksichtigt, dass bei Durchführung einer Quellen-TKÜ durch technische Maßnahmen sichergestellt sein muss, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird. Eine Alternative bietet § 100 a Abs. 5 S. 1 Nr. 1 b StPO. Hiernach können auch Inhalte und Umstände der Kommunikation herangezogen werden, die ab dem Zeitpunkt der Anordnung nach § 100 e Abs. 1 StPO auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz hätten überwacht und aufgezeichnet werden können. Der Gesetzgeber hält nach § 100 a Abs. 5 S. 1 Nr. 2 StPO nur Veränderungen an dem informationstechnischen System, beispielsweise eines Mobiltelefons für zulässig, die für die Datenerhebung unerlässlich sind. Diese vorgenommenen Veränderungen sind bei Beendigung

[196] BVerfG, 2 BvR 1444/00, Rn. 34.
[197] Vgl. Keller et al., 2015, S. 31.

der Maßnahme, soweit technisch möglich, nach § 100 a Abs. 5 S. 1 Nr. 3 StPO automatisiert rückgängig zu machen. Nach § 100 a Abs. 5 S. 2 und 3 StPO sind das eingesetzte Mittel sowie kopierte Daten nach dem Stand der Technik gegen Veränderung, unbefugte Nutzung, Löschung und Kenntnisnahme zu schützen.

Zu jeder Quellen-TKÜ sind, so legt der Gesetzgeber in § 100 a Abs. 6 StPO fest, die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes (Nr. 1), die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen (Nr. 2), die Angaben, die die Feststellung der erhobenen Daten ermöglichen (Nr. 3) sowie die Organisationseinheit, die die Maßnahme durchführt zu protokollieren.

3.2.5. Kritische Stellungnahmen zu dem reformierten § 100 a StPO

An dieser Stelle soll ein Exkurs einige kritische Stellungnahmen zu dem reformierten § 100 a StPO darstellen, insbesondere zu den Änderungen, die die Regelungen zur Quellen-TKÜ betreffen. *Buermeyer* bemängelt, dass der § 100 a Abs. 1 S. 3 StPO die Vorgaben aus der Entscheidung des BVerfG zu Online-Durchsuchungen verfehle, in der es heißt, dass nur laufende Kommunikation erhoben werden darf. § 100 a Abs. 1 S. 3 StPO erlaube über die laufende Kommunikation hinaus die Erhebung gespeicherter Inhalte und die Umstände der Kommunikation unter den erleichterten Voraussetzungen der Quellen-TKÜ. Dies würde in einem offenen Widerspruch zu den Vorgaben des BVerfG stehen, welches lediglich die Erhebung laufender und nicht früherer Kommunikation benannte.[198] Würden anhand der Zeitangaben einer gespeicherten Nachricht Inhalte ausgelesen werden, die vor Beginn der Maßnahme gespeichert wurden, würde statt einer Quellen-TKÜ eine Online-Durchsuchung durchgeführt werden, die die Eingriffstiefe deutlich erhöhe.[199] Dieser rechtlichen Auffassung schließen sich auch Reporter ohne Grenzen an. Der § 100 a Abs. 1 S. 2 und 3 StPO gehe über eine klassische Telekommunikationsüberwachung hinaus, weil auch auf gespeicherte Inhalte zugegriffen werden

[198] Vgl. Buermeyer, 2017, S. 15 ff.
[199] Vgl. Buermeyer, 2017, S. 17.

soll. Die Maßnahme sei deshalb am Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme zu messen.[200] Gemäß des Urteils des BVerfG 2008 sei das „Computer-Grundrecht“ nur dann nicht maßgeblich für eine Quellen-TKÜ, wenn ausschließlich „laufende Kommunikation“ erfasst wird. Darüber setze sich die Gesetzesformulierung jedoch hinweg, da eine Quellen-TKÜ hiernach auch „gespeicherte Inhalte und Umstände der Kommunikation“ erfassen können soll. Hiermit sehen die Reporter genau wie *Buermeyer* die Grenze zur Online-Durchsuchung überschritten.[201] Nach Haltung des CCC kann die Tatsache, dass bei einer Quellen-TKÜ ausschließlich Art. 10 Abs. 1 GG beeinträchtigt sein soll, insgesamt nicht überzeugen, da mit einer solchen Maßnahme immer auch die Integrität des Zielsystems verletzt werde. Entsprechend werde bei Betroffenen einer Quellen-TKÜ in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme eingegriffen.[202] Des Weiteren stellen einzelne Mitglieder des CCC zur Diskussion, ob bei einem Einsatz einer Spionagesoftware im Zusammenhang mit einer Quellen-TKÜ überhaupt von einer Telekommunikationsüberwachung im eigentlichen Sinne gesprochen werden kann. Die Telekommunikation beginnt laut Auslegung erst in dem Moment des Aussendens einer Mitteilung.[203] Da die Quellen-TKÜ jedoch davor ansetzen und aufzeichnen soll, nämlich beim Erstellen einer Nachricht, würde es sich bei dieser Form des Aufzeichnens nicht um eine Telekommunikationsüberwachung handeln, weil sie gerade vor oder nach, aber nicht während der Telekommunikation stattfindet.[204] Somit seien festgehaltene Gedanken und Notizen eines Betroffenen, die sein informationstechnisches System nicht verlassen, aber von dem Staatstrojaner aufgezeichnet werden, keine Kommunikation. Für die Quellen-TKÜ dürfe der Datenzugriff nur auf dem Transportweg erfolgen, anderenfalls handele es sich um eine Online-Durchsuchung, die rechtlich anders zu behandeln sei.[205]

[200] Vgl. O.V., Stellungnahme zur Einführung der Quellen-TKÜ und Online-Durchsuchung, 2017, S. 4.
[201] Vgl. O.V., Stellungnahme zur Einführung der Quellen-TKÜ und Online-Durchsuchung, 2017, S. 5.
[202] Vgl. Kurz et al., 2017, S. 7.
[203] Vgl. Kurz et al., 2017, S. 7.
[204] Vgl. Kurz et al., 2017, S. 8.
[205] Vgl. Kurz et al., 2017, S. 8.

Singelnstein hält die Adressatenregelung im § 100 a Abs. 3 StPO für problematisch. Er betont, dass Tatsachen bzw. Anhaltspunkte keine sehr hohe Grenze bilden und somit im Alltag auch Geräte von Personen angegriffen werden, die eben nicht Beschuldigte im jeweiligen Strafverfahren sind.[206] Auch zu den Regelungen, die den Kernbereichsschutz privater Lebensgestaltung betreffen, macht der Kriminologe deutlich, dass diese den von dem Bundesverfassungsgericht festgelegten Maßstab für den Großen Lauschangriff deutlich absenke. Es sei praktisch nie der Fall, dass eine Maßnahme nach § 100 d Abs. 1 StPO zu unterbleiben hat, weil allein Informationen aus dem Kernbereich erlangt würden. Weder habe man auf dem Computer nur Informationen aus dem persönlichen Kernbereich gespeichert noch werde am Telefon oder in der Wohnung nur über die Intimsphäre gesprochen.[207] Der CCC verweist zu diesem Thema auf den § 20 l Abs. 6 Satz 1 BKAG, in dem der Trojanereinsatz ebenfalls mit dieser Regelung vorhanden war.[208] Der Satz sei gemäß des Urteils des BVerfG 2016 so zu interpretieren, „dass eine Kommunikation über Höchstvertrauliches nicht schon deshalb aus dem strikt zu schützenden Kernbereich herausfällt, weil sich in ihr höchstvertrauliche mit alltäglichen Informationen vermischen.“[209]

Hinsichtlich der Sicherstellung und Protokollierung fasst *Buermeyer* zusammen, dass die Eingriffsbefugnis aus § 100 a Abs. 5 StPO zwar bestimmte an der Rechtsprechung des BVerfG orientierte Begrenzungen des Eingreifens enthalte, nämlich eine Beschränkung von Veränderungen auf das Notwendige, diese Regelungen im Gesetz jedoch keine verfahrensrechtliche Absicherung finden. Im Vergleich zu den Anforderungen an die Maßnahmenanordnung und ihre Begründung nach § 100 e Abs. 3 und 4 StPO müsse das technische Mittel, somit der eingesetzte Staatstrojaner, weder benannt noch in seinen technischen Spezifikationen näher bezeichnet werden. Der Richter hält diese Gesetzesformulierung angesichts der Eingriffstiefe sowie der Gefahren einer schleichenden Ausweitung einer Quellen-TKÜ hin zu einer Online-

[206] Vgl. Kurz, Interview über Staatstrojaner: Der intensivste Grundrechtseingriff in der Strafprozessordnung, 2017.
[207] Vgl. Kurz, Interview über Staatstrojaner: Der intensivste Grundrechtseingriff in der Strafprozessordnung, 2017.
[208] Vgl. Kurz et al., 2017, S. 5.
[209] BvR 966/09, Rn. 222.

Durchsuchung für unangemessen. Einer Ausweitung könne nur durch die Gestaltung und Nennung des Staatstrojaners entgegengewirkt werden.[210] „Zudem sollte ausschließlich der Einsatz erfolgreich geprüfter Staatstrojaner zulässig sein.“[211]

3.3. Staatliche Interessenskonflikte bei der Ausnutzung von Sicherheitslücken

Wie die bereits genannten unterschiedlichen Möglichkeiten der Infiltration zeigen, fällt auch die rechtliche Bewertung der Zugriffe unterschiedlich aus. Das Betreten von Räumlichkeiten zur Infektion von Systemen erscheint im Hinblick auf Art. 13 Abs. 1 GG ohne eine spezifische Ermächtigungsgrundlage rechtswidrig. Das Aufspielen bei einer Personen- und Grenzkontrolle wäre als solches unbedenklich, ebenso das Zusenden einer E-Mail mit einem getarnten Staatstrojaner im Anhang, soweit dieser keine Sicherheitslücken ausnutzt. Die zuletzt genannten Varianten können unter dem Begriff der kriminalistischen List verstanden werden.[212] Dennoch führe die Infektion eines Zielsystems durch Ausnutzen von Sicherheitslücken zu gravierenden Fehlanreizen, mahnt *Buermeyer*. In den letzten Jahren sei international eine verstärkte Verbreitung kommerziell angebotener staatlicher Überwachungstrojaner zu verzeichnen. Das staatliche Ausnutzen von Software-Schwachstellen stellt einen Interessenkonflikt dar.[213] Dieser besteht darin, dass aus wirtschaftlichen und Gemeinwohlerwägungen heraus ein hohes Interesse daran besteht, Software-Sicherheitslücken schnell zu schließen, um Märkte, in denen mit Sicherheitslücken gehandelt wird, nicht zu bestärken sowie Wirtschaftsspionage zurückzudrängen.[214] Wenn Bundesbehörden solche Schwachstellen ausnutzen dürfen, um diese Staatstrojaner einsetzen zu können, so hat der Staat ein Interesse daran, ein Arsenal von Sicherheitslücken aufzubauen, um in der konkreten Fallkonstellation eine Zielperson angreifen zu können.[215] Dieses Interesse wird ihn davon abhalten, gefundene oder gekaufte Sicherheitslücken den jeweiligen Herstellern der IT-Systeme mitzuteilen, damit die Lücken geschlossen

[210] Vgl. Buermeyer, 2017, S. 18.
[211] Buermeyer, 2017, S. 20.
[212] Vgl. Buermeyer, 2017, S. 21.
[213] Vgl. Kurz et al., 2016, S. 15.
[214] Vgl. Kurz et al., 2016, S. 15.
[215] Vgl. Buermeyer, 2017, S. 21.

werden können. So entstehen Anreize für Strafverfolgungsbehörden, ihnen bekannte Sicherheitslücken zu horten, anstelle sie schließen zu lassen.[216] Solange die Schwachstellen nicht von den Herstellern der Systeme geschlossen werden, weil sie von ihnen keine Kenntnis erlangen, können nicht nur Ermittlungsbehörden diese Sicherheitslücken für den Einsatz von Staatstrojanern ausnutzen. Vielmehr kann jede Person, die die Schwachstellen findet oder auf dem Schwarzmarkt kauft, diese zur Infiltration informationstechnischer Systeme missbrauchen. Zu denken wäre beispielsweise an Cyber-Kriminelle, die darauf abzielen, betroffene Systeme zum Teil eines Botnetzes zu machen oder Zahlungsdaten für Online-Überweisungen abzugreifen.[217] Ein Botnetz ist aus technischer Sicht ein Zusammenschluss automatisierter Computerschadprogramme. Die Rechner werden mit einer Malware des Typs Backdoor infiziert und darüber als Bot in das Botnetz eingebunden.[218] Durch diesen staatlichen Konflikt, ob Sicherheitslücken erkannt und genutzt oder weitergeleitet und geschlossen werden, würden Bundesbehörden viele Millionen Nutzer von IT-Systemen weltweit, die von einer entsprechenden Schwachstelle betroffen sind, einem fortbestehendem Risiko von Cyber-Angriffen aussetzen. Dieses Missbrauchsrisiko, das durch das Horten von Sicherheitslücken eingegangen wird, steht nach Ansicht *Buermeyers* in keinem ausgewogenen Verhältnis zu dem verfolgten Zweck, der nämlich bessere Strafverfolgung im Einzelfall bedeutet.[219]

3.4. Rechtliche und technische Bedenken bei der Abgrenzung zwischen der Quellen-TKÜ und der Online-Durchsuchung

Die Online-Durchsuchung findet ihre bundesweite Regelung in § 100 b StPO und schließt sich der Quellen-TKÜ in der Strafprozessordnung nahtlos an. Hiernach darf unter den Voraussetzungen des § 100 b Abs. 1 Nr. 1 bis 3 StPO auch ohne Wissen des Betroffenen mit technischen Mitteln in ein von dem Betroffenen genutztes informationstechnisches System eingegriffen und daraus Daten erhoben werden. Der Katalog der besonders schweren Straftaten i.S.d. § 100 b Abs. 1 Nr. 1 StPO ist in § 100 b Abs. 2 StPO aufgeführt. Dieser

[216] Vgl. Buermeyer, 2017, S. 21.
[217] Vgl. Buermeyer, 2017, S. 22.
[218] Vgl. O.V., Was ist ein Botnet und wie funktioniert es?, 2018.
[219] Vgl. Buermeyer, 2017, S. 22.

überschreite nach *Buermeyer* den Rahmen des verfassungsrechtlich Möglichen.[220] Der Katalog enthalte Straftatbestände, die Rechtsgüter schützen, für die das BVerfG selbst eine präventive Online-Durchsuchung nicht für zulässig hält. Die präventive Online-Durchsuchung dürfe also nicht einmal zur Abwehr einer konkret drohenden Gefahr für ein Rechtsgut eingesetzt werden, sondern ausschließlich im Zusammenhang mit überragend wichtigen Rechtsgütern.[221] Wie bei der Quellen-TKÜ darf sich diese strafprozessuale Maßnahme gegen den Beschuldigten und andere Personen gemäß § 100 b Abs. 3 StPO richten. Die Online-Durchsuchung umfasse all jene Eingriffe, die bisher bereits nach § 100 c StPO als akustische Wohnraumüberwachung/großer Lauschangriff zulässig waren und fügt noch weitere erhebliche Eingriffe hinzu: Die Auswertung der gesamten laufenden und früheren Kommunikation, die Auswertung aller digital gespeicherten Inhalte auf den infizierten Systemen sowie ein Spähangriff auf die Umgebung des überwachten Systems, sofern es über eine Kamerafunktion verfügt.[222] Hinzu kommt bei der Maßnahme die Möglichkeit des Live-Zugriffs. Hierbei könnten Ermittler den Betroffenen virtuell heimlich über die Schulter blicken. Ein Zugriff auf einen derart umfassenden Datenbestand ist mit dem Risiko verbunden, dass die Daten in der Gesamtschau Rückschlüsse auf die Persönlichkeit des Betroffenen ermöglichen, bis hin zu einer Bildung von Kommunikations- und Verhaltensprofilen.[223]

Funktional ist die Quellen-TKÜ von einer Online-Durchsuchung nur in Hinsicht auf die nach der Infiltration auszuführenden Befehle abzugrenzen. Die Datenzugriffe auf das jeweilige informationstechnische System und das anschließende Ermitteln der auf dem Gerät installierten Software sind Bestandteil einer heimlichen Ermittlungsmethode, die das Platzieren von Spionagesoftware auf ein System zum Ziel hat.[224] Der CCC und Weitere führen aus, dass die Beschränkung der Trojaner-Funktionen auf die laufenden Telekommunikationsinhaltsdaten zuverlässig und technisch beweisbar umzusetzen, praktisch kaum möglich ist. Denn Zielpersonen können mit der Spionagesoftware auf

[220] Vgl. Buermeyer, 2017, S. 12.
[221] Vgl. Buermeyer, 2017, S. 12.
[222] Vgl. Buermeyer, 2017, S. 4.
[223] Vgl. Buermeyer, 2017, S. 5.
[224] Vgl. Kurz et al., 2017, S. 5.

eine Vielzahl von Kommunikationskanälen zugreifen, auf E-Mails, Direktnachrichten in sozialen Netzwerken, Instant Messenger, Audio Dienste und Weitere. Für jede dieser Kommunikationsmöglichkeiten müssten spezifische Lösungen entwickelt und an das jeweilige System des Betroffenen angepasst werden.[225] Auch IT-Sicherheits-Experten sind sich darin einig, „dass die Anforderungen an eine Quellen-TKÜ technisch nicht zu erfüllen sind."[226] *Buermeyer* betont die besondere Gefährlichkeit einer Quellen-TKÜ, die stets Gefahr läuft, bei einer Fehlfunktion der eingesetzten Spionagesoftware oder bewusst pflichtwidrigem oder fahrlässigem Handeln des bedienenden Personals in eine vollumfängliche Online-Durchsuchung abzugleiten.[227]

3.5. Beschleunigter Gesetzgebungsprozess des § 100 a StPO

Im Gegensatz zu einem herkömmlichen Gesetzgebungsverfahren wurde die Gesetzesänderung des § 100 a StPO durch den Rechtsausschuss des Deutschen Bundestages an ein schon laufendes Gesetzgebungsverfahren angehangen, bei dem es u.a. um den Führerschein-Entzug bei Nicht-Verkehrsstraftaten ging.[228] Hierdurch wurde der Gesetzgebungsprozess, der die neuen heimlichen Ermittlungsmaßnahmen nach §§ 100 a und b StPO regeln soll, zum Ende der Legislaturperiode der Großen Koalition, nämlich sechs Wochen vor der Sommerpause, wesentlich beschleunigt.[229] Trotz der inhaltlich angreifbaren Diskussionspunkte blieb eine öffentliche, medial geführte Debatte um das geplante Gesetz bis kurz vor seiner Verabschiedung aus.[230]

3.5.1. Gesetzgebungsverfahren für Bundesgesetze

Bundesgesetze können nur erlassen werden, soweit dem Bund die ausschließliche oder konkurrierende Gesetzgebungskompetenz zusteht, anderenfalls verbleibt sie nach Art. 70 GG bei den Ländern.[231] In Art. 73 GG sind die Gegenstände aufgelistet, die ausschließlich den Bund zum Erlass von Ge-

[225] Vgl. Kurz et al., 2017, S. 6.
[226] Buermeyer, 2017, S. 9.
[227] Vgl. Buermeyer, 2017, S. 9.
[228] Vgl. Prantl, Bundestag will den Staatstrojaner beschließen, 2017, S. 4.
[229] Vgl. Gruber et al., Hackerangriff aus dem Bundestag, 2017.
[230] Vgl. O.V., Staatstrojaner zur Online-Durchsuchung von Smartphones und zur Überwachung von WhatsApp, 2017.
[231] Vgl. O.V., Duden Recht A-Z, Gesetzgebungsverfahren, 2017.

setzen befugen. Dazu zählen u.a. auswärtige Angelegenheiten, das Postwesen, die Währung und die Telekommunikation. Eine Gesetzgebung der Länder setzt nach Art. 71 GG voraus, dass eine ausdrückliche Ermächtigung durch Bundesgesetz erfolgt ist.[232]

Für den Erlass von Bundesgesetzen, wie der Strafprozessordnung, die Eingriffe in den Telekommunikationsverkehr vorsieht, werden Gesetzesvorlagen von der Bundesregierung, durch den Bundesrat oder aus der Mitte des Bundestags in diesen eingebracht.[233] Gemäß der Geschäftsordnung des Bundestages müssen Vorlagen von Mitgliedern des Bundestags entweder von einer Fraktion oder von fünf Prozent der Mitglieder des Bundestages unterzeichnet werden. Am häufigsten sind die Gesetzesvorlagen der Bundesregierung. Diese sind zunächst dem Bundesrat zuzuleiten und gehen mit dessen Stellungnahme in den Bundestag. Vorlagen des Bundesrats sind dem Bundestag durch die Bundesregierung zuzuleiten, die ihre eigene Auffassung zu der Vorlage darlegen soll.[234] Im Bundesrat werden die Bundesgesetze in dreimaliger Lesung beraten. In der ersten Lesung wird in der Regel beschlossen, den Entwurf an einen oder mehrere Bundestagsausschüsse zu überweisen. Auf Grundlage deren Stellungnahme werden sodann die zweite und dritte Lesung durchgeführt. Oftmals geschieht das in der gleichen Sitzung. Über die Ablehnung oder Annahme des Gesetzes wird nach Abschluss der Beratung, zumeist am Ende der dritten Lesung, abgestimmt. Nach Annahme im Bundestag, für die eine einfache Mehrheit genügt, werden die Bundesgesetze dem Bundesrat vorgelegt. Dieser hat die Möglichkeit, in Bezug auf das vom Bundestag beschlossene Gesetz innerhalb einer dreiwöchigen Frist den Vermittlungsausschuss anzurufen. Der Ausschuss besteht aus jeweils 16 Vertretern des Bundestages und des Bundesrates und hat die Aufgabe, einen Kompromiss auszuarbeiten, welcher von Bundestag und Bundesrat mitgetragen werden kann. Bei Einspruchsgesetzen nach Art. 77 Abs. 2, 3 und 4 GG muss der Bundesrat vor der Einlegung des Einspruchs ebenfalls das Vermittlungsverfahren beschreiten.[235] Hält der Vermittlungsausschuss eine Änderung des Gesetzes für

[232] Vgl. O.V., Duden Recht A-Z, Gesetzgebungsverfahren, 2017.
[233] Vgl. O.V., Duden Recht A-Z, Gesetzgebungsverfahren, 2017.
[234] Vgl. O.V., Duden Recht A-Z, Gesetzgebungsverfahren, 2017.
[235] Vgl. Schacht, Gesetzgebungsverfahren, 2017.

erforderlich, muss der Bundestag darüber entscheiden, ob er sich dem Änderungsvorschlag anschließen möchte.[236] Dieses Vorgehen bringt den Vorteil mit sich, dass verhindert würde, dass der Bundesrat seine Zustimmung verweigert oder Einspruch einlegt. Stimmen sowohl der Bundestag als auch der Bundesrat den Vorschlägen des Vermittlungsausschusses zu, gilt das Gesetz in dieser Fassung als verabschiedet.[237] Bei zustimmungsbedürftigen Gesetzen nach Art. 77 Abs. 2 und 2 a GG steht auch dem Bundestag und der Bundesregierung diese Verfahrensweise zu. Sofern das Vermittlungsverfahren abgeschlossen ist, richtet sich das weitere Verfahren danach, ob es sich um ein Bundesgesetz handelt, das der Zustimmung des Bundesrats bedarf oder nicht.[238] Gesetze sind zustimmungsbedürftig, wenn dies im Grundgesetz ausdrücklich vorgesehen ist. Im Wesentlichen lassen sich hierbei drei Gruppen unterscheiden.[239] Erstens sind Gesetze zustimmungsbedürftig, die die Verfassung ändern. Bei solchen muss der Bundesrat nach Art. 79 Abs. 2 GG sogar mit einer Zweidrittelmehrheit zustimmen. Zweitens bedürfen Gesetze der Zustimmung, die in bestimmter Weise Auswirkungen auf die Finanzen der Länder haben. Zu diesen zählen solche über Steuern, an deren Aufkommen die Länder und Gemeinden beteiligt sind, wie z.B. Einkommens- und Lohnsteuer, Gewerbe- und Mehrwertsteuer. Diese werden in Art. 105 Abs. 3 GG genannt. Auf der Ausgabenseite zählen hierzu nach Art. 104 a Abs. 4 GG alle Bundesgesetze, die Pflichten der Länder zur Erbringung von Geldleistungen, geldwerten Sachleistungen oder vergleichbare Dienstleistungen gegenüber Dritten begründen.[240] Drittens gelten die Gesetze als zustimmungsbedürftig, für deren Umsetzung in die Organisations- und Verwaltungshoheit der Länder eingegriffen wird. Die Länder haben nach Art. 84 Abs. 1 GG das Recht, von bundesgesetzlichen Regelungen über die Einrichtung der Behörden sowie über das Verwaltungsverfahren durch Landesgesetz abweichen zu dürfen. Die Zustimmung des Bundesrates ist nur insoweit erforderlich, wenn im Bundesgesetz wegen eines besonderen Bedürfnisses nach bundeseinheitlicher Regelung das Verwaltungsverfahren ausnahmsweise ohne Abweichungsmöglichkeit für

[236] Vgl. O.V., Duden Recht A-Z, Gesetzgebungsverfahren, 2017.
[237] Vgl. Schacht, Gesetzgebungsverfahren, 2017.
[238] Vgl. O.V., Duden Recht A-Z, Gesetzgebungsverfahren, 2017.
[239] Vgl. O.V., Bundesrat, Zustimmungs- und Einspruchsgesetze, 2017.
[240] Vgl. O.V., Bundesrat, Zustimmungs- und Einspruchsgesetze, 2017.

die Länder geregelt wird. Bei den genannten Zustimmungsgesetzen ist das vom Bundestag beschlossene Bundesgesetz dann endgültig abgelehnt, wenn der Bundesrat nicht zustimmt.[241] Bei Einspruchsgesetzen, also solchen Gesetzen, die der Zustimmung des Bundesrats nicht bedürfen, kann dieser nach Beendigung des Vermittlungsverfahrens Einspruch einlegen. Dieser wird als suspensives Veto bezeichnet und kann nach Art. 76 und 77 GG vom Bundestag mit einer einfachen oder Zweidrittelmehrheit zurückgewiesen werden, mit der der Bundesrat ihn beschlossen hat. Mindestens jedoch nach Art. 77 Abs. 4 GG mit der Mehrheit seiner Mitglieder, womit der Bundesrat überstimmt ist.[242]

Die vom Bundestag beschlossenen Bundesgesetze werden vom Bundespräsidenten nach Gegenzeichnung durch den Bundeskanzler und die zuständigen Bundesminister ausgefertigt. Der Bundespräsident hat die Aufgabe, zu prüfen, ob das Bundesgesetz auf einem ordnungsgemäßen Wege zustande gekommen ist und es inhaltlich mit der Verfassung in Einklang steht. Als weitere Voraussetzung für das Inkrafttreten des Gesetzes gilt die Verkündung dessen im Bundesgesetzblatt (BGBl.). Der Tag des Inkrafttretens soll in der Regel in dem Bundesgesetz bestimmt sein. Ist das nicht der Fall, tritt das Gesetz mit dem 14. Tag nach Ausgabe des entsprechenden Bundesgesetzblatts in Kraft.[243] In Ausnahmefällen ist ein rückwirkendes Inkrafttreten möglich. Über die Vereinbarkeit der Bundesgesetze mit dem Grundgesetz entscheidet aufgrund einer abstrakten oder konkreten Normenkontrolle bzw. einer Verfassungsbeschwerde das Bundesverfassungsgericht.[244]

3.5.2. Zustandekommen der Änderung des § 100 a StPO

Kritiker, wie Oppositionspolitiker und Datenschützer bemängeln[245], dass die Schwarz-Rote Koalition den Gesetzesentwurf für die Änderung des § 100 a StPO per Eilverfahren[246] oder wie ein „trojanisches Pferd“ in das Parlament gebracht und nachträglich an zwei weitgehend sachfremde Gesetzesentwürfe

[241] Vgl. O.V., Bundesrat, Zustimmungs- und Einspruchsgesetze, 2017.
[242] Vgl. O.V., Duden Recht A-Z, Gesetzgebungsverfahren, 2017.
[243] Vgl. O.V., Duden Recht A-Z, Gesetzgebungsverfahren, 2017.
[244] Vgl. O.V., Duden Recht A-Z, Gesetzgebungsverfahren, 2017.
[245] Vgl. Brodersen, Scharfe Kritik an Quellen-TKÜ und Online-Durchsuchung: „Der Staat hackt gleich ganze Smartphones“, 2017.
[246] Vgl. Grunert, Durch die Hintertür zur Online-Überwachung, 2017.

angefügt habe. Mit diesen soll das Strafverfahren allgemein effektiver und praxistauglicher ausgestaltet werden.[247] Es geht um die Möglichkeit, zusätzlich zu den bisherigen Sanktionen Fahrverbote für Straftäter zu verhängen und des Weiteren mehr DNA-Abgleiche durchführen zu können. Das Vorhaben, die Quellen-TKÜ noch in der laufenden Wahlperiode in die Strafprozessordnung einzubringen, wurde erst spät und in einer Formulierungshilfe der Bundesregierung bekannt. Dabei übernahmen die Fraktionen von CDU/CSU und SPD diesen Vorschlag fast unverändert. Indem die Große Koalition die Änderungen in ein laufendes Gesetzgebungsverfahren hineinbrachte, vermied sie sowohl eine erste Beteiligung des Bundesrates als auch die verfassungsrechtlich vorgesehenen drei Lesungen zu den Änderungen. In das Eilverfahren seien zudem die Bundesdatenschutzbeauftragten nicht einbezogen worden.[248] Der Bundesrat habe den Gesetzesentwurf schließlich bestätigt, ohne den Vermittlungsausschuss anzurufen. Dieser hätte das Gesetz erneut geprüft und möglicherweise die Änderungen in der Strafprozessordnung gestrichen bzw. korrigiert. Der Bundesrat folgte letztlich der Empfehlung des federführenden Rechtsausschusses.[249] Dieser hatte erwartungsgemäß keine Bedenken gegen den Entwurf, schließlich hatten die Innenminister der Länder die polizeiliche Lizenz zum Abhören von Computern und Smartphones zuvor auf einer Konferenz gefordert.[250] Ohne eine öffentliche Debatte sei versucht worden, mit Rechtsgrundlagen wie der Quellen-TKÜ, schwerste Grundrechtseingriffe in die Strafprozessordnung einzuführen.[251] *Prantl* spricht bei dem Gesetzgebungsverfahren von einer „derartigen Dreistigkeit, dass einem die Spucke wegbleibt.“[252] Das Gesetz mit derart weitreichenden Konsequenzen, das den staatlichen Zugriff auf private Computer und Handys erlaubt, sei auf fast betrügerische Weise an der Öffentlichkeit vorbeigeschleust worden und wie ein Dieb über Nacht gekommen.[253] Ein problematisches Gesetz würde gewiss nicht dadurch besser, dass man es mit Tricks beschließt.[254] Ähnlich beschreibt

[247] Vgl. Krempl, Bundestag gibt Staatstrojaner für die alltägliche Strafverfolgung frei, 2017.
[248] Vgl. Grunert, Durch die Hintertür zur Online-Überwachung, 2017.
[249] Vgl. Mansdörfer, Bundesrat beschließt StPO-Reform: Die GroKro räumt auf, 2017.
[250] Vgl. Künstler, Staatstrojaner auf leisen Sohlen, 2017.
[251] Vgl. Grunert, Durch die Hintertür zur Online-Überwachung, 2017.
[252] Prantl, Bundestag will den Staatstrojaner beschließen, 2017, S. 4.
[253] Vgl. Prantl, Bundestag will den Staatstrojaner beschließen, 2017, S. 4.
[254] Vgl. Prantl, Bundestag will den Staatstrojaner beschließen, 2017, S. 4.

der Journalist *Köpke* den Gesetzgebungsprozess. Der Staat habe sich langsam und gut getarnt angepirscht und einen unscheinbaren Änderungsantrag an ein Gesetzesvorhaben angehangen, das eine ganz andere Absicht hatte, nämlich die Ausweitung von Fahrverboten für Kriminelle.[255] Was Union und SPD im Kleingedruckten versteckt und schließlich im Bundestag verabschiedet haben, „halten Experten für einen der massivsten Eingriffe in die Grundrechte der Bürger seit dem großen Lauschangriff."[256] Auch *Singelnstein* kritisiert das Vorgehen. Er hält das Verfahren, über das die Gesetzesänderung umgesetzt wurde, für absolut unangemessen und politisch unredlich.[257] *Buermeyer* forderte in seiner gutachterlichen Stellungnahme im Mai 2017 für eine so gewichtige Einschränkung von Grundrechten, eine eingehende Diskussion in der Öffentlichkeit sowie im Parlament und merkte an, dass eine Entscheidung bis zum Ende der Legislaturperiode nicht mehr realistisch erscheine. Einen Sachgrund, der zum damaligen Zeitpunkt zur Eile hätte drängen können, erkannte der Richter nicht.[258] Das Bundesverfassungsgericht habe den Gesetzgeber in der Vergangenheit angehalten, alle Sicherheitsgesetze zu überprüfen und die Gummiformeln für Grundrechtseingriffe klar und konkret zu formulieren. Der Gesetzgeber schere sich aber hierum nicht und produziere den Gummi noch weicher als bisher.[259]

4. Technische Probleme im Zusammenhang mit der Quellen-TKÜ

In diesem Kapitel wird insbesondere auf die Staatstrojaner und ihre Software eingegangen, welche zur Umsetzung der Quellen-TKÜ teilweise gekauft und (weiter-) entwickelt werden. Das Kompetenzzentrum des Bundeskriminalamts arbeitet seit einigen Jahren an der Entwicklung rechtskonformer Staatstrojaner, mit denen es gelingen soll, die verschlüsselte Kommunikation von Betriebssystemen wie Android und iOS abzuhören. Seit September 2017 ist zudem die Zentrale Stelle für Informationstechnik im Sicherheitsbereich in Betrieb, welche zukünftig die Forschung und Entwicklung neuer Methoden und

[255] Vgl. Köpke, Wenn der Staat zum Hacker wird, 2017.
[256] Köpke, Wenn der Staat zum Hacker wird, 2017.
[257] Vgl. Tanriverdi, Vertraulichkeit – das war einmal, 2017.
[258] Vgl. Buermeyer, 2017, S. 25.
[259] Vgl. Prantl, Bundestag will den Staatstrojaner beschließen, 2017, S. 4.

Strategien zur nachhaltigen Sicherung der TKÜ-Fähigkeiten des Bundeskriminalamts, der Bundespolizei und des Bundesamts für Verfassungsschutz unterstützen soll. Dabei verfügt die Zentrale Stelle selber über keine eigenen Befugnisse zur Telekommunikationsüberwachung, stellt jedoch Werkzeuge bereit und berät die Behörden bei der Durchführung ihrer gesetzlichen Aufgaben.[260] 2019 soll zudem das Gemeinsame Zentrum für Telekommunikationsüberwachung, auch betitelt als „Abhörzentrum Ost“[261] eröffnet werden. Berlin, Brandenburg, Sachsen, Sachsen-Anhalt und Thüringen planen ein gemeinsames Überwachungszentrum auf dem Gebiet der Telekommunikationsüberwachung. Dieses soll es technisch ermöglichen, verschlüsselte Telekommunikation durch Strafverfolgungsbehörden abzuhören.[262] Zuletzt wird der Staatstrojaner in seiner Eigenschaft als Schadprogramm beleuchtet. Als solches können mögliche Gefahren im Zusammenhang mit der heimlichen Infiltration auf einem Endgerät auftreten, etwa beim sogenannten Nachladen oder durch das Auslösen von Fehlfunktionen, welche im Folgenden erläutert werden. Derzeit ist es technisch noch immer problematisch, die Staatstrojaner so zu entwickeln, dass sich die Zielrichtung des Abhörens auf die laufende Telekommunikation beschränkt.

4.1. Staatstrojanerentwicklung im Bundeskriminalamt

Seit 2006 beschäftigen sich Mitarbeiter des Bundeskriminalamts (BKA) bereits mit der Entwicklung von Staatstrojanern für die Strafverfolgung.[263] Derzeit wird in dem „Kompetenzzentrum Informationstechnische Überwachung“ (CC ITÜ) des BKA an der Entwicklung rechtskonformer Staatstrojaner gearbeitet, um diese auf Mobilbetriebssysteme wie Android und iOS ausdehnen zu können[264]. Aus einem Bericht des Innenministeriums geht hervor, dass im dritten Quartal 2016 mit der Weiterentwicklung des Bundestrojaners *RCIS* zur Version 2.0 begonnen wurde.[265] Während das BKA mit dem eigenen Trojaner zunächst nur *Skype* für Windows-Betriebssysteme überwachen konnte, sollte

[260] Vgl. Zentrale Stelle für Informationstechnik im Sicherheitsbereich, Telekommunikationsüberwachung, 2017.
[261] Vgl. O.V., Endlich kommt das Abhörzentrum Ost, 2017.
[262] Vgl. Biselli, Gemeinsames Überwachungszentrum von fünf Bundesländern soll 2019 starten, 2017.
[263] Vgl. O.V., Staatstrojaner - was ist das und wie funktioniert er?, 2017.
[264] Vgl. Kling, Staatstrojaner: Bundeskriminalamt will Messenger hacken, 2017.
[265] Vgl. Kling, Staatstrojaner: Bundeskriminalamt will Messenger hacken, 2017.

2017 die Eigenentwicklung für das Hacken von Smartphone-Apps sowie der Zugriff auf iOS-Betriebssysteme abgeschlossen werden.[266] Zur ersten *RCIS*-Version wurde 2016 öffentlich, dass diese nicht praxistauglich sei und sich insbesondere nicht für die Überwachung von Messenger-Programmen wie *WhatsApp*, *Telegram* und *Threema* eigne. Als Alternative zu der eigenen Software *RCIS* plant das BKA den Einsatz der kommerziellen Spähsoftware *FinSpy.* Dieses Programm wird etwa für den Fall begründet, dass die eigenentwickelte Spähsoftware von Betroffenen entdeckt werde.[267] *FinSpy* dient dem Ausspähen verschiedener Plattformen und „wurde nach erfolgter Überarbeitung durch die Herstellerfirma im Zeitraum Juni 2016 bis Februar 2017 durch ein externes Softwareprüflabor einer erneuten Quellcodeprüfung hinsichtlich ihrer Konformität mit der SLB unterzogen."[268] Mit SLB ist die standardisierte Leistungsbeschreibung gemeint. Nach erneuter Prüfung der Funktionen der Software könnten dem BKA bis Ende 2017 zwei verschiedene Programme zur Quellen-TKÜ zur Verfügung stehen.[269] Inwiefern die Planungen für das Jahr 2017 eingehalten werden konnten, ist zum jetzigen Zeitpunkt nicht bekannt.

4.2. Zentrale Stelle für Informationstechnik im Sicherheitsbereich

Im September 2017 stellte der Bundesminister des Inneren *de Maizière* die neue Sicherheitsbehörde *ZITiS* vor. Die Zentrale Stelle für Informationstechnik im Sicherheitsbereich hat ihren Sitz in München und bedient komplexe Aufgabenfelder.[270] Auf ihrer Homepage werden diese im Einzelnen vorgestellt. Hierzu zählen die digitale Forensik, die Kryptoanalyse, die Big-Data-Analyse sowie die Telekommunikationsanalyse. Mit der digitalen Forensik unterstützt *ZITiS* die Sicherheitsbehörden im Bereich der Forschung und Entwicklung neuer Methoden zur forensischen Sicherung digitaler Asservate. Diese Methoden bilden die Grundlage für die gerichtsfeste Verwertung digitaler Spuren.[271] Während der Einsatz von Kryptografie in der Vergangenheit insbesondere für

[266] Vgl. Eichenseher, BKA will Android und iOS hacken, 2017.
[267] Vgl. Kling, Staatstrojaner: Bundeskriminalamt will Messenger hacken, 2017.
[268] O.V., BKA will bald Messengerdienste hacken können, 2017.
[269] Vgl. O.V., BKA will bald Messengerdienste hacken können, 2017.
[270] Vgl. Meister, Geheimes Dokument: Das BKA will schon dieses Jahr Messenger-Apps wie WhatsApp hacken, 2017.
[271] Vgl. Zentrale Stelle für Informationstechnik im Sicherheitsbereich, Digitale Forensik, 2017.

das Militär von großer Bedeutung war, ist sie in der heutigen Zeit allgegenwärtig und dient dem permanenten Schutz der Privatsphäre sowie dem Schutz sensibler Daten der Bevölkerung. *ZITiS* bündelt die technische und wissenschaftliche Expertise im Umgang mit verschlüsselten Daten. In hochmodernen Laboren werden Angriffe auf informationstechnische Systeme erprobt und anwendbare Methoden im Anschluss für die Ermittlungsbehörden zur Verfügung gestellt. Im Zusammenhang mit der Big-Data-Analyse beschäftigt sich die Zentrale Stelle mit intensiver Forschung und Entwicklung von Methoden, um die Sicherheitsbehörden im Umgang mit der großen Menge an Daten zu unterstützen.[272]

Aufgrund der rasanten technologischen Entwicklungen in der Telekommunikationswelt sind sowohl Unternehmen durch die Nutzung moderner Kommunikationsmittel erfolgreich, als auch Privatpersonen, die ihre Lebensführung mit mobilen Geräten und Internetzugang gestalten. Da sich diesen Vorteilen ebenso Straftäter bei der Vorbereitung und Begehung von Straftaten bedienen und einige Begehungsweisen vollständig auf der Grundlage von Kommunikationskanälen geplant und durchgeführt werden, stellt die Telekommunikationsüberwachung ein wichtiges Ermittlungsinstrument dar.[273] Der stetige Wandel in der Telekommunikationswelt hat zur Folge, dass die Telekommunikationsüberwachung ständig an die technologische Entwicklung angepasst werden muss. Er stellt die Sicherheitsbehörden vor große Herausforderungen. *ZITiS* soll deshalb die Forschung und Entwicklung neuer Methoden und Strategien zur nachhaltigen Sicherung der TKÜ-Fähigkeiten des Bundeskriminalamts, der Bundespolizei und des Bundesamts für Verfassungsschutz unterstützen. Dabei verfügt die Zentrale Stelle selber über keine eigenen Befugnisse zur Telekommunikationsüberwachung, stellt jedoch Werkzeuge bereit und berät die Behörden bei der Durchführung ihrer gesetzlichen Aufgaben.[274] Nachdem der Gesetzgeber die Ermittlungsbehörden zu dem Einsatz von technischen

[272] Vgl. Zentrale Stelle für Informationstechnik im Sicherheitsbereich, Kryptoanalyse, Big-Data-Analyse, 2017.
[273] Vgl. Zentrale Stelle für Informationstechnik im Sicherheitsbereich, Telekommunikationsüberwachung, 2017.
[274] Vgl. Zentrale Stelle für Informationstechnik im Sicherheitsbereich, Telekommunikationsüberwachung, 2017.

Instrumenten, wie der Quellen-TKÜ, ermächtigt hat, wird *ZITiS* zukünftig Werkzeuge entwickeln, mit denen es gelingen soll, die verschlüsselte Telekommunikation abzuhören und zu überwachen.[275] Insbesondere geht es darum, die entsprechende rechtskonforme Spähsoftware herzustellen.[276] Die Zentrale Stelle für Informationstechnik im Sicherheitsbereich hat die Aufgabe Methoden und Produkte u.a. in Bezug auf Staatstrojaner zu entwickeln, Softwaretests und Quellcodeprüfungen durchzuführen[277] und Ermittlern den Zugriff zu verschlüsselten Daten auf Handys oder Computern zu verschaffen.[278] Für das Jahr 2017 wurden 120 Angestellte und zehn Millionen Euro eingeplant. In den nächsten fünf Jahren soll die *ZITiS* auf 400 Mitarbeiter wachsen.[279]

4.3. Gemeinsames Kompetenz- und Dienstleistungszentrum der Polizeien

Ab 2019 soll zudem das Gemeinsame Zentrum für Telekommunikationsüberwachung von fünf Bundesländern in Betrieb gehen. Berlin, Brandenburg, Sachsen, Sachsen-Anhalt und Thüringen planen ein gemeinsames Überwachungszentrum auf dem Gebiet der Telekommunikationsüberwachung, kurz *GKDZ*. Als Hauptstandorte wurden Leipzig und Dresden gewählt. An diesen soll es technisch ermöglicht werden, dass Telefongespräche abgehört, SMS mitgelesen und Internetverbindungen mitgeschnitten werden.[280] Auf den Punkt gebracht, soll das gemeinsame Zentrum u.a. die verschlüsselte Telekommunikation im Fokus haben. Die Bundesländer erhoffen sich hiervon Kostenersparnisse, da sie durch den Zusammenschluss keine fünf Überwachungsinfrastrukturen samt Technik parallel betreiben müssen. Ziel ist es, in den ersten fünf Jahren ca. elf Millionen Euro einzusparen. Das *GKDZ* ist nicht das erste Projekt, bei welchem sich Bundesländer bei dem Thema Telekommunikationsüberwachung zusammenschließen.[281] Das Überwachungszent-

[275] Vgl. Cornette, Neue Behörde überwacht künftig Whatsapp, Skype und Co, 2017.
[276] Vgl. Keller et al., 2015, S. 48.
[277] Vgl. Keller et al., 2015, S. 48.
[278] Vgl. Cornette, Neue Behörde überwacht künftig Whatsapp, Skype und Co, 2017.
[279] Vgl. Meister, Geheimes Dokument: Das BKA will schon dieses Jahr Messenger-Apps wie WhatsApp hacken, 2017.
[280] Vgl. Biselli, Gemeinsames Überwachungszentrum von fünf Bundesländern soll 2019 starten, 2017.
[281] Vgl. Biselli, Gemeinsames Überwachungszentrum von fünf Bundesländern soll 2019 starten, 2017.

rum Nord ist eine Kooperation der Bundesländer Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen und Schleswig-Holstein. Da das Abhören von Telefonaten und das Mitlesen von Nachrichten für die Polizei nach eigener Aussage eine wichtige Maßnahme darstellt, wenn sie Straftäter verfolgt, wird hierfür zunehmend bessere und teurere Technik sowie mehr Personal benötigt. In Hannover soll ab 2020 eine zentrale Stelle die Telekommunikationsüberwachung als Dienstleister für die Strafverfolgungsbehörden durchführen. Diese Bündelung soll ebenfalls Kosten sparen.[282]

4.4. Schwierigkeit bei der Entwicklung der Staatstrojaner

Obwohl sich die vorgestellten Abteilungen, Einrichtungen und Abhörzentren mit der Entwicklung rechtskonformer Staatstrojaner befassen, liegt die Schwierigkeit insbesondere darin, dass bis zum heutigen Tag kein Staatstrojaner vorgestellt und getestet wurde, der nachweislich nur auf die laufenden Telekommunikationsdaten gerichtet ist und somit den Vorgaben des Bundesverfassungsgerichts entspricht. Den Zugriff auf ein Zielsystem herzustellen, gelingt den Strafverfolgungsbehörden und IT-Abteilungen zuweilen, die Beschränkung der Abhörsoftware auf die laufende Telekommunikation erweist sich in der Programmierung als problematisch.

4.5. Gefahren der Infiltration

Bei einem Staatstrojaner handelt es sich um eine Art Trojanisches Pferd. Er ist eine Form von Malware. Diese ist Teil eines nützlichen Programms und erfüllt im Hintergrund eine ganz andere Funktion, meist ohne, dass der Nutzer etwas bemerkt.[283] Mit Hilfe des Programms gelangt der Trojaner auf den Computer, das Handy oder Tablet und installiert darauf, häufig versteckt, ein Schadprogramm. Diese Malware funktioniert dann eigenständig auf dem Zielgerät und lässt sich durch das Löschen des ursprünglichen Trägerprogramms nicht beeindrucken. Trojaner haben in der Regel viele Funktionen. Sie können beispielsweise Bildschirmkopien erstellen, Daten ausspähen, Eingaben in der Tastatur aufzeichnen, Geräte manipulieren, lahmlegen und fernsteuern und Schadprogramme installieren.[284]

---

[282] Vgl. Moßbrucker, Überwachungszentrum Nord: Pläne und Bedenken, 2016.
[283] Vgl. O.V., Staatstrojaner - was ist das und wie funktioniert er?, 2017.
[284] Vgl. O.V., Staatstrojaner - was ist das und wie funktioniert er?, 2017.

Risiken, die im Zusammenhang mit der Infiltration des Staatstrojaners auftreten können, sollen im Folgenden aufgezeigt werden. Als Nachladen wird der Vorgang bezeichnet, der erforderlich sein kann, um bei Änderungen am System des Betroffenen oder bei Updates der jeweiligen Kommunikationssoftware die Spionagesoftware anzupassen.[285] Durch das Nachladen kann aus einer Quellen-TKÜ während des laufenden Einsatzes eine Online-Durchsuchung entstehen, da neue Softwarefunktionen nachgeladen werden, die sich über die laufende Kommunikation hinaus beispielsweise auf gespeicherte Inhalte des Zielsystems konzentrieren können. Des Weiteren wäre hierdurch auch eine Wohnraumüberwachung technisch möglich und denkbar. Das Nachladen birgt zudem die Gefahr, dass auch unberechtigte Dritte eigene Module auf das Zielsystem einschleusen.[286] Bei der Untersuchung des *Digitask*-Trojaners durch den CCC konnte nachgewiesen werden, dass ein Nachladen vorgesehen war. Jedoch blieb die Frage offen, ob dieses im Einsatz dazu diente, neue Überwachungsfunktionen auf das bereits infizierte Endgerät nachzuladen.[287] Um diese Möglichkeit ausschließen zu können, fordern Mitglieder des CCC für den Betroffenen und seinen Verteidiger die Gewährleistung der Einsichtnahme in den Quellcode des Trojaners sowie in die Protokollierung des Einsatzes.[288] Eine weitere mögliche Gefahr stellt die Ermittlungsarbeit selbst dar. Aufgrund der alltäglichen permanenten Bedrohung durch Schadsoftware verfügen viele Computer-Nutzer über Abwehr- und Detektionssoftware auf ihren Geräten, sogenannte Virenscanner. Diese schützen in der Regel vor bereits bekannter Malware.[289] Wird also ein Staatstrojaner durch einen Virenscanner und den Betroffenen entdeckt, kann davon ausgegangen werden, dass sämtliche verdeckte parallele Ermittlungsverfahren in kürzester Zeit akut von einer Entdeckung bedroht sind. Sobald weitere Zielpersonen die Schadsoftware-Definitionen aktualisieren, werden sie über die Infektion informiert.[290] Gefährdungen können bei informationstechnischen Systemen zudem entstehen, wenn durch die Infiltration des Trojaners ungewollte Fehlfunktionen ausgelöst werden oder

[285] Vgl. Kurz et al., 2016, S. 10.
[286] Vgl. Kurz et al., 2016, S. 10.
[287] Vgl. Kurz et al., 2016, S. 10.
[288] Vgl. Kurz et al., 2016, S. 10.
[289] Vgl. Kurz et al., 2016, S. 11.
[290] Vgl. Kurz et al., 2016, S. 11.

die anvisierte Kommunikation unterbunden wird.[291] Als Beispiele können ein medizinisches Gerät, eine Smart-Watch oder ein Mobiltelefon dienen, die den Blutdruck oder Insulinwerte messen und den Arzt oder Patient informieren sollen. Durch Fehlfunktionen bliebe etwa eine Meldung oder Messung aus, die gesundheitliche Beeinträchtigungen nach sich ziehen könnten.[292]

5. Diskussion um die Notwendigkeit der Quellen-TKÜ

Das letzte Kapitel stellt Meinungen und Stellungnahmen von Vertretern aus Politik, Presse und Wissenschaft zu der Gesetzesänderung und der heimlichen Überwachungsmaßnahme vor. Dabei wird der Fragestellung nachgegangen, ob die Quellen-TKÜ für die Strafverfolgung für notwendig gehalten wird. Hierzu findet ein Diskurs statt, in dem Befürworter der Eingriffsbefugnis anführen, dass polizeiliche Werkzeuge an die fortschreitende Digitalisierung angepasst werden müssen, um eine wirksame Strafverfolgung und Straftatenaufklärung gewährleisten zu können, während sich Kritiker der Quellen-TKÜ auf das beschleunigte Gesetzgebungsverfahren berufen, welches scheinbar zum Ziel hatte, eine öffentliche Debatte weitestgehend zu verhindern. Sie bezeichnen die Ausgestaltung des Gesetzestextes als solchen, der sich in § 100 a Abs. 1 S. 3 StPO über die laufende Telekommunikation und somit die Entscheidung des Bundesverfassungsgerichts hinwegsetzt. Auszugsweise sieht *Bratke* die Quellen-TKÜ als kriminalistische Notwendigkeit im Zusammenhang mit erfolgreicher Strafverfolgung im Zeitalter der Digitalisierung und Nutzung von VoIP-Diensten an[293], während der deutsche Anwaltsverein (DAV) die Rechtsgrundlage als schwerwiegenden Eingriff in die Persönlichkeitsrechte der Betroffenen bezeichnet.[294] Kritiker, wie Bürgerrechtler, Datenschützer und Sicherheitsexperten sprechen sich bereits für eine Klage vor dem Bundesverfassungsgericht aus.[295] Ergänzend zu den Argumenten, die für eine mögliche Klage in Karlsruhe herangezogen werden, werden strafprozessuale Maßnahmen, welche im Gegensatz zu der Quellen-TKÜ als milder angesehen werden

[291] Vgl. Kurz et al., 2016, S. 12.
[292] Vgl. Kurz et al., 2016, S. 12.
[293] Vgl. Bratke, 2013, S. 482.
[294] Vgl. Brodersen, Scharfe Kritik an Quellen-TKÜ und Online-Durchsuchung: Der Staat hackt gleich ganze Smartphones, 2017.
[295] Vgl. Gruber et al., Hackerangriff aus dem Bundestag, 2017.

können und weniger in die Grundrechte der betroffenen Bürger eingreifen, genannt.

5.1. Befürwortende Stimmen

Der Jurist *Bratke* spricht sich für die kriminalistische Notwendigkeit der Quellen-TKÜ aus. Mit der zunehmenden Digitalisierung und Verschlüsselung von Telekommunikation würden die Beweisermittlung und Erkenntnisgewinnung zur Aufklärung von Straftaten kriminaltaktisch und technisch anspruchsvoller und schwieriger. Aufgrund von neuen Formen der Kriminalität als auch neuen technischen Möglichkeiten, die im Zusammenhang mit der Begehung von Straftaten genutzt werden können, stünden staatliche Behörden vor erheblichen Ermittlungsproblemen.[296] Für eine wirkungsvolle Strafverfolgung und Straftatenaufklärung bestehe das Bedürfnis, neue Wege bei der Ermittlungsarbeit zu gehen und an die technische Entwicklung angepasste Ermittlungsmaßnahmen einsetzen zu können. Die Nutzung spezieller technischer Mittel sei für die Durchführung moderner Ermittlungsarbeit unverzichtbar geworden.[297] Dabei liege die Notwendigkeit eines Ermittlungsinstruments wie der Quellen-TKÜ angesichts der stetig zunehmenden Verbreitung von *Skype* sowie vergleichbaren Programmen und der fortschreitenden Etablierung von VoIP als technischer Standard für Telefonate in der Gesellschaft auf der Hand. Die Weiterentwicklung für die Verschlüsselung von Kommunikationsinhalten mache gegenwärtig und zukünftig einen technischen Wettlauf der Strafverfolgungsbehörden mit den modernen Telekommunikationsdiensten unausweichlich.[298] Die automatisierte, bereits auf dem Endgerät des Nutzers stattfindende Verschlüsselung von Telekommunikationsdaten vor deren Übermittlung, wie dies bei vielen VoIP-Anbietern der Fall ist, mache ein Anknüpfen der Überwachung „an der Quelle“ der Telekommunikation erforderlich.[299] Die Bedeutung der Maßnahme müsse hierbei im Zusammenhang mit der sich entwickelnden Technik und dem zukünftigen Kommunikationsverhalten der Bevölkerung gesehen werden.[300] Nach Angaben der Bundesnetzagentur zeichnet sich bei den Netzstrukturen ein eindeutiger Trend weg von den leitungsvermittelten

[296] Vgl. Bratke, 2013, S. 482.
[297] Vgl. Bratke, 2013, S. 482.
[298] Vgl. Bratke, 2013, S. 482.
[299] Vgl. Bratke, 2013, S. 482 ff.
[300] Vgl. Bratke, 2013, S. 482 ff.

Netzen des herkömmlichen öffentlichen Festnetzes hin zu paketvermittelten Netzen ab.[301] Die Kommunikation via Internetprotokoll habe daher neben dem technischen auch das wirtschaftliche Potential, die Konvergenz der Systeme voranzutreiben, den Telekommunikationsmarkt neu zu ordnen und die herkömmliche Festnetztelefonie abzulösen.[302] *Bratke* beschreibt die Quellen-TKÜ als wichtigen Baustein, der in das Gesamtkonzept strafprozessualer heimlicher Ermittlungsmaßnahmen hinzugehöre. Auf diesen brauche der Staat unter der Achtung von verfassungsrechtlichen und einfachgesetzlichen Aspekten nicht zu verzichten.[303]

Wirth, in der Position eines Ersten Polizeihauptkommissars des bayrischen Landeskriminalamts, verglich die verschiedenen Möglichkeiten strafprozessualer heimlicher Ermittlungsmaßnahmen mit einem „Klavier, und eine Taste ist die Quellen-TKÜ, und wenn die fehlt, dann fehlt eine Taste – dann können Sie nicht mehr spielen.“[304] Damit den Sicherheitsbehörden bei verschlüsselten Telefonaten nicht im wörtlichen Sinne die Hände gebunden sind, sollte die Telekommunikationsüberwachung der technischen Entwicklung folgen und rechtlich so ausgestaltet sein, dass sich das Strafverfolgungsinteresse des Staates sowie das Sicherheitsinteresse der Allgemeinheit mit den Freiheits- und Grundrechten des Einzelnen in einem gerechten Gleichgewicht befinden. Dies könne nach *Bratke* durch einen sensiblen und verantwortungsbewussten Umgang mit der Quellen-TKÜ gewährleistet werden.[305]

Der Bund Deutscher Kriminalbeamter (BDK) begrüßte den erreichten Durchbruch der Innenministerkonferenz in Dresden im Juni 2017. *Guld* als Landesvorsitzender der Gewerkschaft in Sachsen begründete diesen insbesondere mit dem Terrorismus, der sich in seinem Handeln nicht nach landespolitischen Gegebenheiten orientiere, sondern sich vielmehr bundesweit ausrichte.[306] Deshalb seien bundesweit einheitliche polizeirechtliche Regelungen sowie ab-

[301] Vgl. Bundesnetzagentur, Digitalisierung, 2016.
[302] Vgl. Bratke, 2013, S. 483.
[303] Vgl. Bratke, 2013, S. 484.
[304] Wirth, Persönliches Gespräch mit Bratke, 2010.
[305] Vgl. Bratke, 2013, S. 484.
[306] Vgl. Guld, Durchbruch bei der Innenministerkonferenz in Dresden. Die Chance nutzen, 2017.

gestimmte polizeitaktische Maßgaben in der Bekämpfung schwerer Kriminalität und des Terrorismus nicht mehr zu umgehen. Angeführt wurden Vorschläge, wie z.B. die bestehende Sicherheitsarchitektur in Deutschland effizienter und schlanker zu gestalten. Neben der Vorstellung eines Musterpolizeigesetzes für die Polizei des Bundes und der Länder sei es weiter sinnvoll, technische Sicherungs- und Überwachungsmöglichkeiten auszubauen, etwa bei der Videoüberwachung, die mit geeigneter Gesichtserkennung in öffentlichen Räumen verbunden werden könne. Schließlich wurde die Forderung gestellt, die rechtlichen Möglichkeiten zur Überwachung der Telekommunikation im strafrechtlichen als auch gefahrenabwehrrechtlichen Sinne so auszugestalten, dass Strafverfolgung und Gefahrenabwehr in Zeiten der Digitalisierung möglich bleiben. Insbesondere sei die Schaffung der rechtlichen Möglichkeiten zur Überwachung der Messenger-Dienste überfällig.[307]

Im September 2017 beschlossen die Minister und Senatoren der sozialdemokratisch geführten Innenressorts die Hannoversche Erklärung, welche im Wesentlichen Forderungen und Vorschläge zur Inneren Sicherheit beinhaltet. *Pistorius* als niedersächsischer Minister für Inneres und Sport spricht im Zusammenhang mit der Erklärung von der Aufgabe, einen rechtsstaatlichen Ausgleich zwischen Freiheit und Sicherheit zu schaffen.[308] Freiheit ohne Sicherheit gäbe es ebenso wenig wie Sicherheit ohne Freiheit. Für eine wirksame Strafverfolgung und Gefahrenabwehr müsse es möglich sein, Kommunikation vor ihrer Verschlüsselung abgreifen zu können. Das Internet dürfe keinen rechtsfreien Raum darstellen. Hierin müssen dieselben Regeln wie in der analogen Welt gelten.[309]

Vertreter der Regierungsfraktionen verteidigen das verabschiedete Gesetz.[310] *Bähr-Losse* (SPD) räumte zur Quellen-TKÜ ein, dass es nicht immer die beste Lösung sei, große Gesetzespakete auf den letzten Drücker zu schnüren. Den Vorwurf einer Nacht-und-Nebel-Aktion durch die Hintertür wies sie von sich und machte inhaltlich deutlich, dass für die Strafverfolgung auch Chat-Räume

[307] Vgl. Guld, Durchbruch bei der Innenministerkonferenz in Dresden. Die Chance nutzen, 2017.
[308] Vgl. O.V., Niedersächsische Staatskanzlei, Meldung vom 27.09.2017.
[309] Vgl. O.V., Niedersächsische Staatskanzlei, Meldung vom 27.09.2017.
[310] Vgl. Brodersen, Scharfe Kritik an Quellen-TKÜ und Online-Durchsuchung: Der Staat hackt gleich ganze Smartphones, 2017.

und die Messenger-Kommunikation offenstehen müssten.[311] *Winkelmeier-Becker* (CDU/CSU) nannte die neuen Ermittlungsinstrumente der Quellen-TKÜ und Online-Durchsuchung unerlässlich für eine wirksame Strafverfolgung. Sie bezeichnete es als Unsinn, wenn sich die Möglichkeiten der Ermittlungsbehörden nicht daran orientieren würden, wie Täter und Banden heutzutage agieren.[312] Mit einer herkömmlichen TKÜ würden Ermittler „gerade noch mitkriegen, wer gerade welche Pizza bestellt."[313] Zudem sei der Einsatz der Maßnahmen an strenge Voraussetzungen gebunden. Tatsachen müssten den Verdacht begründen, dass jemand Täter oder Teilnehmer einer schweren Straftat ist. Aus diesem Grund stelle die Quellen-TKÜ keine Standardmaßnahme dar.[314] Der bayrische Justizminister *Bausback* (CSU) freute sich über die neuen Ermittlungsmaßnahmen: „Was lange währt, wird endlich gut."[315] Ermittler dürften nach seiner Auffassung nicht blind und taub gelassen werden, wenn sich Täter über *Skype* und *WhatsApp* unterhielten.[316]

Dem schließt sich der Deutsche Richterbund (DRB) an und brach damit eine Lanze für den Gesetzesentwurf.[317] Geschäftsführer *Rebehn* betonte, dass es nicht sein könne, dass die Ermittler bei einem Verdacht auf gravierende Straftaten Telefongespräche abhören und E-Mails mitlesen dürfen, hingegen nicht auf die Kommunikation von *WhatsApp*, *Telegram* oder *Threema* zugreifen können. Es sei wichtig, dass der Gesetzgeber die Strafverfolgungsbehörden bei der Überwachung der Telekommunikation auf die Höhe der Zeit bringe.[318]

Ermittler geben zur Quellen-TKÜ an, warum sie ein geheimes kriminaltaktisches Vorgehen auch im Bereich der Strafverfolgung bevorzugen. Bei der Aufgabe, Terroristen auf die Spur zu kommen, sei es nicht sinnvoll, diese durch

---

[311] Vgl. Krempl, Bundestag gibt Staatstrojaner für die alltägliche Strafverfolgung frei, 2017.
[312] Vgl. Brodersen, Scharfe Kritik an Quellen-TKÜ und Online-Durchsuchung: Der Staat hackt gleich ganze Smartphones, 2017.
[313] Brodersen, Scharfe Kritik an Quellen-TKÜ und Online-Durchsuchung: Der Staat hackt gleich ganze Smartphones, 2017.
[314] Vgl. Brodersen, Scharfe Kritik an Quellen-TKÜ und Online-Durchsuchung: Der Staat hackt gleich ganze Smartphones, 2017.
[315] Krempl, Bundesrat bringt Staatstrojaner für die gängige Strafverfolgung auf die Spur, 2017.
[316] Vgl. Krempl, Bundesrat bringt Staatstrojaner für die gängige Strafverfolgung auf die Spur, 2017.
[317] Vgl. Krempl, Staatstrojaner-Gesetz: Nächster Halt Bundesverfassungsgericht, 2017.
[318] Vgl. Krempl, Staatstrojaner-Gesetz: Nächster Halt Bundesverfassungsgericht, 2017.

offene Maßnahmen vorzuwarnen, in dem sie die informationstechnischen Geräte z.B. bei einer Durchsuchungsmaßnahme beschlagnahmen. Zu diesem Zeitpunkt wisse der Betroffene, dass gegen ihn ermittelt würde. Es gehe den Strafverfolgern darum, Nachrichten mitzulesen, kriminelle Netzwerke zu überwachen und diese auszuheben. Dafür sei eine Befugnisnorm, wie die der Quellen-TKÜ notwendig.[319]

Die Rechtsreferendarin und Volontärin bei der FAZ *Grunert* vermutet, dass die Große Koalition mit der Gesetzesänderung zur Quellen-TKÜ dem dringenden Wunsch von Polizei und Staatsanwaltschaft nachgekommen sei. In der Anhörung zur Einführung der Quellen-TKÜ berichteten Ermittlungspersonen davon, dass gerade in der organisierten Kriminalität unverschlüsselt lediglich Belanglosigkeiten zwischen den Straftätern ausgetauscht würden.[320]

5.2. Ablehnende Stimmen

Das Gesetz zur Einführung der Staatstrojaner stieß bereits vor seiner Verabschiedung auf vielfache Kritik. Insbesondere wurde der außergewöhnlich schwerwiegende Eingriff in das allgemeine Persönlichkeitsrecht der Betroffenen durch die staatlichen Maßnahmen angeführt.[321] „Staatliches Hacking ist viel schlimmer als der Große Lauschangriff, weil heute auf dem Handy das gesamte Privatleben enthalten ist“ [322], so *Korte* (die Linke). Das Gesetz würde zukünftig dazu führen, dass tiefgreifende Überwachungsmaßnahmen deutlich häufiger zum Einsatz kommen.[323] Eingriffe mittels Staatstrojanern sind nicht am „Computer-Grundrecht“ des Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG, sondern lediglich am Telekommunikationsgeheimnis des Art. 10 Abs. 1 GG zu messen, wenn ausschließlich laufende Kommunikation mitgeschnitten werden soll, entschied das BVerfG 2008. Bei einer Quellen-TKÜ, die *Buermeyer* auch als „Online-Durchsuchung light“ bezeichnet, müsse durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt werden, dass sich die Datenerhebung

[319] Vgl. Tanriverdi, „Vertraulichkeit – das war einmal“, 2017.
[320] Vgl. Grunert, Durch die Hintertür zur Online-Überwachung, 2017.
[321] Vgl. O.V., Staatstrojaner zur Online-Durchsuchung von Smartphones und zur Überwachung von Whatsapp, 2017.
[322] Gruber et al., Hackerangriff aus dem Bundestag, 2017.
[323] Vgl. Gruber et al., Hackerangriff aus dem Bundestag, 2017.

tatsächlich nur auf laufende Kommunikation beschränkt.[324] Die Rechtsgrundlage zur Quellen-TKÜ gehe jedoch über den Rahmen dessen hinaus, was das Bundesverfassungsgericht in seiner Entscheidung zu Online-Durchsuchungen als Eingriff allein in Art. 10 Abs. 1 GG für zulässig gehalten hat. Nach § 100 a Abs. 1 Satz 3 StPO soll über die laufende Kommunikation hinaus, auch die Erhebung gespeicherter Inhalte und Umstände der Kommunikation ausgelesen werden dürfen, was nach Meinung *Buermeyers*, eine an dem „Computer-Grundrecht“ zu messende Online-Durchsuchung darstelle.[325] Als weiterer Kritikpunkt wird angeführt, dass der Gesetzestext zur Quellen-TKÜ zu unklar formuliert sei. Er lasse zu, dass die Spionageprogramme technisch mehr erfassen können, als das, was sie rechtlich dürften.[326] Das eingesetzte technische Mittel müsse gemäß § 100 a Abs. 6 Nr. 1 StPO im Zusammenhang mit der Telekommunikationsüberwachung zwar genannt, aber in seinen Funktionen nicht näher bezeichnet werden. Dies sei angesichts der massiven Gefahren einer schleichenden Ausweitung einer Quellen-TKÜ hin zu einer Online-Durchsuchung, welcher nur durch die Gestaltung des Trojaners entgegengewirkt werden könne, unangemessen.[327] Des Weiteren wurden Bedenken geäußert, auf welche Weise sichergestellt werden könne, dass die Behörden die technischen Möglichkeiten nicht ausnutzen und tatsächlich nur laufende Telekommunikation mithören.[328] *Prantl* bezweifele als Jurist und Journalist, dass Richter über das zur Kontrolle notwendige technische Verständnis verfügen, wenn es darum geht einer heimlichen polizeilichen Abhörmaßnahme zuzustimmen.[329]

FOCUS-Redakteur *Niesmann* erinnert an die Protestwelle der Bevölkerung gegen die Volkszählung in den Achtzigerjahren sowie den großen Lauschangriff in den Neunzigern. Während zu diesen staatlichen Maßnahmen über viele Wochen kontrovers debattiert wurde, verabschiedete der Deutsche Bundestag

[324] Vgl. Buermeyer, 2017, S. 9.
[325] Vgl. Buermeyer, 2017, S. 16.
[326] Vgl. O.V., Staatstrojaner zur Online-Durchsuchung von Smartphones und zur Überwachung von Whatsapp, 2017.
[327] Vgl. Buermeyer, 2017, S. 18.
[328] Vgl. O.V., Staatstrojaner zur Online-Durchsuchung von Smartphones und zur Überwachung von Whatsapp, 2017.
[329] Vgl. Prantl, Bundestag will den Staatstrojaner beschließen, 2017.

2017 im Vorbeigehen ein Überwachungsgesetz, das nach Meinung von Experten den größten Eingriff des Staates in die Privatsphäre seiner Bürger darstellt und eine öffentliche Diskussion blieb aus.[330] *Niesmann* wolle keinen Staat, der Computer hacken, Spionageprogramme auf Handys installieren und Chatprotokolle mitlesen könne. Sicherheit sei wichtig, jedoch kein Selbstzweck. Sie müsse der Bewahrung der Freiheit und keinem Stimmenfang im Wahlkampf dienen.[331] Netzpolitik.org kritisiert die Befugnisse zur Quellen-TKÜ und spricht von einer Ausweitung des Staatstrojaners auf die Alltagskriminalität, sowie dem größten Angriff der Großen Koalition auf die Privatsphäre des Bürgers nach dem BND-Gesetz und der Vorratsdatenspeicherung.[332]

Auch Politiker halten den Eingriff in die Grundrechte des Bürgers bei der Quellen-TKÜ für umfassender als beim großen Lauschangriff. „Die Einführung sogenannter Staatstrojaner hält den strengen Regeln, wie sie Karlsruhe vorschreibt, nicht stand“[333], so *Ströbele* (Bündnis 90/Die Grünen). Es gehe dem Staat mit den neuen Maßnahmen nicht um die Verhinderung von Terrorismus, sondern um die Verfolgung vieler anderer Straftaten. Deshalb bestehe die Gefahr, dass die Online-Durchsuchung und Quellen-TKÜ überhandnehmen könnten.[334] Zwar bestehe ein wachsendes Bedürfnis, an die Kommunikation Terrorismusverdächtiger zu gelangen. Ein derart intensiver Grundrechtseingriff müsse jedoch sauber ausgearbeitet werden.[335] *Leutheusser-Schnarrenberger* (FDP) sprach über „den tiefsten Eingriff in die Privatsphäre der Bürger“ sowie „einem Trauerspiel, das ein Nachspiel beim Bundesverfassungsgericht braucht“.[336] Das geplante Gesetz sei der entscheidende Schritt zum Überwachungsstaat.[337]

Singelnstein, Professor für Kriminologe an der Ruhr-Universität in Bochum, führt an, dass Straftaten in der Gesellschaft weit verbreitet seien und von die-

[330] Vgl. Niesmann, Dein Freund und Hacker, 2017.
[331] Vgl. Niesmann, Dein Freund und Hacker, 2017.
[332] Vgl. Brodersen, Scharfe Kritik an Quellen-TKÜ und Online-Durchsuchung: Der Staat hackt gleich ganze Smartphones, 2017.
[333] Köpke, Wenn der Staat zum Hacker wird, 2017.
[334] Vgl. Köpke, Wenn der Staat zum Hacker wird, 2017.
[335] Vgl. Grunert, Durch die Hintertür zur Online-Überwachung, 2017.
[336] Tanriverdi, Vertraulichkeit – das war einmal, 2017, S. 5.
[337] Vgl. Tanriverdi, Vertraulichkeit – das war einmal, 2017, S. 5.

sen nur ein geringer Teil von den Strafverfolgungsbehörden ermittelt und aufgeklärt werde. Demzufolge trage eine weitere Ermittlungsbefugnis, wie die Quellen-TKÜ nicht zwingend dazu bei, dass mehr Straftaten entdeckt und aufgeklärt würden.[338] Dem schließt sich Rechtswissenschaftler *Rienhoff* an und empfindet das Gesetz als eines „der krassesten Strafverschärfungen der vergangenen Jahre".[339] Obwohl der Eingriff in die Grundrechte umfassender sei als der große Lauschangriff, seien die Voraussetzungen deutlich geringer. *Rienhoff* warnt vor einem massenhaften Einsatz des Staatstrojaners.[340]

Der ehemalige Bundesbeauftragte für Datenschutz *Schaar* äußerte seine Besorgnis um die Sicherheit von IT-Systemen. Er verglich den Einsatz von Staatstrojanern mit den Methoden, die Kriminelle zur Manipulation von Computern nutzen. Dritte könnten die von den Sicherheitsbehörden verwendeten Kenntnisse und Schwachstellen der Systeme etwa für kriminelle Zwecke ausnutzen.[341] Wenn der Staat Spähprogramme gegen seine Bürger einsetze, würde er letztlich selbst zum Hacker und müsse Sicherheitslücken ausnutzen, anstelle sie dem Hersteller zu melden, der sie zum Wohle aller Nutzer schließen kann.[342] Der Großen Koalition warf *Schaar* vor, dass diese fast wöchentlich Gesetze verabschiedete, die die Bürgerrechte einschränken und die Privatsphäre beeinträchtigen. Diesen Umstand bezeichnete *Schaar* als „ziemlich arroganten Umgang mit der Macht zulasten der Demokratie und des Rechtsstaats."[343] Auch die Berliner Datenschutzbeauftragte *Smoltczyk* warf dem Gesetzgeber vor, die technischen und verfassungsrechtlichen Bedenken, mit denen Maßnahmen, wie die Quellen-TKÜ behaftet seien, unter den Tisch zu kehren. Dies halte sie angesichts der schweren Grundrechtseingriffe für sehr bedenklich.[344]

[338] Vgl. Kurz, Interview über Staatstrojaner: Der intensivste Grundrechtseingriff in der Strafprozessordnung, 2017.
[339] Pichl, Dein Freund und Hacker, 2017.
[340] Vgl. Pichl, Dein Freund und Hacker, 2017.
[341] Vgl. Brodersen, Scharfe Kritik an Quellen-TKÜ und Online-Durchsuchung: Der Staat hackt gleich ganze Smartphones, 2017.
[342] Vgl. Gruber et al., Hackerangriff aus dem Bundestag, 2017.
[343] Krempl, Staatstrojaner-Gesetz: Nächster Halt Bundesverfassungsgericht, 2017.
[344] Vgl. Krempl, Staatstrojaner-Gesetz: Nächster Halt Bundesverfassungsgericht, 2017.

5.3. Zusammenfassung des Diskurses

Die Stellungnahmen zu der Frage, ob die Quellen-TKÜ für den Bereich der Strafverfolgung für notwendig gehalten wird, gehen inhaltlich weit auseinander. Die Aussage der ehemaligen niedersächsischen Justizministerin *Niewisch-Lennartz* (Bündnis 90/Die Grünen) macht den Zwiespalt zwischen den Befürwortern und Kritikern der Quellen-TKÜ deutlich. Sie gab zu bedenken, dass nicht elementare Grundrechte aus unangebrachter Eile gefährdet werden dürften. Andererseits sei es auch verständlich, dass sich die Strafverfolgung den gestiegenen Sicherheitsproblemen der heutigen Zeit stellen müsse und Ermittler nicht handlungsunfähig gelassen werden dürfen, sofern sich potentielle Täter über *Skype* oder *WhatsApp* unterhalten.[345] Die Befürworter der Quellen-TKÜ i.S.d. § 100 a StPO halten die Befugnisnorm in Zeiten der Digitalisierung und zunehmenden Nutzung von VoIP-Programmen für erforderlich. Strafverfolgungsbehörden müssen technisch auf einem aktuellen Stand und in der Lage sein, Straftaten mit angepassten Ermittlungsmethoden zu verfolgen und aufzuklären. Die Quellen-TKÜ reihe sich nach Meinung von Befürwortern erfolgreich in die heimlichen Ermittlungsmaßnahmen in der Strafprozessordnung ein. Kritiker der Abhörmaßnahme betonen den schweren Eingriff in die Grundrechte der Bürger. Sie halten den Gesetzestext des § 100 a StPO für ungenügend und zudem verfassungswidrig. Hierbei verweisen sie auf das BVerfG-Urteil aus dem Jahr 2008 zu Online-Durchsuchungen, in welchem die Richter festhalten, dass eine Quellen-TKÜ nur dann an Art. 10 Abs. 1 GG zu messen sei, wenn ausschließlich laufende Kommunikation erhoben wird. Nach § 100 a Abs. 1 Satz 3 StPO soll jedoch über die laufende Kommunikation hinaus, auch die Erhebung gespeicherter Inhalte und Umstände der Kommunikation ausgelesen werden dürfen, was nach Meinung *Buermeyers*, eine an dem „Computer-Grundrecht“ zu messende Online-Durchsuchung darstelle.[346] Somit sei der § 100 a StPO nicht ausschließlich auf laufende Kommunikation beschränkt und verfassungswidrig. Weitere Kritiker der Quellen-TKÜ zielen auf die Schwächung der IT-Systeme ab, in dem von den Strafverfolgungsbehörden Schwachstellen zur Infiltration der Staatstrojaner genutzt

[345] Vgl. Künstler, Staatstrojaner auf leisen Sohlen, 2017.
[346] Vgl. Buermeyer, 2017, S. 16.

werden, anstatt diese von den verantwortlichen Netzbetreibern schließen zu lassen.

5.4. Angekündigte Klage vor dem Bundesverfassungsgericht

Die Gesellschaft für Freiheitsrechte e.V. (GFF), eine noch junge Organisation, die auf dem Weg strategischer Prozessführung Grundrechte verteidigen will, hat bereits eine Verfassungsbeschwerde gegen die Gesetzesänderungen angekündigt.[347] Gemeinsam mit anderen zivilgesellschaftlichen Akteuren bereitet die GFF die Beschwerde gegen Staatstrojaner in der StPO vor und kündigt diese auf ihrer Homepage an.[348] Die Gesetzeseinführung sieht die GFF u.a. deshalb kritisch, weil der Gesetzestext die Vorgaben des Bundesverfassungsgerichts für den Einsatz von Trojanern nicht umsetze und den Anforderungen aus späteren Entscheidungen des BVerfG nicht genüge.[349] Als Vorsitzender des GFF kommt *Buermeyer* in seiner gutachterlichen Stellungnahme zur Formulierungshilfe der Regelung zur Quellen-TKÜ zu dem Schluss, dass die vorgeschlagene Norm zur Quellen-TKÜ die Vorgaben des BVerfG verfehle. Dies begründet er, wie bereits dargestellt, mit der Aussage des BVerfG, wonach die Quellen-TKÜ nur an Art. 10 Abs. 1 GG zu messen sei, sofern ausschließlich laufende Kommunikation erhoben werde. § 100 a Abs. 1 Satz 3 StPO setze sich in der Formulierung über die laufende Kommunikation hinaus und erlaubt unter den erleichterten Voraussetzungen der Quellen-TKÜ das Auslesen kondensierter Kommunikation.[350] „Ein solcher Taschenspielertrick des Gesetzgebers dürfte vor dem BVerfG kaum Bestand haben".[351] Die Argumente des GFF teilt auch der Verein für Grundrechte und Datenschutz *digitalcourage* und betitelt die Staatstrojaner mit einer „Überwachungskanone gegen die Bevölkerung."[352] Für diese müsse es in allen Computern und Smartphones Hintertüren geben, durch die staatliche Hacker und Kriminelle nach Lust und Laune in die

[347] Vgl. Pichl, Dein Freund und Hacker, 2017.
[348] Vgl. Gesellschaft für Freiheitsrechte, 2017.
[349] Vgl. Gesellschaft für Freiheitsrechte, Staatstrojaner im Strafprozess, 2017.
[350] Vgl. Buermeyer, 2017, S. 16.
[351] Buermeyer, 2017, S. 17.
[352] Vgl. Digitalcourage, Staatstrojaner: Überwachungskanone gegen die Bevölkerung, 2017.

Geräte einsteigen können. Die 5-Minuten-Info auf der Internetseite von *digital-courage* liefert Hintergründe zu den Staatstrojanern und ruft die Leser zur Unterstützung der Verfassungsbeschwerde auf.[353]

Ausführungen zu den entscheidenden Stellen des BVerfG-Urteils 2008 macht *Pichl*, welcher in seinem Verfassungsblog die Themen Gerichte und Grundrechte verfolgt.[354] In dem wegweisenden Urteil zu Online-Durchsuchungen leitete das BVerfG das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus dem allgemeinen Persönlichkeitsrecht ab. Hiermit wollte das Gericht den Grundrechtsschutz auf die Kommunikation in der digitalen Sphäre ausweiten, da Computer und Smartphones Träger einer Vielzahl von privaten Daten, Bankverbindungen, persönlichen Nachrichten bis hin zu sexuellen Vorlieben darstellen.[355] Laut BVerfG Urteil sei eine heimliche Infiltration dieser Geräte nur zulässig, wenn überragend wichtige Gemeinschaftsgüter gefährdet seien. Entgegen dieser sehr engen Auslegung ermögliche das neue Gesetz den Einsatz von Staatstrojanern in einer Vielzahl von Fällen. Beispielsweise dürfe die Quellen-TKÜ hiernach bei dem Verdacht auf Urkundenfälschung oder Steuerhinterziehung eingesetzt werden.[356] Die vorgesehenen Straftatbestände betreffen nicht die öffentlich genannten terroristischen Gefahren, sondern bewegen sich auf der Stufe der mittelschweren Kriminalität, was dem Urteil des BVerfG widerspreche. [357]

Neben dem Inhalt des Gesetzes wurde auch die Art und Weise kritisiert, wie es in das Parlament eingebracht wurde. Die neuen Überwachungsmaßnahmen, darunter die Quellen-TKÜ, kamen erst nachträglich durch einen Formulierungsvorschlag der Bundesregierung in die Strafprozessordnung.[358] Auf diesem Wege erregte das Vorhaben nur geringe öffentliche Aufmerksamkeit, eine öffentliche Debatte blieb aus. Aus dem Bereich der Politik erwägen die Parteien Die Linke und Bündnis 90/Die Grünen ebenfalls eine Beschwerde beim Bundesverfassungsgericht.[359] *Wunderlich* (Die Linke) sprach von dem

[353] Vgl. Digitalcourage, Staatstrojaner: Überwachungskanone gegen die Bevölkerung, 2017.
[354] Vgl. Pichl, Verfassungsblog, 2018.
[355] Vgl. Pichl, Dein Freund und Hacker, 2017.
[356] Vgl. Pichl, Dein Freund und Hacker, 2017.
[357] Vgl. Pichl, Dein Freund und Hacker, 2017.
[358] Vgl. Pichl, Dein Freund und Hacker, 2017.
[359] Vgl. Pichl, Dein Freund und Hacker, 2017.

invasivsten Überwachungsgesetz der letzten Jahre, welches „mit Worten jenseits der Fäkalsprache nicht mehr zu beschreiben ist“.[360] Die Maßnahmen seien weitgehender, als der große Lauschangriff. Daher sei er gespannt, was das Bundesverfassungsgericht zu dem mit einem Verfahrenstrick durchgepeitschten Gesetz sagen werde. Ein solches Hauruckverfahren halte er für unzulässig.[361]

Der Bundesverband IT-Sicherheit *Teletrust*, dem neben dem Bundeskriminalamt das Bundesamt für Sicherheit in der Informationstechnik angehört, will den Einsatz von staatlichen Überwachungsprogrammen auf Smartphones und Computern juristisch stoppen.[362] „Anstatt die Bürgerinnen und Bürger aktiv vor IT-Schwachstellen zu schützen, toleriert sie der Staat und hält sie für den potentiellen Einsatz seines Trojaners sogar aufrecht“.[363] *Teletrust* sehe in der Maßnahme der Quellen-TKÜ eine legalisierte Schwächung von modernen IT-Systemen, da Sicherheitsbehörden für die Infiltration der Überwachungssoftware unbekannte Sicherheitslücken ausnutzen müssen. Daher wolle der Verband Verfassungsbeschwerde gegen das vom Bundestag beschlossene Gesetz einlegen. Er würde bedauern, wenn das BKA und BSI wegen der Klage den Verband verließen. Eine Prüfung, inwieweit der Verband klageberechtigt ist, steht noch aus. *Teletrust* möchte in jedem Fall ein politisches Signal setzen. Schließlich sei es Zweck des Verbands, Beiträge zu einer sicheren und vertrauenswürdigen Informationsverarbeitung und Informationsübertragung zu leisten.[364]

5.5. Alternative Ermittlungsmaßnahmen als milderes Mittel zur Quellen-TKÜ

„Staatstrojaner sind ein außerordentlich eingriffsintensives Instrument“[365] führt *Buermeyer* an, mit welchem Strafverfolgungsbehörden nahezu alles über eine Zielperson in Erfahrung bringen können.[366] Hingegen wird in einem als geheim

[360] Krempl, Bundestag gibt Staatstrojaner für die alltägliche Strafverfolgung frei, 2017.
[361] Vgl. Krempl, Bundestag gibt Staatstrojaner für die alltägliche Strafverfolgung frei, 2017.
[362] Vgl. Greis, IT-Sicherheitsverband will gegen Staatstrojaner klagen, 2017.
[363] Greis, IT-Sicherheitsverband will gegen Staatstrojaner klagen, 2017.
[364] Vgl. Greis, IT-Sicherheitsverband will gegen Staatstrojaner klagen, 2017.
[365] Buermeyer, 2017, S. 2.
[366] Vgl. Buermeyer, 2017, S. 2.

eingestuften Bericht des Innenministeriums festgestellt, dass es keine grundrechtsschonenderen Alternativen zu der Quellen-TKÜ gäbe.[367] Aus diesem Grund sollen hier weitere Ermittlungsmaßnahmen angesprochen werden, die im Gegensatz zu einer Quellen-TKÜ weniger eingriffsintensiv erscheinen und ein milderes Mittel darstellen könnten.

Ermittlungsbehörden haben die Möglichkeit Verkehrsdatenabfragen durchzuführen. Diese werden durch die Telekommunikationsanbieter weiterhin unverschlüsselt erhoben und dürfen nach § 96 Abs. 1 TKG verwendet werden.[368] Bei Verkehrsdaten handelt es sich nach § 96 Abs. 1 Nr. 1 bis 5 TKG, um die Rufnummern der beteiligten Anschlüsse, personenbezogene Berechtigungskennungen, Kartennummern, Standortdaten, den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit, die übermittelten Datenmengen, den in Anspruch genommenen Telekommunikationsdienst, die Endpunkte von festgeschalteten Verbindungen und sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten. Zusammengefasst sind Telekommunikationsdaten „Daten, aus denen sich ergibt, von welchem Anschluss aus zu welchem Anschluss hin, wann und wie lange telekommuniziert wurde, also die genutzten Rufnummern und Kennungen, die Uhrzeit und das Datum der Verbindungen.“[369] Zu den Verkehrsdaten zählen auch die Standortdaten i.S.d. § 96 Abs. 1 Nr. 1 TKG. Nach § 3 Nr. 19 TKG werden als Standortdaten die Daten bezeichnet, die in einem Telekommunikationsnetz erhoben oder verwendet werden und die den Standort des Endgeräts eines Endnutzers eines Telekommunikationsdienstes für die Öffentlichkeit angeben.[370] Mit der Einholung dieser Daten erhalten Ermittlungsbehörden weitreichende Erkenntnisquellen hinsichtlich der Aufenthaltsorte, den Kontaktpersonen, der Häufigkeit der Nutzung sowie den Rufnummern einer betroffenen Person.[371]

Erkenntnisse für ein Strafverfahren, die sich mittels Quellen-TKÜ gewinnen ließen, können für die Ermittler ebenfalls durch einen offenen Zugriff und die

[367] Vgl. Kling, Staatstrojaner: Bundeskriminalamt will Messenger hacken, 2017.
[368] Vgl. Keller et al., 2015, S. 23.
[369] Keller et al., 2015, S. 24.
[370] Vgl. Keller et al., 2015, S. 24.
[371] Vgl. Buermeyer, 2017, S. 25.

Auswertung beschlagnahmter Systeme erlangt werden, sofern die Voraussetzungen für eine Beschlagnahme vorliegen.[372] Insbesondere ist an Mobiltelefone, Tablets oder Personal Computer zu denken, die Straftäter als Tatmittel, zur Vor- oder Nachbereitung von Straftaten nutzen, mit ihnen Erinnerungsbilder fertigen oder rechtswidrig erlangte Wertgegenstände darüber veräußern. Die genannten Endgeräte könnten exemplarisch im Rahmen einer Wohnungsdurchsuchung oder dem Antreffen des Betroffenen auf frischer Tat bzw. einer Personenkontrolle polizeilich beschlagnahmt werden. Während die Strafverfolger sowohl bei der Quellen-TKÜ als auch der Beschlagnahme der informationstechnischen Systeme an die Erkenntnisse gelangen würden, unterscheidet sich hierbei der Zeitpunkt der Erkenntnisgewinnung.[373] Bei der Quellen-TKÜ würden die Ermittler im besten Fall zeitgleich oder einige Stunden bzw. Tage später mithören und Hinweise zeitnah erhalten, wogegen der Zugriff und die anschließende Auswertung von Endgeräten erst ex post, also im Nachhinein Erkenntnisse mit sich bringen. *Singelnstein* beschreibt die Beschlagnahme der Geräte als offene Maßnahme, die deshalb nicht gerne von Strafverfolgungsbehörden angewandt werde, weil man damit das Ermittlungsverfahren offenlege.[374] *Buermeyer* kritisiert, dass es bei der Quellen-TKÜ weniger darum ginge, Erkenntnisse überhaupt zu erlangen, sondern vielmehr darum, sie früher und heimlich zu erhalten.[375]

Liebig führt als mildere Maßnahme zu dem Staatstrojaner die Verwendung eines sogenannten Key-Loggers oder Tasten-Protokollierers an, der ebenfalls zu Überwachungszwecken genutzt werden kann. Hierbei handelt es sich wie bei einem Trojaner um eine Spionage-Hard- oder Software, die aber im Gegensatz zu diesem nicht den Speicherinhalt des Rechners umfassen könne, sondern stattdessen die Bildschirminhalte und Tastaturanschläge aufzeichnet. Beide würden mit Hilfe des Key-Loggers auf dem infiltrierten Endgerät sichtbar gemacht. Tasten-Protokollierer werden von Cyber-Kriminellen, Ermittlungsbehörden und Nachrichtendiensten verwendet, um an vertrauliche Daten, etwa

[372] Vgl. Kurz, Interview über Staatstrojaner: Der intensivste Grundrechtseingriff in der Strafprozessordnung, 2017.
[373] Vgl. Buermeyer, 2017, S. 25.
[374] Vgl. Kurz, Interview über Staatstrojaner: Der intensivste Grundrechtseingriff in der Strafprozessordnung, 2017.
[375] Vgl. Buermeyer, 2017, S. 25.

Kennwörter oder PINs zu gelangen. Die Form der Infiltration sowie die Übermittlung der erhobenen Daten unterscheiden sich nicht von der Vorgehensweise mittels Staatstrojaners. Die Gefahr des Übertritts von einer Quellen-TKÜ zu einer Online-Durchsuchung würde bei der Nutzung eines Key-Loggers nicht bestehen.[376] Anzumerken ist, dass die Nutzung eines Key-Loggers zwar das Abgreifen von verschlüsselter schriftlicher Kommunikation ermöglicht, die verschlüsselte mündliche Kommunikation wäre von diesem jedoch nicht erfasst.

6. Fazit

In einem Rückblick sollen die Ergebnisse der Arbeit zur Beantwortung der Ausgangsfrage zusammengefasst werden. Diese lautete: Wie gelingt es Ermittlern i.S.d. § 100 a StPO laufende und zum Teil verschlüsselte Kommunikation abzuhören? Mit der zunehmenden Digitalisierung und Verschlüsselung von Telekommunikation wird auch die Beweisermittlung und Erkenntnisgewinnung zur Aufklärung von Straftaten kriminaltaktisch und technisch anspruchsvoller und schwieriger. Sowohl neue Formen der Kriminalität, als auch neue technische Möglichkeiten, die im Zusammenhang mit der Begehung von Straftaten genutzt werden, können für staatliche Behörden mitunter zu erheblichen Ermittlungsproblemen führen. Für eine wirkungsvolle Strafverfolgung und Straftatenaufklärung besteht aus unterschiedlichen Perspektiven das Bedürfnis, neue Wege bei der Ermittlungsarbeit zu gehen und an die technische Entwicklung angepasste Ermittlungsmaßnahmen einsetzen zu dürfen.

Im Zentrum der Arbeit standen drei Themengebiete: Die Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) als Ermittlungsgrundlage, daraus entstehende rechtliche und technische Probleme und der Diskurs um die Notwendigkeit der Maßnahme. Zur Beantwortung der Ausgangsfrage wurde schwerpunktmäßig die Quellen-TKÜ behandelt, welche als angepasstes Ermittlungsinstrument im Bereich der Strafverfolgung gilt. Mit dieser Eingriffsbefugnis soll es Ermittlern gelingen, den laufenden Kommunikationsverkehr bereits „an der Quelle“, also dem Absender, vor der Verschlüsselung des Telekommunikationsanbieters abzufangen und an die Strafverfolgungsbehörden weiterzuleiten. Hierzu ist es erforderlich, das Zielgerät, welches der Straftäter nutzt, zuvor

[376] Vgl. Liebig, 2015, S. 130.

heimlich mit einer Abhörsoftware, in den Medien als Staatstrojaner bekannt, zu versehen. Somit sind Ermittler im Ergebnis mit dem reformierten § 100 a StPO befugt, gewünschte Rufnummern von Telekommunikationsanbietern aufschalten zu lassen (TKÜ im herkömmlichen Sinne) und darüber hinaus ein technisches Mittel einzusetzen, um unverschlüsselte Kommunikationen abzufangen (Quellen-TKÜ).

Im zweiten Kapitel wurde die Quellen-TKÜ deskriptiv u.a. mit ihren technischen Grundlagen und in Abgrenzung zur herkömmlichen TKÜ und Online-Durchsuchung vorgestellt. Bei einer Quellen-TKÜ handelt es sich aus technischer Sicht um eine Spionagesoftware, die auf einem informationstechnischen System möglichst ohne Wissen des Nutzers unbemerkt verdeckte Funktionen ausführt. Wie sie beschaffen sein kann, zeigte ausschnittsweise die Analyse des Chaos Computer Clubs (CCC), der 2011 einen von einem privaten Softwareunternehmen programmierten Trojaner untersuchte. Dieser wurde ursprünglich zum Abhören der Telekommunikation seitens des Staates eingesetzt und verfügte über die Funktionen, Bildschirmfotos anzufertigen, Voice-over-IP-Gespräche abzuhören und beliebige Schad-Module nachzuladen. Durch Schad-Module wäre es technisch denkbar, die Funktionalität des Trojaners dahingehend zu erweitern, dass auch das Durchsuchen, Lesen, Manipulieren und Schreiben von Dateien möglich wäre. Des Weiteren wäre ein Zugriff auf das Mikrofon, die Kamera und Tastatur vorstellbar. Dieser 2011 eingesetzte Trojaner war nicht ausschließlich auf die laufende Telekommunikation beschränkt, weshalb sein Einsatz vom CCC kritisiert wurde. Ein solcher Staatstrojaner kann durch die Strafverfolgungsbehörden mit einem Direkt- oder Fernzugriff auf das Zielsystem gebracht werden, was sowohl von den technischen Gegebenheiten als auch den persönlichen Gewohnheiten des Nutzers abhängt. Die Quellen-TKÜ ähnelt zwar von ihrem Namen einer herkömmlichen Telekommunikationsüberwachung, ist aber technisch nicht mit dem Abhören von Telekommunikation auf dem Leitungsweg zu vergleichen. Der technische Aufwand und die möglichen Gefahren werden bei der Quellen- gegenüber der herkömmlichen Telekommunikationsüberwachung für deutlich höher befunden. In Abgrenzung zur Online-Durchsuchung wurde erörtert, dass bei beiden

Maßnahmen fremde Computersysteme heimlich mit einem Staatstrojaner ausgespäht werden. Die Online-Durchsuchung zielt auf alle gespeicherten Daten ab, die sich auf dem Endgerät befinden, während sich die Quellen-TKÜ auf laufende Kommunikationsdaten beschränken soll. Somit ist die Quellen-TKÜ funktional nur in Hinsicht auf die nach der Infiltration auszuführenden Befehle abzugrenzen.

Im dritten Kapitel wurden analytisch die rechtlichen Probleme erörtert, die im Zusammenhang mit der Quellen-TKÜ entstehen können. Hierzu wurden die einschlägigen Grundrechte, insbesondere das Fernmeldegeheimnis sowie das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme erläutert. Resümierend kann festgehalten werden, dass das Fernmeldegeheimnis als spezielles Grundrecht Anwendung findet, sofern mit der Maßnahme der Quellen-TKÜ ausschließlich laufende Telekommunikationsdaten erhoben werden. Die Beschränkung „muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein“[377], betonte das Bundesverfassungsgericht in einem Urteil. Sofern die Gefahr besteht, dass durch die Infiltration einer Spionagesoftware neben den laufenden Kommunikationsdaten weitere sensible Daten auf dem betroffenen informationstechnischen System erhoben werden können, bietet das Fernmeldegeheimnis keinen ausreichenden Schutz.[378] Hier würde das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme greifen. Anschließend wurde ein Vergleich des reformierten § 100 a StPO mit der vorherigen Norm durchgeführt. Hinsichtlich der kritischen Stellungnahmen zu dem reformierten § 100 a StPO soll an dieser Stelle *Buermeyer* wiederholt werden, der als Richter am Landgericht Berlin zum Ausdruck brachte, dass der § 100 a Abs. 1 S. 3 StPO die Vorgaben aus dem Urteil des Bundesverfassungsgerichts zu Online-Durchsuchungen verfehle, in denen es heißt, dass nur laufende Kommunikation erhoben werden darf. § 100 a Abs. 1 S. 3 StPO erlaube darüber hinaus die Erhebung gespeicherter Inhalte und die Umstände der Kommunikation unter den erleichterten Voraussetzungen der Quellen-

[377] BVerfGE 120, 274, S. 22.
[378] Vgl. BVerfGE 120, 274, S. 21.

TKÜ. Dies würde in einem offenen Widerspruch zu den Vorgaben des Bundesverfassungsgerichts stehen, welches nur die Erhebung laufender Kommunikation und nicht früherer Kommunikation benannte.

Der im Zusammenhang mit § 100 a StPO stehende beschleunigte Gesetzgebungsprozess wurde vorgestellt. Im Gegensatz zu einem herkömmlichen Gesetzgebungsverfahren wurde die Gesetzesänderung des § 100 a StPO durch den Rechtsausschuss des Deutschen Bundestages an ein schon laufendes Gesetzgebungsverfahren angehangen, bei dem es u.a. um den Führerschein-Entzug bei Nicht-Verkehrsstraftaten ging. Hierdurch wurde der Gesetzgebungsprozess zum Ende der Legislaturperiode der Großen Koalition 2017 wesentlich beschleunigt. Trotz der inhaltlich angreifbaren Diskussionspunkte blieb eine öffentliche, medial geführte Debatte um das geplante Gesetz bis kurz vor seiner Verabschiedung aus.

Das vierte Kapitel glich einem Exkurs, welcher die technischen Probleme aufzeigte, die in Bezug auf die Quellen-TKÜ auftreten können, von der Entwicklung der Staatstrojaner im Bundeskriminalamt bis hin zu den Gefahren, die bei einer Infiltration entstehen können. Die Problematik besteht insbesondere darin, dass bis zum heutigen Tag kein rechtskonformer Staatstrojaner vorgestellt und getestet worden ist, der nachweislich nur auf die laufenden Telekommunikationsdaten ausgerichtet ist und somit den Vorgaben des Bundesverfassungsgerichts entspricht. Das bedeutet, dass die gesetzliche Befugnis einer Quellen-TKÜ zwar besteht, es aber an der technischen Umsetzung und Genauigkeit der Staatstrojaner für diese Maßnahme mangelt. Ohne einen solchen Staatstrojaner muss an dieser Stelle den Kritikern gefolgt werden, die aufgrund der Ausführungen vor der Gefahr eines Abgleitens von einer Quellen-TKÜ hin zu einer Online-Durchsuchung warnen. Für die Beantwortung der Ausgangsfrage heißt das, dass nach § 100 a Abs. 1 S. 2 StPO Ermittler die Quellen-TKÜ zwar rechtlich einsetzen dürfen, sofern die Voraussetzungen hierfür vorliegen, diese jedoch aufgrund des sich in der Entwicklung befindlichen technischen Mittels derzeit nicht durchgeführt werden kann.

Im fünften Kapitel wurde ein Diskurs um die Notwendigkeit der Quellen-TKÜ geführt. In diesem lag das Hauptaugenmerk auf den befürwortenden und ablehnenden Stimmen von Vertretern aus Wissenschaft, Politik und Presse. Die

Kernaussagen beider Lager werden hier nochmal festgehalten. Die Befürworter der Quellen-TKÜ i.S.d. § 100 a StPO halten die Befugnisnorm in Zeiten der Digitalisierung und zunehmenden Nutzung von Voice-over-IP-Programmen für erforderlich. Strafverfolgungsbehörden müssen technisch auf einem aktuellen Stand und in der Lage sein, Straftaten mit angepassten Ermittlungsmethoden zu verfolgen und aufzuklären. Die Quellen-TKÜ reihe sich erfolgreich in die heimlichen Ermittlungsmaßnahmen in der Strafprozessordnung ein. Kritiker der Abhörmaßnahme betonen dagegen den schweren Eingriff in die Grundrechte der Bürger. Sie halten den Gesetzestext des § 100 a StPO für ungenügend und zudem verfassungswidrig. Hierbei verweisen sie auf das Bundesverfassungsgerichtsurteil zu Online-Durchsuchungen, in welchem die Richter festhalten, dass eine Quellen-TKÜ nur dann am Fernmeldegeheimnis zu messen sei, wenn ausschließlich laufende Kommunikation erhoben wird. Nach § 100 a Abs. 1 S. 3 StPO soll jedoch über die laufende Kommunikation hinaus, auch die Erhebung gespeicherter Inhalte und Umstände der Kommunikation ausgelesen werden dürfen, was eine an dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu messende Online-Durchsuchung darstelle. Weitere Kritiker der Quellen-TKÜ zielen auf die Schwächung der IT-Systeme ab, in dem von den Strafverfolgungsbehörden Software-Sicherheitslücken zur Infiltration der Staatstrojaner genutzt werden, anstatt diese von den verantwortlichen Netzbetreibern schließen zu lassen. Aufgrund des Umstandes, dass der Gesetzestext des § 100 a StPO die Vorgaben des Bundesverfassungsgerichts für den Einsatz von Staatstrojanern nicht umsetze und den Anforderungen aus späteren Entscheidungen des Gerichts nicht genüge, kündigten erste Vertreter von Datenschutz und Grundrechten bereits eine Verfassungsbeschwerde gegen die Gesetzesänderungen vor dem Bundesverfassungsgericht an.

Das staatliche Abhören von verschlüsselter Kommunikation stellt sowohl für die Strafverfolgungsbehörden, als auch für (Rechts-) Wissenschaftler und Datenschützer ein aktuelles und sensibles Thema dar, das medial sowie in dieser Arbeit kontrovers diskutiert wurde. Die Quellen-TKÜ wurde 2017 in die Strafprozessordnung aufgenommen und steht den Ermittlern zumindest in rechtli-

cher Hinsicht bereits zur Verfügung. Die technische rechtskonforme Fertigstellung der Staatstrojaner für diverse Betriebssysteme wurde für die folgenden Jahre angekündigt. Die staatliche Aufrüstung in diesem Bereich, wie die Abteilung im Bundeskriminalamt, die Zentrale Stelle für Informationstechnik im Sicherheitsbereich und gemeinsame Überwachungszentren auf dem Gebiet der Telekommunikationsüberwachung zeigen, bringen die Dringlichkeit und Notwendigkeit der Entwicklung entsprechender Staatstrojaner für die Strafverfolgungsbehörden zum Ausdruck. Sie verdeutlichen aber auch, dass der Bereich der Entwicklung der Staatstrojaner im Gegensatz zu dem digitalen Fortschritt der Telekommunikation zurückliegt. Die angekündigte Klage vor dem Bundesverfassungsgericht weist auf die angesprochenen Defizite bei der Ausgestaltung des reformierten § 100 a StPO hin. Eine Verfassungsbeschwerde kann, ebenso wie die technische Entwicklung der Staatstrojaner einige Zeit in Anspruch nehmen, solange hat die Regelung zur (Quellen-) Telekommunikationsüberwachung Bestand. Das Thema um die Abhörung von verschlüsselter Telekommunikation wird deshalb auch zukünftig von großer Bedeutung sein und entsprechend neuer Entwicklungsstände in den Mittelpunkt des öffentlichen Interesses rücken. Derzeit kann keine Aussage darüber getroffen werden, welche Staatstrojaner den Strafverfolgungsbehörden in den nächsten Jahren und Jahrzehnten zur Verfügung stehen, wie sie gestaltet sein werden, welche Quellcodes und welchen Anteil sie an erfolgreicher Ermittlungsarbeit haben werden. Vielleicht wird es dann möglich sein, die verschlüsselten Nachrichten von morgen bereits heute „an der Quelle“ abzufangen.

7. Quellenverzeichnis

Beuth, P.: Snowden-Enthüllungen. Alles Wichtige zum NSA-Skandal. Online verfügbar unter: http://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal, abgerufen am 08.10.2017.

Biselli, A.: Gemeinsames Überwachungszentrum von fünf Bundesländern soll 2019 starten. Online verfügbar unter: https://netzpolitik.org/2017/gemeinsames-ueberwachungszentrum-von-fuenf-bundeslaendern-soll-2019-starten/, abgerufen am 10.11.2017.

Bleckmann A.; Eckhoff, R.: Der „mittelbare" Grundrechtseingriff. In: DVBI 1988, S. 373-382.

Bratke, B.: Die Quellen-Telekommunikationsüberwachung im Strafverfahren. Grundlagen, Dogmatik, Lösungsmodelle. Berlin, 2013.

Brodersen, B.: Scharfe Kritik an Quellen-TKÜ und Online-Durchsuchung: „Der Staat hackt gleich ganze Smartphones". Online verfügbar unter: http://www.areamobile.de/news/44595-scharfe-kritik-an-quellen-tkue-und-online-durchsuchung-der-staat-hackt-gleich-ganze-smartphones, abgerufen am 19.11.2017.

Buermeyer, U.: Gutachterliche Stellungnahme zur öffentlichen Anhörung zur Formulierungshilfe des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKÜ im Strafprozess. Berlin, 2017. Online verfügbar unter: https://www.bundestag.de/blob/508848/bdf7512e32578b699819a5aa33dde93c/buermeyer-data.pdf, abgerufen am 27.10.17.

Bundesministerium der Justiz und für Verbraucherschutz: Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation. Online verfügbar unter: https://www.gesetze-im-internet.de/tk_v_2005/BJNR313600005.html, abgerufen am 09.01.2018.

Bundesamt für Justiz: Übersicht Telekommunikationsüberwachung für 2016. Online verfügbar unter: https://www.bundesjustizamt.de/DE/SharedDocs/Publikationen/Justizstatistik/Uebersicht_TKUE_2016.pdf?__blob=publicationFile&v=2, abgerufen am 08.10.2017.

Bundesministerium für Wirtschaft und Energie: Den digitalen Wandel gestalten. Online verfügbar unter: https://www.bmwi.de/Redaktion/DE/Dossier/digitalisierung.html, abgerufen am 17.12.2017.

Bundesnetzagentur: Digitalisierung. Online verfügbar unter: https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Digitalisierung/digitalisierung-node.html, abgerufen am 26.11.2017.

Cornette, V.: De Maizière eröffnet ZITiS. Neue Behörde überwacht künftig Whatsapp, Skype und Co. Online verfügbar unter: http://www.br.de/nachrichten/cdu-minister-de-maiziere-eroeffnet-sicherheitsbehoerde-zitis-100.html, abgerufen am 10.11.2017.

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

Digitalcourage: Staatstrojaner: Überwachungskanone gegen die Bevölkerung. Online verfügbar unter: https://digitalcourage.de/suche?keys=Staatstrojaner, abgerufen am 11.12.2017.

Donner, A.: Was ist ein Proxy Server? Online verfügbar unter: https://www.ip-insider.de/was-ist-ein-proxy-server-a-665349/, abgerufen am 13.01.2018.

Eichenseher, A.: BKA will Android und iOS hacken. Online verfügbar unter: http://de.ubergizmo.com/2017/07/24/bka-will-android-und-ios-hacken.html, abgerufen am 10.11.2017.

Epping, V.: Grundrechte. Hannover, 2017.

Gesellschaft für Freiheitsrechte: Staatstrojaner im Strafprozess? Online verfügbar unter: https://freiheitsrechte.org/, abgerufen am 11.12.2017.

Gorgass, T.: Staatliche Abhörmaßnahmen bei Voice over IP. Eine rechtsvergleichende Untersuchung zwischen Deutschland und den USA unter besonderer Berücksichtigung der Ausleitung des Sprachkanals (RTP-Streams). Münster, 2011.

Greis, F.: IT-Sicherheitsverband will gegen Staatstrojaner klagen. Online verfügbar unter: https://www.golem.de/news/teletrust-it-sicherheitsverband-will-gegen-staatstrojaner-klagen-1708-129395.html, abgerufen am 11.12.2017.

Gruber, A.; Horchert, J.; Reinbold F.: Hackerangriff aus dem Bundestag. Online verfügbar unter: http://www.spiegel.de/netzwelt/netzpolitik/staatstrojaner-hackerangriff-aus-dem-bundestag-a-1153618.html, abgerufen am 19.11.2017.

Grunert, M.: Bundestrojaner. Durch die Hintertür zur Online-Überwachung. Online verfügbar unter: http://www.faz.net/aktuell/politik/online-durchsuchung-quellen-tkue-bundestrojaner-wird-gesetz-15071053.html, abgerufen am 19.11.2017.

Guld, P.: Durchbruch bei der Innenministerkonferenz in Dresden - Die Chance nutzen. Online verfügbar unter: https://www.bdk.de/lv/sachsen/aktuelles/durchbruch-bei-der-innenministerkonferenz-in-dresden-die-chance-nutzen, abgerufen am 27.10.17.

Herrmann, C.: Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Entstehung und Perspektiven. Frankfurt am Main, 2010.

Hesseling, C.: Verschlüsselte Messenger: Threema, Signal, Telegram, WhatsApp. Online verfügbar unter: https://mobilsicher.de/apps-kurz-vorgestellt/verschluesselt-kommunizieren-per-app, abgerufen am 25.11.2017.

Keller, C.; Braun, F.; Hoppe, R.: Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen. Stuttgart, 2015.

Kling, B.: Staatstrojaner: Bundeskriminalamt will Messenger hacken. Online verfügbar unter: http://www.zdnet.de/88305503/staatstrojaner-bundeskriminalamt-will-messenger-hacken/?inf_by=5a11b4de681db8b9428b46e3, abgerufen am 19.11.2017.

Köpke, J.: Wenn der Staat zum Hacker wird. Grüne sehen im Bundestrojaner Verstoß gegen das Grundgesetz – und drohen mit Karlsruhe. Lübecker Nachrichten vom 23.06.2017, S. 3.

Krempl, S.: Bundestag gibt Staatstrojaner für alltägliche Strafverfolgung frei. Online verfügbar unter: https://www.heise.de/newsticker/meldung/Bundestag-gibt-Staatstrojaner-fuer-die-alltaegliche-Strafverfolgung-frei-3753530.html?artikelseite=all, abgerufen am 18.11.2017.

Krempl, S.: Staatstrojaner-Gesetz: Nächster Halt Bundesverfassungsgericht. Online verfügbar unter: https://www.heise.de/newsticker/meldung/Staatstrojaner-Gesetz-Naechster-Halt-Bundesverfassungsgericht-3754891.html, abgerufen am 27.11.2017.

Kurz, C.: Interview über Staatstrojaner: Der intensivste Grundrechtseingriff in der Strafprozessordnung. Online verfügbar unter: https://netzpolitik.org/2017/interview-ueber-staatstrojaner-der-intensivste-grundrechtseingriff-in-der-strafprozessordnung/, abgerufen am 27.10.17.

Kurz, C., Neumann, L., Rieger, F., Engling, D.: Stellungnahme zur „Quellen-TKÜ“ nach dem Urteil des Bundesverfassungsgerichts vom 20. April 2016 1 BvR 966/09. Online verfügbar unter: http://docplayer.org/34085993-Stellungnahme-zur-quellen-tkue-9-august-2016-nach-dem-urteil-des-bundesverfassungsgerichts-vom-20-april-bvr-966-09.html, abgerufen am 10.11.2017.

Künstler, D.: Staatstrojaner auf leisen Sohlen. Online verfügbar unter: http://www.funkschau.de/telekommunikation/artikel/143847/, abgerufen am 19.11.2017.

Liebig, B. M.: Der Zugriff auf Computerinhaltsdaten im Ermittlungsverfahren. Cloud Computing, E-Mail und IP-Telefonie als neue rechtliche und technische Herausforderungen für die Strafverfolger. Hamburg, 2015.

Mansdörfer, M.: Bundesrat beschließt StPO-Reform: Die GroKo räumt auf. Online verfügbar unter: https://www.lto.de/recht/hintergruende/h/stpo-reform-quellen-tkue-staatstrojaner-verfassungswidrigkeit/, abgerufen am 19.11.2017.

Meister, A.: Geheimes Dokument: Das BKA will schon dieses Jahr Messenger-Apps wie WhatsApp hacken. Online verfügbar unter: https://netzpolitik.org/2017/geheimes-dokument-das-bka-will-schon-dieses-jahr-messenger-apps-wie-whatsapp-hacken/, abgerufen am 10.11.2017.

Meister, A.: Kritik vom Bundesrechnungshof: Das Bundeskriminalamt will gleich zwei Staatstrojaner einsetzen. Online verfügbar unter: https://netzpolitik.org/2016/kritik-vom-bundesrechnungshof-das-bundeskriminalamt-will-gleich-zwei-staatstrojaner-einsetzen/, abgerufen am 18.10.2017.

Meister, A.: Telefonüberwachung: Berliner Polizei hat letztes Jahr zwei Telefongespräche pro Minute abgehört. Online verfügbar unter: https://netzpolitik.org/2017/telefonueberwachung-berliner-polizei-hat-letztes-jahr-zwei-telefongespraeche-pro-minute-abgehoert/, abgerufen am 08.10.2017.

Moßbrucker, D.: Überwachungszentrum Nord: Pläne und Bedenken. Online verfügbar unter: http://www.ndr.de/nachrichten/netzwelt/Die-Fakten-zum-norddeutschen-Ueberwachungszentrum,ueberwachungszentrum100.html#anchor0, abgerufen am 26.11.2017.

Niesmann, A.: Dein Freund und Hacker. Lübecker Nachrichten vom 23.06.2017, S. 2.

o.V.: Änderungen an der Strafprozeßordnung (StPO). Online verfügbar unter: https://www.buzer.de/gesetz/5815/l.htm, abgerufen am 23.11.2017.

o.V.: BKA will bald Messengerdienste hacken können. Online verfügbar unter: https://www.golem.de/news/bundestrojaner-bka-will-bald-messengerdienste-hacken-koennen-1707-129050.html, abgerufen am 10.11.2017.

o.V.: Endlich kommt das Überwachungszentrum Ost. Online verfügbar unter: http://www.sz-online.de/sachsen/endlich-kommt-das-abhoerzentrum-ost-3730343.html, abgerufen am 10.01.2018.

o.V.: Gesetzgebungsverfahren. Zustimmungs- und Einspruchsgesetze. Online verfügbar unter: http://www.bundesrat.de/DE/aufgaben/gesetzgebung/zust-einspr/zust-einspr-node.html;jsessionid=DB28E7E123A72F5F5BE31B529E2FD43E.1_cid349#doc4353672bodyText1, abgerufen am 18.11.2017.

o.V.: Gesetzgebungsverfahren. In: Duden Recht A-Z. Fachlexikon für Studium, Ausbildung und Beruf. Berlin, 2015. Online verfügbar unter: http://www.bpb.de/nachschlagen/lexika/recht-a-z/22287/gesetzgebungsverfahren, abgerufen am 18.11.2017.

o.V.: Hannover, Meldung vom 27.09.2017. Online verfügbar unter: http://www.focus.de/regional/hannover/hannover-meldung-vom-27-09-2017_id_7647524.html, abgerufen am 01.12.2017.

o.V.: Staatstrojaner – was ist das und wie funktioniert er? Online verfügbar unter: http://www.focus.de/digital/praxistipps/ueberwachung-staatstrojaner-was-ist-das-eigentlich-und-wie-funktioniert-es_id_7398204.html, abgerufen am 10.11.2017.

o.V.: Staatstrojaner zur Online-Durchsuchung von Smartphones und zur Überwachung von WhatsApp. Online verfügbar unter: https://www.wbs-law.de/it-recht/staatstrojaner-zur-online-durchsuchung-von-smartphones-und-zur-ueberwachung-von-whatsapp-73728/, abgerufen am 19.11.2017.

o.V.: Stellungnahme zur Einführung der Quellen-TKÜ und Online-Durchsuchung. Online verfügbar unter: https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Dokumente/20170531_Stellungnahme_Quellen_TKUE_Online_Durchsuchung_ROG.pdf, abgerufen am 25.11.2017.

o.V.: StPO-Reform 2017: Änderungen im Ermittlungsverfahren. Online verfügbar unter: https://www.strafakte.de/strafprozessrecht/stpo-reform-2017-ermittlungsverfahren/, abgerufen am 25.11.2017.

o.V.: Was ist ein Botnet und wie funktioniert es? Online verfügbar unter: http://www.was-ist-malware.de/allgemein/botnet/, abgerufen am 14.01.2018.

Pichl, M.: Dein Freund und Hacker. Online verfügbar unter: https://jungle.world/artikel/2017/26/dein-freund-und-hacker, abgerufen am 04.12.2017.

Pichl, M.: Verfassungsblog. Online verfügbar unter: http://verfassungsblog.de/author/maximilian-pichl/, abgerufen am 14.01.2018.

Prantl, H.: Bundestag will den Staatstrojaner beschließen. Gesetz über die heimliche Infiltration soll den Zugriff auf private Computer und Handys sowie deren Kontrolle erlauben. Süddeutsche Zeitung vom 22.06.17, S. 1.

Reuter, M: Nordrhein-Westfalen will den BKA-Staatstrojaner nutzen. Online verfügbar unter: https://netzpolitik.org/2017/nordrhein-westfalen-will-den-bka-staatstrojaner-nutzen/, abgerufen am 25.11.2017.

Schacht, H.: Gesetzgebungsverfahren. Online verfügbar unter: https://www.bmi.bund.de/DE/themen/verfassung/gesetzgebung/gesetzgebungsverfahren/gesetzgebungsverfahren-node.html, abgerufen am 18.11.2017.

Siller, H.: Gabler Wirtschaftslexikon, Stichwort: Exploit. Online verfügbar unter: http://wirtschaftslexikon.gabler.de/Archiv/1408531/exploit-v4.html, abgerufen am 13.01.2018.

Statistisches Bundesamt: Ausstattung privater Haushalte mit Informations- und Kommunikationstechnik – Deutschland. Online verfügbar unter: https://www.destatis.de/DE/ZahlenFakten/GesellschaftStaat/EinkommenKonsumLebensbedingungen/AusstattungGebrauchsguetern/Tabellen/Infotechnik_D.html, abgerufen am 20.12.2017.

Tanriverdi, H.: „Vertraulichkeit – das war einmal“. Behörden sollen künftig Rechner, Smartphones und Tablet-PCs mit Schadsoftware infizieren dürfen, um Verbrechern auf die Spur zu kommen. Die Kritik am sogenannten Staatstrojaner ist fundamental. Süddeutsche Zeitung vom 23.06.17, S. 5.

Wirth, E. (bayrisches Landeskriminalamt): Persönliches Gespräch mit Bratke zur Quellen-TKÜ. München, 2010. Siehe auch *Bratke, B.:* Die Quellen-Telekommunikationsüberwachung im Strafverfahren. Grundlagen, Dogmatik, Lösungsmodelle. Berlin, 2013.

Zentrale Stelle für Informationstechnik im Sicherheitsbereich: Arbeitsfelder, Telekommunikationsüberwachung. Online verfügbar unter: https://www.zitis.bund.de/DE/Arbeitsfelder/Ueberwachung/ueberwachung_node.html, abgerufen am 25.11.2017.

Eidesstattliche Erklärung:

Ich versichere, dass ich die Masterarbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Berlin, 31.01.2018

Nandy Hielscher