Schriften zum Strafrecht

Heft 243

Die Quellen-Telekommunikationsüberwachung im Strafverfahren

Grundlagen, Dogmatik, Lösungsmodelle

Von

Bastian Bratke

Duncker & Humblot · Berlin

BASTIAN BRATKE

Die Quellen-Telekommunikationsüberwachung im Strafverfahren

Schriften zum Strafrecht

Heft 243

Die Quellen-Telekommunikations-überwachung im Strafverfahren

Grundlagen, Dogmatik, Lösungsmodelle

Von

Bastian Bratke

Duncker & Humblot · Berlin

Die Rechts- und Wirtschaftswissenschaftliche Fakultät – Fachbereich Rechtswissenschaft – der Friedrich-Alexander-Universität Erlangen-Nürnberg hat diese Arbeit im Jahre 2012 als Dissertation angenommen.

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

D29

Fremddatenübernahme: L101 Mediengestaltung, Berlin
Druck: Berliner Buchdruckerei Union GmbH, Berlin
Printed in Germany

ISSN 0558-9126
ISBN 978-3-428-14037-4 (Print)
ISBN 978-3-428-54037-2 (E-Book)
ISBN 978-3-428-84037-3 (Print & E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ♾

Internet: http://www.duncker-humblot.de

Für Rudolf

Vorwort

Die Arbeit lag der Rechts- und Wirtschaftswissenschaftlichen Fakultät – Fachbereich Rechtswissenschaft der Friedrich-Alexander-Universität Erlangen-Nürnberg im Juli 2012 als Inaugural-Dissertation vor. Sie behandelt mit der Quellen-Telekommunikationsüberwachung im Strafverfahren ein Thema, welches praktisch wie wissenschaftlich hochaktuell ist und angesichts der stetig zunehmenden technischen Möglichkeiten des (verschlüsselten) Telekommunizierens auch in Zukunft für strafprozessuale Ermittlungstätigkeit eine bedeutsame Rolle spielen wird. Die Arbeit berücksichtigt Gesetzgebung, Rechtsprechung und Schrifttum bis einschließlich Juni 2012.

Die Veröffentlichung einer Dissertation gibt an dieser Stelle – und hierbei sei relativierenden Stimmen ausdrücklich widersprochen – die Gelegenheit, denjenigen Personen, welche am Entstehen und Gelingen dieser Arbeit Anteil hatten, in ganz besonderer Weise *Danke* zu sagen.

Meinem Doktorvater, Herrn Prof. Dr. Hans Kudlich, danke ich für die angenehme Betreuung und Begleitung des Entstehungsprozesses der Arbeit sowie die fachlich anregenden Gespräche. Herrn Prof. Dr. Matthias Jahn danke ich für das Interesse an der Arbeit und die rasche Erstellung des Zweitgutachtens.

Des Weiteren bedanke ich mich bei allen Personen, die sich im Rahmen von Expertengesprächen und Anfragen die Zeit für eine Auskunft nahmen und im Wege eines durchweg freundlichen und interessanten Gedankenaustauschs die inhaltliche Ausgestaltung der Arbeit um Erfahrungswerte aus der Praxis bereicherten.

Von Herzen danke ich meiner Mutter, meiner Großmutter und meiner Freundin für deren mentale Unterstützung und treues Zurseitestehen, aber auch für deren Verständnis, als die Arbeit an diesem Werk so manchen Verzicht notwendig machte.

Fürth, im November 2012 *Bastian Bratke*

Inhaltsverzeichnis

3. Teil

Einleitung: Überwachungsgegenstand Internettelefonie

Telekommunikation und die Nutzungsgewohnheiten ihrer Verwender[1] befinden sich im stetigen Wandel der Zeit. Der rasante Fortschritt moderner Kommunikationstechnologien beeinflusst das Kommunikationsverhalten der Menschen in grundlegender Weise. War dieses vor Jahren und Jahrzehnten noch geprägt von reinen Fernmeldeeinrichtungen und Analogtelefonie, so verfügen die modernen Bürgerinnen und Bürger der Informationsgesellschaft des 21. Jahrhunderts über ein buntes Potpourri an Möglichkeiten, mittels technischer Anlagen – stationär wie auch mobil – miteinander zu kommunizieren und Informationen auszutauschen. Auch das Internet hat sich in den vergangenen Jahren hin zu einem Multikommunikationsmedium entwickelt und dient schon lange nicht mehr „nur" dem bloßen Surfen im World Wide Web oder dem gewöhnlichen E-Mail-Versand wie es im ausklingenden 20. Jahrhundert noch der Fall war. Gerade das Internet erfüllt mit seinem (technischen) Potential hinsichtlich Leistungs- und Ausbaufähigkeit die Anforderungen, die von der heutigen Gesellschaft an weltweit erreichbare, 24 Stunden verfügbare und individuell ausgestaltete Telekommunikationsdienste gestellt werden. So drücken gerade Begriffe wie das („Mitmach"-)„Web 2.0", „neue Medien", „Social Networks", „Next Generation Networks" und viele weitere den technischen Zeitgeist aus und stehen sinnbildlich für den Wandel in der Gesellschaft, weg von direkter, persönlicher Kommunikation hin zu einem stetig zunehmenden Nachrichtenaustausch mittels komplexer, multifunktionaler (informations-)technischer Einrichtungen und Systeme in immer mehr Bereichen des alltäglichen beruflichen, sozialen und privaten Lebens.

Bedingt durch die gestiegene Verbreitung von (immer leistungsfähigeren) Computern in den Privathaushalten – so verfügten laut Statistischem Bundesamt im Jahr 2011 bereits 81 Prozent der privaten Haushalte in Deutschland über einen Computer, 77 Prozent über einen Internetzugang und 72 Prozent über einen Breitbandanschluss[2] – und der zunehmenden Verwen-

---

[1] Soweit im Nachfolgenden ausschließlich die maskuline Form Verwendung findet, erfolgt dies aus Gründen der Vereinfachung.

[2] Statistisches Bundesamt, Wirtschaftsrechnungen 2011, Private Haushalte mit Ausstattung von Informations- und Kommunikationstechnologien (alle Haushalte), S. 10, abrufbar unter https://www.destatis.de/DE/Publikationen/Thematisch/Einkom

dung des Internets in immer mehr Bereichen der täglichen Lebensgestaltung[3], gewinnt seit Beginn des 21. Jahrhunderts im Bereich der Telefonie die neue Technik der Internettelefonie[4], die sog. *Voice-over-IP-Kommunikation* (kurz *VoIP*), auf dem Telekommunikationsmarkt und für das Kommunikationsverhalten großer Teile der Bevölkerung an Bedeutung. Funktional ist die Internettelefonie vergleichbar mit der „klassischen" Festnetztelefonie („PSTN")[5] oder der Mobilfunktelefonie. Das Übertragungsprinzip baut auch bei der modernen IP-Telefonie auf den drei grundsätzlichen Vorgängen des Verbindungsaufbaus, der Gesprächsübertragung und des Verbindungsabbaus auf. Der Unterschied zur klassischen leitungsvermittelten Festnetztelefonie liegt jedoch darin, dass bei der paketvermittelten Internettelefonie die Kommunikation nicht im Rahmen einer festen Verbindung über speziell hierfür vorgesehene Leitungen geführt wird, sondern digitalisiert und in einzelne Datenpakete aufgeteilt über das weltweite Datennetz mittels Internetprotokoll (*IP*)[6] transportiert wird, also paketvermittelt stattfindet.[7] Erfolgt die VoIP-Kommunikation über den Computer mittels spezieller Software[8], so nimmt die VoIP-Software, welche für die Kommunikation über den Computer benötigt wird, i. d. R. automatisch auch eine Verschlüsselung der Daten während der Übermittlung im Datennetz vor.

Die zunehmende Digitalisierung und Verschlüsselung von Kommunikation über das Internet bleibt deshalb nicht ohne Auswirkung auf die Arbeit staatlicher Stellen bei der Verhütung, Bekämpfung, Verfolgung und Aufklärung von Straftaten. Denn moderne Internetdienste werden heutzutage nicht nur zur Begehung von computerspezifischen Delikten genutzt, sondern vor allem auch zur Kommunikation und Absprache zwischen Straftätern bei vielen anderen schwerwiegenden (nichtcomputerspezifischen) Deliktsarten, wie z. B. aus dem Bereich der Wirtschaftskriminalität oder der organisierten

---

menKonsumLebensbedingungen/PrivateHaushalte/PrivateHaushalteIKT2150400117004.pdf?__blob=publicationFile (zuletzt aufgerufen 15.06.2012).

3 Vgl. auch BVerfG NJW 2008, 822 (824).

4 Auch *Internet-Protokoll-Telefonie* („IP-Telefonie").

5 *Public Switched Telephone Network*.

6 Engl. *Internet Protocol*, weit verbreitetes Netzwerkprotokoll zum Datenaustausch in Computernetzen und Übertragungsstandard für Daten im Internet, welches als IP-Netzwerk bezeichnet werden kann, vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 121; http://de.wikipedia.org/wiki/Internet_Protocol (zuletzt aufgerufen 15.06.2012); http://www.voip-information.de/voip-protokoll.html (zuletzt aufgerufen 15.06.2012).

7 Vgl. http://www.itwissen.info/definition/lexikon/voice-over-IP-VoIP.html (zuletzt aufgerufen 15.06.2012).

8 Zu den einzelnen Erscheinungsformen von IP-Kommunikation, siehe 1. Teil A.I.2.

Kriminalität.[9] Konnten die herkömmlichen Ermittlungsmethoden mit den technischen Standards der klassischen (unverschlüsselten) Festnetztelefonie, der Mobiltelefonie und des E-Mailings noch (mehr oder weniger) Schritt halten, stellen die neuen Möglichkeiten verschlüsselter Kommunikation, wie bspw. i. d. R. codiert übermittelte Internettelefonie via Computer Ermittlungsbehörden bei der Überwachung von Telekommunikation hingegen vor gesteigerte technische wie rechtliche Schwierigkeiten. Während die Telekommunikationsüberwachung (TKÜ) nämlich den Behörden bislang meist problemlosen Einblick in die Inhalte der (unverschlüsselten) Kommunikation ermöglichte, liefert die herkömmliche Überwachung und Aufzeichnung verschlüsselter VoIP-Kommunikation auf dem Transportwege im Datennetz den Ermittlungsbehörden nur kryptierte Daten.[10] Dieser Umstand macht es erforderlich, die VoIP-Kommunikation noch vor deren Verschlüsselung bzw. nach deren Entschlüsselung abzugreifen. Als entsprechendes Ermittlungsinstrument hierfür wurde die sog. *Quellen-Telekommunikationsüberwachung* (kurz *Quellen-TKÜ*) entwickelt. Bei dieser neuen Ermittlungsmethode wird eine spezielle Überwachungssoftware auf dem Computer des Betroffenen[11] heimlich bzw. verdeckt[12] installiert, welche abgehende bzw. eingehende VoIP-Kommunikationsdaten noch vor deren Verschlüsselung auf dem Absendersystem bzw. nach deren Entschlüsselung auf dem Empfängersystem

---

[9] Vgl. *Sieber*, Stellungnahme zu dem Fragenkatalog des BVerfG in dem Verfahren 1 BvR 370/07, S. 9, abrufbar unter http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf (zuletzt aufgerufen 15.06.2012).

[10] Für Einzelheiten zur kriminalistischen Notwendigkeit der Quellen-TKÜ, siehe 1. Teil A.II.1.

[11] Zielperson und Betroffener der Überwachungsmaßnahme können in der Praxis durchaus auseinanderfallen: bei Einzelsystemen wie bei PCs, Notebooks/Laptops, Mobiltelefone kann nie ausgeschlossen werden, dass diese von mehreren Personen genutzt werden und somit auch andere von der Maßnahme (mit-)betroffen sind; dies ergibt sich zwangsläufig aus der grundsätzlichen Anschluss- bzw. Einrichtungsgebundenheit einer TKÜ-Maßnahme. Im Rahmen der vorliegenden Arbeit erfolgen die grundsätzlichen Untersuchungen anhand des „Idealfalls" (Betroffener der Maßnahme = Zielperson), weshalb beide Begriffe zunächst synonym verwendet werden; sofern eine Unterscheidung (rechtlich) relevant werden sollte, wird dies in den Ausführungen entsprechend dargestellt.

[12] Der Begriff „verdeckt" wird oftmals synonym mit dem Begriff „heimlich" verwendet (i. S. v. „ohne Wissen des Betroffenen"); dies entspricht auch der üblichen Terminologie in Rspr. und Schrifttum; bei strenger Begriffsauslegung beschreibt der Begriff der „Verdecktheit" indes eher den Umstand, dass der Betroffene zwar die (sichtbaren) Handlungen/Auswirkungen der Maßnahmeumsetzung mitbekommt, den dahinter stehenden tatsächlichen (ermittlungstaktischen) Anlass/Zweck aber nicht erkennt (bspw. durch das Handeln der Ermittlungspersonen unter einem bestimmten Vorwand und/oder Anwendung einer Legende), während der Begriff der „Heimlichkeit" hingegen eher auf eine völlige Unkenntnis des Betroffenen vom Ablaufen einer Maßnahme ihm gegenüber überhaupt hindeutet.

(„an der Quelle“) abgreift und zur Aufzeichnung an die Ermittlungsbehörden in Echtzeit („Live“)[13] ausleitet.[14]

Doch gerade die hierbei stattfindende heimliche Infiltration eines informationstechnischen Systems mit einer staatlich kontrollierten Fremdsoftware, welche das Abfangen und Ausleiten verschlüsselt geführter Internettelekommunikation an der Quelle erst möglich macht, ist höchst umstritten. Wie die im Herbst 2011 im Zusammenhang mit der Analyse und Veröffentlichung einer „Regierungs-Malware“[15] als sog. *Staatstrojaner*[16] durch den *Chaos Computer Club* (*CCC*)[17] von einem entsprechenden Medienecho und markigen Schlagzeilen begleitete, teils überaus emotional und kontrovers geführte Diskussion (einerseits: „Der Staatstrojaner wurde geknackt“[18], „Dreiste Lauscher“[19], „Anatomie eines digitalen Ungeziefers“[20], „Trojaner fressen Grundrecht auf“[21], „‚Eine Dimension wie die ‚Spiegel‘-Affäre‘“[22], „Trojaner in Lederhosen“[23], „Alle gegen den großen Feind da draußen“[24]

---

13 In Echtzeit („Live“): simultan im Moment des Stattfindens der Kommunikation und Entstehens der Signale, vgl. auch *Köhler*/*Kirchmann*, IT von A bis Z, S. 76.

14 *Wirth*, Sachgebietsleiter Kompetenzzentrum TKÜ Bayern, Bayerisches Landeskriminalamt (BayLKA), persönliches Gespräch mit dem Verfasser, München, 12.11.2010; für technische Einzelheiten zur Durchführung der Quellen-TKÜ, siehe 1. Teil A.II.3. und 4.

15 Bericht „Analyse einer Regierungs-Malware“ vom 08.10.2011, abrufbar unter http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf (zuletzt aufgerufen 15.06.2012); die vom *Chaos Computer Club* analysierte und veröffentlichte Software stammt aus einer Quellen-TKÜ in einem Ermittlungsverfahren aus dem Jahre 2009, deren Anordnung und Durchführung auch Gegenstand eines Beschwerdeverfahrens nach § 101 VII S. 3 StPO vor dem LG Landshut (MMR 2011, 690) waren, vgl. auch *Biermann*, http://www.zeit.de/digital/datenschutz/2011-10/ccc-staatstrojaner-bayern (zuletzt aufgerufen 15.06.2012); für Einzelheiten zur Entscheidung des LG Landshut, siehe 2. Teil A.II.4.

16 Bei einem sog. *Trojaner*, abgeleitet vom Trojanischen Pferd aus der griechischen Mythologie, handelt es sich um ein unerwünschtes, i. d. R. auch schadhaftes Computerprogramm (sog. *Malware*), welches entweder als nützliche Anwendung getarnt oder auch unbewusst vom Betroffenen auf sein System geladen wird und dieses dort im Hintergrund ausspionieren oder auch manipulieren kann, vgl. *Bär*, TK-Überwachung, Glossar, S. 375; *Köhler*/*Kirchmann*, IT von A bis Z, S. 235; vgl. auch dpa-Artikel „Lauscher im Hintergrund“, Nürnberger Nachrichten/Fürther Nachrichten vom 11.10.2011, S. 2.

17 Europäische Hackervereinigung, welche sich primär der Lobbyarbeit für den Datenschutz zuwendet, vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 44.

18 Frankfurter Allgemeine Sonntagszeitung vom 09.10.2011, S. 1.

19 *Fuehr*, in: Nürnberger Nachrichten/Fürther Nachrichten vom 10.10.2011, S. 2.

20 *Rieger*, in: Frankfurter Allgemeine Sonntagszeitung vom 09.10.2011, S. 41.

21 *Prantl*, in: Süddeutsche Zeitung vom 11.10.2011, S. 4.

22 *Nerz*, zitiert nach *Ehrenstein*/*Bewarder*, in: Die Welt vom 10.10.2011, S. 6.

23 *Bewarder*/*Ehrenstein*, in: Die Welt vom 11.10.2011, S. 5.

und „Nicht sehr souverän“[25], andererseits: „Trojaner sind nicht verboten“[26], „Bayerns Polizei wehrt sich gegen Trojaner-Affäre“[27], „‚Wir arbeiten nicht außerhalb der Gesetze‘“[28], „Bayerns Innenminister geht in die Offensive“[29] und „Friedrich verteidigt Überwachung durch Trojaner“[30]) zeigt, sind die grundrechtlichen Freiheiten, die im modernen Zeitalter der Informationsgesellschaft vehemente Verteidigung vor staatliche Beeinträchtigung erfahren, längst nicht mehr „nur“ Fragen des Schutzes der Pressefreiheit vor staatlichen Eingriffen[31] oder des Schutzes der informationellen Selbstbestimmung vor Beeinträchtigungen durch Volkszählungen[32], sondern die grundsätzliche Frage des Vertrauens des Einzelnen in die (überhaupt gewährleistbare?) Vertraulichkeit und Integrität seiner informationellen Selbstbestimmung in einer das öffentliche wie private Leben in immer stärkerem Maße durchdringende Verwebung des einzelnen Menschen, seiner persönlichen Daten, seines Tagesablauf, seiner sozialen Kontakte und letztlich seiner gesamten (digitalen) Identität mit den von ihm benutzten informationstechnischen Systemen des (mittlerweile wohl) täglichen Lebens. Der Schutz dieser neuen Ausprägung der informationellen Selbstbestimmung des Einzelnen in seinen von der alltäglichen Nutzung moderner informationstechnischer Systeme geprägten Lebensverhältnissen hat in bestimmten Punkten nunmehr auch Niederschlag in dem vom BVerfG[33] neu entwickelten Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer

---

24 *Goetz*/*Leyendecker*, in: Süddeutsche Zeitung vom 11.10.2011, S. 5.

25 *Gaycken*, in: Handelsblatt vom 11.10.2011, S. 8.

26 *Müller*, in: Frankfurter Allgemeine Zeitung vom 11.10.2011, S. 2.

27 *Bachmeier*, in: Augsburger Allgemeine vom 12.10.2011, S. 7.

28 *Dathe*, Präsident des Bayerischen Landeskriminalamts, zitiert nach *Szymanski*, in: Süddeutsche Zeitung vom 12.10.2011, S. 5.

29 *Englisch*, in: Nürnberger Nachrichten/Fürther Nachrichten vom 13.10.2010, S. 18.

30 faz.net vom 15.10.2011, abrufbar unter http://www.faz.net/aktuell/politik/online-durchsuchung-friedrich-verteidigt-ueberwachung-durch-trojaner-11494164.html (zuletzt aufgerufen 15.06.2012).

31 So sorgten für ein großes Medienecho bspw. im Jahr 1962 Durchsuchungen und Beschlagnahmen in Presseräumen des Nachrichtenmagazins „Der Spiegel“ wegen des Verdachts des Landesverrates in der sog. *Spiegel-Affäre*; hierzu auch das *Spiegel-Urteil* des BVerfG vom 05.08.1966 (BVerfG NJW 1966, 1603).

32 So die gesellschaftlich intensiv diskutierte Volkszählung in den 1980er Jahren; hierzu auch das *Volkszählungsurteil* des BVerfG vom 15.12.1983 (BVerfG NJW 1984, 419), in welchem erstmals das Grundrecht auf informationelle Selbstbestimmung aus Art. 2 I i. V. m. Art. 1 I GG hergeleitet worden ist.

33 Urteil des Bundesverfassungsgerichts vom 27.02.2008 (BVerfG NJW 2008, 822).

Systeme aus Art. 2 I i. V. m. Art. 1 I Grundgesetz (GG)[34], abgekürzt auch als *IT-Grundrecht*[35] oder *Computer-Grundrecht*[36] bezeichnet, gefunden.

Ob und inwieweit das heimliche staatliche Einschleusen und Verwenden einer Überwachungssoftware auf informationstechnischen Systemen im Rahmen staatlicher Ermittlungstätigkeit auf der bestehenden Rechtslage zulässig ist oder aus Gründen des wirksamen grundrechtlichen Schutzes als unzulässig anzusehen ist, ist rechtlich noch nicht in allen Bereichen abschließend geklärt. Eine generelle Unzulässigkeit des Einsatzes staatlicher Überwachungssoftware – wie manch plakativ und mit Nachdruck verfasster Bericht in der Tagespresse es erwarten ließe – ist verfassungsrechtlich jedenfalls nicht begründet. So hat das BVerfG in seiner Entscheidung vom 27.02.2008[37] den (heimlichen) Einsatz einer staatlichen Überwachungssoftware auf informationstechnischen Systemen – wenn auch unter strengen Voraussetzungen – insbesondere zum Zwecke des Zugriffs auf verschlüsselte Internettelekommunikation im Rahmen von Maßnahmen der Quellen-TKÜ unter grundrechtlichen Gesichtspunkten gerade nicht generell ausgeschlossen.[38]

Die rechtliche Verankerung der besonderen Ermittlungsmaßnahme der Quellen-TKÜ und deren Zulässigkeit zu Strafverfolgungszwecken auf Grund der bestehenden Gesetzeslage sind im Einzelnen indes heftig umstritten. Ob IP-Kommunikation, insbesondere Telefonate, die verschlüsselt über das Internet geführt werden, de lege lata „an der Quelle" überwacht werden dürfen, ist – anders als die sog. Online-Durchsuchung – noch nicht abschließend geklärt. Sowohl innerhalb der Literatur als auch innerhalb der Rechtsprechung ist das hierzu bestehende rechtsdogmatische Meinungsbild im Wesentlichen in zwei große Lager geteilt, die dogmatisch entweder von der Zulässigkeit der Quellen-TKÜ als Überwachung und Aufzeichnung von Telekommunikation auf Grund der geltenden Rechtslage ausgehen, oder aber diese neuartige Ermittlungsmethode mit ihrer spezifischen Realisierung und Eingriffswirkung als von keiner der in der Strafprozessordnung gegenwärtig vorhandenen Eingriffsbefugnisse gedeckt ansehen. Auf politischer Ebene knüpft an diese *dogmatische Uneinigkeit* über die Beurteilung der

---

[34] Grundgesetz für die Bundesrepublik Deutschland vom 23.05.1949 (BGBl. S. 1).

[35] So bspw. das Bundesministerium der Justiz, http://www.bmj.de/DE/Buerger/digitaleWelt/IT_Grundrecht/onlineDuchsuchung_node.html (zuletzt aufgerufen 15.06.2012).

[36] So bspw. *Krempl*, http://www.heise.de/newsticker/meldung/Neues-Computer-Grundrecht-schuetzt-auch-Laptops-und-Daten-im-Arbeitsspeicher-184298.html (zuletzt aufgerufen 15.06.2012).

[37] BVerfG NJW 2008, 822.

[38] Vgl. BVerfG NJW 2008, 822 (826).

Zulässigkeit der strafprozessualen Ermittlungsmaßnahme der Quellen-TKÜ auf Grundlage der geltenden Strafprozessordnung nahtlos die rechts- und gesellschaftspolitische Diskussion über die Zulässigkeit oder Unzulässigkeit des heimlichen staatlichen Einsatzes von Überwachungssoftware an („Die derzeitige Grauzone für die sogenannte Quellen-TKÜ im Bereich der Strafverfolgung halte ich für gefährlich“[39]; „Es gibt keine rechtliche Grauzone“[40]). Doch selbst zwischen den verantwortlichen staatlichen Stellen für die rechtliche und tatsächliche Bewertung und Anwendung solcher technischer Mittel zu Ermittlungszwecken werden deutlich unterschiedliche Auffassungen in Bezug auf die Zulässigkeit von Maßnahmen wie der Quellen-TKÜ, die auf dem Einsatz staatlicher Überwachungssoftware aufbaut, vertreten. So besteht zwischen dem Bundesministerium des Innern[41] und dem Bundesministerium der Justiz[42] als den beiden Ministerien, deren Ressort naturgemäß von dem Thema des (repressiven wie präventiven) staatlichen Einsatzes von Überwachungssoftware auf Bundesebene[43] zu einem wesentlichen Teil[44] betroffen ist, nicht erst seit der durch den *Chaos Computer Club* angestoßene Diskussion Uneinigkeit darüber, wie der Einsatz von staatlichen Überwachungsprogrammen zu bewerten und insbesondere mit der modernen Ermittlungsmaßnahmen der Quellen-TKÜ umzugehen ist.[45]

---

39 *Schaar*, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, zitiert nach *Höll*, in: „Gefährliche Grauzone, Süddeutsche Zeitung vom 13.10.2011, S. 6.

40 *Friedrich*, Bundesminister des Innern, zitiert nach faz.net, in: „Friedrich verteidigt Überwachung durch Trojaner“, faz.net vom 15.10.2011, abrufbar unter http://www.faz.net/aktuell/politik/online-durchsuchung-friedrich-verteidigt-ueberwachung-durch-trojaner-11494164.html (zuletzt aufgerufen 15.06.2012).

41 Diesem unterstehen Bundespolizei, Bundeskriminalamt und das Bundesamt für Verfassungsschutz.

42 Als ressortbedingt federführendes Ministerium für Angelegenheiten der Bundesgesetzgebung insb. zuständig für Angelegenheiten der Strafprozessordnung als Bundesgesetz (Art. 74 I Nr. 1, Art. 72 I GG).

43 Maßnahmen im präventiv-polizeilichen Bereich fallen in die Gesetzgebungskompetenz der Länder (Art. 70 I GG); bei den Strafverfolgungsbehörden, die Ermittlungsbefugnisse nach der StPO in Anspruch nehmen, also Staatsanwaltschaften sowie die von diesen zur Durchführung von Ermittlungsmaßnahmen herangezogenen (i. d. R.) Polizeibehörden, handelt es sich insoweit um Länderbehörden, die auf der Grundlage der StPO als Bundesgesetz handeln.

44 Der Zollfahndungsdienst (inkl. Zollkriminalamt als Mittelbehörde des Zollfahndungsdienstes, vgl. § 1 I ZFdG) ist als Teil der Bundeszollverwaltung dem Bundesministerium der Finanzen unterstellt; für Einzelheiten zur Frage der Befugnis zu (präventiven) Quellen-TKÜ-Maßnahmen auf Grundlage der §§ 23a ff. ZFdG, siehe 2. Teil A.I.1.f).

45 Während die Bundesministerin der Justiz, *Leutheusser-Schnarrenberger*, fordert, „dass man von diesen Ermittlungsmöglichkeiten so lange keinen Gebrauch macht, bis man ein klares Ermittlungs- und Lagebild hat“, zitiert nach *Meier*/*von*

Damit Ermittlungsbehörden mit der wesentlichen technischen Neuerung der VoIP-Kommunikation und dem Wandel des Kommunikationsverhalten in der Gesellschaft bei der Verfolgung und Aufklärung von Straftaten mithalten können, brauchen sie Rechtssicherheit dahingehend, ob und mit welchen Eingriffsbefugnissen und unter welchen Voraussetzungen ein praktikabler, rechtlich zulässiger und damit auch revisionsfester Zugriff auf Daten aus derartigen Kommunikationsformen erfolgen darf, um keine – weder politisch noch gesellschaftlich noch rechtsdogmatisch gewollten – rechtsfreien Räume zu schaffen.[46] Hierfür erforderlich ist allerdings, dass der heimliche staatliche Zugriff auf Telekommunikation an die – heutigen wie zukünftigen – Entwicklungen ausreichend angepasst ist, sowohl hinsichtlich technischer Standards als auch mit Blick auf das den Ermittlungsbehörden zur Verfügung gestellte rechtliche Instrumentarium heimlicher Ermittlungsmaßnahmen.

Ziel der vorliegenden Arbeit ist es, den strafprozessualen Zugriff auf Internettelefonie (VoIP)[47] „an der Quelle“ auf seine rechtliche Legitimation

---

Tiesenhausen, in: „Trojaner infiziert Schwarz-Gelb“, Financial Times Deutschland vom 12.10.2011, S. 9, und davor warnt, dass „wenn man von außen die volle Kontrolle über einen Rechner erlangen kann, […] sich auch Informationen unterschieben und verändern [lassen]“, zitiert nach *Herholz*, in: „‚Schnelle Aufklärung‘“, Passauer Neue Presse vom 11.10.2011, S. 4, kommentiert der Bundesminister des Innern, *Friedrich*, dies mit „den Generalverdacht gegen unsere Sicherheitsbehörden, der unter anderem von Frau Leutheusser-Schnarrenberger ausgesprochen wird, weise ich zurück“, zitiert nach *Meier*/*von Tiesenhausen*, in: „Trojaner infiziert Schwarz-Gelb“, Financial Times Deutschland vom 12.10.2011, S. 9, und bekräftigt, dass es nach jetzigem Kenntnisstand „keinerlei Hinweise [gibt], dass gegen Recht und Gesetz verstoßen worden ist“, zitiert nach *Hoffmann*/*Tomik*, in: „‚Es gibt keine rechtliche Grauzone‘“, faz.net vom 15.10.2011, abrufbar unter http://www.faz.net/aktuell/politik/im-interview-bundesinnenminister-friedrich-csu-es-gibt-keine-rechtliche-grauzone-11494291.html (zuletzt aufgerufen 15.06.2012).

46 Daneben besteht für Ermittlungspersonen aber auch ein Bedürfnis nach Rechtssicherheit zum Schutz vor etwaigen strafrechtlichen Kosequenzen ihres Handelns, da sich diese bei einem Überschreiten gesetzlicher Grenzen des Einsatzes von Überwachungssoftware dem Vorwurf des Ausspähens von Daten (§ 202a StGB), des Abfangens von Daten (§ 202b StGB) und des Vorbereitens des Ausspähens und Abfangens von Daten (§ 202c StGB), der Verletzung des Post- oder Fernmeldegeheimnisses (§ 206 StGB) sowie ggf. der Datenveränderung (§ 303a StGB) und der Computersabotage (§ 303b StGB) zumindest ausgesetzt sähen, hierzu näher *Basak*, „Strafbare Strafverfolger?“, Legal Tribune Online vom 10.10.2011, abrufbar unter http://www.lto.de/de/html/nachrichten/4513/vorwuerfe-wegen-spaeh-software-trojaner-kann-fuer-ermittler-zum-bumerang-werden/ (zuletzt aufgerufen 15.06.2012); für eine regelmäßige Strafbarkeit nach § 202a I StGB, *Albrecht*, JurPC Web-Dok. 59/2011, Abs. 23 sowie *Albrecht*/*Dienst*, JurPC Web-Dok. 5/2012, Abs. 57 ff.; a. A. hingegen Anm. *Brodowski*, JR 2011, 533 (538).

47 Wobei sich die Frage der Quellen-TKÜ theoretisch nicht nur bei der Internettelefonie stellt, sondern generell bei verschlüsselter Kommunikation (bspw. auch bei

hin zu untersuchen und in den Kontext der heimlichen Ermittlungsmaßnahmen der Strafprozessordnung einzuordnen. Die Untersuchungen befassen sich hierbei im Schwerpunkt mit der Frage der rechtlichen Zulässigkeit des neuen Ermittlungsinstruments der Quellen-Telekommunikationsüberwachung für den Zugriff auf verschlüsselt übermittelte Internettelefonie, sowohl im Kontext mit der Gesetzeslage de lege lata als auch mit Blick auf deren (bestmögliche) Einordnung in ein *harmonisches Gesamtkonzept heimlicher strafprozessualer Ermittlungsmaßnahmen*[48] de lege ferenda.

Hierfür werden in *Teil 1* zunächst die technischen und verfassungsrechtlichen Grundlagen einer Quellen-Telekommunikationsüberwachung dargestellt, in *Teil 2* Primär- und Sekundärmaßnahmen dogmatisch beleuchtet und deren rechtliche Kernfragen herausgearbeitet sowie in *Teil 3* zu deren Beantwortung verschiedene Lösungsmodelle entwickelt, welche auf ihre Rechts- und Praxistauglichkeit hin untersucht werden.

Die Dissertation berücksichtigt hierbei die Gesetzeslage und den Meinungsstand in Rechtsprechung und Schrifttum bis einschließlich Juni 2012.

---

verschlüsseltem Instant Messaging, verschlüsseltem E-Mailing u. ä.); gleichwohl stellt die Überwachung von Internettelefonie bislang den Hauptüberwachungsgegenstand von Maßnahmen der Quellen-TKÜ in der Praxis dar, weshalb sich nachfolgende Ausführungen schwerpunktmäßig an dieser ausrichten, grundsätzlich aber auch auf andere verschlüsselte Telekommunikationsformen entsprechend übertragbar sind.

48 Antwort der Bundesregierung, BT-Drs. 15/4725, S. 34; vgl. auch BT-Drs. 14/7679, S. 2; BT-Drs. 14/7008, S. 6, 8; BR-Drs. 702/01, S. 10.

1. Teil

Grundlagen

A. Technische Grundlagen

I. Voice-over-IP (VoIP)

1. Begriffserklärung

Für das Telefonieren über Netzwerke, die nach Internet-Standards aufgebaut sind, gibt es viel Bezeichnungen: „Internettelefonie", „IP-Telefonie", „Voice-over-Internet-Protocol" oder einfach nur „VoIP". Diese Begriffe werden i. d. R. allesamt synonym für die moderne Form der Telefonie, bei der die Sprache nicht über die herkömmlichen (leitungsvermittelten) Netze (bspw. Festnetz) übertragen wird, sondern mittels des Internetprotokolls über das (paketvermittelte) weltweite Datennetz des Internets (als IP-Netzwerk) verwendet.[1] Vereinfacht dargestellt werden im Unterschied zur klassischen Festnetztelefonie[2] bei VoIP-Kommunikation die Gesprächsinhalte nicht über hierfür (exklusiv) vorgehaltene Leitungen befördert, sondern in digitalisierter Form und in kleine Datenpakete zerlegt über das für den Datentransport nutzbare Internet übertragen[3], um beim Gesprächspartner schließlich wieder zusammengesetzt zu werden.[4] Beginnend in den 1980er

---

[1] Wobei teilweise unter strengerer begrifflicher Differenzierung unter dem Oberbegriff der „IP-Telefonie" mit „Internettelefonie" konkret das Telefonieren über das öffentliche Internet bezeichnet wird, während „Voice-over-IP" auch interne IP-Netze miteinschließt, vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 122.

[2] Bei der herkömmlichen Festnetztelefonie wird dem Teilnehmer exklusiv ein Nutzkanal überlassen, über den in Echtzeit eine Verbindung zum Zielanschluss hergestellt wird, nachdem der angewählte Anschluss über einen Signalisierungskanal ausfindig gemacht wurde, vgl. *Seitlinger*/*Strobl*, Voice over IP – eine rechtliche Beurteilung vom Kommunikationsdienst bis zum Netzzugang, S. 3 ff., abrufbar unter http://www.it-law.at/uploads/tx_publications/Voice_over_IP__eine_rechtliche_Beurteilung_vom_Kommunikationsdienst_bis_zum_Netzzugang.pdf (zuletzt aufgerufen 15.06.2012).

[3] Vgl. http://www.itwissen.info/definition/lexikon/voice-over-IP-VoIP.html (zuletzt aufgerufen 15.06.2012).

[4] Für Einzelheiten zu den technischen Abläufe bei softwarebasierter VoIP, siehe 1. Teil A.I.4.

Jahren mit der Vernetzung von EDV-Systemen und fortschreitend seit dem Internet-Boom der 1990er Jahre steigt die Datenübertragungsleistung bis heute kontinuierlich an.[5] Die technischen IP-Standards, die bereits Datenübertragungsraten von 25 Mbit/s per DSL[6] bzw. 50 Mbit/s und mehr per VDSL[7]-Verbindung über die Hausanschlüsse oder das Kabel-Netz erreichen können[8], bilden die Grundlage für IP-basierte Datennetzwerke und die zunehmende Nutzung des Internets als öffentliches Netz für Telekommunikationsangebote.

2. Erscheinungsformen der IP-Telekommunikation

Die moderne IP-Technologie eröffnet zahlreiche Möglichkeiten der Kommunikation über das Internet, sei es in Sprache, Schrift oder Bild. Die heute am Markt befindlichen unterschiedlichen Varianten und Erscheinungsformen sind vielzählig, was es grds. schwierig macht, alle möglichen Ausprägungen von IP-basierter Kommunikation mit universell gültigen Aussagen zu erfassen, wenngleich sich vorliegende Arbeit möglichst allgemeinverbindliche Ausführungen für die angestellten Untersuchungen zum Ziel gesetzt hat.

Bezüglich der von vorliegender Arbeit als Schwerpunkt thematisierten sprachbezogenen VoIP-Kommunikation können (und müssen zum Zwecke der dogmatischen Analyse) je nach verwendetem Endgerät grds. drei Haupterscheinungsformen der Internettelefonie unterschieden werden:

Es gibt a) die Möglichkeit der VoIP über das herkömmliche (analoge) Festnetztelefon mittels VoIP-fähigen Routers, b) VoIP über ein spezielles „VoIP-Telefon“ und c) VoIP über einen handelsüblichen Computer mittels spezieller VoIP-Software, z. B. Skype[9].

---

[5] Vgl. http://de.wikipedia.org/wiki/IP-Telefonie (zuletzt aufgerufen 15.06.2012); hierzu auch BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 31.

[6] *Digital Subscriber Line* (engl. für Digitaler Teilnehmeranschluss), ermöglicht Breitbandzugang in das Internet mit hoher Datenübertragungsrate, welches als Asymmetric Digital Subscriber Line (ADSL, „normales DSL“) die gegenwärtig gängigste Technik von Breitbandanschlüssen darstellt.

[7] *Very High Speed Digital Subscriber Line*, ermöglicht noch höhere Übertragungsraten als normales DSL.

[8] Mit VDSL bspw. bei der Telekom erreichbar: bis zu 50 Mbit/s Download-Geschwindigkeit und bis zu 10 MBit/s Upload-Geschwindigkeit, vgl. http://hilfe.telekom.de/hsp/cms/content/HSP/de/3370/FAQ/faq-149477317 (zuletzt aufgerufen 15.06.2012).

[9] Skype stellt eine kostenlose VoIP-Software zur Sprach- und/oder Videotelefonie zur Verfügung, die hierzu ein eigenes VoIP-Protokoll verwendet und mit Programmen anderer Anbieter grds. nicht kompatibel ist, siehe 1. Teil A.I.2.c).

a) VoIP über herkömmliches Telefon mittels VoIP-fähigen Routers

Diese Form der (anschluss- bzw. infrastrukturbasierten) Internettelefonie wird vor allem von den beiden größten deutschen Access-Providern[10], der Deutsche Telekom AG und Arcor[11], für ihr DSL-Angebot bereitgestellt. Bei dieser VoIP-Technik können Telefonate über das normale Telefon geführt werden, welches mittels eines speziellen Adapters oder eines technischen Gerätes (i. d. R. DSL-Router) über einen verfügbaren Breitbandanschluss[12] mit dem Internet verbunden ist. Hierzu erhält der Nutzer von seinem Internetdienstanbieter (Provider) eine spezielle Internetrufnummer, über die er seine Telefonate abwickeln kann[13]. Die Internetrufnummern setzen sich zusammen aus einer feste Vorwahl „032-" (eigene Rufnummerngasse), der Blockkennung für einen bestimmten Provider und einer zugeteilten eigenen Endnummer für den Anschluss des jeweiligen Nutzers. Die Internetrufnummer wird hierbei standortunabhängig und unabhängig von der (ortsabhängigen) Festnetznummer vergeben, weshalb sie auch im Falle eines Umzugs beibehalten werden kann.[14] Außer ggf. zum einmaligen Einrichten und Konfigurieren der Benutzer- und Zugangsdaten im Router wird ein Computer bei dieser Form der VoIP nicht benötigt. Mittels seines auf diese Weise mit dem IP-Netz verbundenen (normalen) Telefongerätes kann der Teilnehmer[15] dann über das Internet Verbindungen zu anderen mit dem VoIP-Netz

---

10 Unternehmen, die den Zugang ins Internet vermitteln und Dienste sowie technische Leistungen anbieten, die für die Nutzung oder den Betrieb von Diensten oder Inhalten im Internet notwendig sind; die Bezeichnung „Access-Provider" unterfällt als Teilbereich dem Oberbegriff des „Internet-Service-Provider" als Gesamtdienstleister, oftmals im Sprachgebrauch aber auch nur „Provider", vgl. http://www.itwissen.info/definition/lexikon/Internet-service-provider-ISP.html (zuletzt aufgerufen 15.06.2012).

11 Nach Übernahme durch die Vodafone Group 2008 mittlerweile in der Vodafone D2 GmbH aufgegangen.

12 Internetzugang mit hoher Datenübertragungsrate; je höher die Bandbreite, desto besser i. d. R. die Übertragungs- und Sprachqualität; nach alter Definition ab einer Übertragungsrate von mehr als 128 kbit/s downstream, nach neuer ab 1000 kbit/s downstream, vgl. Bundesministerium für Wirtschaft und Technologie, Breitbandatlas 2009_02, abrufbar unter http://www.zukunft-breitband.de/Dateien/BBA/PDF/breitbandatlas-bericht-2009-02-teil-2,property=pdf,bereich=bba,sprache=de,rwb=true.pdf (zuletzt aufgerufen 15.06.2012).

13 Dies ist jedoch i. d. R. optional, d. h. der Nutzer kann (technisch) seine Telefonate auch über das normale Telefonnetz abwickeln, dann aber je nach (vertraglicher) Vereinbarung ggf. kostenpflichtig.

14 Vgl. http://de.wikipedia.org/wiki/IP-Telefonie (zuletzt aufgerufen 15.06.2012).

15 Begriff des „Teilnehmers" in freier Begriffswahl und ohne Bezugnahme auf gesetzliche Begriffsbestimmungen, insbesondere des TKG.

verbundenen Telefongeräten herstellen bzw. über ein sog. *Gateway*[16] auch in das öffentliche Festnetz („PSTN") und Mobilfunknetz telefonieren. Bei dieser Erscheinungsform der VoIP erfolgt die Vermittlung und Übermittlung der Datenpakete auf IP-Ebene durch den Netzbetreiber (i. d. R. zugleich der Provider), welcher hier regelmäßig selbst als Anbieter des VoIP-Dienstes auftritt.

Eine spezielle Verschlüsselungsweise wie sie üblicherweise bei einer VoIP-Kommunikation von Computer zu Computer mittels VoIP-Software erfolgt, findet bei der Internettelefonie über das normale Telefon mittels Router i. d. R. (noch) nicht statt.[17] Eine entsprechende Routine[18] zur automatischen Codierung der Kommunikationsdaten wird im Rahmen solcher routerbasierter DSL-Dienste grds. nicht bereitgehalten. Eine standardmäßige Verschlüsselung ließe sich gegenwärtig auch technisch kaum realisieren, da ein herkömmliches Telefon nicht die technischen Möglichkeiten aufweist, eine solche Verschlüsselung zu lesen und zu entschlüsseln.[19] Wie bei normalen Festnetz- oder Mobiltelefonaten sollte daher für Provider und Sicherheitsbehörden die Möglichkeit bestehen, die im Rahmen einer derartigen Telefonie anfallenden Gesprächsdaten durch Zugriff während des Übertragungsvorgangs mittels „klassischer" TKÜ[20] nach §§ 100a, 100b Strafpro-

---

16 Engl. für „Protokollumsetzer", eine Art Schnittstelle, die es Netzen, welche auf unterschiedlichen Protokollen basieren und deshalb an sich nicht kompatibel sind, ermöglicht, miteinander zu kommunizieren, indem bspw. die ausgetauschten Sprachdaten zwischen dem paketvermittelten Internet (IP-Netz) und dem leitungsvermittelten öffentlichen Festnetz oder Mobilfunknetz „übersetzt" werden, vgl. *Köhler/Kirchmann*, IT von A bis Z, S. 98; http://de.wikipedia.org/wiki/Gateway_%28Informatik%29 (zuletzt aufgerufen 15.06.2012).

17 In diese Richtung auch *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11.2010 und *Bär*, Richter am OLG Bamberg, seit 01.11.2011 Leiter Referat „Internetkriminalität, Missbrauch neuer Technologien und Kriminologie" im Bayerischen Staatsministerium der Justiz, persönliches Gespräch mit dem Verfasser, Bamberg, 09.12.2010; zur „end-to-end"-Verschlüsselung bei VoIP von Computer zu Computer mittels Skype-Software, siehe 1. Teil A.I.2.c).

18 Unter einer *Routine* wird im Bereich der Softwareprogrammierung eine bestimmte Programm(teil)funktion verstanden, vgl. http://www.duden.de/rechtschreibung/Routine (zuletzt aufgerufen 15.06.2012).

19 Vgl. http://www.voip-information.de/skype-sicherheit.html (zuletzt aufgerufen 15.06.2012).

20 „Herkömmliche" bzw. „normale" TKÜ i. S. v. Überwachen und Aufzeichnen *unverschlüsselt* übertragener Telekommunikation auf der Transportstrecke, regelmäßig in Form des Zurverfügungstellens von Kopien der übermittelten TK-Daten durch den jeweiligen Provider (§ 100b III S. 2 StPO, § 110 TKG, §§ 3 ff. TKÜV), aber auch durch die Ermittlungsbehörde selbst, für Einzelheiten siehe auch 2. Teil A.II.6.; das Anbringen einer Überwachungsvorrichtung bspw. an einem normalen Telefonapparat zum Abhören unverschlüsselter Festnetztelefonie ließe sich allein begrifflich zwar durchaus auch als ein Überwachen von Telekommunikation „an der Quelle"

zessordnung (StPO)[21] zu überwachen und aufzuzeichnen.[22] Mithin begründet der neue § 110 I S. 1 Nr. 1a Telekommunikationsgesetz (TKG)[23] diesbezüglich spezielle Mitwirkungs- und Bereitstellungsspflichten für betroffene Betreiber von TK-Anlagen i. S. d. § 110 I S. 1 TKG.[24] Das Erfordernis einer Quellen-TKÜ ergibt sich für diese Konstellation somit nicht.

b) VoIP über spezielles VoIP-Telefon

Bei dieser Erscheinungsform bieten Diensteanbieter (i. d. R. kombiniert mit einem Breitbandzugang ins Internet) anschluss-/infrastrukturbasierte VoIP-Kommunikation über ein spezielles auf Internettelefonie spezialisiertes Telefonendgerät, ein sog. *VoIP-Telefon* oder auch *SIP*[25]*-Telefon*, an. Zusatzgeräte wie bspw. ein Computer oder ein Router werden hier nicht benötigt. Erforderlich ist neben dem speziellen Endgerät nur das Vorhandensein eines nutzbaren (Breitband-)Anschlusses. Das VoIP-Telefon sieht aus wie ein normales Festnetz-Telefon und lässt sich im Prinzip auch wie ein solches bedienen, es versendet jedoch die Gesprächsdaten, wie bei VoIP üblich, in einzelne Datenpakete zerteilt über das Internet innerhalb des IP-Netzes an andere VoIP-Telefone bzw. über ein Gateway auch in das öffentliche Festnetz („PSTN") und Mobilfunknetz. Bei dieser Erscheinungsform der VoIP erfolgt die Vermittlung und Übermittlung der Datenpakete auf IP-Ebene durch den Netzbetreiber (i. d. R. zugleich der Provider), welcher hier regelmäßig selbst als Anbieter des VoIP-Dienstes auftritt.

Technisch ist eine besondere Verschlüsselungsweise der Gespräche von VoIP-Telefon zu VoIP-Telefon zwar grds. möglich. Bereitgestellt wird dies

---

verstehen, gehört aber nicht zu dem Ermittlungsinstrument der Quellen-TKÜ im technischen Sinne.

21 Strafprozessordnung i. d. F. der Bekanntmachung vom 07.04.1987 (BGBl. I S. 1074, ber. S. 1319).

22 In diese Richtung auch *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11.2010 und *Bär*, persönliches Gespräch mit dem Verfasser, Bamberg, 09.12.2010; für entsprechende rechtliche Verpflichtungen und Maßgaben zur Umsetzung von Überwachungsmaßnahmen für Provider bei Vorliegen der dort genannten Voraussetzungen, siehe § 100b III StPO, § 110 I S. 1 Nr. 1a, S. 2 TKG, § 3 II S. 3 TKÜV.

23 Telekommunikationsgesetz vom 22.06.2004 (BGBl. I S. 1190).

24 Vgl. hierzu auch BT-Drs. 16/2581, S. 28; vgl. insoweit auch *Klesczewski*, ZStW 2011, 737 (741).

25 *Session Initiation Protocol*, Signalisierungsprotokoll, welches Sitzungen zwischen zwei oder mehr Teilnehmern aufbauen, modifizieren und beenden kann, und damit wesentliches Protokoll für die Implementierung von VoIP, vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 212.

derzeit jedoch nur von wenigen Modellen. Die im Handel erhältlichen VoIP-Telefone unterstützen eine end-to-end-Verschlüsselung i. d. R. (noch) nicht.[26]

Eine Verschlüsselung der gesamten Anrufstrecke wäre zudem nur für die besagte Kommunikation von VoIP-Telefon zu VoIP-Telefon möglich – vorausgesetzt die verwendeten VoIP-Telefone beherrschen dieselbe Verschlüsselungstechnologie. Bei einer Verbindung vom VoIP-Telefon ins (analoge) Festnetz würde jedoch eine etwaige Verschlüsselung spätestens beim Übergang ins Festnetz enden, da ein diesbezüglich erforderliches „technologieübergreifendes" Verschlüsselungsverfahren derzeit noch nicht entwickelt ist. Die technischen Gegebenheiten sprechen deshalb dafür, dass sich auch diese Erscheinungsform von VoIP mittels „herkömmlicher" TKÜ in erfolgversprechender Weise auf der Transportstrecke abgreifen lässt.[27] Auch sie stellt daher keine in Bezug auf die Maßnahme der Quellen-TKÜ relevante VoIP-Kommunikationsform dar.

c) VoIP über Computer mittels VoIP-Software

Die VoIP-Telefonie über einen handelsüblichen Computer[28] mittels einer speziellen auf dem System installierten VoIP-Software („softwarebasierte VoIP") zur direkt verbundenen Kommunikation von Computer zu Computer („*peer-to-peer*"[29]) erfreut sich dank zahlreicher Vorteile wie weltweite, kos-

---

26 Vgl. http://www.testberichte.de/testsieger/level3_telefongeraete__isdn_internet_telefone_681.html (zuletzt aufgerufen 15.06.2012); http://de.wikipedia.org/wiki/SIP-Telefon (zuletzt aufgerufen 15.06.2012).

27 In diese Richtung auch *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11.2010 und *Bär*, persönliches Gespräch mit dem Verfasser, Bamberg, 09.12.2010; für entsprechende rechtliche Verpflichtungen und Maßgaben zur Umsetzung von Überwachungsmaßnahmen für Provider bei Vorliegen der dort genannten Voraussetzungen, siehe § 100b III StPO, § 110 I S. 1 Nr. 1a, S. 2 TKG, § 3 II S. 3 TKÜV; vgl. hierzu auch BT-Drs. 16/2581, S. 28; vgl. insoweit auch *Klesczewski*, ZStW 2011, 737 (741).

28 *Personal Computer* (PCs) als stationäre Geräte ebenso wie *Notebooks*/*Laptops* als mobile Geräte; für die praktische Ermittlungsarbeit v. a. bei einer Überwachungsmaßnahme auf mobilen Endgeräten ist hierbei zu beachten, dass für den Fall, dass sich das Gerät zum Zeitpunkt der Überwachung im europäischen Ausland befinden bzw. im Zeitraum der Überwachung dorthin verbracht worden sein sollte, nach Art. 20 des *Übereinkommens gemäß Artikel 34 des Vertrags über die Europäische Union über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union* (EU-RhÜbk) der betreffende Mitgliedstaat von der Überwachung zu unterrichten ist.

29 Auch „P2P": direkte Verbindung und Datenübertragung von Rechner zu Rechner (engl. „peers", z. Dt. „Gleichgestellte", „Gleichrangige") zur Kommunikation auf gleicher Stufe in einem Rechnernetzwerk, ohne Übermittlung der Daten über einen (zwischengeschalteten) Server wie bei einem „Server-Client-Modell", vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 180; *Bär*, TK-Überwachung, Glossar, S. 374.

tenlose[30] und (i. d. R.) verschlüsselte[31] Kommunikation stetig wachsender Beliebtheit. Als „technisches Equipment" (Hardware) neben der bei allen Nutzern installierten VoIP-Kommunikationssoftware benötigt der VoIP-Nutzer für softwarebasierte Internettelefonie lediglich einen eingeschalteten Computer inklusive vollduplex[32]-fähiger Soundkarte, Lautsprecher und Mikrofon bzw. Kopfhörer oder Kopfsprechhörer („Headset") sowie einen Internetzugang[33] mit aktiver Internetverbindung (i. d. R. über DSL-Anschluss). Hierüber kann bei einer entsprechenden Anwahl und einem Verbindungsaufbau über die aktiv geschaltete VoIP-Software zwischen den jeweiligen Gesprächsteilnehmern eine peer-to-peer-Verbindung zur (sprach- und/oder videobasierten) Kommunikation hergestellt werden.[34]

Hinsichtlich der technischen Abläufe[35] werden bei dieser VoIP-Kommunikation die Gesprächsinhalte als analoge Eingangssignale durch das Computer-Mikrofon aufgezeichnet und per Analog-Digital-Umsetzer in elektronische Signale umgewandelt (digitalisiert). Die digitalisierten Daten werden dann im nächsten Schritt in einzelne Datenpakete zerlegt, komprimiert, ggf. verschlüsselt und auf IP-Ebene über das Internet via Internetprotokoll zum Gesprächspartner übertragen. Im letzten Schritt werden die Datenpakete bei diesem wieder zusammengesetzt, in Sprache umgewandelt und über die Computer-Lautsprecher oder den angeschlossenen Kopfhörer ausgegeben.[36] Bei dieser Erscheinungsform der VoIP erfolgt die unmittelbare Übertragung

---

30 Ausgenommen Kosten für die Internetbenutzung.

31 Soweit von der jeweiligen VoIP-Software unterstützt.

32 Die *Vollduplex*-Technik ermöglicht eine Übertragung der digitalen Sprachsignale zwischen den Gesprächspartnern in beide Richtungen zur selben Zeit, die gleichzeitiges Hören und Sprechen zulässt (im Gegensatz zur *Halbduplex*-Technik, die jeweils nur das abwechselnde Hören oder Sprechen nacheinander gestattet wie bspw. oftmals bei Funkgeräten, und der *Simplex*-Technik wie bspw. bei TV- und Radioübertragungen), vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 253, 104, 211.

33 Bei stationärer Nutzung: i. d. R. Breitbandanschluss; bei mobiler Nutzung: WLAN-Karte und Access-Point mit Breitbandzugang; für die Grundfunktionalität (Sprachanrufe) von Skype wird ein Internetanschluss mit einer Mindestdatenübertragungsrate von 30 Kbit/s benötigt, weshalb ein Schmalbandanschluss technisch grds. ausreichend wäre; mittlerweile stellt jedoch auf Grund der zunehmenden Verbreitung von DSL-Anschlüssen der Breitband-Internetzugang mit Datenübertragungsraten weit über 128 Kbit/s den technischen Standard dar.

34 Vgl. auch *Bär*, Handbuch zur EDV-Beweissicherung, Rn. 121 ff.; ebenso Anm. *Bär*, MMR 2011, 691 (691) und Anm. *Bär*, MMR 2010, 267 (267).

35 Für Einzelheiten zu den technischen Vorgängen bei softwarebasierter VoIP, siehe 1. Teil A.I.4.

36 Vgl. zur Technik auch *Bär*, TK-Überwachung, § 100a StPO, Rn. 31; ders., Handbuch zur EDV-Beweissicherung, Rn. 121 ff.; auch Anm. *Bär*, MMR 2010, 267 (267) und Anm. *Bär*, MMR 2011, 691 (691).

der Datenpakete auf IP-Ebene über den Netzbetreiber (i. d. R. zugleich der Internet-Service-Provider).[37]

Zur Steuerung dieser Abläufe wird neben der erforderlichen Hardware eine spezielle VoIP-Software benötigt. Im Internet stehen eine Vielzahl derartiger Programme von verschiedenen Anbietern (nachfolgend *VoIP-Diensteanbieter*[38]) kostenlos zum Download bereit (z. B. *Skype, Google Talk, QuteCom* u. a.[39]) Die bekannteste und mit rund 560 Mio. Nutzern[40] weltweit am weitesten verbreitete Software ist die des Anbieters „*Skype*“[41].[42] Die Skype-Software verwendet ein eigenes („proprietäres“) Protokoll und ist daher nicht mit anderer Internettelefonie-Software kompatibel.[43] Besonderer Anreiz neben der Kostenfreiheit von internen Skype-zu-Skype-Anrufen und weltweiter Verfügbarkeit des Dienstes[44], ist die automatische „*end-to-end*“-*Verschlüsselung*[45] der Kommunikationsinhalte während der Übermittlung. Alle Skype-internen Audio- und Videogespräche von Computer zu Computer werden laut Unternehmensangaben automatisch durch einen sicheren skype-eigenen (proprietären) Verschlüsselungsalgorithmus nach dem *Advanced Encryption Standard (AES)* mit 256-Bit-Schlüssel vor un-

---

37 Für Einzelheiten zum Anteil des softwarebasierten VoIP-Diensteanbieters am Zustandekommen der Telekommunikation, siehe 2. Teil A.II.6.b).

38 Als Oberbegriff für die Anbieter von VoIP-Diensten in freier Begriffswahl und ohne Bezugnahme auf gesetzliche Begriffsbestimmungen, insbesondere des TKG.

39 Siehe zu weiteren vergleichbaren Programmen auch BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 32.

40 Vgl. http://diepresse.com/home/techscience/internet/560334/560-Mio-Nutzer_Skype-ist-groesser-als-Facebook- (zuletzt aufgerufen 15.06.2012); Simonite, http://www.heise.de/tr/artikel/Schau-mich-an-wenn-ich-mit-Dir-rede-1168389.html (zuletzt aufgerufen 15.06.2012); die angegebene Zahl dürfte aber auch Mehrfachanmeldungen enthalten und ist daher nicht absolut zu sehen.

41 Das Unternehmen „Skype“ mit Hauptsitz in Luxemburg wurde im Juli 2003 gegründet, im September 2005 von der eBay Inc. erworben und im Mai 2011 an die Microsoft Corp. verkauft; mit Abschluss der Übernahme im Oktober 2011, ist Skype nunmehr eine Tochtergesellschaft der Microsoft Corp., welche ihren Hauptsitz in den USA hat, vgl. http://de.wikipedia.org/wiki/Skype (zuletzt aufgerufen 15.06.2012); hierzu auch http://www.microsoft.com/germany/newsroom/pressemitteilung.mspx?id=533433 (zuletzt aufgerufen 15.06.2012); die Untersuchungen der vorliegenden Arbeit erfolgen größtenteils anhand von Skype als derzeit populärster VoIP-Software, lassen sich aber auf vergleichbare VoIP-Programme entsprechend übertragen.

42 Vgl. auch BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 107a.

43 Vgl. auch http://www.spiegel.de/netzwelt/tech/0,1518,434092,00.html (zuletzt aufgerufen 15.06.2012).

44 Vgl. http://www.skype.com/intl/de/features/allfeatures/skype-to-skype-calls/ (zuletzt aufgerufen 15.06.2012).

45 Generell zum Verfahren der „end-to-end“-Verschlüsselung, siehe *Silvan*/*Huber*, http://www.computerwoche.de/security/1894253/index3.html (zuletzt aufgerufen 15.06.2012).

befugten Zugriffen Dritter geschützt.[46] Die spezielle „end-to-end"-Verschlüsselung sorgt hierbei für eine verschlüsselte Direktübertragung zwischen den miteinander („peer-to-peer", P2P) verbundenen Gesprächspartnern vom Absenden der Daten bis zu deren Eingang beim anhand der angewählten Skype-Nummer eindeutig identifizierten Zielsystem. Von der Skype-Software automatisch gesteuert, erfolgt die Verschlüsselung lokal auf dem Computer des jeweiligen Absenders der Kommunikationsdaten, während die Entschlüsselung („Decodierung") erst auf dem Computer des jeweiligen Empfängers stattfindet. Dieser geschlossene Übermittlungsvorgang macht ein Ansetzen der Überwachungsmaßnahme noch vor der Verschlüsselung auf dem System des Absenders bzw. nach der Entschlüsselung auf dem System des Empfängers und mithin eine *Quellen-TKÜ* erforderlich, da ein Zugriff auf dem Übermittlungsweg den Ermittlungsbehörden nur kryptierte Daten liefern würde.[47]

Neben dem kostenlosen softwarebasierten P2P-VoIP-Dienst, mit dem die Nutzer untereinander per Sprach- und Videotelefonie kommunizieren können (Skype „Basis-Dienst"), bietet das Unternehmen Skype als einen zusätzlichen, entgeltlichen VoIP-Dienst auch das Führen von Telefonaten zwischen Computer und Anschlüssen im öffentlichen Telefonnetz (Festnetz/PSTN und Mobilfunknetz) an[48]:

Der sog. *SkypeOut-Dienst* ermöglicht es hierbei seinen Nutzern, zu einem bestimmten Minutentarif[49], der über vorher aufgeladenes Guthaben abgerechnet wird, direkt vom Computer aus über die Skype-Software Telefonate ins öffentliche Festnetz und Mobilfunknetz zu führen.

Beim sog. *SkypeIn-Dienst*[50] werden Telefonate vom öffentlichen Netz in das IP-Netz zu Skype ermöglicht. Speziell für diesen Dienst erhält der Skype-Nutzer gegen Zahlung einer festen Monatsgebühr[51] eine eigene

---

46 Vgl. https://support.skype.com/de/faq/FA143/Ist-Skype-sicher?q=verschl%C3%BCsselung&fromSearchFirstPage=false (zuletzt aufgerufen 15.06.2012); https://support.skype.com/de/faq/FA31/Verwendet-Skype-Verschlusselung (zuletzt aufgerufen 15.06.2012).

47 Vgl. auch BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 107a; für Einzelheiten zur kriminalistischen Notwendigkeit der Quellen-TKÜ, siehe 1. Teil A.II.1.

48 Für weitere Einzelheiten, siehe auch 2. Teil A.II.6.b).

49 Vgl. http://www.skype.com/intl/de/features/allfeatures/call-phones-and-mobiles/ (zuletzt aufgerufen 15.06.2012).

50 Seit 2012 wird dieser Dienst von Skype auch als „Online-Nummer" bezeichnet, vgl. http://www.skype.com/intl/de/features/allfeatures/online-number/ (zuletzt aufgerufen 15.06.2012); http://de.wikipedia.org/wiki/Skype (zuletzt aufgerufen 15.06.2012).

51 Vgl. http://www.skype.com/intl/de/features/allfeatures/online-number/ (zuletzt aufgerufen 15.06.2012).

Skype-Telefonnummer[52], unter der er von herkömmlichen Telefonen oder von Mobiltelefonen aus angerufen werden kann. Derartige Anrufe „von außen" kann der Nutzer bei eingeschaltetem und mit dem Internet verbundenen Computer über das aktivierte VoIP-Programm, über das er bei Skype in seinen Account eingeloggt ist, annehmen.

Bei derartigen Gesprächen unter Beteiligung des öffentlichen Telefonnetzes können die Signale technisch bedingt nicht end-to-end-verschlüsselt übertragen werden.[53] Gespräche in das bzw. aus dem öffentlichen Telefonnetz können daher höchstens bis zu bzw. ab den Gateways, also den Schnittstellen zwischen Internet und Festnetz oder Mobilfunknetz, im Teilbereich des IP-Netzes verschlüsselt übertragen werden. Bei der Weiterleitung der mit Hilfe des Gateways in herkömmliche Signale „übersetzten" Datenpakete im öffentlichen Telefonnetz findet eine Verschlüsselung nicht statt.[54] Eine solche kommt bereits deshalb nicht in Betracht, da ein herkömmliches Telefon, schon nicht die technischen Möglichkeiten aufweist, eine solche Verschlüsselung zu lesen und zu entschlüsseln.[55] Eine Überwachung derartiger „netzübergreifender" Internettelefonate kann daher (technisch) i. d. R. über eine „klassische" TKÜ nach §§ 100a, 100b StPO realisiert werden, da sich die Kommunikationsdaten jedenfalls auf demjenigen Teilstück des Übertragungsweges, das sich im öffentlichen Leitungsnetz befindet, also zwischen Gateway und PSTN-Endgerät oder Mobiltelefon, in unverschlüsseltem Zustand durch Ansetzen am Gateway oder an den leitungsvermittelnden Netzeinrichtungen abgreifen und ausleiten lassen[56]. Einer besonderen Maßnahme wie der Quellen-TKÜ bedarf es daher zur

---

52 Derzeit kann ein Nutzer bis zu 10 *SkypeIn*-Nummern für seinen Skype-Account registrieren lassen; derartige *SkypeIn*-Nummern sind gegenwärtig u. a. in Deutschland, den USA, Großbritannien, Frankreich, Polen, Dänemark, Finnland, Schweden, Polen, der Schweiz, Estland, Hongkong, Australien, Brasilien und Japan verfügbar, vgl. http://www.skype.com/intl/de/features/allfeatures/online-number/ (zuletzt aufgerufen 15.06.2012); https://support.skype.com/de/faq/FA256/Wie-richte-ich-meine-Online-Nummer-ein?fromSearchFirstPage=false (zuletzt aufgerufen 15.06.2012).

53 Vgl. https://support.skype.com/de/faq/FA31/Verwendet-Skype-Verschlusselung (zuletzt aufgerufen 15.06.2012).

54 Vgl. auch *Bär*, Handbuch zur EDV-Beweissicherung, Rn. 125.

55 Vgl. http://www.voip-information.de/skype-sicherheit.html (zuletzt aufgerufen 15.06.2012).

56 In diese Richtung auch die Antwort des Parl. Staatssekretärs beim Bundesminister des Innern, *Bergner*, für die Bundesregierung im Rahmen der 135. Sitzung des Deutschen Bundestags am 26.10.2011, BT-PlPr. 17/135 16064 D; hierauf weist auch Skype in seiner Stellungnahme an die Bundesnetzagentur aus dem Jahr 2004, S. 3, hin, abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Stellungnahmen/SkypeTechnologiesId714pdf.pdf?__blob=publicationFile (zuletzt aufgerufen 15.06.2012).

Überwachung von netzübergreifender Internettelefonie (z. B. *SkypeIn*/*SkypeOut*) nicht.

d) VoIP über Mobiltelefon/PDA/Smartphone

Bereits seit 2004 ist die Skype-Software in modifizierter Form auch für mobile internetfähige Geräte wie bspw. bestimmte PDAs[57] verfügbar[58] und unterstützt seit 2008 auch die mobile Nutzung des Skype-Dienstes auf einigen internetfähigen Mobiltelefonen[59]. Seit 2010 ist nun auch eine Skype-Software zur mobilen Nutzung des Dienstes, insbesondere der Videotelefonie, für bestimmte Smartphones[60] erhältlich.[61]

Wie ein Computer verfügen diese modernen mobilen Endgeräte über ein Betriebssystem, welches das Ausführen von Programmen und Prozessen ermöglicht.[62] Ermöglichen sie daneben auch einen Zugang ins Internet, so besteht auch hier die Möglichkeit mittels spezieller VoIP-Software zwischen mobilen Endgeräten (i. d. R. kostenlos[63]) Sprach- und/oder Videotelefonie

---

[57] *Personal Digital Assistent*, tragbarer digitaler Organizer (Kleinstcomputer) im Format eines Taschenrechners, zumeist mit Mobiltelefoniefunktion, vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 179.

[58] Für PDAs über die„Skype for Pocket-PC-Software“ bereits seit September 2004 mit Version 1.0 und seit Februar 2006 mit der Version 2.0, vgl. http://about.skype.com/2004/09/skype_for_pocket_pc_version_10.html (zuletzt aufgerufen 15.06.2012); http://blogs.skype.com/en/2006/02/skype_for_pocket_pc.html (zuletzt aufgerufen 15.06.2012).

[59] Vgl. http://about.skype.com/2008/04/skype_tests_software_for_massm.html (zuletzt aufgerufen 15.06.2012); zu Internet-Telefondiensten über internetfähige Mobilfunkgeräte, siehe auch die Ausführungen von *Buermeyer*/*Bäcker*, HRRS 2009, 433 (434), Fn. 5.

[60] Eine Art Kombination aus Mobiltelefon und PDA, welches umfassende Nutzungsmöglichkeiten eröffnet, d. h. neben dem Telefonieren u. a. auch E-Mail-Kommunikation, Instant Messaging, Internetsurfen sowie zahlreiche Organizer-Funktionen, vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 215.

[61] Seit Oktober 2010 ist eine offizielle Skype-Version für Smartphones mit Android-Betriebssystemen sowie seit Dezember 2010 auch für das iPhone 4 und weitere mobile Endgeräte verfügbar, vgl. http://www.heise.de/newsticker/meldung/Telefonie-Software-Skype-fuer-Android-Handys-1101618.html (zuletzt aufgerufen 15.06.2012); http://about.skype.com/press/2010/12/iphone_video_calls.html (zuletzt aufgerufen 15.06.2012); hierzu auch http://www.skype.com/intl/de/get-skype/on-your-mobile/download/ (zuletzt aufgerufen 15.06.2012).

[62] Vgl. auch *Sieber*, Stellungnahme zu dem Fragenkatalog des BVerfG in dem Verfahren 1 BvR 370/07, S. 9, abrufbar unter http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf (zuletzt aufgerufen 15.06.2012).

[63] Vgl. http://www.skype.com/intl/de/get-skype/on-your-mobile/download/ (zuletzt aufgerufen 15.06.2012); http://www.skype.com/intl/de/get-skype/on-your-mobile/ (zuletzt aufgerufen 15.06.2012).

sowie Instant Messaging über das IP-Netz zu führen. Sofern über diese Geräte und der darauf installierten Software auch eine end-to-end-verschlüsselte Kommunikation hergestellt werden kann[64], wäre auch hier der technische Anknüpfungspunkt für eine Infiltration des Systems zum Abgreifen von Daten an der Quelle gegeben.[65]

Bei der hiervon zu unterscheidenden, oben dargestellten Nutzung von Skype zur netzübergreifenden Kommunikation (vom öffentlichen Mobilfunknetz ins IP-Netz und umgekehrt) zwischen Mobiltelefon/PDA/Smartphone und softwaregesteuertem Computer (z. B. *SkypeIn*/*SkypeOut*[66]), also über die normale Mobiltelefonnummer und ohne spezielle auf dem Mobiltelefon/PDA/Smartphone installierte Software, wird das Telefonat im Mobilfunknetz als normaler Sprachanruf getätigt und erst durch eine Gateway in der Vermittlungsstelle des Mobilfunknetzes bzw. des IP-Netzes die Verbindung zwischen Mobilfunknetz und dem IP-Netz hergestellt. Die Nutzung netzübergreifender VoIP-Dienste ist jedoch – wie oben bereits näher erläutert – im Regelfall nicht in besonderer Weise vor dem Zugriff Dritter geschützt. Denn wegen der Beteiligung des öffentlichen Telefonnetzes (Festnetz und Mobilfunknetz) an dem Gespräch, findet eine geschlossene „end-to-end"-Verschlüsselung nicht statt.[67] Aus diesem Grunde stellt sich bei der netzübergreifenden Kommunikation zwischen Computer und Mobiltelefon/PDA/Smartphone auch nicht das Bedürfnis für eine Ermittlungsmaßnahme der Quellen-TKÜ wie bei end-to-end-verschlüsselter Kommunikation von Computer zu Computer.

Die eher neuere Variante[68] der *softwarebasierten* Nutzung von mobilen internetfähigen Endgeräten zur (i. d. R. kostenlosen) VoIP-Kommunika-

---

64 Was bei einer reinen Beteiligung des IP-Netzes technisch realisierbar sein dürfte.

65 In diese Richtung auch *Sieber*, Stellungnahme zu dem Fragenkatalog des BVerfG in dem Verfahren 1 BvR 370/07, S. 9, abrufbar unter http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf (zuletzt aufgerufen 15.06.2012); für die praktische Ermittlungsarbeit ist zu beachten, dass für den Fall, dass sich das mobile Gerät zum Zeitpunkt der Überwachung im europäischen Ausland befinden bzw. im Zeitraum der Überwachung dorthin verbracht werden sollte, gemäß Art. 20 des *Übereinkommen gemäß Artikel 34 des Vertrags über die Europäische Union über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union* (EU-RhÜbk) der betreffende Mitgliedstaat von der Überwachung zu unterrichten ist.

66 Für Einzelheiten zu den kostenpflichtigen Diensten *SkypeIn* und *SkypeOut*, siehe 1. Teil A.I.2.c).

67 Vgl. https://support.skype.com/de/faq/FA31/Verwendet-Skype-Verschlusselung (zuletzt aufgerufen 15.06.2012).

68 Eine optimale Nutzung der mobilen VoIP-Dienste vor allem in Hinblick auf Bedienkomfort und Datenübertragungsgeschwindigkeit dürften vor allem die sich in den letzten Jahren zunehmend verbreitenden Smartphones ermöglichen.

tion[69] kommt zwar bei einer stattfindenden end-to-end-Verschlüsselung der Datenpakete auf der Übermittlungsstrecke auch für Maßnahmen des Ansetzens „an der Quelle“ in Betracht, spielt auf Grund ihres derzeitigen geringen Anteils an der Gesamtnutzung der von Anbietern wie Skype bereitgestellten VoIP-Dienste in der Ermittlungspraxis gegenwärtig (noch) eine untergeordnete Rolle.[70] In rechtlicher Hinsicht ergeben sich hierfür jedenfalls dieselben Anforderungen und Problemstellungen wie bei verschlüsselter VoIP-Kommunikation über den Computer.

e) Video-Internettelefonie („Video-over-IP“)

Viele der softwarebasierten Internettelefonie-Dienste bieten (ggf. kostenpflichtig) neben der Übertragung der *Sprach*signale via IP-Protokoll die simultane Übertragung des *Video*signals, welches mittels Webcam erzeugt wird, an. Nutzern bietet sich somit je nach verwendetem Dienst die Möglichkeit, zwischen dem Führen einer reinen Sprach-Internettelefonie und einer Sprach-/Bild-Internettelefonie auszuwählen.

Mit Skype-Version 2.0 wurde im Januar 2006 eine Funktion zur Videotelefonie in die Skype-Software integriert.[71] Diese ermöglicht zusätzlich zur Sprachkommunikation auch die Übertragung eines Videosignals in Echtzeit. Erforderlich hierfür ist neben der Software eine an den Computer angeschlossene betriebsbereite Webcam. Auch die Übertragung des Videosignals ist von der speziellen AES-Verschlüsselung der Skype-Software mitumfasst.[72] Demnach wäre auch hier zu Ermittlungszwecken ein Anknüpfen und entsprechendes Abgreifen der Videodaten „an der Quelle“ veranlasst, um diese zusammen mit den Sprachsignalen in unverschlüsselter Form erfassen zu können.

Aus technischer Sicht dürfte die entsprechende Anpassung und Konfiguration der Überwachungssoftware zur „Live-Ausleitung“ auch der Videosignale der geführten Internettelefonie bei ausreichend großer Bandbreite (Übertragungsrate) für die Datenübertragung wohl ohne weiteres möglich sein.[73]

---

[69] Gemeint ist also nicht die „normale“ Mobiltelefonie über das Mobilfunknetz.

[70] In diese Richtung *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11.2010.

[71] Vgl. http://de.wikipedia.org/wiki/Skype (zuletzt aufgerufen 15.06.2012); http://www.skype.com/intl/de/support/user-guides/call-with-video/ (zuletzt aufgerufen 15.06.2012).

[72] Vgl. https://support.skype.com/de/faq/FA31/Verwendet-Skype-Verschlusselung (zuletzt aufgerufen 15.06.2012).

[73] Vgl. auch die Angaben einer im Internet veröffentlichten Leistungsbeschreibung einer Überwachungssoftware, abrufbar unter http://wiki.piratenpartei.de/wiki/

Aus rechtlicher Sicht stellen sich für die Überwachung der im Rahmen einer Video-Internettelefonie ausgetauschten Videosignale dieselben Fragen wie bei der Überwachung der Sprachsignale der geführten Internettelefonie.[74]

Da Kommunikation auch über visuelle Inhalte betrieben werden kann, handelt es sich bei Video-Internettelefonie um einen Austausch von als Nachrichten identifizierbaren Video- und Sprachsignalen (*audiovisuelle Inhalte*) via Telekommunikationsanlagen und mithin um Telekommunikation i. S. d. § 3 Nr. 22 TKG.[75] Auch die Videosignale, sprich die visuellen Inhalte der Kommunikation, sind Bestandteile des bei einer Video-Internettelefonie anfallenden und ausgetauschten Datenmaterials.[76] Somit ist auch der Zugriff auf die unverschlüsselten Videosignale[77] an der Quelle mittels der besonderen Ermittlungsmaßnahme der Quellen-TKÜ allein am Fernmeldegeheimnis aus Art. 10 I GG zu messen, sofern – in Einklang mit den Vorgaben des BVerfG[78] – durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt ist, dass ausschließlich Daten aus laufenden Telekommunikationsvorgängen von der Überwachungsmaßnahme erfasst werden.[79]

Streng zu unterscheiden ist die Überwachung und Aufzeichnung der Videosignale einer stattfindenden Internettelefonie allerdings von der Anfertigung sog. *Screenshots*, also dem „Ablichten" (Kopieren) und Speichern des im Zeitpunkt des Screenshots *aktuellen/aktiven grafischen Bildschirminhaltes* als Grafikdatei(en). Das heimliche Anfertigen derartiger „Bildschirmablichtungen" (auch „Bildschirmfotografien") stellt eine Maßnahme zur Überwachung von Datenverarbeitungsvorgängen, welche nicht der Telekommunikation dienen, dar und ist im Rahmen von (Quellen-)TKÜ-Maßnahmen,

---

images/5/54/Bayern-skype-tkue.pdf (zuletzt aufgerufen 15.06.2012), S. 5; siehe zu dieser Quelle auch 1. Teil A.II.3.a).

74 Es kann deshalb insoweit auf die Ausführungen der vorliegenden Arbeit zur (technischen und rechtlichen) Überwachbarkeit der VoIP-Sprachtelefonie entsprechend verwiesen werden.

75 Vgl. Ausführungen zur Überwachung der Sprachsignale von Internettelefonie entsprechend.

76 So auch LG Hamburg, MMR 2011, 693 (693 f.).

77 Hierzu zählen unter entspr. Berücksichtigung der Rspr. zu Hintergrundgeräuschen (vgl. BGH NStZ 2008, 473, 474; BGH NStZ 2003, 668, 669), wonach auch Hintergrundgeräusche und -gespräche während eines Telefonats Teil der Telekommunikation sind und damit zulässiger Gegenstand einer TKÜ sein können, wohl auch Hintergrundbilder, also die Abbildung von Teilen der Räumlichkeiten, in denen die Video-Internettelefonie abläuft.

78 Vgl. BVerfG NJW 2008, 822 (826).

79 Vgl. zutr. LG Hamburg, MMR 2011, 693 (693 f.); auch BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 107c; die Ausführungen zum Zugriff auf Sprachsignale der Internettelefonie gelten insoweit entsprechend.

die das Überwachen und Aufzeichnen von Telekommunikation zum Gegenstand haben, unzulässig[80]. Eine solche Maßnahme wäre nur über eine – von der Quellen-TKÜ streng zu unterscheidende – Maßnahme der sog. Online-Durchsuchung in Form der Online-Überwachung realisierbar, die gegenwärtig jedoch in den bestehenden Regelungen der Strafprozessordnung keine Rechtsgrundlage findet.[81] Ein solches (de lege lata unzulässiges) Anfertigen heimlicher Ablichtungen des grafischen Bildschirminhalts stellt das Abgreifen und Aufzeichnen der im Rahmen einer laufenden Internettelefonie anfallenden Videosignale gerade nicht dar. Auch von der Eingriffsintensität sowie dem Maßnahmegegenstand ist die (Quellen-)TKÜ-Maßnahme als Maßnahme zur Überwachung der (Video-)Signale einer laufenden Video-Audio-Internettelefonie nicht mit einer derartigen Maßnahme vergleichbar.

f) Nachrichtensofortversand („Instant Messaging-over-IP")

VoIP-Programme bieten neben Sprachtelefonie i. d. R. auch eine Reihe weiterer Dienste zur Kommunikation über das IP-Netz an. Hierzu zählt regelmäßig auch die Möglichkeit zur Übertragung von Textnachrichten in Echtzeit im Rahmen der Nutzung einer speziellen Dienstfunktion zum sofortigen („instant") Nachrichtenversand und -empfang (sog. *Instant Messaging*).

Auch zu den Basisfunktionalitäten der Skype-Software zählt eine solche Instant Messaging-Funktion („*Skype Instant Messenger*"), also das direkte Kommunizieren von Skype-Nutzern über Textnachrichten mittels Nachrichtensofortversandes („Chatten").[82] Beim Instant Messaging sind die Computer der Teilnehmer bei aktivierter Software direkt und zeitgleich[83] miteinander verbunden, wodurch die Textnachricht nach Betätigung des „Versende-

---

[80] So zutr. auch das LG Landshut mit Beschluss vom 20.01.2011, MMR 2011, 690 (691) zum Anfertigen von Screenshots im Rahmen des Vollzugs eines (Quellen-)TKÜ-Beschlusses, bei dem im zeitlichen Abstand von 30 Sekunden zum Zwecke der Überwachung der Eingaben im Rahmen des Eintippens von Textnachrichten (vor Betätigung des „Versende-Buttons" und damit noch vor Aussenden der Textnachricht) Ablichtungen von der Bildschirmoberfläche gefertigt wurden; hierzu auch zutr. Anm. *Brodowski,* JR 2011, 533 (536); für weitergehende Einzelheiten, siehe auch 2. Teil A.II.4.

[81] So jedenfalls der 3. Strafsenat des Bundesgerichtshofs, Beschluss vom 31.01. 2007, BGH NJW 2007, 930; für Einzelheiten, siehe auch 1. Teil A.II.2.a).

[82] Vgl. http://de.wikipedia.org/wiki/Skype (zuletzt aufgerufen 15.06.2012); http://www.skype.com/intl/de/features/allfeatures/instant-messaging/ (zuletzt aufgerufen 15.06.2012).

[83] Insoweit im Unterschied zu E-Mail-Diensten, bei denen der Austausch gerade zeitversetzt erfolgt.

Buttons“ unmittelbar beim Empfänger ankommt und eine Echtzeitkommunikation ermöglicht wird.[84] Wie bei Skype-internen Audio- und Videotelefonaten werden auch beim Instant Messaging die Textnachrichten mit einem sicheren und leistungsstarken Verschlüsselungsalgorithmus verschlüsselt über das IP-Netz übertragen[85].

Die besondere Verschlüsselung würde für die Durchführung einer Überwachungsmaßnahme konsequenterweise auch hier ein Ansetzen „an der Quelle“ erforderlich machen. Der Zugriff auf die unverschlüsselten Instant Messaging-Daten dürfte in technischer Hinsicht ebenfalls realisierbar sein.[86] Eine Überwachungssoftware ließe sich demnach in ähnlicher Weise für die „Live-Ausleitung“ des Chatverkehrs konfigurieren, wie es im Rahmen der Überwachung von verschlüsselter Internettelefonie für die Ausleitung von Gesprächsdaten[87] stattfindet. Der Fokus der Quellen-TKÜ richtet sich in der Ermittlungspraxis dennoch schwerpunktmäßig auf Internettelefonie als Überwachungsgegenstand[88]. Aus rechtlicher Sicht stellen sich jedenfalls grds. dieselben Fragen.[89]

Eine weitere Konstellation von Messaging[90] über das IP-Netz ist das Versenden von Fax-Nachrichten über das Internet, das sog. *Fax-over-IP* („FoIP“). Bei der Übermittlung von Textnachrichten mittels FoIP gibt es eine Reihe technischer Schwierigkeiten, die einer umfassenden Etablierung dieser Technik bislang entgegenstanden. Während ein herkömmliches Fax über analoge Geräte relativ zuverlässig über den Sprachkanal des normalen Telefonnetzes übertragen werden kann, ist dies bei einem Fax über den Sprachkanal des IP-Netzes ohne weiteres nicht der Fall. So kann bspw. der Verlust einzelner Datenpaketen, der bei VoIP-Telefonaten bis zu einer gewissen Verlustrate für das Gehör kaum wahrnehmbar ist, bei Fax-Übermitt-

---

84 Vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 117; http://de.wikipedia.org/wiki/Instant_Messaging (zuletzt aufgerufen 15.06.2012).

85 Vgl. https://support.skype.com/de/faq/FA31/Verwendet-Skype-Verschlusselung (zuletzt aufgerufen 15.06.2012); http://de.wikipedia.org/wiki/Skype (zuletzt aufgerufen 15.06.2012).

86 Vgl. auch die Angaben einer im Internet veröffentlichten Leistungsbeschreibung einer Überwachungssoftware, abrufbar unter http://wiki.piratenpartei.de/wiki/images/5/54/Bayern-skype-tkue.pdf (zuletzt aufgerufen 15.06.2012), S. 5; siehe zu dieser Quelle auch 1. Teil A.II.3.a).

87 Für Einzelheiten zum technischen Ablauf bei der Überwachung von Internettelefonie, siehe 1. Teil A.II.3.a) u. b).

88 Siehe auch 1. Teil A.I.3.

89 Insbesondere da die Textnachricht erst nach Betätigung des „Versende-Buttons“ abgegriffen werden dürfte, weil erst dann ein unumkehrbar eingeleiteter Telekommunikationsvorgang vorliegt.

90 Wenn auch nicht „instant“.

lungen zu einem sofortigen Verbindungsabbruch führen.[91] Zur Behebung diverser Übertragungsprobleme wurden die Übermittlungsstandards T.37 und T.38 eingeführt. Beim (wenig verbreiteten) T.37-Standard wird das Fax einfach als Anhang per E-Mail übermittelt, während beim T.38-Standard Faxe mittels eines eigenständigen Protokolls mit eigenem Paketformat über das Internet versendet werden.[92] Um ein mit dem T.38-Standard über das IP-Netz versendetes Fax an ein herkömmliches Faxgerät im normalen Telefonnetz übermitteln zu können, sind auch hier entsprechend zwischengeschaltete Gateways erforderlich, da beide Übertragungswege nicht kompatibel sind.[93] Trotz technischer Verbesserungen und bereits erschienener erster Kombinationsgeräte[94] von VoIP- und FoIP-Kommunikation steckt diese Technologie noch im Entwicklungsstadium. Gar eine „end-to-end"-Verschlüsselung der Kommunikation mittels Fax über das Internet ist hierbei noch Zukunftsmusik.

3. Gegenstand der Quellen-TKÜ: Verschlüsselte VoIP von Computer zu Computer mittels VoIP-Software

Unter Berücksichtigung der technischen Besonderheiten der oben dargestellten unterschiedlichen Erscheinungsformen von IP-Kommunikation, stellt im Zusammenhang mit der Quellen-TKÜ die direkte, „end-to-end"-verschlüsselte IP-Kommunikation von Computer zu Computer („peer-to-peer") über das Internet mittels einer speziellen Kommunikationssoftware, welche von Anbieter wie Skype & Co regelmäßig kostenlos angeboten wird, den relevanten „Regel"-Überwachungsgegenstand dieses modernen Ermittlungsinstruments dar.[95] Die Besonderheit der hier automatisch erfol-

---

91 Vgl. http://www.voip-information.de/foip.php (zuletzt aufgerufen 15.06.2012).

92 Vgl. http://www.voip-information.de/foip.php (zuletzt aufgerufen 15.06.2012).

93 Vgl. http://de.wikipedia.org/wiki/T.38 (zuletzt aufgerufen 15.06.2012).

94 Z. B. Sagem IP-Phonefax 49A.

95 Zur Frage, ob die spezielle Konstellation der Durchführung eines Zugriffs mittels Überwachungssoftware zur Feststellung der vom Access-Provider zugeteilten dynamischen IP-Adresse nebst Zeitstempel als Verkehrsdatum bevor diese auf Grund der Nutzung eines *Anonymisierungsdienstes* anonymisiert wird (vgl. AG Hamburg, CR 2010, 249) einen Zugriff auf Daten aus einem laufenden Telekommunikationsvorgang und damit eine taugliche Konstellation der Quellen-TKÜ darstellt, vgl. (zu Recht bezweifelnd) BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 107c sowie *Spoenle*, jurisPR-ITR 6/2010 Anm. 5; zur speziellen Konstellation des sog. „*Cloud-Computing*" (Abspeichern von Datenbeständen nicht mehr auf dem eigenen Rechner, sondern extern auf dem System eines Dienstleisters, welcher i. d. R. die Option der verschlüsselten Dateiübertragung und -speicherung anbietet) und zur Frage, ob hier ggf. ein weiter Telekommunikationsbegriff eine Quellen-TKÜ rechtfertigen könnte

genden Verschlüsselung der ausgetauschten Daten, welche jede Einsichtnahme während der Übermittlung grds.[96] unterbindet, macht den Zugriff „an der Quelle" erforderlich. Größte praktische Relevanz entfaltet hierbei der Zugriff auf (Sprach- bzw. Sprach/Video-)Internettelefonie.

Die nachfolgenden Erörterungen und dogmatischen Untersuchungen erfolgen schwerpunktmäßig bezogen auf die Erfassung der Sprachkommunikation via Internetprotokoll, also den Zugriff auf die Sprachsignale von softwarebasierter Voice-over-IP-Kommunikation, gelten für den Zugriff auf die Videosignale einer Sprach/Videokommunikation aber insoweit entsprechend.

4. Phasen und technische Vorgänge softwarebasierter VoIP

Für die softwarebasierte IP-Telefonie über das Internet lassen sich unter näherer Betrachtung der spezifischen (in Sekundenbruchteilen ablaufenden) technischen Vorgänge dieser modernen Kommunikationstechnik – zugunsten der anschließenden juristischen Analyse in vereinfachter Form – einzelne Phasen herausarbeiten, anhand derer insbesondere die spezifisch mit dem Aussenden und Empfangen verbundenen Vorgänge – hier am Bsp. der *Sprach*-Internettelefonie[97] – verdeutlicht werden können.

Zum Abhalten eines Gesprächsaustauschs über das „weltweite Datennetz" via VoIP bedarf es im Vorfeld zunächst der Herstellung einer Verbindung der beiden (potentiellen) Gesprächspartner mit dem Internet. Dies kann je nach verwendeter Technik vor der Anwahl oder auch zeitgleich mit der Anwahl der Kennung (i. d. R. VoIP-Nummer) des angerufenen Gesprächspartners im Rahmen der Ausführung der VoIP-Software geschehen. Des Weiteren erforderlich ist nämlich auch die Herstellung einer Verbindung der Gesprächspartner zu- bzw. miteinander, die während des gesamten Internettelefonats besteht. Handelt es sich um computergestützte Internettelefonie

---

oder ob die Maßnahme hierdurch „faktisch zu einer ‚mittelschweren' Online-Durchsuchung" ausgeweitet werden würde und unter diesem Gesichtspunkt speziell und getrennt von einer Quellen-TKÜ zu regeln wäre, vgl. (im Erscheinen) *Sieber,* Gutachten zum 69. Deutschen Juristentag 2012, D.II.1.b).

96 Anders eventuell, wenn ein Schlüssel zur Dechiffrierung vorhanden wäre; zur kontroversen Frage, ob für die Skype-Verschlüsselung überhaupt ein Schlüssel existiert und ob das Verschaffen des Schlüssels eine wirkliche Alternative zur Quellen-TKÜ und der damit verbundenen Einbringung einer Überwachungssoftware darstellt, siehe 2. Teil B.III.2.b)aa) sowie 3. Teil A.I.1.c).

97 Die Ausführungen gelten für Video-Internettelefonie jedoch insoweit entsprechend; für Einzelheiten zu Video-Internettelefonie siehe 1. Teil A.I.2.e).

mittels speziellen VoIP-Programms eines der unzähligen Anbieter von softwarebasierter VoIP wie *Skype*[98], *Google Talk, QuteCom* u. a.[99] (*VoIP-Diensteanbieter*[100]) bedarf es zur Herstellung der Verbindung zwischen den Gesprächspartnern einer Aktivschaltung des VoIP-Programms[101] auf beiden Rechnern bei bestehender Verbindung ins Internet sowie der Anwahl des gewünschten Gesprächspartners durch den Anrufenden und das Annehmen des Gesprächsgesuchs durch den Angerufenen, wodurch eine Verbindung zwischen den Gesprächspartnern aufgebaut wird[102], über die im Anschluss ein direkter (peer-to-peer-verbundener) Datenaustausch im Rahmen des Internettelefonates stattfindet.[103]

Im Rahmen des nachfolgenden vereinfachten Modells lassen sich die grundsätzlichen technischen Abläufe[104] des Sprachdatenaustauschs wie folgt skizzieren:

Am Anfang des eigentlichen Informationsaustauschs der Gesprächspartner steht im wahrsten sprichwörtlichen Sinne zunächst „das Wort". In einer ersten Phase werden die akustischen Signale der (laufenden) Sprache von dem Nutzer „in den Raum" entäußert (*„Emissionsphase"*) und diese über das Mikrofon oder den Kopfsprechhörer („Headset") des mit dem Empfängersystem über das Internet verbundenen Absendersystems als analoge Eingangssignale eingefangen. In Sekundenbruchteilen werden die analogen Eingangssignale mittels Analog-Digital-Umsetzer[105] in elektronische Signale

---

98 Skype stellt als gegenwärtig wohl populärstes VoIP-Programm eine kostenlose VoIP-Software zur Sprach- und/oder Videotelefonie zur Verfügung, die hierzu ein eigenes VoIP-Protokoll verwendet und mit Programmen anderer Anbieter grds. nicht kompatibel ist, siehe 1. Teil A.I.2.c).

99 Siehe zu weiteren vergleichbaren Programmen auch BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 32.

100 Als Oberbegriff für die Anbieter von VoIP-Diensten in freier Begriffswahl und ohne Bezugnahme auf gesetzliche Begriffsbestimmungen, insbesondere des TKG.

101 Das Skype-Programm ist i. d. R. so konfiguriert, dass es sich in das Autostart-Menü installiert und bei jedem Hochfahren des Computers selbständig aktiviert.

102 I. d. R mittels des Signalisierungsprotokolls *Session Initiation Protocol* (SIP), aber auch mittels proprietärer Protokolle (wie z. B. Skype); für Einzelheiten, siehe auch 2. Teil A.II.6.b).

103 Vgl. auch Anm. *Bär*, MMR 2011, 691 (691) und Anm. *Bär*, MMR 2010, 267 (267).

104 Vgl. allgemein zur Technik auch *Bär*, TK-Überwachung, § 100a StPO, Rn. 31 sowie ders., Handbuch zur EDV-Beweissicherung, Rn. 121 ff.; auch Anm. *Bär*, MMR 2010, 267 (267) und Anm. *Bär*, MMR 2011, 691 (691); des Weiteren auch LG Hamburg, MMR 2011, 693 (695).

105 Auch *Analog-Digital-Wandler*, setzt nach unterschiedlichen Methoden analoge Eingangssignale in digitale Daten um, die dann weiterverarbeitet oder gespeichert werden können, vgl. http://www.telkopedia.de/fachlexikon/fachlexikon/detail/0/glossary-detail/analog-digital-wandlung.html (zuletzt aufgerufen 15.06.2012).

umgewandelt und hierdurch in eine digitale Form überführt (*Umwandlungsvorgang*), sogleich an die jeweils verwendete aktiv geschaltete VoIP-Software weitergeleitet und von dieser – automatisiert gesteuert – in einzelne Datenpakete zerlegt, komprimiert (*Aufbereitungsvorgang*) und – wie etwa bei Skype – verschlüsselt[106] (*Verschlüsselungsvorgang*), mit einer Art Steuerungsinformation zur Adressierung der Datenpakete versehen[107] und aus dem Herrschaftsbereich des Absendersystems[108] in das IP-Netz entlassen/eingespeist (*„Aussendephase"*). Im (weltweiten) Datennetz werden die verschlüsselten Datenpakete dann durch den/die Netzbetreiber auf IP-Ebene direkt zum Gesprächspartner transportiert (*„Übermittlungsphase"*). Die Übermittlung der Telefonie-Datenpakete erfolgt hierbei in Echtzeit[109] auf Grundlage bestimmter Transportprotokolle[110]. Am Ende der Transportstrecke nach erfolgreichem Erreichen ihres adressierten „Bestimmungsortes" werden die verschlüsselten Datenpakete aus dem Datennetz wieder ausgeleitet und dem Empfangsgerät zugeleitet. Im Rahmen des Empfangens der als Nachrichten identifizierbaren Signale (*„Empfangsphase"*) werden die Datenpakete – wiederum automatisiert gesteuert von der aktiv geschalteten VoIP-Software – auf dem Empfängersystem, welches mit dem Absendersystem über das Internet weiterhin verbundenen ist, wieder entschlüsselt (*Entschlüsselungsvorgang*), dekomprimiert und zusammengesetzt (*Aufbereitungsvorgang 2*), mittels Digital-Analog-Umsetzer in analoge Sprachsignale rückumgewandelt (*Umwandlungsvorgang 2*) und an der Ausgabeschnittstelle, also entweder an den Computer-Lautsprechern oder an dem angeschlossenen Kopfhörer bzw. Kopfsprechhörer („Headset") bereitgestellt und ausgegeben. Je nach technischer Möglichkeit und Einrichtung wird die über VoIP geführte Kommunikation ggf. von den Gesprächspartnern[111] aufge-

---

106 Beim wohl bekanntesten VoIP-Programm Skype mit einem proprietären Verschlüsselungsalgorithmus nach dem *Advanced Encryption Standard (AES)*, siehe auch 1. Teil A.I.2.c).

107 Für Einzelheiten, siehe auch 2. Teil A.II.6.b).

108 Wegen der (i. d. R.) wechselseitigen/dynamischen Gesprächsführung im Rahmen eines Telefonats befinden sich die Gesprächspartner in einem ständigen Wechsel in der Rolle des Absenders und des Empfängers; aus Gründen der Übersichtlichkeit werden die technischen Vorgänge vereinfacht anhand einer einzelnen Signalübertragung erläutert.

109 In Echtzeit („Live"): wechselseitiger, zeitgleicher (simultaner) Datenaustausch im Moment des Entstehen der Kommunikationssignale während der laufenden Kommunikation.

110 I. d. R mittels des *Real-Time Transport Protocol* (RTP), aber auch mittels proprietärer Protokolle (wie z. B. Skype).

111 Bspw. mit der kostenlosen Software „Skype Call Recorder", http://voipcallrecording.com (zuletzt aufgerufen 15.06.2012).

zeichnet und abgespeichert. In diesem Fall schließt sich noch eine *„Speicherungsphase“*[112] an.

Mit der Abwahl der aktiven Verbindung zwischen beiden Gesprächspartnern erfolgt die Beendigung des VoIP-Gesprächs. Dies geschieht entweder durch Trennen der Internetverbindung bzw. bei VoIP-Programmen wie Skype[113] durch „virtuelles Auflegen“, indem das jeweilige Befehlsfeld zum Trennen der Verbindung angeklickt wird, wobei dann trotz Beendigung des VoIP-Dienstes ggf. noch einen Verbindung mit dem Internet bestehen wird, was jedoch ohne Auswirkung auf die nunmehr beendete VoIP-Kommunikation ist.

II. Quellen-TKÜ

1. Begriffserklärung und kriminalistische Notwendigkeit

Die Quellen-TKÜ ist ein modernes Ermittlungsinstrument, welches in direkter Weise mit der fortschreitenden technischen Entwicklung auf dem Telekommunikationsmarkt und der damit einhergehenden Erschwernis v. a. strafprozessualer Ermittlungstätigkeit korreliert. Die Quellen-TKÜ stellt hierbei eine Antwort auf die zunehmende Verbreitung solcher softwarebasierter VoIP-Kommunikation dar, bei welcher in technischer Hinsicht eine umfassende und automatisierte end-to-end Verschlüsselung[114] der ausgetauschten Kommunikationsdaten während des Übermittlungsvorgangs im Datennetz stattfindet, weshalb ein „klassisches“ Abgreifen der Daten auf dem Transportwege wenig erfolgversprechend ist.

Bei der verschlüsselten Internettelefonie über den Computer mittels Skype oder ähnlicher Programme lassen sich nämlich mit der „klassischen“ Realisierungsweise einer TKÜ keine brauchbaren Erkenntnisse hinsichtlich des Inhalts der geführten Kommunikation gewinnen. Die durchführende Behörde könnte zwar die durchgehenden Daten bei deren Übermittlung abgreifen bzw. sich von dem gemäß § 100b III S. 2 StPO i. V. m. § 110 I S. 1, II TKG, §§ 3 I, 5 II S. 1 TKÜV verpflichteten Netzbetreiber/Provider eine Kopie der von ihm transportierten Daten ausleiten lassen, hätte hiervon jedoch keinerlei Erkenntnisgewinn, da die Aufzeichnung nur die verschlüsselte Form der

---

112 Zum Schutz von nach Abschluss des Übertragungsvorgangs im Herrschaftsbereich eines Teilnehmers abgespeicherte Nachrichten durch das Grundrecht auf informationelle Selbstbestimmung, siehe BVerfG NJW 2006, 976.

113 Für Einzelheiten zu Skype und vergleichbaren VoIP-Programmen, siehe 1. Teil A.I.2.c).

114 Hierzu auch Anm. *Brodowski*, JR 2011, 533 (533).

Kommunikation erfassen würde und den Ermittlern lediglich eine Ansammlung kryptierter Daten liefern würde. Dieser Umstand machte es erforderlich, neue technische Wege beim Zugriff auf derart kodierte Daten und den darin enthaltenen Informationen zu gehen. Als taugliches Ermittlungsinstrument für den Zugriff auf verschlüsselte Internettelefonie hat sich die sog. *Quellen-Telekommunikationsüberwachung*, kurz „*Quellen-TKÜ*", erwiesen. Bei dieser Maßnahme erfolgt der Zugriff auf die Telekommunikationsdaten – wie der Name schon sagt – „an der Quelle", d. h. je nach Person des Überwachten entweder vor der Verschlüsselung der Inhaltsdaten auf dem System des Absenders oder nach deren Entschlüsselung auf dem System des Empfängers, da die Daten zu diesen Zeitpunkten noch bzw. wieder im „Klartext" bzw. – genauer – im „Klarton" vorliegen.[115] Hierfür wird mittels einer heimlich bzw. verdeckt[116] auf dem jeweiligen Zielcomputer aufgespielten *Überwachungssoftware* die laufende Kommunikation vor deren Verschlüsselung bzw. nach deren Entschlüsselung in Echtzeit abgegriffen, auf einen speziellen Server[117] ausgeleitet und von der durchführenden Behörde entweder direkt ausgewertet oder ggf. an ermittelnde Behörden (z. B. Polizeidienststelle) weitergeleitet.[118]

Ziel einer Quellen-TKÜ ist der Zugriff auf die Daten des jeweiligen Telekommunikationsvorgangs in unverschlüsselter, sprich in einsehbarer Form, und damit letztlich die Erlangung von (beweisverwertbaren) Erkenntnissen zur Verfolgung und Aufklärung von Straftaten. Wesentlicher Gegenstand der Ermittlungsmaßnahme sind hierbei im Regelfall die *Inhalte* der geführten VoIP-Kommunikation. Wie bei herkömmlichen TKÜ-Maßnahmen können daneben im Rahmen einer Quellen-TKÜ aber auch die näheren Umstände

---

115 Vgl. Bundesministerium des Innern, Fragenkatalog BMJ, S. 8, 9, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012); *Gercke*/*Brunst*, Internetstrafrecht, Kap.5, S. 347, Rn. 885.

116 Der Begriff „verdeckt" wird oftmals synonym mit dem Begriff „heimlich" verwendet (i. S. v. „ohne Wissen des Betroffenen"); dies entspricht auch der üblichen Terminologie in Rspr. und Schrifttum; bei strenger Begriffsauslegung beschreibt der Begriff der „Verdecktheit" indes eher den Umstand, dass der Betroffene zwar die (sichtbaren) Handlungen/Auswirkungen der Maßnahmeumsetzung mitbekommt, den dahinter stehenden tatsächlichen (ermittlungstaktischen) Anlass/Zweck aber nicht erkennt (bspw. durch das Handeln der Ermittlungspersonen unter einem bestimmten Vorwand und/oder Anwendung einer Legende), während der Begriff der „Heimlichkeit" hingegen eher auf eine völlige Unkenntnis des Betroffenen vom Ablaufen einer Maßnahme ihm gegenüber überhaupt hindeutet.

117 I. d. R. ein von der durchführenden Behörde zu Zwecken der Überwachung eigens eingerichteter Server.

118 Für Einzelheiten zum technischen Ablauf, siehe 1. Teil A.II.3.a).

der Telekommunikation (Verkehrsdaten i. S. d. § 3 Nr. 30 TKG, § 96 I, *§ 113a*[119] TKG)[120] im Fokus der Überwachung stehen.[121]

Technisch durchgeführt werden TKÜ-Maßnahmen, präventive wie repressive, i. d. R. von speziellen Abteilungen, sog. *TKÜ-Kompetenzzentren*[122], welche bei den Landeskriminalämtern angesiedelt sind. In Bayern ist dies bspw. das „Kompetenzzentrum TKÜ" beim Bayerischen Landeskriminalamt (BayLKA), welches u. a. sämtliche richterlichen Beschlüsse nach §§ 100a, 100b StPO (Überwachung der Telekommunikation) zentral für Bayern, sämtliche Beschlüsse nach § 100g StPO (Erhebung von Verkehrsdaten) zentral für Bayern und sämtliche Beschlüsse nach § 100i StPO (Maßnahmen bei Mobilfunkendgeräten, sog. IMSI-Catcher) sowie diesbezügliche Peripheriemaßnahmen (Begleitmaßnahmen/Sekundärmaßnahmen) umsetzt.[123]

Angaben zur Anordnungs- und Durchführungshäufigkeit pro Jahr lassen sich nur schwer machen, da Maßnahmen der Quellen-TKÜ in den Statistiken der Bundes- bzw. Landesbehörden nicht separat ausgewiesen werden. Soweit die Quellen-TKÜs im repressiven Bereich auf die §§ 100a, 100b

---

119 Mit Entscheidung des BVerfG vom 02.03.2010, BVerfG NJW 2010, 833, wurde festgestellt, dass § 113a TKG in seiner bisherigen Form gegen Art. 10 I GG verstößt und nichtig ist.

120 Vgl. Löwe-Rosenberg – *Schäfer*, StPO und GVG, Zweiter Band, § 100a StPO, Rn. 47.

121 Vgl. auch *Sieber*, Stellungnahme zu dem Fragenkatalog des BVerfG in dem Verfahren 1 BvR 370/07, S. 3, abrufbar unter http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf (zuletzt aufgerufen 15.06.2012); zur speziellen Konstellation der Durchführung eines Zugriffs mittels Überwachungssoftware zum Zwecke der Ermittlung der vom Access-Provider zugeteilten IP-Adresse nebst Zeitstempel bei der Nutzung eines Anonymisierungsdienstes, vgl. insoweit AG Hamburg, CR 2010, 249, wobei diesbezüglich zu Recht bezweifelt wird, ob in solchen Fällen, also zur bloßen Ermöglichung der Feststellung einer dynamischen IP-Adresse als Verkehrsdatum vor deren Anonymisierung, überhaupt ein Zugriff auf Daten aus einen laufenden Telekommunikationsvorgang vorliegt und ein Fall der Quellen-TKÜ überhaupt gegeben ist, vgl. hierzu BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 107c und *Spoenle*, jurisPR-ITR 6/2010 Anm. 5; die restriktive Lösung des AG in Bezug auf das Vorliegen einer Annexkompetenz für die Begleitmaßnahmen der Quellen-TKÜ stellt jedenfalls nicht das einzig vertretbare Auslegungsergebnis dar, vgl. auch *Kudlich*, JA 2010, 310 (312); zur Frage des Vorliegens einer Annexkompetenz, siehe 2. Teil B.III.

122 Bspw. in Bayern das seit 2006 existierende „Kompetenzzentrum TKÜ" beim Bayerischen Landeskriminalamt, in Baden-Württemberg die „Inspektion Technische Einsatzunterstützung und Service (TEUS)" beim Landeskriminalamt Baden-Württemberg, in Rheinland-Pfalz das „Kompetenzzentrum für TKÜ (PG TKÜ-CC)" beim Landeskriminalamt Rheinland-Pfalz sowie in Nordrhein-Westfalen das Mitte 2011 gegründete „Cybercrime-Zentrum" beim Landeskriminalamt Nordrhein-Westfalen.

123 *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11. 2010.

StPO gestützt werden[124], fließen diese in die jährlichen Statistiken[125] zu den durchgeführten Telekommunikationsüberwachungen nach §§ 100a, 100b StPO mit ein. Unter Würdigung der Angaben von offizieller Seite dürfte sich deren Zahl – verglichen mit der Gesamtzahl an TKÜ-Maßnahmen – (noch) in einem überschaubaren Rahmen bewegen. Die Anordnungstendenzen divergieren hierbei von Bundesland zu Bundesland. So wurden bspw. in Bayern – das mit 1.341 Verfahren mehr als ein Fünftel der Verfahren, in denen im Berichtsjahr 2010[126] Maßnahmen nach § 100a I StPO angeordnet wurden (insgesamt 5.493), auf sich verzeichnet – seit Einführung der Berichtspflichten nach § 100b V und VI StPO zum 01.01.2009 insgesamt 22 Maßnahmen mit Quellen-TKÜ-Software durch das BayLKA im Rahmen von Ermittlungsverfahren erfasst.[127] Auch in anderen Bundesländern zählten in der jüngeren Vergangenheit Maßnahmen der Quellen-TKÜ zum Ermittlungsrepertoire.[128] In manchen Bundesländern wiederum bestünden zum Teil noch keine[129] bzw. nur wenige[130] praktische Erfahrungen mit präventiven und/oder repressiven Quellen-TKÜ-Maßnahmen.

Die Quellen-TKÜ gliedert sich im Rahmen ihrer Durchführung in zwei Teile, nämlich in die *Primärmaßnahme* und die *Sekundärmaßnahme*. Primärmaßnahme ist die Überwachung an sich, sprich das Abgreifen und Ausleiten der Kommunikationsdaten noch vor deren Verschlüsselung bzw.

---

124 Bislang Regelfall in der Praxis.

125 Vgl. jährliche Statistiken auf der Homepage des Bundesamtes für Justiz, http://www.bundesjustizamt.de/nn_2037064/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung__node.html?__nnn=true (zuletzt aufgerufen 15.06.2012); die ab dem Jahr 2008 in den Statistiken aufgeführte Anzahl der Überwachungsanordnungen in Bezug auf „Internettelekommunikation" (5.3) bezieht sich wohl nicht speziell auf die im Zusammenhang mit Quellen-TKÜ stehende Kommunikation, sondern wird jegliche Art von Kommunikation über das Internet (wie bspw. E-Mailing, Blogs, Internetforen, Chats etc.) erfassen.

126 Vgl. http://www.bundesjustizamt.de/cln_115/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Uebersicht__TKUE__2010,templateId=raw,property=publicationFile.pdf/Uebersicht_TKUE_2010.pdf (zuletzt aufgerufen 15.06.2012).

127 Antwort des Bayerischen Staatsministeriums des Innern, LT-Drs. 16/10082, S. 2 und LT-Drs. 16/10469, S. 2, 4 ff.

128 Vgl. bspw. *Reißmann*/*Stöcker*/*Lischka*, http://www.spiegel.de/netzwelt/web/0,1518,790931,00.html (zuletzt aufgerufen 15.06.2012); Badische Zeitung vom 11.10.2011, „Land stoppt Trojaner-Einsatz", S. 1.

129 Laut Auskünften des Ministeriums des Innern und für Sport Rheinland-Pfalz, E-Mail vom 27.07.2010, des Justizministeriums Mecklenburg-Vorpommern, E-Mail vom 02.08.2010; des LKA Sachsen-Anhalt, Schreiben vom 04.08.2010 sowie des LKA Sachsen, Schreiben vom 21.07.2010.

130 Laut Auskunft der Generalstaatsanwaltschaft Oldenburg, E-Mail vom 06.08.2010, wusste der Leiter der Abteilung für Organisierte Kriminalität bei der Staatsanwaltschaft Oldenburg nur von einem Fall zu berichten.

nach deren Entschlüsselung in Echtzeit mit Hilfe der Überwachungssoftware sowie deren Aufzeichnung. Als Sekundärmaßnahmen (= Begleitmaßnahmen) werden die Maßnahmen bezeichnet, die zur notwendigen Infiltration des Zielsystems mit der Überwachungssoftware ergriffen werden, also das heimliche/verdeckte Installieren der Überwachungssoftware auf dem Zielcomputer bzw. das Deinstallieren nach Abschluss der Ermittlungsmaßnahme.

Die technische Umsetzung der Quellen-TKÜ ähnelt hierbei teilweise derjenigen anderer heimlicher Ermittlungsmaßnahmen, was einen Abgrenzung im Folgenden erforderlich macht. Insbesondere besteht in technischer Sicht eine Nähe zur sog. *Online-Durchsuchung*[131]. Beide Ermittlungsmaßnahmen können in ihrer *technischen* Einbringungsmethode sowie in ihrer grundsätzlichen technischen Aufbau- und Funktionsweise[132] zwar durchaus vergleichbar sein, zielen jedoch auf völlig unterschiedliche Überwachungsgegenstände ab.[133] Während die Online-Durch-suchung v. a. den Zugriff auf die auf dem überwachten System abgespeicherten Daten zum Ziel hat[134], sollen mit der Quellen-TKÜ maßnahmespezifisch ausschließlich die Inhalte laufender Telekommunikationsvorgänge erfasst werden[135].

2. Abgrenzung zu anderen heimlichen Ermittlungsmaßnahmen

a) Online-Durchsuchung

Wie bereits eingangs angesprochen, ist streng zu unterscheiden von der Quellen-TKÜ die sog. *Online-Durchsuchung*. Unter dem Begriff der Online-Durchsuchung wird v. a. die heimliche Suche nach verfahrensrelevanten Inhalten auf informationstechnischen Systemen[136] unter Einsatz elektronischer Mittel verstanden[137]. Die Durchsuchung des Systems erfolgt hierbei

---

131 Für Einzelheiten zur Online-Durchsuchung, siehe 1. Teil A.II.2.a).

132 Zugriff mittels einer speziellen Software; vgl. hierzu auch 1. Teil A.II.2.a) und 1. Teil A.II.3.b).

133 Vgl. Bundesministerium des Innern, Fragenkatalog BMJ, S. 1, 7, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012).

134 Für Einzelheiten zum Gegenstand der Online-Durchsuchung, siehe 1. Teil A.II.2.a).

135 Für Einzelheiten zum Gegenstand der Quellen-TKÜ, siehe 1. Teil A.I.3. sowie 1. Teil B.IV.

136 Zum Begriff des *informationstechnischen Systems*, siehe 1. Teil B.III.1.

137 Der Begriff Online-„Durchsuchung“ ist daher in gewisser Weise irreführend, da wesentliche Formvorschriften der „normalen“ Durchsuchung (insb. Offenheit der Maßnahme) gerade nicht zum Tragen kommen.

nicht durch direkten Zugriff der Sicherheitsbehörden, sondern über das Datennetz mittels einer sog. *Remote Forensic Software* (kurz „RFS“)[138]. Maßnahmen der Online-Durchsuchung zählen somit zu den heimlichen Ermittlungsmaßnahmen. Die Heimlichkeit bzw. Verdecktheit des Vorgehens im Rahmen einer solchen Maßnahme dient hierbei dem Zweck, dass verdächtige Zielpersonen nicht gewarnt und Beweise beiseite geschafft werden, sodass Ermittlungsbehörden ohne eine erhöhte Gefahr von Beweismittelverlusten agieren können.[139]

Zum Zwecke einer vollständigen Darstellung der Maßnahmevarianten kann der Begriff „Online-Durchsuchung“ noch weiter unterteilt werden. Er umfasst sowohl die einmalig durchgeführte „Online-Durchsicht“ als auch die auf einen gewissen Zeitraum angelegte „Online-Überwachung“.[140] Zwingend ist diese Unterscheidung indes nicht, da die dauerhafte Online-Überwachung lediglich eine Vertiefung des Grundrechtseingriff darstellt, jedoch zu keiner substantiellen Wesensänderung der Maßnahme führt.[141] Sie ist jedoch dem besseren Verständnis der unterschiedlichen Anforderungen an die Verhältnismäßigkeit bei Online-Durchsuchung und Quellen-TKÜ dienlich.

Bei der sog. *Online-Durchsicht*, der „Online-Durchsuchung im engeren Sinne“, findet ein (i. d. R.) *einmaliger* heimlicher Zugriff auf die Datenspeicher von informationstechnischen Systemen (PC, Mobiltelefon etc.) zur Ermittlung des Status Quo statt. Hierfür werden die dort gespeicherten

---

138 Zu Dt. „fern-forensische“ Software, also zur Beweiserhebung auf informationstechnischen Systemen aus der Ferne; vom BKA speziell entwickelte Software für verdeckte Eingriffe in informationstechnische Systeme zum Zwecke der Online-Durchsuchung, vgl. auch BT-Drs. 17/7760, S. 10.

139 Vgl. auch *Sieber*, Stellungnahme zu dem Fragenkatalog des BVerfG in dem Verfahren 1 BvR 370/07, S. 2, abrufbar unter http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf (zuletzt aufgerufen 15.06.2012).

140 Die Untergliederung basiert auf den Ergebnissen der Arbeitsgruppe der Bundesministerien des Innern und der Justiz, vgl. Bundesministerium des Innern, Fragenkatalog BMJ, S. 1, 2, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012); so auch *Henrichs*, Kriminalistik 2008, 438 (439); teilw. werden auch andere Begrifflichkeiten verwendet: so verwendet *Buermeyer* bspw. die Begriffe „Daten-Spiegelung“ für den einmaligen Zugriff und „Daten-Monitoring“ für eine kontinuierliche Überwachung, vgl. *Buermeyer*, HRRS 2007, 154 (160); *Sieber* wiederum differenziert unter dem Oberbegriff „Online-Zugriff“ zwischen i. d. R. einmaliger „Online-Durchsuchung“ und dauerhafter „Online-Überwachung“, vgl. *Sieber*, Stellungnahme zu dem Fragenkatalog des BVerfG in dem Verfahren 1 BvR 370/07, S. 2, abrufbar unter http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf (zuletzt aufgerufen 15.06.2012); inhaltlich laufen die unterschiedlichen Begrifflichkeiten jedoch auf dasselbe hinaus.

141 Vgl. Bundesministerium des Innern, Fragenkatalog BMJ, S. 1, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012).

Daten „online“, sprich über das Datennetz, mittels des individuell an das Zielsystem angepassten und im Vorfeld heimlich eingebrachten Programms (*Remote Forensic Software*)[142] auf dem fremden System einmalig durchgesehen und zum Zwecke der Auswertung ggf. kopiert und über das Internet ausgeleitet.[143]

Von der „Online-Durchsicht“ kann die sog. *Online-Überwachung* als zweiter Unterfall der Online-Durchsuchung unterschieden werden. Bei einer solchen finden *über einen bestimmten Zeitraum* (wiederholt) heimliche Zugriffe auf das informationstechnische Zielsystem zur (i.d.R umfassenden) Protokollierung der Aktivitäten des Nutzers statt. Hierdurch lassen sich fortlaufende Erkenntnisse über gespeicherte Daten einschließlich des flüchtigen Datenspeichers (z. B. des Cache-Speicher) sowie aller internen und externen Systemschnittstellen (z. B. Screenshots vom Bildschirm, Warteschlangen zum Drucker etc.) erlangen.[144] Auch die Online-Überwachung erfolgt mittels spezieller Remote Forensic Software zum Ermöglichen des Zugriffs auf das System bzw. dessen Speichermedien und zum Erfassen und Ausleiten ggf. aufgefundener ermittlungsrelevanter Daten über das Internet an die Ermittlungsbehörde. Zusätzlich kann die Software auch in der Weise zum Einsatz kommen, dass Tastatureingaben bspw. von Passwörtern oder kryptographischen Schlüsseln heimlich durch sog. *Keylogger*[145] mitprotokolliert werden[146], oder auch jegliche Änderung des Systemzustandes in Echtzeit an die staatlichen Behörden übermittelt wird[147].

In *technischer* Hinsicht ließen sich über dem Mitschnitt von auf dem Zielsystem stattfindenden Tastatureingaben und Bildschirmanzeigen hinaus

---

142 Für Einzelheiten zur Überwachungssoftware bei Maßnahmen der Quellen-TKÜ, siehe 1. Teil A.II.3.b).

143 Vgl. Polizeikurier RLP, Feb 08, S. 09.

144 Vgl. Polizeikurier RLP Feb 08, S. 09; Bundesministerium des Innern, Fragenkatalog BMJ, S. 1, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012).

145 Ein *Keylogger* ist ein Programm, welches im Hintergrund heimlich Eingaben in die Tastatur mitprotokolliert und an den Verwender des Keyloggers ausleitet bzw. zum Abruf zur Verfügung stellt, sodass jedes Drücken einer Taste wie auch die Reihenfolge des Drückens und damit jegliche über die Tastatur getätigten Eingaben (z. B. Eingabe von Zugangsdaten, Texteingaben etc.) einsehbar werden, vgl. hierzu auch die Erläuterung bei *Buermeyer*, HRRS 2007, 154 (157).

146 Vgl. Arbeitskreis „Technische und organisatorische Datenschutzfragen“, Technische Aspekte, S. 3, abrufbar unter http://www.lfd.m-v.de/dschutz/informat/internet/onlinedurchsuchung.pdf (zuletzt aufgerufen 15.06.2012); vgl. auch *Sieber*, Stellungnahme zu dem Fragenkatalog des BVerfG in dem Verfahren 1 BvR 370/07, S. 2, 16, abrufbar unter http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf (zuletzt aufgerufen 15.06.2012).

147 Vgl. Polizeikurier RLP, Feb 08, S. 09.

im Wege der Fernsteuerung („Remote“) sogar Systemgeräte wie Mikrofon oder Webcam heimlich aktiv schalten und deren Aufzeichnungen mitprotokollieren und damit letztlich sogar für eine akustische oder räumliche Überwachung des Umfeldes des Zielsystems heranziehen.[148] Staatlichen Angaben zufolge soll ein solcher Zugriff auf Systemgeräte im Rahmen von Online-Durchsuchungen insbesondere mit Blick auf die Abgrenzung zu Maßnahmen der Wohnraumüberwachung und deren unterschiedliche Zielrichtung jedoch nicht stattfinden.[149]

Der Maßnahmezweck von Online-Durchsuchungen ist deutlich vom reinen Überwachen und Aufzeichnen von Internettelefonaten im Rahmen von Quellen-TKÜ-Maßnahmen zu unterscheiden.[150] Anders als bei der Quellen-TKÜ[151] findet bei der Online-Durchsuchung in Form einer Online-Durchsicht ein Abgreifen und Ausleiten der auf dem System *gespeicherten* Daten in Echtzeit, also im Moment ihres Entstehens, i. d. R. nicht statt. Schon ihre Eigenschaft als Ermittlungsinstrument zum „Durchsuchen“ bzw. zur „Durchsicht“ informationstechnischer Systeme auf ermittlungsrelevante Daten impliziert, dass die Daten bei Beginn der Online-Durchsuchung regelmäßig bereits auf dem System vorhanden sind. Anders kann sich dies wiederum bei einer Online-Überwachung verhalten, bei der gerade auch das aktive Eingabeverhalten oder ggf. sonstige Systemprozesse bzw. Datenverarbeitungsvorgänge erfasst werden, nicht jedoch (verschlüsselt übermittelte) Daten aus laufenden Telekommunikationsvorgängen, für welche die Quellen-TKÜ das speziellere Ermittlungsinstrument darstellt.[152] Die im Rahmen einer Online-Durchsuchung in das System eingeschleuste Software ist demnach so konfiguriert, dass das System über das Netz („Online“) gesichtet werden kann und etwaige ermittlungsrelevante Daten auf dessen Speichermedien (ggf. aber auch im flüchtigen Arbeitsspeicher) gezielt gesucht, erfasst und kopiert werden können.[153] Die erhobenen Daten werden von der Überwachungssoftware dann – je nach Konfiguration – wiederum („behördenseits“) verschlüsselt und entweder direkt auf einen von der durchführen-

---

148 Vgl. auch *Sieber*, Stellungnahme zu dem Fragenkatalog des BVerfG in dem Verfahren 1 BvR 370/07, S. 2, abrufbar unter http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf (zuletzt aufgerufen 15.06.2012).

149 Vgl. Bundesministerium des Innern, Fragenkatalog BMJ, S. 7 f., abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012).

150 So auch zutr. *Bär*, TK-Überwachung, § 100a StPO, Rn. 67.

151 Für Einzelheiten zum technischen Ablauf der Quellen-TKÜ, siehe 1. Teil A.II.3.a) und b).

152 Vgl. Bundesministerium des Innern, Fragenkatalog BMJ, S. 2, 4, 7, 14, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012).

153 Vgl. Polizeikurier RLP, Feb 08, S. 09; vgl. auch *Bär*, MMR. 2010, 266 (267).

den Behörde genutzten Server ausgeleitet oder – bei inaktiver Verbindung – so lange auf dem überwachten Rechner zwischengelagert, bis eine Verbindung ins Internet durch die Zielperson hergestellt wird und dann ausgeleitet. Nach erfolgreicher Übermittlung an den Server werden die auf dem Zielsystem zwischengelagerten Daten wieder gelöscht.[154] Im weiteren Verlauf werden die auf den Behörden-Server übertragenen Daten von der „behördeneignen" Verschlüsselung wieder gelöst und zur Auswertung der aufgezeichneten Kommunikationsinhalte entsprechend aufbereitet.[155] Anders als bei der Online-Durchsuchung gibt es eine solche Phase der Zwischenspeicherung bei der Quellen-TKÜ nicht. Da eine Maßnahme der Quellen-TKÜ ausschließlich Daten aus laufenden Telekommunikationsvorgängen zum Gegenstand hat, ist eine Internetverbindung bei Durchführung der Maßnahme zwangsläufig aktiv. Dementsprechend greift die Überwachungssoftware bei einer Quellen-TKÜ die Kommunikationsinhalte im Moment ihres Entstehens ab und leitet diese während des laufenden Kommunikationsvorgangs in Echtzeit („live") auf einen Behörden-Server zur Aufzeichnung aus.[156]

Inhaltlich lassen sich Online-Durchsuchung und Quellen-TKÜ dadurch voneinander abgrenzen, dass sich Online-Durchsuchungen nicht auf Daten aus laufenden Telekommunikationsvorgängen erstrecken (sollen).[157] Für derartige Daten sei allein die Quellen-TKÜ einschlägige Ermittlungsmaßnahme.[158] Überwachungsgegenstand von Online-Durchsuchungen sind viel-

---

154 Vgl. Bundesministerium des Innern, Fragenkatalog BMJ, S. 13, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012).

155 Vgl. Bundesministerium des Innern, Fragenkatalog BMJ, S. 13, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012).

156 *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11.2010; für Einzelheiten zum technischen Ablauf der Überwachung bei der Quellen-TKÜ, siehe 1. Teil A.II.3.a) und b).

157 Vgl. Bundesministerium des Innern, Fragenkatalog BMJ, S. 2, 4, 7, 14, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012); obgleich im Rahmen einer Online-Überwachung die Software (technisch) wohl ohne weiteres so konfiguriert werden könnte, dass diese im Rahmen der Maßnahme auch Daten aus laufenden Telekommunikationsvorgängen ausleitet, verfolgen beide Maßnahmen jedoch völlig unterschiedliche Ermittlungsziele; vgl. hierzu auch *Sieber*, Stellungnahme zu dem Fragenkatalog des BVerfG in dem Verfahren 1 BvR 370/07, S. 3, 16, abrufbar unter http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf (zuletzt aufgerufen 15.06.2012); inhaltlich und in Bezug auf ihre (verfassungs-)rechtlichen Anforderungen sind Online-Durchsuchung und Quellen-TKÜ streng voneinander zu unterscheiden.

158 Vgl. Bundesministerium des Innern, Fragenkatalog BMJ, S. 2, 7, 14, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012), wonach „Online-Durchsicht und Online-Überwachung […] sich nicht auf Telekommunikationsdaten erstrecken [sollen]" (S. 7).

mehr alle sonstigen, bspw. auf der Festplatte bzw. auf lokal angeschlossenen externen Medien (CD-ROMs, externe Festplatte etc.) abgespeicherten Daten bzw. bei der Online-Überwachung auch das aktive Eingabeverhalten und ggf. sonstige auf dem System ablaufende Datenverarbeitungsvorgänge, die wiederum nicht zulässiger Maßnahmegegenstand einer Quellen-TKÜ sein können.[159] Die Online-Durchsuchung dient zwar wie die Quellen-TKÜ der Erlangung ermittlungsrelevanter Erkenntnisse. Sie ist jedoch in ihrer Eingriffsintensität im Vergleich zur Quellen-TKÜ um ein Vielfaches höher. Auf Grund des umfassenden Zugriffs auf das gesamte Zielsystem samt seiner Speichermedien, bei Online-Durchsuchung in Form der der *Online-Überwachung* gerade auch über einen längeren Zeitraum, sowie der technisch möglichen Übermittlung jeglicher Änderung des Systemzustandes – insbesondere auch in Echtzeit – kommt dieser Maßnahme eine „neue Dimension der Personenüberwachung“[160] zu und stellt wohl den gegenwärtig grundrechtsintensivsten Eingriff in informationstechnische Systeme dar.

Ebenso wie die Quellen-TKÜ lässt sich die Online-Durchsuchung zu repressiven als auch zu präventiven Zwecken einsetzen. Hierfür sind entsprechende gesetzliche Ermächtigungsgrundlagen erforderlich:

Im *repressiven Bereich* existiert für Maßnahmen der Online-Durchsuchung bislang keine Rechtsgrundlage. Nach Auffassung des 3. Strafsenates des Bundesgerichtshofs (BGH) im Beschluss vom 31.01.2007[161], decken die bestehenden Regelungen der StPO die heimlich stattfindende Online-Durchsuchung von informationstechnischen Systemen zum Zwecke der Strafverfolgung nicht[162].

Bis zu dieser grundsätzlichen Entscheidung des BGH, wurde die Frage der Zulässigkeit einer strafprozessualen Online-Durchsuchung uneinheitlich gehandhabt:

Wurde mit Beschluss des BGH-Ermittlungsrichters vom 21.02.2006[163] die heimliche (Fern-)Durchsuchung eines Computers, insbesondere der auf der Festplatte und im Arbeitsspeicher abgelegten Dateien noch gestützt auf die

---

159 Vgl. Bundesministerium des Innern, Fragenkatalog BMJ, S. 2, 3, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012).

160 *Sieber*, Stellungnahme zu dem Fragenkatalog des BVerfG in dem Verfahren 1 BvR 370/07, S. 15, abrufbar unter http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf (zuletzt aufgerufen 15.06.2012).

161 Beschluss des 3. Strafsenates des Bundesgerichtshofs vom 31.01.2007, BGH NJW 2007, 930; bereits BGH-Ermittlungsrichter BeckRS 2007, 00295; a.A. noch BGH-Ermittlungsrichter StV 2007, 60.

162 Hierzu ausführlich *Jahn*/*Kudlich*, JR 2007, 57 und *Gercke*/*Brunst*, Internetstrafrecht, Kap.5, S. 341, Rn. 864 ff.

163 BGH-Ermittlungsrichter StV 2007, 60.

allgemeinen Regelungen zur Durchsuchung nach §§ 102 ff. StPO angeordnet, so lehnte ein anderer BGH-Ermittlungsrichter bereits mit Beschluss vom 25.11.2006[164] einen entsprechenden Antrag auf Durchführung einer Online-Durchsuchung ab. Mit der am 31.01.2007 ergangenen Grundsatzentscheidung des BGH[165] wurde die im Beschluss vom 25.11.2006 vertretene Auffassung bestätigt, wonach die strafprozessualen Vorschriften der §§ 102 ff. StPO wegen des zwingenden offenen Charakters einer Durchsuchung[166] als Rechtsgrundlage für die Durchführung einer heimlich stattfindenden Online-Durchsuchung nicht in Betracht komme.[167]

Eine solche Maßnahme befinde sich auch nicht mehr innerhalb der Grenzen zulässiger Auslegung der §§ 102 ff. StPO, da ein derart weitreichender und schwerwiegender Eingriff[168], wie er mit dem heimlichen Ausforschen eines Computers und dem heimlichen Zugriff auf die darauf gespeicherten Daten verbunden ist, nur über eine (unzulässige) Analogie[169] gerechtfertigt werden könnte.[170]

Auch auf sonstige Befugnisnormen der StPO lasse sich die heimliche Online-Durchsuchung nicht stützen.[171] Eine Kombination einzelner Elemente von Befugnisnormen „um eine Grundlage für eine neue technisch mögliche Ermittlungsmaßnahme zu schaffen“[172], widerspräche dem Grundsatz des allgemeinen Vorbehaltes des Gesetzes für Eingriffe in Grundrechte wie auch dem Gebot der Normenklarheit und Tatbestandsbestimmtheit strafprozessualer Eingriffsnormen und scheide daher ebenfalls aus.[173]

---

164 BGH-Ermittlungsrichter BeckRS 2007, 00295.

165 BGH NJW 2007, 930.

166 Dies ergibt sich u. a. aus dem Recht auf Anwesenheit, § 106 I S. 1 StPO, und der Zuziehung von Zeugen, § 105 II, § 106 I S. 2 StPO.

167 Vgl. BGH NJW 2007, 930 (931); zust. *Kudlich*, HFR 2007, S. 203.

168 So kann einer Durchsuchung im virtuellen Raum sowohl hinsichtlich Datenmenge und Datenqualität als auch mit Blick auf die hierbei mögliche vereinfachte Suche mittels indexbasierter Suchmaschinen gegenüber der klassischen (physischen) Durchsuchung eine weitaus höhere Eingriffsintensität zugemessen werden, vgl. *Sieber*, Stellungnahme zu dem Fragenkatalog des BVerfG in dem Verfahren 1 BvR 370/07, S. 15, abrufbar unter http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf (zuletzt aufgerufen 15.06.2012), zumal diese (i.d.R) gerade eben nicht offen, sondern heimlich abläuft.

169 Das Analogieverbot aus Art. 103 GG, § 1 StGB erfasst im Grundsatz zwar nicht das Strafprozessrecht, eine Rechtsgrundlage für derart schwerwiegende Eingriffe könne gleichwohl nicht im Wege entsprechender Anwendung anderer Befugnisnormen geschaffen werden, vgl. BGH-Ermittlungsrichter BeckRS 2007, 00295; zum Analogieverbot im Strafprozessrecht, siehe 2. Teil A.II.1.a).

170 Vgl. BGH-Ermittlungsrichter BeckRS 2007, 00295.

171 Vgl. BGH NJW 2007, 930 (931 f.).

172 BGH NJW 2007, 930 (932).

Wegen der Schwere des mit einer Online-Durchsuchung verbundenen Eingriffs und mangels einschlägiger strafprozessualer Rechtsgrundlage de lege lata bedürfte es für die Zulässigkeit dieser Ermittlungsmaßnahme im repressiven Bereich deshalb erst der Schaffung einer ausdrücklichen Regelung in der StPO.

Für den Bereich der *Gefahrenabwehr* gilt es zunächst zwischen Bund und Ländern zu differenzieren.

Auf Bundesebene ist eine Befugnis zur Durchführung präventiver Online-Durchsuchungen durch das Bundeskriminalamt (BKA) in § 20k BKAG normiert.[174]

Auf Länderebene hat der 1. Senat des Bundesverfassungsgerichts (BVerfG) mit Urteil vom 27.02.2008[175] entschieden, dass die Regelungen des nordrhein-westfälischen Verfassungsschutzgesetzes zur Online-Durchsuchung mit dem Grundgesetz nicht vereinbar und nichtig sind. Es stellte hierbei allerdings den Grundsatz auf, dass eine Online-Durchsuchung nicht schlechthin verfassungswidrig sei. Die besondere Nähe des vom BVerfG im Rahmen der Entscheidung aus dem allgemeinen Persönlichkeitsrecht neu entwickelten sog. *IT-Grundrechts*[176] zur Unverletzlichkeit der Menschenwürde aus Art. 1 I GG mache diese Maßnahme aber von strengen Bedingungen abhängig. Für die Zulässigkeit im präventiven Bereich müsse die Online-Durchsuchung in einer dem Gebot der Normenklarheit und Normenbestimmtheit genügenden Weise hinreichend gesetzlich geregelt sein, der Abwehr einer *konkreten Gefahr* für *überragend wichtige Rechtsgüter* dienen sowie unter dem Vorbehalt richterlicher Anordnung stehen.[177]

Auch ist die Online-Durchsuchung in etlichen Sicherheits- bzw. Polizeigesetzen der Länder präventiv geregelt. Seit 01.08.2008[178] besteht bspw. für die Bayerische Polizei in Art. 34d BayPAG sowie für den Bayerischen Verfassungsschutz in Art. 6e BayVSG die Befugnis zum verdeckten Zugriff auf informationstechnische Systeme zum Zwecke der Gefahrenabwehr, wo-

---

173 Vgl. BGH NJW 2007, 930 (932).

174 Auf Ausführungen zu etwaigen geheimdienstlichen Befugnissen des Militärischen Abschirmdienstes und des Bundesnachrichtendienstes wird in vorliegender Arbeit verzichtet.

175 Urteil des 1. Senates des Bundesverfassungsgerichts vom 27.02.2008, BVerfG NJW 2008, 822; zu den im Rahmen der Entscheidung auch zur Quellen-TKÜ getroffenen Aussagen, siehe 1. Teil B.IV.

176 Für Einzelheiten, siehe 1. Teil B.III.

177 Vgl. BVerfG NJW 2008, 822 (827 f.; 831; 832).

178 Gesetz zur Änderung des Polizeiaufgabengesetzes vom 08.07.2008, GVBl. S. 365; Gesetz zur Änderung des Verfassungsschutzgesetzes, des Ausführungsgesetzes Art. 10-Gesetz und des Parlamentarischen Kontrollgremium-Gesetzes vom 08.07.2008, GVBl. S. 357.

bei die Vorgaben des BVerfG in den Normen entsprechend Berücksichtigung fanden.

b) Akustische Wohnraumüberwachung, §§ 100c ff. StPO

Bei Vorliegen der materiellen Eingriffsvoraussetzungen des Abs. 1 Nr. 1 bis 4 gestattet die im Jahr 1998 in ihrer ursprünglichen Fassung in die StPO eingefügte[179], im Jahr 2005 auf Grund des Urteils des BVerfG vom 03.03.2004[180] wesentlich umgestaltete und ergänzte[181] sowie zum 01.01.2008 abermals (im Wesentlichen redaktionell) geänderte[182] Regelung des § 100c StPO[183] über die akustische[184] Wohnraumüberwachung als grundrechtsintensivste heimliche Ermittlungsmaßnahme[185] das heimliche[186] Abhören und Aufzeichnen des in einer Wohnung[187] nichtöffentlich[188] gesprochenen Wortes mit technischen Mitteln[189] (sog. *großer Lauschangriff*[190]).

---

179 Durch das Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG) vom 04.05.1998 (BGBl. I S. 845).

180 BVerfG NJW 2004, 999.

181 Durch das Gesetz zur Umsetzung des Urteils des BVerfG vom 24.06.2005 (BGBl. I S. 1841).

182 Durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (VDSG) vom 21.12.2007 (BGBl. I S. 3198).

183 Für Einzelheiten zur Entstehungsgeschichte, siehe Meyer-Goßner – *Cierniak*, StPO, § 100c, Rn. 1.

184 Gedeckt ist nach dem Gesetzeswortlaut nur der Einsatz akustischer und nicht optischer Maßnahmen bspw. in Form von Videoaufzeichnungen, vgl. auch *Bär*, TK-Überwachung, § 100c StPO, Rn. 8.

185 Wegen der hohen Bedeutung des Grundrechts auf Unverletzlichkeit der Wohnung aus Art. 13 I GG; vgl. auch Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 74 m. w. N., wonach das Mittel der akustischen Wohnraumüberwachung „ultima ratio der Strafverfolgung" (Rn. 74) sei.

186 Wobei die gesetzliche Formulierung „auch ohne Wissen der Betroffenen" verdeutlicht, dass die Anordnung weder unzulässig noch überflüssig ist, wenn ein Betroffener die ohne sein Einverständnis vorgenommene Überwachungsmaßnahme bemerkt hat, vgl. Meyer-Goßner – *Cierniak*, StPO, § 100c, Rn. 10.

187 Hierzu zählen sämtliche dem Wohnungsbegriff des Art. 13 I GG unterfallende Räumlichkeiten; der Begriff der akustischen Überwachung von *Wohnraum* ist dementsprechend weit auszulegen, vgl. BGH NJW 2005, 3295 (3296); bereits BGH NJW 1997, 1018 (1019); BVerfG NJW 1971, 2299 (2299); für Einzelheiten zum sachlichen Schutzbereich des Art. 13 I GG, siehe 1. Teil B.II.1.

188 *Nichtöffentlich* sind alle Äußerungen und Gespräche, die allein für den/die Gesprächspartner bestimmt sind, vgl. Meyer-Goßner – *Cierniak*, StPO, § 100c, Rn. 3; erfasst sind hiervon aber auch Selbstgespräche wie auch (ggf. unbewusst artikulierte) Spontanäußerungen, die letztlich nur für den Betroffenen selbst (als sein

Erforderlich hierfür ist das Vorliegen eines von *bestimmten Tatsachen begründeten Tatverdachts*, dass jemand als Täter oder Teilnehmer eine der von § 100c II StPO[191] – in Einklang mit der Vorgabe des Art. 13 III S. 1 GG – enumerativ bestimmten *besonders schweren Straftaten* begangen oder – bei Versuchsstrafbarkeit – zu begehen versucht hat (§ 100c I Nr. 1 StPO)[192], ein *besonderes Schwerwiegen der Tat auch im Einzelfall* (§ 100c I Nr. 2 StPO), auf Grund tatsächlicher Anhaltspunkte die *Annahme*, dass durch die akustische Wohnraumüberwachung *Äußerungen des Beschuldigten erfasst werden*, die für die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes eines Mitbeschuldigten *von Bedeutung sind* (§ 100c I Nr. 3 StPO) *und* die Erforschung des Sachverhaltes oder Ermittlung des Aufenthaltsortes eine *Mit*beschuldigten[193] *auf andere Weise unverhältnismäßig erschwert oder aussichtslos*[194] wäre (§ 100c I Nr. 4 StPO).

---

eigener „Gesprächspartner“) bestimmt sind, vgl. insoweit auch BT-Drs. 15/4533, S. 12, 14 sowie *Bär*, TK-Überwachung, § 100c StPO, Rn. 7, 14.

189 Wobei eine zeitliche und räumliche „Rundumüberwachung“ unzulässig ist, vgl. BVerfG NJW 2004, 999 (1004); eine solche „Rundumüberwachung“ liegt nach Auffassung des BGH bei Kombination einer Wohnraumüberwachung mit Maßnahmen der §§ 99, 100a oder 163f StPO („kumulatives Hinzutreten“) wegen der vorhandenen verfahrensrechtlichen Sicherungen allerdings nicht vor, vgl. BGH NJW 2009, 3448 (3458); näher ausführend auch Meyer-Goßner – *Cierniak*, StPO, § 100c, Rn. 2.

190 In Abgrenzung zu Maßnahmen der akustischen Überwachung außerhalb von Wohnungen nach § 100f I StPO (sog. *kleiner Lauschangriff*); Maßnahmen der akustischen Wohnraumüberwachung nach §§ 100c ff. StPO wurden im Jahr 2010 in vier Fällen, im Jahr 2009 in neuen Fällen und im Jahr 2008 in sieben Fällen angeordnet, vgl. dpa-Artikel „Vier große Lauschangriffe“, Süddeutsche Zeitung vom 15.09.2011, S. 6; der Grund für die vergleichsweise geringe Zahl an Anordnungen in der Praxis liegt v. a. in den strengen gesetzlichen Eingriffsvoraussetzungen für eine akustische Überwachung von Wohnraum.

191 Insgesamt enger gefasst als der Straftatenkatalog des § 100a II StPO.

192 Anders als bei § 100a I Nr. 1, II StPO für TKÜ-Maßnahmen genügt es für eine akustische Wohnraumüberwachung gemäß § 100c I Nr. 1, II StPO neben dem Begehen oder dem Versuch einer dort aufgeführten Katalogstraftat nicht auch, dass ein Täter oder Teilnehmer eine Katalogstraftat durch eine (sonstige) Straftat vorbereitet hat.

193 Da bei einer Maßnahme der akustischen Wohnraumüberwachung bereits als Eingriffsvoraussetzung Anhaltspunkte für die Annahme bestehen müssen, dass mit der Maßnahme Äußerungen des Beschuldigten in den überwachten Räumen erfasst werden (§ 100c I Nr. 3 StPO), sich die Maßnahme nur gegen den Beschuldigten richten darf (§ 100c III S. 1 StPO) und auch bei der Überwachung von Wohnungen Dritter anzunehmen sein muss, dass sich der Beschuldigte dort aufhält (§ 100c III S. 2 StPO), muss der (auf Grund tatsächlicher Anhaltspunkte vermutete) Aufenthaltsort des Beschuldigten notwendigerweise bekannt sein, so auch BT-Drs. 13/8651, S. 13.

194 Insoweit verschärfte Subsidiaritätsklausel im Vergleich zur Subsidiaritätsklausel des § 100a I Nr. 3 StPO.

Gemäß § 100c IV S. 1 StPO darf die Maßnahme aber nur dann angeordnet werden, soweit auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass durch die akustische Wohnraumüberwachung keine Äußerungen erfasst werden, welche dem *Kernbereich privater Lebensgestaltung*[195] zuzurechnen sind, wobei Gespräche in Betriebs- oder Geschäftsräumen gemäß der Regelvermutung des S. 2 ebenso wenig dem Kernbereich zuzurechnen sind, wie gemäß der Regelvermutung[196] des S. 3 Gespräche über begangene Straftaten und Äußerungen, mittels derer Straftaten begangen (oder geplant[197]) werden.

Eine akustische Wohnraumüberwachung nach §§ 100c ff. StPO wird v. a. mit dem Ziel durchgeführt, bestimmte Vorgänge innerhalb der Wohnung (ermittlungs- und aufklärungsbedeutsame Äußerungen und Gespräche des Beschuldigten) zum Zwecke der Erforschung des den Ermittlungen zugrunde liegenden Sachverhaltes, (vgl. § 100c I Nr. 3 StPO) zu erfassen. Bei der (Quellen-)Telekommunikationsüberwachung nach §§ 100a, 100b StPO hingegen geht es um den Zugriff auf Fernmeldeverkehr zur Erhebung von Daten aus laufenden Telekommunikationsvorgängen.

Es kann zwar durchaus der Fall sein, dass im Rahmen einer akustischen Wohnraumüberwachung zufällig auch ein stattfindendes (Internet-)Telefonat (teilweise[198] oder auch vollständig[199]) von der Maßnahme erfasst wird. Mit Blick auf die im Vergleich zu TKÜ-Maßnahmen nach §§ 100a, 100b StPO nochmals erhöhten Eingriffsvoraussetzungen einer Maßnahme der akustischen Wohnraumüberwachung nach §§ 100c ff. StPO, ist das Erfassen von in der überwachten Wohnung stattfindender (akustischer) Telekommunika-

---

195 Auf eine gesetzliche Definition, was zum *Kernbereich privater Lebensgestaltung* gehört, hat der Gesetzgeber auf Grund der Vielzahl möglicher Lebenssituationen, in denen dieser betroffen sein kann, (zu Recht) verzichtet, vgl. BT-Drs. 15/4533, S. 14; für die Einordnung im konkreten Einzelfall kann sich an der bisherigen Rspr. des BVerfG und der sich entwickelnden Kasuistik orientiert werden sowie darauf abgestellt werden, ob die Inhalte nach den jeweiligen Besonderheiten des Einzelfalles höchstpersönlichen Charakter haben und welche Art von Beziehung zwischen den überwachten Gesprächspartnern (z. B. Gespräche mit Personen des höchstpersönlichen Vertrauens wie bspw. neben engen Verwandten auch Seelsorger, Ärzte oder Strafverteidiger) vorliegt, aber auch um was für einen Ort es sich bei der überwachten Räumlichkeit handelt, vgl. *Bär*, TK-Überwachung, § 100c StPO, Rn. 23 f.

196 Vgl. Formulierung des § 100c IV S. 3 StPO („Das Gleiche gilt").

197 Vgl. *Bär*, TK-Überwachung, § 100c StPO, Rn. 27.

198 Sprachsignale des in der überwachten Wohnung befindlichen Gesprächsteilnehmers.

199 Sprachsignale sowohl des in der überwachten Wohnung befindlichen Gesprächsteilnehmers als auch dessen Gesprächspartners bspw. bei „Lautschalten" des Telefons.

tion – bei welcher der Telekommunizierende bewusst Informationen über eine Telekommunikationsanlage zwar in der abgeschirmten Privatsphäre seiner Wohnung, aber aus diesem geschützten Refugium über ein (fremdkontrolliertes) Leitungsnetz hinaus in die Außenwelt entäußert[200] – im Rahmen einer Maßnahme der akustischen Wohnraumüberwachung, welche bei Vorliegen ihrer Voraussetzungen sogar zum Erfassen des in einer Wohnung nichtöffentlich gesprochenen Wortes (Äußerungen im Rahmen eines Gespräches mit einem Gesprächspartner, aber auch Selbstgespräche sowie – ggf. unbewusst getätigte – Spontanäußerungen[201]) legitimiert, in (verfassungs-)rechtlicher Hinsicht ebenfalls nicht zu beanstanden („Erst-recht-Schluss").

Auch ein Erfassen von Äußerungen des Gesprächspartner im Rahmen der akustischen Wohnraumüberwachung, für die Konstellation der (Internet-) Telefonie bspw. denkbar bei einem zufälligen „Lautschalten" des Gesprächs in der überwachten Wohnung, steht der Zulässigkeit der Durchführung nicht entgegen, da eine Aufspaltung der akustischen Überwachung der Wohnung je nach Person des gerade Sprechenden bereits technisch kaum möglich ist. Deshalb stellt auch § 100c III S. 3 StPO ausdrücklich klar, dass die unvermeidbare Betroffenheit Dritter[202] der Durchführung der Maßnahme nicht entgegensteht.[203]

Dies ändert auch nichts daran, dass beide Maßnahmen schon von ihrer gesetzlichen Zielrichtung, von den jeweiligen Ermittlungsgegenständen wie auch von den zu ihrer Durchführung eingesetzten technischen Mitteln her verschieden sind:

Während eine Maßnahme der akustischen Wohnraumüberwachung wie oben erläutert dem Erfassen bestimmter Vorgänge innerhalb von Wohnungen dient, geht es bei der Quellen-TKÜ um die Erlangung von Daten aus verschlüsselt geführten VoIP-Telekommunikationsvorgängen. Während somit Maßnahmen der akustischen Wohnraumüberwachung nach §§ 100c ff. StPO zum Zwecke der Verfolgung und Aufklärung *besonders schwerer Straftaten* gemäß § 100c II StPO in die Vertraulichkeit und Privatheit der Wohnung eingreifen, sind Maßnahmen der Quellen-TKÜ zur Aufklärung

---

200 Vgl. insoweit auch *Sankol*, CR 2008, 13 (15).

201 Vgl. BT-Drs. 15/4533, S. 12, 14, sofern diese nicht dem Kernbereich privater Lebensgestaltung zuzurechnen sind; vgl. zur Kernbereichsrelevanz von Selbstgesprächen auch BGH NJW 2005, 3295.

202 Auch bei einer TKÜ-Maßnahme nach §§ 100a, 100b StPO wird das Miterfassen auch von Telefongesprächen ggf. unbeteiligter Dritter – wie bspw. der Gesprächspartner der Zielperson oder der Personen, die den Anschluss des Überwachten (mit-)benutzen – als unvermeidbar angesehen, vgl. BGH NJW 1980, 67 (68).

203 Vgl. auch Meyer-Goßner – *Cierniak*, StPO, § 100c, Rn. 12.

und Verfolgung *schwerer Straftaten* auf den strafprozessualen Einblick in die Vertraulichkeit des Telekommunikationsverkehrs via softwarebasierter VoIP-Dienste ausgerichtet.

Auch soweit es im Zuge der Durchführung einer akustischen Wohnraumüberwachung zufällig zu einem Erfassen von Teilen der (bzw. bei „Lautschalten" ggf. auch der gesamten) im Rahmen eines laufenden (Internet-)Telefonats innerhalb der Wohnung getätigten Äußerungen kommen sollte (vgl. oben), ist dieser Eingriff nicht am Fernmeldegeheimnis aus Art. 10 I GG zu messen, sondern auf Grund der akustischen Kenntnisnahme von Vorgängen, welche innerhalb von Räumen, die der allgemeinen Zugänglichkeit entzogenen sind, stattfinden, an dem Grundrecht auf Unverletzlichkeit der Wohnung aus Art. 13 I GG. Wenngleich ein (Internet-) Telefonat freilich im Vertrauen auf die grundsätzliche Privatheit und Vertraulichkeit der mit dem Gesprächspartner geführten individuellen Kommunikation abgehalten wird[204], greift die Überwachung nach §§ 100c ff. StPO nicht in den Fernmeldeverkehr ein, sondern erfasst seinem Regelungszweck gemäß allein die akustisch „abfangbaren" Signale innerhalb der überwachten Räumlichkeit.

Erst recht bieten die erhöhten Eingriffsvoraussetzungen des § 100c StPO einen vergleichbaren – mit Blick auf die strengeren Eingriffsvoraussetzungen sogar höheren – Schutz für die akustisch erfassten Gesprächsteile eines in den überwachten Räumlichkeiten laufenden Telekommunikationsvorgangs im Vergleich zur Eingriffbefugnis aus § 100a StPO. Auch der Einbuße an Privatheit bei der Erfassung von Äußerungen im Rahmen von Telefongesprächen, die innerhalb geschützter Räume stattfinden, wird durch das hohe Eingriffsniveau des § 100c StPO allgemein wie auch im Besonderen durch die Regelungen zum Kernbereichsschutz in § 100c IV StPO, in verfassungsrechtskonformer Weise Rechnung getragen.[205]

---

[204] Wobei sich der Nutzer von Internettelefonie (ebenso wie bei herkömmlicher Telefonie) im Vergleich zu Gesprächen unter Anwesenden in Wohnungen selbst aus der abgeschirmten Privatsphäre der Wohnung begibt, indem er über (fremdkontrollierte) technische Anlagen mit anderen Personen kommuniziert, vgl. auch *Sankol*, CR 2008, 13 (15).

[205] Daraus ist jedoch nicht zu schließen, dass Maßnahmen nach § 100c StPO damit eine Alternative zur Quellen-TKÜ darstellen, da Maßnahmen der akustischen Wohnraumüberwachung als „ultima ratio der Strafverfolgung" (Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 74) und gegenwärtig grundrechtsintensivste heimliche Ermittlungsmaßnahme bereits kein „milderes" Mittel darstellen und überdies auch keine vergleichbare Eignung (geschweige denn gesetzliche Zielrichtung) zur Überwachung von Telekommunikation aufweisen, da hierbei im Regelfall (anders nur bei einem zufälligen „Lautschalten" des Gesprächs) wohl nur ein Teil des Telefongesprächs, nämlich die gesprochenen Worte der Zielperson, erfasst werden könnte; siehe hiezu auch die Ausführungen unter 3. Teil A.I.1.c).

Zusätzliche Eingriffsvoraussetzung für Maßnahmen nach § 100c I StPO ist hierbei die Bestimmung des § 100c I Nr. 3 StPO, wonach auf Grund tatsächlicher Anhaltspunkte anzunehmen sein muss, dass durch die akustische Wohnraumüberwachung Äußerungen des Beschuldigten erfasst werden, die für die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes eines Mitbeschuldigten von Bedeutung sind. Nur wenn sich die akustische Wohnraumüberwachung von vornherein ausschließlich auf Gespräche des Beschuldigten richtet, ist eine solche Maßnahme verfassungsrechtlich zulässig, da nur dann die Annahme bestehen kann, dass die erfassten Gespräche einen hinreichenden Bezug zur ermittlungsgegenständlichen Straftat aufweisen.[206] Hierfür ist allerdings notwendig, dass sich der Beschuldigten in den überwachten Räumlichkeiten aktuell – wenn auch ggf. nur auf Grund tatsächlicher Anhaltspunkte vermutet[207] – aufhalten und an überwachungsgegenständlichen Gesprächen teilnehmen wird[208], wobei auch Selbstgespräche sowie (ggf. unbewusst artikulierte) Spontanäußerungen u. ä. in zulässiger Weise erfasst werden können.[209]

Die im Vergleich zu Maßnahmen nach §§ 100a, 100b StPO noch gesteigerte Eingriffsqualität von Maßnahmen der akustischen Wohnraumüberwachung tritt des Weiteren auch darin zu Tage, dass die in § 100c I Nr. 4 StPO enthaltene qualifizierte Subsidiaritätsklausel[210] im Vergleich zur der Regelung des § 100a I Nr. 3 StPO für Maßnahmen nach §§ 100a, 100b StPO

---

206 Vgl. BVerfG NJW 2004, 999 (1013); *Bär*, TK-Überwachung, § 100c StPO, Rn. 14.

207 Vgl. BVerfG NJW 2004, 999 (1013).

208 Wobei es im Rahmen der Durchführung der Maßnahme unschädlich ist, wenn nicht nur Gespräche des Beschuldigten, sondern auch sonstige Gespräche, welche in der zulässigerweise überwachten Wohnung geführt werden, abgehört werden, vgl. Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 81.

209 Sofern keine Kernbereichsrelevanz der Äußerungen zu erwarten ist, § 100c IV StPO; vgl. BT-Drs. 15/4533, S. 12, 14; *Bär*, TK-Überwachung, § 100c StPO, Rn. 14; Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 81; zur Kernbereichsrelevanz von Selbstgesprächen, vgl. BGH NJW 2005, 3295.

210 Hinsichtlich der im Rahmen heimlicher strafprozessualer Ermittlungsmaßnahmen gesetzlich normierten Subsidiaritätsklauseln handelt es sich bei derjenige des § 100c I Nr. 4 StPO („auf andere Weise unverhältnismäßig erschwert oder aussichtslos“) für Maßnahmen der akustischen Wohnraumüberwachung um die strengste Subsidiaritätsklausel im Vergleich zu der bereits abgeschwächten Klausel des § 100a I Nr. 3 StPO („auf andere Weise wesentlich erschwert oder aussichtslos“) für Maßnahmen der Telekommunikationsüberwachung sowie des § 100f I StPO für Maßnahmen der akustischen Überwachungen außerhalb von Wohnungen und der niedrigsten Subsidiaritätsklausel des § 100h I StPO („weniger erfolgversprechend oder erschwert“) für Bildaufnahmen und den Einsatz sonstiger technischer Mittel nach § 100h I Nr. 1 und Nr. 2 StPO, vgl. hierzu auch *Bär*, TK-Überwachung, § 100a StPO, Rn. 24 f., § 100c StPO, Rn. 15 und § 100f StPO, Rn. 15.

wesentlich strenger ausgestaltet ist. Anders als bei § 100a I Nr. 3 StPO genügt nach § 100c I Nr. 4 StPO nicht nur, dass die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthalts eines Mitbeschuldigten auf andere Weise *wesentlich* erschwert (oder aussichtslos) wäre, sondern setzt voraus, dass diese auf andere Weise (bspw. durch TKÜ-Maßnahmen nach §§ 100a, 100b StPO) als durch eine akustische Überwachung des Wohnraumes *unverhältnismäßig* erschwert (oder aussichtslos) wäre. Die Subsidiaritätsklausel des § 100c I Nr. 4 StPO stellt hierbei klar, dass die akustische Wohnraumüberwachung wegen ihres besonders schweren Grundrechteingriffs „ultima ratio der strafprozessualen Ermittlungsmaßnahmen“[211] sein soll. Auf Grund dieser Vorgabe sind somit Erschwernisse bei der Ermittlungsarbeit bis zum Grade der Unverhältnismäßigkeit hinzunehmen, ehe auf das strafprozessuale Instrument der akustischen Wohnraumüberwachung gemäß §§ 100c ff. StPO zugegriffen werden darf.[212]

Auch im Hinblick auf die Zielperson einer Maßnahme der akustischen Wohnraumüberwachung bestehen restriktivere gesetzliche Vorgaben. Im Unterschied zu Maßnahmen nach §§ 100a, 100b StPO dürfen Maßnahmen der akustischen Wohnraumüberwachung nach § 100c III S. 1 StPO nur gegen den Beschuldigten gerichtet sein und grds. nur in dessen Wohnungen durchgeführt werden. Allein unter den – im Vergleich zu § 100a III StPO deutlich strengeren – Voraussetzungen des § 100c III S. 2 StPO darf sich eine akustische Wohnraumüberwachung auch auf Wohnungen Dritter ausdehnen.[213] Erforderlich hierfür ist nach § 100c III S. 2 StPO allerdings das Vorliegen bestimmter Tatsachen, auf Grund derer anzunehmen ist, dass sich der Beschuldigte in der Wohnung des Dritten aufhält (Nr. 1) und die akustische Überwachung in Wohnungen des Beschuldigten allein nicht zur Erforschung des Sachverhaltes oder zur Ermittlung des Aufenthaltsortes eines Mitbeschuldigten führen wird (Nr. 2). Dies bedeutet aber nicht, dass im Rahmen der Durchführung der Maßnahme nur Äußerungen des Beschuldigten erfasst werden dürften. Vielmehr kann sich die Überwachung in zulässiger Weise auf alle geführten Gespräche in den betreffenden Räumlichkeiten erstrecken, deren akustische Überwachung angeordnet wurde[214], insbesondere da die Maßnahme gemäß § 100c III S. 3 StPO auch angeordnet und durchgeführt werden darf, wenn andere Personen unvermeidbar betroffen sind – mit Blick auf den Schutz unverdächtiger Dritter[215] und die gesetzli-

---

211 Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 82.

212 Vgl. Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 82.

213 Vgl. auch *Bär*, TK-Überwachung, § 100c StPO, Rn. 16.

214 Vgl. Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 81.

215 Dem Schutzinteresse unvermeidbar betroffener Dritter tragen die Regelungen über die Verwertbarkeit (§ 100c V, VI StPO; § 100d V StPO) sowie Benachrichti-

che Formulierung „aufhält“ in § 100c III S. 2 Nr. 1 StPO allerdings nur bei einer aktuellen, wenn auch ggf. lediglich auf Grund tatsächlicher Anhaltspunkte vermuteten[216], Anwesenheit des Beschuldigten in den überwachten Räumlichkeiten.[217]

Als weitere Besonderheit normiert § 100c IV S. 1 StPO eine *negative Kernbereichsprognose*.[218] Während bei Maßnahmen der Überwachung und Aufzeichnung von Telekommunikation nach §§ 100a, 100b StPO eine solche gemäß § 100a IV S. 1 StPO unzulässig ist, wenn (positiv) tatsächliche Anhaltspunkte für die Annnahme einer alleinigen Kernbereichsbetroffenheit vorliegen, kann eine Maßnahme der akustischen Wohnraumüberwachung von vornherein nur angeordnet werden, soweit – neben den Eingriffsvoraussetzungen des § 100c I StPO – als weitere Voraussetzung für die Zulässigkeit einer solchen Maßnahme auf Grund tatsächlicher Anhaltspunkte (negativ) anzunehmen ist, dass durch die Überwachung Äußerungen aus dem Kernbereich privater Lebensgestaltung nicht erfasst werden. Für die Beurteilung des Vorliegens der Voraussetzungen im Rahmen der Entscheidung über den Antrag zur Anordnung einer Maßnahme nach §§ 100c ff. StPO bedarf es deshalb stets einer (zusätzlichen) Prognoseentscheidung des Gerichts, dass eine gewisse Wahrscheinlichkeit dafür vorliegt, dass es zu keinem Zugriff auf kernbereichsrelevante Äußerungen kommen wird[219], während die Zulässigkeit einer Maßnahme nach §§ 100a, 100b StPO nur bei entsprechendem Vorliegen positiver Anhaltspunkten für eine Kernbereichsbetroffenheit tangiert wird. Die zu treffende Prognoseentscheidung im Rahmen der Anordnung von Maßnahmen nach §§ 100c ff. StPO wird jedoch durch die Regelvermutungen des § 100c IV S. 2 und S. 3 StPO insoweit

---

gungspflichten (§ 101 IV S. 1 Nr. 4b StPO) entsprechend Rechnung, vgl. auch *Bär*, TK-Überwachung, § 100c StPO, Rn. 20.

216 Vgl. BVerfG NJW 2004, 999 (1013).

217 Vgl. Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 81.

218 Vgl. *Bär*, TK-Überwachung, § 100c StPO, Rn. 25; Meyer-Goßner – *Cierniak*, StPO, § 100c, Rn. 14; auf eine gesetzliche Definition, was zum *Kernbereich privater Lebensgestaltung* gehört, hat der Gesetzgeber auf Grund der Vielzahl möglicher Lebenssituationen, in denen dieser betroffen sein kann, (zu Recht) verzichtet, vgl. BT-Drs. 15/4533, S. 14; für die Einordnung im konkreten Einzelfall kann sich an der bisherigen Rspr. des BVerfG und der sich entwickelnden Kasuistik orientiert werden sowie darauf abgestellt werden, ob die Inhalte nach den jeweiligen Besonderheiten des Einzelfalles höchstpersönlichen Charakter haben und welche Art von Beziehung zwischen den überwachten Gesprächspartnern (z. B. Gespräche mit Personen des höchstpersönlichen Vertrauens wie bspw. neben engen Verwandten auch Seelsorger, Ärzte oder Strafverteidiger) vorliegt, aber auch um was für einen Ort es sich bei der überwachten Räumlichkeit handelt, vgl. *Bär*, TK-Überwachung, § 100c StPO, Rn. 23 f.

219 Vgl. *Löffelmann*, NJW 2005, 2033 (2033) m. w. N.

wiederum relativiert, als Gespräche in Betriebs- und Geschäftsräumen (S. 2) sowie Gespräche über begangene Straftaten und Äußerungen, mittels derer Straftaten begangen werden (S. 3) „in der Regel“ nicht dem Kernbereich privater Lebensgestaltung zuzurechnen sind. Anders als § 100a IV S. 1 StPO für Maßnahmen der Telekommunikationsüberwachung, fordert § 100c IV S. 1 StPO zugunsten eines erhöhten Schutzes des Grundrechtsträgers vor akustischen Wohnraumüberwachungen im höchstpersönlichen Bereich auch keinen alleinigen Kernbereichsbezug.[220]

Beide Maßnahmen finden zwar grds. heimlich statt, d. h. ohne Wissen der Betroffenen von deren Durchführung. Anders aber als bei der Wohnraumüberwachung nach §§ 100c ff. StPO kommt der Telekommunikationsanlage bei der Quellen-TKÜ nicht die bloße Funktion einer Abhöranlage i. S. d. § 100c StPO zu.[221] Die Telekommunikationsanlage wird bei einer Quellen-TKÜ-Maßnahme gerade nicht zielgerichtet ohne oder gegen den Willen des von der Maßnahme Betroffenen in Betrieb genommen.[222] Vielmehr wird die Aktivschaltung der Überwachung durch ein bewusstes Benutzen der Telekommunikationsanlage durch den Betroffenen (Einleiten und Führen eines Telefongespräches mittels Computer über das Internet), also durch dessen eigenständiges Handeln ausgelöst. Maßnahmen der akustischen Wohnraumüberwachung hingegen werden ohne ein spezifisches Handeln des Betroffenen, also ohne dessen Mitwirken, in Gang gesetzt. Die Quellen-TKÜ besitzt damit auf Grund des fehlenden zusätzlichen Elementes eines „einflusslosen“ Auslösens des Überwachungsvorgangs durch den von der Maßnahme Betroffenen keinen mit der Fallkonstellation des § 100c StPO vergleichbaren Eingriffscharakter und entfaltet keine grundrechtliche Eingriffswirkung von vergleichbarer Intensität.

Das für die Durchführung der akustischen Wohnraumüberwachung nach §§ 100c ff. StPO ggf. notwendige Betreten der Wohnräume zum Anbringen einer entsprechenden Vorrichtung zum Abhören („Wanze“) und/oder Aufzeichnen (Tonbandgerät u. ä.) der in der Wohnung erzeugten akustischen

---

220 Die insgesamt erhöhten Anforderungen des § 100c IV StPO für Maßnahmen der akustischen Wohnraumüberwachung im Vergleich zu den Bestimmungen des § 100a IV StPO für Maßnahmen der Überwachung und Aufzeichnung von Telekommunikation sind auch gerechtfertigt, da ein Bürger zu höchstpersönlicher Kommunikation nicht in gleicher Weise auf Telekommunikation wie auf eine (Privat-)Wohnung als „letztes Refugium“ angewiesen ist, vgl. BVerfG NJW 2004, 999 (1002); BVerfG NJW 2005, 2603 (2612).

221 Vgl. *Bär*, TK-Überwachung, § 100a StPO, Rn. 32; BGH NJW 2003, 2034 (2035); a. A. *Sankol*, CR 2008, 13 (15).

222 Vgl. *Bär*, TK-Überwachung, § 100a StPO, Rn. 32; aus diesem Grunde ist auch der Sichtweise von *Braun*/*Roggenkamp*, K&R 2011, 681 (682) zu widersprechen, wonach „es treffender [wäre], von einer ‚Staatswanze‘ zu sprechen“ (682).

Signale findet seine Grundlage ebenfalls in den verfassungsrechtlichen Vorschriften des Art. 13 III GG. Die Schranke aus Art. 13 III GG, die repressive Eingriffe in Art. 13 I GG sowohl für die (Primärmaßnahme der) akustische(n) Überwachung der Wohnung mit technischen Mitteln an sich als auch für das hierzu notwendige vorherige *heimliche Betreten* der Wohnung zum Anbringen entsprechender Überwachungsvorrichtungen[223] als Annex (Sekundärmaßnahme) (verfassungs-)rechtlich erlaubt[224], ist auf Maßnahmen der (Quellen-)Telekommunikationsüberwachung nach §§ 100a, 100b StPO nicht anwendbar.[225]

Zuständig für die – gemäß § 100d II, III StPO schriftlich zu ergehende und gemäß § 100d I S. 4 StPO höchstens auf einen Monat[226] zu befristende[227] – Anordnung einer akustischen Wohraumüberwachungsmaßnahme ist anders als bei TKÜ-Maßnahmen nach § 100b I S. 1 und S. 2 StPO nicht der Ermittlungsrichter[228] bzw. das mit der Sache befasste Gericht[229] oder (bei Gefahr im Verzug[230]) die Staatsanwaltschaft, sondern gemäß § 100d I S. 1 StPO die nach § 74a IV GVG eigens hierfür einzurichtende, nicht mit Hauptverfahren in Strafsachen befasste Kammer (Staatsschutzkammer) desjenigen Landgerichtes, in dessen Bezirk das jeweilige OLG seinen Sitz hat, für den gesamten OLG-Bezirk (§ 74a IV GVG).[231] Gemäß § 100d I S. 2 StPO besteht für den Vorsitzenden der Strafkammer – nicht auch für die Staatsanwaltschaft wie bei §§ 100a, 100b I S. 2 StPO – eine Eilkompetenz bei Gefahr in Verzug, die allerdings nach § 100d I S. 3 StPO außer Kraft tritt, wenn sie nicht binnen drei Werktagen von der Kammer bestätigt wird.

---

223 Vgl. BVerfG NJW 1984, 419 (421).

224 Vgl. BT-Drucks. 13/8651, S. 13; BGH NJW 2001, 1658 (1659).

225 Für Einzelheiten zu Fragen des Betretungsrechtes, siehe auch 2. Teil B.I.2.b).

226 Wobei die Frist bereits mit Erlass der gerichtlichen Anordnung beginnt; auf Grund der höheren Eingriffsintensität der Maßnahme ist nur eine maximale (Erst-) Anordnungsdauer von einem Monat und nicht wie bei TKÜ-Maßnahmen gemäß § 100b I S. 4 StPO von 3 Monaten zulässig.

227 Gemäß der Regelung des § 100d IV S. 2 StPO darf eine angeordnete akustische Wohnraumüberwachung nur solange durchgeführt werden, wie die materiellen Voraussetzungen des § 100c StPO gegeben sind.

228 Im Ermittlungsverfahren, § 162 I S. 1 StPO.

229 Nach Erhebung der öffentlichen Klage, § 162 III StPO.

230 *Gefahr im Verzug* liegt grds. dann vor, wenn das vorherige Einholen der richterlichen Anordnung den Erfolg der Maßnahme gefährden würde, vgl. BVerfG NJW 1979, 1539 (1540); bei strafprozessualen Maßnahmen ist dies regelmäßig dann der Fall, wenn ein Verlust von Beweismitteln droht, der allerdings nicht von den Ermittlungsbehörden selbst herbeigeführt worden sein darf, vgl. BVerfG NJW 2001, 1121 (1123).

231 Vgl. BeckOK – *Hegmann*, StPO, Ed. 13, § 100d, Rn. 1.

Der nach § 100d I S. 1 StPO, § 74a IV GVG zuständigen Strafkammer beim Landgericht obliegen auch die weiteren im Zusammenhang mit der akustischen Wohnraumüberwachung anfallenden Entscheidungen, wie Abbruch der Maßnahme (§ 100d IV S. 2 StPO), Unterbrechung und Fortführung (§ 100c V S. 6 StPO i. V. m. § 100d IV StPO entspr.) und Verwertung kernbereichsrelevanter Erkenntnisse (§ 100c VII S. 1 StPO) als auch die Entscheidung über die weitere Zurückstellung der Benachrichtigung gemäß § 101 VII S. 1 StPO.[232] Nicht zuständig hingegen ist die Strafkammer für die Entscheidung über gleichzeitig beantragte andere heimliche Ermittlungsmaßnahmen, wie Anordnungen zur Überwachung der Telekommunikation nach §§ 100a, 100b StPO oder die akustischen Überwachung außerhalb von Wohnungen nach § 100f StPO, die in den gesetzlichen Zuständigkeitsbereich des Ermittlungsrichters fallen, weshalb es hier getrennter Entscheidungen bedarf.[233]

Spezifische Maßgaben zur Verwendbarkeit personenbezogener Daten aus einer akustischen Wohnraumüberwachung für andere Zwecke als denjenigen, für die sie im Ausgangsverfahren erhoben wurden, sind in den Regelungen des § 100d V StPO enthalten. Zur Weiterverwendung von aus einer Maßnahme nach § 100c StPO erlangten Daten in anderen Strafverfahren geht die Vorschrift des § 100d V Nr. 1 StPO als lex specialis den allgemeinen Regelungen in § 161 II StPO und § 477 II S. 2 StPO insoweit vor.[234]

c) Akustische Überwachung außerhalb von Wohnungen, § 100f StPO

Die auch als sog. *kleiner Lauschangriff* bezeichnete heimliche[235] strafprozessuale Ermittlungsmaßnahme der akustischen[236] Überwachung des nichtöffentlich gesprochenen Wortes außerhalb von Wohnungen[237] ist – als

---

232 Vgl. *Bär*, TK-Überwachung, § 100d StPO, Rn. 4.

233 Vgl. *Bär*, TK-Überwachung, § 100d StPO, Rn. 4 m. w. N., wobei dies natürlich umgekehrt auch für den Ermittlungsrichter in Bezug auf akustische Wohnraumüberwachungsanordnungen nach §§ 100c ff. StPO gilt.

234 Vgl. im Einzelnen auch Meyer-Goßner – *Cierniak*, StPO, § 100d, Rn. 6.

235 Wobei die gesetzliche Formulierung „auch ohne Wissen der Betroffenen" verdeutlicht, dass die Anordnung weder unzulässig noch überflüssig ist, wenn ein Betroffener die ohne sein Einverständnis vorgenommene Überwachungsmaßnahme bemerkt hat, vgl. Meyer-Goßner – *Cierniak*, StPO, § 100f, Rn. 1.

236 Gedeckt ist nach dem Gesetzeswortlaut nur der Einsatz akustischer und nicht optischer Maßnahmen bspw. in Form von Videoaufzeichnungen; für Videoaufzeichnungen außerhalb der Wohnung kommt aber ggf. eine Maßnahme nach § 100h I Nr. 1 StPO in Betracht, vgl. auch *Bär*, TK-Überwachung, § 100f StPO, Rn. 8.

237 Von einer Maßnahme nach § 100f StPO nicht gedeckt ist demnach ein jedes Abhören und Aufzeichnen von Äußerungen und Gesprächen, welche innerhalb von Räumlichkeiten stattfinden, die der allgemeinen Zugänglichkeit entzogen sind und

„Pendant“ zur akustischen Überwachung von Wohnraum nach §§ 100c ff. StPO – in der Vorschrift des § 100f StPO geregelt. Wegen der geringeren Eingriffsintensität einer solchen Maßnahme und entsprechend herabgesetzter Eingriffsvoraussetzungen in § 100f StPO entfaltet der kleine Lauschangriff indes eine größere praktische Relevanz[238] als der – auf Grund seiner hohen Eingriffsintensität restriktiv gehandhabte – große Lauschangriff nach §§ 100c ff. StPO.

Voraussetzung für das Abhören und Aufzeichnen des nichtöffentlich[239] gesprochenen Wortes mit technischen Mitteln[240] ist gemäß § 100f I StPO[241] das Vorliegen *bestimmter Tatsachen*, *die den Verdacht begründen*, dass jemand als Täter oder Teilnehmer eine der in *§ 100a II StPO bezeichneten Straftaten* begangen oder – bei Versuchsstrafbarkeit – zu begehen versucht hat. Notwendig ist des Weiteren, dass die Straftat hierbei *auch im Einzelfall schwer wiegt* und die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes eines Beschuldigten *auf andere Weise aussichtslos oder wesentlich erschwert*[242] wäre.

Außer gegen den Beschuldigten[243] darf eine Maßnahme der akustischen Überwachung außerhalb von Wohnungen auch gegen andere Personen angeordnet werden, nach Maßgabe des § 100f II S. 2 StPO allerdings nur dann, wenn auf Grund bestimmter Tatsachen[244] die Annahme besteht, dass diese (als Nachrichtenmittler) mit einem Beschuldigten in Verbindung ste-

---

der Entfaltung des Privatlebens dienen; für Einzelheiten zum sachlichen Schutzbereich des Art. 13 I GG, vgl. 1. Teil B.II.1.

238 Vgl. *Bär*, TK-Überwachung, § 100f StPO, Rn. 2.

239 *Nichtöffentlich* sind alle Äußerungen und Gespräche, die allein für den/die Gesprächspartner oder bei Selbstgesprächen sowie bei (ggf. unbewusst artikulierten) Spontanäußerungen nur für den Betroffenen selbst (als sein eigener „Gesprächspartner“) bestimmt sind, vgl. insoweit auch BT-Drs. 15/4533, S. 12,14; hingegen lässt sich das Abhören und Aufzeichnen des außerhalb von Wohnungen *öffentlich* gesprochene Wort auf die Ermittlungsgeneralklausel der §§ 161, 163 StPO stützen, vgl. auch *Bär*, TK-Überwachung, § 100f StPO, Rn. 7.

240 Z. B. versteckte Abhörgeräte (sog. Wanzen), Richtmikrofone u. ä., wobei mit Hilfe der technischen Mittel das gesprochene Wort in zulässiger Weise durch Verstärkung oder Übertragung über den normalen Klangbereich hinaus unmittelbar wahrnehmbar gemacht werden darf, vgl. *Bär*, TK-Überwachung, § 100f StPO, Rn. 8.

241 Der sich in seinen Eingriffsvoraussetzungen an § 100a I StPO anlehnt, vgl. auch *Bär*, TK-Überwachung, § 100f StPO, Rn. 1.

242 Insoweit dieselben Subsidiaritätsanforderungen wie bei § 100a I Nr. 3 StPO.

243 Der wie bei einer Maßnahme nach §§ 100a, 100b StPO namentlich noch nicht bekannt sein muss, sondern dessen Identität auch erst durch die akustische Überwachungsmaßnahme ermittelt werden kann, vgl. *Bär*, TK-Überwachung, § 100f StPO, Rn. 17.

244 Zur Reichweite der Voraussetzung „auf Grund bestimmter Tatsachen“, siehe Meyer-Goßner – *Cierniak*, StPO, § 100f, Rn. 11 m. w. N.

hen oder eine solche Verbindung hergestellt wird, die Maßnahme (gegen den Dritten) zur Erforschung des Sachverhaltes oder zur Ermittlung des Aufenthaltsortes eines Beschuldigten führen wird *und* dies auf andere Weise aussichtslos oder wesentlich erschwert wäre.

Bezogen auf die spezifischen Konstellation der Internettelefonie und das Verhältnis dieser Ermittlungsmaßnahme zu der Maßnahme der Überwachung und Aufzeichnung von Telekommunikation nach §§ 100a, 100b StPO lässt sich feststellen, dass auch Situationen denkbar sind, in denen bspw. mit einem mobilen Endgerät (z. B. Mobiltelefon, Notebook) Internettelefonie außerhalb einer Wohnung geführt wird und im Rahmen einer akustischen Überwachungsmaßnahme nach § 100f StPO Teile dieser Kommunikation (das gesprochene Wort der überwachten Person) zufällig erfasst werden. Das Erfassen von Kommunikationsteilen anlässlich einer Maßnahme nach § 100f StPO ist indes mit ähnlichen Argumenten wie bei dem Erfassen von geführten (Internet-)Telefonaten in akustisch überwachten Wohnräumen nach §§ 100c ff. StPO[245] insoweit als unproblematisch zu betrachten. Zum einen handelt es sich – wie bei Maßnahmen nach §§ 100c ff. StPO – auch bei der akustischen Überwachung außerhalb von Wohnungen nach § 100f StPO zwar um eine Maßnahme, die mit Blick auf ihren Regelungszweck auf einen anderen Maßnahmegegenstand abzielt als die Telekommunikationsüberwachung nach §§ 100a, 100b StPO. Während nämlich Maßnahmen nach §§ 100a, 100b StPO die Überwachung und Aufzeichnung von mittels Telekommunikationsanlagen geführter Kommunikation zum Gegenstand haben, sprich bei (Internet-)Telefonie der (heimliche) Zugriff auf die (vollständigen) Inhaltsdaten des geführten Gesprächs und damit die Erfassung der wechselseitig ausgetauschten Kommunikationssignalen im Mittelpunkt steht, zielen Maßnahmen nach § 100f StPO auf das Erfassen des außerhalb von Wohnungen nichtöffentlich gesprochenen Wortes ab. Dies trifft allerdings generell auf Äußerungen und Gespräche der Zielperson an nicht vom Schutzbereich des Art. 13 I GG erfassten Örtlichkeiten zu, und zwar auch dann, wenn diese im Rahmen einer Internettelefonie außerhalb der geschützten Räumlichkeiten vom Maßnahmeadressaten – (willentlich) mehr oder weniger laut hörbar – in seine Umgebung entäußert werden.[246] Diese akustischen Signale, welche „auf freier Flur" mit technischen Mitteln abgefangen werden, unterliegen nicht dem Schutz des Fernmeldegeheimnisses aus Art. 10 I GG. Betroffenes Grundrecht einer solchen Maßnahme ist allein

---

245 Siehe 1. Teil A.II.2.b).

246 Ein Abhören und Aufzeichnen von Gesprächen, die innerhalb der Wohnung stattfinden, durch geöffnete Fenster oder Türen hindurch mit technischen Mitteln, die sich außerhalb der Wohnung befinden, kann hingegen nur über eine Maßnahme nach § 100c StPO realisiert werden, vgl. auch *Bär*, TK-Überwachung, § 100f StPO, Rn. 5.

das allgemeine Persönlichkeitsrecht aus Art. 2 I i. V. m. Art. 1 I GG.[247] Aus diesem Grunde ist es auch unbeachtlich, dass § 100f StPO keine Regelungen zum Schutz des Kernbereiches privater Lebensgestaltung enthält, wie § 100a IV StPO und § 100c IV StPO – obwohl das außerhalb von nach Art. 13 I GG geschützten Räumen nichtöffentlich gesprochene Wort freilich auch sehr private Dinge enthalten kann. Das Ausmaß und die Intensität eines Eingriffs in das allgemeine Persönlichkeitsrecht betrifft jedoch typischerweise nicht den unantastbaren Kernbereich der privaten Lebensgestaltung.[248] Dies ist auch folgerichtig, da außerhalb der Wohnung keine gleichermaßen hohe Privatsphäre wie in Wohnräumen als elementarer Lebens- und Rückzugsort besteht und daher auch ein entsprechend schützenswertes Vertrauen des Grundrechtsträgers hierin nicht vorliegt. Gleiches gilt auch für das nichtöffentlich gesprochene Wort im Rahmen von Telefongesprächen außerhalb der nach Art. 13 I GG geschützten Räumlichkeiten. Zwar sind die gesprochenen Worte als *nichtöffentliche* i. d. R. nur für den Gesprächspartner bestimmt. Dies ändert jedoch nichts daran, dass bei Telefongesprächen außerhalb geschützter Räume zwar ein schützenswertes (und durch das Fernmeldegeheimnis aus Art. 10 I GG geschütztes) Vertrauen des Maßnahmeadressaten in die Vertraulichkeit der Nutzung des zum Zwecke der Telekommunikation verwendeten technischen Kommunikationsmediums besteht[249], jedoch keines dergestalt, dass an derartigen vor der Öffentlichkeit nicht abgeschotteten Örtlichkeiten die in die Umgebung entäußerten Worte vor (auch staatlicher) Einsichtnahme geschützt wären. Bei Gesprächen außerhalb der Wohnung sowie sonstiger abgeschotteter Räumlichkeiten ist sich der verständige Grundrechtsträger vielmehr deren allgemeiner Zugänglichkeit und der deshalb nicht garantierten Privatsphäre bewusst. Hierfür spricht auch die der Regelvermutung des § 100c IV S. 2 StPO entsprechend zugrunde liegende Wertung des Gesetzgebers, wonach Überwachungsmaßnahmen außerhalb der Wohnung typischerweise nicht den Kernbereich privater Lebensgestaltung tangieren. In bestimmten Ausnahmefällen der Erfassung höchst privater Äußerungen wird nach teilweise vertretener Auffassung im Einzelfall allerdings eine analoge Anwendung des § 100a IV StPO, zumindest jedoch ein verfassungsunmittelbares Verwertungsverbot zu erwägen sein.[250]

Zum anderen unterliegt eine Maßnahme der akustischen Überwachung außerhalb von Wohnungen nach § 100f I StPO aber auch dem gleichen

---

247 Vgl. *Bär*, TK-Überwachung, § 100f StPO, Rn. 3.

248 Vgl. *Bär*, TK-Überwachung, § 100f StPO, Rn. 3 m. w. N.

249 Vgl. insoweit *Bär*, TK-Überwachung, § 100a StPO, Rn. 5.

250 So Meyer-Goßner – *Cierniak*, StPO, § 100f, Rn. 19; ebenso *Bär*, TK-Überwachung, § 100f StPO, Rn. 23.

hohen Niveau hinsichtlich der erforderlichen Voraussetzungen für deren Anordnung, wie dies bei einer TK-Überwachung nach § 100a I StPO der Fall ist. Da die strafprozessuale Ermittlungsmaßnahme des § 100f StPO hinsichtlich ihrer Eingriffstiefe eher mit derjenigen des §§ 100a, 100b StPO als mit der des § 100c StPO vergleichbar ist[251], sind die Vorschriften bezüglich der formellen und materiellen Eingriffsvoraussetzungen an die Vorschriften der Telekommunikationsüberwachung angeglichen.[252] Im Rahmen der akustische Überwachung nach § 100f StPO erfasste Gesprächsteile (bzw. auch des gesamten Gesprächs bei zufälligem „Lautschalten") aus (Internet-) Telefonaten unterliegen deshalb auch keinem niedrigeren Schutz- und Eingriffsniveau als bei einem Zugriff auf die Äußerungen und Gespräche im Wege der Überwachung des Telekommunikationsverkehrs. Nach § 100f III StPO darf die Maßnahme auch dann durchgeführt werden, wenn Dritte unverhältnismäßig betroffen werden. Für die hier behandelten Fälle der (Internet-)Telefonie steht folglich ein Erfassen auch des nicht öffentlich gesprochenen Wortes des Gesprächspartners (in den besagten Fällen des zufälligen „Lautschaltens" des Gesprächs) der Durchführbarkeit nicht entgegen, zumal eine Trennung der mit technischen Mitteln (z. B. Richtmikrofone) außerhalb der Wohnung aufgefangenen akustischen Signale auch technisch kaum möglich wäre.[253]

In formeller Hinsicht verweist § 100f IV StPO auf bestimmte entsprechend anzuwendende Vorschriften des § 100b StPO sowie des § 100d StPO. So ist für die Anordnung einer Überwachungsmaßnahme nach § 100f StPO

---

251 Vgl. BT-Drs. 16/5846, S. 49.

252 Vgl. *Bär*, TK-Überwachung, § 100f StPO, Rn. 1.

253 Hieraus jedoch den Umkehrschluss zu ziehen, dass außerhalb des räumlichen Schutzbereiches des Art. 13 GG deshalb ein „probates technisches Mittel" zum Abhören von verschlüsselten Telefonaten (über mobile Endgeräte) „an der Quelle" zur Verfügung stünde und eine Quellen-TKÜ damit nicht erforderlich sei (Anm. *Brodowski*, JR 2011, 533, 534), greift jedoch zu kurz, da Maßnahmen nach § 100f I StPO bereits vom Regelungszweck her nicht vorrangig auf – erst recht nicht als Ersatz für – eine Überwachung und Aufzeichnung von Telekommunikation ausgerichtet und ausgelegt sind (vgl. bspw. auch das Fehlen entsprechender Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung). Darüber hinaus wäre in einem solchen Falle das Erfassen der begehrten Kommunikation von erheblichen Zufälligkeiten abhängig (z. B. Abhör- und Aufzeichnungsqualität bei Einsatz von Richtmikrofonen, Aufrechterhalten der Überwachung bei einem Fortbewegen der Zielperson etc.) und würde zudem im Regelfall mitunter nur einen Teil des Telefonates für Ermittlungspersonen erfassbar machen, nämlich das gesprochene Wort der Zielperson, da ein Lautschalten von Gesprächen im Außenbereich eher den Ausnahmefall darstellen dürfte. Maßnahmen nach § 100f StPO stellen somit weder ein geeignetes technisches Mittel zum Abhören verschlüsselter Telefonate noch eine vergleichbar effiziente Alternative zu einer Maßnahme der Quellen-TKÜ dar; siehe hierzu auch die Ausführungen unter 3. Teil A.I.1.c).

gemäß § 100f IV i. V. m. § 100b I S. 1 StPO das Gericht (im Ermittlungsverfahren der Ermittlungsrichter, §§ 162 I S. 1, 169 StPO bzw. nach Erhebung der öffentlichen Klage das mit der Sache befasste Gericht, § 162 III StPO), bei Gefahr im Verzug der Staatsanwalt (§ 100b I S. 2 StPO) zuständig. Diesbezüglich gelten auch die übrigen Bestimmungen des § 100b I StPO, also die Regelungen zur richterlichen Bestätigung staatsanwaltschaftlicher Anordnungen binnen drei Werktagen gemäß § 100b I S. 3 StPO sowie die Vorschriften über die Befristung und Verlängerung von Anordnungen nach § 100b I S. 4 und S. 5 StPO, entsprechend. Hinsichtlich der unverzüglichen Beendigung der Maßnahme bei Wegfall der Anordnungsvoraussetzungen ist § 100b IV S. 1 StPO entsprechend anzuwenden. Im Hinblick auf die formalen inhaltlichen Anforderungen der Anordnung gelten kraft Verweisung des § 100f IV StPO auf § 100d II StPO allerdings die – im Vergleich zu § 100b II S. 2 StPO – strengeren Vorgaben des § 100d II S. 2 StPO. Diese verlangen in der Entscheidungsformel des Beschlusses u. a. zusätzlich die Angabe des Tatvorwurfs (§ 100d II S. 2 Nr. 2 StPO) sowie Angaben zur Art der zu erhebenden Informationen und deren Bedeutung für das Verfahren (§ 100d II S. 2 Nr. 5 StPO).

Für die Verwertung von Zufallsfunden zu repressiven Zwecken in anderen Verfahren gilt die Regelung des § 477 II S. 2 StPO. Auch bei Maßnahmen nach § 100f StPO sind gemäß § 101 I StPO die dort vorgeschriebenen grundrechtssichernden Verfahrensregelungen zu beachten.[254]

d) Erhebung von Verkehrsdaten, § 100g StPO

Die Vorschrift des § 100g StPO[255] enthält die strafprozessuale Befugnis zur heimlichen Erhebung[256] von sowie Auskunftseinholung[257] über Verkehrsdaten und ermöglicht damit den Zugriff auf solche Daten, die bei der Erbringung eines Telekommunikationsdienstes[258] erhoben, verarbeitet oder genutzt werden (*Verkehrsdaten*[259], § 3 Nr. 30 TKG) und als sog. *nähere Umstände des Telekommunikationsvorgangs* ebenfalls dem Fernmeldege-

254 Vgl. *Bär*, TK-Überwachung, § 100f StPO, Rn. 23 f.

255 In der gegenwärtigen Fassung durch Gesetz vom 21.12.2007 (BGBl. I S. 3198) m. W. v. 01.01.2008 unter Zusammenfassung und Erweiterung der früheren §§ 100g, h StPO a. F.

256 Durch die Strafverfolgungsbehörden selbst.

257 Bei den Telekommunikationsdiensteanbieter.

258 Auch bei erfolglosen Verbindungsversuchen, vgl. § 88 I S. 2 TKG.

259 Auch *Verbindungsdaten*; hiervon erfasst sind bspw. Häufigkeit, Zeitpunkt und Dauer von Telekommunikationsverbindungen sowie die Kennungen der daran beteiligte Anschlüsse, vgl. auch *Bär*, TK-Überwachung, § 100g StPO, Rn. 3.

heimnis aus Art. 10 I GG unterliegen.[260] Inhaltlich konkretisieren sich die über § 100g StPO erhebbaren Verkehrsdaten kraft der allgemeinen Verweisung in § 100g I S. 1 StPO anhand des abschließenden Katalog des § 96 I TKG.[261] Die Maßnahme dient hierbei der Beschaffung von Beweismitteln, der Ermittlung der Identität bislang unbekannter Täter, der Ermittlung von Kommunikationspartnern bzw. etwaigen Komplizen, der Standortbestimmung des Beschuldigten zu einem bestimmten Zeitpunkt (insbesondere der Tatzeit) oder dessen gegenwärtigen Aufenthaltsortes sowie auch der Feststellung, ob und gegen wen bspw. Maßnahmen der (Quellen-)Telekommunikationsüberwachung erfolgversprechend sein könnten.[262]

Bei Vorliegen eines *von bestimmten Tatsachen begründeten Verdachts*[263], dass jemand als Täter oder Teilnehmer 1. eine *Straftat von auch im Einzelfall erheblicher Bedeutung*, insbesondere[264] eine in § 100a II StPO bezeichnete Straftat, begangenen hat, bei Versuchsstrafbarkeit zu begehen versucht hat oder durch eine Straftat vorbereitet hat (§ 100g I S. 1 Nr. 1 StPO), *oder* (alternativ) 2. eine (grds. auch minderschwere[265]) *Straftat mittels Telekommunikation* begangen hat (§ 100g I S. 1 Nr. 2 StPO)[266], dürfen auch ohne

---

260 Vgl. BVerfG NJW 2007, 351 (353); BVerfG NJW 2005, 2603 (2604); BVerfG NJW 2003, 1787 (1788); BVerfG NJW 2000, 55 (56); st. Rspr.; siehe auch § 88 I S. 1 TKG; für Einzelheiten zur Reichweite des sachlichen Schutzbereichs des Fernmeldegeheimnisses aus Art. 10 I GG, siehe 1. Teil B.I.1.

261 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100g, Rn. 4; BT-Drs. 16/5846, S. 51; BeckOK – *Hegmann*, StPO, Ed. 13, § 100g, Rn. 1.

262 Vgl. BT-Drs. 14/7008, S. 6; Meyer-Goßner – *Cierniak*, StPO, § 100g, Rn. 3 u. 16; auch *Backes*/*Gusy*, Wer kontrolliert die Telefonüberwachung?, S. 128.

263 Somit ist für die Maßnahme nach § 100g I StPO derselbe Verdachtsgrad wie für eine Maßnahme nach § 100a I StPO erforderlich.

264 Die Verweisung auf den Katalog des § 100a II StPO ist daher nicht abschließend; es muss sich bezüglich des Merkmals *Straftat von erheblicher Bedeutung* aber mindestens um eine Straftat der mittleren Kriminalität handeln, diese den Rechtsfrieden empfindlich stören und dazu geeignet sein, das Rechtssicherheitsgefühl der Bevölkerung erheblich zu beeinträchtigen, vgl. BVerfG NJW 2005, 1338 (1339), weshalb eine Maßnahme nach § 100g StPO bei Antrags- und Bagatelldelikten sowie bei Ordnungswidrigkeiten ausscheidet, vgl. Meyer-Goßner – *Cierniak*, StPO, § 100g, Rn. 13; *Bär*, TK-Überwachung, § 100g StPO, Rn. 10 f. m. w. N.

265 Da eine Aufklärung mittels Telekommunikation begangener Straftaten ohne Zugriff auf Verkehrsdaten wie insb. der Nummer des relevanten Anschlusses i. d. R. nicht möglich wäre, vgl. BR-Drs. 702/01, S. 7; ebenso Meyer-Goßner – *Cierniak*, StPO, § 100g, Rn. 17 m. w. N.; da der Beschuldigte das jeweilige Telekommunikationsmedium bewusst zur Begehung seiner strafbaren Handlungen verwendet, steht die Absenkung der Anforderungen an die Schwere der Straftat auch in Einklang mit dem verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz, vgl. BVerfG NJW 2006, 3197 (3198).

266 Hierzu zählen alle Straftaten, bei denen Telekommunikation bspw. über (Mobil- oder Festnetz-)Telefon, Faxgerät oder internetfähigen Computer (z. B. Internet-

Wissen des Betroffenen Telekommunikationsverkehrsdaten (§ 96 I TKG, *§ 113a TKG*[267]) erhoben bzw. Auskünfte eingeholt werden. Dies ist gemäß § 100g I S. 1 StPO nur zulässig, soweit die Erhebung für die *Erforschung des Sachverhaltes* oder die *Ermittlung des Aufenthaltsortes* des Beschuldigten *erforderlich* ist. Unter einer darüber hinausgehenden Subsidiaritätsklausel stehen zumindest die Fälle des § 100g I S. 1 Nr. 1 StPO (*Straftat von erheblicher Bedeutung*) nicht.[268] In den Fällen des § 100g I S. 1 Nr. 2 StPO (*Straftat mittels Telekommunikation*) ist die Maßnahme allerdings nur unter der erhöhten Voraussetzung des § 100g I S. 2 StPO zulässig, dass die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise *aussichtslos* wäre und (kumulativ) die Erhebung der Daten in einem *angemessenen Verhältnis* zur Bedeutung der Sache steht, § 100g I S. 3 StPO.

Bei Vorliegen dieser Voraussetzungen legitimiert die Eingriffbefugnis aus § 100g StPO Strafverfolgungsbehörden hierbei zum Erheben und Aufzeichnen von Verkehrsdaten mit *eigenen technischen Mitteln* in Echtzeit („Live).[269]

Die Norm umfasst darüber hinaus auch einen *Auskunftsanspruch* gegenüber TK-Diensteanbietern über vergangene als auch über zukünftig anfallende Verkehrsdaten, wie er bis zum 31.12.2007 in den früheren Vorschrif-

---

telefonie oder E-Mailing) als Mittel zur Tatausführung (im Sinne eines Tatinstruments) genutzt wird, vgl. auch *Bär*, TK-Überwachung, § 100g StPO, Rn. 12; Meyer-Goßner – *Cierniak*, StPO, § 100g, Rn. 17 m. w. N.

267 Die zum Zwecke der Umsetzung der Richtlinie 2006/24/EG zur Speicherung von bestimmten Verkehrsdaten für die Dauer von 6 Monaten auf Vorrat (sog. *Vorratsdatenspeicherung*) in das nationale Recht eingefügten §§ 113a, 113b TKG wurden durch Entscheidung des BVerfG vom 02.03.2010 wegen Verstoßes gegen Art. 10 I GG für nichtig erklärt; soweit gegenwärtig über § 100g I S. 1 StPO Verkehrsdaten nach § 113a TKG erhoben werden dürfen, verstößt auch diese Vorschrift gegen Art. 10 I GG und ist insoweit nichtig; nach Auffassung des BVerfG sei eine vorsorgliche, anlasslose Speicherung von Telekommunikationsverkehrsdaten durch private Diensteanbieter allerdings mit Art. 10 GG nicht schlechthin unvereinbar, bedürfe zur Wahrung der Verhältnismäßigkeit aber hinreichend anspruchsvoller und normenklarer Regelungen hinsichtlich Datensicherheit, Datenverwendung, Transparenz und Rechtsschutz, vgl. BVerfG NJW 2010, 833; für Einzelheiten siehe auch die Ausführungen bei Meyer-Goßner – *Cierniak*, StPO, § 100g, Rn. 7 m. w. N. und BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 115; hiervon unberührt bleibt aber der Zugriff über § 100g I S. 1 StPO auf (zurückliegende) Verkehrsdaten, die von TK-Diensteanbietern gemäß §§ 96 ff. TKG erhoben und gespeichert werden.

268 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100g, Rn. 16, wobei allerdings ergänzend der Verhältnismäßigkeitsgrundsatz zu beachten ist.

269 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100g, Rn. 3; insoweit handelt es sich bei § 100g StPO n. F. um eine dem § 100a StPO inhaltlich nachgebildete umfassende Befugnis zum Erheben von Verkehrsdaten, und zwar auch in Echtzeit („Live"), vgl. *Bär*, TK-Überwachung, § 100g StPO, Rn. 1 sowie BT-Drs. 16/5846, S. 50.

ten der *§§ 100g, h StPO a. F.*[270] enthalten war.[271] Dies ergibt sich aus der entsprechenden Verweisung des § 100g II S. 1 StPO auf die Mitwirkungspflichten des § 100b III StPO (i. V. m. § 110 II TKG, § 1 Nr. 8 TKÜV[272]).[273] Neben der Verpflichtung zur (unverzüglichen) Mitwirkung an einer „Live"-Ausleitung von (zukünftigen) Verkehrsdaten an die Strafverfolgungsbehörden[274] haben TK-Diensteanbieter auf Grund der Regelung des § 100g I StPO auch Auskunft über solche (vergangene sowie zukünftige) Verkehrsdaten zu erteilen, welche von ihnen in Einklang mit den bestehenden gesetzlichen Bestimmungen (in der Vergangenheit) erhoben worden und noch gespeichert sind bzw. (zukünftig) hiernach anfallen werden.[275] So ist über § 100g I S. 1 StPO ein strafprozessualer Zugriff auf die nach § 96 I TKG von Dienteanbietern in telekommunikations- und datenschutzrechtlich zulässiger Weise zu Zwecken der §§ 97 ff. TKG, insbesondere der Entgeltermittlung und Entgeltabrechnung (§ 97 TKG), der Bereitstellung von Diensten im Zusammenhang mit Standortdaten (§ 98 TKG) und des Einzelverbindungsnachweises (§ 99 TKG), erhobenen und gespeicherten Verkehrsdaten möglich.

Zu den abschließend[276] in § 96 I TKG aufgeführten, nach § 100g I StPO erhebbaren Verkehrsdaten zählen hierbei v. a. Nummer oder Kennung[277] der beteiligten Anschlüsse/Endeinrichtungen, personenbezogene Berechtigungskennungen und bei mobilen Anschlüssen auch Standortdaten (vgl. Nr. 1), Beginn und Ende der Verbindungen (vgl. Nr. 2), der vom Nutzer jeweils in Anspruch genommene Telekommunikationsdienst (vgl. Nr. 3), Endpunkte

---

270 §§ 100g, h StPO a. F. als Nachfolgeregelung des bis zum 31.12.2001 gültigen § 12 Fernmeldeanlagengesetz (FAG) durch Gesetz v. 20.12.2001 (BGBl. I 2001, 3879) m. W. v. 01.01.2002 in die StPO eingefügt, zunächst befristet bis zum 31.12.2004, durch Gesetz v. 09.12.2004 (BGBl. I 2004, 3231) bis zum 31.12.2007 verlängert.

271 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100g, Rn. 3 u. 11.

272 Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Telekommunikations-Überwachungsverordnung – TKÜV) vom 03.11.2005 (BGBl. I S. 3136).

273 Vgl. BT-Drs. 16/5846, S. 50.

274 Oder alternativ die gebündelte Auskunft an die Strafverfolgungsbehörden in bestimmten Zeitabständen, vgl. BT-Drs. 16/5846, S. 51; BeckOK – *Hegmann*, StPO, Ed. 13, § 100g, Rn. 7; Meyer-Goßner – *Cierniak*, StPO, § 100g, Rn. 29.

275 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100g, Rn. 29 f. m. w. N.; BT-Drs. 16/5846, S. 50.

276 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100g, Rn. 4.

277 Hierzu zählen insbesondere die IMEI-Nummer von mobilen GSM- und UMTS-Endgeräten sowie (dynamische) IP-Adressen von an das Internet angeschlossenen Endgeräten, anhand derer sich letztlich im Wege des manuellen Auskunftsverfahrens nach §§ 161, 163 StPO i. V. m. § 113 TKG Anschlussinhaber eindeutig individualisieren lassen, vgl. hierzu auch Meyer-Goßner – *Cierniak*, StPO, § 100g, Rn. 5 m. w. N.; BeckOK – *Hegmann*, StPO, Ed. 13, § 100g, Rn. 6 m. w. N.; aber str.

von festgeschalteten Verbindungen mit Beginn und Ende (vgl. Nr. 4) als auch sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten (vgl. Nr. 5). Erfasst sind von diesen Fallkonstellationen auch die im Rahmen erfolgloser Verbindungsversuche angefallenen Verkehrsdaten (vgl. § 88 I S. 2 TKG).

Nach Abschluss des Telekommunikationsvorgangs kommen für die Erhebung von (vergangenen) Verkehrsdaten gemäß der klarstellenden Vorschrift des § 100g III StPO zudem auch die allgemeinen Vorschriften in Betracht, allerdings nur soweit die Erhebung nicht beim TK-Diensteanbieter erfolgt.[278] Denn nach Auffassung des BVerfG bestehen die spezifischen Gefahren der räumlich distanzierten Kommunikation (und mithin der Schutzzweck des Fernmeldegeheimnisses aus Art. 10 I GG) im Herrschaftsbereich des Empfängers nicht, da dieser eigene Schutzvorkehrungen gegen einen ungewollten Datenzugriff treffen kann.[279] Deshalb dürfen bspw. Gegenstände im Herrschaftsbereich des Betroffenen, die Verkehrsdaten enthalten oder Erkenntnisse über Verkehrsdaten vermitteln können, wie z. B. Datenträger mit darauf abgespeicherten Verkehrsdaten, nach den allgemeinen Vorschriften der §§ 94 ff. und §§ 102 ff. StPO sichergestellt werden[280], allerdings unter Rücksichtnahme auf die erhöhte Schutzwürdigkeit von Verkehrsdaten, die beim Betroffenen gespeichert sind und außerhalb dessen Herrschaftsbereichs dem besonderen Schutz des Art. 10 I GG unterliegen.[281]

Wie bereits oben angesprochen, gestattet die Befugnisnorm des § 100g StPO neben der Ermittlung von vergangenen Verkehrsdaten grds. auch ein Erheben der Verkehrsdaten in Echtzeit.[282] Das Erheben von Standortdaten[283] (§ 96 I Nr. 1 TKG, typischerweise von Mobilfunkgeräten) in Echtzeit ist

---

278 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100g, Rn. 11.

279 Vgl. BVerfG NJW 2006, 976 (978).

280 Beeinträchtigtes Grundrecht ist insoweit nicht das Fernmeldegeheimnis aus Art. 10 I GG, sondern das Grundrecht auf informationelle Selbstbestimmung aus Art. 2 I i. V. m. 1 I GG sowie ggf. hinsichtlich der Örtlichkeit der Sicherstellung das Grundrecht auf Unverletzlichkeit der Wohnung aus Art 13 I GG, vgl. BVerfG NJW 2006, 976 (978).

281 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100g, Rn. 11; BVerfG NJW 2006, 976 (982).

282 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100g, Rn. 3.

283 Z. B. durch Abgleich von Funkzellendaten über eingeloggte Mobiltelefone mit der jeweiligen IMEI-Nummer des Zielgerätes; Positionsmeldungen (sog. *geografische Daten*) von Mobiltelefonen können hierbei sowohl bei aktiver Telekommunikation als auch bei bloßem empfangsbereiten Zustand des Endgerätes (*Standby)* erfasst werden, da sich ein Mobiltelefon, auch während damit nicht aktiv telekommuniziert wird, zur Gewährleistung der Empfangsbereitschaft stets in die sich geografisch am nähesten befindliche Funkzelle einloggt, vgl. insoweit *Demko*, NStZ 2004, 57 (57).

nach § 100g I S. 3 StPO aus Verhältnismäßigkeitsgründen[284] allerdings nur im Falle des § 100g I S. 1 Nr. 1 StPO (*Straftat von auch im Einzelfall erheblicher Bedeutung*) zulässig.

Im Gegensatz zu einer Maßnahme der Telekommunikationsüberwachung nach §§ 100a, 100b StPO – in deren Rahmen zwar auch auf Verkehrsdaten der jeweiligen Telekommunikation zugegriffen werden darf, deren Schwerpunkt aber in der Erfassung der jeweils ausgetauschten Inhaltsdaten einer geführten Telekommunikation liegt – hat eine Maßnahme nach § 100g StPO allein die Erhebung von bzw. Auskunft über Verkehrsdaten zum Gegenstand. Ein Zugriff auf Inhalte der jeweiligen Kommunikation ist – gerade auf Grund der abgesenkten Eingriffsvoraussetzungen des § 100g StPO – über eine solche Maßnahme nicht möglich. Bezogen auf die besondere Fallkonstellation der Internettelefonie kann über eine Maßnahme nach § 100g StPO somit kein Zugriff auf die Inhalte der via Internet ausgetauschten Telekommunikationssignale erfolgen.[285] Auf die Verbindungsdaten (*Verkehrsdaten*) hingegen, die im Rahmen der Erbringung des VoIP-Dienstes als Telekommunikationsdienst[286] anfallen, wie insbesondere die Kennungen der (Internet-)Anschlüsse der an der VoIP-Kommunikation beteiligten Gesprächspartner sowie die den Anschlüssen zum Zeitpunkt (Datum, Uhrzeit) der Telekommunikation zugeteilten IP-Adressen[287], kann auch – gesondert von einer (Quellen-)TKÜ-Maßnahme – mit einer Maßnahme nach § 100g StPO zugegriffen werden. Ggf. wird eine solche Maßnahme im Vorfeld einer (Quellen-)TKÜ-Maßnahme durchzuführen sein, insbesondere um die nach § 100b II S. 2 StPO in die Anordnung einzustellenden Angaben – vor allem hinsichtlich der Rufnummer bzw. anderen Kennung des zu überwachenden Anschlusses oder des Endgerätes (vgl. § 100b II S. 2 Nr. 2 StPO) sowie des Namens und der Anschrift[288] des Maßnahmeadressaten (vgl. § 100b II S. 2 Nr. 1 StPO) – zu eruieren.

---

284 Da sich über die systematische Erfassung und Auswertung der Positionsmeldungen eines Mobiltelefons bei ständiger Ortung regelrechte Bewegungsprofile in Echtzeit erstellen lassen.

285 Vgl. auch Meyer-Goßner – *Cierniak*, StPO, § 100g, Rn. 3.

286 Zur Frage der rechtlichen Einordnung eines softwarebasierten VoIP-Dienstes als Telekommunikationsdienst i. S. d. TKG, siehe 2. Teil A.II.6.b).

287 Sog. *Internet-Protokoll-Adresse*, eine Art „postalische" Adresse für die in einem auf dem Internetprotokoll aufbauenden Computernetz befindlichen Rechner/Geräte (Server, PCs etc.), wodurch die Rechner/Geräte adressierbar und damit erreichbar gemacht werden, vgl. BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 14; http://de.wikipedia.org/wiki/IP-Adresse (zuletzt aufgerufen 15.06.2012).

288 Nach Ermittlung der einem bestimmten Anschluss zu einer bestimmten Uhrzeit zugeordneten dynamischen IP-Adresse im Wege der Maßnahme nach § 100g StPO, lassen sich anschließend anhand dieser individualisierenden Verkehrsdaten die Identität der dahinter stehenden Person und deren Anschrift als Bestandsdaten

Hinsichtlich des Maßnahmeadressaten gilt gemäß § 100g II S. 1 StPO die Vorschrift des § 100a III StPO entsprechend. Somit kann sich auch die Erhebung von oder die Auskunft über Verkehrsdaten neben dem Beschuldigten auch gegen Dritte in den Fällen der Nachrichtenmittlung oder Anschlussbenutzung richten.

Auch bei Maßnahmen nach § 100g StPO enthält die Befugnisnorm im Wege der Annexkompetenz hierbei konkludent die Ermächtigung zu solchen Maßnahmen, die als Begleitmaßnahmen (sog. *Sekundärmaßnahmen*) zur Vorbereitung und Durchführung der *Primärmaßnahmen* der Verkehrsdatenerhebung bzw. Auskunftseinholung über Verkehrsdaten bei den TK-Diensteanbietern erforderlich sind.[289]

In formeller Hinsicht gelten über die Verweisung des § 100g II S. 1 StPO die Vorschriften des § 100b I bis IV S. 1 StPO entsprechend. Bezüglich der Anordnungskompetenz findet § 100b I S. 1 und S. 2 StPO entsprechende Anwendung. Hinsichtlich Form und Inhalt der Anordnung einer Maßnahme nach § 100g I StPO sind zwar (auch bei Straftaten von erheblicher Bedeutung) in der schriftlichen Anordnung Art, Umfang und Dauer der Maßnahme (entspr. § 100b II S. 2 Nr. 3 StPO) anzugeben.[290] Gemäß § 100g II S. 2 StPO genügt im Falle einer *Straftat von erheblicher Bedeutung* (§ 100g I S. 1 Nr. 1 StPO) abweichend von § 100b II S. 2 Nr. 2 StPO (Angabe der Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgerätes) eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation[291], wenn die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre.

In die Anordnung ist eine Befristung der Maßnahme mit aufzunehmen, soweit durch die Erhebung – mit eigenen technischen Mitteln oder durch Auskunftseinholung – auf zukünftige Verkehrsdaten zugegriffen werden soll.[292]

(§§ 111, 95, 3 Nr. 3 TKG) im Wege des manuellen Auskunftsverfahrens nach §§ 161, 163 StPO i. V. m. § 113 TKG abrufen, vgl. Meyer-Goßner – *Cierniak*, StPO, § 100g, Rn. 5; BeckOK – *Hegmann*, StPO, Ed. 13, § 100g, Rn. 6 m. w. N.; aber str.

289 Vgl. *Bär*, TK-Überwachung, § 100g, Rn. 36 m. w. N.; hierzu auch BGH-Ermittlungsrichter NStZ 2005, 278 (278).

290 Name und Anschrift des Betroffenen, gegen den sich die Maßnahme richtet, sind unter entsprechender Anwendung des § 100b II S. 2 Nr. 1 StPO ohnehin nur „soweit möglich" anzugeben.

291 Womit auch die sog. *Funkzellenabfrage* zur Auskunft über Verkehrsdaten aus Mobilfunktelefonaten, welche von einem (noch) unbekannten Täter oder Nachrichtenmittler aus einer bestimmten Funkzelle zu einem bestimmten Zeitpunkt geführt wurden, möglich ist, vgl. auch Meyer-Goßner – *Cierniak*, StPO, § 100g, Rn. 27; vgl. zur Funkzellenabfrage auch *Wohlers*/*Demko*, StV 2003, 241 (247).

292 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100g, Rn. 28.

Die Dauer der Maßnahme darf gemäß der Verweisung des § 100g II S. 1 StPO auf § 100b I S. 4 und S. 5 StPO auf maximal 3 Monate festgesetzt werden, wobei eine Verlängerung um jeweils nicht mehr als 3 Monate zulässig ist, soweit die Voraussetzungen des § 100g StPO fortbestehen.

Auch bezüglich Maßnahmen nach § 100g StPO finden die grundrechtssichernden Regelungen des § 101 StPO Anwendung (§ 101 I StPO).

Die Verwertung der rechtmäßig erlangten Erkenntnisse gestaltet sich in entsprechender Weise nach den allgemeinen Grundsätzen, wie sie auch für Maßnahmen nach §§ 100a, 100b StPO Anwendung finden. Die Verwertung von Zufallsfunden in anderen Strafverfahren richtet sich nach den Vorschriften des § 477 II S. 2 StPO.[293]

e) Einsatz sonstiger technischer Mittel, § 100h I S. 1 Nr. 2 StPO

Die Befugnisnorm des § 100h StPO regelt in der Tatbestandsvariante des Abs. 1 S. 1 Nr. 2 die Verwendung von sog. *sonstigen besonderen für Observationszwecke bestimmten technischen Mitteln* außerhalb von Wohnungen[294] (einschließlich sonstiger Räumlichkeiten, die dem Schutz des Art. 13 I GG unterfallen) auch ohne Wissen der Betroffenen. Einschlägiges Grundrecht bei Maßnahmen nach § 100h StPO ist das allgemeine Persönlichkeitsrecht aus Art. 2 I i. V. m. Art. 1 I GG.[295] Im Sinne einer entwicklungsoffen gehaltenen Tatbestandsformulierung ist hierbei die Bezeichnung des Merkmal der *besonderen für Observationszwecke bestimmten technischen Mittel*, wie in § 100h I S. 1 Nr. 2 StPO erfolgt, in hinreichendem Maße konkretisiert und wird mithin den verfassungsrechtlichen Anforderungen an Grundrechtseingriffe gerecht.[296]

Als Eingriffsvoraussetzung genügt – mangels qualifizierter gesetzlicher Anforderung – das Vorliegen sog. *einfachen Tatverdachts* (Anfangsverdacht, §§ 152 II, 160 I StPO).[297] Zudem ist gemäß § 100h I S. 1 StPO erforderlich, dass die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise *weniger erfolgversprechend oder erschwert* wäre, als zu beachtende – im Vergleich zu den anderen heimlichen Ermittlungsmaßnahmen, insbesondere § 100a I Nr. 3 StPO („wesent-

---

293 Vgl. im Einzelnen Meyer-Goßner – *Cierniak*, StPO, § 100g, Rn. 34 f. m. w. N.

294 In klarer Trennung zur akustischen Wohnraumüberwachung nach §§ 100c ff. StPO, siehe hierzu 1. Teil A.II.2.b).

295 Vgl. BVerfG NJW 2005, 1338 (1340).

296 Vgl. BVerfG NJW 2005, 1338 (1339 f.); *Bär*, TK-Überwachung, § 100h StPO, Rn. 6.

297 Vgl. BeckOK – *Hegmann*, StPO, Ed. 13, § 100h, Rn. 12; KK – *Nack*, StPO, § 100h, Rn. 6.

lich erschwert oder aussichtslos“) deutlich abgeschwächte[298] – Subsidiäritätsklausel.[299] Wegen der im Vergleich zur Herstellung von Bildaufnahmen nach § 100h I S. 1 Nr. 1 StPO schwerwiegenderen technischen Mitteln i. S. d. § 100h I S. 1 Nr. 2 StPO ist die Verwendung sonstiger besonderer Mittel zur Observation nur unter der zusätzlichen Voraussetzung des § 100h I S. 2 StPO zulässig, dass Gegenstand der Untersuchung eine *Straftat von erheblicher Bedeutung* ist, wobei das Gesetz hier – anders als bspw. bei § 100g I S. 1 Nr. 1 StPO oder § 100a I Nr. 2 StPO – auf die zusätzliche Bedingung „auch im Einzelfall“ verzichtet hat.[300]

Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung werden von § 100h StPO nicht vorgehalten, da Eingriffe in das allgemeine Persönlichkeitsrecht durch den Einsatz technischer Observationsmittel nach Auffassung des BVerfG in ihrem Ausmaß und ihrer Intensität typischerweise nicht den unantastbaren Kernbereich der privaten Lebensgestaltung erfassen.[301]

Neben dem Beschuldigten nach § 100h II S. 1 dürfen sich Maßnahmen nach § 100h I S. 1 Nr. 2 StPO gegen andere Personen (sog. Nichtbeschuldigte als Maßnahmeadressaten) nur unter den zusätzlichen (erhöhten) Voraussetzungen des § 100h II S. 2 Nr. 2 StPO (Annahme auf Grund bestimmter Tatsachen[302], dass die Person mit dem Beschuldigten in Verbindung steht oder eine solche herstellen wird, Erfolgsprognose und strengere Subsidiaritätsklausel[303]), welche kumulativ erfüllt sein müssen, richten.

Die – i. d. R. bereits technisch – unvermeidbare Mitbetroffenheit Dritter von Maßnahmen der technischen Observation außerhalb der Wohnung, bspw. neben der Zielperson befindliche unbeteiligte Passanten, ist gemäß § 100h III StPO für die Anordnung und Durchführung der Maßnahmen unschädlich.[304]

Bei Vorliegen der Voraussetzungen gestattet die Vorschrift des § 100h I S. 1 Nr. 2 StPO den heimlichen Einsatz solcher „sonstiger“ technischer

---

298 Auf Grund der gesetzgeberischen Wertung von Maßnahmen nach § 100h I StPO als „verhältnismäßig wenig eingriffsintensive[.] Maßnahmen“ (BT-Drs. 12/989, S. 39).

299 Vgl. *Bär*, TK-Überwachung, § 100h StPO, Rn. 3.

300 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100h, Rn. 3 u. 4; *Bär*, TK-Überwachung, § 100h StPO, Rn. 13, wonach auch hier dennoch der Verhältnismäßigkeitsgrundsatz zu beachten ist.

301 Vgl. BVerfG NJW 2005, 1338 (1340).

302 Zur Reichweite der Voraussetzung „auf Grund bestimmter Tatsachen“, siehe Meyer-Goßner – *Cierniak*, StPO, § 100h, Rn. 7, § 100f, Rn. 11 m. w. N.

303 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100h, Rn. 7.

304 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100h, Rn. 9.

Mittel außerhalb von Wohnungen, die weder das Herstellen von Bildaufnahmen i. S. d. § 100h I S. 1 Nr. 1 StPO[305] betreffen noch ein Überwachen und Aufzeichnen des gesprochenen Wortes außerhalb von Wohnungen i. S. d. § 100f I StPO zum Gegenstand haben, aber die Observation ermöglichen.[306] Abzugrenzen sind Maßnahmen nach § 100h I StPO auch von Maßnahmen der längerfristigen Observation nach § 163f I StPO[307], für die in Ergänzung der Vorschrift des § 100h StPO unabhängig vom Einsatz technischer Mittel zusätzliche Voraussetzungen formuliert sind[308] und – anders als § 100h I StPO – gemäß § 163f III S. 1 StPO grds. unter Richtervorbehalt stehen. Unter die Vorschrift des § 100h I S. 1 Nr. 2 StPO fallen demnach u. a. die Verwendung von Bewegungsmeldern und Peilsendern wie auch der Einsatz neuartiger technischer Observationsmittel wie bspw. die satellitengestützte Ortung mittels GPS (*Global Positioning System*).[309]

Nicht erfasst von der Befugnis des § 100h I S. 1 Nr. 2 StPO zum Einsatz sonstiger technischer Mittel hingegen ist die Verwendung staatlicher Überwachungsprogramme wie bspw. *Trojaner*[310], *Keylogger* und sonstige

---

305 Die Eingriffsbefugnis des § 100h I S. 1 Nr. 1 StPO hingegen bezieht sich auf die Herstellung von Bildaufnahmen zu Observationszwecken und gestattet hierfür die (heimliche) Herstellung von Lichtbildern sowie Video- und Filmaufnahmen außerhalb von Wohnungen und nicht allgemein zugänglichen Räumen, also bspw. das Fotografieren des Beschuldigten auf der Straße oder auch beim Verlassen seines Grundstücks, vgl. Meyer-Goßner – *Cierniak*, StPO, § 100h, Rn. 1. m. w. N.; im Zusammenhang mit dem Zugriff auf Internettelefonie ist lediglich denkbar, dass eine Zielperson beim Führen eines solchen Telefonats in allgemein zugänglichen Räumen oder im Freien gestützt auf die Befugnisnorm des § 100h I S. 1 Nr. 1 StPO fotografiert oder gefilmt wird; der Zugriff auf die visuellen TK-Daten bspw. einer geführten Videotelefonie oder gar die Erstellung sog. *Screenshots* von der Benutzeroberfläche des verwendeten Endgerätes ist vom Merkmal des „Herstellens von Bildaufnahmen" i. S. d. § 100h I S. 1 Nr. 1 StPO freilich nicht erfasst.

306 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100h, Rn. 2; *Bär*, TK-Überwachung, § 100h StPO, Rn. 6 m. w. N.; BeckOK – *Hegmann*, StPO, Ed. 13, § 100h, Rn. 6.

307 Gemäß der Legaldefinition des § 163f I S. 1 StPO ist unter einer längerfristigen Observation eine planmäßig angelegte Beobachtung zu verstehen, die durchgehend länger als 24 Stunden dauern (Nr. 1) oder an mehr als zwei Tagen stattfinden soll.

308 Vgl. BVerfG NJW 2005, 1338 (1340).

309 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100h, Rn. 2 m. w. N.

310 Bei einem sog. *Trojaner*, abgeleitet vom Trojanischen Pferd aus der griechischen Mythologie, handelt es sich um ein unerwünschtes, i. d. R. auch schadhaftes Computerprogramm (sog. *Malware*), welches entweder als nützliche Anwendung getarnt oder auch unbewusst vom Betroffenen auf sein System geladen wird und dieses dort im Hintergrund ausspionieren oder auch manipulieren kann, vgl. *Bär*, TK-Überwachung, Glossar, S. 375; *Köhler*/*Kirchmann*, IT von A bis Z, S. 235; vgl. auch dpa-Artikel „Lauscher im Hintergrund", Nürnberger Nachrichten/Fürther Nachrichten vom 11.10.2011, S. 2.

Spionagesoftware. Eine Subsumtion derartiger Programme – wohlgemerkt weder zum Herstellen von Bildaufnahmen noch zum Aufzeichnen des gesprochenen Wortes[311] – unter die Befugnisnorm des § 100h I S. 1 Nr. 2 StPO ließe sich – z. B. bei Keyloggern – zwar grds. noch auf das Merkmal eines „sonstigen technischen Mittels" stützen, dessen Verwendung „für Observationszwecke" mit einer herkömmlichen Observation zur Erforschung des Sachverhaltes oder der Ermittlung des Aufenthaltsortes eines Beschuldigten verglichen werden könnte.[312] Ein Einsatz derartiger technischer Mittel wäre aber weder mit der (verfassungs-)rechtlichen Ausgestaltung noch mit der gesetzgeberischen Intention[313] oder dem Sinn und Zweck der Vorschrift begründbar[314]. Jenseits einer ausschließlichen Überwachung und Aufzeichnung von Daten aus laufenden Telekommunikationsvorgängen[315] führt der Einsatz von Überwachungsprogrammen auf informationstechnischen Systemen zudem zu einem Eingriff in das vom BVerfG in seiner Entscheidung vom 27.02.2008[316] aus dem allgemeinen Persönlichkeitsrecht nach Art. 2 I i. V. m. Art. 1 I GG neu entwickelten Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Ein solcher wäre jedoch gemäß der Feststellung des BVerfG nur dann verfassungsrechtlich zulässig, wenn „tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut vorliegen"[317]. Entsprechend den erhöhten verfassungsrechtlichen Anforderungen solcher Eingriffe auch im repressiven Bereich wird die Befugnisnorm des § 100h I S. 1 Nr. 2 StPO, welche lediglich Eingriffe in das allgemeine Persönlichkeitsrecht zulässt[318] und überdies keinen Richtervorbehalt enthält, diesen jedoch nicht gerecht.[319]

In formeller Hinsicht besteht hinsichtlich der Zuständigkeit für die Anordnung von Maßnahmen nach § 100h I StPO kein gesetzlicher Richtervorbehalt. Die Maßnahmen dürfen demnach durch die Staatsanwaltschaft

---

311 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100h, Rn. 2.

312 So *Bär*, TK-Überwachung, § 100h StPO, Rn. 10; vgl. auch KK – *Nack*, StPO, § 100h, Rn. 2.

313 Insbesondere auch unter Berücksichtigung der gesetzgeberischen Einordnung von Maßnahmen nach § 100h I StPO als „verhältnismäßig wenig eingriffsintensive […] Maßnahmen" (BT-Drs. 12/989, S. 39).

314 Vgl. *Bär*, TK-Überwachung, § 100h StPO, Rn. 2.

315 Wofür gemäß Feststellung des BVerfG Art. 10 I GG der alleinige grundrechtliche Maßstab ist, vgl. BVerfG NJW 2008, 822 (826).

316 BVerfG NJW 2008, 822.

317 BVerfG NJW 2008, 822 (831) für Eingriffe im Rahmen präventiver Zielsetzung.

318 Vgl. BVerfG NJW 2005, 1338 (1340) m. w. N.

319 Vgl. *Bär*, TK-Überwachung, § 100h StPO, Rn. 10 m. w. N.

(§ 161 I StPO) als auch durch Beamte des Polizeidienstes[320] (§ 163 I StPO) angeordnet werden.[321]

Nach § 101 I StPO gelten auch für Maßnahmen nach § 100h StPO die grundrechtssichernden Verfahrensregelungen des § 101 II bis VIII StPO. Insbesondere sind gemäß § 101 IV S. 1 Nr. 7 StPO die Zielperson sowie erheblich mitbetroffene Personen von den Maßnahmen zu unterrichten, soweit nicht eine Ausnahme nach § 101 IV S. 3 bis S. 5 vorliegt und sobald dies ohne Gefährdung des Untersuchungszwecks möglich ist, § 101 V S. 1 StPO.

Die Verwendung von Zufallsfunden auf Grund von Maßnahmen nach § 100h I S. 1 Nr. 2 StPO in anderen Verfahren richtet sich nach der Vorschrift des § 477 II S. 2 StPO.[322]

3. Technische Umsetzung der Primärmaßnahme

a) Primärmaßnahme der Quellen-TKÜ

Primärmaßnahme einer Quellen-TKÜ ist die eigentliche Überwachung und Aufzeichnung der Telekommunikation an sich. Dies gliedert sich in das Abgreifen, Ausleiten und Aufzeichnen der TK-Daten im Zeitpunkt des Stattfindens der VoIP-Kommunikation[323], also in „Echtzeit", mit dem jeweils für die IP-Kommunikation genutzten System als technischem Anknüpfungspunkt der Maßnahme. Der Zugriff auf die Kommunikationsinhalte erfolgt hierbei entweder vor deren Verschlüsselung auf dem System des Absenders oder nach deren Entschlüsselung auf dem System des Empfängers.[324]

---

320 Eine Beschränkung auf polizeiliche Ermittlungspersonen i. S. d. § 152 GVG – wie bspw. für Durchsuchungsanordnungen bei Gefahr im Verzug nach § 105 I S. 1 StPO – ist der Vorschrift des § 100h StPO nicht zu entnehmen, vgl. *Bär*, TK-Überwachung, § 100h StPO, Rn. 16.

321 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100h, Rn. 10 m. w. N.; ebenso *Bär*, TK-Überwachung, § 100h StPO, Rn. 16.

322 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100h, Rn. 13.

323 Für technische Einzelheiten zu verschlüsselter VoIP, siehe 1. Teil A.I.2.c) sowie 1. Teil A.I.4.

324 Vgl. auch Bundesministerium des Innern, Fragenkatalog BMJ, S. 8, 9, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012); die Argumente, die auf den Zugriff vor der Verschlüsselung auf dem Absendersystem Anwendung finden, lassen sich mutatis mutandis auch auf die Situation des Zugriffs nach der Entschlüsselung auf dem Empfängersystem übertragen; soweit sich deshalb aus dem Zusammenhang nichts anderes ergibt, ist bei den Ausführungen zum Anknüpfen am Absendersystem das Anknüpfen am Empfängersystem entsprechend mitgemeint.

Für die (dogmatische) Beurteilung der Frage, ob der (technische) Ablauf des eigentlichen Zugriffsvorgangs im Rahmen einer Quellen-TKÜ einem Tatbestandsmerkmal der „Überwachung und Aufzeichnung der Telekommunikation" gerecht werden kann, ist eine Konkretisierung des Zugriffsvorgangs angezeigt.

Zum genauen technischen Ablauf der Überwachung im Rahmen einer Quellen-TKÜ-Maßnahme in der behördlichen Praxis finden sich in der einschlägigen Fachliteratur wenige, größtenteils allgemein gehaltenen Ausführungen, die die einzelnen technischen Schritte nur rudimentär schildern.

Vielfach wird der Ablauf des eigentlichen Überwachungsvorgangs pauschal mit „Kopieren und Ausleiten" beschrieben. Diese Darstellung führt zwar zwei wesentliche Grundelemente des Zugriffs an, streift jedoch den regelmäßigen technischen Ablauf einer Quellen-TKÜ-Maßnahme in der Praxis nur peripher.

Unter Berücksichtigung auch von Auskünften des BayLKA[325] – bayernweit zuständige staatliche Stelle für die Durchführung von Quellen-TKÜs[326] – lassen sich die technischen Abläufe der Überwachung und Aufzeichnung im Rahmen einer Quellen-TKÜ-Maßnahme noch weiter konkretisieren:

Sobald der Nutzer den Aufbau einer aktiven Gesprächsverbindung über den VoIP-Dienst (z. B. Skype) einleitet, *aktiviert* sich automatisch auch die bereits vorher heimlich installierte[327] Überwachungssoftware[328].

Nun werden die nach Zustandekommen der Verbindung im Rahmen des laufenden Telekommunikationsvorgangs anfallenden Gesprächsdaten noch vor deren automatischer Verschlüsselung („Codierung") durch die verwendete VoIP-Software[329] mittels der zuvor eingebrachten Überwachungssoftware heimlich „an der Quelle" *in Echtzeit* („*Live*")[330] *abgegriffen*, gedoppelt und – parallel zur Übermittlung an den Empfänger – an einen eigens für die Überwachung genutzten Server zur Aufzeichnung *ausgeleitet*. So jedenfalls, wenn die Quellen-TKÜ-Maßnahme am Rechner des anrufenden Nutzers (Absendersystem) anknüpft. Wird die Maßnahme hingegen auf dem Rechner des angerufenen Nutzers (Empfängersystem) realisiert, so wird die

---

325 *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11.2010.

326 Für Einzelheiten, siehe auch 1. Teil A.II.1.

327 Für technische Einzelheiten zur heimlichen Installation der Überwachungssoftware, siehe 1. Teil A.II.4.

328 Für technische Einzelheiten zur Überwachungssoftware, siehe 1. Teil A.II.3.b).

329 Für technische Einzelheiten zum Ablauf der VoIP-Kommunikation, siehe 1. Teil A.I.1. u. 4.

330 In Echtzeit („Live"): simultan im Moment des Stattfindens der Kommunikation und Entstehens der Signale.

laufende Telekommunikation entsprechend erst nach Eingang und Entschlüsselung („Decodierung“) der Gesprächsdaten auf dem Empfängersystem in Echtzeit („Live“) abgegriffen, gedoppelt und wie beim Ansetzen am Absendersystem über das Datennetz an einen im Vorfeld der Überwachung eigens hierfür behördenseits eingerichteten Server ausgeleitet[331], auf dem die *Aufzeichnung* der in Echtzeit abgegriffenen und ausgeleiteten Telekommunikationsdaten stattfindet.[332] Während ihrer Übermittlung zum Behörden-Server werden die ausgeleiteten Daten über eine von der Überwachungssoftware automatisch vorgenommene Verschlüsselung vor unbefugtem Zugriff geschützt.[333]

Einzelheiten für einen beispielhaften technischen Ablauf des Abgreifens, Ausleitens und Aufzeichnung lassen sich indes auch der Anlage zu einem Schreiben des Bayerischen Staatsministeriums der Justiz zur Frage der „Kostenverteilung zwischen Polizei und Staatsanwaltschaften im Strafverfahren“[334] bezüglich der „Kosten der Telekommunikationsüberwachung bei Einsatz von Voice-over-IP und der Software Skype“ entnehmen, welches seitens der *Piratenpartei* bereits im September 2008 im Internet veröffentlicht[335] wurde. Dessen tatsächliche Authentizität vorausgesetzt[336], würde

---

331 In diese Richtung *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11.2010.

332 In diese Richtung *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11.2010 und E-Mail vom 21.02.2011.

333 Vgl. auch die Antwort des Bayerischen Staatsministeriums des Innern, LT-Drs. 16/10607, S. 2.

334 Die konkrete Frage der Kostenverteilung soll im weiteren Verlauf der Arbeit nicht näher thematisiert werden; laut Angaben der Bundesregierung belaufen sich die Kosten einer Quellen-TKÜ für Bundesbehörden bei einer Dauer der Überwachung von bis zu drei Monaten i. d. R. auf 13.000 bis 15.000 Euro, so die Antwort vom 26.10.2011, BT-PlPr. 17/135 16065 C.

335 http://wiki.piratenpartei.de/wiki/images/5/54/Bayern-skype-tkue.pdf (zuletzt aufgerufen 15.06.2012).

336 Vgl. *Krempl*, http://www.heise.de/newsticker/meldung/Kein-Dementi-aus-Bayern-zum-Trojaner-Einsatz-fuers-VoIP-Abhoeren-183301.html (zuletzt aufgerufen 15.06.2012); für die Echtheit des Schreibens spricht mittlerweile, dass im Zuge der mit der Veröffentlichung einer „Regierungs-Malware“ durch den *Chaos Computer Club* angestoßenen öffentlichen Diskussion über den Einsatz staatlicher Überwachungssoftware von staatlicher Seite das Bestehen geschäftlicher Beziehungen zur Firma DigiTask GmbH in der Vergangenheit nunmehr eingeräumt wurde, vgl. bspw. die Angaben des Bundesministers des Innern, *Friedrich*, in: „‚Es gibt keine rechtliche Grauzone‘“, faz.net vom 15.10.2011, abrufbar unter http://www.faz.net/aktuell/politik/im-interview-bundesinnenminister-friedrich-csu-es-gibt-keine-rechtliche-grauzone-11494291.html (zuletzt aufgerufen 15.06.2012) wie auch die Antwort des Parl. Staatssekretärs beim Bundesminister des Innern, *Schröder*, im Rahmen der 132. Sitzung des Deutschen Bundestages am 19.10.2011 (BT-PlPr. 17/132 15587 B) in Bezug auf Bundesbehörden sowie die Antwort des Bayerischen Staatsministeriums

gemäß der dort aufgeführten Leistungsbeschreibung der Softwarefirma „DigiTask“ das Überwachungsprogramm (hier als „Skype-Capture-Unit“ bezeichnet, also eine Art „Abfang-/Abgreif“-Einheit) die laufende Skype-Kommunikation mitschneiden und die abgegriffenen Daten über einen anonymen[337], zwischengeschalteten Proxy-Server[338] („Recording Proxy“) an den eigentlichen „Recording-Server“ ausleiten, auf dem dann die abgegriffenen und ausgeleiteten Telekommunikationsdaten aufgezeichnet und gespeichert werden.[339] Die Übermittlung der Daten zum Recording-Server erfolge hierbei ebenfalls (behördenseits) AES-verschlüsselt sowie komprimiert.[340] Mittels mobiler Auswertungsstationen könne dann auf die am Recording-Server eingegangenen Daten zugegriffen werden.[341] An diesen Stationen könne die Kommunikation mittels streamingfähigen[342] Multimedia-Players (zum *direkten Mithören*) „live“ wiedergegeben und ggf. bereits ausgewertet werden.[343] Im Übrigen werden die aufgezeichneten Kommunikationsinhalte zur *Auswertung* für den weiteren Verlauf der Ermittlungen entsprechend aufbereitet und gespeichert.

b) Technische Umsetzung mittels individueller Überwachungssoftware

Für das Abgreifen und Ausleiten der Gesprächsinhalte kommt eine spezielle *Überwachungssoftware* zum Abgreifen und Ausleiten der TK-Daten zum Einsatz.

---

des Innern, LT-Drs. 16/10470, S. 2 in Bezug auf Landesbehörden des Freistaates Bayern.

337 Zur Verschleierung des Kommunikationskanals der Überwachungssoftware aus kriminaltaktischen Gründen, vgl. Antwort der Bundesregierung, BT-Drs. 17/7760, S. 15; in dieselbe Richtung die Antwort des Bayerischen Staatsministeriums des Innern, LT-Drs. 16/10470, S. 3.

338 Eine Art „Zwischen-“ bzw. Stellvertreter-Server“, der als Kommunikationsschnittstelle zwischen dem System/Server des Proxy-Benutzers und dem angewählten System geschaltet ist und zu diesem über seine Adresse eine eigene Verbindung herstellt, vgl. *Bär*, TK-Überwachung, Glossar, S. 374; http://de.wikipedia.org/wiki/Proxy_%28Rechnernetz%29 (zuletzt aufgerufen 15.06.2012).

339 Vgl. http://wiki.piratenpartei.de/wiki/images/5/54/Bayern-skype-tkue.pdf (zuletzt aufgerufen 15.06.2012), S. 4; in diese Richtung auch *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11.2010.

340 Vgl. http://wiki.piratenpartei.de/wiki/images/5/54/Bayern-skype-tkue.pdf (zuletzt aufgerufen 15.06.2012), S. 4, 5.

341 Vgl. http://wiki.piratenpartei.de/wiki/images/5/54/Bayern-skype-tkue.pdf (zuletzt aufgerufen 15.06.2012), S. 4, 6.

342 *Streaming,* direkte Wiedergabe bereits während des laufenden Lade-/Übertragungsvorgangs, vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 223.

343 Vgl. http://wiki.piratenpartei.de/wiki/images/5/54/Bayern-skype-tkue.pdf (zuletzt aufgerufen 15.06.2012), S. 4 ff.

Die speziell für staatliche Zugriffe auf informationstechnische Systeme über das Internet entwickelte Software ähnelt rein technisch gesehen Schadprogrammen wie sog. *Trojaner*, *Keyloggern* und sonstiger *Spyware*.

Hinsichtlich der eingesetzten Softwareart besteht auch gewisse Parallelität zur Online-Durchsuchung, für die vom BKA eine spezielle *Remote Forensic Software* entwickelt worden ist. Zur technischen Realisierung der Maßnahmen kommt bei der Online-Durchsuchung wie auch bei der Quellen-TKÜ speziell konfigurierte Überwachungssoftware zur Anwendung. Für das Abgreifen und Ausleiten von Daten wird bei beiden Ermittlungsinstrumente an vergleichbare technische Grundlagen und Vorgehensweisen angeknüpft.[344] Technisch ähnlich wie die *Remote Forensic Software* bei Maßnahmen der Online-Durchsuchung, ermöglicht spezielle Überwachungssoftware bei der Quellen-TKÜ einen heimlichen Zugriff auf laufende Telekommunikation am jeweiligen Endgerät. Auch die Methode zur Einbringung der Software[345] kann bei Online-Durchsuchung und Quellen-TKÜ identisch sein.[346]

Mit der teilweisen Ähnlichkeit in der *technischen* Vorgehensweise erschöpfen sich die Gemeinsamkeiten von Online-Durchsuchung und Quellen-TKÜ allerdings auch schon. Anders gestaltet sich das Verhältnis beider Maßnahmen nämlich hinsichtlich der jeweils fokussierten Überwachungsgegenstände. Die Daten, auf die mit Online-Durchsuchung und Quellen-TKÜ jeweils zugegriffen werden soll, sind völlig unterschiedlicher Natur. Während sich die Online-Durchsuchnung nicht auf Telekommunikationsdaten erstrecken soll, darf die Quellen-TKÜ keine Daten außerhalb laufender Telekommunikationsvorgänge erfassen[347] (z. B. auch keine durch den Nutzer abgespeicherten E-Mail-Adressbücher oder VoIP-Telefonbücher). Beide Ermittlungsinstrumenten müssen auf Grund ihrer unterschiedlichen Eingriffsintensität streng voneinander differenziert werden.[348]

Gemäß den verfassungsrechtlichen Vorgaben[349] muss technisch gewährleistet sein, dass die Quellen-TKÜ ausschließlich Daten aus laufenden Telekommunikationsvorgängen erfasst, damit der alleinige grundrechtliche

---

344 Vgl. Bundesministerium des Innern, Fragenkatalog BMJ, S. 7, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012).

345 Für Einzelheiten zu Einbringungsmethoden, siehe 1. Teil A.II.4.b).

346 *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11. 2010.

347 Vgl. Bundesministerium des Innern, Fragenkatalog BMJ, S. 7, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012); vgl. auch BVerfG NJW 2008, 822 (826).

348 Für Einzelheiten zur Abgrenzung von Online-Durchsuchung und Quellen-TKÜ, siehe 1. Teil A.II.2.a).

349 Vgl. BVerfG NJW 2008, 822 (826).

Maßstab des Art. 10 I GG eröffnet ist. Um diesen Vorgaben gerecht zu werden, ist die Überwachungssoftware laut Behördenangaben[350] bei Quellen-TKÜ-Maßnahmen so konfiguriert, dass *ausschließlich* Daten der aktiven Telekommunikation ausgeleitet werden. Die Software werde nur dann aktiv, wenn der VoIP-Dienst (z. B. Skype) aktiviert wird, vergleichbar mit dem Abnehmen eines Hörers durch den Verdächtigen bei herkömmlicher Festnetztelefonie.[351] Die Konfiguration der Software stelle hierbei sicher, dass auf Datenbestände außerhalb laufender Telekommunikationsvorgänge, insbesondere auf die auf der Festplatte gespeicherten Daten, nicht zugegriffen wird.[352] Ein über den mit der Quellen-TKÜ verfolgten Überwachungszweck hinausgehender, mit der Online-Durchsuchung vergleichbarer Eingriff könne durch entsprechende Konfiguration der Überwachungssoftware von vornherein ausgeschlossen werden.[353]

Anders als in vielen Beiträgen dargestellt, handelt es sich bei dem technischen Einsatz von Überwachungssoftware nicht um eine einzige, universell einsetzbare Software (Stichwort „Der Bundestrojaner" oder „Der Staatstrojaner"), die für jede Überwachungsmaßnahme über das Internet schlechthin zur Anwendung kommt und hierfür „auf Abruf" zur Verfügung steht. Vielmehr wird die Software, staatlichen Angaben zufolge, stets anhand der technischen Parameter des konkreten Zielsystems individuell angefertigt und speziell auf dieses abgestimmt.[354] Bei der Überwachung von Internettelefonie gebe es deshalb keine Software für „die" Quellen-TKÜ.[355] Zwar knüpft die Software bei jeder Maßnahme freilich an stets gleich bleibende technische Grundprinzipien und Konfigurationselemente an. Es gebe aber

---

350 *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11.2010; so auch die Antworten des Bayerischen Staatsministeriums des Innern, LT-Drs. 16/10469, S. 2 sowie LT-Drs. 16/10470, S. 2; so auch schon die Antwort der Bundesregierung, BT-Drs. 16/6885, S. 3 und 4.

351 *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11.2010; in diese Richtung auch die Antwort der Bundesregierung, BT-Drs. 16/6885, S. 3; für Einzelheiten zum dahinter stehenden Prinzip der sog. „Inside-Out-Kommunikation" der Quellen-TKÜ-Software, siehe die Antwort des Bayerischen Staatsministeriums des Innern, LT-Drs. 16/10607, S. 2.

352 *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11. 2010.

353 Vgl. schon BT-Drs. 16/6885, S. 4; krit., ob eine solche Beschränkbarkeit der Software überhaupt technisch möglich ist, hingegen *Hoffmann-Riem*, JZ 2008, 1009 (1022) sowie *Buermeyer*/*Bäcker*, HRRS 2009, 433 (439).

354 *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11.2010; vgl. auch die Antwort des Bayerischen Staatsministeriums des Innern in Einvernehmen mit dem Staatsministerium der Justiz und für Verbraucherschutz, LT-Drs. 16/10607, S. 2.

355 *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11. 2010.

immer nur *eine* Software für *eine* konkrete Maßnahme.[356] Diese werde auf den von der jeweiligen Überwachung konkret betroffenen Einzelfall speziell zugeschnitten und stets auch an die laufenden technischen Entwicklungen und neuesten Sicherheitsstandards von Virenscanner- und Firewall-Softwareprodukten angepasst.[357]

Wenngleich in der öffentlichen Diskussion die grundverschiedenen Ermittlungsmaßnahmen der Online-Durchsuchung und der Quellen-TKÜ unter dem Schlagwort „Der Staatstrojaner" bisweilen vermengt werden – wie dies zuletzt im Zuge der Analyse und Veröffentlichung einer „Regierungs-Malware"[358] durch den *Chaos Computer Club*, welche (wie dies jedenfalls zahlreiche Pressestimmen nahelegten) als „der" Staatstrojaner zu identifizieren sei, im Herbst 2011 festzustellen war – ist hier doch eine exakte Differenzierung und Begriffswahl nötig. Aus technischer Sicht handelt es sich nicht um eine Software mit der „allround" einsetzbar jegliche Eingriffe in informationstechnische Systeme erfolgen können. Vielmehr ist – insbesondere unter Berücksichtigung des obigen Umstandes, dass es für jede konkrete Maßnahme stets eine eigens dafür entwickelte Software gibt – davon auszugehen, dass eine technische Beschränkbarkeit[359] und Konfigurierung der Überwachungssoftware entsprechend der Vorgaben des BVerfG[360] ausschließlich auf Daten aus laufenden Telekommunikationsvorgängen unter Ausschluss einer weitergehenden Durchsuchung des Systems auf sonstige dort gespeicherte Daten technisch durchaus möglich ist.[361] So können die

---

356 *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11. 2010.

357 Vgl. auch Bundesministerium des Innern, Fragenkatalog BMJ, S. 14, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012) zu *Remote Forensic Software*; gilt für die Quellen-TKÜ insoweit entsprechend.

358 Bericht „Analyse einer Regierungs-Malware" vom 08.10.2011, abrufbar unter http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf (zuletzt aufgerufen 15.06.2012).

359 Für Einzelheiten zur rechtlichen Beschränkbarkeit des Software-Einsatzes im richterlichen Beschluss, siehe 3. Teil A.I.1.b) u. 3. Teil A.I.2.

360 BVerfG NJW 2008, 822 (826).

361 Vgl. bspw. die Antwort der Bundesregierung, BT-Drs. 17/7760, S. 5; in dieselbe Richtung auch die Antwort des Bayerischen Staatsministeriums des Innern, LT-Drs. 16/10082, S. 2 u. 3; auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, *Schaar*, widerspricht insoweit kritischen Stimmen, wonach der Einsatz von Überwachungsprogrammen grds. ungeeignet sei, weil diese stets die technische Möglichkeit zum Ausspähen des Systems eröffnen würden, vgl. *Höll,* „Gefährliche Grauzone", Süddeutsche Zeitung vom 13.10.2011, S. 6; nach Einschätzung von *Schaar* sei „es […] durchaus möglich, Programme einzusetzen, die dem Urteil des Bundesverfassungsgerichts von 2008 entsprechen", zitiert nach *Höll*, in: „‚Gefährliche Grauzone'", Süddeutsche Zeitung vom 13.10.2011, S. 6; für Einzel-

Überwachungsprogramme einer Online-Durchsuchung und einer Quellen-TKÜ zwar durchaus auf vergleichbaren Softwarekomponenten aufbauen (z. B. heimliches Sich-Selbst-Installieren der Software nach deren Einbringen in das System; Verifizierung des Zielsystems anhand dessen technischer Parameter; Verborgenbleiben und heimliches Ablaufen der Software im Hintergrund; Ausleitung nur an den festgelegten Behörden-Server; automatisierte und/oder manuelle Löschroutinen nach Beendigung der Maßnahme), jedoch erfolgt die Erstellung der Software für jeden konkreten Fall hinsichtlich des jeweiligen Zielsystems (Betriebssystem und -version, Prozessorarchitektur, verwendeter Browser etc.), hinsichtlich der Art der jeweiligen Maßnahme und vor allem hinsichtlich des konkreten Überwachungsumfangs offenbar nach dem *Baukastenprinzip*. Wenn Stimmen aus IT-Fachkreisen darauf hinweisen, dass für Maßnahmen der Quellen-TKÜ in der Vergangenheit zum Einsatz gekommene Software wohl aus verschiedenen Komponenten zusammengesetzt worden sei bzw. um zusätzliche Funktionen optional erweiterbar sei[362], liegt der (Umkehr-)Schluss nahe, dass damit für eine potentielle künftige („Ideal"-)Überwachungssoftware aber auch die technischen Möglichkeiten gegeben sein dürften, diese in ihrer Funktionsweise von vornherein entsprechend zu beschränken bzw. die Überwachungssoftware um weitere, ggf. von der Anordnung nicht mehr gedeckte Funktionen im weiteren Verfahren entsprechend nicht zu erweitern.[363]

Zum Zuschnitt der Überwachungssoftware speziell auf das von der Maßnahme betroffene Zielsystem werden im Vorfeld der Maßnahme indes genaue Informationen zum jeweiligen Betriebssystem und zur Betriebssystem-

---

heiten zur Erstellung und Konfiguration der Überwachungssoftware, siehe 1. Teil A.II.3.b).

362 So spricht bspw. der Antiviren-Programm-Hersteller Sophos davon, dass Teile der Überwachungssoftware „offenbar eingekauft und dann zusammengestückelt" wurden, *Pfeiffer*, zitiert nach *Reißmann*/*Stöcker*/*Lischka*, in: „Virenprogramme erkennen den Schnüffler", abrufbar unter http://www.spiegel.de/netzwelt/web/0,1518,790931,00.html (zuletzt aufgerufen 15.06.2012); der Sprecher des *Chaos Computer Clubs* berichtet davon, dass „die untersuchten Trojaner […] auch eine Fernsteuerungsfunktion zum Nachladen und Ausführen beliebiger weiterer Schadsoftware [bieten]", *Rieger*, zitiert nach dpa-Artikel „Trojaner für den Lauschangriff", Nürnberger Nachrichten/Fürther Nachrichten vom 10.10.2011, S. 1.

363 Zumal die im Herbst 2011 vom Chaos Computer Club veröffentlichte „Regierungs-Malware" in der dort analysierten Fassung nicht die einzige verfügbare bzw. künftig konfigurierbare Software sein wird; zudem ist es naheliegend, dass entsprechende Programme zur (ausschließlichen) Überwachung von verschlüsselter VoIP-Kommunikation technisch (als ein „Minus" zur Konfiguration von Programmen zur Überwachung des gesamten Systems und seiner Speichermedien) realisierbar sind und mit den heutigen zur Verfügung stehenden Programmierungsmöglichkeiten durch Fachleute (sei es durch beauftragte IT-Firmen, sei es durch Programmierer der Ermittlungsbehörden selbst) entsprechend erstellt werden können.

version, zu Browsertyp und Browserversion, zur installierten Software, zu etwaigen vorhandenen Antiviren- und Firewall-Programmen, zu vorhandenen Internetzugängen sowie bei Maßnahmen der Quellen-TKÜ insbesondere zum jeweils genutzten VoIP-Dienst benötigt.[364] Diese für die genaue Anfertigung und Ausgestaltung der Software relevanten Informationen lassen sich in der Praxis je nach konkretem Einzelfall im Wege der „normale" Telekommunikationsüberwachung wie auch der übrigen strafprozessualen Ermittlungsmaßnahmen im Vorfeld[365] ermitteln.[366]

4. Technische Umsetzung der Sekundärmaßnahmen

a) Sekundärmaßnahmen der Quellen-TKÜ

Als Begleitmaßnahmen (Sekundärmaßnahmen) im Zusammenhang mit einer Quellen-TKÜ sind das *Installieren* der Überwachungssoftware vor Beginn der eigentlichen Überwachung einerseits sowie deren vollständiges *Entfernen* nach Beendigung der Überwachungsmaßnahme andererseits zu unterscheiden und von bloßen Vorfeldermittlungen abzugrenzen:

aa) Abgrenzung zu Vorfeldermittlungen

Eine Maßnahme der Quellen-TKÜ „startet […] nicht von der grünen Wiese weg"[367]. Bevor eine Quellen-TKÜ überhaupt durchgeführt werden kann, muss eine individuell auf den konkreten Fall abgestimmte Vorgehensmethodik entwickelt werden.[368] Hierfür müssen bestimmte Informationen über das System der Zielperson (vgl. oben) sowie deren Kommunikations-

---

364 Vgl. Bundesministerium des Innern, Fragenkatalog BMJ, S. 10, 14, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012) zu *Remote Forensic Software*; vgl. ebenso Bundesministerium des Innern, Fragenkatalog SPD, S. 12, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

365 Für Einzelheiten zu den Vorfeldermittlungen, siehe 1. Teil A.II.4.a)aa).

366 Vgl. Bundesministerium des Innern, Fragenkatalog BMJ, S. 10, 11, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012) zu *Remote Forensic Software*, gilt für die Quellen-TKÜ insoweit entsprechend; vgl. auch die Antwort des Bayerischen Staatsministeriums des Innern im Einvernehmen mit dem Bayerischen Staatsministerium der Justiz und für Verbraucherschutz, LT-Drs. 16/10469, S. 2, 3.

367 *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11.2010.

368 Vgl. Bundesministerium des Innern, Fragenkatalog SPD, S. 17, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt

und Nutzungsverhalten bekannt sein, um eine Überwachungssoftware „maßgeschneidert" aus das jeweilige Zielsystem und die verwendete VoIP-Software entwerfen und gangbare Wege für ein heimliches Einspielen der Software eruieren zu können. Zu diesem Zwecke sind in aller Regel umfangreiche Vorfeldermittlungen erforderlich, welche regelmäßig mit einem hohen organisatorischen Aufwand verbunden sind[369] und noch nicht zur eigentlichen Quellen-TKÜ oder deren Begleitmaßnahmen zählen. In der Praxis fallen hierfür regelmäßige Vorlaufzeiten von nicht selten bis zu zwei Wochen an.[370]

Einer Vorlaufzeit bedarf es meist zunächst zur Durchführung umfassender Ermittlungen in Bezug auf das Zielsystem wie auch des Nutzungsverhalten der Zielperson.[371] Im Rahmen herkömmlicher TKÜ-Maßnahmen nach §§ 100a, 100b StPO wurde im Regelfall bereits der Umstand festgestellt, dass die betreffende Person mittels verschlüsselter VoIP-Dienste kommuniziert[372] und welche VoIP-Soft-ware hierfür verwendet wird. Zweck der weiteren Ermittlungen ist es, die technischen Parameter des Zielsystems zu eruieren.[373] Hierzu zählt stets das jeweilige Betriebssystem und dessen verwendete Version. Daneben sind im Einzelfall ggf. Informationen zur Prozessorarchitektur (32bit; 64bit), zu Browsertyp und -version, zu installierten

---

aufgerufen 15.06.2012) zu *Remote Forensic Software*; gilt für die Quellen-TKÜ insoweit entsprechend.

369 *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11.2010; Generalstaatsanwaltschaft Oldenburg, E-Mail vom 06.08.2010; generell für Online-Zugriffe auch *Sieber*, Stellungnahme zu dem Fragenkatalog des BVerfG in dem Verfahren 1 BvR 370/07, S. 11, abrufbar unter http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf (zuletzt aufgerufen 15.06.2012).

370 *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11.2010.

371 In diese Richtung *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11.2010 und *Dathe*, Präsident des BayLKA, öffentliche Anhörung im Rahmen der 14. Sitzung des Innenausschusses des Hessischen Landtags am 30.09.2009 zum Gesetzesentwurf der Fraktionen der CDU und der FDP für ein Gesetz zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung und anderer Gesetze – Drucks. 18/861 –, stenografischer Bericht, Ausschussvorlage INA/18/14, S. 53 f.

372 Vgl. auch Bericht des Innenausschusses, BT-Drs. 16/10822, S. 6.

373 In diese Richtung *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11.2010 und *Dathe*, Präsident des BayLKA, öffentliche Anhörung im Rahmen der 14. Sitzung des Innenausschusses des Hessischen Landtags am 30.09.2009 zum Gesetzesentwurf der Fraktionen der CDU und der FDP für ein Gesetz zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung und anderer Gesetze – Drucks. 18/861 –, stenografischer Bericht, Ausschussvorlage INA/18/14, S. 53 f.; vgl. auch die Antwort des Bayerischen Staatsministeriums des Innern im Einvernehmen mit dem Bayerischen Staatsministerium der Justiz und für Verbraucherschutz, LT-Drs. 16/10469, S. 2 u. 3.

Softwareprodukten und -versionen (insbesondere verwendete VoIP-Software, etwaige Antivirus- und Firewall-Programme etc.) sowie zum vorhandenen Internetzugang erforderlich.[374] Anhand der Parameter *dieses einen Zielsystems* lasse sich dann die Überwachungssoftware speziell für eine konkrete Quellen-TKÜ-Maßnahme nachbauen.[375] Die so erstellte Software werde, bevor sie zum Einsatz kommt, getestet und – wenn sie den Vorgaben entspricht – letztlich zertifiziert.[376] Zudem sei jede Quellen-TKÜ-Software durch einen sog. *digitalen Fingerabdruck*[377] gekennzeichnet und damit auch individualisiert.[378]

Der Vorlaufzeit bedarf es jedoch nicht nur zur Feststellung der technischen Parameter des Zielsystems. Zur Vorbereitung der Maßnahme ist es außerdem i. d. R. erforderlich, Möglichkeiten und Wege zur Einbringung der Überwachungssoftware zu ermitteln. Hierfür ist mitunter zeitintensive Recherchearbeit zum Onlineverhalten sowie zu sonstigen Lebensgewohnheiten der Zielperson im Vorfeld zu leisten.[379] Das Beschaffen entsprechender Informationen im Vorfeld wird sich hierbei regelmäßig als wenig intensiv (bzw. gar nicht[380]) in die die Rechte des Betroffenen eingreifende Ermitt-

---

374 Vgl. Bundesministerium des Innern, Fragenkatalog BMJ, S. 10, 11, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012); siehe auch 1. Teil A.II.3.b).

375 *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11. 2010, weshalb es „keine Software für ‚die' Quellen-TKÜ" gebe, sondern „eine Software für eine Maßnahme"; für Einzelheiten zur Überwachungssoftware, siehe 1. Teil A.II.3.b).

376 *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11. 2010; gemäß der Antwort des Bayerischen Staatsministeriums des Innern, LT-Drs. 16/10082, S. 8, werde „durch umfangreiche technische, der Einbringung auf das Zielsystem vorgeschaltete Funktionsprüfungen im Rahmen eines Qualitätssicherungsprozesses in jedem Einzelfall geprüft, sichergestellt und protokolliert, dass der Funktionsumfang der Quellen-TKÜ-Software den rechtlichen Vorgaben und insbesondere dem der Maßnahme zu Grunde liegenden richterlichen Beschluss entspricht" (S. 8).

377 Mittels eines sog. *Hashwertes* zur eindeutigen Kennzeichnung im Sinne einer Signatur; mit Hilfe des Hashverfahrens lässt sich bspw. die Authentizität einer Datei überprüfen, vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 105.

378 Vgl. Antwort des Bayerischen Staatsministeriums des Innern, LT-Drs. 16/10607, S. 2.

379 Vgl. Bundesministerium des Innern, Fragenkatalog BMJ, S. 10, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012).

380 Für „Bagatell"-Ermittlungshandlungen (bloße Spurensuche, Erkundigungen, Nutzung allgemein zugängliche Informationen u. ä.) bedürfte es mangels entsprechender Eingriffsqualität der Vorfeldermittlungsmaßnahme mitunter nicht einmal eines Abstellens auf die Ermittlungsgeneralklausel der §§ 161 I S. 1, 163 I StPO (vergleichbar mit dem materiellrechtlichen Bagatellausschlussprinzip *minima non*

lungshandlung auf die allgemeine strafprozessuale Ermittlungsgeneralklausel aus §§ 161 I S. 1, 163 I StPO stützen lassen.[381]

Bei eingriffsintensiveren Vorfeldermittlungen, die sich nicht mehr auf die Ermittlungsgeneralklausel der §§ 161 I S. 1, 163 I StPO stützen lassen, beschränkt sich allerdings die Bandbreite möglicher Vorfeldmaßnahmen nicht nur auf die Durchführung klassischer Telekommunikationsüberwachung (§ 100a StPO) oder die Erhebung von Verkehrsdaten nach (§ 100g StPO).[382] Als Mittel zur Feststellung der erforderlichen Informationen im Vorfeld stehen darüber hinaus natürlich auch die übrigen strafprozessualen Ermittlungsmaßnahmen zur Verfügung. Je nach Ermittlungssituation und Vorliegen der jeweiligen Eingriffsvoraussetzungen im konkreten Einzelfall kann daher zur Erlangung der relevanten Informationen über das Zielsystem sowie über Nutzungsgewohnheiten und Umfeld der Zielperson für die Durchführung hierauf gerichteter Vorfeldmaßnahmen prinzipiell aus dem gesamten von der StPO zur Hand gegebene Ermittlungsinstrumentarium geschöpft werden. Hierfür können bei Vorliegen der Voraussetzungen nicht nur – wenn auch regelmäßig – heimliche Ermittlungsmaßnahmen wie bspw. neben Observationen (§ 100h StPO; § 163f StPO) auch Einsätze von Vertrauenspersonen (kurz *V-Person*[383]) oder verdeckten Ermittlern (§§ 110a ff.

---

curat praetor), vgl. Löwe-Rosenberg – *Schäfer*, StPO und GVG, Zweiter Band, 25. Aufl. 2004, Vor § 94 StPO, Rn. 32 u. 54 f.

381 In diese Richtung auch *Thönnes*, Leiter PG TKÜ-CC (Kompetenzzentrum für TKÜ), Landeskriminalamt Rheinland-Pfalz, schriftliche Befragung vom 26.10.2010; von derartigen Vorfeldermittlungen strikt abzugrenzen ist hingegen die Installation (wie auch Deinstallation) der Überwachungssoftware als Vorbereitungs-/Begleitmaßnahme (Sekundärmaßnahme) zur anschließenden Realisierung der Überwachung der laufenden VoIP-Telekommunikation auf dem betroffenen System (Primärmaßnahme); auf Grund der damit verbundenen grundrechtlichen Eingriffswirkung in Art. 10 I GG (vgl. BVerfG NJW 2008, 822, 826) handelt es sich bei dem heimlichen bzw. verdeckten Einbringen (wie auch Entfernen) der Überwachungssoftware im Rahmen der Vorbereitung (bzw. Nachbereitung) von Quellen-TKÜ-Maßnahmen nicht um eine Maßnahme, welche sich – gerade auch im Vergleich zu den anerkannte Fallgruppen dieser Ermittlungsbefugnis – auf die Ermittlungsgeneralklausel aus §§ 161 I S. 1, 163 I StPO als Rechtsgrundlage stützen lässt, vgl. insoweit zutr. auch *Sankol*, CR 2008, 13 (18); vgl. zu den Voraussetzungen auch Meyer-Goßner – *Cierniak*, StPO, § 161, Rn. 1; zur Frage des Vorliegens der Voraussetzungen einer Annexkompetenz zu § 100a I StPO als Rechtsgrundlage für die Installation und Deinstallation der Software, siehe 2. Teil B.III.

382 Vgl. hierzu auch die Antwort des Bayerischen Staatsministeriums des Innern im Einvernehmen mit dem Bayerischen Staatsministeriums der Justiz und für Verbraucherschutz, LT-Drs. 16/10469, S. 2 u. 3.

383 Gegenwärtig auf Grundlage der *Gemeinsamen Richtlinien der Justizminister/-senatoren und der Innenminister/-senatoren der Länder über die Inanspruchnahme von Informanten sowie über den Einsatz von Vertrauenspersonen (V-Perso-*

StPO) u. a. in Betracht kommen[384], sondern grds. auch offene Ermittlungsmaßnahmen wie bspw. Durchsuchungen (§§ 102 ff. StPO).

Die Auswertung der mit der jeweiligen Vorfeldmaßnahme erlangten Informationen ergibt dann je nach Sachlage und Einzelfall, ob sich auf deren Grundlage eine Quellen-TKÜ realisieren lässt oder nicht.

bb) Installieren der Überwachungssoftware

Für die Durchführung einer Überwachung und Aufzeichnung der über das Zielsystem geführten verschlüsselten Internettelekommunikation ist die vorherige Installation einer entsprechenden Überwachungssoftware erforderlich. Als Maßnahme zur Ermöglichung des primären Überwachens und Aufzeichnens von Telekommunikation „an der Quelle" stellt das vorherige heimliche bzw. verdeckte Einbringen/Installieren der Überwachungssoftware auf betroffenen Zielsystem eine die Primäreingriffe begleitende bzw. vorbereitende Maßnahme (Sekundärmaßnahme) dar.[385]

cc) Entfernen der Überwachungssoftware

Nach Abschluss der Maßnahme ist die Überwachungssoftware von dem Zielsystem wieder zu entfernen.[386] Als „actus contrarius" zum Installieren der Software ist auch das anschließende Entfernen der Überwachungssoftware nach Beendigung der Überwachungsmaßnahme als Begleitmaßnahme der Quellen-TKÜ einzuordnen. Deinstallation der Software bedeutet hierbei grds. das vollständige – jedenfalls soweit nach dem Stand der Technik möglich, da auch von staatlichen Behörden insoweit nichts technisch Unmögliches verlangt werden kann – Entfernen aller installierten Softwarekomponenten und getätigten Konfigurationen vom überwachten Zielsystem, sodass auf diesem – jedenfalls soweit von der Einbringung der Überwachungssoftware tangiert – wieder ein „uninfiltrierter" Zustand wie vor der technischen Infiltration hergestellt ist.[387]

---

nen) und verdeckten Ermittlern im Rahmen der Strafverfolgung, Anlage D zur Richtlinie für das Strafverfahren und das Bußgeldverfahren (RiStBV).

384 Vgl. Bundesministerium des Innern, Fragenkatalog BMJ, S. 10, 11, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012).

385 Für Einzelheiten zu Vorgehensweisen des Einbringens der Software, siehe 1. Teil A.II.4.b); zur Frage, ob die Sekundärmaßnahme in rechtlicher Hinsicht auf eine Annexkompetenz zu § 100a StPO gestützt werden kann, siehe 2. Teil B.III.

386 Ein Belassen der Software auf dem System käme nur in Ausnahmefällen in Frage, bspw. wenn weitere Quellen-TKÜ-Maßnahme bereits angeordnet sind.

b) Vorgehensweisen zum Installieren

In der Praxis haben sich eine Vielzahl von Vorgehensweisen entwickelt, wie die Überwachungssoftware unbemerkt in das Zielsystem eingebracht und dort installiert werden kann. Die Auswahl hängt sowohl von den jeweiligen technischen Gegebenheiten wie auch vom individuellen Nutzungsverhalten und den Gewohnheiten der Zielperson im konkreten Einzelfall ab.[388] Eine gewisse kriminalistische Kreativität der durchführenden Behörde ist bei der großen Bandbreite an Einzelkonstellationen unerlässlich. Allen Vorgehensweisen gleich ist die Heimlichkeit bzw. Verdecktheit[389] der Durchführung. Je nach Fallgestaltung ist hierbei auch eine (unbewusste) „Mitwirkungshandlung" der Zielperson erforderlich.

Nachfolgend sollen die in der Praxis in Frage kommenden Vorgehensweisen zum Einbringen der Überwachungssoftware überblicksartig dargestellt werden. Auf Grund der Vielschichtigkeit der Einbringungsmöglichkeiten je nach den besonderen Umständen des Einzelfalls sind jedoch generelle Aussagen zu möglichen Einbringungsweisen nur bis zu einem gewissen Maße möglich.[390] Die vorliegende Arbeit bildet deshalb einen Auszug der behördlichen Handhabe anhand der in der Praxis bislang geläufigen Vorgehensweisen ab, ohne damit andere, hier nicht genannte (ggf. auch erst künftig entwickelte) konkrete Einbringungsweisen ausschließen zu wollen.[391]

---

387 Für Einzelheiten zu Vorgehensweisen des Entfernens der Software, siehe 1. Teil A.II.4.c); zur Frage, ob die Sekundärmaßnahme in rechtlicher Hinsicht auf eine Annexkompetenz zu § 100a StPO gestützt werden kann, siehe 2. Teil B.III.

388 Vgl. Bundesministerium des Innern, Fragenkatalog SPD, S. 18, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012); vgl. auch Antwort des Bayerischen Staatsministeriums des Innern, LT-Drs. 16/10469, S. 2.

389 Der Begriff „verdeckt" wird oftmals synonym mit dem Begriff „heimlich" verwendet (i. S. v. „ohne Wissen des Betroffenen"); dies entspricht auch der üblichen Terminologie in Rspr. und Schrifttum; bei strenger Begriffsauslegung beschreibt der Begriff der „Verdecktheit" indes eher den Umstand, dass der Betroffene zwar die (sichtbaren) Handlungen/Auswirkungen der Maßnahmeumsetzung mitbekommt, den dahinter stehenden tatsächlichen (ermittlungstaktischen) Anlass/Zweck aber nicht erkennt (bspw. durch das Handeln der Ermittlungspersonen unter einem bestimmten Vorwand und/oder Anwendung einer Legende), während der Begriff der „Heimlichkeit" hingegen eher auf eine völlige Unkenntnis des Betroffenen vom Ablaufen einer Maßnahme ihm gegenüber überhaupt hindeutet.

390 Vgl. auch Bundesministerium des Innern, Fragenkatalog SPD, S. 18, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

391 Vgl. für zusätzliche Details auch die anschaulichen Ausführungen bei *Hansen*/*Pfitzmann*, DRiZ 2007, 225 (227).

Die verschiedenen Vorgehensweisen zur heimlichen Einbringung der Software lassen sich hierfür zunächst nach Art und Weise des Zugriffs – entweder über das Leitungsnetz oder durch direkten physischen Zugriff – aufgliedern:

aa) Online/aus der Ferne

Gangbare Vorgehensweise in der Praxis ist das verdeckte Einbringen der Software online, also über das Leitungsnetz, von außen („Remote-Installation“[392]), ohne direkten physischen Zugriff auf das Gerät.[393] Mit einer verdeckten Vorgehensweise schon begrifflich verbunden ist eine gewisse „Täuschung“ des Nutzers, um diesen zu einer (unbewussten) Mitwirkungshandlung zu veranlassen:

In der Praxis ließe sich dies bspw. im Wege einer *zugesandten E-Mail* realisieren.[394] Den Ablauf kann man sich hierbei so vorstellen, dass eine „präparierte“ E-Mail durch die Überwachungsbehörde an den Betroffenen versendet wird, welche die Überwachungssoftware (versteckt) enthält.[395] Hierfür kann die Überwachungssoftware theoretisch auch als verdeckter Bestandteil in eine sonstige (unverdächtige) Datei integriert werden, die der E-Mail als Anhang beigefügt wird. Nach Herunterladen und Öffnen der E-Mail durch die Zielperson installiert sich die Überwachungssoftware im Hintergrund ohne weitere Zwischenschritte und ohne Kenntnis des Betroffenen auf dem Zielsystem selbständig.[396] Dies setzt ein gewisses (unbewusstes) Mitwirken des Empfängers voraus. Damit sich die Software installieren kann, ist in aller Regel erforderlich, dass der Betroffene den Dateianhang der E-Mail manuell öffnet, was eine gewisse Arglosigkeit voraussetzt.[397]

---

392 Antwort des Bayerischen Staatsministeriums des Innern, LT-Drs. 16/10469, S. 2.

393 So auch *Bär*, persönliches Gespräch mit dem Verfasser, Bamberg, 09.12.2010.

394 Vgl. auch das Bundesministerium des Innern zu *Remote Forensic Software*, Fragenkatalog SPD, S. 19, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012), wonach „die Einbringung der RFS im Wege der E-Mail-Kommunikation […] je nach Einzelfall ein geeignetes Mittel darstellen [kann]“ (S. 19).

395 *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11. 2010.

396 Vgl. in diese Richtung auch Bundesministerium des Innern, Fragenkatalog SPD, S. 19, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-online durchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

397 Vgl. *Platz*, sic! 11/2008, 838, S. 4, abrufbar unter https://www.sic-online.ch/fileadmin/user_upload/Sic-Online/2008/documents/838.pdf (zuletzt aufgerufen 15.06.2012).

Damit der Betroffene von der beigefügten Software nichts mitbekommt und deren Installation durch sein eigenes Handeln (Abholen und Öffnen der E-Mail) unbewusst veranlasst, wird die E-Mail i. d. R. unter einer bestimmten Legende, bspw. unter einem fremden Namen und unter einem bestimmten Vorwand, verschickt, um dem Empfänger besondere Vertrauenswürdigkeit vorzutäuschen[398] oder bei diesem ein entsprechendes Interesse für ein Abholen und Öffnen der E-Mail zu wecken[399].

Die präparierte E-Mail könnte hierbei auch als offizielles Schreiben unter dem Namen einer anderen Behörde[400] und unter dem Vorwand normalen behördlichen Schriftverkehrs z. B. im Rahmen des sog. *E-Government*[401] versendet werden, was sich jedoch zum Schutz der Akzeptanz und des Vertrauens in elektronische Schreiben und Angebote staatlicher Stellen auf begründete Ausnahmefälle in Absprache mit der betroffenen Behörde beschränken sollte.[402]

Daneben befinden sich aber auch eine Reihe weiterer Möglichkeiten im Gespräch, die – zumindest prinzipiell – geeignet wären, eine Überwachungssoftware heimlich einzuschleusen. Die Zurückhaltung staatlicher Stellen bei der Preisgabe von Einzelheiten zu Methoden der Einbringung lässt indes Raum für Spekulationen. In Erwägung ziehen ließe sich bspw. auch das Einrichten einer (manipulierten) *fingierten Internetseite*, die bei Downloads durch die Zielperson heimlich auch die Überwachungssoftware mit überträgt, oder bereits beim bloßen Aufrufen der Seite heimlich die Software auf das System überträgt (sog. *Drive-By-Downloads*).[403]

---

398 Vgl. Arbeitskreis „Technische und organisatorische Datenschutzfragen", Technische Aspekte, S. 6, abrufbar unter http://www.lfd.m-v.de/dschutz/informat/internet/onlinedurchsuchung.pdf (zuletzt aufgerufen. 15.06.2012).

399 Vgl. im Einzelnen auch *Hansen*/*Pfitzmann*, DRiZ 2007, 225 (227), die in diesem Zusammenhang von „verheißungsvollen" Dateien bzw. Begleittexten sprechen.

400 Vgl. Bundesministerium des Innern, Fragenkatalog BMJ, S. 14, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012), für begründete Ausnahmefälle.

401 Vereinfachung und Durchführung von Informations-, Kommunikations- und Transaktionsprozessen zwischen staatlichen Stellen und Bürgern bzw. Unternehmen unter Verwendung von Informations- und Kommunikationstechnologien, vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 78.

402 Vgl. Bayerischer Landesbeauftragter für den Datenschutz, Presseerklärung vom 30.08.2007, http://www.datenschutz-bayern.de/presse/20070830_eGovernment.html (zuletzt aufgerufen 15.06.2012); Bundesministerium des Innern, Fragenkatalog BMJ, S. 14, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012); ausführlich auch Arbeitskreis „Technische und organisatorische Datenschutzfragen", Technische Aspekte, S. 11, 12, abrufbar unter http://www.lfd.m-v.de/dschutz/informat/internet/onlinedurchsuchung.pdf (zuletzt aufgerufen 15.06.2012).

Eine in der Praxis erfolgversprechende Vorgehensweise ist auch der Einsatz von *manipulierten Datenträgern* wie CDs, DVDs, USB-Sticks etc., die dem Betroffenen unter einer bestimmten Legende zugespielt werden, z. B. als Werbegeschenk im Rahmen einer fingierten Verteilaktion[404] oder als Fund bei einem gezielten „Verlieren“[405]. Für den Betroffenen nicht ohne weiteres erkennbar, können diese externen Datenträger dann entweder ein Programm enthalten, welches beim erstmaligen Anschließen des präparierten Speichermediums heimlich eine „Hintertür“ in das Zielsystem öffnet um die Software von außen einspielen zu können[406], oder aber gleich die Überwachungssoftware selbst enthalten, welche sich beim Anschließen unbemerkt im Hintergrund auf das Zielsystem (mit-)installiert[407].

Daneben gibt es aber auch Möglichkeiten zur heimlichen Installation, die ohne ein Ausnutzen von Arglosigkeit beim Nutzer insofern auskommen, als hier eine „Mitwirkungshandlung“ des Nutzers nicht erforderlich ist:

Eine solche Vorgehensweise stellt vor allem das Ausnutzen von (im Zeitpunkt des Eingriffs) *bestehenden Sicherheitslücken oder Fehlfunktionen* in Betriebssystemen und/oder Anwendungsprogrammen mit Hilfe virtueller Werkzeuge (sog. *Exploits*[408]) dar, welche derartige Lücken als Einfallstor in das System für ein heimliches Einbringen der Überwachungssoftware benutzen.[409]

---

403 Vgl. Arbeitskreis „Technische und organisatorische Datenschutzfragen“, Technische Aspekte, S. 6, abrufbar unter http://www.lfd.m-v.de/dschutz/informat/internet/onlinedurchsuchung.pdf (zuletzt aufgerufen 15.06.2012).

404 *Bär*, persönliches Gespräch mit dem Verfasser, Bamberg, 09.12.2010.

405 Vgl. Schilderungen zu entsprechenden Feldversuchen einer Sicherheitsfirma bei *Sieber*, Stellungnahme zu dem Fragenkatalog des BVerfG in dem Verfahren 1 BvR 370/07, S. 12, abrufbar unter http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf (zuletzt aufgerufen 15.06.2012).

406 Vgl. *Sieber*, Stellungnahme zu dem Fragenkatalog des BVerfG in dem Verfahren 1 BvR 370/07, S. 12, abrufbar unter http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf (zuletzt aufgerufen 15.06.2012).

407 *Bär*, persönliches Gespräch mit dem Verfasser, Bamberg, 09.12.2010.

408 Programme bzw. Befehlsfolgen, welche eine Sicherheitslücke oder Schwachstelle (z. B. eine bestimmte Fehlfunktion) eines Betriebssystems oder einer Software ausnutzen können, um diese gezielt anzugreifen, vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 87; diesbezüglich zu unterscheiden: *„normale“ Exploits*, die eine schon länger bekannte Lücke/Schwachstelle ausnutzen, sog. *Zero-Day-Exploits*, welche noch am Tag des allgemeinen Bekanntwerdens der Lücke erscheinen und bei denen Schutzmaßnahmen zu dem Zeitpunkt i.d.R noch nicht verfügbar sind, sowie *Less-Than-Zero-Day-Exploits*, welche bereits vor dem allgemeinen Bekanntwerden der Lücke angeboten werden und bei denen wohl praktisch keine Schutzmöglichkeit besteht, vgl. Arbeitskreis „Technische und organisatorische Datenschutzfragen“, Technische Aspekte, S. 6 f., abrufbar unter http://www.lfd.m-v.de/dschutz/informat/internet/onlinedurchsuchung.pdf (zuletzt aufgerufen 15.06.2012).

Des Weiteren stellt auch das Benutzen *herstellerseits eingebauter Hintertüren* (*sog. Backdoors*[410]) in das jeweilige System eine derartige Möglichkeit zur heimlichen Softwareinstallation von außen dar.

bb) Direkter Zugriff

Das heimliche Aufspielen der Überwachungssoftware kann aber auch manuell, durch direktes physisches Einwirken der Ermittlungspersonen am Zielgerät erfolgen. Eine (unbewusste) unmittelbare Mitwirkungshandlung der Zielperson ist zur Durchführung der Installation hier nicht erforderlich. Aber auch das Vorgehen über einen direkten physischen Zugriff ist regelmäßig mit einer gewissen „Täuschungshandlung" gegenüber dem Nutzer verbunden.

Im Rahmen des direkten Aufspielens „per Hand" durch Ermittlungspersonen lassen sich wiederum zwei Vorgehensweisen unterscheiden:

In der Praxis Anwendung findende Vorgehensweise ist hierbei einerseits das *kurzzeitige Verschaffen direkten physischen Zugriffs* auf das Zielgerät durch Ermittlungspersonen – sei es gelegentlich einer in den Räumlichkeiten, in denen sich das Gerät befindet, durchgeführten Ermittlungsmaßnahme (z. B. eine angeordnete offene Durchsuchungsmaßnahme gemäß §§ 102 ff. StPO)[411], sei es außerhalb geschützter Räumlichkeiten bei entsprechender Gelegenheit zum unbemerkten physischen Zugriff, auch unter einem be-

---

409 Vgl. Arbeitskreis „Technische und organisatorische Datenschutzfragen", Technische Aspekte, S. 6 f., abrufbar unter http://www.lfd.m-v.de/dschutz/informat/internet/onlinedurchsuchung.pdf (zuletzt aufgerufen 15.06.2012).

410 Eine „Hintertür" (engl. „Backdoor") im computertechnischen Sinne stellt einen (oftmals bewusst durch den Programmierer „von Haus aus" eingebauten) Bestandteil einer Software (bspw. eines Betriebssystems oder eines Anwendungsprogramms) dar, der die Möglichkeit eröffnet, unter Umgehung der normalen Zugriffssicherungen alternativ „über die Hintertür" Zugang in ein System oder in eine an sich geschützte Funktion eines Programms zu erhalten, vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 24; ob eine solche Backdoor in die Skype-Software besteht, ist indes unklar, mit Blick auf die Antwort des Parl. Staatssekretärs beim Bundesminister des Innern, *Bergner*, für die Bundesregierung im Rahmen der 135. Sitzung des Deutschen Bundestags am 26.10.2011 (BT-PlPr. 17/135 16064 D), wonach es in den Fällen P2P-geführter VoIP zwischen zwei internetfähigen Endgeräten (softwarebasierte P2P-VoIP) „Skype […] nach derzeitigem Kenntnisstand der Bundesregierung schon aus technischen Gründen nicht möglich [ist], Inhaltsdaten den Justiz-, Strafvollzugs- oder Regierungsbehörden zur Verfügung zu stellen" (16064 D), jedoch mehr als fraglich; siehe hierzu auch 2. Teil B.III.2.b)bb).

411 Vgl. bspw. dpa-Artikel „Hintergrund: So arbeitet eine Trojaner-Software", http://www.focus.de/finanzen/news/computer-hintergrund-so-arbeitet-eine-trojaner-software_aid_673226.html (zuletzt aufgerufen 15.06.2012) sowie BayLT-Drs. 16/8881, S. 7; siehe hierzu auch 2. Teil B.I.2.b)bb).

stimmten Vorwand bzw. Ausnutzen einer bestimmten Situation, um die Zielperson nicht misstrauisch werden zu lassen. Je nach den konkreten Umständen des Einzelfalls könnte dies bspw. dann stattfinden, während sich das Gerät bei einer Reparatur befindet[412], aber auch anlässlich einer Zollkontrolle am Flughafen[413] denkbar unter dem Vorwand erfolgen, das Gerät (z. B. Notebook/Laptop, Smartphone) kurzfristig an sich nehmen zu müssen, bspw. um dessen Eigenschaft als Neu- oder Gebrauchtgerät bzw. dessen Wert festzustellen. Derartige Vorgehensweisen zum Erreichen eines direkten physischen Zugriff auf das Gerät erfordern mithin eine gewisse kriminalistische bzw. kriminaltaktische Kreativität. All diesen Vorgehensweisen ist indes gemein, dass sie regelmäßig intensive Ermittlungsarbeit im Vorfeld[414] (bspw. in Bezug auf Vorlieben, Gewohnheiten, soziales Umfeld etc.) erfordern[415], um die sich für einen direkten Zugriff herauskristallisierenden Gelegenheiten rechtzeitig zu erkennen. Eine direkte (aktive) Mitwirkung der Zielperson beim manuellen Aufspielen ist nicht erforderlich. Allein die Bereitschaft des Zielperson zur kurzzeitigen Herausgabe des Gerätes ist notwendig. So ist sich bspw. der Betroffenen bei der oben geschilderten Konstellation des heimlichen Einschleusen der Software gelegentlich einer Zollkontrolle zwar darüber bewusst, dass sich das Gerät (bspw. das Notebook) vorübergehend in staatlicher Hand befindet, weiß jedoch nicht, dass die Begründung für das kurzzeitige Verbringen des Geräts aus seiner Blickweite (bspw. zur Kontrolle der Seriennummer oder zur Feststellung des Wertes) ggf. nur vorgeschoben ist[416], um heimlich eine Überwachungssoftware aufspielen zu können.

Eine andere Methode wäre das *Verschaffen direkten physischen Zugriffs durch heimliches Eindringen* in die vom Maßnahmeadressaten (i. S. d. § 100a III StPO) benutzten Räume, insbesondere in dessen Wohn- oder Betriebs-/Geschäftsräume[417], je nachdem, wo sich das Zielgerät befindet,

---

412 *Bär*, persönliches Gespräch mit dem Verfasser, Bamberg, 09.12.2010.

413 *Bär*, persönliches Gespräch mit dem Verfasser, Bamberg, 09.12.2010; eine solche Vorgehensweise lag einer im Jahr 2009 in einem Ermittlungsverfahren der StA Landshut durchgeführten Quellen-TKÜ-Maßnahme zugrunde, deren Anordnung durch das AG Landshut und Umsetzung Gegenstand der Entscheidung des LG Landshut vom 20.01.2011 (MMR 2011, 690) im Rahmen eines Beschwerdeverfahrens nach § 101 VII S. 3 StPO war; hierzu auch BT-PlPr. 17/132 15597 A.

414 Siehe 1. Teil A.II.4.a)aa).

415 So auch *Bär*, persönliches Gespräch mit dem Verfasser, Bamberg, 09.12.2010, zudem unter Hinweis auf den deutlichen finanziellen Aufwand von Quellen-TKÜ-Maßnahmen.

416 Zur Frage, wie ein verdecktes Handeln unter Vorwand (verfassungs-)rechtlich zu bewerten ist, siehe 2. Teil B.I.2.a) und b).

417 Zur Frage der Zulässigkeit eines (heimlichen) Betretens unter (verfassungs-) rechtlichen Gesichtspunkten, siehe 2. Teil B.I.2.b).

ähnlich der akustischen Wohnraumüberwachung nach §§ 100c ff. StPO. Vor allem bei der (in der Praxis aber wohl eher seltenen) Möglichkeit zu mehrfachen Zugriffen auf das Zielsystem in den betreffenden Räumlichkeiten, wäre es hierbei auch denkbar, bspw. zunächst die Systemparameter in Erfahrung bringen, um dann über die verfügbaren Systeminformationen eine auf das jeweilige Zielsystem individuell zugeschnittene Überwachungssoftware zu entwerfen und diese bei einem erneuten Betreten der Räume am Zielsystem einzuspielen. Zudem eröffnet der direkte physische Zugriff auf das Gerät auch die unmittelbare Möglichkeit sicherzugehen, dass das richtige Zielgerät mit der Überwachungssoftware infiltriert wird.[418]

Diese Vorgehensweise zum Erlangen des direkten physischen Zugriffs auf das Zielgerät ist jedoch dann kritisch zu sehen, soweit es hierbei zu einem heimlichen Betreten von Wohnräumen und sonstigen durch Art. 13 I GG geschützten Räumlichkeiten (auch der allgemeinen Zugänglichkeit entzogene Betriebs-/Geschäftsräume)[419] des Maßnahmeadressaten kommt, weil für das heimliche Sich-Zugang-Verschaffen zum Gerät dann – wie bei Maßnahmen nach §§ 100c ff. StPO – zur Rechtfertigung des Eingriffs in Art. 13 I GG zusätzlich ein Betretungsrecht erforderlich wäre, was gegenwärtig für Maßnahmen der Telekommunikationsüberwachung aber weder eine verfassungsrechtliche Grundlage in Art. 13 GG findet noch aus der (einfachgesetzlichen) Rechtsgrundlage der §§ 100a, 100b StPO hervorgeht.[420]

In der Praxis kommt es damit entscheidend darauf an, wo sich das Zielgerät befindet und ob es ggf. frei zugänglich ist.[421] Denn anders als in Wohnräumen oder sonstigen nach Art. 13 I GG geschützten Räumlichkeiten des Maßnahmeadressaten kann einem *direkten Zugriff* durch Ermittlungspersonen auf Zielgeräte *in öffentlich zugänglichen Räumen* oder *in Räumen Dritter* mit deren Einverständnis, aber auch in Wohnräumen und sonstigen geschützten *Räumlichkeiten des Maßnahmeadressaten mit dessen* (wenn auch ggf. unter einem Vorwand erwirkten[422]) *Einverständnis* nicht entgegen-

---

418 In diese Richtung bezüglich Maßnahmen der Online-Durchsuchung auch *Sieber*, Stellungnahme zu dem Fragenkatalog des BVerfG in dem Verfahren 1 BvR 370/07, S. 12 f., abrufbar unter http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf (zuletzt aufgerufen 15.06.2012).

419 Für Einzelheiten zum Schutzbereich des Art. 13 I GG, siehe 1. Teil B.II.1.

420 Für Einzelheiten zur dogmatischen Auseinandersetzung mit der Frage des Betretungsrechts, siehe 2. Teil B.I.2.b).

421 *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11. 2010.

422 Da der Schutzbereich des Art. 13 I GG nach überzeugender Auffassung nicht das Vertrauen des Grundrechtsträgers in die Redlichkeit von Personen, die er freiwillig in seine Wohnung eintreten lässt, erfasst, vgl. insoweit BeckOK – *Fink*, GG, Ed. 13, Art. 13, Rn. 11 m. w. N.

gehalten werden, dass ein Recht zum heimlichen Betreten der Räume nicht bestünde. Ein direkter physischer Zugriff auf das Zielgerät zum Zwecke des Einspielens der für eine Quellen-TKÜ-Maßnahme notwendigen Überwachungssoftware kann in diesen Fällen – jedenfalls unter Art. 13 I GG-Gesichtspunkten[423] – ohne weiteres in zulässiger Weise erfolgen.[424]

c) Vorgehensweisen zum Entfernen

In technischer Hinsicht gibt es grds. drei Möglichkeiten, nach Abschluss der Ermittlungsmaßnahme die zuvor installierte Überwachungssoftware vom Zielsystem – ggf. heimlich bzw. verdeckt[425] – wieder zu entfernen, nämlich über das Leitungsnetz von außen[426], durch direkten physischen Zugriff am Gerät oder auch durch automatisierte Löschung[427]:

aa) Online/aus der Ferne

Soll Überwachungssoftware nach Beendigung einer Maßnahme wieder entfernt werden, so kann diese einerseits manuell angewiesen werden, sich selbst zu deinstallieren.[428] Eine der Möglichkeiten zur manuellen Entfernung installierter Software vom Zielsystem ist hierbei der Zugriff über das Leitungsnetz („Online“) von außen. Eine Überwachungssoftware lässt sich so konfigurieren, dass die Initialisierung der Deinstallation aus der Ferne über den normalen Datenstrom („remote“) bei bestehender Internetverbindung jederzeit möglich ist.[429]

---

423 Für Einzelheiten zum Grundrecht auf Unverletzlichkeit der Wohnung aus Art. 13 I GG, siehe 1. Teil B.II.

424 Für Einzelheiten zur dogmatischen Begründung, siehe 2. Teil B.I.2.b).

425 Für (verfassungs-)rechtliche Fragen, die sich hieraus ergeben, siehe 2. Teil B.II.

426 Vgl. http://wiki.piratenpartei.de/wiki/images/5/54/Bayern-skype-tkue.pdf (zuletzt aufgerufen 15.06.2012), S. 5; siehe zu dieser Quelle auch 1. Teil A.II.3.a).

427 Vgl. http://wiki.piratenpartei.de/wiki/images/5/54/Bayern-skype-tkue.pdf (zuletzt aufgerufen 15.06.2012), S. 5; siehe zu dieser Quelle auch 1. Teil A.II.3.a).

428 Vgl. Bundesministerium des Innern, Fragenkatalog SPD, S. 13, 17, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

429 Vgl. http://wiki.piratenpartei.de/wiki/images/5/54/Bayern-skype-tkue.pdf (zuletzt aufgerufen 15.06.2012), S. 5; siehe zu dieser Quelle auch 1. Teil A.II.3.a); vgl. zudem auch die Antwort des Bayerischen Staatsministeriums des Innern, LT-Drs. 16/10469, S. 2.

bb) Direkter Zugriff

Die zweite Möglichkeit zur manuellen Entfernung der Überwachungssoftware vom Zielsystem ist – wie bereits beim Aufspielen – der direkte physische Zugriff auf das System am Endgerät. Auch hierfür sind für die praktische Umsetzung im konkreten Fall wieder verschiedene Vorgehensweisen denkbar, die – soweit das Ablaufen einer Maßnahme zum Schutz des Untersuchungszwecks dem Betroffenen noch nicht zur Kenntnis gelangen soll (vgl. auch Zurückstellungsmöglichkeit nach § 101 V S. 1 StPO) und daher das Entfernen heimlich bzw. verdeckt stattfinden muss – der Ermittlungsbehörde im Einzelfall wiederum eine gewisse Kreativität abverlangen kann (bspw. heimlicher/verdeckter Zugriff im Rahmen einer Kontrollsituation u. ä.).

cc) Automatische Löschung

Ist eine Überwachungsmaßnahme zeitlich begrenzt – wie dies bei Maßnahmen nach §§ 100a, 100b StPO gemäß § 100b II S. 2 Nr. 3, § 100b I S. 4 StPO in der Anordnung vorzunehmen ist – so lässt sich die rechtzeitige Entfernung der Überwachungssoftware nach Ablauf des Überwachungszeitraums auch durch automatische Löschung erreichen. Eine entsprechende Konfiguration der Software mit Zeitlimit ist technisch durchführbar.[430] Staatlichen Angaben zufolge kämen für eine automatische Entfernungsroutine[431] als Zeitgeber neben der Systemzeit weitere Module wie bspw. einprogrammierte Verfallsdaten und Zeitzählmechanismen für die Zeitberechnung parallel zum Einsatz.[432] Die Software deinstalliert sich dann automatisch bei Erreichen des „Ablaufdatums“ von selbst.

Aber auch in anderen Fällen kann eine automatische Löschung zum Einsatz kommen. Sollte bspw. ein Kommunikations-Port während einer laufenden Überwachungsmaßnahme geschlossen werden (z. B. auf Grund einer „anschlagenden“ Firewall oder eines Abbruchs der Internetverbindung) und eine Kontaktaufnahme mit dem Steuerungssystem nicht (mehr) möglich

---

430 Vgl. http://wiki.piratenpartei.de/wiki/images/5/54/Bayern-skype-tkue.pdf (zuletzt aufgerufen 15.06.2012), S. 5; siehe zu dieser Quelle auch 1. Teil A.II.3.a); vgl. zudem die Antwort des Bayerischen Staatsministeriums des Innern, LT-Drs. 16/10469, S. 2.

431 Unter einer *Routine* wird im Bereich der Softwareprogrammierung eine bestimmte Programm(teil)funktion verstanden, vgl. http://www.duden.de/rechtschreibung/Routine (zuletzt aufgerufen 15.06.2012).

432 Vgl. Bundesministerium des Innern, Fragenkatalog SPD, S. 13, 16, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

sein, so könne eine Überwachungssoftware auch so konfiguriert werden, dass sich diese in einem solchen Falle durch einen einprogrammierte Selbstdeinstallationsroutine selbständig und rückstandsfrei vom Zielsystem entfernt.[433]

B. Verfassungsrechtliche Grundlagen

Mit dem öffentlichen Interesse an wirksamer Verbrechensbekämpfung, effektiver Strafverfolgung und möglichst vollständiger Wahrheitsermittlung (bei repressiven Eingriffsbefugnissen) bzw. wirksamer Gefahrenabwehr (bei präventiven Eingriffsbefugnissen) im Dauerkonflikt steht das Bedürfnis nach effektivem grundrechtlichen Schutz für die von staatlichen Maßnahmen betroffenen Grundrechtsträger.[434]

Die im Zusammenhang mit einer staatlichen Maßnahme zur Überwachung und Aufzeichnung von Telekommunikation unter Anknüpfung an einem informationstechnischen System mittels einer Überwachungssoftware näher in Betracht kommenden Grundrechte sind das *Fernmeldegeheimnis* aus Art. 10 I GG, die *Unverletzlichkeit der Wohnung* aus Art. 13 I GG sowie das aus dem allgemeinen Persönlichkeitsrecht abgeleiteten *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* nach Art. 2 I i.V.m Art. 1 I GG:

I. Fernmeldegeheimnis, Art. 10 I GG

1. Schutzbereich

In persönlicher Hinsicht handelt es sich bei dem neben dem Brief- und Postgeheimnis in Art. 10 I GG gewährleisteten *Fernmeldegeheimnis*[435] um ein sog. *Jedermann-Grundrecht*, d.h. es macht hinsichtlich des persönlichen Schutzbereichs keine Einschränkungen, bspw. durch Anknüpfen an die deutsche Staatsangehörigkeit wie dies bei den sog. *Deutschen-Grundrechten* (z.B. die Versammlungsfreiheit in Art. 8 I GG) der Fall ist. Zudem

---

433 Vgl. Bundesministerium des Innern, Fragenkatalog SPD, S. 12, 21, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

434 Vgl. BVerfG NJW 2000, 55 (65); bereits BVerfG NJW 1966, 243 (243 f.); BVerfG NJW 1988, 329 (330) m.w.N.; BVerfG NJW 1990, 563 (564).

435 Soweit im Nachfolgenden aus Vereinfachungsgründen nur von „Art. 10 I GG" die Rede ist, wird hiermit nur auf das Fernmeldegeheimnis Bezug genommen, es sei denn, die Ausführungen beziehen sich nach dem Gesamtzusammenhang oder ausdrücklich (auch) auf das Brief- oder Postgeheimnis.

können sich neben natürlichen Personen nach Maßgabe des Art. 19 III GG auch juristische Personen des Privatrechts auf den Schutz des Art. 10 I GG berufen.[436]

In sachlicher Hinsicht schützt das Grundrecht des Fernmeldegeheimnisses (nach neuerer Terminologie auch *Telekommunikationsgeheimnis*) „die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs“[437]. Es dient der freien Persönlichkeitsentfaltung durch Gewährleistung eines von der öffentlichen Gewalt grds. nicht einsehbaren („freien“) Kommunikationsaustauschs mit Mitteln des Fernmelde-/Telekommunikationsverkehrs.[438] Denn Schutzgut des Art. 10 I GG ist die Privatsphäre des Einzelnen, welche in Form der „Vertraulichkeit der individuellen Kommunikation gegenüber staatlicher Kenntnisnahme“[439] geschützt wird.[440] Das Fernmeldegeheimnisses nach Art. 10 I GG schützt hingegen nicht die Vertraulichkeit und Integrität von informationstechnischen Systemen.[441]

Vom sachlichen Schutzbereich des Fernmeldegeheimnisses erfasst ist zunächst der Inhalt der Kommunikation (*Inhaltsdaten)*.[442] Die öffentliche Gewalt soll diesbezüglich „grundsätzlich nicht die Möglichkeit haben, sich Kenntnis vom Inhalt des über Fernmeldeanlagen abgewickelten mündlichen oder schriftlichen Informations- und Gedankenaustauschs zu verschaffen“[443]. Hierbei ist unerheblich, um was für Inhalte es sich handelt und ob diese privater, geschäftlicher politischer oder sonstiger Natur sind.[444] Der Schutz des Art. 10 I GG ist hierbei nicht nur auf die früher durch die Deutsche Bundespost angebotenen („klassischen“) Fernmeldedienste wie Telefon und Telefax beschränkt, sondern erfasst sämtlichen Austausch von Informationen, der mit Hilfe verfügbarer Telekommunikationstechniken abgewickelt wird.[445] Die konkrete Art der Übermittlung, also ob bspw. über Kabel oder Funk, im Wege der analogen oder digitalen Vermittlung, ist hierbei ebenso wenig ausschlaggebend, wie die gewählte Ausdrucksform, d. h. ob in Spra-

---

436 Vgl. *Epping*, Grundrechte, Kap. 17, S. 348, Rn. 736.

437 BVerfG NJW 2009, 2431 (2432).

438 Vgl. BVerfG NJW 2002, 3619 (3620); BVerfG NJW 2000, 55 (56).

439 *Epping*, Grundrechte, Kap. 17, S. 349, Rn. 737.

440 Vgl. *Epping*, Grundrechte, Kap. 17, S. 337, Rn. 713; S. 349, Rn. 737.

441 Vgl. BVerfG NJW 2008, 822 (825).

442 Vgl. BVerfG NJW 2000, 55 (56).

443 BVerfG NJW 2000, 55 (56).

444 Vgl. BVerfG NJW 2000, 55 (56); BVerfG NJW 2002, 3619 (3620); BVerfG NJW 2009, 2431 (2432).

445 Vgl. BVerfG NJW 2000, 55 (56); BVerfG NJW 2002, 3619 (3620); BVerfG NJW 2009, 2431 (2432).

che, Tönen, Bildern, Zeichen oder sonstigen Daten.[446] Der Schutzbereich des Fernmeldegeheimnisses erstreckt sich hierbei auch auf Kommunikationsdienste des Internets.[447]

Der Schutz des Fernmeldegeheimnisses umfasst neben dem Inhalt aber auch die näheren Umstände des jeweiligen Telekommunikationsvorgangs.[448] Gerade im Zuge der Digitalisierung der Telekommunikation werden bei so gut wie jeder Nutzung digitale Spuren hinterlassen, welche ebenfalls gespeichert und ausgewertet werden können.[449] Hierzu zählt insbesondere, ob, wann und wo[450], wie oft und zwischen welchen Personen bzw. Anschlüssen eine Telekommunikation stattgefunden hat oder versucht worden ist.[451] Derartige Daten haben „einen eigenen Aussagegehalt“[452] und „können im Einzelfall erhebliche Rückschlüsse auf das Kommunikations- und Bewegungsverhalten zulassen“[453], da vor allem „Häufigkeit, Dauer und Zeitpunkt von Kommunikationsverbindungen […] Hinweise auf Art und Intensität von Beziehungen [geben] und […] auf den Inhalt bezogene Schlussfolgerungen [ermöglichen]“[454]. Vom Schutzbereich des Art. 10 I GG erfasst sind neben Inhaltsdaten deshalb insbesondere auch die sog. *Verkehrsdaten* i. S. d. § 3 Nr. 30 TKG, § 96 I TKG.[455]

Da die Kommunikation bei der Verwendung von Telekommunikationseinrichtungen der besonderen Gefahrenlage einer Kenntnisnahme durch Dritte ausgesetzt ist, unterliegt Telekommunikation dem besonderen Schutz des Art. 10 I GG.[456] Denn anders als bei dem Gespräch unter Anwesenden haben die Gesprächspartner bei der Nutzung von Einrichtungen der Telekommunikation gerade nicht die Möglichkeit, „die Rahmenbedingungen der Kommunikation allein festzulegen und dabei auch über deren Privatheit und über die beteiligten Personen selbst zu wachen“[457]. Auf Grund der räumli-

---

446 Vgl. BVerfG NJW 2002, 3619 (3620); auch BVerfG NJW 2008, 822 (825).

447 Vgl. BVerfG NJW 2008, 822 (825); BVerfG NJW 2009, 2431 (2432).

448 Vgl. BVerfG NJW 2008, 822 (825); BVerfG NJW 2007, 351 (353); BVerfG NJW 2006, 976 (978); BVerfG NJW 2005, 2603 (2604); BVerfG NJW 2003, 1787 (1788); BVerfG NJW 2000, 55 (56); st. Rspr.

449 Vgl. BVerfG NJW 2006, 976 (978).

450 Vgl. BGH-Ermittlungsrichter NJW 2001, 1587 (1587).

451 Vgl. BVerfG NJW 2000, 55 (56); auch BVerfG NJW 2008, 822 (825); vgl. auch Maunz/Dürig – *Durner*, GG, Art. 10, 62. EL 2011, Rn. 86.

452 BVerfG NJW 2006, 976 (978).

453 BVerfG NJW 2006, 976 (978).

454 BVerfG NJW 2006, 976 (978) m. w. N.

455 Für Einzelheiten zum heimlichen Zugriff auf Verkehrsdaten nach § 100g StPO, siehe 1. Teil A.II.2.d).

456 Vgl. BVerfG NJW 2002, 3619 (3620).

457 BVerfG NJW 2002, 3619 (3620).

chen Trennung der Gesprächspartner sind diese „auf einen technischen Übermittlungsvorgang angewiesen, der nicht in ihrem ausschließlichen Einflussbereich liegt“[458]. Zweck der grundrechtlichen Verbürgung der Unverletzlichkeit des Fernmeldegeheimnisses ist es hierbei zu vermeiden, „dass der Meinungs- und Informationsaustausch mittels Fernmeldeanlagen deswegen unterbleibt oder nach Form und Inhalt verändert verläuft, weil die Beteiligten damit rechnen müssen, dass staatliche Stellen sich in die Kommunikation einschalten und Kenntnisse über die Kommunikationsbeziehungen oder Kommunikationsinhalte gewinnen“[459].

Mit der Vielfältigkeit der technischen Möglichkeiten für einen Zugriff durch Dritte, steigt auch das Risiko, dass sich Dritte Zugang zu Inhalt und Umständen der Kommunikation verschaffen.[460] Mit Blick auf die „Vernetzung moderner Infrastrukturen der Telekommunikation und der Einschaltung mehrerer Dienste für einen Übermittlungsvorgang“[461] besteht dieses Risiko heutzutage mehr denn je.[462]

Das Fernmeldegeheimnis aus Art. 10 I GG normiert deshalb zum Schutz der Vertraulichkeit von Telekommunikation „ein Abwehrrecht gegen die Kenntnisnahme des Inhalts und der näheren Umstände der Telekommunikation durch den Staat“[463] und begründet zugleich auch „einen Auftrag an den Staat, Schutz auch insoweit vorzusehen, als private Dritte sich Zugriff auf die Kommunikation verschaffen“[464]. Der Schutzauftrag bezieht sich[465] indes „auch auf die von Privaten betriebenen Telekommunikationsanlagen“[466].[467]

Allerdings endet die Reichweite des grundrechtlichen Schutzes des Fernmeldegeheimnisses „nicht in jedem Fall am Endgerät der Telekommunikationsanlage“[468]. Denn „eine Gefährdung der durch Art. 10 GG geschützten Vertraulichkeit der Telekommunikation kann auch durch einen Zugriff

---

458 BVerfG NJW 2002, 3619 (3620).

459 BVerfG NJW 2000, 55 (57).

460 Vgl. BVerfG NJW 2002, 3619 (3620).

461 BVerfG NJW 2002, 3619 (3620).

462 Vgl. BVerfG NJW 2002, 3619 (3620).

463 BVerfG NJW 2002, 3619 (3620).

464 BVerfG NJW 2002, 3619 (3620).

465 Nach der gemäß Art. 87f II GG erfolgten Liberalisierung des Telekommunikationswesens, vgl. BVerfG NJW 2002, 3619 (3620).

466 BVerfG NJW 2002, 3619 (3620).

467 So verpflichtet § 88 II TKG jeden Diensteanbieter i. S. d. TKG umfassend zur Wahrung des Fernmeldegeheimnisses.

468 BVerfG NJW 2006, 976 (979); vgl. bereits BVerfG NJW 2002, 3619 (3620); auch BVerfG NJW 2008, 822 (825).

am Endgerät erfolgen“[469]. Mit Blick auf diese neuere Rechtsprechung des BVerfG, die der technologischen Entwicklung sowie den vielfältigen modernen Kommunikationsdiensten, -mitteln und -wegen Rechnung trägt[470], dürften frühere Sichtweisen, wonach „der Schutzbereich des Art. 10 I GG [*allein*, Anm. d. Verf.] […] durch den Herrschaftsbereich des Betreibers des Fernmeldenetzes umgrenzt [wird]“[471], „Nachrichten [*nur*, Anm. d. Verf.] während des technischen Übermittlungsvorgangs [erfasst sind]“[472] und „der Grundrechtsschutz am Endgerät des Fernsprechteilnehmers [endet]“[473] zwischenzeitlich als überholt anzusehen sein:

Nach der jüngeren Rechtsprechung des BVerfG „[endet] die Reichweite des grundrechtlichen Schutzes […] *nicht* [Hervorh. d. Verf.] am so genannten Endgerät der Telekommunikationsanlage“[474]. Denn die modernen Endgeräte – auf einem von Konvergenz der Systeme[475] geprägten Telekommunikationsmarkt – ermöglichen eine Vielzahl von Leistungen, insbesondere „auch solche, die untrennbar in den Übermittlungsvorgang eingebunden […] sind“[476]. Diese Leistungen „[sind] dem Endteilnehmer häufig gar nicht in den Einzelheiten bekannt“[477] und „[unterliegen] jedenfalls nicht seiner alleinigen Einflussnahme“[478].

Nach dieser neueren Sichtweise kann deshalb „eine Gefährdung der durch Art. 10 I GG geschützten Vertraulichkeit der Telekommunikation […] auch durch Zugriff am Endgerät erfolgen“[479]. Gemäß fortgeführter Rspr. des BVerfG gelte dies – also die Betroffenheit des Schutzbereichs des Fernmeldegeheimnisses bei einem Zugriff am Endgerät – insbesondere für die Überwachung des „laufende[n] Kommunikationsvorgang[s][480] und hierbei „grundsätzlich auch dann, wenn das Endgerät ein vernetztes komplexes informationstechnisches System ist, dessen Einsatz zur Telekommunikation nur eine unter mehreren Nutzungsarten darstellt“[481].

---

469 BVerfG NJW 2006, 976 (979); vgl. bereits BVerfG NJW 2002, 3619 (3620); auch BVerfG NJW 2008, 822 (825).

470 Vgl. BVerfG NJW 2002, 3619 (3621).

471 BGH NJW 1996, 2940 (2943).

472 BGH NJW 1996, 2940 (2943).

473 BGH NJW 1996, 2940 (2943).

474 BVerfG NJW 2002, 3619 (3620); vgl. auch BVerfG NJW 2006, 976 (979); BVerfG NJW 2008, 822 (825).

475 Für Einzelheiten zur Konvergenz der Systeme, siehe 2. Teil A.II.6.b).

476 BVerfG NJW 2002, 3619 (3621).

477 BVerfG NJW 2002, 3619 (3621).

478 BVerfG NJW 2002, 3619 (3621).

479 BVerfG NJW 2002, 3619 (3621); vgl. auch BVerfG NJW 2006, 976 (979).

480 BVerfG NJW 2006, 976 (979); vgl. auch BVerfG NJW 2008, 822 (825).

481 BVerfG NJW 2008, 822 (825).

Auch in Bezug auf Kommunikation, welche über an das Internet angeschlossene informationstechnische Systeme geführt wird, sind die Feststellungen des BVerfG zur Reichweite des Fernmeldegeheimnisses sachgerecht, da – mit Blick auf den Zweck der Freiheitsverbürgung in Art. 10 I GG[482] – auch bei diesen modernen technischen Kommunikationsformen jene „spezifische Gefährdungslage“[483] einer (ungewollten) Kenntnisnahme der Kommunikationsdaten durch Dritte besteht – und zwar nicht nur auf der reinen Transportstrecke im (IP-)Netzbereich des jeweiligen Netzbetreibers, sondern – mit Blick auf die mittlerweile zur Verfügung stehenden technischen Zugriffsmöglichkeiten auf informationstechnische Systeme und darüber stattfindende Telekommunikation – gerade auch auf Endgeräten (v. a. Computern).[484] Denn auch bei Kommunikation über vernetzte informationstechnische Endgeräte haben die Gesprächspartner „nicht die Möglichkeit, die Rahmenbedingungen der Kommunikation allein festzulegen und dabei auch über deren Privatheit und über die beteiligten Personen selbst zu wachen“[485].[486]

Telekommunikationsdaten – Inhalte wie auch die näheren Umstände[487] – allerdings, die *nach Abschluss des Kommunikationsvorgangs* im Herrschaftsbereich des Telekommunikationsteilnehmers (ab-)gespeichert sind, unterliegen nicht mehr dem Fernmeldegeheimnis aus Art. 10 I GG, sondern sind durch das (subsidiäre[488]) Grundrecht auf informationelle Selbstbestimmung aus Art. 2 I i. V. m. Art. 1 I GG geschützt[489] sowie ggf. die Örtlichkeit ihrer Speicherung durch Art. 13 I GG. Der Schutz des Art. 10 I GG „endet insoweit in dem Moment, in dem die Nachricht bei dem Empfänger angekommen und der Übertragungsvorgang beendet ist“[490]. Im Herrschaftsbereich

---

482 Vgl. BVerfG NJW 2002, 3619 (3621).

483 BVerfG NJW 2009, 2431 (2433).

484 Ähnlich auch wie bei einem Telefon, in das ein Abhörgerät eingebracht wird und ebenfalls dem Schutz des Art. 10 I GG unterliegt, vgl. BVerfG NJW 2002, 3619 (3621).

485 BVerfG NJW 2002, 3619 (3620).

486 Knüpft doch nach st. Rpsr. des BVerfG der Schutz des Fernmeldegeheimnisses gerade an das jeweilige „Kommunikationsmedium an und will jenen Gefahren für die Vertraulichkeit begegnen, die sich gerade aus der Verwendung dieses Mediums ergeben“ (BVerfG NJW 2000, 55, 58); auch BVerfG NJW 2009, 2431 (2432).

487 Vgl. Löwe-Rosenberg – *Schäfer*, StPO und GVG, Zweiter Band, § 100a StPO, Rn. 47.

488 Vgl. BVerfG NJW 2000, 55 (56) m. w. N.

489 Vgl. BVerfG NJW 2008, 822 (825); bereits BVerfG NJW 2006, 976 (978); zur Eröffnung des Schutzbereichs bei einem Zugriff auf zugangsgesicherte Kommunikationsinhalte in einem E-Mail-Postfach, welches sich auf dem Server des Provider befindet und auf das der Nutzer nur über eine Internetverbindung zugreifen kann, siehe BVerfG NJW 2009, 2431 (2432 f.).

490 BVerfG NJW 2006, 976 (978).

des Empfängers fehlt es an der typischen Gefährdungslage einer Kommunikation zwischen örtlich getrennten Kommunikationspartner unter Verwendung von Telekommunikationsanlagen. Denn „die Nachricht ist mit Zugang bei dem Empfänger nicht mehr den erleichterten Zugriffsmöglichkeiten Dritter – auch des Staates – ausgesetzt, die sich aus der fehlenden Beherrschbarkeit und Überwachungsmöglichkeit des Übertragungsvorgangs durch die Kommunikationsteilnehmer ergeben“[491], da „die gespeicherten Inhalte und Verbindungsdaten […] sich dann nicht mehr von Dateien, die der Nutzer selbst angelegt hat [unterscheiden]“[492] und der Empfänger in seinem Herrschaftsbereich „eigene Schutzvorkehrungen gegen den ungewollten Datenzugriff treffen kann“[493].

In räumlicher Hinsicht (territorialer Schutzbereich) ist der Geltungsumfang des Fernmeldegeheimnisses nicht zwingend nur auf das Inland beschränkt.[494] Dies spielt gerade bei den – in der Praxis nicht seltenen – Fällen der Telekommunikation mit Auslandsbezug eine Rolle. Insbesondere bei den modernen Kommunikationsmöglichkeiten, wie u. a. der (weltweit von jedem Internetzugang mit den notwendigen Hard- und Softwareanforderungen theoretisch möglichen) Internettelefonie, kann ein extraterritorialer Bezug dergestalt vorliegen, dass sich ein oder auch beide Gesprächspartner (denkbar bei einem mobilen Endgerät, welches mit einer Überwachungssoftware versehen ist[495]) im Ausland befindet. Nach der Rspr. des BVerfG[496] kann aber der räumliche Schutzbereich des Art. 10 I GG ohne weiteres auch dann eröffnet sein, wenn bezüglich der Kommunikation mit Auslandsbezug das Erfassen und Aufzeichnen des Telekommunikationsverkehrs bzw. das anschließende Auswerten der erfassten Telekommunikationsvorgänge im Inland stattfindet und damit ein hinreichender territorialer Bezug zu inländischem staatlichen Handeln hergestellt ist. Auch in diesen Fällen greife eine Bindung durch Art. 10 I GG ein.[497]

---

491 BVerfG NJW 2006, 976 (978).

492 BVerfG NJW 2006, 976 (978).

493 BVerfG NJW 2006, 976 (978).

494 Vgl. BVerfG NJW 2000, 55 (57 f.).

495 Für die praktische Ermittlungsarbeit ist zu beachten, dass für den Fall, dass sich das mobile Gerät zum Zeitpunkt der Überwachung im europäischen Ausland befinden bzw. im Zeitraum der Überwachung dorthin verbracht werden sollte, gemäß Art. 20 des *Übereinkommen gemäß Artikel 34 des Vertrags über die Europäische Union über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union* (EU-RhÜbk) der betreffende Mitgliedstaat von der Überwachung zu unterrichten ist.

496 Vgl. BVerfG NJW 2000, 55 (58).

497 Vgl. BVerfG NJW 2000, 55 (58); zust. auch Maunz/Dürig – *Durner*, GG, Art. 10, 63. EL 2011, Rn. 64.

2. Eingriff und Rechtfertigung

Da das Fernmeldegeheimnis aus Art. 10 I GG die Vertraulichkeit von Telekommunikation umfassend zu schützen bezweckt, stellt „jede Kenntnisnahme, Aufzeichnung und Verwertung kommunikativer Daten [durch staatliche Stellen, Anm. d. Verf.[498]] ohne Einwilligung des Betroffenen ein[en] Grundrechtseingriff“[499] dar.

Nach Art. 10 II S. 1 GG sind Beschränkungen des Fernmeldegeheimnisses zulässig. Diese dürfen allerdings nur auf Grund eines Gesetzes angeordnet werden. Die Norm des Art. 10 II S. 1 GG enthält damit einen einfachen Gesetzesvorbehalt[500] (sog. *Schranke*). Anders als bspw. in Art. 13 GG (Unverletzlichkeit der Wohnung) ist in Art. 10 GG für Eingriffe zwar kein Richtervorbehalt in der Grundrechtsnorm niedergelegt. In (einfachgesetzlichen) Vorschriften, welche die Grundrechte aus Art. 10 I GG einschränken, ist ein solcher jedoch „zur verfahrensrechtlichen Absicherung des Kommunikationsgeheimnisses“[501] regelmäßig enthalten (vgl. bspw. §§ 100a, 100b I S. 1 StPO).[502]

Gemäß den allgemeinen Anforderungen an die Rechtfertigung von Grundrechtseingriffen, unterliegen Beschränkungen des Fernmeldegeheimnisses insbesondere dem Gebot der Verhältnismäßigkeit als sog. *Schranken-Schranke*. Repressive Eingriffsnormen und darauf gestützte Eingriffe müssen den legitimen Zwecken der Effektivität der Strafverfolgung und Verbrechenskämpfung sowie dem öffentlichen Interesse an möglichst vollständiger Wahrheitsermittlung im Strafverfahren[503] dienen, da diese Zwecke insoweit Einschränkungen des Fernmeldegeheimnisses aus Art. 10 I GG rechtfertigen (können).[504] Zur Erreichung dieser Zwecke müssen die jeweilige Eingriffsnorm und der darauf gestützte Eingriff des Weiteren geeignet, erforderlich wie auch verhältnismäßig im engeren Sinne (= angemessen) sein.

Um den Anforderungen an die Rechtfertigung eines Grundrechtseingriffs gerecht zu werden, erfordern Beschränkungen des Fernmeldegeheimnisses aus Art. 10 I GG aber nicht nur die Beachtung der allgemeinen verfassungsrechtlichen Voraussetzungen für grundrechtseinschränkende gesetzliche Re-

---

498 Vgl. vertiefend *Epping*, Grundrechte, Kap. 17, S. 353, Rn. 747.

499 BVerfG NJW 2009, 2431 (2433); vgl. bereits BVerfG NJW 2000, 55 (59).

500 Nicht jedoch – wie Art. 10 II S. 2 GG die Vermutung nahe legen könnte – einen sog. qualifizierten Gesetzesvorbehalt, vgl. Epping, Grundrechte, Kap. 17, S. 354, Rn. 749.

501 *Epping*, Grundrechte, Kap. 17, S. 354, Rn. 750.

502 Vgl. *Epping*, Grundrechte, Kap. 17, S. 354, Rn. 750.

503 Vgl. BVerfG NJW 2000, 55 (65); BVerfG NJW 2009, 2431 (2434).

504 Vgl. BVerfG NJW 2009, 2431 (2434).

gelungen, die einem legitimen Gemeinwohlzweck dienen und auch im Übrigen den Verhältnismäßigkeitsgrundsatz wahren.[505] Es ergeben sich aus Art. 10 GG vielmehr auch „besondere Anforderungen an den Gesetzgeber, die gerade die Verarbeitung personenbezogener Daten betreffen, welche mittels Eingriffen in das Fernmeldegeheimnis erlangt worden sind“[506]. Nach ständiger Rechtsprechung des BVerfG lassen sich „insoweit […] die Maßgaben, die das BVerfG im Volkszählungsurteil aus Art. 2 I i.V. mit Art. 1 I GG entwickelt hat […], weitgehend auf die speziellere Garantie in Art. 10 GG übertragen“[507]. Zu diesen Maßgaben gehört, „dass sich Voraussetzungen und Umfang der Beschränkungen [des Fernmeldegeheimnisses, Anm. d. Verf.] klar und für den Einzelnen erkennbar aus dem Gesetz ergeben“[508]. Insbesondere müsse „der Zweck, zu dem Eingriffe in das Fernmeldegeheimnis vorgenommen werden dürfen, bereichsspezifisch und präzise bestimmt werden und das erhobene Datenmaterial […] für diesen Zweck geeignet und erforderlich sein“[509]. Auch die „Speicherung und Verwendung erlangter Daten sind […] grundsätzlich an den Zweck gebunden, den das zur Kenntnisnahme ermächtigende Gesetz festgelegt hat“[510].

Des Weiteren vermittelt Art. 10 GG dem betroffenen Grundrechtsträger mit Blick auf den verfassungsrechtlichen Belang effektiven Rechtsschutzes (Art. 19 IV GG) auch einen Anspruch auf (nachträgliche) Kenntnisgewährung/Benachrichtigung von (heimlich durchgeführten) Maßnahmen der Telekommunikationsüberwachung. Denn ohne Kenntnis von derartigen Maßnahmen wäre es dem Betroffenen weder möglich die Unrechtmäßigkeit der Erfassung und Kenntnisnahme seiner Telekommunikationsdaten geltend zu machen noch etwaige Rechte auf Löschung oder Berichtigung einzufordern.[511] Der Anspruch auf Kenntnisgewährung verengt sich hierbei auch nicht sogleich auf den gerichtlichen Rechtsschutz aus Art. 19 IV GG. Es handele sich zunächst „vielmehr um ein spezifisches Datenschutzrecht, das gegenüber der informations- und datenverarbeitenden staatlichen Stelle geltend gemacht werden kann“[512]. Da allerdings auch die Pflicht zur Mitteilung dem Gesetzesvorbehalt des Art. 10 II GG unterfällt, ist es für den Fall, dass

---

505 Vgl. BVerfG NJW 2000, 55 (57).

506 BVerfG NJW 2000, 55 (57).

507 BVerfG NJW 2000, 55 (57); Zum sog. *Volkszählungsurteil* des BVerfG (BVerfG NJW 1984, 419) und dessen Konsequenzen für den Eingriff in das Fernmeldegeheimnis, siehe auch die Ausführungen unter 2. Teil A.II.1.b) sowie 3. Teil A.I.1.b).

508 BVerfG NJW 2000, 55 (57).

509 BVerfG NJW 2000, 55 (57).

510 BVerfG NJW 2000, 55 (57).

511 Vgl. BVerfG 2000, 55 (57).

512 BVerfG NJW 2000, 55 (57).

die Kenntnis von dem Eingriff dazu führen würde, dass der Eingriffszweck verfehlt bzw. gefährdet wird, von Verfassungs wegen jedoch nicht zu beanstanden, die Kenntnisgewährung entsprechend einzugrenzen, bspw. erst durch nachträgliche Inkenntnissetzung über den erfolgten Eingriff.[513]

Auf Grund der (prinzipiellen) Unbemerkbarkeit (heimlicher) Eingriffe in das Fernmeldegeheimnis, der Undurchsichtigkeit sich anschließender Datenverarbeitungsvorgänge für den Betroffenen, der Möglichkeit, Kenntnisgewährung zu beschränken und der hierdurch entstehenden Rechtsschutzlücken[514], beansprucht Art. 10 GG „zudem eine Kontrolle durch unabhängige und an keine Weisung gebundene staatliche Organe und Hilfsorgane“[515]. Nähere Vorgaben, wie die Kontrolle auszugestalten ist, enthält die Verfassung in Art. 10 GG allerdings nicht.[516] Dem Gesetzgeber stehe es damit „frei, die ihm geeignet erscheinende Form zu wählen, wenn sie nur hinreichend wirksam ist“[517]. Zur Wirksamkeit gehöre es hierbei, „dass sich die Kontrolle auf alle Schritte des Prozesses der Fernmeldeüberwachung erstreckt“[518]. Kontrollbedürftig sei „sowohl die Rechtmäßigkeit der Eingriffe als auch die Einhaltung der gesetzlichen Vorkehrungen zum Schutz des Fernmeldegeheimnisses“[519].

Abschließend gebieten es die Anforderungen an die Eingriffsrechtfertigung im Lichte von Art. 19 IV GG, erlangte Telekommunikationsdaten – deren Erfassung und Aufzeichnung genauso wie die Verwendung der darin enthaltenen Informationen an bestimmte Zwecke gebunden sind[520] – zu vernichten, sobald sie für die festgelegten Zwecke und/oder den gerichtlichen Rechtsschutz nicht mehr erforderlich sind.[521]

II. Unverletzlichkeit der Wohnung, Art. 13 I GG

Das Grundrecht aus Art. 13 I GG entfaltete in der rechtspolitischen und rechtsdogmatischen Diskussion hauptsächlich Relevanz im Zusammenhang mit der Thematik der sog. „Online-Durchsuchung“ unter Fernzugriff auf in Wohnungen oder sonstigen nach Art. 13 I GG geschützten Räumlichkeiten

513 Vgl. BVerfG NJW 2000, 55 (57).
514 Vgl. BVerfG NJW 2000, 55 (57) m. w. N.
515 BVerfG NJW 2000, 55 (57).
516 Vgl. BVerfG NJW 2000, 55 (57).
517 BVerfG NJW 2000, 55 (57).
518 BVerfG NJW 2000, 55 (57).
519 BVerfG NJW 2000, 55 (57).
520 Für Einzelheiten zum Grundsatz der Zweckbindung, siehe auch 2. Teil A.III.3.
521 Vgl. BVerfG NJW 2000, 55 (57 f.).

befindliche informationstechnische Systeme.[522] Hierzu hat das BVerfG in seiner Grundsatzentscheidung vom 27.02.2008 Stellung bezogen und eine generelle, von den Zugriffsmodalitäten unabhängige Anwendung des Grundrechtsmaßstabs aus Art. 13 I GG auf die Infiltration informationstechnischer Systeme verneint.[523] Im Zusammenhang mit der Quellen-TKÜ und der Infiltration eines informationstechnischen Systems mit einer Software zum Zwecke der Telekommunikationsüberwachung kommen daher – auf Grund der insoweit eindeutigen Feststellungen des BVerfG[524] – Art. 13 I GG-Gesichtspunkten nur noch begrenzte Bedeutung zu. Relevant wird das Grundrecht auf Unverletzlichkeit der Wohnung jedenfalls bei der Frage der Legitimation eines heimlichen Betretens von Wohnräumen bspw. zum unbemerkten Installieren der Überwachungssoftware im Rahmen der Sekundärmaßnahme einer Quellen-TKÜ.[525]

1. Schutzbereich

Bei dem Grundrecht auf *Unverletzlichkeit der Wohnung* aus Art. 13 I GG handelt es sich – wie bei Art. 10 GG – um ein *Jedermann-Grundrecht*. Vom Schutzbereich in persönlicher Hinsicht erfasst ist jeder Bewohner[526] einer von Art. 13 I GG geschützten Räumlichkeit.[527] Dem persönlichen Schutzbereich des Art. 13 I GG unterfallen allerdings nicht nur natürliche Personen.

---

522 Zum Stand der Diskussion vor der Entscheidung des BVerfG vom 27.02.2008 (NJW 2008, 822), vgl. Anm. *Vogel*/*Brodowski*, StV 2009, 632 (633).

523 Vgl. BVerfG NJW 2008, 822 (826); Anwendungsfall des Art. 13 I GG sei nach Auffassung des BVerfG aber die Infiltration eines in einer Wohnung befindlichen informationstechnischen Systems, um hierüber bestimmte Vorgänge innerhalb der Wohnung zu überwachen, indem angeschlossene Peripheriegeräte dazu genutzt werden, also etwa die Aktivierung eines angeschlossenen Mikrofons oder einer Webcam; wie die Abgrenzung unter 1. Teil A.II.2.a) zeigt, handelt es sich bei einem solchen Vorgehen um eine Maßnahme der Online-Durchsuchung.

524 Vgl. BVerfG NJW 2008, 822 (826), wonach „Art. 13 I GG […] dem Einzelnen allerdings keinen generellen, von den Zugriffsmodalitäten unabhängigen Schutz gegen die Infiltration seines informationstechnischen Systems [vermittelt], auch wenn sich dieses System in einer Wohnung befindet“ (826), m. w. N.; zur Entscheidung des BVerfG vom 27.02.2008 im Einzelnen, siehe 1. Teil B.IV.

525 Für Einzelheiten zur Frage des Betretens von Wohnräumen zum Aufspielen einer Überwachungssoftware, siehe 1. Teil A.II.4.b)bb) sowie 2. Teil B.I.2.b).

526 Abzustellen ist diesbezüglich allein auf den tatsächlichen Besitz, nicht auf das Eigentum an den Räumlichkeiten; nach teilw. vertretener Ansicht kommt es hierbei auf eine Rechtmäßigkeit des Besitzes im zivilrechtlichen Sinne nicht an, sofern eine persönliche Privatheit der Räume besteht, vgl. *Epping*, Grundrechte, Kap. 17, S. 339, Rn. 715, a. A. Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 12, der insoweit auf das berechtigte Innehaben abstellt.

527 Vgl. *Epping*, Grundrechte, Kap. 17, S. 339, Rn. 715.

Nach Maßgabe des Art. 19 III GG können sich auch inländische juristische Personen des Privatrechts auf das Grundrecht aus Art. 13 I GG berufen, da auch sie Inhaber von Wohn- oder Geschäftsräumen sein können.[528]

In sachlicher Hinsicht schützt das Grundrecht aus Art. 13 I GG „den räumlich gegenständlichen Bereich der Privatsphäre“[529]:

In den sachlichen Schutzbereich einbezogen ist – wie es der Wortlaut des Art. 13 I GG nahe legt – zunächst die *Wohnung i. e. S.* Schutzgut des Grundrechts aus Art. 13 I GG ist gemäß der Rspr. des BVerfG die Privatheit der Wohnung als elementarer Lebensraum[530], in deren räumlicher Sphäre die freie Persönlichkeitsentfaltung des Einzelnen stattfindet.[531] Das Grundrecht aus Art. 13 I GG steht deshalb sowohl mit dem allgemeinen Persönlichkeitsrecht aus Art. 2 I i. V. m. Art. 1 I GG als auch mit der Menschenwürdegarantie aus Art. 1 I GG in engem Zusammenhang.[532] Nach sachgerechter Definition fallen unter den Begriff der *Wohnung* daher all diejenigen Räume, „die der allgemeinen Zugänglichkeit durch eine räumliche Abschottung entzogen und zur Stätte privaten Lebens und Wirkens gemacht werden“[533], anders ausgedrückt „alle privaten Wohnzwecken gewidmete […] Räumlichkeiten, in denen der Mensch das Recht hat, in Ruhe gelassen zu werden“[534].

Unter Berücksichtigung des historischen Begriffsverständnisses wie auch des Schutzzweckes der Grundrechtsnorm werden von der Rspr. und dem überwiegenden Teil der Literatur neben der Wohnung i. e. S. aber auch grds. *Betriebs- und Geschäftsräume* in den sachlichen Anwendungsbereich des Art. 13 I GG miteinbezogen.[535] Der Begriff der *Wohnung* in Art. 13 I GG ist nach st. Rspr. des BVerfG insofern „weit auszulegen“[536]. Auch Arbeit, Beruf und Gewerbe dienen der freien Persönlichkeitsentfaltung des Einzelnen, weshalb nach teleologischer Auslegung auch die Räume, in denen

---

528 Vgl. BVerfG NJW 1971, 2299 (2299); BVerfG NJW 1976, 1735 (1735).

529 BeckOK – *Fink*, GG, Ed. 13, Art. 13, Rn. 1; bereits BVerfG NJW 1971, 2299 (2300); auch BVerfG NJW 2008, 822 (826).

530 Vgl. BVerfG NJW 2008, 822 (826); BVerfG NJW 1979, 1539 (1540); bereits BVerfG NJW 1976, 1735 (1735) m. w. N.

531 Vgl. Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 1; *Epping*, Grundrechte, Kap. 17, S. 339, Rn. 716; S. 340, Rn. 720.

532 Vgl. BeckOK – *Fink*, GG, Ed. 13, Art. 13, Rn. 1; BVerfG NJW 1971, 2299 (2300); BVerfG NJW 2008, 822 (826).

533 *Epping*, Grundrechte, Kap. 17, S. 339, Rn. 716 m. w. N.

534 BeckOK – *Fink*, GG, Ed. 13, Art. 13, Rn. 1; vgl. auch BVerfG NJW 1969, 1707 (1707).

535 Grundlegend BVerfG NJW 1971, 2299 (2299 ff.); ebenso BVerfG NJW 2008, 822 (826); vgl. auch *Epping*, Grundrechte, Kap. 17, S. 340, Rn. 718. ggf. jedoch unter herabgesetzter Schutzbedürftigkeit, vgl. BVerfG NJW 1998, 1627 (1631).

536 BVerfG NJW 1971, 2299 (2299), unter historischer Auslegung.

diese Persönlichkeitsentfaltung stattfindet, der räumlichen Privatsphäre unterfallen und somit dem Schutz des Art. 13 I GG unterliegen.[537] Differenzierend wird diese Sichtweise teilweise dahingehend eingeschränkt, dass betriebliche und geschäftliche Räume nur dann unter den sachlichen Schutzbereich des Art. 13 I GG fallen[538] bzw. die volle Schutzwirkung des Art. 13 I GG erhalten sollen[539], wenn zu diesen keine unkontrollierten, sondern nur vom Hausrecht des Inhabers abhängige Zugangsmöglichkeiten der Öffentlichkeit bestehen, also eine *gewisse räumliche Abschottung* im Sinne obiger Definition vorliegt.

In Bezug auf die technische Infiltration von informationstechnischen Systemen, welche sich in Wohnräumen oder sonstigen nach Art. 13 I GG geschützten Räumlichkeiten befinden, ist der sachliche Schutzbereich des Art. 13 I GG mit der Grundsatzentscheidung des BVerfG von 27.02.2008 nunmehr dahingehend konkretisiert worden, dass „Art. 13I GG […] dem Einzelnen […] keinen generellen, von den Zugriffsmodalitäten unabhängigen Schutz gegen die Infiltration seines informationstechnischen Systems [vermittelt], auch wenn sich dieses System in einer Wohnung befindet“[540].

2. Eingriff und Rechtfertigung

Beeinträchtigungen des Grundrechts aus Art. 13 I GG stellen alle staatlichen Handlungen dar, die ein Eindringen in die geschützten Räumlichkeiten gegen den Willen des Wohnungsinhabers zum Gegenstand haben.[541] Neben dem Betreten der geschützten Räume kann aber auch das dortige (fortgesetzte) Verweilen der Staatsgewalt – bspw. wenn das Betreten zunächst mit Willen des Hausrechtsinhabers erfolgt ist, dieser jedoch im weiteren Verlaufe seinen Willen ändert – eine Beeinträchtigung des Art. 13 I GG darstellen.[542]

Da das Grundrecht auf Unverletzlichkeit der Wohnung dem Schutz der räumlichen Privatsphäre und der freien Persönlichkeitsentwicklung des Einzelnen in den der allgemeinen Zugänglichkeit entzogenen Räumlichkeiten dient, kann ein Eingriff in Art. 13 I GG neben dem körperlichen Betreten

---

537 Vgl. BVerfG NJW 1971, 2299 (2299); *Epping*, Grundrechte, Kap. 17, S. 340, Rn. 720.

538 Vgl. bei *Epping*, Grundrechte, Kap. 17, S. 340, Rn. 718, 720 m. w. N.

539 Vgl. Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 14.

540 BVerfG NJW 2008, 822 (826); für Einzelheiten hierzu, siehe 1. Teil B.IV. sowie 2. Teil B.I.1.b) und 2.b).

541 Vgl. BVerfG NJW 1984, 419 (421); BVerfG NJW 1987, 2499 (2499).

542 Vgl. BVerfG NJW 1984, 419 (421); BVerfG NJW 1987, 2499 (2499); *Epping*, Grundrechte, Kap. 17, S. 342, Rn. 722.

auch durch ein nichtkörperliches Eindringen in die geschützten Räume in Form eines Sich-Einblick-Verschaffens in Vorgänge, welche innerhalb der Wohnung ablaufen und sich der natürlichen Wahrnehmung von außen entziehen, mit besonderen Hilfsmitteln erfolgen[543]. Denn in gleicher Weise wie die optische Überwachung kann insbesondere auch das akustische Überwachen einer Wohnung von außen durch in der Wohnung angebrachte Abhörvorrichtungen (einschließlich dem deren Benutzung vorgeschalteten und wiederum mit einem körperlichen Betreten verbundenen Anbringen in der geschützten Räumlichkeit[544]) die Privatsphäre beeinträchtigen und damit das Grundrecht aus Art. 13 I GG einschränken, wenn hierdurch eine Überwachung der in der Wohnung stattfindenden Vorgänge möglich wird.[545]

Anders als bspw. das Fernmeldegeheimnis in Art. 10 II S. 1 GG enthält Art. 13 GG keinen allgemeinen Gesetzesvorbehalt, sondern eine ausdifferenzierte Schrankendogmatik.[546] Von Verfassungs wegen zulässige Eingriffe in den Schutzbereich des Art. 13 I GG können durch körperliches Betreten im Rahmen von *Durchsuchungen*[547] (Art. 13 II GG), durch Überwachung der Vorgänge in der Wohnung von außen mittels technischen Geräts („unkörperliches Eindringen"[548]) im Rahmen von *bestimmten technischen Maßnahmen* (Art. 13 III GG repressiv[549], Art. 13 IV GG präventiv[550], Art. 13 V, VI GG) sowie durch Beschränkungen der Privatsphäre jeglicher Art – die nur nicht dem Zwecke des Durchsuchens (Abs. 2 insoweit lex specialis) oder dem Einsatz technischer Mittel (insoweit Abs. 3 bis 6 leges

---

543 So auch BVerfG NJW 2008, 822 (826).

544 Vgl. BVerfG NJW 1984, 419 (421); BVerfG NJW 2004, 999 (1005 f.).

545 Vgl. *Epping*, Grundrechte, Kap. 17, S. 342, Rn. 722; BeckOK – *Fink*, GG, Ed. 13, Art. 13, Rn. 8; auch die Messung elektromagnetischer Abstrahlungen, vgl. BVerfG NJW 2008, 822 (826).

546 So treffend *Kudlich*, HFR 2007, S. 205 m. w. N.

547 Kennzeichnend für eine Durchsuchung ist nach allgemeinem Begriffsverständnis „das ziel- und zweckgerichtete Suchen staatlicher Organe in einer Wohnung, um dort planmäßig etwas aufzuspüren, was der Inhaber der Wohnung von sich aus nicht offenlegen oder herausgeben will" (BVerwG NJW 1975, 130, 131); charakteristisch für das von der Strafprozessordnung geprägte Bild einer Durchsuchung (§§ 102 ff. StPO) ist hierbei die Offenlegung der Ermittlungen durch körperlich am Ort der Durchsuchung anwesende Ermittlungspersonen, vgl. BGH NJW 2007, 930 (930 f.).

548 Wobei der Vorbehalt des Art. 13 III GG auch das heimliche (körperliche) Betreten der Wohnung zum Anbringen des technischen Mittels mit umfasst, vgl. BT-Drs. 13/8651, S. 13; auch Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 79.

549 Nur akustische Überwachung, vgl. Art. 13 III S. 1 StPO („zur akustischen Überwachung").

550 Akustische wie auch optische Überwachung, vgl. Art. 13 IV S. 1 StPO („zur Überwachung").

speciales) dienen – bspw. durch Betreten, Besichtigen, Verweilen etc.[551] im Rahmen von *sonstigen (präventiven) Maßnahmen* (Art. 13 VII GG[552]) stattfinden.[553]

Bei den unter Art. 13 II bis VII GG formulierten speziellen Grundrechtsschranken, die einen Eingriff in das Grundrecht aus Art. 13 I GG rechtfertigen, handelt es sich i. d. R. um sog. *qualifizierte Gesetzesvorbehalte*[554]:

Verfassungsrechtlich zulässig ist ein Eingriff in Form der *Durchsuchung*[555], und zwar nach Maßgabe des Art. 13 II GG bei Vorliegen einer Anordnung durch den Richter (sog. *präventiver Richtervorbehalt*[556]) bzw. bei Gefahr im Verzug durch die in den jeweiligen (einfachgesetzlichen) Normen vorgesehenen anderen Organe sowie bei Vorliegen der Formerfordernisse, wie in den jeweiligen Gesetzen vorgeschrieben. Gemäß dem hieraus in leicht „verklausulierter" Form[557] zum Ausdruck kommenden Gesetzesvorbehalt, bedarf jeder auf Art. 13 II GG gestützte Eingriff in Art. 13 I GG einer einfachgesetzlichen Rechtsgrundlage, die insbesondere auch das Zitiergebot nach Art. 19 I S. 2 GG zu beachten hat.[558]

Der Verankerung von Grundrechtsschranken in Art. 13 GG für *technische Maßnahmen* zur Überwachung von Wohnungen ging eine lange rechtliche wie rechtspolitische Debatte voraus. Die im Jahr 1998 in Art. 13 GG eingefügten[559] Absätze 3 bis 6 enthalten nunmehr für derartige technische Maßnahmen speziellen Schranken zur Rechtfertigung des damit verbundenen Grundrechtseingriffs in Art. 13 I GG.

---

551 Unter bestimmten Voraussetzungen soll ein Betreten von Betriebs- und Geschäftsräumen auf Grund besonderer Befugnisnormen (z. B. § 17 HandwO oder § 22 GastG) zur Nachschau, ob bestimmte gesetzliche Bestimmungen eingehalten werden (z. B. Hygienevorschriften), schon gar keinen Eingriff in Art. 13 GG darstellen, vgl. hierzu im Einzelnen *Epping*, Grundrechte, Kap. 17, S. 343 f., Rn. 723 f. sowie BVerfG NJW 1971, 2299 (2301); vertieft auch bei Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 141 ff.

552 Als subsidiärer Auffangtatbestand, vgl. BeckOK – *Fink*, GG, Ed. 13, Art. 13, Rn. 27 ff.

553 Vgl. *Epping,* Grundrechte, Kap. 17, S. 342, Rn. 722.

554 Vgl. *Epping*, Grundrechte, Kap. 17, S. 344, Rn. 726.

555 Auf einfachgesetzlicher Ebene sowohl auf Grundlage des Strafprozessrechts, des Polizei- und Sicherheitsrechts, des übrigen Verwaltungsrechts als auch des Zivilprozessrechts, vgl. Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 23.

556 Vgl. hierzu Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 21.

557 Vgl. Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 21.

558 Vgl. *Epping*, Grundrechte, Kap. 17, S. 346, Rn. 729.

559 Für Einzelheiten zu Vorgeschichte, Inhalt und Verlauf der Grundgesetzänderung vom 26.03.1998, siehe Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 47 ff. m. w. N.

Zu repressiven Zwecken rechtfertigen nach Maßgabe des Art. 13 III S. 1 GG ein durch bestimmte Tatsachen begründeter Verdacht der Begehung einer besonders schweren Straftat und die Wahrung der Subsidiaritätsvorgabe, dass die Erforschung des Sachverhaltes auf andere Weise unverhältnismäßig erschwert oder aussichtslos wäre, die befristete (Art. 13 III S. 2 GG) akustische Überwachung von Wohnungen durch technische Mittel (einschließlich dem vorherigen Anbringen der Abhöreinrichtung). Außer bei Gefahr im Verzug ist hierfür die Anordnung durch eine mit drei Richtern besetzte Spruchkammer erforderlich (Art. 13 III S. 3 u. 4 GG). Trotz der detaillierten Regelungen formeller wie materieller Voraussetzungen stellt Art. 13 III GG keine verfassungsunmittelbare Rechtsgrundlage für eine akustische Überwachung von Wohnräumen zu repressiven Zwecken dar.[560] Eine derartige Maßnahme bedarf vielmehr einer einfachgesetzlichen Umsetzung, welche gegenwärtig in den Vorschriften der §§ 100c ff. StPO[561] normiert ist.

Hingegen erlaubt die Abwehr einer dringenden Gefahr für die öffentliche Sicherheit nach Maßgabe des Art. 13 IV S. 1 GG den präventiven Einsatz technischer Mittel zur Wohnraumüberwachung auf Grund (bei Gefahr im Verzug unverzüglich nachzuholender, vgl. Art. 13 IV S. 2 GG) richterlicher Anordnung, ohne Beschränkung auf akustische Mittel wie bei der repressiven Maßnahme nach Art. 13 III GG, weshalb der Einsatz akustischer wie auch optischer Überwachungsmittel zu präventiven Zwecken von Art. 13 IV S. 1 GG gedeckt ist.

Ausschließlich zum Schutz einer beim Einsatz in einer Wohnung tätigen Person (v. a. verdeckte Ermittler[562], ggf. auch Vertrauenspersonen[563]) kann nach Maßgabe des Art. 13 V S. 1 GG der Einsatz technischer Mittel durch eine gesetzlich bestimmte Stelle angeordnet werden. Eine Verwertung der hierbei erlangten Erkenntnisse zu Zwecken der Strafverfolgung oder der

---

560 Vgl. Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 73.

561 Einfachgesetzlich ist die repressive Befugnis zur Durchführung von Maßnahmen der heimlichen akustischen Überwachung von Wohnräumen in den §§ 100c ff. StPO (sog. *Großer Lauschangriff*) normiert; für Einzelheiten zur Maßnahme der akustischen Wohnraumüberwachung nach §§ 100c ff. StPO in Abgrenzung zur Maßnahme der Quellen-TKÜ, siehe 1. Teil A.II.2.b).

562 Verdeckte Ermittler sind gemäß der Legaldefinition in § 110a II StPO „Beamte des Polizeidienstes, die unter einer ihnen verliehenen, auf Dauer angelegten, veränderten Identität (Legende) ermitteln".

563 Eine Vertrauensperson („V-Mann") ist im Gegensatz zu einem verdeckten Ermittler eine Privatperson, die von staatlicher Seite zum Zwecke der Aufklärung von Straftaten eingesetzt wird; zur Frage, ob diese unter den Tatbestand des Art. 13 V S. 1 GG („bei einem Einsatz") fallen, vgl. Maunz/Dürig – *Papier*, GG, Art. 13, 63. EL 2011, Rn. 110.

Gefahrenabwehr ist jedoch nach Art. 13 V S. 2 HS 1 GG nur nach (bei Gefahr im Verzug unverzüglich nachzuholender, Art. 13 V S. 2 HS 2 GG) richterlicher Feststellung der Rechtmäßigkeit der Maßnahme zulässig.

Für *sonstige Maßnahmen*[564] (präventiver Natur) nach Art. 13 VII GG gelten die dort formulierten speziellen Schranken hinsichtlich der Abwehr von Gefahren, an denen sich ein solcher Eingriff messen lassen muss. Bei der „Abwehr einer gemeinen Gefahr oder Lebensgefahr" unterliegt das Grundrecht auf Unverletzlichkeit der Wohnung nach überwiegender Ansicht einer grundrechtsunmittelbaren Schranke[565], bei der „Verhütung dringender Gefahr für die öffentliche Sicherheit und Ordnung" einem qualifizierten Gesetzesvorbehalt.[566]

III. Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, Art. 2 I i.V.m. Art. 1 I GG (sog. *IT-Grundrecht*)

1. Schutzbereich

Im Rahmen seiner Grundsatzentscheidung vom 27.02.2008 zur Zulässigkeit der Online-Durchsuchung im Verfassungsschutzgesetz des Landes Nordrhein-Westfalen[567], hat das BVerfG erstmals aus dem allgemeinen Persönlichkeitsrecht nach Art. 2 I i.V.m. Art. 1 I GG das neue *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* (kurz: *IT-Grundrecht*[568]) abgeleitet und formuliert.[569]

---

564 D.h. jede in das Grundrecht aus Art. 13 I GG eingreifende Maßnahme, die weder eine Durchsuchung i.S.d. Art. 13 II GG noch einen Einsatz technischer Mittel i.S.d. Art. 13 III-V GG darstellt.

565 Vgl. *Epping*, Grundrechte, Kap. 17, S. 344, Rn. 726; insoweit sind Eingriffe in Art. 13 I GG bereits auf Grundlage des Art. 13 VII GG zulässig, ohne dass es einer zusätzlichen einfachgesetzlichen Rechtsgrundlage bedarf, vgl. Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 121 f.

566 Für Zwecke, die mit der (Quellen-)TKÜ verfolgt werden, enthält Art. 13 GG demnach keine Schranke; für Einzelheiten hierzu, siehe 2. Teil B.I.2.b)aa) sowie 3. Teil B.III.4.

567 BVerfG NJW 2008, 822.

568 So bspw. das Bundesministerium der Justiz, http://www.bmj.de/DE/Buerger/digitaleWelt/IT_Grundrecht/onlineDuchsuchung_node.html (zuletzt aufgerufen 15.06.2012).

569 Vgl. BVerfG NJW 2008, 822 (824), wonach es sich bei dem *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* um eine besondere Ausprägung des allgemeinen Persönlichkeitsrechts aus Art. 2 I i.V.m. Art 1 I GG handele; hierzu auch *Kudlich*, JA 2008, 475 (478), dem zufolge

Die zunehmende Verbreitung von über das Internet miteinander vernetzbaren komplexen informationstechnischen Systemen in den Haushalten – allen voran der stationäre Personal Computer (PC), aber auch mobile Geräte wie Laptops/Notebooks, Smartphones etc. – eröffnen dem Einzelnen nicht nur neue Möglichkeiten der Persönlichkeitsentfaltung, sondern begründen vor allem auch neue Gefährdungen der Persönlichkeit. Dies vor allem in der Hinsicht, als komplexe informationstechnische Systeme eine Vielzahl von Möglichkeiten der Nutzung bieten, die allesamt mit einem – bewussten wie auch selbsttätigen – Erzeugen, Verarbeiten und (ggf. auch nur temporären) Speichern von Daten verbunden sind.[570] Sowohl die vom Nutzer bewusst angelegten Daten als auch die durch das System selbsttätig generierten (mitunter auch flüchtigen) Daten geben Rückschlüsse auf Verhaltensweisen, Eigenschaften sowie persönliche Verhältnisse des Nutzers und lassen sich bis hin zur Persönlichkeitsprofilbildung entsprechend auswerten.[571] Die Gefährdungen erhöhen sich abermals, wenn die Systeme – insbesondere über das Internet – miteinander vernetzt sind. Denn im Vergleich zu alleinstehenden Systemen führt die mit der fortschreitenden Vernetzung von informationstechnischen Systemen verbundene Zunahme an Nutzungsmöglichkeiten nicht nur zu einer zusätzlichen Vielzahl und Vielfalt der anfallenden Daten wie insbesondere Kommunikationsinhalte und (sonstige) Daten mit Bezug zur Netzkommunikation, sondern schafft darüber hinaus für Dritte vor allem auch die Möglichkeit, technisch auf das System über das Datennetz zuzugreifen.[572] Im Rahmen solcher Zugriffe auf informationstechnische Systeme besteht die Gefahr eines Ausspähens oder gar Manipulierens dort vorhandener Daten, ohne dass der Durchschnittsnutzer zum Teil derartige Zugriffe auf sein System überhaupt bemerkt und es ihm möglich wäre, jeden Fall des Zugriffs wirkungsvoll abzuwehren.[573]

Mit Blick auf die Bedeutung der Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung sowie auf die hiermit verbundenen Gefährdungen, besteht ein „grundrechtlich erhebliches Schutzbedürfnis“[574] dahingehend, dass „der Einzelne […] darauf angewiesen [ist], dass der Staat die […] berechtigten Erwartungen an die Integrität und Vertraulichkeit derartiger Systeme achtet“[575]. Dem Schutzbedürfnis hinsichtlich der staatlichen

---

die Statuierung eines eigenständigen Grundrechts durchaus „Charme“ habe und in der Bedeutung mit der Entwicklung des Grundrechts auf informationelle Selbstbestimmung vergleichbar werden könnte.

570 Vgl. auch BVerfG NJW 2008, 822 (824).

571 Vgl. auch BVerfG NJW 2008, 822 (824).

572 Vgl. auch BVerfG NJW 2008, 822 (825).

573 Vgl. auch BVerfG NJW 2008, 822 (825).

574 BVerfG NJW 2008, 822 (825).

575 BVerfG NJW 2008, 822 (825).

Achtung der Integrität und Vertraulichkeit informationstechnischer Systeme zur ungehinderten Entfaltung der Persönlichkeit wird allerdings nach Auffassung des BVerfG durch die grundrechtlichen Gewährleistungen der Art. 10 GG und Art. 13 GG sowie durch das allgemeine Persönlichkeitsrecht aus Art. 2 I i. V. m. Art. 1 I GG in seinen bisher von der höchstrichterlichen Rspr. entwickelten Ausprägungen in Gestalt des *Schutzes der Privatsphäre* wie auch des *Rechts auf informationelle Selbstbestimmung* nicht hinreichend und vollständig Rechnung getragen.[576] Denn gemäß den Feststellungen des BVerfG bleibt eine grundrechtliche Schutzlücke, „soweit der heimliche Zugriff auf ein informationstechnisches System dazu dient, Daten auch insoweit zu erheben, als Art. 10 I GG nicht vor einem Zugriff schützt“[577], also gemäß den im Rahmen der Entscheidungsbegründung getätigten Aussagen des BVerfG zum Grundrechtsschutz des Fernmeldegeheimnisses[578] insbesondere dann, wenn „eine staatliche Stelle die Nutzung eines informationstechnischen Systems als solche überwacht oder die Speichermedien des Systems durchsucht“[579] oder wenn „Inhalte oder Umstände außerhalb der laufenden Telekommunikation“[580] erfasst werden.

Sachlicher Schutzbereich des neu entwickelten *IT-Grundrechts* ist daher in besonderer Ausprägung des allgemeinen Persönlichkeitsrechts aus Art. 2 I i. V. m. Art. 1 I GG die *Vertraulichkeit* und *Integrität* von *informationstechnischen Systemen*.[581]

Nicht jedes informationstechnische System, welches personenbezogene Daten erzeugen, verarbeiten oder speichern kann, ist indes in den Schutzbereich eines eigenständigen persönlichkeitsrechtlichen Grundrechts einzubeziehen.[582] Der Schutz durch das *Recht auf informationelle Selbstbestimmung* ist zur Wahrung berechtigter Geheimhaltungsinteressen von Betroffenen ausreichend, soweit ein System gemäß seiner technischen Konstruktion lediglich Daten enthält, die nur einen punktuellen Bezug zu einem bestimmten Lebensbereich des Betroffenen aufweisen[583], da sich in diesen Fällen „ein staatlicher Zugriff auf den vorhandenen Datenbestand qualitativ nicht von anderen Datenerhebungen [unterscheidet]“[584]. Unter den Begriff

---

576 Vgl. BVerfG NJW 2008, 822 (825 ff.).

577 BVerfG NJW 2008, 822 (825).

578 Für Einzelheiten, siehe 1. Teil B.IV.1.

579 BVerfG NJW 2008, 822 (825).

580 BVerfG NJW 2008, 822 (825).

581 Vgl. im Einzelnen BVerfG NJW 2008, 822 (827).

582 So BVerfG NJW 2008, 822 (827).

583 Bspw. „nicht vernetzte elektronische Steuerungsanlagen der Haustechnik“ (BVerfG NJW 2008, 822, 827).

584 BVerfG NJW 2008, 822 (827).

des *informationstechnischen Systems* i. S. d. besonderen Ausprägung des allgemeinen Persönlichkeitsrechts als *IT-Grundrecht* sind vielmehr nur solche Systeme zu fassen, die „allein oder in ihren technischen Vernetzungen 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“[585]. Diese Möglichkeit besteht vor allem bei (komplexen) Systemen wie bspw. (stationären) PCs, (mobilen) Notebooks/Laptops, Faxgeräten, (multifunktionalen) Mobiltelefonen, PDAs, Smartphones sowie vergleichbaren Systemen. Zudem ist ein Ziehen von Rückschlüssen aus dem Nutzungsverhalten auf persönliche Eigenschaften und Vorlieben hierbei i. d. R. unabhängig davon möglich, ob derartige Systeme privat oder geschäftlich genutzt werden.[586] Der Begriff des informationstechnischen Systems kann – innerhalb dieser Schutzbereichsvoraussetzungen – durchaus weit verstanden werden, um derzeitigen und zukünftigen technischen Entwicklungen Rechnung zu tragen.[587]

Schutzgut des neuen IT-Grundrechts ist hierbei zunächst das Interesse des Nutzers an der Wahrung der *Vertraulichkeit* der Daten, die von einem in den Schutzbereich des Grundrechts fallenden informationstechnischen System erzeugt, verarbeitet und gespeichert werden.[588] Vertraulichkeit bedeutet in diesem Zusammenhang, dass eine erzeugte, verarbeitete und gespeicherte Information nur für „befugte“ Personen zugänglich ist.[589]

Geschützt durch das IT-Grundrecht ist darüber hinaus auch das Interesse des Nutzers an der Gewährleistung der *Integrität* seiner von der besonderen Ausprägung des allgemeinen Persönlichkeitsrechts erfassten informationstechnischen Systeme. Die Integrität ist tangiert, wenn auf ein solches System in einer Weise zugegriffen wird, „dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können“[590], da „dann […]

---

585 BVerfG NJW 2008, 822 (827).

586 So BVerfG NJW 2008, 822 (827).

587 So jedenfalls das Bundesministerium des Innern, welches hierunter ein System subsumiert, das „aus Hard- und Software sowie aus Daten besteht, das der Erfassung, Speicherung, Verarbeitung, Übertragung und Anzeige von Informationen und Daten dient“ (Fragenkatalog BMJ, S. 2, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf, zuletzt aufgerufen 15.06.2012); auch Bundesministerium des Innern, Fragenkatalog SPD, S. 15, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

588 So BVerfG NJW 2008, 822 (827).

589 Vgl. auch *Holznagel*/*Schumacher*, MMR 2009, 3 (3).

590 BVerfG NJW 2008, 822 (827).

die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen [ist]“[591].

Zwar gewährleistet das allgemeine Persönlichkeitsrecht aus Art. 2 I i. V. m. Art. 1 I GG gemäß wiederholter Rspr. des BVerfG „Elemente der Persönlichkeit, die nicht Gegenstand der besonderen Freiheitsgarantien des Grundgesetzes sind, diesen aber in ihrer konstituierenden Bedeutung für die Persönlichkeit nicht nachstehen“[592]. Die besondere Ausprägung als *IT-Grundrecht* tritt allerdings zu den anderen Konkretisierungen des allgemeinen Persönlichkeitsrechts aus Art. 2 I i. V. m. Art. 1 I GG – wie bspw. dem *Recht auf informationelle Selbstbestimmung* – sowie zu den Grundrechtsgewährleistungen des *Fernmeldegeheimnisses* aus Art. 10 I GG und der *Unverletzlichkeit der Wohnung* aus Art. 13 I GG nur hinzu, „soweit diese keinen oder keinen hinreichenden Schutz gewähren“[593]. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme schützt deshalb „vor Eingriffen in informationstechnische Systeme nur, soweit der Schutz nicht durch andere Grundrechte, insbesondere Art. 10 oder Art. 13 GG, sowie das Recht auf informationelle Selbstbestimmung gewährleistet ist“[594].

2. Eingriff und Rechtfertigung

Ein Eingriff in den Schutzbereich des IT-Grundrechts liegt dann vor, wenn die Vertraulichkeit der von einem der geschützten Systeme erzeugten, verarbeiteten und gespeicherten Daten durch (vom Nutzer nicht autorisiertes) Sich-Zugang-Verschaffen beeinträchtigt wird. Ein Eingriff liegt des Weiteren vor, wenn die Integrität eines hiervon erfassten informationstechnischen Systems tangiert wird, indem auf das System in der Weise zugegriffen wird, „dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können“[595], da „dann […] die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen [ist]“[596]. So schütze das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gemäß den durch das BVerfG entwickelten Grundsätzen gerade „vor einem heimlichen Zugriff, durch den die auf dem System vorhandenen Daten ganz oder

---

591 BVerfG NJW 2008, 822 (827).

592 BVerfG NJW 2008, 822 (824); vgl. bereits BVerfG NJW 1980, 2070 (2070); BVerfG NJW 1999, 1322 (1323); BVerfG NJW 2006, 207 (208).

593 BVerfG NJW 2008, 822 (824).

594 BVerfG NJW 2009, 2431 (2433).

595 BVerfG NJW 2008, 822 (827).

596 BVerfG NJW 2008, 822 (827).

zu wesentlichen Teilen ausgespäht werden können“[597], wobei der Grundrechtsschutz „sowohl die im Arbeitsspeicher gehaltenen als auch die temporär oder dauerhaft auf den Speichermedien des Systems abgelegten Daten“[598] umfasse. Dabei schützt das Grundrecht „auch vor Datenerhebungen mit Mitteln, die zwar technisch von den Datenverarbeitungsvorgängen des betroffenen informationstechnischen Systems unabhängig sind, aber diese Datenverarbeitungsvorgänge zum Gegenstand haben“[599], wie dies bspw. beim Einsatz von Keyloggern oder bei Messung der elektromagnetischen Abstrahlungen von Bildschirm oder Tastatur der Fall ist.[600]

Der grundrechtliche Schutz des neuen IT-Grundrechts ist indes nicht schrankenlos. Eingriffe in die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme können sowohl zu präventiven als auch zu repressiven Zwecken gerechtfertigt sein, soweit die Beschränkungen des Grundrechts auf einer verfassungsmäßigen gesetzlichen Grundlage beruhen.[601]

IV. Urteil des BVerfG vom 27.02.2008

Im Rahmen seiner Grundsatzentscheidung vom 27.02.2008[602] hat das BVerfG zur (präventiven) Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalen festgestellt, dass eine solche Maßnahme nicht zwangsläufig in Art. 10 GG und Art. 13 GG eingreifen muss. Denn das *Fernmeldegeheimnis* aus Art. 10 I GG schütze nämlich nur die im Rahmen des Telekommunikationsverkehrs stattfindende unkörperliche Informationsübermittlung.[603] Das Recht auf *Unverletzlichkeit der Wohnung* aus Art. 13 GG gewähre nur den Schutz vor körperlichem Eindringen in die Wohnung sowie vor dem Einblick in Vorgänge innerhalb der Wohnung mit besonderen Hilfsmitteln.[604] Das im Zusammenhang mit der Online-Durchsuchung maßgebende Grundrecht sei vielmehr das im Rahmen der Grundsatzentscheidung erstmals hergeleitete *Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme* als besondere Ausprägung des *allgemeinen Persönlichkeitsrechts* aus Art. 2 I i. V. m. Art. 1 I GG. Denn die Online-Durch-

---

597 BVerfG NJW 2008, 822 (827).

598 BVerfG NJW 2008, 822 (827).

599 BVerfG NJW 2008, 822 (827).

600 Vgl. BVerfG NJW 2008, 822 (827).

601 So BVerfG NJW 2008, 822 (827).

602 Urteil des 1. Senates des Bundesverfassungsgerichts vom 27.02.2008 (BVerfG NJW 2008, 822).

603 Vgl. BVerfG NJW 2008, 822 (825).

604 Vgl. auch BVerfG NJW 2008, 822 (826).

suchung stelle eine Maßnahme dar, die regelmäßig auf die Überwachung der Nutzung des Systems sowie das Auslesen der auf seinen Speichermedien enthaltenen Daten gerichtet ist.[605] Im Rahmen präventiver Zielsetzung sei daher ein solcher Eingriff verfassungsrechtlich nur gerechtfertigt, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen.[606]

Anders stellt sich dies angesichts der grundlegenden und differenzierenden Feststellungen des BVerfG wiederum für die verfassungsrechtliche Bewertung der technischen Infiltration informationstechnischer Systeme zum Zwecke der Telekommunikationsüberwachung („Quellen-TKÜ") dar.[607] Online-Durchsuchung und Quellen-TKÜ stellen bereits von ihrem Überwachungsgegenstand her zwei unterschiedliche Maßnahmen dar, die daher differenziert zu betrachten sind. Da die eigentliche Überwachung und Aufzeichnung der Telekommunikation an der Quelle in ähnlicher Weise wie die Online-Durchsuchung durch vorherige Infiltration des Systems vorbereitet wird, hat das BVerfG im Rahmen seiner Entscheidung zur Verfassungsmäßigkeit der Vorschriften zur (präventiven) Online-Durchsuchung im nordrhein-westfälischen Verfassungsschutzgesetz spezifische Aussagen zur Reichweite des grundrechtlichen Schutzes des Art. 10 I GG (1.) wie auch zur technischen Infiltration informationstechnischer Systeme zum Zwecke der Telekommunikationsüberwachung (2.) getroffen, welche auch für die (verfassungs-)rechtliche Bewertung und nähere Einordnung der Quellen-TKÜ in das strafprozessuale Befugnisnormensystem von Bedeutung sind.

Die besondere Systematik der Entscheidung – über deren absolute Schlüssigkeit bzw. Widerspruchsfreiheit sich freilich streiten lässt – eröffnet indes Raum für Interpretationen (auf Seiten beider „Lager") darüber, welche genauen Vorstellung und Anforderungsmaßstäbe des BVerfG bei seinen Aussagen zum Ermittlungsinstrument der Quellen-TKÜ letztlich vor Augen gehabt hat. So trifft das BVerfG zum Teil sehr konkrete und grundsätzliche Aussagen, zum Teil bleiben dessen Ausführungen eher an der Oberfläche. Einerseits stellt das BVerfG fest, dass technische Infiltrationen zum Zwecke der Telekommunikationsüberwachungen spezifische Gefährdungen der Persönlichkeit bewirken können, denen durch Art. 10 I GG nicht oder nicht hinreichend begegnet werden kann, andererseits stellt es aber insoweit auch ausdrücklich klar, dass Art. 10 I GG mitunter der alleinige Grundrechtsmaßstab für Ermächtigungen zu Quellen-TKÜ-Maßnahmen ist, wenn ausschließlich Daten aus laufenden Telekommunikationsvorgängen erfasst werden und dies entsprechend durch technische Vorkehrungen und rechtliche Vorgaben

605 Vgl. BVerfG NJW 2008, 822 (827).
606 Vgl. BVerfG NJW 2008, 822 (831).
607 Vgl. BVerfG NJW 2008, 822 (825 f.).

sichergestellt ist.[608] Offenbar hatte das BVerfG – wobei schon hier die Interpretation beginnt – zwei „Infiltrations-Konstellationen" vor Augen gehabt hatte, nämlich einmal der „reine" und hierfür entsprechend abgesicherte Quellen-TKÜ-Zugriff, welcher allein am Maßstab des Art. 10 I GG zu messen ist, und auf der anderen Seite der „weitergehende" Zugriff, dem mit Art. 10 I GG nicht oder nicht hinreichend begegnet werden kann. Zum einen sagt das BVerfG also deutlich, dass bei reiner Quellen-TKÜ allein Art. 10 I GG grundrechtlicher Maßstab für die Beurteilung einer Ermächtigungsnorm ist, zum anderen trifft das BVerfG freilich kein eindeutiges Votum (um die strafprozessuale Situation ging es in der Entscheidung auch nicht) zugunsten der §§ 100a, 100b StPO als repressive Ermächtigungsgrundlage für eine solche Quellen-TKÜ.

1. Aussagen zur Reichweite des Schutzes durch Art. 10 I GG

Zur Reichweite der Grundrechtsgewährleistung aus Art. 10 I GG stellt das BVerfG in Bezug auf laufende Telekommunikation im Rechnernetz zunächst fest, dass ein Eingriff allein an Art. 10 I GG zu messen ist,

> „soweit eine Ermächtigung sich auf eine staatliche Maßnahme beschränkt, durch welche die Inhalte und Umstände der laufenden Telekommunikation im Rechnernetz erhoben oder darauf bezogene Daten ausgewertet werden […]"[609].

Gemäß wiederholter Rspr. des BVerfG ist der Schutzbereich des Fernmeldegeheimnisses „dabei unabhängig davon betroffen, ob die Maßnahme technisch auf der Übertragungsstrecke oder am Endgerät der Telekommunikation ansetzt"[610]. Diese Aussage wird vom BVerfG im Rahmen seiner Entscheidung vom 27.02.2008 für die besondere Konstellation vernetzter Systeme dahingehend konkretisiert, dass dies

> „grundsätzlich auch dann [gilt], wenn das Endgerät ein vernetztes komplexes informationstechnisches System ist, dessen Einsatz zur Telekommunikation nur eine unter mehreren Nutzungsarten darstellt"[611].

In Bestätigung seiner Rspr. vom 02.03.2006[612] merkt das BVerfG auch in der vorliegenden Entscheidung an, dass sich der Grundrechtsschutz des Fernmeldegeheimnisses aus Art. 10 I GG hingegen „nicht auf die nach Abschluss eines Kommunikationsvorgangs im Herrschaftsbereich eines Kom-

---

608 Vgl. BVerfG NJW 2008, 822 (826).

609 BVerfG NJW 2008, 822 (825).

610 BVerfG NJW 2008, 822 (825); vgl. bereits BVerfG NJW 2002, 3619 (3620 f.) und BVerfG NJW 2006, 976 (979).

611 BVerfG NJW 2008, 822 (825).

612 BVerfG NJW 2006, 976.

munikationsteilnehmers gespeicherten Inhalte und Umstände der Telekommunikation, soweit dieser eigene Schutzvorkehrungen gegen den heimlichen Datenzugriff treffen kann“[613] erstreckt. Denn in diesen Fällen „bestehen hinsichtlich solcher Daten die spezifischen Gefahren der räumlich distanzierten Kommunikation, die durch das Telekommunikationsgeheimnis abgewehrt werden sollen, nicht fort“[614].

Im Rahmen seiner Entscheidung über die Verfassungsmäßigkeit der verfahrensgegenständlichen Vorschriften des Verfassungsschutzgesetzes Nordrhein-Westfalen zur Online-Durchsuchung stellt das BVerfG – unter Beschreibung des charakteristischen Eingriffsumfangs von Maßnahmen der Online-Durchsuchung – für den Grundrechtsschutz des Art. 10 I GG ferner fest, dass

> „der durch das Telekommunikationsgeheimnis bewirkte Schutz […] ebenfalls nicht [besteht], wenn eine staatliche Stelle die Nutzung eines informationstechnischen Systems als solche überwacht oder die Speichermedien des Systems durchsucht“[615].

Hierzu führt das BVerfG weiter aus, dass

> „hinsichtlich der Erfassung der Inhalte oder Umstände außerhalb der laufenden Telekommunikation […] ein Eingriff in Art. 10I GG selbst dann nicht vor[liegt], wenn zur Übermittlung der erhobenen Daten an die auswertende Behörde eine Telekommunikationsverbindung genutzt wird, wie dies etwa bei einem Online-Zugriff auf gespeicherte Daten der Fall ist“[616].

In Bezug auf die daraus zu ziehenden Konsequenzen für den effektiven Grundrechtsschutz konstatiert das BVerfG, dass

> „soweit der heimliche Zugriff auf ein informationstechnisches System dazu dient, Daten auch insoweit zu erheben, als Art. 10I GG nicht vor einem Zugriff schützt, […] eine Schutzlücke [bleibt], die durch das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Schutz der Vertraulichkeit und Integrität von informationstechnischen Systemen zu schließen ist“[617].

2. Aussagen zur Quellen-TKÜ

Im Rahmen seiner Entscheidung vom 27.02.2008 trifft das BVerfG anlässlich der Auslotung der grundrechtlichen Schutzbereiche im Zusammenhang mit dem neuen IT-Grundrecht sowie der Abgrenzung der auf unterschiedliche Überwachungsgegenstände ausgerichteten Maßnahmen der On-

---

613 BVerfG NJW 2008, 822 (825); vgl. bereits BVerfG NJW 2006, 976 (978).
614 BVerfG NJW 2008, 822 (825); vgl. bereits BVerfG NJW 2006, 976 (978).
615 BVerfG NJW 2008, 822 (825).
616 BVerfG NJW 2008, 822 (825).
617 BVerfG NJW 2008, 822 (825).

line-Durchsuchung und Quellen-TKÜ auch spezifische Aussagen zur *Quellen-Telekommunikationsüberwachung*, welche maßgebend Auswirkung auf die Frage der grundrechtlichen Beurteilung und Einordnung dieses Ermittlungsinstruments in den bestehenden Kanon heimlicher präventiv-polizeilicher wie auch strafprozessualer Ermittlungsmaßnahmen hat.

In diesem Zusammenhang stellt das BVerfG zunächst fest, dass in den Fällen, in denen

> „[…] ein komplexes informationstechnisches System zum Zwecke der Telekommunikationsüberwachung technisch infiltriert [wird] (‚Quellen-Telekommunikationsüberwachung'), […] mit der Infiltration die entscheidende Hürde genommen [ist], um das System insgesamt auszuspähen"[618].

Als Begründung führt das BVerfG hierzu aus, dass

> „die dadurch bedingte Gefährdung […] weit über die hinaus[geht], die mit einer bloßen Überwachung der laufenden Telekommunikation verbunden ist. Insbesondere können auch die auf dem Personalcomputer abgelegten Daten zur Kenntnis genommen werden, die keinen Bezug zu einer telekommunikativen Nutzung des Systems aufweisen"[619].

Weiter führt das BVerfG aus, dass

> „es im Übrigen dazu kommen [kann], dass im Anschluss an die Infiltration Daten ohne Bezug zur laufenden Telekommunikation erhoben werden, auch wenn dies nicht beabsichtigt ist. In der Folge besteht für den Betroffenen – anders als in der Regel bei der herkömmlichen netzbasierten Telekommunikation – stets das Risiko, dass über die Inhalte und Umstände der Telekommunikation hinaus weitere persönlichkeitsrelevante Informationen erhoben werden. Den dadurch bewirkten spezifischen Gefährdungen der Persönlichkeit kann durch Art. 10I GG nicht oder nicht hinreichend begegnet werden"[620].

Diese Feststellung wird vom BVerfG jedoch – was die markante Besonderheit des vorliegenden Urteils darstellt[621] und indes Spielraum für unterschiedliche Interpretationen in Bezug auf die Frage der Zulässigkeit von (strafprozessualen) Quellen-TKÜ-Maßnahmen lässt – zugleich wiederum dahingehend eingeschränkt, dass

> „Art. 10I GG […] hingegen der alleinige grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zu einer ‚Quellen-Telekommunikationsüberwachung' [ist], wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt"[622].

---

618 BVerfG NJW 2008, 822 (825).

619 BVerfG NJW 2008, 822 (825).

620 BVerfG NJW 2008, 822 (825 f.).

621 *Klesczewski*, ZStW 2011, 737 (744) spricht diesbezüglich von einer „Aufsehen erregende[n] Einschränkung" (744).

622 BVerfG NJW 2008, 822 (826).

Für die alleinige Anwendung des Grundrechtsmaßstabs des Fernmeldegeheimnisses, an dem eine einfachgesetzliche Ermächtigungsnorm zu einer Quellen-TKÜ – also gemäß dem Begriffsverständnis des BVerfG zu einer Maßnahme bei der „ein komplexes informationstechnisches System zum Zwecke der Telekommunikationsüberwachung technisch infiltriert [wird] (‚Quellen-Telekommunikationsüberwachung')"[623] – demnach zu messen wäre, muss die vorausgesetzte notwendige Beschränkung der Überwachung ausschließlich auf Daten aus laufenden Telekommunikationsvorgängen gemäß der weiteren Feststellung des BVerfG allerdings

„durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein"[624].

In solchen Fällen stellt – so der Ansatz des BVerfG – Art. 10 I GG demnach den alleinigen Grundrechtsmaßstab für eine Ermächtigung zu einer Quellen-TKÜ dar, d. h. sowohl für das primäre Überwachen und Aufzeichnen als auch für das begleitende Einbringen (wie auch nachbereitende Entfernen) des hierfür erforderlichen technischen Mittels in Gestalt der Überwachungssoftware.

Anders als dies vor dem grundsätzlichen Urteil des BVerfG teilweise angenommen wurde[625], stellt die heimliche Infiltration eines in einer Wohnung oder sonstigen nach Art. 13 I GG geschützten Räumlichkeit befindlichen informationstechnischen Systems, im Falle der Quellen-TKÜ mit einer Überwachungssoftware zum Zwecke der Telekommunikationsüberwachung, auch keinen Eingriff in das Grundrecht aus Art. 13 I GG dar. Gemäß den nunmehr klarstellend erfolgten Feststellungen des BVerfG vermittelt

„Art. 13I GG […] dem Einzelnen […] keinen generellen, von den Zugriffsmodalitäten unabhängigen Schutz gegen die Infiltration seines informationstechnischen Systems, auch wenn sich dieses System in einer Wohnung befindet […]"[626].

Das BVerfG stützt sich diesbezüglich auf den Umstand, dass

„der Eingriff […] unabhängig vom Standort erfolgen [kann], so dass ein raumbezogener Schutz nicht in der Lage ist, die spezifische Gefährdung des informationstechnischen Systems abzuwehren. Soweit die Infiltration die Verbindung des betroffenen Rechners zu einem Rechnernetzwerk ausnutzt, lässt sie die durch die Abgrenzung der Wohnung vermittelte räumliche Privatsphäre unberührt."[627]

---

623 BVerfG NJW 2008, 822 (825).

624 BVerfG NJW 2008, 822 (826).

625 So bspw. LG Hamburg, MMR 2008, 423 (424); zum Diskussionsstand vor der Entscheidung des BVerfG vom 27.02.2008 (NJW 2008, 822), vgl. auch Anm. *Vogel/Brodowski*, StV 2009, 632 (633).

626 BVerfG NJW 2008, 822 (826).

627 BVerfG NJW 2008, 822 (826); anders stellt es sich nach Auffassung des BVerfG allerdings für die Fälle dar, bei denen das Einbringen der Überwachungssoftware durch physische Einwirkung auf das Gerät unter Eindringen in eine Woh-

Weiter führt das BVerfG hierzu aus, dass

„der Standort des Systems […] in vielen Fällen für die Ermittlungsmaßnahme ohne Belang und oftmals für die Behörde nicht einmal erkennbar sein [wird]. Dies gilt insbesondere für mobile informationstechnische Systeme wie etwa Laptops, Personal Digital Assistants (PDAs) oder Mobiltelefone."[628]

nung erfolgt: So „kann eine Maßnahme, die mit dem heimlichen technischen Zugriff auf ein informationstechnisches System im Zusammenhang steht, an Art. 13I GG zu messen sein, […] beispielsweise, wenn und soweit Mitarbeiter der Ermittlungsbehörde in eine als Wohnung geschützte Räumlichkeit eindringen, um ein dort befindliches informationstechnisches System physisch zu manipulieren" (826); eine solche Vorgehensweise zum heimlichen Einbringen der Telekommunikationsüberwachungssoftware ist mangels entsprechenden Betretungsrechts gegenwärtig unzulässig, vgl. hierzu 2. Teil B.I.2.b); für Einzelheiten zu Einbringungsmöglichkeiten der Software, siehe 1. Teil A.II.4.b).

628 BVerfG NJW 2008, 822 (826).

2. Teil

Dogmatische Analyse

A. Primärmaßnahme: Überwachung und Aufzeichnung

I. Gesetzliche Rechtsgrundlagen der Quellen-TKÜ

Ob und inwieweit das Ermittlungsinstrument der Quellen-TKÜ im Bereich des Strafprozessrechts durch die bestehende Gesetzeslage rechtlich legitimiert ist oder aber einen unzulässigen Eingriff in die Grundrechte der Betroffenen darstellt, ist heftigst umstritten. Sowohl Gesetzgebung, Rechtsprechung als auch Literatur sind in dieser Frage uneinig und verfolgen unterschiedliche Ansätze.

1. Rechtsgrundlagen außerhalb der Strafprozessordnung

In der überwiegenden Zahl der Fälle in der Praxis erfolgen Maßnahmen der Quellen-TKÜ zu repressiven Zwecken.[1] Dies ist vor allem auch dadurch bedingt, dass eine Quellen-TKÜ-Maßnahme – zumindest bei erstmaliger Durchführung auf dem jeweiligen Zielsystem – i. d. R. eine gewisse Vorlaufzeit zur Vorbereitung[2] der Maßnahme benötigt und daher zur Abwehr einer akuten Gefahr zunächst nur bedingt geeignet erscheint.

Dennoch gibt es Fallkonstellationen, in denen die Quellen-TKÜ das Mittel der Wahl ist, um eine *konkrete* (§ 31 III POG RP[3]), *dringende* (§ 20l BKAG) oder auch erst *gegenwärtige* Gefahr (insoweit strenger § 15b HSOG) abzuwehren. Die Durchführung einer Quellen-TKÜ zu präventiven Zwecken bietet sich insbesondere dann an, wenn die Überwachungssoftware bereits aus einer vorherigen Überwachung installiert ist und noch nicht entfernt wurde, wodurch die zeitintensive Ermittlung der Systemparameter sowie der Einbringungsmöglichkeiten entfällt. Daneben kann eine präventive Quellen-TKÜ auch in Fällen relevant werden, in denen eine Dauergefahr

---

[1] *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11. 2010, ohne Berücksichtigung präventiver Quellen-TKÜs nach §§ 23a ff. ZFdG.

[2] Siehe hierzu 1. Teil A.II.4.a)aa).

[3] Vgl. hierzu auch LT RP-Drs. 15/4879, S. 32; so auch die vom BVerfG geforderten Mindestanforderungen, vgl. BVerfG NJW 2008, 822 (831).

vorliegt und die Maßnahme zur Verhinderung weiterer Gefahren beiträgt. Die Maßnahme kann aber auch bei akut auftretenden Gefahrenlagen zur Gefahrenabwehr in Betracht kommen, wenn bspw. die Vorfeldermittlungen dann mit entsprechend höherem Ressourceneinsatz beschleunigt betrieben werden.[4]

Außerhalb der Strafprozessordnung wurde die Quellen-TKÜ in eine Reihe von präventiv-polizeilichen Gesetzen auf Bundes- und Länderebene in ausdrücklicher Weise geregelt. Die Eingliederung dieser Maßnahme in den jeweils bestehenden Kanon präventiver Eingriffsbefugnisse erfolgt hierbei auf unterschiedliche Art und Weise. Zum Teil wird die Quellen-TKÜ als Maßnahme der Gefahrenabwehr in Form eines zusätzlichen Absatzes innerhalb einer bestehenden Befugnisnorm zur Telekommunikationsüberwachung eingefügt (z. B. § 20l II BKAG; § 34a II S. 2 ThürPAG; § 31 III POG Rheinland-Pfalz), zum Teil in Form einer neu geschaffenen Befugnisnorm eigenständig geregelt (z. B. § 15b Hessisches SOG). Teilweise wird die Quellen-TKÜ aber auch unter den Tatbestand bestehender Befugnisnormen zur Telekommunikationsüberwachung subsumiert, ohne ausdrücklich in deren Tatbestand geregelt zu sein (so z. B. eine weit verbreitete Ansicht zu Art. 34a ff. BayPAG[5] und §§ 23a ff. ZFdG). Aus dem letztgenannten Grund ist nachfolgende Auflistung in der Praxis als Rechtsgrundlagen für (präventiv-polizeiliche) Maßnahmen der Quellen-TKÜ heranziehbarer Befugnisnormen auch nicht als abschließend anzusehen:

a) § 20l II BKAG

Auf Bundesebene besteht seit 01.01.2009 für das Bundeskriminalamt in § 20l II BKAG[6] eine Befugnisnorm zur Durchführung präventiver Quellen-TKÜs bei Vorliegen der Voraussetzungen des § 20l I BKAG für einen

---

[4] Vgl. Bundesministerium des Innern, Fragenkatalog BMJ, S. 17, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012) zur präventiven Online-Durchsuchung, gilt für die Quellen-TKÜ insoweit entsprechend.

[5] So *Berner*/*Köhler*/*Käß*, BayPAG, Art. 34a, Rn. 3, 8, 21 u. Art. 34d, Rn. 3; *Käß*, BayVBl. 2010, 1 (5 f.); auch *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11.2010; a. A. hingegen *Albrecht*/*Dienst*, JurPC Web-Dok. 5/2012, Abs. 36; a. A. auch der Bayerische Landesbeauftragte für den Datenschutz, 24. Tätigkeitsbericht, S. 79 f., abrufbar unter http://www.datenschutz-bayern.de/tbs/tb24/tb24.pdf (zuletzt aufgerufen 15.06.2012), wiederum unter Hinweis auf die von der Sichtweise des Landesbeauftragten abweichende Auffassung des Bayerischen Staatsministeriums des Innern; hierzu im Einzelnen 2. Teil A.I.1.e).

[6] § 20l Bundeskriminalamtgesetz, eingefügt m. W. v. 01.01.2009 durch das Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt vom 25.12.2008 (BGBl. I S. 3083).

Zugriff auf Telekommunikation. Die Durchführung der Überwachung und Aufzeichnung von Telekommunikation in der Weise des Eingriffs in informationstechnische Systeme mit technischen Mitteln ist hierbei als zusätzlicher Abs. 2 in die Vorschrift des § 20l BKAG zur *Überwachung der Telekommunikation* aufgenommen.

§ 20l BKAG
Überwachung der Telekommunikation

(1) Das Bundeskriminalamt kann ohne Wissen des Betroffenen die Telekommunikation einer Person überwachen und aufzeichnen,

1. die entsprechend § 17 oder § 18 des Bundespolizeigesetzes verantwortlich ist, und dies zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Staates oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse liegt, geboten ist,
2. bei der bestimmte Tatsachen die Annahme rechtfertigen, dass sie Straftaten gemäß § 4a Abs. 1 Satz 2 vorbereitet,
3. bei der bestimmte Tatsachen die Annahme rechtfertigen, dass sie für eine Person nach Nummer 1 bestimmte oder von dieser herrührende Mitteilungen entgegennimmt oder weitergibt, oder
4. bei der bestimmte Tatsachen die Annahme rechtfertigen, dass eine Person nach Nummer 1 deren Telekommunikationsanschluss oder Endgerät benutzen wird,

und die Abwehr der Gefahr oder Verhütung der Straftaten auf andere Weise aussichtslos oder wesentlich erschwert wäre. Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

(2) [1]Die Überwachung und Aufzeichnung der Telekommunikation darf ohne Wissen des Betroffenen in der Weise erfolgen, dass mit technischen Mitteln in vom Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn

1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird, und
2. der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen.

[2]§ 20k Abs. 2 und 3 gilt entsprechend. [3]§ 20k bleibt im Übrigen unberührt.

(3) [1]Maßnahmen nach den Absätzen 1 und 2 dürfen nur auf Antrag des Präsidenten des Bundeskriminalamtes oder seines Vertreters durch das Gericht angeordnet werden. (…)

(4) [1]Die Anordnung ergeht schriftlich. [2]In ihr sind anzugeben

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich, mit Name und Anschrift,

2. die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgeräts, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist,
3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes und
4. im Fall des Absatzes 2 auch eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll. (…)

§ 20k BKAG
(Abs. 2 und 3 gilt entsprechend)

(…)

(2) [1]Es ist technisch sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und
2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden.

[2]Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. [3]Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(3) [1]Bei jedem Einsatz des technischen Mittels sind zu protokollieren

1. die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,
2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,
3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und
4. die Organisationseinheit, die die Maßnahme durchführt.

[2]Die Protokolldaten dürfen nur verwendet werden, um dem Betroffenen oder einer dazu befugten öffentlichen Stelle die Prüfung zu ermöglichen, ob die Maßnahme nach Absatz 1 rechtmäßig durchgeführt worden ist. [3]Sie sind bis zum Ablauf des auf die Speicherung folgenden Kalenderjahres aufzubewahren und sodann automatisiert zu löschen, es sei denn, dass sie für den in Satz 2 genannten Zweck noch erforderlich sind.

(…)

b) §§ 34a II S. 2, 34b ThürPAG

Unter dem Eindruck der Entscheidung des BVerfG zur präventiven Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalen vom 27.02.2008 wurde die bereits im Jahr 2007 eingebrachte und schon in der

parlamentarischen Beratung befindliche Novellierung des ThürPAG im Juni 2008 in weiten Teilen nochmals neu formuliert. Insbesondere wurde § 34a ThürPAG[7] grundlegend überarbeitet und in Abs. 2 S. 2, 3 um eine ausdrückliche Befugnis zur Quellen-TKÜ erweitert.[8]

§ 34a ThürPAG
Überwachung der Telekommunikation,
Datenerhebung von Mobilfunkkarten und -endgeräten
und sonstige Eingriffe

(…)

(2) (…). [2]Ferner kann die Polizei die laufenden Telekommunikationsinhalte in der Weise überwachen und aufzeichnen, dass mit informationstechnischen Programmen in vom Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn

1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich eine laufende Telekommunikation überwacht und aufgezeichnet wird, und
2. der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation in unverschlüsselter Form zu ermöglichen.

[3]Im Übrigen ist ein Zugriff auf Dateien sowie alle anderen auf dem informationstechnischen System integrierten technischen Systemkomponenten unzulässig.

(…)

(5) [1]Eine Maßnahme nach Absatz 1 bis 4 darf nur auf Antrag des Leiters der Polizeibehörde oder bei Verhinderung seines Stellvertreters durch den Richter angeordnet werden. (…)

(6) [1]Der Antrag ergeht schriftlich. [2]Er enthält

1. soweit bekannt, den Namen und die Anschrift des Betroffenen, gegen den sich die Maßnahme richtet,
2. bei einer Überwachung oder Datenerhebung der Telekommunikation zusätzlich
   a) die Rufnummer oder
   b) eine andere Kennung des Telekommunikationsanschlusses oder die Kennung des Endgerätes, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist, oder

---

[7] § 34a Thüringer Gesetz über die Aufgaben und Befugnisse der Polizei, neu gefasst m. W. v. 30.07.2008 durch Gesetz vom 16.07.2008 (GVBl. S. 245).

[8] Vgl. hierzu auch Thüringer Landesbeauftragter für den Datenschutz, 8. Tätigkeitsbericht, S. 67, abrufbar unter http://www.thueringen.de/imperia/md/content/datenschutz/taetigkeitsberichte/microsoft_word_-_tlfd08-_endfassung_stand_07.06.2010_f__r_internet.pdf (zuletzt aufgerufen 15.06.2012).

c) auch die Bezeichnung des informationstechnischen Systems,

3. die Art, den Umfang und die Dauer der Maßnahme unter Benennung des Endzeitpunktes und

4. die wesentlichen Gründe.

(…)

§ 34b ThürPAG
Umgangsverbot mit personenbezogenen Daten
aus der Telekommunikationsüberwachung, Mitwirkungspflichten
der Diensteanbieter, Unterrichtung des Landtags

(…)

(5) [1]Bei einer Maßnahme nach § 34a Abs. 2 Satz 2 ist technisch sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Erfassung und Ausleitung von Sprachsignalen am Audiosystem unerlässlich sind, und

2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.

[2]Das eingesetzte Programm ist nach dem Stand der Wissenschaft und Technik gegen unbefugte Nutzung zu schützen. [3]Die überwachte und aufgezeichnete Telekommunikation ist nach dem Stand der Wissenschaft und Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(6) [1]Bei einer Maßnahme nach § 34a Abs. 2 sind zum Zwecke der Datenschutzkontrolle und der Beweissicherung entsprechend des Einsatzmittels

1. die Bezeichnung der technischen Erfassungsanlage, Ort und der Zeitpunkt des Einsatzes,

2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,

3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und

4. die Organisationseinheit, die die Maßnahme durchführt, zu protokollieren.

[2]Die Protokolldaten dürfen nur verwendet werden, um dem Betroffenen oder einer dazu befugten öffentlichen Stelle die Prüfung zu ermöglichen, ob die Maßnahme nach § 34a Abs. 2 rechtmäßig durchgeführt worden ist. [3]Sie sind bis zum Ablauf des auf die Speicherung folgenden Kalenderjahres aufzubewahren und sodann zu löschen, es sei denn, dass sie für den in Satz 2 genannten Zweck erforderlich sind.

(…)

c) § 31 III POG RP

Mit dem Ziel ein modernes und effizientes Polizei- und Ordnungsbehördengesetz zu schaffen, welches die aktuellen technischen Entwicklungen berücksichtigt, hat der Landtag Rheinland Pfalz am 26.01.2011 eine entsprechende Novelle des Polizei- und Ordnungsbehördengesetzes Rheinland-Pfalz beschlossen. Die Gesetzesnovelle enthält in § 31 III POG RP[9] auch eine ausdrückliche präventive Befugnisnorm zur Durchführung von Quellen-TKÜs. Die Regelung der Quellen-TKÜ erfolgt als zusätzlicher Absatz in den Vorschriften des § 31 POG RP über die *Datenerhebung durch den Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation, Auskunft über die Telekommunikation*.

§ 31 POG RP
Datenerhebung durch den Einsatz technischer Mittel
zur Überwachung und Aufzeichnung der Telekommunikation,
Auskunft über die Telekommunikation

(…)

(3) [1]Zur Abwehr einer Gefahr für Leib oder Leben einer Person oder für solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt, darf die Überwachung und Aufzeichnung der Telekommunikation ohne Wissen des Betroffenen in der Weise erfolgen, dass mit technischen Mitteln in vom Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn

1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird, und
2. der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen.

[2]§ 31 c Abs. 2 und 4 gilt entsprechend. [3]Im Übrigen bleibt § 31 c unberührt.

(4) Die Datenerhebung bedarf der richterlichen Entscheidung. In der schriftlichen Anordnung sind insbesondere

1. Voraussetzungen und wesentliche Abwägungsgesichtspunkte,
2. die Person, gegen die sich die Datenerhebung richtet, soweit möglich mit Name und Anschrift,
3. Art, Umfang und Dauer der Datenerhebung unter Benennung des Endzeitpunkts,

---

[9] Novelle des Polizei- und Ordnungsbehördengesetz Rheinland-Pfalz, beschlossen vom Landtag Rheinland-Pfalz am 26.01.2011 (Drs. 15/4879), m. W. v. 15.02.2011 (GVBl. S. 26).

4. soweit möglich die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgeräts, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist, und
5. im Fall des Absatzes 3 möglichst genau das informationstechnische System, in das zur Datenerhebung eingegriffen werden soll, sowie das technische Mittel zu bestimmen. (…)

§ 31c POG RP
(Abs. 2 und 4 gilt entsprechend)

(…)

(2) [1]Es ist technisch sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und
2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.

[2]Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. [3]Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(…)

(4) [1]Bei jedem Einsatz des technischen Mittels sind zu protokollieren:

1. die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,
2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,
3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und
4. die Organisationseinheit, die die Maßnahme durchführt.

[2]Die Protokolldaten dürfen nur verwendet werden, um dem Betroffenen oder einer dazu befugten öffentlichen Stelle die Prüfung zu ermöglichen, ob die Maßnahme nach Absatz 1 rechtmäßig durchgeführt worden ist. [3]Sie sind unverzüglich zu löschen, soweit sie für den in Satz 2 genannten Zweck nicht mehr erforderlich sind.

(…)

d) § 15b HSOG

Mit § 15b HSOG[10] wurde mit dessen Inkrafttreten zum 01.01.2010 eine eigenständige Befugnisnorm in das Hessische Gesetz über die öffentliche Sicherheit und Ordnung eingefügt. Diese erlaubt den Gefahrenabwehr- und Polizeibehörden (§ 1 HSOG) *Telekommunikationsüberwachung an informationstechnischen Systemen*.

§ 15b HSOG
Telekommunikationsüberwachung an informationstechnischen Systemen

(1) Wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person unerlässlich ist, kann die Überwachung und Aufzeichnung der Telekommunikation ohne Wissen der betroffenen Person in der Weise erfolgen, dass mit technischen Mitteln in von der betroffenen Person genutzte informationstechnische Systeme eingegriffen wird, wenn

1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird, und
2. der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen.

(2) [1]Es ist technisch sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und
2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden.

[2]Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen.

(3) [1]Bei jedem Einsatz des technischen Mittels sind zum Zwecke der Datenschutzkontrolle und der Beweissicherung zu protokollieren:

1. die Bezeichnung des technischen Mittels und der Zeitraum seines Einsatzes,
2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,
3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und
4. die Organisationseinheit, die die Maßnahme durchführt.

[2]Die Protokolldaten dürfen nur verwendet werden, um der betroffenen Person oder einer hierzu befugten öffentlichen Stelle oder einem Gericht die Prüfung zu ermöglichen, ob die Maßnahme nach Abs. 1 rechtmäßig durchgeführt

---

[10] § 15b Hessisches Gesetz über die öffentliche Sicherheit und Ordnung, eingefügt m. W. v. 23.12.2009 durch Gesetz vom 14.12.2009 (GVBl. I S. 635).

worden ist. [3]Sie sind bis zum Ablauf des auf die Speicherung folgenden Kalenderjahres aufzubewahren und sodann automatisiert zu löschen, wenn sie für den in Satz 2 genannten Zweck nicht mehr erforderlich sind.

(4) Die Maßnahme darf sich nur gegen eine Person richten, die nach den §§ 6 oder 7 verantwortlich ist. Sie darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

(5) § 15 Abs. 4 Satz 2 bis 5 und Abs. 5 gilt entsprechend mit der Maßgabe, dass das informationstechnische System, in das zur Datenerhebung eingegriffen werden soll, in der Anordnung möglichst genau zu bezeichnen ist.

§ 15 HSOG
(Abs. 4 Satz 2 bis 5 und Abs. 5 gilt entsprechend)

(…)

(4) (…) [2]Ein Eingriff mit technischen Mitteln ist nicht zulässig, soweit keine Auskunftspflicht der betroffenen Person nach § 12 Abs. 2 besteht. [3]Das Verbot nach Satz 2 gilt auch, wenn durch eine gegen einen Dritten gerichtete Maßnahme Erkenntnisse erlangt würden, die nicht der Auskunftspflicht nach § 12 Abs. 2 unterliegen. [4]Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch die Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. [5]Bestehen insoweit Zweifel, darf die Datenerhebung ausschließlich durch eine automatische Aufzeichnung erfolgen und fortgesetzt werden. (…)

(5) [1]Maßnahmen nach Abs. 4 sowie das Abhören oder Aufzeichnen des nicht öffentlich gesprochenen Wortes durch den Einsatz technischer Mittel dürfen außer bei Gefahr im Verzug nur durch richterliche Anordnung getroffen werden. [2]Für das Verfahren gilt § 39 Abs. 1 mit der Maßgabe, dass, soweit es sich nicht um Maßnahmen nach Abs. 4 handelt, das Amtsgericht zuständig ist, in dessen Bezirk die Polizeibehörde ihren Sitz hat. [3]Die Anordnung ergeht schriftlich. [4]Sie muss die Personen, gegen die sich die Maßnahmen richten sollen, so genau bezeichnen, wie dies nach den zur Zeit der Anordnung vorhandenen Erkenntnissen möglich ist. [5]Art und Dauer der Maßnahmen sind festzulegen. [6]Die Anordnung ist auf höchstens drei Monate zu befristen und, soweit möglich, räumlich zu begrenzen. [7]Eine dreimalige Verlängerung um jeweils höchstens drei weitere Monate ist zulässig, soweit die Voraussetzungen fortbestehen. [8]Hat die Polizeibehörde bei Gefahr im Verzug die Anordnung getroffen, so beantragt sie unverzüglich die richterliche Bestätigung der Anordnung. [9]Die Anordnung tritt außer Kraft, wenn sie nicht bis zum Ablauf des folgenden Tages richterlich bestätigt wird. [10]Automatische Aufzeichnungen nach Abs. 4 Satz 5 sind unverzüglich dem anordnenden Gericht zur Entscheidung über die Verwertbarkeit oder Löschung der Daten vorzulegen. [11]Für die nicht verwertbaren Teile ordnet das Gericht die unverzügliche Löschung an. [12]Das Gericht unterrichtet die Polizeibehörde unverzüglich über den Inhalt der verwertbaren Teile der Aufzeichnung.

(…)

e) Art. 34a I BayPAG?

Die überwiegende Zahl der Polizei- und Sicherheitsgesetze der Länder enthält keine ausdrückliche Regelung der Quellen-TKÜ. Oftmals ist nur die präventive *Überwachung und Aufzeichnung der Telekommunikation* gesetzlich geregelt[11]. Unter diese Befugnisnormen werden in der Praxis mitunter auch präventive Quellen-TKÜ-Maßnahmen subsumiert.

Dies sei am Beispiel der Regelungen im Bayerischen Polizeiaufgabengesetzes näher verdeutlicht. Eine ausdrückliche Regelung der präventiven Quellen-TKÜ enthält das BayPAG zwar nicht. Die spezielle Ermittlungsmaßnahme lasse sich jedoch nach Auffassung zuständiger Behörden wie auch gewichtiger Stimmen aus der Literatur[12] auf die bestehenden Befugnisnormen zur Telekommunikationsüberwachung nach Art. 34a I BayPAG i. V. m. den Regelungen des Art. 34c BayPAG[13] (*Datenerhebung und Eingriffe in den Telekommunikationsbereich*) stützen.

Art. 34a BayPAG
Datenerhebung und Eingriffe in den Telekommunikationsbereich

(1) [1]Die Polizei kann durch die Überwachung und Aufzeichnung der Telekommunikation personenbezogene Daten erheben

1. über die für eine Gefahr Verantwortlichen, soweit dies zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder für Sachen, soweit eine gemeine Gefahr besteht, erforderlich ist, oder

2. über Personen, soweit bestimmte Tatsachen die begründete Annahme rechtfertigen, dass

---

[11] Z. B. in Bayern: Art. 34a BayPAG; im Saarland: § 28b SPolG; in Niedersachsen: § 33a Nds.SOG (i. d. F. vom 01.01.2008).

[12] So *Berner*/*Köhler*/*Käß,* BayPAG, Art. 34a, Rn. 3, 8, 21 u. Art. 34d, Rn. 3; *Käß*, BayVBl. 2010, 1 (5 f.) m. w. N.; auch *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11.2010; a. A. hingegen *Albrecht*/*Dienst*, JurPC Web-Dok. 5/2012, Abs. 36; a. A. auch der Bayerische Landesbeauftragte für den Datenschutz, 24. Tätigkeitsbericht, S. 79 f., abrufbar unter http://www.datenschutz-bayern.de/tbs/tb24/tb24.pdf (zuletzt aufgerufen 15.06.2012), wiederum unter Hinweis auf die von der Sichtweise des Landesbeauftragten abweichende Auffassung des Bayerischen Staatsministeriums des Innern, welches in Art. 34a BayPAG eine ausreichende Rechtsgrundlage auch für die Quellen-TKÜ sehe.

[13] Art. 34a Bayerisches Polizeiaufgabengesetz, eingefügt m. W. v. 01.01.2006 durch Gesetz vom 24.12.2005 (GVBl. S. 641); Abs. 1 S. 3 geändert, S. 4 neu eingefügt m. W. v. 01.08.2008 durch Gesetz vom 08.07.2008 (GVBl. S. 365); Abs. 1 S. 1 Nr. 2 aufgehoben, bish. Nr. 3 wird Nr. 2 und lit. a) und b) geändert m. W. v. 01.08.2009 durch Gesetz vom 27.07.2009 (GVBl. S. 380).

a) sie für Personen nach Nr. 1 bestimmte oder von diesen herrührende Mitteilungen entgegennehmen, ohne insoweit das Recht zur Verweigerung des Zeugnisses nach §§ 53, 53a StPO zu haben, oder weitergeben oder

b) die unter Nr. 1 genannten Personen ihre Kommunikationseinrichtungen benutzen werden.

[2]Datenerhebungen nach Satz 1 dürfen nur durchgeführt werden, wenn die Erfüllung einer polizeilichen Aufgabe auf andere Weise aussichtslos oder wesentlich erschwert wäre. [3]Wird erkennbar, dass in ein durch ein Berufsgeheimnis geschütztes Vertrauensverhältnis im Sinn der §§ 53, 53a StPO eingegriffen wird, ist die Datenerhebung insoweit unzulässig, es sei denn, die Maßnahme richtet sich gegen den Berufsgeheimnisträger selbst. [4]Wird erkennbar, dass dem Kernbereich privater Lebensgestaltung zuzurechnende Daten betroffen sind und bestehen keine Anhaltspunkte dafür, dass diese Daten dem Zweck der Herbeiführung eines Erhebungsverbots dienen sollen, ist die Datenerhebung insoweit unzulässig.

(…)

Art. 34c BayPAG
Verfahrensregelungen, Verwendungsverbote, Zweckbindung, Benachrichtigung und Löschung

(1) Für Maßnahmen nach Art. 34a und Art. 34b gilt Art. 34 Abs. 4 Sätze 1 und 2 entsprechend; bei Gefahr im Verzug sind die in Art. 33 Abs. 5 Sätze 1 und 2 genannten Stellen anordnungsbefugt.

(…)

Art. 34 BayPAG
(Abs. 4 Sätze 1 und 2 gilt entsprechend)

(…)

(4) [1]Eine Maßnahme nach Abs. 1 Satz 1 darf nur durch den Richter angeordnet werden, bei Gefahr im Verzug auch durch die in Art. 33 Abs. 5 Satz 1 genannten Dienststellenleiter; in diesem Fall ist unverzüglich eine Bestätigung der Maßnahme durch einen Richter einzuholen. [2]Für die richterliche Anordnung ist Art. 24 Abs. 1 Satz 3 entsprechend anzuwenden; zuständig ist das Amtsgericht, in dessen Bezirk die beantragende Polizeidienststelle ihren Sitz hat. (…)

f) § 23a I ZFdG?

Auch auf Bundesebene spielt das Thema der präventiven Quellen-TKÜ – neben entsprechenden Maßnahmen des BKA auf Grundlage des § 20l II BKAG – eine nicht minder relevante Rolle. Wie das Bundesministerium der Finanzen in einem Antwortschreiben auf die Anfrage der FDP-Bundtagsabgeordneten *Piltz* eingeräumt habe, zähle die Quellen-TKÜ zum gängigen

Maßnahmerepertoire des Zollkriminalamtes für den heimlichen Zugriff auf Internettelefonie im Rahmen der Verhütung zollfahndungsrelevanter Straftaten.[14] Nach Auffassung der Zollbehörden lasse sich eine solche Maßnahme auf die Regelungen zur präventive Telekommunikationsüberwachung nach §§ 23a I, 23b ZFdG[15] stützen.[16] Besteht der Verdacht der Vorbereitung einer der in § 23a I S. 1 ZFdG aufgeführten Straftaten, könne daher mit entsprechender richterlicher Anordnung verschlüsselte Internettelefonie mittels heimlich installierter Software überwacht werden.

§ 23a ZFdG
Beschränkung des Brief-, Post- und Fernmeldegeheimnisses

(1) [1]Rechtfertigen Tatsachen die Annahme, dass Personen Straftaten nach § 19 Abs. 1 oder 2, § 20 Abs. 1, § 20a Abs. 1 oder 2 oder § 22a Abs. 1 Nr. 4, 5 und 7 oder Abs. 2 des Gesetzes über die Kontrolle von Kriegswaffen vorbereiten, ist das Zollkriminalamt befugt, zur Verhütung dieser Straftaten dem Brief- oder Postgeheimnis unterliegende Sendungen zu öffnen und einzusehen sowie die dem Fernmeldegeheimnis unterliegende Telekommunikation zu überwachen und aufzuzeichnen. [2]Die Überwachung und Aufzeichnung bedarf der vorherigen richterlichen Anordnung.

(2) Eine Vorbereitung von Straftaten im Sinne von Absatz 1 Satz 1 ist (…).

(…)

(4a) [1]Beschränkungen nach Absatz 1, 3 oder 4 sind unzulässig, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch sie allein Kommunikationsinhalte aus dem Kernbereich privater Lebensgestaltung erlangt würden. [2]Kommunikationsinhalte aus dem Kernbereich privater Lebensgestaltung, die durch eine Beschränkung nach Absatz 1, 3 oder 4 erlangt worden sind, dürfen nicht verwertet werden. [3]Sie sind unverzüglich unter Aufsicht eines Bediensteten, der die Befähigung zum Richteramt hat, zu löschen. [4]Die Tatsache der Erfassung der Daten und ihrer Löschung ist zu dokumentieren. [5]Diese Daten dürfen ausschließlich zu Zwecken der Datenschutzkontrolle verwendet werden. [6]Sie sind zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich sind, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentierung folgt.

(…)

---

[14] Vgl. http://www.spiegel.de/netzwelt/netzpolitik/0,1518,722221,00.html (zuletzt aufgerufen 15.06.2012); vgl. hierzu nunmehr auch die Antworten des Parl. Staatssekretärs beim Bundesminister der Finanzen, *Koschyk*, im Rahmen der 132. Sitzung des Deutschen Bundestages am 19.10.2011 (BT-PlPr. 17/132 15595 D ff.).

[15] § 23a Zollfahndungsdienstgesetz, zuletzt geändert m. W. v. 15.06.2007 durch Gesetz vom 12.06.2007 (BGBl. I S. 1037).

[16] *Pfister*, Abgeordnetenbüro Gisela *Piltz*, MdB, E-Mail vom 09.11.2010; vgl. hierzu nunmehr auch die Antworten des Parl. Staatssekretärs beim Bundesminister der Finanzen, *Koschyk*, im Rahmen der 132. Sitzung des Deutschen Bundestages am 19.10.2011 (BT-PlPr. 17/132 15595 D ff.).

(6) [1]Beschränkungen nach Absatz 1, 3 oder 4 dürfen nur angeordnet werden, wenn es ohne die Erkenntnisse aus den damit verbundenen Maßnahmen aussichtslos oder wesentlich erschwert wäre, die vorbereiteten Taten zu verhindern und die Maßnahmen nicht außer Verhältnis zur Schwere der zu verhindernden Tat stehen. [2]Die Maßnahmen dürfen auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

(…)

§ 23b ZFdG
Gerichtliche Anordnung

(1) [1]Die Anordnung nach § 23a Abs. 1, 3 oder 4 ergeht auf zu begründenden Antrag der Behördenleitung des Zollkriminalamts persönlich, bei deren Verhinderung von deren Stellvertretung, nach Zustimmung des Bundesministeriums der Finanzen durch das Landgericht. [2]Bei Gefahr im Verzug kann die Anordnung vom Bundesministerium der Finanzen getroffen werden; sie tritt außer Kraft, wenn sie nicht binnen drei Tagen vom Landgericht bestätigt wird. [3]Die gewonnenen Erkenntnisse dürfen nicht verwertet werden. [4]Damit im Zusammenhang stehende Unterlagen sind unverzüglich zu vernichten.

(2) [1]In der Begründung der Anordnung oder Verlängerung sind deren Voraussetzungen und die wesentlichen Abwägungsgesichtspunkte darzulegen. [2]Insbesondere sind einzelfallbezogen anzugeben

1. die Bezeichnung der zu verhindernden Tat;
2. die Tatsachen, die die Annahme rechtfertigen, dass die Tat vorbereitet wird;
3. die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme.

(…)

(4) [1]Die Anordnung ergeht schriftlich. [2]Sie enthält

1. soweit bekannt den Namen und die Anschrift des Betroffenen, gegen den sie sich richtet,
2. bei einer Überwachung der Telekommunikation zusätzlich die Rufnummer oder eine andere Kennung des Telekommunikationsanschlusses oder die Kennung des Endgerätes, wenn diese allein diesem Endgerät zuzuordnen ist,
3. die Bestimmung von Art, Umfang und Dauer der Maßnahmen.

(…)

2. Frage: strafprozessuale Rechtsgrundlage de lege lata?

Die Strafprozessordnung enthält gegenwärtig keine ausdrückliche gesetzliche Regelung der Quellen-TKÜ. Es ist deshalb rechtsdogmatisch heftig umstritten, ob es de lege lata für Primär- und Sekundärmaßnahmen einer Quellen-TKÜ ausreichende Rechtsgrundlagen in der StPO gibt.

Zur Grundsatzfrage der rechtlichen Zulässigkeit einer Quellen-TKÜ als Ermittlungsinstrument im Strafverfahren haben sich in Wissenschaft und Praxis im Wesentlichen zwei große Meinungsblöcke herausgebildet – einerseits die Stimmen, die eine Quellen-TKÜ auf Grund der bestehenden strafprozessualen Rechtslage generell für unzulässig halten[17] und andererseits diejenigen, die die bestehenden Regelungen der §§ 100a, 100b StPO für grds. ausreichend erachten[18], um eine derartige Ermittlungsmaßnahme durchführen zu können. Vereinzelt werden hierzu auch vermittelnde Ansichten[19] vertreten.

Die Diskussion über die Zulässigkeit der Quellen-TKÜ wird hierbei auf Grund ihrer (technischen) Nähe zur Online-Durchsuchung und angesichts des hohen (auch gesellschaftspolitischen) Stellenwertes der informatorischen Selbstbestimmung des Einzelnen, gerade auch im täglichen Umgang mit informationstechnischen Systemen, mitunter mit deutlichen Worten geführt[20] und von rechtdogmatischen sowie rechtspolitischen[21] „Grabenkämpfen" begleitet, welche nicht zuletzt durch die Veröffentlichung einer „Regierungs-Malware" durch den *Chaos Computer Club* im Oktober 2011 zusätzlich angeheizt wurden.

Eine höchstrichterliche Klärung der Frage fand bislang nicht statt. Auch die Entscheidung des BVerfG vom 27.02.2008 zur (präventiven) Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalen[22] hat zwar Art. 10 I GG als den alleinigen grundrechtlichen Maßstab für die Beurtei-

---

17 So z. B. *Sankol*, CR 2008, 13 (15 ff.); *Hoffmann-Riem*, JZ 2008, 1009 (1022); *Buermeyer*/*Bäcker*, HRRS 2009, 433 (440); *Becker*/*Meinicke*, StV 2011, 50 (52); *Braun*/*Roggenkamp*, K&R 2011, 681 (681); Anm. *Brodowski*, JR 2011, 533 (535); *Albrecht*/*Dienst*, JurPC Web-Dok. 5/2012, Abs. 42 ff.; SK – *Wolter*, StPO, § 100a, Rn. 27 ff.; bereits LG Hamburg, MMR 2008, 423 (424); auch noch AG Hamburg, CR 2010, 249 (249); a. A. mittlerweile LG Hamburg, MMR 2011, 693 (693).

18 So z. B. Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 7a; BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 107c; *Bär*, TK-Überwachung, § 100a StPO, Rn. 32 f. und Anm. *Bär*, MMR 2011, 691 (693).; AG Bayreuth, MMR 2010, 266 (266); LG Hamburg, MMR 2011, 693 (693); insoweit auch LG Landshut, MMR 2011, 690 (691).

19 So z. B. KK – *Nack*, StPO, § 100a, Rn. 27, der sich für eine Zulässigkeit der Quellen-TKÜ auf Grundlage des § 100a StPO „für die Übergangszeit" bis zu einer gesetzlichen Regelung ausspricht.

20 *Becker*/*Meinicke*, StV 2011, 50 (50) sprechen in diesem Zusammenhang bspw. gegenüber den befürwortenden Stimmen einer Zulässigkeit der Quellen-TKÜ auf Grundlage der bestehenden §§ 100a, 100b StPO von einem „an Selbstreferenzialität grenzende[n] Prozess" zur Entwicklung einer „h. M.", *Buermeyer*, http://ijure.org/wp/archives/756 (zuletzt aufgerufen 15.06.2012) gar von einer „Selbstermächtigung der Justiz".

21 Vgl. hierzu auch die einberufene *Aktuelle Stunde* im Bundestag, BT-PlPr. 17/135 15603 B ff.

22 BVerfG NJW 2008, 822.

lung einer Ermächtigung zu Quellen-TKÜ-Maßnahmen, welche auf die ausschließliche Überwachung von laufenden Telekommunikationsvorgängen beschränkt sind, festgelegt[23] und insoweit Klarheit im Bezug auf die tangierten Grundrechte geschaffen, hinsichtlich der Frage der (gegenwärtigen) Zulässigkeit einer repressiven Quellen-TKÜ und der Tauglichkeit der §§ 100a, 100b StPO als Rechtsgrundlage keine (direkte) Aussage getroffen.

Der Gesetzgeber sah bislang offensichtlich keine Veranlassung zur Änderung oder Ergänzung der StPO. Ob dieser Umstand nun für oder gegen die Zulässigkeit der Quellen-TKÜ auf Grundlage der bestehenden strafprozessualen Rechtslage spricht, sei an dieser Stelle dahingestellt. Ob jedoch auf Grund der Tatsache, dass der Bundesgesetzgeber das Ermittlungsinstrument der Quellen-TKÜ für den präventiven Befugniskatalog des BKA in § 20l II BKAG ausdrücklich geregelt hat und in der StPO bislang nicht, bereits ein systematisches Argument zu einem Ausscheiden der §§ 100a, 100b StPO als Rechtsgrundlage einer repressive Quellen-TKÜ zu führen habe[24], erscheint indes fraglich. Darüber, ob der Gesetzgeber hier die ausdrückliche Regelung für zwingend erforderlich erachtet hat, oder aber die Norm unter dem Eindruck der Entscheidung des BVerfG vom 27.02.2008 nur „besonders gut" ausgestalten wollte[25], lässt sich streiten. Von einer abschließenden gesetzgeberischen Klärung der Rechtsfrage hat der Bundesgesetzgeber jedenfalls bislang abgesehen.

Demzufolge hat auch noch keine der beiden Rechtsansichten den Streit „für sich" entscheiden können. Dennoch ist gegenwärtig in der Rechtsprechung und der (strafprozessualen) Literatur eine mehrheitliche Tendenz in Richtung der §§ 100a, 100b StPO als ausreichende Rechtsgrundlagen für die strafprozessuale Durchführung einer Quellen-TKÜ festzustellen. Nicht

---

23 Was durch rechtliche Vorgaben und technische Vorkehrungen sichergestellt sein muss, vgl. BVerfG NJW 2008, 822 (826); das BVerfG spricht hier von *rechtlichen* Vorgaben und nicht zwingend von *gesetzlichen* Vorgaben, weshalb entgegen teilw. vertretener Ansicht auch Vorgaben durch den Richter (§ 100b II S. 2 Nr. 3 StPO) in Betracht kommen; vgl. zutr. Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 7a; a. A. *Braun*, juris PR-ITR 3/2011 Anm. 3, auch *Buermeyer*, http://ijure.org/wp/archives/756 (zuletzt aufgerufen 15.06.2012).

24 So bspw. Anm. *Brodowski*, JR 2011, 533 (537) m. w. N.; auch *Klesczewski*, ZStW 2011, 737 (747).

25 Hierauf deutet bspw. auch die Kurzzusammenfassung des BKAG durch das Bundesministerium des Innern auf dessen Internetseite unter Punkt I.2.b. hin, wonach es sich bei der dortigen Regelung der Quellen-TKÜ in der Vorschrift zur TKÜ „in erster Linie um eine Klarstellung [handelt], weil „Maßnahmen zur Quellen-TKÜ schon bisher auf die geltenden TKÜ-Regelungen nach Landesrecht bzw. der StPO gestützt werden" (http://www.bmi.bund.de/SharedDocs/Standardartikel/DE/Themen/Sicherheit/Terrorismus/InfoErgaenzungBKAG_gesetz.html, zuletzt aufgerufen 15.06.2012).

zuletzt auch seit Umschwenken einiger bislang kritisch hierzu eingestellter Gerichte[26] hat diese Rechtsauffassung zusätzlichen Auftrieb erhalten. Ob hierbei wirklich bereits von einer „h. M." gesprochen werden kann, oder ob dies eher auf einem an „Selbstreferenzialität grenzende[n] Prozess"[27] beruht, kann dahinstehen. Der zu einem überwiegenden Teil von Rechtsprechung, Strafverfolgungspraxis sowie weiten Teilen des Schrifttums verfolgte Ansatz, dass die bestehenden Befugnisnormen der §§ 100a, 100b StPO die Durchführung von Quellen-TKÜ-Maßnahmen im Strafprozessrecht legitimieren, gilt es im Nachfolgenden eingehend dogmatisch zu untersuchen.

II. Rechtsgrundlage: §§ 100a, 100b StPO?

Die i. d. R. heimlich („auch ohne Wissen der Betroffenen") stattfindende[28] Überwachung und Aufzeichnung von Telekommunikation im Bereich der Strafverfolgung ist in den §§ 100a, 100b StPO[29] geregelt. Bei der im Jahre 1968 in die StPO eingefügten Befugnisnorm des § 100a StPO handelt es sich (insbesondere auch auf Grund des umfangreichen und von rechtspolitischen Erwägungen geprägten Straftatenkataloges) um eine der meistgeänderten Normen des Strafprozessrechts. Zuletzt wurde die Vorschrift zum 01.01.2008 grundlegenden novelliert. Hierbei haben auch die Verfahrensregelungen in § 100b StPO eine Überarbeitung erfahren.[30]

Anordnungen von Überwachungsmaßnahmen nach §§ 100a, 100b StPO haben – nicht zuletzt bedingt durch die rasante technische Entwicklung sowie die zunehmende „Technisierung" der Gesellschaft und deren Kommunikationsformen – in den vergangenen Jahren kontinuierlich zugenommen. So belief sich die Zahl der gerichtlich angeordneten Überwachungsmaßnah-

---

26 Vgl. LG Hamburg, MMR 2011, 693 (693); a. A. noch LG Hamburg, MMR 2008, 423 (424) sowie AG Hamburg, CR 2010, 249 (249).

27 *Becker*/*Meinicke*, StV 2011, 50 (50).

28 Wobei die gesetzliche Formulierung „auch ohne Wissen der Betroffenen" verdeutlicht, dass die Anordnung weder unzulässig noch überflüssig ist, wenn ein Betroffener die ohne sein Einverständnis vorgenommene Überwachungsmaßnahme bemerkt hat, vgl. *Bär*, TK-Überwachung, § 100a StPO, Rn. 14 sowie insoweit auch entspr. Meyer-Goßner – *Cierniak*, StPO, § 100f, Rn. 1.

29 § 100a StPO eingef. durch G. v. 13.08.1968 (BGBl I S. 949), neu gefasst m. W. v. 01.01.2008 durch G. v. 21.12.2007 (BGBl. I S. 3198); Abs. 2 Nr. 8 geändert m. W. v. 19.03.2008 durch G. v. 11.03.2008 (BGBl. I S. 306); Abs. 2 Nr. 1 lit. g) geändert m. W. v. 05.11.2008 durch G. v. 31.10.2008 (BGBl. I S. 2149); Abs. 2 Nr. 1 lit. a) geändert m. W. v. 04.08.2009 durch G. v. 30.07.2009 (BGBl. I S. 2437); § 100b StPO eingef. durch G. v. 13.08.1968 (BGBl I S. 949), neu gefasst m. W. v. 01.01.2008 durch G. v. 21.12.2007 (BGBl. I S. 3198).

30 Vgl. *Bär*, TK-Überwachung, § 100a StPO, Rn. 1.

men gemäß den jährlich nach § 100b V, VI StPO zu erstellenden Berichten[31] im Jahr 2010 auf 3.519 Überwachungsanordnungen bezüglich Festnetztelekommunikation, 16.510 bezüglich Mobilfunktelekommunikation und 997 bezüglich Internettelekommunikation[32].

Eine Überwachung und Aufzeichnung[33] von Telekommunikation darf nach § 100a I StPO (nur) dann durchgeführt werden, wenn *bestimmte Tatsachen den Verdacht*[34] *begründen*, dass jemand als Täter oder Teilnehmer eine der in § 100a II StPO abschließend bezeichneten *schweren Straftaten*[35] (sog. *Katalogstraftaten*) begangen hat, zu begehen versucht (soweit strafbar) oder durch eine Straftat vorbereitet hat (§ 100a I Nr. 1 StPO). Kumulativ hinzutreten muss, dass die Tat auch *im Einzelfall schwer wiegt* (§ 100a I Nr. 2 StPO) und dass die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten *auf andere Weise* als durch einen Eingriff in Telekommunikation *wesentlich erschwert oder aussichtslos* wäre (§ 100a I Nr. 3 StPO). Zum Schutz des Kernbereichs privater Lebensgestaltung dürfen gemäß § 100a IV S. 1 StPO zudem keine tat-

---

31 Vgl. jährliche Statistiken auf der Homepage des Bundesamtes für Justiz, abrufbar unter http://www.bundesjustizamt.de/nn_2037064/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung__node.html?__nnn=true (zuletzt aufgerufen 15.06.2012).

32 Vgl. http://www.bundesjustizamt.de/cln_115/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Uebersicht__TKUE__2010,templateId=raw,property=publicationFile.pdf/Uebersicht_TKUE_2010.pdf (zuletzt aufgerufen 15.06.2012), es handelt sich insoweit um absolute Zahlen, Mehrfachnennung einzelner Überwachungsanordnungen möglich; die ab dem Jahr 2008 in den Statistiken aufgeführte Anzahl der Überwachungsanordnungen in Bezug auf „Internettelekommunikation" (5.3) bezieht sich wohl nicht speziell auf die im Zusammenhang mit Quellen-TKÜ stehende Kommunikation, sondern wird jegliche Art von Kommunikation über das Internet (wie bspw. E-Mailing, Blogs, Internetforen, Chats etc.) erfassen.

33 Bei einem Zugriff auf Fern*sprech*verkehr muss beides – sowohl Überwachung als auch Aufzeichnung – für sich angeordnet werden, vgl. Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 8, § 100b, Rn. 4.

34 Es bedarf hierfür weder eines „dringenden Tatverdachts" i. S. d. § 112 I S. 1 StPO noch eines „hinreichenden Tatverdachts" i. S. d. § 203 StPO; „einfacher" Tatverdacht (Anfangsverdacht, §§ 152 II, 160 I StPO) ist ausreichend, soweit dieser auf bestimmten Tatsachen beruht; hierfür ist erforderlich, dass sich der Verdacht auf eine hinreichend sichere Tatsachenbasis stützt, durch schlüssiges Beweismaterial bereits ein gewisses Maß an Konkretisierung erreicht hat und nicht nur unerheblich ist, vgl. BGH NJW 1995, 1974 (1975); BGH NJW 2001, 2266 (2268); BVerfG NJW 2000, 55 (66); BVerfG NJW 2003, 1787 (1791); Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 9 m. w. N.; *Bär*, TK-Überwachung, § 100a StPO, Rn. 17 m. w. N.

35 Der Begriff der „schweren Straftat" nach § 100a I Nr. 1, II StPO nimmt insoweit eine Zwischenstellung zwischen dem Begriff der „besonders schweren Straftat" nach § 100c I Nr. 1, II StPO und dem Begriff der „Straftat von erheblicher Bedeutung" nach § 100g I S. 1 Nr. 1 StPO ein.

sächlichen Anhaltspunkte für die Annahme vorliegen, dass durch eine Maßnahme *allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung* erlangt würden.[36]

Die überwachbare Telekommunikation umfasst hierbei sowohl den Inhalt[37] als auch die näheren Umstände[38] des betroffenen Telekommunikationsvorgangs.[39]

§ 100a StPO
[Überwachung der Telekommunikation]

(1) Auch ohne Wissen der Betroffenen darf die Telekommunikation überwacht und aufgezeichnet werden, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete schwere Straftat begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht, oder durch eine Straftat vorbereitet hat,

2. die Tat auch im Einzelfall schwer wiegt und

---

[36] Mit Beschluss vom 12.10.2011, Az.: 2 BvR 236/08, 2 BvR 237/08, 2 BvR 422/08 hat das BVerfG unter Zurückweisung mehrerer Verfassungsbeschwerden gegen die zum 01.01.2008 in Kraft getretene umfassende Novellierung der strafprozessualen Telekommunikationsüberwachung (BGBl. I S. 3198) nunmehr höchstrichterlich festgestellt, dass sowohl die erfolgte Erweiterung des Straftatenkatalogs in § 100a II StPO den Verhältnismäßigkeitsgrundsatz wahre, die Eingriffsvoraussetzung des *Schwerwiegens der Tat auch im Einzelfall* in § 100a I Nr. 2 StPO dem Bestimmtheitsgebot genüge, das zweistufige Schutzkonzept in § 100a IV StPO den Kernbereich privater Lebensgestaltung ausreichend schütze, die Regelung zu den Benachrichtigungspflichten in § 101 IV bis VI StPO verfassungskonform ausgestaltet als auch die Privilegierung bestimmter zeugnisverweigerungsberechtigter Berufsgeheimnisträger in § 160a I StPO gerechtfertigt sei, vgl. hierzu auch die Zusammenfassungen bei beck-aktuell, becklink 1017596 (zuletzt aufgerufen 15.06.2012).

[37] Sog. *Inhaltsdaten*, Begriff indes gesetzlich nicht definiert; auch Hintergrundgeräusche und -gespräche während des Telefonats sind Teil der Telekommunikation und können damit zulässiger Gegenstand einer TKÜ sein, vgl. BGH NStZ 2008, 473 (474); BGH NStZ 2003, 668 (669); BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 92; Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 2; findet eine Überwachung des audiovisuellen Telekommunikationsinhalts statt, d. h. werden bei einer Überwachung von Video-Internettelefonie neben den Sprach-Signalen auch die Video-Signale der jeweiligen Kommunikation abgegriffen, so steht es der Zulässigkeit der Maßnahme unter entspr. Berücksichtigung der Rspr. zu Hintergrundgeräuschen nicht entgegen, wenn hierdurch auch Hintergrundbilder, also Abbildungen von Teilen der Räumlichkeiten, in denen die Video-Internettelefonie abläuft, mit erfasst werden, in diese Richtung auch LG Hamburg, MMR 2011, 693 (694); für Einzelheiten zu Video-Internettelefonie, siehe auch 1. Teil A.I.2.c), d) u. e) und 2. Teil A.II.4.

[38] Insbesondere *Verkehrsdaten* i. S. d § 96 I, § 113a TKG sowie § 7 I TKÜV.

[39] Vgl. Löwe-Rosenberg – *Schäfer*, StPO und GVG, Zweiter Band, § 100a StPO, Rn. 47.

3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

(2) Schwere Straftaten im Sinne des Absatzes 1 Nr. 1 sind: (…)

(3) Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, 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 benutzt.

(4) [1]Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach Absatz 1 allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. [2]Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach Absatz 1 erlangt wurden, dürfen nicht verwertet werden. [3]Aufzeichnungen hierüber sind unverzüglich zu löschen. [4]Die Tatsache ihrer Erlangung und Löschung ist aktenkundig zu machen.

Eine Maßnahme nach §§ 100a, 100b StPO darf nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden, § 100b I S. 1 StPO. Bei Gefahr im Verzug[40] kann sie gemäß § 100b I S. 2 StPO auch durch die Staatsanwaltschaft getroffen werden, bedarf dann aber nach § 100b I S. 3 StPO der Bestätigung durch das Gericht binnen drei Werktagen, damit sie nicht außer Kraft tritt[41].

Die Anordnungen haben hierbei gemäß § 100b II S. 1 StPO stets schriftlich zu ergehen. In die jeweilige Anordnung sind die notwenigen Angaben nach § 100b II S. 2 Nr. 1, 2 und 3 StPO aufzunehmen. Die Angaben zur Rufnummer oder anderen Kennung des zu überwachenden Anschlusses oder des Endgerätes (Nr. 2) sowie zu Art, Umfang und Dauer einschließlich Endzeitpunkt[42] der Maßnahme (Nr. 3) sind hierbei obligatorisch in die

---

[40] *Gefahr im Verzug* liegt grds. dann vor, wenn das vorherige Einholen der richterlichen Anordnung den Erfolg der Maßnahme gefährden würde, vgl. BVerfG NJW 1979, 1539 (1540); bei strafprozessualen Maßnahmen ist dies regelmäßig dann der Fall, wenn ein Verlust von Beweismitteln droht, der allerdings nicht von den Ermittlungsbehörden selbst herbeigeführt worden sein darf, vgl. BVerfG NJW 2001, 1121 (1123).

[41] Wobei bei Außerkrafttreten der staatsanwaltschaftlichen Anordnung wegen fehlender richterlicher Bestätigung innerhalb von drei Werktagen die bis dahin auf Grund der Eilanordnung rechtmäßig gewonnenen Erkenntnisse nach zutr. Ansicht verwertbar bleiben, vgl. *Bär*, TK-Überwachung, § 100b StPO, Rn. 3 f. sowie Meyer-Goßner – *Cierniak*, StPO, § 100b, Rn. 1, jeweils m. w. N.; zur Unverwertbarkeit bei willkürlicher Annahme von Gefahr im Verzug, siehe 2. Teil A.III.2.

[42] Gemäß § 100b I S. 4 StPO ist die Anordnung auf höchstens 3 Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als 3 Monate ist jedoch nach S. 5 zulässig, soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen.

Anordnung aufzunehmen. Name und Anschrift des Betroffenen, gegen den sich die Maßnahme richtet, sind in der Anordnung anzugeben, soweit dies möglich ist (Nr. 1). Überwachungsmaßnahmen sind deshalb grds. auch gegen (namentlich) unbekannte Personen bzw. Personen, deren wahre Identität (noch) nicht bekannt ist (z. B. bei Alias- oder Decknamen), möglich.[43]

§ 100b StPO
[Anordnung und Umsetzung der Überwachung der Telekommunikation]

(1) [1]Maßnahmen nach § 100a dürfen nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden. [2]Bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft getroffen werden. [3]Soweit die Anordnung der Staatsanwaltschaft nicht binnen drei Werktagen von dem Gericht bestätigt wird, tritt sie außer Kraft. [4]Die Anordnung ist auf höchstens drei Monate zu befristen. [5]Eine Verlängerung um jeweils nicht mehr als drei Monate ist zulässig, soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen.

(2) [1]Die Anordnung ergeht schriftlich. [2]In ihrer Entscheidungsformel sind anzugeben:

1. soweit möglich, der Name und die Anschrift des Betroffenen, gegen den sich die Maßnahme richtet,
2. die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgerätes, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist,
3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes.

(3) [1]Auf Grund der Anordnung hat jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt, dem Gericht, der Staatsanwaltschaft und ihren im Polizeidienst tätigen Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) die Maßnahmen nach § 100a zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen. [2]Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, bestimmt sich nach dem Telekommunikationsgesetz und der Telekommunikations-Überwachungsverordnung. [3]§ 95 Abs. 2 gilt entsprechend.

(4) [1]Liegen die Voraussetzungen der Anordnung nicht mehr vor, so sind die auf Grund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden. [2]Nach Beendigung der Maßnahme ist das anordnende Gericht über deren Ergebnisse zu unterrichten.

(5) [1]Die Länder und der Generalbundesanwalt berichten dem Bundesamt für Justiz kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgen-

---

[43] Vgl. *Gercke*/*Brunst*, Internetstrafrecht, Kap.5, S. 319, Rn. 796; *Bär*, TK-Überwachung, § 100a StPO, Rn. 8.

den Jahres über in ihrem Zuständigkeitsbereich angeordnete Maßnahmen nach § 100a. [2]Das Bundesamt für Justiz erstellt eine Übersicht zu den im Berichtsjahr bundesweit angeordneten Maßnahmen und veröffentlicht diese im Internet.

(6) In den Berichten nach Absatz 5 sind anzugeben:

1. die Anzahl der Verfahren, in denen Maßnahmen nach § 100a Abs. 1 angeordnet worden sind;
2. die Anzahl der Überwachungsanordnungen nach § 100a Abs. 1, unterschieden nach
   a) Erst- und Verlängerungsanordnungen sowie
   b) Festnetz-, Mobilfunk- und Internettelekommunikation;
3. die jeweils zugrunde liegende Anlassstraftat nach Maßgabe der Unterteilung in § 100a Abs. 2.

Nach Abschluss der Maßnahme sind die Beteiligten der überwachten Telekommunikation (d. h. die Personen, die telekommuniziert haben[44]) grds. gemäß § 101 IV S. 1 Nr. 3 StPO von der nach §§ 100a, 100b StPO erfolgten Maßnahme zu benachrichtigen, soweit nicht ein besonderer Rückstellungsgrund nach § 101 V S. 2 StPO vorliegt. Die Benachrichtigungspflicht unter Hinweis auf die Möglichkeit nachträglichen Rechtsschutzes nach § 101 IV S. 2, VII StPO stellt hierbei eine wesentliche Ausprägung des Rechtsstaatsgebotes (Art. 20 III GG) und der Rechtsweggarantie (Art. 19 IV GG) bei ohne Wissen der Betroffenen durchgeführten strafprozessualen Ermittlungsmaßnahmen dar.

§ 101 StPO
[Benachrichtigung; Löschung personenbezogener Daten]

(1) Für Maßnahmen nach den §§ 98a, 99, 100a, 100c bis 100i, 110a, 163d bis 163f gelten, soweit nichts anderes bestimmt ist, die nachstehenden Regelungen.

(2) (…)

(3) (…)

(4) [1]Von den in Absatz 1 genannten Maßnahmen sind im Falle

(…)

3. des § 100a die Beteiligten der überwachten Telekommunikation,

(…)

zu benachrichtigen. [2]Dabei ist auf die Möglichkeit nachträglichen Rechtsschutzes nach Absatz 7 und die dafür vorgesehene Frist hinzuweisen. [3]Die Benachrichtigung unterbleibt, wenn ihr überwiegende schutzwürdige Belange

44 Vgl. BT-Drs. 15/5846, S. 58.

einer betroffenen Person entgegenstehen. [4]Zudem kann die Benachrichtigung einer in Satz 1 Nr. 2, 3 und 6 bezeichneten Person, gegen die sich die Maßnahme nicht gerichtet hat, unterbleiben, wenn diese von der Maßnahme nur unerheblich betroffen wurde und anzunehmen ist, dass sie kein Interesse an einer Benachrichtigung hat. [5]Nachforschungen zur Feststellung der Identität einer in Satz 1 bezeichneten Person sind nur vorzunehmen, wenn dies unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber dieser Person, des Aufwands für die Feststellung ihrer Identität sowie der daraus für diese oder andere Personen folgenden Beeinträchtigungen geboten ist.

(5) [1]Die Benachrichtigung erfolgt, sobald dies ohne Gefährdung des Untersuchungszwecks, des Lebens, der körperlichen Unversehrtheit und der persönlichen Freiheit einer Person und von bedeutenden Vermögenswerten, im Fall des § 110a auch der Möglichkeit der weiteren Verwendung des Verdeckten Ermittlers möglich ist. [2]Wird die Benachrichtigung nach Satz 1 zurückgestellt, sind die Gründe aktenkundig zu machen.

(6) (…)

(7) [1]Gerichtliche Entscheidungen nach Absatz 6 trifft das für die Anordnung der Maßnahme zuständige Gericht, im Übrigen das Gericht am Sitz der zuständigen Staatsanwaltschaft. [2]Die in Absatz 4 Satz 1 genannten Personen können bei dem nach Satz 1 zuständigen Gericht auch nach Beendigung der Maßnahme bis zu zwei Wochen nach ihrer Benachrichtigung die Überprüfung der Rechtmäßigkeit der Maßnahme sowie der Art und Weise ihres Vollzugs beantragen. [3]Gegen die Entscheidung ist die sofortige Beschwerde statthaft. [4]Ist die öffentliche Klage erhoben und der Angeklagte benachrichtigt worden, entscheidet über den Antrag das mit der Sache befasste Gericht in der das Verfahren abschließenden Entscheidung.

(8) (…)

Ermittlungsschwerpunkt der Quellen-TKÜ ist der Zugriff auf Inhaltsdaten, also die Erlangung eines Einblicks in die Inhalte einer geführten VoIP-Kommunikation. Es stellt sich im Folgenden die Frage, ob die Regelungen der §§ 100a, 100b StPO de lege lata zu einer Maßnahme der Quellen-TKÜ überhaupt legitimieren können. Die Befugnisnorm der §§ 100a, 100b StPO kann der Quellen-TKÜ dann als Rechtsgrundlage dienen, wenn die dortige strafprozessuale Regelung der Telekommunikationsüberwachung und -aufzeichnung für eine derartige Ermittlungsmaßnahme hinreichend bestimmt ist und die gesetzlichen Voraussetzungen einer TKÜ i. S. d. §§ 100a, 100b StPO vorliegen. Dies ist der Fall, wenn sich die Quellen-TKÜ unter die Tatbestandsbegrifflichkeiten der §§ 100a, 100b StPO subsumieren lässt und die einer derartigen Maßnahme zugrunde liegenden Eingriffsumstände, Ermittlungsmöglichkeiten und Eingriffsgrenzen für Normadressaten (zumindest im Grundsatz) erkennbar und einschätzbar sind.

1. Bestimmtheitsgebot und Vorbehalt des Gesetzes

Das *Bestimmtheitsgebot* ist spezielle Ausprägung des in Art. 20 III, 28 I S. 1 GG verfassungsrechtlich verankerten Rechtsstaatsprinzips.[45] Neben der Sicherstellung, dass alle wesentlichen Entscheidungen über Grundrechtseingriffe und deren Reichweite durch den demokratisch legitimierten Parlamentsgesetzgeber selbst getroffen werden, dass gesetzesanwendende bzw. -ausführende staatliche Stellen im Gesetz steuernde und begrenzende Handlungsmaßstäbe vorfinden sowie Gerichte Rechtskontrolle leisten können[46], sieht dessen Prinzip auch vor, dass der Durchschnittsbürger als Normadressat aus Rechtsnormen erkennen können muss, welche Rechtsfolgen ein von ihm gewähltes Verhalten nach sich ziehen kann, damit er sein Handeln danach ausrichten kann. Die staatlichen Reaktionen auf sein spezifisches Handeln müssen hierbei für den betroffenen Bürger hinreichend vorhersehbar, erkennbar und einschätzbar sein.[47]

Für gesetzliche Normen, auf deren Grundlage der Staat gegenüber dem Bürger hoheitlich auftritt, ist es daher erforderlich, dass diese hinreichend klar formuliert und hinsichtlich ihres Anwendungsbereichs, ihrer Voraussetzungen sowie ihrer Rechtsfolgen bestimmt genug sind.[48] Hierfür hat der Gesetzgeber „Anlass, Zweck und Grenzen des Eingriffs hinreichend bereichsspezifisch, präzise und normenklar festzulegen“[49]. Wegen des andererseits bestehenden gesetzgeberischen Bedürfnisses nach ausreichender Gesetzesabstraktheit zur Erfassung möglichst vieler Lebenssachverhalte, die mit dem Regelungsgegenstand in Zusammenhang stehen, ist die Verwendung von Generalklauseln, unbestimmten Rechtsbegriffen und Ermessenstatbestände[50] wie auch die Verwendung von auslegungsfähigen Tatbestands(ober) begrifflichkeiten[51] durch das Bestimmtheitsgebot hingegen nicht ausgeschlossen. Denn die rechtsstaatlichen Prinzipien erfordern indes nicht das Vorliegen bestmöglicher („optimaler“[52]) Bestimmtheit. Für die verfassungs-

---

45 Vgl. BVerfG NJW 2008, 822 (827); auch BVerfG NJW 2004, 2213 (2216); BVerfG NJW 2005, 2603 (2607); BVerfG NJW 2006, 1939 (1947); aus diesem ergeben sich im Strafverfahrensrecht die Anforderungen an Normenklarheit und Tatbestandsbestimmtheit, vgl. BVerfG NJW 2005, 1338 (1339).

46 Vgl. BVerfG NJW 2004, 2213 (2215); BVerfG NJW 2008, 822 (827 f.).

47 Vgl. Maunz/Dürig – *Grzeszick*, GG, Art. 20, Abschnitt VII, 63. EL 2011, Rn. 58 ff; BVerfG NJW 2005, 1338 (1339).

48 Richtungsweisend BVerfG NJW 1984, 419 (*Volkszählungsurteil*).

49 BVerfG NJW 2008, 822 (828) m. w. N.

50 Vgl. BeckOK – *Huster/Rux*, GG, Ed. 13, Art. 20, Rn. 169; ebenso Maunz/Dürig – *Grzeszick*, GG, Art. 20, Abschnitt VII, 63. EL 2011, Rn. 62 f. m. w. N.

51 Vgl. i. E. BVerfG NJW 1969, 1059 (1061); BVerfG NStZ 1989, 229 (229).

52 Maunz/Dürig – *Grzeszick*, GG, Art. 20, Abschnitt VII, 63. EL 2011, Rn. 61.

rechtlichen Anforderungen an die Ausgestaltung von Normen genügt das Vorliegen *hinreichender* Bestimmtheit[53], soweit sich mit Hilfe üblicher juristischer Auslegungsmethodik – insbesondere durch Heranziehen anderer Gesetzesvorschriften, des Normzusammenhangs und der Gesetzesbegründung[54] – eine „zuverlässige Grundlage für die Auslegung und Anwendung der Vorschrift gewinnen lässt“[55] und insbesondere beim Verwenden unbestimmter Rechtsbegriffe „verbleibende Ungewissheiten nicht so weit gehen, dass die Vorhersehbarkeit und Justiziabilität des Handelns der durch die Normen ermächtigten staatlichen Stellen gefährdet sind“[56].

Für den Bereich der belastenden staatlichen Eingriffe in (grundrechtliche) Freiheiten des Bürgers gelten für diese Grundsätze tendenziell erhöhte Anforderungen.[57] Insbesondere bei heimlich stattfindenden staatlichen Maßnahmen bestehe daher ein gesteigertes Bedürfnis, die Voraussetzungen für einen Eingriff relativ genau zu regeln, da sich Betroffene der Maßnahme mangels Kenntnis im Zeitpunkt ihres Stattfindens i. d. R. erst nachträglich erwehren können.[58] Aber auch hier finde die Bestimmbarkeit des Tatbestandes anhand von Rechtsbegriffen ihre Grenzen grds. in der „möglichen Vielgestaltigkeit der zu regelnden Sachverhalte“[59]. Insbesondere „wo die zu erfassenden Einzelfälle eine sehr hohe Streubreite an einzelfallspezifischen Besonderheiten aufweisen“[60], sei es dem Gesetzgeber auch im Bereich des Eingriffshandelns gestattet, im Rahmen abstrakt-genereller Vorschriften auf Tatbestandsseite mit abstrakten bzw. unbestimmten Rechtsbegriffen zu arbeiten bzw. auch auf Rechtsfolgenseite dem Rechtsanwender durch Einräumen eines Ermessenspielraums einen Entscheidungsspielraum zuzuordnen.[61] Nach Auffassung des BVerfG[62] hat der Gesetzgeber hierbei eine gewisse Freiheit „generalisierende, typisierende und pauschalierende Regelungen zu verwenden“[63], insbesondere wenn es sich um die „Ordnung von Massenerscheinungen“[64] handelt.[65]

---

53 Auch BVerfG NJW 2003, 2004 (2006).

54 Vgl. Maunz/Dürig – *Grzeszick*, GG, Art. 20, Abschnitt VII, 63. EL 2011, Rn. 61.

55 BayVerfGH BeckRS 2004, 25078.

56 BVerfG NJW 2008, 822 (828) m. w. N.

57 Vgl. Maunz/Dürig – *Grzeszick*, GG, Art. 20, Abschnitt VII, 63. EL 2011, Rn. 65.

58 Vgl. Maunz/Dürig – *Grzeszick*, GG, Art. 20, Abschnitt VII, 63. EL 2011, Rn. 65 m. w. N.

59 Maunz/Dürig – *Grzeszick*, GG, Art. 20, Abschnitt VII, 63. EL 2011, Rn. 65.

60 Maunz/Dürig – *Grzeszick*, GG, Art. 20, Abschnitt VII, 63. EL 2011, Rn. 65.

61 So Maunz/Dürig – *Grzeszick*, GG, Art. 20, Abschnitt VII, 63. EL 2011, Rn. 65.

62 Vgl. BVerfG NJW 1992, 423 (424); BVerfG NJW 1999, 2505 (2507); BVerfG BeckRS 2005, 25896; BVerfG BeckRS 2011, 49814.

63 BVerfG NJW 1992, 423 (424).

64 BVerfG NJW 1999, 2505 (2507).

a) Analogieverbot im Strafprozessrecht

Das Gebot gesetzlicher Bestimmtheit im Bereich des Strafrechts *(nulla poena sine lege certa)*, das verfassungsrechtlich in Art. 103 II GG und einfachgesetzlich in § 1 Strafgesetzbuch (StGB)[66] enthaltenen ist, legt fest, dass eine Tat nur bestraft werden kann, wenn die Strafbarkeit gesetzlich bestimmt war, bevor die Tat begangen wurde *(nulla poena sine lege praevia)*.[67] Das Bestimmtheitsgebot entspringt hierbei dem allgemeinen Rechtsprinzip *nulla poena sine lege (scripta)* und bedingt ein Verbot strafbegründender und strafschärfender Analogie.[68] Dies bedeutet, dass über den Inhalt einer gesetzlichen Eingriffsnorm nicht durch analoge Rechtsanwendung zu Lasten des Betroffenen hinausgegangen werden darf *(nulla poena sine lege stricta)*.[69]

Das Verbot analoger Rechtsanwendung gilt nach überwiegender Ansicht in Rspr. und Literatur[70] (zumindest im Grundsatz[71]) nur für den Bereich des materiellen Strafrechts, nicht für den des Strafprozessrechts.[72] Dieser Grundsatz besteht jedoch nach teilweise vertretender Auffassung nicht ausnahmslos. Das Analogieverbot finde demnach im Strafprozessrecht jedenfalls auf beweisbildenden Verfahrensnormen Anwendung[73], da solche strafbegründenden Charakter aufweisen. Gleiches könne auch für strafprozessuale Eingriffe in grundgesetzlich geschützte Rechte angenommen werden.[74] Nur wenn die strafprozessuale Norm ausschließlich der Verfahrens-

---

65 Worunter sich durchaus telekommunikationsbezogene Vorschriften fassen lassen, deren Gegenstand – wie bspw. in den Fällen des § 100a I StPO – nach dem Willen des Gesetzgebers ein breites Spektrum an Kommunikationstechniken und Nutzungsweisen umfassen soll, weil der Normgegenstand der *Telekommunikation* naturgemäß einem rasanten technischen Fortschritt unterworfen ist.

66 Strafgesetzbuch i. d. F. der Bekanntmachung vom 13.11.1998 (BGBl. I S. 3322).

67 Gemäß st. Rspr. des BVerfG, jüngst BVerfG NJW 2009, 2370 (2370 f.).

68 Vgl. BeckOK – *Heintschel-Heinegg*, StGB, Ed. 17, § 1, Rn. 12; BeckOK – *Huster/Rux*, GG, Ed. 13, Art. 20, Rn. 169.1.

69 Vgl. BVerfG NJW 1986, 1671 (1672).

70 Vgl. KG NJW 1997, 1668 (1669); Meyer-Goßner – *Meyer-Goßner*, StPO, Einl., Rn. 198; *Bär*, Handbuch zur EDV-Beweissicherung, Rn. 5; a. A. Löwe-Rosenberg – *Lüderssen/Jahn*, StPO und GVG, Erster Band, Einl. M, Rn. 47 m. w. N.

71 Nunmehr mit Einschränkung „im Grundsatz" BVerfG NJW 2005, 1338 (1339); so auch BGH-Ermittlungsrichter BeckRS 2007, 00295, demzufolge das Analogieverbot „im Grundsatz" zwar nicht das Strafprozessrecht erfasst, die entsprechende Anwendung einer anderen Eingriffsnorm bei schwerwiegenden Eingriffen aber einer Umgehung des Gesetzesvorbehaltes gleichkäme.

72 Zu den gleichwohl zu beachtenden Anforderungen des Bestimmtheitsgebotes und des allgemeinen Vorbehaltes des Gesetzes, siehe nachfolgend 2. Teil A.II.1.b).

73 Vgl. *Jäger*, GA 2006, 615 (628).

74 Vgl. *Welp*, JR 1991, 265 (267).

ordnung bzw. der Verfahrensleitung dient oder keinerlei beschwerende Wirkung für den Betroffenen hat, könnten Ausnahmen vom Prinzip des Analogieverbotes angebracht sein.[75]

Eine solche Ausnahme vom Analogieverbot läge demnach bei der Quellen-TKÜ nicht vor. Die strafprozessualen Befugnisnormen, die eine solche Maßnahme legitimieren, dienen im Kern der Gewinnung von Beweisen sowie Spurenansätzen und haben belastende Wirkung für den Betroffenen.

Für die repressive Quellen-TKÜ bestünde – bei dieser Sichtweise – grds. das Bedürfnis für eine Abgrenzung zwischen noch zulässiger Tatbestandauslegung der in Frage kommenden §§ 100a, 100b StPO und bereits unzulässiger analoger Rechtsanwendung.

Der Schluss, dass sich die Quellen-TKÜ allenfalls im Wege einer (ggf. unzulässigen) analogen Anwendung der §§ 100a, 100b StPO realisieren ließe, entfällt jedenfalls dann, wenn sich die Vorgehensweise einer Quellen-TKÜ im Wege zulässiger Auslegung des strafprozessualen Eingriffstatbestandes bereits in direkter Weise unter die §§ 100a, 100b StPO subsumieren lässt.

b) Auslegung strafprozessualer Eingriffsnormen

Folgt man der h. M., welche eine Anwendbarkeit des Analogieverbotes des Art. 103 II GG auf das Strafverfahrensrecht verneint, so unterliegen die §§ 100a, 100b StPO zwar nicht den starren Grenzen, die Art. 103 II GG für das materielle Strafrecht setzt. Dies bedeutet aber nicht, dass im Strafverfahrensrecht einer Rechtsfortbildung keine Grenzen gesetzt wären.[76] Hier sind gleichwohl die Anforderungen des Bestimmtheitsgebotes aus Art. 20 III, 28 I S. 1 GG zu beachten. Dies gilt nicht zuletzt auch zum Schutz des demokratisch legitimierten Gesetzgebers.

Nicht für jedwede staatliche Ermittlungsmaßnahme ist zwar gleichzeitig auch eine Befugnisnorm notwendig. Gemäß der vom BVerfG entwickelten *Wesentlichkeitstheorie*[77] ist für eine Maßnahme staatlicher Gewalt allerdings dann eine spezielle Befugnisnorm erforderlich, wenn diese einen Grundrechtseingriff mit sich bringt[78], da alle „wesentlichen Entscheidungen“ zu Grundrechtseinschränkungen durch das Parlament als Gesetzgeber

---

[75] Vgl. BeckOK – *Heintschel-Heinegg*, StGB, Ed. 17, § 1, Rn. 12a; ausführlich *Jäger*, GA 2006, 615 (628).

[76] Vgl. *Bär*, Handbuch zur EDV-Beweissicherung, Rn. 5.

[77] Vgl. BVerfG NJW 1998, 2515; BVerfG NJW 1979, 359; BVerfG NJW 1978, 807; BVerfG NJW 1972, 1504.

[78] Vgl. *Gercke*/*Brunst*, Internetstrafrecht, Kap.5, S. 315, Rn. 783.

selbst getroffen werden müssen. Um dem Erfordernis gesetzlicher Bestimmtheit gerecht zu werden, bedarf jeder Eingriffe in grundrechtlich geschützte Freiheitsrechte daher einer gesetzlichen Ermächtigungsgrundlage (Grundsatz vom Vorbehalt des Gesetzes aus Art. 20 III GG[79]). Dies gilt erst recht bei heimlichen bzw. verdeckten[80] Eingriffen, da der Staat grds. dazu gehalten ist, offen zu agieren und gegenüber dem Bürger offen aufzutreten, die verdeckte Ermittlung hingegen – vom gesetzlichen Grundsatzgedanken her – auf bestimmte (Ausnahme-)Fälle beschränkt sein soll.[81]

Eine derartige (strafprozessuale) Befugnisnorm muss als Rechtsgrundlage für Eingriffe in die hiervon betroffenen Grundrechte auf Grund des Bestimmtheitsgebotes aus Art. 20 III, 28 I S. 1 GG hinreichend klar formuliert und ihr Tatbestand bestimmt genug sein (*Gebot der Normenklarheit und Tatbestandsbestimmtheit*).[82] Die Maßgaben, welche das BVerfG im Rahmen des Volkszählungsurteils[83] unter Herleitung des Grundrechts auf informationelle Selbstbestimmung aus den Art. 2 I i. V. m. Art. 1 I GG entwickelt hat, sind grds. auch auf Eingriffe in das Grundrecht aus Art. 10 I GG übertragbar.[84] Um dem Gebot der Normenklarheit und Tatbestandsbestimmtheit zu genügen, ist es nach st. Rspr. des BVerfG erforderlich, dass „sich die Voraussetzungen [des Eingriffs] und der Umfang der Beschränkungen [des Grundrechts] aus dem Gesetz klar und für den Bürger erkennbar ergeben“[85], damit dieser die Rechtslage anhand der gesetzlichen Regelung so erkennen und einschätzen kann, dass er sein Verhalten und Handeln

---

79 Grundlegend BVerfG NJW 1976, 34 (34 f.); für Einzelheiten zur dogmatischen Herleitung, siehe auch Löwe-Rosenberg – *Schäfer*, StPO und GVG, Zweiter Band, 25. Aufl. 2004, Vor § 94 StPO, Rn. 25 ff.; zum Gesetzlichkeitsgrundsatz im Strafverfahrensrecht, *Kudlich*, GA 2011, 193 (195) m. w. N.

80 Der Begriff „verdeckt“ wird oftmals synonym mit dem Begriff „heimlich“ verwendet (i. S. v. „ohne Wissen des Betroffenen“); dies entspricht auch der üblichen Terminologie in Rspr. und Schrifttum; bei strenger Begriffsauslegung beschreibt der Begriff der „Verdecktheit“ indes eher den Umstand, dass der Betroffene zwar die (sichtbaren) Handlungen/Auswirkungen der Maßnahmeumsetzung mitbekommt, den dahinter stehenden tatsächlichen (ermittlungstaktischen) Anlass/Zweck aber nicht erkennt (bspw. durch das Handeln der Ermittlungspersonen unter einem bestimmten Vorwand und/oder Anwendung einer Legende), während der Begriff der „Heimlichkeit“ hingegen eher auf eine völlige Unkenntnis des Betroffenen vom Ablaufen einer Maßnahme ihm gegenüber überhaupt hindeutet.

81 Vgl. *Gercke*/*Brunst*, Internetstrafrecht, Kap.5, S. 316, Rn. 786.

82 Vgl. BVerfG NJW 2005, 1338 (1339 f.); BVerfG NJW 2006, 976 (979); vgl. auch BVerfG NJW 2005, 1338 (1339), wonach sich die Anforderungen an Normenklarheit und Tatbestandsbestimmtheit im Strafverfahrensrecht aus Art. 20 III, 28 I S. 1 GG ergeben.

83 BVerfG NJW 1984, 419.

84 Vgl. BVerfG NJW 2009, 2431 (2434); BVerfG NJW 2004, 2213 (2215).

85 BVerfG NJW 2009, 2431 (2434).

danach auszurichten vermag.[86] Hierfür müssen Anlass, Zweck und Grenzen des Eingriffs in das betroffene Grundrecht (hier das Fernmeldegeheimnis aus Art. 10 I GG) aus der Ermächtigungsnorm bereichsspezifisch und präzise hervorgehen.[87]

Da eine gesetzliche Norm allerdings nicht alle ihr unterfallenden Konstellationen im Wortlaut ausdrücklich regeln kann, können diese auch im Wege der Auslegung vom Tatbestand der Befugnisnorm erfasst sein, ohne mit diesen Prinzipien in Konflikt zu geraten. Dies gilt insbesondere für strafprozessuale Eingriffsnormen, die in sachlichem Zusammenhang mit technischen Entwicklungen stehen.[88]

Technischen Neuerungen kann durch entsprechend angepasste Auslegung strafprozessualer Eingriffsnormen Rechnung getragen werden.[89] Dabei bildet der mögliche *Wortsinn* des Gesetzes die äußerste Grenze zulässiger richterlicher Gesetzesinterpretation/-auslegung.[90]

Eine Anwendung der §§ 100a, 100b StPO auf die Quellen-TKÜ wäre demnach möglich, wenn sich die Überwachung und Aufzeichnung von Telekommunikation unter Verwendung einer Überwachungssoftware in den Grenzen zulässiger Gesetzesauslegung des – im Falles der §§ 100a, 100b StPO relativ entwicklungsoffen gehaltenen[91] – Eingriffstatbestandes subsumieren lässt. Um diesen Anforderungen gerecht zu werden, darf eine zulässige Auslegung der für die Quellen-TKÜ als Rechtsgrundlage in Frage kommenden §§ 100a, 100b StPO von ihrem Begriffsverständnis her zwar durchaus weit ausfallen, muss sich jedoch innerhalb des möglichen Wortsinns der dort niedergelegten Eingriffsvoraussetzungen einer Telekommunikationsüberwachung und -aufzeichnung bewegen.

Es gilt daher, sich im Rahmen der nachfolgenden Untersuchungen dogmatisch mit der Frage auseinanderzusetzen, ob das Überwachen und Aufzeichnen von Telekommunikation unter Verwendung einer Überwachungssoftware auf einem zur Kommunikation verwendeten Endgerät vom Normzweck sowie vom Wortsinn der einzelnen Tatbestandsbegrifflichkeiten der §§ 100a, 100b StPO umfasst ist[92] und die Subsumtion der Quellen-TKÜ

---

86 Vgl. BVerfG NJW 2004, 2213 (2215).

87 Vgl. bereits BVerfG NJW 2000, 55 (57); ebenso BVerfG NJW 2004, 2213 (2215); BVerfG NJW 2005, 2603 (2607); BVerfG NJW 2009, 2431 (2434).

88 Vgl. BGH-Ermittlungsrichter BeckRS 2007, 00295.

89 Vgl. BGH-Ermittlungsrichter BeckRS 2007, 00295.

90 Vgl. BVerfG NJW 2008, 3627 (3627); auch *Bär*, Handbuch zur EDV-Beweissicherung, Rn. 6; hierzu auch *Böckenförde*, Die Ermittlung im Netz, S. 419.

91 Vgl. BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 2 u. 6; vgl. auch *Kudlich*, JuS 2001, 1165 (1166) m. w. N.; *ders*., JA 2010, 310 (312).

92 Siehe hierzu die nachfolgenden Ausführungen sowie 3. Teil A.I.1.a).

unter die bestehenden strafprozessualen Regelungen zur Überwachung und Aufzeichnung von Telekommunikation ohne Verstoß gegen den Bestimmtheitsgrundsatz[93] möglich ist.

2. Schluss vom Schutzbereich auf Eingriffsbefugnis?

Zur Frage, ob und wann bei Quellen-TKÜ-Maßnahmen (allein) der Schutzbereich des Fernmeldegeheimnisses aus Art. 10 I GG eröffnet ist, hat das BVerfG im Rahmen seiner Entscheidung zur (präventiven) Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalen vom 27.02.2008[94] grundlegend Stellung bezogen[95]. Wie bereits erörtert[96], verfolgt das BVerfG zur Frage, an welchen Grundrechten eine Maßnahme der Quellen-TKÜ zu messen ist, eine Sichtweise, die sich vor allem auch an der technischen Art der Überwachung orientiert[97].

So hat das BVerfG festgestellt, dass Art. 10 I GG der alleinige Grundrechtsmaßstab für die Beurteilung einer Ermächtigung zu einer Quellen-TKÜ und der darauf gestützten Eingriffe sei, „wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt“[98] und dies „durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt“[99] ist.

Eine potentielle Rechtsgrundlage für die Quellen-TKÜ muss somit zunächst so ausgestaltet sein, dass sie zu *Eingriffen in das Fernmeldegeheimnis* aus Art. 10 I GG legitimiert.

Der Umstand, dass die Vorschriften der §§ 100a, 100b StPO über die Überwachung und Aufzeichnung der Telekommunikation Eingriffe in das Fernmeldegeheimnis gestatten, könnte hierbei zu der (vorschnellen) Annahme verleiten, dass diese Befugnisnorm dann automatisch auch eine Quellen-TKÜ erlauben müsse. Eine Anlehnung des § 100a StPO an den Schutzbereich des Art. 10 I GG erschiene zunächst auch naheliegend, da § 100a I StPO ja zu Eingriffen in das Fernmeldegeheimnis legitimieren soll.[100]

Dieser Schluss vom Schutzbereich eines Grundrechtes auf die (automatische) Einschlägigkeit des Eingriffsbereichs einer bestimmten Befugnisnorm

---

93 Siehe hierzu 3. Teil A.I.1.b).

94 Vgl. BVerfG NJW 2008, 822.

95 Für Einzelheiten zur Grundsatzentscheidung des BVerfG vom 27.02.2008 (BVerfG NJW 2008, 822), siehe 1. Teil B.IV.

96 Für Einzelheiten zu den verfassungsrechtlichen Grundlagen, siehe 1. Teil B.

97 Vgl. insoweit auch *Gercke*/*Brunst*, Internetstrafrecht, Kap.5, S. 349, Rn. 893.

98 BVerfG NJW 2008, 822 (826).

99 BVerfG NJW 2008, 822 (826).

100 Vgl. *Kudlich*, JuS 2001, 1165 (1167).

erweckt jedoch bei näherem Hinsehen gewisse Zweifel.[101] Während grundrechtliche Schutzbereiche nämlich im Sinne einer größtmöglichen Effektivität des Grundrechtsschutzes eher weit gefasst sein sollen, sind strafprozessuale Eingriffsermächtigungen mit Blick auf das geltende Bestimmtheitsgebot[102] eher nah am Normtext[103] – jedenfalls innerhalb des möglichen Wortsinns der einzelnen Tatbestandsvoraussetzungen[104] – auszulegen. Dies soll zwar nicht bedeuten, dass zur Bezeichnung einer bestimmten Art von Kommunikation als „Telekommunikation" i. S. d. § 100a I StPO nicht auf den weiten grundrechtlichen Begriff aus Art. 10 I GG zurückgegriffen werden dürfte. Das heißt aber nicht, dass sämtliche Ermittlungsmaßnahmen, die auf irgendeine Art und Weise mit dieser Kommunikationsform im Zusammenhang stehen, *zwangsläufig*, d. h. automatisch auch eine „Überwachung der Telekommunikation" i. S. d. § 100a StPO darstellen müssen.[105]

Auf den hier vorliegenden Fall bezogen bedeutet dies: nur weil softwarebasierte Internettelefonie ohne weiteres als eine Form von Telekommunikation (sowohl i. S. d. weiteren verfassungsrechtlichen als auch i. S. d. engeren strafprozessualen Verständnisses) qualifiziert werden kann, heißt dies nicht, dass damit *automatisch* die Quellen-TKÜ-spezifische Vorgehensweise im Zeitpunkt des Zugriffs (bereits bzw. noch) eine „Überwachung von Telekommunikation" darstellen[106] und deshalb insoweit vom Eingriffstatbestand der §§ 100a, 100b StPO erfasst sein *muss*[107].

Vielmehr ist nach dem überzeugenden Ansatz *Kudlichs* für jeden Eingriff gerade wegen der grundrechtlichen Absicherung nach den allgemeinen Grundsätzen für die Auslegung von strafprozessualen Befugnisnormen genau zu prüfen, ob die mit der jeweiligen Ermittlungsmaßnahme einhergehende *spezifische Vorgehensweise* von der konkreten Befugnisnorm auch tatsächlich gedeckt ist.[108] Denn auf eine Befugnisnorm, die bestimmte

---

101 Vgl. *Kudlich*, GA 2011, 193 (201); *ders*., JuS 2001, 1165 (1167); *ders*., JA 2000, 227 (232); *ders*., JuS 1998, 209 (213); vgl. hierzu auch *Böckenförde*, Die Ermittlung im Netz, S. 419, 427 u. 429.

102 Für Einzelheiten zum Bestimmtheitsgebot, siehe 2. Teil A.II.1.

103 Vgl. *Kudlich*, JuS 2001, 1165 (1167).

104 Für Einzelheiten zum möglichen Wortsinn als äußerste Grenze der Auslegung, siehe 2. Teil A.II.1.b).

105 So zutr. *Kudlich*, JuS 2001, 1165 (1167).

106 So halten es bspw. *Becker*/*Meinicke* insoweit für „fraglich, ob die bei einer Quellen-TKÜ erhobenen Daten überhaupt als ‚Telekommunikation' […] anzusehen sind", als nach deren Sichtweise „der Zugriff gerade vor dem Aussenden bzw. nach dem Empfang [erfolgt]" (StV 2011, 50, 51); in diese Richtung auch LG Hamburg, MMR 2008, 423 (424).

107 Sehr wohl aber erfasst sein kann und i. E. auch erfasst ist, siehe hierzu 2. Teil A.II.3. sowie 3. Teil A.I.1.a)aa).

Eingriffe in ein Grundrecht erlaubt, können nicht automatisch sämtliche Eingriffe in dieses Grundrecht gestützt werden.[109] Nur weil die §§ 100a, 100b StPO also zur Überwachung und Aufzeichnung von Telekommunikation einen Eingriff in das Grundrecht aus Art. 10 I GG gestatten, heißt das nicht, dass gleichsam jeder Eingriff in das Fernmeldegeheimnis automatisch von §§ 100a, 100b StPO gedeckt ist.[110]

Für die hier vorliegende Fragestellung hat dies zur Konsequenz, dass allein auf Grund der Tatsache, dass laufende VoIP-Kommunikation dem Schutz des Fernmelde*geheimnisses* aus Art. 10 I GG unterliegt und die §§ 100a, 100b StPO zu (bestimmten) Eingriffen in den Schutzbereich des Fernmeldegeheimnisses legitimieren, noch *nicht automatisch* auf die Einschlägigkeit der strafprozessualen Befugnisnormen zur Überwachung und Aufzeichnung von Fernmelde*verkehr* (nunmehr *Telekommunikation*) auch für die mit der Durchführung von Quellen-TKÜs verbundene spezifische Vorgehensweise geschlossen werden kann.[111]

Dies soll nicht heißen, dass der Schutzbereich des Fernmeldegeheimnisses für die Eingriffsvoraussetzungen des § 100a I StPO unbeachtlich wäre. Denn gemäß höchstrichterlicher Rechtsprechung[112] hat sich die nähere Bestimmung des Begriffs „Telekommunikation" im Rahmen der Eingriffsbefugnis des § 100a StPO am grundrechtlichen Schutz des Betroffenen durch das Fernmeldegeheimnis des Art. 10 I GG zu *orientieren*.[113]

Aus den genannten Bedenken gegen einen automatischen Schluss vom Schutzbereich des Art. 10 I GG auf die spezielle Eingriffsbefugnis des § 100a I StPO ist es deshalb erforderlich zu untersuchen, ob es sich im Rahmen einer Quellen-TKÜ im Zeitpunkt des Ansetzens der Maßnahme (bereits bzw. noch) um ein Überwachen und Aufzeichnen von „Telekommunikation" handelt, d. h. ob der Telekommunikationsvorgang also schon be-

---

108 Vgl. *Kudlich*, JuS 2001, 1165 (1167); *ders*. auch GA 2011, 193 (201); *ders*. bereits JuS 1998, 209 (213).

109 Vgl. *Kudlich*, JuS 2001, 1165 (1167); in diese Richtung auch *Böckenförde*, Die Ermittlung im Netz, S. 419, 427 u. 429.

110 Bzw. die §§ 100a, 100b StPO für jeden Eingriff in das Fernmeldegeheimnis erforderlich sind, vgl. BVerfG NJW 2009, 2431 (2432 f.), wonach E-Mails, die auf dem Mail-Server des Providers gespeichert sind, dem Schutz des Fernmeldegeheimnisses aus Art. 10 I GG unterliegen, die §§ 94 ff. StPO für einen offenen Zugriff auf die beim Provider gespeicherte Nachricht als Rechtsgrundlage indes den verfassungsrechtlichen Anforderungen grds. genügen.

111 Vgl. *Kudlich*, JuS 2001, 1165 (1167); *ders*., JA 2000, 227 (232); *ders*., JuS 1998, 209 (213); vgl. auch *Böckenförde*, Die Ermittlung im Netz, S. 419, 427 u. 429.

112 BVerfG NJW 1978, 313 (314 f.); BVerfG NJW 2000, 55 (57); BGH NStZ 1997, 247 (247 f.); BGH-Ermittlungsrichter NJW 2001, 1587 (1587).

113 Vgl. auch *Bär*, TK-Überwachung, § 100a StPO, Rn. 10.

gonnen hat (bei Anknüpfen der Maßnahmen am Absendersystem) bzw. noch nicht abgeschlossen ist (bei Anknüpfen am Empfängersystem). Diese eng am Normtext orientierte Betrachtungsweise ist gerade Konsequenz des Abrückens einer am Endgerät der Kommunikation ansetzenden Maßnahme wie der Quellen-TKÜ jedenfalls vom Regelfall[114] der Überwachung von Telekommunikation nach §§ 100a, 100b StPO in Form des Abgreifens und Ausleitens der Daten durch den Netzbetreiber während der Übermittlung auf dem Transportwege (§ 100b III S. 2 StPO i. V. m. § 110 I S. 1, II TKG, § 3 I TKÜV).

Festzuhalten ist damit, dass die Vorschriften der §§ 100a, 100b StPO über die Telekommunikationsüberwachung zwar Eingriffe in das Grundrecht des Fernmeldegeheimnisses aus Art. 10 I GG rechtfertigen, jedoch nur innerhalb ihres spezifischen Tatbestandes. Das soll nicht bedeuten, dass sich Maßnahmen der Quellen-TKÜ nicht auf die Vorschriften der §§ 100a, 100b StPO stützen ließen. Dies gilt es gerade in den nachfolgenden Ausführungen dogmatisch zu untersuchen. Erforderlich für eine taugliche Rechtsgrundlage ist, dass der Zugriff im Rahmen der spezifische Vorgehensweise der Quellen-TKÜ von Normzweck wie auch Eingriffstatbestand der §§ 100a, 100b StPO umfasst ist.

3. Vorliegen von Telekommunikation im Zugriffszeitpunkt?

Nach § 100a I StPO darf unter den dort genannten Voraussetzungen in den unter Absatz 2 aufgeführten Fällen schwerer Straftaten *Telekommunikation* überwacht und aufgezeichnet werden.

Unter dogmatischen Gesichtspunkten stellt sich für die besondere Konstellation der Quellen-TKÜ die Frage, ab wann bei verschlüsselter softwarebasierter IP-Kommunikation über den Computer der laufende Daten-

---

[114] Dass dies aber ein alleiniges „Leitbild" für Maßnahmen nach §§ 100a, 100b StPO darstellt, ist, insbesondere mit Blick auf die offene Formulierung des § 100a I StPO wie auch den Regelungsinhalt des § 100b III StPO, der nur eine Mitwirkungspflicht für die TK-Diensteerbringer festschreibt, nicht jedoch eine Obliegenheit für Ermittlungsbehörden begründet, die TKÜ-Maßnahme stets nur unter deren Mitwirkung durchzuführen, zu Recht zu bezweifeln, vgl. auch *Kudlich*, JA 2010, 310 (312); so zum Verständnis von § 100b III StPO jedenfalls Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 7a, 8; auch *Bär*, TK-Überwachung, § 100a StPO, Rn. 32; *ders*., MMR 2008, 215 (219); zust. *Gercke*/*Brunst*, Internetstrafrecht, Kap.5, S. 350, Rn. 895, Fn. 377; a. A. *Sankol*, CR 2008, 13 (17); ebenso noch LG Hamburg, MMR 2008, 423 (424); nunmehr zust. LG Hamburg, MMR 2011, 693 (696); so ausdrücklich auch BT-Drs. 16/5846, S. 47, wonach „eine Obliegenheit der Strafverfolgungsbehörden, Telekommunikationsüberwachungsmaßnahmen stets unter Mitwirkung eines Telekommunikationsdienstleisters durchzuführen, […] nicht begründet [wird]" (S. 47); für Einzelheiten, siehe 2. Teil A.II.6.

austausch im Rahmen von Telekommunikation überhaupt beginnt bzw. endet und ob in dem Moment, in dem die Überwachungssoftware auf die Kommunikationsdaten zugreift, das Tatbestandsmerkmal „Telekommunikation" schon (bei Überwachung des Absendersystems) bzw. noch (bei Überwachung des Empfängersystems) erfüllt ist, oder ob eine solche zu diesem Zeitpunkt noch nicht bzw. nicht mehr vorliegt.

Der Begriff der *Telekommunikation* wird in der Strafprozessordnung selbst nicht definiert oder näher erläutert. Eine Definition ließe sich § 3 Nr. 22 TKG entnehmen, der den Begriff „Telekommunikation" als den „technische[n] Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen" bestimmt. Von dieser Definition erfasst sind Nachrichten jeglicher Art, seien sie aus Zeichen, Bildern oder Tönen, einzeln oder zusammenhängend aufgebaut[115], welche unter Verwendung von Telekommunikationsanlagen, sprich „technische[n] Einrichtungen oder Systeme[n], die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können" (§ 3 Nr. 23 TKG), ausgetauscht werden.

An diese Begriffsbestimmung des TKG lässt sich grds. auch im Strafprozessrecht für die nähere Auslegung und Konkretisierung der grundrechtseinschränkenden Norm des § 100a StPO anknüpfen.[116] Bei der Anwendung der Legaldefinition des TKG ist gleichwohl zu beachten, dass diese ihrem Wortlaut nach direkt nur für das TKG Geltung beansprucht („Im Sinne dieses Gesetzes…") und sich für das Strafprozessrecht wegen der Zielrichtung des § 100a als strafprozessuale Befugnisnorm mitunter eine solche Bestimmung des Telekommunikationsbegriffs empfiehlt, die unter Berücksichtigung der ratio legis – nämlich dem Gewinnen von Erkenntnissen zu Beweiszwecken oder als Spurenansätze – die grds. weite Definition des TKG jedenfalls auf die genannten Ermittlungsziele der StPO eingrenzt.[117]

Wie das Fernmeldegeheimnis in Art. 10 I GG[118], welches auch neuartige Übertragungstechniken mit umfasst[119], ist auch der Begriff der *Telekommu-*

---

115 Vgl. *Gercke*/*Brunst*, Internetstrafrecht, Kap.5, S. 321, Rn. 802.

116 Vgl. BGH-Ermittlungsrichter NJW 2001, 1587 (1587) („wesentliche Orientierungshilfe", 1587); auch BGH NJW 2003, 2034 (2034) („insoweit inhaltsgleich mit der Legaldefinition des § 3 Nr. 16 TKG [mittlerweile § 3 Nr. 22 TKG 2004, Anm. d. Verf.]", 2034); BGH NJW 2007, 930 (931); vgl. auch *Bär*, TK-Überwachung, § 100a StPO, Rn. 10.

117 Vgl. *Kudlich*, JuS 2001, 1165 (1168) sowie *Wohlers*/*Demko*, StV 2003, 241 (243).

118 Nach neuerer Terminologie auch „Telekommunikationsgeheimnis".

119 Vgl. BVerfG NJW 1978, 313 (314); NJW 2006, 976 (978).

nikation entwicklungsoffen zu sehen und dementsprechend auszulegen.[120] Vom Fernmeldegeheimnis umfasst ist hierbei jede Form von Telekommunikation, und zwar unabhängig von der jeweils konkret benutzten Art der Übermittlung, wie bspw. Kabel oder Funk, analoge oder digitale Übertragung, Nachrichtenübermittlung in Netzwerken etc., sowie der konkret verwendeten Ausdrucksform in Sprache, Tönen, Bildern, Zeichen oder sonstigen Daten.[121] Der Schutzbereich des Art. 10 I GG umfasst auch die Kommunikationsdienste des Internets[122], darunter als geläufigste Dienste vor allem das E-Mailing, das Instant Messaging sowie sämtliche Erscheinungsformen von IP-Kommunikation, insbesondere die von vorliegender Arbeit fokussierte Internettelefonie, welche allesamt Formen von Telekommunikation darstellen.[123]

Klärungsbedürftig im Zusammenhang mit dem Abgreifen verschlüsselt übermittelter Internettelefonie „an der Quelle" ist indes der *Umfang* der Telekommunikation. Wie in Teil 1 der vorliegenden Arbeit zu den technischen Abläufen von VoIP über den Computer[124] und zur Zugriffsweise der Quellen-TKÜ[125] erläutert, setzt die Überwachung der Internettelefonie hier nicht während der Übermittlung der (dann verschlüsselten) Datenpakete im Datennetz an, sondern auf dem benutzten Endgerät. Der Zugriff erfolgt hierbei zu einem Zeitpunkt, zu dem die Kommunikationsdaten (noch bzw. wieder) im „Klartext", also unverschlüsselt, vorliegen. Bei einem Anknüpfen der Maßnahmen auf dem System des Absenders bedeutet dies, dass im Moment des Zugriffs vor der Verschlüsselung die akustischen Signale zwar schon vom Mikrofon als analoge Eingangssignale eingefangen, in elektronische Signale umgewandelt und damit digitalisiert sind, die Datenpakete mit den Kommunikationsinhalten jedoch noch nicht in das weltweite Datennetz zum Transport entlassen sind. Entsprechendes gilt für das Anknüpfen der Maßnahme am Empfängersystem, bei dem die Datenpakete nach deren Entschlüsselung abgegriffen werden. Die Frage, ob im Zeitpunkt des Zugriffs auf die unverschlüsselten Daten vor Verschlüsselung der Kommunika-

---

120 Vgl. BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 2 u. 6; vgl. auch *Kudlich*, JuS 2001, 1165 (1166) m. w. N.; *ders*., JA 2010, 310 (312); auch *Käß*, BayVBl. 2010, 1 (6).

121 Vgl. BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 7; BVerfG NJW 2009, 2431 (2432).

122 Vgl. BVerfG MMR 2008, 315 (316).

123 Vgl. statt vieler BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 7 u. 31; Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 6 ff.

124 Für Einzelheiten zum technischen Ablauf von verschlüsselter VoIP über den Computer, siehe 1. Teil A.I.2.c) sowie 1. Teil A.I.4.

125 Für Einzelheiten zum technischen Ablauf der Primärmaßnahme einer Quellen-TKÜ, siehe 1. Teil A. II.1. sowie 1. Teil A.II.3.

tionsdaten auf dem System des Absenders bzw. nach deren Entschlüsselung auf dem System des Empfängers schon bzw. noch das Tatbestandsmerkmal des Zugriffs auf „Telekommunikation" erfüllt ist, wird teilweise in Frage gestellt[126] und bedarf daher einer näheren dogmatischen Untersuchung:

Ein Teil der Stimmen stellt sich in Bezug auf das Tatbestandsmerkmal „Telekommunikation" auf den Standpunkt, dass Telekommunikation erst in dem Moment vorliege, in dem die Kommunikationsdaten den „Herrschaftsbereich" des Endgerätes – im Fall der softwarebasierten Internettelefonie i. d. R. ein Computer als verwendetes komplexes informationstechnisches System – verlassen haben (bei Anknüpfen am Absendersystem), sich also auf ihrem Weg durch das weltweite Datennetz befinden.[127] Bei Anknüpfen der Maßnahmen am Empfängersystem müsste entsprechend das Eintreten der Daten in den „Herrschaftsbereich" des Empfängercomputers mit Verlassen des Datennetzes als relevanter Zeitpunkt für die Beendigung der Telekommunikation angesetzt werden. Für die Subsumtion der Quellen-TKÜ unter § 100a StPO hätte dies zur Folge, dass im Zeitpunkt des Abgreifens der Daten vor Verschlüsselung *auf* dem System des Absenders bzw. nach Entschlüsselung *auf* dem System des Empfängers keine Telekommunikation vorläge, da eine solche noch nicht begonnen hätte bzw. schon beendet wäre. Allein die Verarbeitung der Sprachsignale durch das VoIP-Programm (z. B. Skype-Software) leite noch keinen Übermittlungsvorgang unumkehrbar ein, da bspw. ein vorhandener Kabeldefekt die Übermittlung noch verhindern könnte.[128]

Diese Sichtweise knüpft hierbei an einem die Reichweite des Zugriffs auf Telekommunikation enger auslegenden Ansatz an, wonach eine Überwachung nach §§ 100a, 100b StPO ausschließlich im Netzbereich, also im Herrschaftsbereich eines Netzbetreibers zulässig sei.[129] So darf sich eine auf die Eingriffsbefugnis des § 100a StPO stützende Überwachungsmaßnahme nach *Sankol* „nur auf den Herrschaftsbereich des Providers beziehen, so dass Eingriffe, die auf Nachrichten oder Daten außerhalb des Netzbereichs

---

126 So *Becker*/*Meinicke*, StV 2011, 50 (51); in diese Richtung, i. E. aber offengelassen, auch LG Hamburg, MMR 2008, 423 (424); diese Problematik anschneidend auch BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 107c, der den Kommunikationsvorgang zum Zeitpunkt der Verschlüsselung als „möglicherweise" noch nicht begonnen ansieht, diese aber als „Vorstufe" dem Kommunikationsvorgang zurechnet.

127 Vgl. *Sankol*, CR 2008, 13 (14 f.); wohl auch SK – *Wolter*, StPO, § 100a, Rn. 28 f.; vgl. hierzu auch die Ausführungen bei *Gercke*/*Brunst*, Internetstrafrecht, Kap.5, S. 349, Rn. 892 sowie *Brunst*, Anonymität im Internet, S. 267.

128 Vgl. *Gercke*/*Brunst*, Internetstrafrecht, Kap.5, S. 349, Rn. 892, Fn. 373; *Brunst*, Anonymität im Internet, S. 267, Fn. 1399.

129 So *Sankol*, CR 2008, 13 (14 f.); auch LG Hamburg, MMR 2008, 423 (425); vgl. auch noch BGH NJW 1996, 2940 (2943); a. A. *Käß*, BayVBl. 2010, 1 (6).

zielen, weder an dieser Vorschrift zu messen sind noch von dieser gedeckt werden“[130]. Deshalb stoße eine Maßnahme zur Überwachung und Aufzeichnung internetbasiert geführter Telefonate an (verfassungs-)rechtliche Grenzen, „sofern […] der technische Anknüpfungspunkt der Ermittlungsbehörden nicht das Leitungsnetz eines Telekommunikationsunternehmens, sondern das Endgerät der jeweiligen Zielperson ist“[131]. So richte sich „die richterliche Gestattung der TK-Überwachung […] gem. § 100b Abs. 3 Satz 1 StPO […] ausschließlich an den Betreiber der TK-Dienste[…]“[132]. Hierbei sei „die Geheimsphäre, in welche auf Basis des in § 100a StPO geregelten Normalfalls eingegriffen werden darf, […] mithin ausschließlich der Herrschaftsbereich des Netzbetreibers“[133]. Nach dieser Sichtweise müssten die §§ 100a, 100b StPO somit bereits an diesem Punkt als Rechtsgrundlage für die Quellen-TKÜ ausscheiden.

Demgegenüber erstrecke sich nach anderer Sichtweise die Reichweite von Telekommunikation zwar vom Absenden der Signale bis zu deren Eintreffen beim Empfänger, umfasse also nur den eigentlichen technischen Vorgang der Übermittlung von Kommunikationsdaten vom Absender zum Empfänger.[134] Aus der Eingrenzung des Umfangs der Telekommunikation folge jedoch nicht, dass Überwachungsmaßnahmen unbedingt und unmittelbar auf dem Übertragungsweg im Leitungsnetz des Netzbetreibers stattfinden müssen.[135] Nach *Graf* kann vielmehr „ein Abhörgerät auch an dem Endgerät eines Teilnehmers, also nicht mehr in der Einflusssphäre des Netzbetreibers, angebracht sein“[136]. Technischer Anknüpfungspunkt einer

---

130 *Sankol*, CR 2008, 13 (14), was durch den Regelungsgehalt des § 100b III StPO verdeutlicht werde.

131 *Sankol*, CR 2008, 13 (14 f.).

132 LG Hamburg, MMR 2008, 423 (425).

133 LG Hamburg, MMR 2008, 423 (425); vgl. auch *Sankol*, CR 2008, 13 (15); vgl. insoweit auch noch BGH NJW 1996, 2940, wonach „der Grundrechtsschutz […] am Endgerät des Fernsprechteilnehmers [endet]“ (2943); mittlerweile jedoch BVerfG NJW 2002, 3619 (3620 f.), wonach „die Reichweite des grundrechtlichen Schutzes […] nicht am so genannten Endgerät der Telekommunikationsanlage [endet]“ (3620).

134 Vgl. BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 8; für den Zugriff im Rahmen von Quellen-TKÜ-Maßnahmen führt dieser unter Rn. 107c aus, dass der Kommunikationsvorgang zum Zeitpunkt der Verschlüsselung „möglicherweise noch nicht begonnen hat“, diese aber als „Vorstufe“ dem Kommunikationsvorgang zuzurechnen sei.

135 Vgl. BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 8; in diese Richtung wohl auch *Käß*, BayVBl. 2010, 1 (6), wonach es maßgeblich darauf ankomme, dass eine Fernkommunikation unter Nutzung von technischen Mitteln vorliegt.

136 BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 8; vgl. auch BVerfG NJW 2002, 3619 (3621).

Überwachung könne auch das Endgerät sein. Durch § 100b II S. 2 Nr. 2 StPO finde das Endgerät nunmehr auch ausdrücklich Erwähnung.[137]

Gemäß dem hieran anknüpfenden Ansatz einer verbreiteten Sichtweise handelt es sich bei IP-basierter Sprachübertragung in Echtzeit um eine Übertragung von Signalen i. S. d. § 3 Nr. 22 TKG, also um das Aussenden, Übermitteln und Empfangen von Signalen mittels Telekommunikationsanlagen und mithin um Telekommunikation, weshalb für einen Zugriff grds. auch der Anwendungsbereich der Telekommunikationsüberwachung nach §§ 100a, 100b StPO eröffnet sei.[138] Dem stehe insbesondere auch nicht das Argument entgegen, dass der Zugriff auf die uncodierten Daten bei einer Quellen-TKÜ auf dem jeweiligen Endgerät erfolge und noch nicht (bzw. nicht mehr) im Rahmen der Nachrichtenübermittlung im Leitungsnetz eines TK-Anbieters. Gemäß *Bär* ist Voraussetzung für die Überwachung nach § 100a I StPO nämlich nur, dass sich eine Person zum Betreiben von Kommunikation einer Telekommunikationsanlage bediene, also „Kommunikation mittels einer solchen Anlage vornimmt“[139].[140] Soweit durch die verwendete Überwachungssoftware gewährleistet werden könne, dass die Überwachung ausschließlich Daten aus laufenden Telekommunikationsvorgängen erfasst und durch entsprechende technische Vorkehrungen sichergestellt wird, dass keine sonstigen Daten wie z. B. auf der Festplatte des Zielsystems gespeicherte Dateien erfasst werden[141], sei „der Begriff Quellen-TKÜ berechtigt und eine klare Grenze zur Online-Durchsuchung gezogen“[142].

Diese (im Ergebnis zwar zutreffende[143], für die besondere Konstellation der Quellen-TKÜ in der Herleitung der Tatbestandsvoraussetzung einer *Überwachung und Aufzeichnung von Telekommunikation* i. S. d. § 100a I StPO im Zeitpunkt des Zugriffs mittels Überwachungssoftware „an der Quelle“ aber „verkürzte“) Sichtweise lässt hierbei jedoch eine nähere Auseinandersetzung mit den technischen Besonderheiten der softwarebasierten

---

137 Vgl. *Bär,* MMR 2008, 215 (218); auch Anm. *Bär*, MMR 2010, 267 (268).

138 Vgl. bspw. Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 7a; *Bär*, TK-Überwachung, § 100a StPO, Rn. 32; BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 31, 107c; AG Bayreuth, MMR 2010, 266; LG Hamburg, MMR 2011, 693; LG Landshut, MMR 2011, 690.

139 BGH NJW 2003, 2034 (2035).

140 *Bär*, TK-Überwachung, § 100a StPO, Rn. 32 unter Verweis auf BGH NJW 1983, 1569 (1569) und BGH NJW 2003, 2034 (2035).

141 Vgl. *Bär*, TK-Überwachung, § 100a StPO, Rn. 32.

142 *Bär*, TK-Überwachung, § 100a StPO, Rn. 32, mit Verweis auf BT-Drs. 16/6885, S. 3 sowie BT-Drs. 16/7279, S. 3.

143 Wie die Ausführungen der vorliegenden Arbeit zur Frage des Vorliegens von Telekommunikation im Zugriffszeitpunkt anhand einer vertieften dogmatischen Auseinandersetzung unter 3. Teil A.I.1.a)aa) zeigen werden.

Internettelefonie sowie der technischen Zugriffsweise der Überwachungssoftware auf dem betroffenen System im Rahmen einer Quellen-TKÜ – welche gerade auch zur erforderlichen Abgrenzung zu Maßnahmen der Online-Durchsuchung[144] angezeigt ist – vermissen, wenn (sinngemäß) allein damit argumentiert wird, dass es sich bei Sprachtelefonie via Internetprotokoll um eine (moderne) Telekommunikationsform handele, technischer Anknüpfungspunkt einer Überwachung auch das Endgerät sein könne und deshalb der Zugriff mittels Quellen-TKÜ eine Überwachung und Aufzeichnung von Telekommunikation i. S. d. § 100a I StPO sei. Denn auch das E-Mailing oder Instant Messaging stellen bspw. Formen von *Telekommunikation* dar, für deren grundrechtlichen Schutz[145] wie auch die Frage der Einschlägigkeit von strafprozessualen Eingriffsbefugnissen[146] es aber entscheidend darauf ankommt, zu welchem Zeitpunkt auf entsprechende Daten der jeweiligen Kommunikation zugegriffen wird. Auch aus dem Umstand, dass VoIP-Telefonie in Echtzeit abläuft, kann nicht bereits automatisch – wie es gerade auch die geäußerten Bedenken in Bezug auf den Zugriffszeitpunkt bei der Quellen-TKÜ deutlich machen[147] – geschlussfolgert werden, dass in den Fällen verschlüsselter VoIP-Telefonie im Moment der spezifischen Abgreifsituation der (unverschlüsselten) Daten mittels spezieller Überwachungssoftware auf dem jeweiligen informationstechnischen System (schon bzw. noch) Telekommunikation vorliegt. Denn nur weil eine bestimmte Kommunikationsart als Telekommunikation i. S. d. § 100a I StPO bezeichnet werden kann, ist nach zutreffender Auffassung „damit […] aber noch nicht gesagt, dass sämtliche Ermittlungsmaßnahmen, die irgendwie im Zusammenhang mit dieser Kommunikationsform stehen, als Überwachung der Telekommunikation erfasst werden können“[148]. Vielmehr ist „für jeden Eingriff nach allgemeinen Auslegungsgrundsätzen zu prüfen, ob das spezifische Vorgehen von der Befugnisnorm gedeckt ist“[149]. Deshalb ist es auch für die Situation der Quellen-TKÜ notwendig zu prüfen und zu begründen, ob an dem „Ort“, an dem der Zugriff realisiert wird (hier: das jeweilige informationstechnischen System), und zu dem Zeitpunkt, zu welchem der Zugriff stattfindet (hier: vor Verschlüsselung bzw. nach Entschlüsselung), unter Berücksichtigung der technischen Besonderheiten softwarebasierter Internettelefonie der Begriff der *Telekommunikation* noch Berechtigung findet und (bereits bzw. noch) ein Vorgang des Aussendens, Übermittelns

144 Hierzu BVerfG NJW 2008, 822.

145 Vgl. BVerfG NJW 2006, 976.

146 Vgl. hierzu LG Landshut, MMR 2011, 690; für Einzelheiten zur Entscheidung des LG Landshut, siehe auch 2. Teil A.II.4.

147 Vgl. *Becker*/*Meinicke*, StV 2011, 50 (51).

148 *Kudlich*, JuS 2001, 1165 (1167).

149 *Kudlich*, JuS 2001, 1165 (1167).

und Empfangens von als Nachrichten identifizierbaren Signalen i. S. d. charakteristischen Begriffsverständnisses nach § 3 Nr. 22, 23 TKG gegeben ist, welcher von der Überwachungssoftware erfasst wird.

Dass bei IP-basierter Signalübertragung in Echtzeit das Vorliegen eines Überwachens und Aufzeichnens von *Telekommunikation* im Zugriffszeitpunkt der Quellen-TKÜ nicht ohne weiteres als selbstverständlich anzunehmen ist, zeigen auch die vorhandenen kritischen Stimmen aus Rspr. und Schrifttum, die sich mit ihrer Argumentation auf den Standpunkt stellen, dass der Zugriff auf die Signale bei der Quellen-TKÜ „gerade vor dem Aussenden bzw. nach dem Empfang“[150] erfolge, und es deshalb „bereits fraglich“[151] sei, „ob die bei einer Quellen-TKÜ erhobenen Daten überhaupt als ‚Telekommunikation‘ anzusehen sind“[152].

Diese Kritik bedarf einer näheren dogmatischen Abklärung, denn eine Quellen-TKÜ ließe sich bspw. dann nicht auf eine (am Maßstab des Art. 10 I GG ausgerichtete) Eingriffsbefugnis wie § 100a I StPO zur Überwachung und Aufzeichnung von Telekommunikation stützen, wenn im Zuge der Umsetzung auf Daten zugegriffen werden würde, die sich außerhalb des Aussendens, Übermittelns und Empfangens von als Nachrichten identifizierbaren Signalen mittels Telekommunikationsanlagen (vgl. § 3 Nr. 22, 23 TKG) befinden, da insoweit ein Telekommunikationsvorgang noch nicht vorliegen würde bzw. (beim Anknüpfen am Empfängersystem) bereits beendet wäre und die Überwachungssoftware auf dem betroffenen informationstechnischen System dann keine *Telekommunikation* überwachen und aufzeichnen würde, sondern ggf. noch bzw. bereits Daten außerhalb laufender Telekommunikationsvorgänge.

Den Stimmen, die dem Vorliegen einer Überwachung und Aufzeichnung von *Telekommunikation* im Zugriffszeitpunkt einer Quellen-TKÜ kritisch gegenüberstehen, lässt sich aber – da das Vorliegen von Telekommunikation im Zugriffszeitpunkt, wie die Untersuchungen im Rahmen vorliegender Arbeit zeigen werden, im Ergebnis zu Recht angenommen wird – ein Argumentationsansatz gegenüberstellen, der anhand der spezifischen Besonderheit des technischen Ablauf der softwarebasierten Internettelefonie das Vorliegen von *Telekommunikation* im Moment des Abgreifens der Daten „an der Quelle“ darlegt. Die spezifischen technischen Abläufe der softwareba-

---

150 *Becker*/*Meinicke*, StV 2011, 50 (51).

151 *Becker*/*Meinicke*, StV 2011, 50 (51).

152 *Becker*/*Meinicke*, StV 2011, 50 (51); in diese Richtung, i. E. aber offengelassen, auch LG Hamburg, MMR 2008, 423 (424); diese Problematik anschneidend auch BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 107c, der den Kommunikationsvorgang zum Zeitpunkt der Verschlüsselung als „möglicherweise“ noch nicht begonnen ansieht, diese aber als „Vorstufe“ dem Kommunikationsvorgang zurechnet.

sierten Internettelefonie gestatten insofern (zugunsten der Annahme eines Vorliegens von Telekommunikation im Zugriffszeitpunkt) den Schluss, dass auch in dem Moment, in dem die Quellen-TKÜ ansetzt, *bereits* (bei einem Ansetzen am Absendersystem) bzw. *noch* (bei einem Ansetzen am Empfängersystem) *Telekommunikation* vorliegt, welche überwacht und aufgezeichnet wird.

Dieser Ansatz, der von vorliegender Arbeit verfolgt und in Teil 3 unter dogmatischen Gesichtspunkten im Einzelnen erörtert wird[153], richtet den Fokus hierbei verstärkt auf die – neben dem technischen Vorgang des Übermittelns der Signale für einen Telekommunikationsvorgang gleichermaßen charakteristischen – technischen Vorgänge des *Aussendens* und *Empfangens*[154] und wie sich diese Vorgänge bei der maßnahmegegenständlichen softwarebasierten Internettelefonie unter Berücksichtigung deren spezifischer technischer Abläufe darstellen.

4. Problem: Anfertigen von Screenshots

Ein mit der Frage des Vorliegens einer Überwachung von *Telekommunikation* in Zusammenhang stehendes Sonderproblem ist die Frage, ob sich auch ein Anfertigen sog. *Screenshots*, also Kopien von grafischen Bildschirminhalten, auf eine Befugnisnorm zur Durchführung von Quellen-TKÜ-Maßnahmen stützen lässt. Mit dieser Frage hatte sich jüngst das LG Landshut in seiner Entscheidung vom 20.01.2011[155] zu beschäftigen.

Beim Anfertigen von Screenshots erfolgt ein „Ablichten“ (Kopieren) und Speichern des im Zeitpunkt des Screenshots aktuellen, aktiven grafischen Bildschirminhaltes als Grafikdatei bzw. Grafikdateien[156]. Mittels derartiger „Bildschirmablichtungen“ (auch „Bildschirmfotografien“) lassen sich sowohl das aktuelle, grafisch am Bildschirm sichtbare Einhabeverhalten des Nutzer des überwachten Systems wie auch die im Zeitpunkt des Zugriffs auf der Bildschirmoberfläche grafisch stattfinden Abläufe in Erfahrung bringen.

Der Entscheidung des LG Landshut im Rahmen einer sofortigen Beschwerde gemäß § 101 VII S. 3 StPO gegen die amtsgerichtliche Zurückweisung des Antrags des Beschuldigten auf Feststellung der Rechtswidrigkeit der Maßnahme als unbegründet nach § 101 VII S. 2 StPO lag hierbei als Sachverhalt zugrunde, dass im Rahmen des Vollzugs eines Beschlusses

---

153 Siehe 3. Teil A.I.1.a)aa).

154 Vgl. § 3 Nr. 22, 23 TKG.

155 LG Landshut, Beschluss vom 20.01.2011, 4 Qs 346/10, MMR 2011, 690.

156 Bei konstanter Anfertigung von Screenshots in regelmäßigen Intervallen über einen bestimmten Zeitraum hinweg.

des AG Landhut zur „Überwachung und Aufzeichnung des Telekommunikationsverkehrs“ einschließlich (u. a.) der über den in der Anordnung genannten Anschluss geführten „verschlüsselten Telekommunikation“ (hier sowohl Internettelefonie/VoIP als auch Chat/Instant Messaging via Skype) und der „Vornahme der hierzu erforderlichen Maßnahmen i. R. e. Fernsteuerung“ die von den durchführenden Behörden installierte Überwachungssoftware neben der Überwachung und Ausleitung der verschlüsselt geführten Telekommunikation via Skype vor Ver- bzw. nach Entschlüsselung auch Screenshots der Skype-Software sowie des Internet-Browsers[157] im Intervall von 30 Sekunden angefertigt hatte.[158]

Dogmatischer Knackpunkt dieses Sachverhaltes ist hierbei die Frage, ob das Anfertigen von Screenshots der Skype-Software und des Internet-Browsers zur Erfassung des auf dem Bildschirm grafisch sichtbaren Eingabeverhaltens des Beschuldigten im Rahmen der Nutzung der Instant Messaging-Funktion der Skype-Software zum Sofortversand von Textnachrichten („Chatten“) im Zeitpunkt des Zugriffs ein Überwachen und Aufzeichnen von *Telekommunikation* darstellt, ob also zum Zeitpunkt dieser Maßnahmen bereits Telekommunikation stattfindet, welche in zulässiger Weise auf Grundlage der §§ 100a, 100b StPO abgegriffen werden darf, oder aber eine solche noch nicht eingeleitet ist:

Wie bereits im vorhergehenden Punkt eingehend dargestellt, gestattet die Eingriffsbefugnis des § 100a I StPO nur ein Überwachen und Aufzeichnen von *Telekommunikation*. Zu einem Erfassen sonstiger Daten ohne Bezug zu den spezifischen technischen Vorgängen einer Telekommunikation in Form des Aussendens, Übermittelns und Empfanges von als Nachrichten identifizierbaren Signalen mittels Telekommunikationsanlagen[159] legitimieren die Eingriffbefugnisse der §§ 100a, 100b StPO sowohl hinsichtlich ihrer grundrechtlichen Schrankenwirkung als auch mit Blick auf ihre tatbestandlichen Voraussetzungen und die damit begründete Rechtsfolgenwirkung gerade nicht.

Das LG Landshut stellt hierzu fest, dass „zwar […] der Beschluss des AG [zur Überwachung und Aufzeichnung des Telekommunikationsverkehrs einschließlich der verschlüsselten Telekommunikation sowie der Vornahme der hierzu erforderlichen Maßnahmen i. R. e. Fernsteuerung, Anm. d. Verf.] […] nicht rechtswidrig [ist], wohl aber seine Umsetzung, soweit die grafischen Bildschirminhalte kopiert, also sog. Screenshots gefertigt wurden“[160].

---

157 Computerprogramm, mit dem Seiten im World Wide Web dargestellt werden.

158 Vgl. im Einzelnen LG Landshut, MMR 2011, 690.

159 Vgl. § 3 Nr. 22 u. 23 TKG.

160 LG Landshut, MMR 2011, 690 (690).

Das LG Landshut begründet dies damit, dass „für das Kopieren und Speichern der grafischen Bildschirminhalte, also der Fertigung von Screenshots, keine Rechtsgrundlage“[161] bestehe, „weil zum Zeitpunkt dieser Maßnahmen [des Kopierens und Speicherns der grafischen Bildschirminhalte, Anm. d. Verf.] noch kein TK-Vorgang stattfindet“[162]. Hierzu führt das LG insbesondere an, dass „nicht außer Acht gelassen werden [kann], dass – anders als bei der Internettelefonie – die E-Mail [hier wohl genauer: die Textnachricht mittels Instant Messaging, Anm. d. Verf.[163]] zum Zeitpunkt ihrer ‚Ablichtung‘ mittels ‚Screenshot‘ noch nicht unmittelbar vor ihrer Versendung steht, insb. auch wieder geändert oder gelöscht werden könnte“[164]. Weiter stellt das LG fest, dass „zwar […] der Beschuldigte, um eine E-Mail [Textnachricht, Anm. d. Verf.] verfassen zu können, eine Verbindung zu einem Server aufbauen [muss], der ihm die erforderliche Maske zur Verfügung stellt“[165], „der Vorgang des Schreibens der E-Mail [der Textnachricht, Anm. d. Verf.] […] dann aber ohne Datenaustausch statt[findet], da die einzelnen Buchstaben [bei der Eingabe, Anm. d. Verf.] nicht sofort an den Server weiter übertragen werden“[166], sondern „die E-Mail [die Textnachricht, Anm. d. Verf.] […] erst dann zum Server und damit in die Außenwelt transportiert [wird], wenn der Beschuldigte den ‚Versenden-Button‘ betätigt“[167]. Das LG Landshut kommt deshalb zu dem Ergebnis, dass „beim Schreiben einer E-Mail [einer Textnachricht, Anm. d. Verf.] noch nicht von einem Vorgang der Telekommunikation gesprochen werden [kann]“[168]. Hierbei könne „etwas anderes […] auch nicht aus dem Umstand hergeleitet werden, dass der Beschuldigte zunächst, um die E-Mail [die Textnachricht, Anm. d. Verf.] schreiben zu können, eine Internetverbindung herstellt“[169], da „anders als beim Aufbau einer Telefonverbindung […] die Verbindung zum Server nach dem Aufruf der […] Maske nicht weiter genutzt [wird]“[170]. Es finde nämlich „beim Schreiben der E-Mail [der Textnachricht, Anm. d. Verf.] […] gerade kein Datenaustausch mit dem Server [im Sinne eines Telekommunikationsvorgangs, Anm. d. Verf.] statt“[171]. Auch könne „nicht davon gespro-

---

161 LG Landshut, MMR 2011, 690 (691).

162 LG Landshut, MMR 2011, 690 (691).

163 Wobei sich diesbezüglich die Frage des Beginns des Telekommunikationsvorgangs für E-Mailing und Instant Messaging in gleicher Weise stellt.

164 LG Landshut, MMR 2011, 690 (691).

165 LG Landshut, MMR 2011, 690 (691).

166 LG Landshut, MMR 2011, 690 (691).

167 LG Landshut, MMR 2011, 690 (691).

168 LG Landshut, MMR 2011, 690 (691).

169 LG Landshut, MMR 2011, 690 (691).

170 LG Landshut, MMR 2011, 690 (691).

171 LG Landshut, MMR 2011, 690 (691).

chen werden, dass das Schreiben der E-Mail [der Textnachricht, Anm. d. Verf.] so eng mit ihrer späteren Versendung verknüpft ist, dass bereits das Schreiben in der Maske ohne Datenaustausch ein Vorgang der Telekommunikation i. S. d. § 100a StPO wäre“[172], was sich „schon darin [zeigt], dass die E-Mail [die Textnachricht, Anm. d. Verf.] während und nach dem Schreiben stets noch geändert oder gelöscht werden kann“[173].

Der Rechtsauffassung des LG Landshut ist zuzustimmen, da in den Fällen des „Abfotografierens“ von Eingaben des Betroffenen in die Instant Messaging-Maske einer VoIP-Software vor Betätigen des „Versende-Buttons“ ein Vorliegen von Telekommunikation, also des technischen Vorgangs des Aussendens, Übermittelns und Empfangens von als Nachrichten identifizierbaren Signalen i. S. v. § 3 Nr. 22, 23 TKG, zu verneinen ist. Zutreffend führt die Kammer hierzu aus, dass „auch im Lichte der Entscheidung des *BVerfG* zur Unzulässigkeit der Onlinedurchsuchung (NJW 2008, 822 […])“[174] „beim Schreiben einer E-Mail (hier genauer: einer Textnachricht, Anm. d. Verf.] noch nicht von einem Vorgang der Telekommunikation gesprochen werden [kann]“[175], insbesondere wenn „man sich diese technischen Vorgänge vor Augen [hält]“[176].

Diese Sichtweise steht auch in Einklang mit den Ausführungen der vorliegenden Arbeit zum Vorliegen von Telekommunikation im Zugriffszeitpunkt bei der Überwachung verschlüsselter Internettelefonie[177], da anders als beim Abgreifen laufender Internettelefonie die hier gegenständliche Anfertigung von Screenshots der Bildschirminhalte während der Texteingabe durch den Betroffenen anlässlich des „Eintippens“ des Textes – also nach zutreffender Sichtweise der bloßen Vorbereitung des Versandes von Textnachrichten – noch kein vom Betroffenen nicht mehr beeinflussbarer Telekommunikationsvorgang in Gang gesetzt wurde (da es dem Betroffenen in dieser Phase noch freisteht, darüber zu entscheiden, ob er die eingetippte Nachricht wirklich versenden will oder doch noch davon absieht[178]) und sich die Textnachricht (beim Anknüpfen am Absendersystem) auch noch nicht im Rahmen einer Aussendephase befindet. Ein unumkehrbar eingelei-

---

172 LG Landshut, MMR 2011, 690 (691).

173 LG Landshut, MMR 2011, 690 (691).

174 LG Landshut, MMR 2011, 690 (691).

175 LG Landshut, MMR 2011, 690 (691).

176 LG Landshut, MMR 2011, 690 (691).

177 Für Einzelheiten zum Vorliegen von Telekommunikation im Zugriffszeitpunkt bei der Überwachung von Internettelefonie, siehe 2. Teil A.II.3. sowie 3. Teil A.I.1.a)aa).

178 Anm. *Brodowski*, JR 2011, 533 (536) spricht insoweit treffend von einem bloßen Nachrichten*entwurf*.

teter Telekommunikationsvorgang ist in diesen Fällen – anders als beim Abgreifen laufender Sprach- und/oder Videotelefonie[179] – in der Phase des Schreibens einer Textnachricht *vor* Anklicken des „Versende-Buttons" durch den Nutzer noch nicht gegeben. Wie auch der BGH im Rahmen seiner Entscheidung zur verdeckten Online-Durchsuchung im Strafprozessrecht zutreffend festgestellt hat, „muss der Computerbenutzer bei der Übertragung der zu durchsuchenden Daten an die Ermittlungsbehörde mit Hilfe des aufgespielten Computervirus [zwar] ‚online' sein […]"[180], „jedoch wird dadurch die verdeckte Online-Durchsuchung nicht zur Telekommunikation […], weil nicht die Kommunikation zwischen dem Tatverdächtigen und einem Dritten überwacht […] wird"[181].

Ein solches Anfertigen von Screenshots zum Kopieren und Speichern des jeweiligen grafischen Bildschirminhalts wäre deshalb als Maßnahme zur Überwachung des Eingabeverhaltens des Nutzer nicht als Quellen-TKÜ, sondern vielmehr als eine (im Strafprozessrecht mangels Eingriffsermächtigung gegenwärtig unzulässige[182]) Online-Durchsuchung (bei laufender Anfertigung von Screenshots in regelmäßigen Intervallen in Form der Online-Überwachung[183]) zu qualifizieren[184], welche bereits maßnahmetypisch nicht auf das Überwachen und Aufzeichnen von Daten laufender Telekommunikationsvorgänge ausgerichtet ist, sondern auf das Überwachen und Erfassen generell auf dem betroffenen System gespeicherter Daten bzw. dort ablaufender Datenverarbeitungsprozessen ohne notwendigen Bezug zu einem Datenaustausch mit anderen Rechnern im Rahmen von Telekommunikation[185]. Um einen solchen Zugriff auf die gespeicherten Inhalte bzw. aktiven Prozesse des betroffenen informationstechnischen Systems handelt es sich auch bei dem hier gegenständlichen Anfertigen von Screenshots zum Erfassen des Bildschirminhalts. Eine solche Maßnahme von der Qualität einer Online-Durchsuchung wäre indes auch nicht mehr allein an dem Grundrecht des Fernmeldegeheimnisses aus Art. 10 I GG – in das die Befugnisnorm der §§ 100a, 100b StPO spezifische Eingriffe gestattet – zu messen, sondern würde vielmehr auch den Anwendungsbereich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer System eröffnen[186].

---

179 Siehe hierzu im Einzelnen 3. Teil A.I.1.a)aa).

180 BGH NJW 2007, 930 (931).

181 BGH NJW 2007, 930 (931 f.).

182 So jedenfalls der 3. Strafsenat des Bundesgerichtshofs, Beschluss vom 31.01. 2007, BGH NJW 2007, 930; für Einzelheiten, siehe auch 1. Teil A.II.2.a).

183 Für Einzelheiten zur Online-Durchsuchung, siehe 1. Teil A.II.2.a).

184 Vgl. insoweit zutr. auch *Braun*, jurisPR-ITR 3/2011 Anm. 3.

185 Vgl. auch *Jahn*/*Kudlich*, JR 2007, 57 (60 f.); *Gercke*/*Brunst*, Internetstrafrecht, Kap.5, S. 338, Rn. 855; Anm. *Bär*, MMR 2011, 691 (692).

Die die Textnachrichten beinhaltenden TK-Daten im Rahmen von Instant Messaging oder E-Mailing könnten allerdings – soweit technisch möglich – nach der hier vertretenen Auffassung in gleicher Weise wie die TK-Daten, welche bei Internettelefonie die digitalisierten Sprachsignale enthalten, *nach* dem Betätigen des „Versende-Buttons" im Rahmen der sogleich automatisiert ablaufenden Aussendevorgänge noch vor einer hierbei erfolgenden Verschlüsselung innerhalb eines dann laufenden Telekommunikationsvorgangs durch eine Maßnahme der Quellen-TKÜ auf Grundlage der §§ 100a, 100b StPO in zulässiger Weise abgegriffen werden.

Streng zu unterscheiden von der Überwachung des aktuellen Bildschirminhalts mittels einer Anfertigung von Screenshots hingegen ist das Abgreifen der je nach verwendeter VoIP-Software und Nutzungsweise ggf. zusätzlich zu den Audio-Signalen übertragenen Video-Signale (*Video-Internettelefonie*). Auch anfallende Video-Signale einer Internettelefonie können – analog zu den ausgetauschten Sprach-Signalen – als Nachrichten identifizierbare Signale mit visuellen Inhalten enthalten und stellen daher wie die Sprach-Signale inhaltsbezogene Daten der jeweiligen Telekommunikation dar[187]. Deshalb können in gleicher (technischer und rechtlicher) Weise wie die Audio-Signale auch die anlässlich eines laufenden Videotelefonats ausgetauschten Video-Signale im Rahmen einer Quellen-TKÜ auf dem überwachten System abgegriffen werden.[188]

5. Umsetzung unter Verwendung technischer Mittel

Bei Vorliegen der materiellen Eingriffsvoraussetzungen des § 100a I Nr. 1 bis Nr. 3, II, IV StPO gestattet § 100a I StPO die Überwachung und Aufzeichnung von Telekommunikation auf die in der jeweiligen Anordnung näher bezeichnete Art und Weise sowie in dem dort festgelegte Umfang für die festgesetzte Dauer (§ 100b II S. 2 Nr. 3 StPO).

Die Durchführung von TKÜ-Maßnahmen – sei es in klassischer[189] oder anderer Weise – erfolgt regelmäßig unter Verwendung *technischer Mittel.* Dass zur Überwachung und Aufzeichnung der Telekommunikation technische Mittel (auch *eigene* technische Mittel der Strafverfolgungsbehörden

---

186 Vgl. auch Anm. *Bär*, MMR 2011, 691 (692).

187 Vgl. auch Anm. *Bär*, MMR 2011, 691 (693); so zutr. auch LG Hamburg, MMR 2011, 693 (693 f.); zust. auch *Albrecht*/*Dienst*, JurPC Web-Dok. 5/2012, Abs. 21.

188 Für weitere Einzelheiten zu Video-Internettelefonie, siehe auch 1. Teil A.I.2.c), d) u. e).

189 In Form des Ausleitens einer Kopie der auf dem Transportweg abgefangenen Daten durch den Netzbetreiber an die Ermittlungsbehörden.

nach Maßgabe der gerichtlichen Anordnungsentscheidung[190]) eingesetzt werden dürfen, ist in der Gesetzesvorschrift zwar nicht ausdrücklich genannt, ergibt sich jedoch nach der in der Gesetzesbegründung niedergelegten Auffassung des Gesetzgeber bereits aus § 100a I StPO selbst[191], da „das dort ausdrücklich erlaubte Überwachen und Aufzeichnen von Telekommunikation regelmäßig nur unter Einsatz technischer Mittel erfolgen kann“[192]. Zudem weisen auch die Worte „Überwachen“ und „Aufzeichnen“ auf die Bewirkung der Maßnahme mit technischen Mitteln hin. Nach zutreffender Auffassung kann hierbei technischer Anknüpfungspunkt der Überwachung auch das jeweilige Endgerät des Teilnehmers sein.[193] Etwas anderes ergibt sich auch nicht aus der Gesetzesbegründung, da § 100a I StPO vielmehr „eine nicht durch die Mitwirkung der Telekommunikationsdienstleister bedingte Befugnis, Telekommunikation zu überwachen und aufzuzeichnen [enthält]“[194], welche „lediglich durch die in der gerichtlichen Anordnungsentscheidung näher zu bestimmende Art der Überwachung (vgl. § 100b Abs. 2 Satz 2 Nr. 3 StPO-E) [beschränkt wird]“[195].

Wie die Aussagen des Gesetzgebers verdeutlichen, sind für die Überwachung und Aufzeichnung von Telekommunikation nach § 100a I StPO somit solche technischen Mittel einzusetzen, die – unter dem Eindruck der Ermächtigungsgrundlage – in technischer Hinsicht ein Überwachen und Auf-

---

190 Vgl. BT-Drs. 16/5846, S. 47.

191 Vgl. BT-Drs. 16/5846, S. 47.

192 BT-Drs. 16/5846, S. 47.

193 Vgl. BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 8; auch *Bär*, TK-Überwachung, § 100a StPO, Rn. 32, zumal nunmehr auch in der Vorschrift des § 100b II S. 2 Nr. 2 StPO das Endgerät erwähnt wird; hierauf weist auch *Kudlich*, GA 2011, 193 (207) hin; die Kritik von *Klesczewski*, ZStW 2011, 737 (743), wonach der Gesetzgeber mit dieser Vorschrift lediglich die Überwachung von Mobiltelefonen auch bei wechselnden SIM-Karten ermöglichen wollte, greift im Ergebnis nicht durch, da die Neuregelung ausweislich der Gesetzesbegründung (BT-Drs. 16/5846, S. 46) dieser Konstellation zwar „Rechnung [trägt]“ (S. 46), jedoch vom Gesetzgeber so (entwicklungs-)offen formuliert wurde, dass hiervon nicht automatisch auf einen Willen des Gesetzgebers zu schließen ist, andere Kommunikationstechniken, die unter besonderer Einbindung von Endgeräten in die jeweiligen Telekommunikationsvorgänge stattfinden, von dem Geltungsbereich der Vorschrift auszuschließen; zur dogmatischen Begründung, dass es sich im Zeitpunkt des Zugriffs auf dem Endgerät in den Fällen der Quellen-TKÜ schon bzw. noch um ein *Überwachen und Aufzeichnen von Telekommunikation* i. S. d. § 100a I StPO handelt, siehe 3. Teil A.I.1.a)aa).

194 Vgl. BT-Drs. 16/5846, S. 47.

195 Vgl. BT-Drs. 16/5846, S. 47; ausweislich der Gesetzesbegründung betreffen die Konkretisierungen in der Anordnung (§ 100b II S. 2 Nr. 3 StPO) ausdrücklich „auch die Art des technischen Zugriffs auf die zu überwachende Telekommunikation“ (S. 47), wodurch sich die Maßnahme zielgerichtet einsetzen lässt.

zeichnen der Telekommunikation im konkreten Fall ermöglichen. Mit welchem konkreten technischen Mittel die jeweilige Überwachung zu realisieren ist oder bspw. wie und worauf die Aufzeichnung stattzufinden hat, schreibt die Befugnisnorm nicht vor. Vielfältige Telekommunikationsformen erfordern spezifisch daran und darauf ausgerichtete technische Überwachungsmittel, die nicht alle – nicht zuletzt auch um dem Gebot der Normenklarheit gerecht zu werden[196] – in der Ermächtigungsgrundlage auch ausdrücklich geregelt werden können. Dies ist gerade bei einer Befugnisnorm wie den §§ 100a, 100b StPO zur Telekommunikationsüberwachung, die in gesteigertem Maße mit der technologischen Entwicklung verknüpft ist, immanent und vom Gesetzgeber auch bewusst in Kauf genommen.[197] So betreffen nach Auffassung des Gesetzgeber die Konkretisierungen in der Anordnung (§ 100b II S. 2 Nr. 3 StPO) ausdrücklich „auch die Art des technischen Zugriffs auf die zu überwachende Telekommunikation“[198]. Dass der Gesetzgeber dem Rechtsanwender bei der Wahl des technischen Mittels einen gewissen Beurteilungsspielraum und ein gewisses Auswahlermessen ein-

---

196 Für Einzelheiten zum Gebot der Normenklarheit und Tatbestandsbestimmtheit, siehe 2. Teil A.II.1.b); generell zum Bestimmtheitsgebot, siehe 2. Teil A.II.1.

197 Aus diesem Grunde überzeugt auch nicht das Argument von *Klesczewski*, ZStW 2011, 737 (747), wonach aus dem Gegenschluss zu § 20l BKAG darauf geschlossen werden müsste, dass der Gesetzgeber durch die (bislang) nicht erfolgte Aufnahme einer entsprechenden Regelung in die StPO zum Ausdruck bringe, die Quellen-TKÜ im Strafverfahren derzeit noch nicht zulassen zu wollen; denn allein der Umstand, dass das BKAG in § 20l II eine ausdrückliche, ggf. „mustergültige“ Regelung der Quellen-TKÜ enthält, mit der der Gesetzgeber die Quellen-TKÜ unter dem Eindruck des Urteils des BVerfG vom 27.02.2008 (BVerfG NJW 2008, 822) möglicherweise lediglich „besonders gut“ regeln wollte, bedeutet nicht, dass eine entwicklungsoffen und technikneutral gehaltene Regelung wie die §§ 100a, 100b StPO zur Überwachung und Aufzeichnung von Telekommunikation nicht ausreichend sein kann, um eine derartige Maßnahme zu legitimieren; vielmehr hat der Gesetzgeber durch die offene Fassung der §§ 100a, 100b StPO gerade zum Ausdruck gebracht, hierunter im Einzelfall – je nach genutzter Telekommunikationsweise – den Einsatz verschiedener Vorgehensweisen zur Überwachung und Aufzeichnung von Telekommunikation zu fassen und hierfür gerade auch technische Mittel zuzulassen; dies verdeutlicht auch der Blick auf die unterschiedliche Handhabe der präventiven Quellen-TKÜ in den Landespolizeigesetzen, da auch dort teilweise eine ausdrückliche Regelung gewählt wurde, teilweise aber auch die bestehenden Regelungen zur Telekommunikationsüberwachung für eine Maßnahme der Quellen-TKÜ als ausreichend erachtet werden (vgl. bspw. Art. 34a BayPAG, 2. Teil A.I.1.e); siehe zu dem (i. E. nicht überzeugenden) systematischen Argument auch die Ausführungen unter 2. Teil A.I.2.; ob es hingegen ggf. sachgerechter bzw. zur Vermeidung weiterer rechtlicher Unsicherheiten wünschenswert wäre (so Anm. *Bär*, MMR 2011, 691, 693), die Quellen-TKÜ in der StPO gesetzlich klarzustellen, steht wiederum auf einem anderen Blatt, vgl. hierzu 3. Teil B.III.

198 Vgl. BT-Drs. 16/5846, S. 47, wodurch insbesondere auch ein zielgerichteter Einsatz der Maßnahme erreicht werde.

räumt, ist gerade Ausdruck und Konsequenz einer *technologieneutralen* und *entwicklungsoffenen Formulierung*[199], wie sie der Gesetzgeber für die §§ 100a, 100b StPO gewählt hat.

Im Rahmen einer Überwachung und Aufzeichnung von Telekommunikation kann deshalb grds. auch der Einsatz einer *spezielle Software* als technisches Mittel im Rahmen der Primärmaßnahme in Betracht kommen. Eine vertiefte Auseinandersetzung mit dieser Frage ist Gegenstand der Untersuchungen im Rahmen der Erörterungen zur Frage der Zulässigkeit der Quellen-TKÜ auf Grundlage der §§ 100a, 100b StPO de lege lata in Teil 3 der Arbeit.[200]

6. Mitwirkung Dritter erforderlich (§ 100b III StPO)?

Der Durchführung einer Überwachung und Aufzeichnung von Telekommunikation mittels einer Überwachungssoftware als eigenes technisches Mittel der Strafverfolgungsbehörden würde es grds. entgegenstehen, wenn für Überwachungsmaßnahmen nach §§ 100a, 100b StPO von Gesetzes wegen die Mitwirkung Dritter erforderlich wäre. Dies könnte sich mithin aus den Vorschriften des § 100b III StPO ergeben.

Zum Zwecke effektiver Umsetzung von TKÜ-Maßnahmen nach § 100a I StPO[201] verpflichtet § 100b III S. 1 StPO jeden, der Telekommunikationsdienste erbringt[202] oder daran mitwirkt, dem Gericht, der Staatsanwaltschaft und ihren polizeilichen Ermittlungspersonen die Maßnahmen nach § 100a I StPO zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen. Für die Frage, ob und in welchem Umfang für die Verpflichtungen nach § 100b III S. 1 StPO Vorkehrungen zu treffen sind, bestimmt sich gemäß § 100b III S. 2 StPO nach dem TKG sowie der TKÜV.

Der gesetzlich vorgesehene Umfang der Mitwirkungspflichten ist im Rahmen der einschlägigen Regelungen der StPO, des TKG sowie der TKÜV für die Durchführung von Ermittlungsmaßnahmen der Telekommunikationsüberwachung zweistufig geregelt:

---

199 Vgl. BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 2 u. 6; vgl. auch *Kudlich*, JuS 2001, 1165 (1166) m. w. N.; *ders*., JA 2010, 310 (312).

200 Für Einzelheiten zur Überwachungssoftware als technisches Mittel, siehe 3. Teil A.I.1.a)bb); zur Frage des Einbringens/Installierens des technischen Mittels vor Durchführung der Überwachungsmaßnahme als notwendige Begleitmaßnahmen und der hierfür einschlägigen Rechtsgrundlagen, siehe 2. Teil B.III.

201 Vgl. BT-Drs. 16/5846, S. 47.

202 Die bisherige Beschränkung auf „geschäftsmäßige" Erbringer von Telekommunikationsdiensten ist mit der Gesetzesnovellierung (BGBl. I S. 3198) zum 01.01.2008 entfallen.

Auf *Stufe 1* der gesetzlich festgelegten Mitwirkungspflichten sind nach § 100b III S. 1 StPO dem Gericht und den für die Umsetzung der richterlichen Beschlüsse verantwortlichen Ermittlungsbehörden die Überwachung und Aufzeichnung der Telekommunikation nach § 100a I StPO *zu ermöglichen* und die hierzu ggf. erforderlichen *Auskünfte* unverzüglich zu erteilen. Dies geschieht im Regelfall durch Ausleitung einer Kopie der auf der Übermittlungsstrecke abgefangenen Telekommunikationssignale an die Ermittlungsbehörden.[203] Der Verpflichtung nach § 100b III S. 1 StPO als „Grundstufe" der Mitwirkung unterliegt 1. jeder Erbringer von Telekommunikationsdiensten – und zwar unabhängig von einer geschäftsmäßigen Erbringung i. S. d. § 3 Nr. 10 TKG[204] – sowie 2. jeder an der Erbringung solcher Dienste Mitwirkende.

Der höhere Mitwirkungsgrad des § 100b III S. 2 StPO stellt als *Stufe 2* die Verpflichtung auf *Vorkehrungen* für die nach S. 1 bestehenden Pflichten zu treffen – ohne dass hiervon die Regelung des § 100b III StPO S. 1 StPO berührt wird (vgl. § 110 I S. 6 TKG sowie § 3 II S. 4 TKÜV). Die im Rahmen dieser erhöhten Mitwirkungsstufe u. a. bestehende Pflicht, zum Zwecke einer unverzüglichen Umsetzung von Überwachungsmaßnahmen ab Betriebsaufnahme auf eigene Kosten technische Einrichtungen (Überwachungseinrichtungen) vorzuhalten und organisatorische Vorkehrungen zu treffen (vgl. § 110 I S. 1 Nr. 1 TKG), besteht gemäß § 100b III S. 2 StPO i. V. m. § 110 I S. 1, II TKG, § 3 I TKÜV für Betreiber von Telekommunikationsanlagen i. S. d. § 2 Nr. 4 TKÜV[205], mit denen öffentlich zugängliche Telekommunikationsdienste[206] erbracht werden und an die mehr als 10.000 Teilnehmer[207] angeschlossen sind. Zudem enthält § 110 I S. 1 Nr. 1a TKG für Betreiber von Telekommunikationsanlagen i. S. d. § 110 I S. 1 TKG in Bezug auf neue Technologien nunmehr auch die Verpflichtung, „in Fällen,

---

203 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100b, Rn. 8; vgl. auch BT-Drs. 16/5846, S. 47.

204 Zur Mitwirkung verpflichtet sind nach § 100b III S. 1 StPO, § 110 I S. 6 TKG seit 01.01.2008 auch solche Telekommunikationsdienstleister, die ihre Dienste nicht geschäftsmäßig i. S. d. § 3 Nr. 10 TKG erbringen.

205 Für denjenigen, der öffentlich zugängliche Telekommunikationsdienste erbringt, ohne hierfür eine Telekommunikationsanlage zu betreiben, bestehen bestimmte „Vergewisserungspflichten" nach § 110 I S. 2 TKG bei der Auswahl des Betreibers.

206 Zur Vereinheitlichung mit der Bezeichnung in den Richtlinienvorgaben spricht das TKG in neuer Terminologie mittlerweile statt von Telekommunikationsdiensten „für die Öffentlichkeit" von „öffentlich zugänglichen" Telekommunikationsdiensten, vgl. § 110 I S. 1, S. 2 TKG i.d. ab dem 10.05.2012 geltenden Fassung (BGBl. I S. 958); eine inhaltliche Änderung ist mit der neuen Begriffswahl indes nicht verbunden, vgl. BT-Drs. 17/5707, S. 91, 50.

207 Vgl. den Befreiungstatbestand des § 3 II S. 1 Nr. 5 TKÜV.

in denen die Überwachbarkeit nur durch das Zusammenwirken von zwei oder mehreren Telekommunikationsanlagen sichergestellt werden kann, die dazu erforderlichen automatischen Steuerungsmöglichkeiten zur Erfassung und Ausleitung der zu überwachenden Telekommunikation in seiner Telekommunikationsanlage bereitzustellen sowie eine derartige Steuerung zu ermöglichen". Die im Jahr 2007 in § 110 I S. 1 TKG eingefügte Nr. 1a[208] bezieht sich hierbei ausweislich der Gesetzesbegründung[209] auf Telekommunikationsdienste, bei denen die zur Steuerung der Telekommunikation erforderlichen Signale und die den Nachrichteninhalt repräsentierenden Signale „über völlig voneinander getrennte Telekommunikationsanlagen übermittelt werden".[210] Die Vorschrift dient der Klarstellung, dass auch im Zusammenhang mit Telekommunikationsdiensten, die auf neuen Technologien beruhen, von Betreibern i. S. d. § 110 I S. 1 TKG technische Einrichtungen zur Umsetzung gesetzlich vorgesehener Maßnahmen zur Überwachung von Telekommunikation vorzuhalten sind. Die Gesetzesbegründung nennt hierbei ausdrücklich auch den Fall der „VoIP-Telefonie" als Beispiel[211]. Durch die Vorschrift wird verdeutlicht „dass sich sowohl die Industrie als auch die Betreiber bei der Suche nach geeigneten technischen Lösungen zur Sicherstellung der Überwachbarkeit für diese modernen Telekommunikationstechnologien darauf einstellen können, auch neue, bisher ungewohnte Lösungsansätze zu verfolgen"[212]. Die Regelung des § 110 I S. 1 Nr. 1a TKG wird wiederum von der Vorschrift des § 3 II S. 3 TKÜV aufgegriffen, die den nach § 110 I S. 1 Nr. 1a TKG zum Treffen von Vorkehrungen für die Umsetzung von Überwachungsmaßnahmen Verpflichteten von den Befreiungstatbeständen des § 3 II S. 1 Nr. 1 und Nr. 2 TKÜV ausnimmt, um ein Leerlaufen des § 110 I S. 1 Nr. 1a TKG zu verhindern.[213] Relevanz entfaltet diese Regelung bezüglich unverschlüsselt übermittelter (anschlussbasierter) VoIP-Dienste (bspw. VoIP über das herkömmliche Telefon mittels VoIP-fähigen Routers[214]), da hier eine Inanspruchnahme der Betreiber[215] und ein

---

208 § 110 I S. 1 Nr. 1a TKG eingefügt m. W. v. 24.02.2007 durch das Gesetz zur Änderung telekommunikationsrechtlicher Vorschriften vom 18. Februar 2007 (BGBl. I S. 106).

209 BT-Drs. 16/2581.

210 BT-Drs. 16/2581, S. 28.

211 Vgl. BT-Drs. 16/2581, S. 28 sowie BR-Drs. 359/06, S. 52, jedoch ohne nähere Differenzierung der „VoIP-Telefonie" nach deren verschiedenen Erscheinungsformen und unterschiedlichen Dienstfunktionen.

212 BR-Drs. 359/06, S. 52.

213 Vgl. BT-Drs. 16/5846, S. 78.

214 Siehe hierzu 1. Teil A.I.2.a) u. b).

215 Bei den Anbietern anschlussbasierter VoIP liegt i. d. R. die Eigenschaft als „*Betreiber einer Telekommunikationsanlage mit der öffentlich zugängliche Telekommunikationsdienste erbracht werden"* i. S. d. § 110 I S. 1 TKG vor; anders stellt sich

Abgreifen der (uncodierten) TK-Daten auf der Transportstrecke erfolgversprechend erscheint.[216]

Ein Unternehmen, das öffentlich zugängliche Telekommunikationsdienste erbringt, ohne zugleich i. S. d. § 110 I S. 1 TKG eine Telekommunikationsanlage zu betreiben, wird von den Verpflichtungen allerdings nicht gänzlich freigestellt. Es muss sich gemäß § 110 I S. 2 TKG bei der Auswahl des jeweiligen Betreibers der genutzten Telekommunikationsanlage nämlich vergewissern, dass dieser dazu in der Lage ist, Anordnungen zur Überwachung der Telekommunikation unverzüglich umzusetzen.

Für die abgestuften Mitwirkungspflichten knüpft das Gesetz in Bezug auf die verpflichteten Dritten somit an *verschiedene Begriffe* an und unterscheidet diesbezüglich zwischen dem „*Erbringer von Telekommunikationsdiensten*" (§ 100b III S. 1 Alt. 1 StPO), dem „*daran Mitwirkenden*" (§ 100b III S. 1 Alt. 2 StPO), dem „*Betreiber einer Telekommunikationsanlage mit öffentlich zugänglichen Telekommunikationsdiensten*" (§ 110 I S. 1 TKG) sowie dem „*Erbringer von öffentlich zugänglichen Telekommunikationsdiensten ohne hierfür eine Telekommunikationsanlage zu betreiben*" (§ 110 I S. 2 TKG).

Sofern eine Mitwirkungsverpflichtungen nach § 100b III StPO auch für Anbieter von softwarebasierten VoIP-Diensten wie z. B. Skype bestünde (vgl. hierzu nachfolgend Punkt b), könnte die Inpflichtnahme des jeweiligen Anbieters durch die Ermittlungsbehörden prinzipiell eine (u. U. mildere[217]) Alternative zur Quellen-TKÜ für die Ermöglichung eines Zugriffs auf die VoIP-Kommunikation und deren Inhalte darstellen.[218] Es bedarf deshalb

---

dies hingegen bei den Anbietern softwarebasierter VoIP-Dienste dar, siehe 2. Teil A.II.6.b).

216 Auf die Problematik verschlüsselt übermittelter P2P-VoIP-Kommunikation, bei der auf Grund von end-to-end-Verschlüsselung ein Abgreifen auf der Transportstrecke regelmäßig nicht erfolgversprechend ist, geht der Gesetzgeber indes mit keinem Wort ein; die Gesetzesbegründung legt vielmehr nahe, dass sich der Gesetzgeber mit den angesprochenen „technischen Lösungen", die von Betreibern zu suchen sind, allein auf die Problematik der völligen Trennung der zur Steuerung erforderlichen Signalen von den Signalen, die den Nachrichteninhalt repräsentieren, und die sich daraus ergebenden Schwierigkeiten für die Überwachbarkeit der Telekommunikation bezieht.

217 Für Einzelheiten zur Frage der Erforderlichkeit der Quellen-TKÜ in diesem Zusammenhang, siehe 2. Teil B.III. 2.b) sowie 3. Teil A.I.1.c).

218 Schwierigkeiten bereitet indes die end-to-end-Verschlüsselung der Datenpakete, bezüglich derer es gegenwärtig fraglich ist, ob für die zahlreichen auf dem Markt befindlichen VoIP-Programme überhaupt technische Möglichkeiten für eine Umgehung der Verschlüsselungsproblematik bspw. durch Nutzung einer Hintertür oder eines Schlüssels existieren; ggf. müssten – soweit technisch überhaupt möglich und unter technologie- und wettbewerbsfördernden Aspekten sowie Belangen der IT-Si-

zunächst einer näheren Auseinandersetzung mit der Frage, ob und inwieweit sich die gesetzlichen Mitwirkungsverpflichtungen neben den jeweiligen Netzbetreibern/Providern (a) auch auf Anbieter von softwarebasierter VoIP-Kommunikation (b) erstrecken. Hierfür ist ein Unterfallen der Anbieter und der von ihnen erbrachten VoIP-„Dienste“ unter die oben genannten gesetzlichen Begrifflichkeiten zu prüfen.

a) Mitwirkungspflicht Netzbetreiber/Provider

Bei Telekommunikation im Zusammenhang mit der Nutzung des Internets trifft die Pflicht des § 100b III S. 1 StPO, nämlich Maßnahmen nach § 100a StPO zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen, regelmäßig den Netzbetreiber sowie – bei Personenverschiedenheit – daneben auch den Access-Provider[219] des von der Überwachungsmaßnahme betroffenen Internetanschlusses. Die Kernaufgabe des Netzbetreibers liegt im Rahmen von Telekommunikationsvorgängen in der Übertragung der Signale auf IP-Ebene, die des Access-Providers[220] in der Zugangsvermittlung ins Internet. Bei diesen Diensten handelt es sich i. S. d. Begriffsbestimmung des § 3 Nr. 24 TKG (bei Access-Providing jedenfalls auch[221]) um einen Telekommunikationsdienst und bei den Dienstleistern mithin um Erbringer von Telekommunikationsdiensten i. S. d. § 100b III S. 1 StPO.

Neben den Pflichten nach § 100b III S. 1 StPO treffen die Netzbetreiber i. d. R. auch die weitergehenden Verpflichtungen des § 100b III S. 2 StPO i. V. m. § 110 I S. 1, II TKG, § 3 I TKÜV, eigene Vorkehrungen für die Ermöglichung von Maßnahmen nach § 100a I StPO zu treffen. Denn als Unternehmen, die die tatsächliche Kontrolle über die Funktionen derjenigen technischen Einrichtungen (IP-Infrastruktur) ausüben, welche i. S. d. § 3 Nr. 23 TKG als Nachrichten identifizierbare Signale übertragen (Transport der Datenpakete auf IP-Ebene), handelt es sich bei diesen um Betreiber von

---

cherheit rechtspolitisch erwünscht – für ein „Ermöglichen von Überwachungsmaßnahmen“ i. S. d. § 100b III 1 StPO dann erst entsprechende Zugriffskomponenten durch den VoIP-Diensteanbieter in die Software bzw. in das Verschlüsselungsprotokoll integriert werden.

219 Unternehmen, das den Zugang ins Internet vermittelt und Dienste sowie technische Leistungen anbietet, die für die Nutzung oder den Betrieb von Diensten oder Inhalten im Internet notwendig sind; die Bezeichnung „Access-Provider“ unterfällt als Teilbereich dem Oberbegriff des „Internet-Service-Provider“ als Gesamtdienstleister, oftmals im Sprachgebrauch aber auch nur „Provider“.

220 Der zur (technischen) Realisierung seiner Dienste entsprechende Vertragsvereinbarungen mit einem Netzbetreiber unterhält.

221 Ggf. neben der Einordnung als Telemediendienst, vgl. vertiefend auch *Hoeren*, NJW 2007, 801 (802).

Telekommunikationsanlagen i. S. d. § 2 Nr. 4 TKÜV, mit denen öffentlich zugängliche Telekommunikationsdienste erbracht werden.

Ein Heranziehen des Netzbetreibers ist jedoch für den Zugriff auf die VoIP-Kommunikation bei softwarebasierten P2P-VoIP-Diensten wenig erfolgversprechend. Der Netzbetreiber könnte – und müsste gemäß seiner gesetzlichen Verpflichtung (vgl. § 5 II S. 1 TKÜV) – zwar eine Kopie der durch ihn auf IP-Ebene übertragenen (verschlüsselten) Datenpakete der softwarebasierten VoIP-P2P-Anwendung an die Ermittlungsbehörden ausleiten, die Kopie der Datenpakete würden dann jedoch nur in codierter Form vorliegen, da der Netzbetreiber, der allein den Transport der Datenpakete über ein IP-Netz bewerkstelligt, keinerlei Einsicht in bzw. Funktionsherrschaft über die Verschlüsselungsparameter der Datenpakete und deren Inhalte hat.[222]

b) Exkurs: Mitwirkungspflicht VoIP-Diensteanbieter?

Um der Mitwirkungspflicht des § 100b III S. 1 StPO zu unterfallen, müsste es sich bei Unternehmen, die softwarebasierte VoIP-Dienste anbieten, um „Erbringer von Telekommunikationsdiensten" oder „daran Mitwirkende" handeln. Ob und inwieweit von einer solchen Eigenschaft bei den am Markt befindlichen Anbietern von VoIP-Diensten ausgegangen werden kann, ist bislang nicht abschließend geklärt und bedarf deshalb einer näheren Untersuchung im Rahmen des nachfolgenden Exkurses[223]:

Unter Heranziehung der Definition des § 3 Nr. 24 TKG handelt es sich bei *Telekommunikationsdiensten* um

> „in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen".

Diese Begriffsbestimmung setzt den Begriff des *elektronischen Kommunikationsdienstes* aus Art. 2 lit. c) der Europäischen Rahmenrichtlinie

---

222 Anders stellt es sich dar, wenn der Netzbetreiber und/oder Access-Provider in Kombination mit seinen Zugangsdiensten, bspw. der Bereitstellung eines Breitbandanschlusses, selbst (anschlussbasierte) VoIP-Dienste anbietet (z. B. VoIP mittels Router oder speziellem VoIP-Telefon); hier kann mangels regelmäßiger Verschlüsselung zudem mittels normaler TKÜ auf die Daten zugegriffen werden, siehe hierzu auch 1. Teil A.I.2.a) u. b).

223 Nachfolgend im Schwerpunkt anhand des bekanntesten Dienstes „Skype"; Maßnahmen der Quellen-TKÜ reduzieren sich natürlich nicht nur auf mit Skype geführte Internettelefonate, sondern kommen in gleicher Weise für jegliche Programme zum Führen softwarebasierter verschlüsselter P2P-VoIP-Kommunikation in Betracht.

(RRL)[224] in das nationale Recht um.[225] Gemäß Art. 2 lit. c) RRL handelt es sich um

> „gewöhnlich gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen, einschließlich Telekommunikations- und Übertragungsdienste in Rundfunknetzen, jedoch ausgenommen Dienste, die Inhalte über elektronische Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben; nicht dazu gehören die Dienste der Informationsgesellschaft im Sinne von Artikel 1 der Richtlinie 98/34/EG, die nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen".

Bezüglich softwarebasierter, peer-to-peer-vernetzter VoIP-Sprachtelefonie – die gegenwärtig wohl populärste Form der am Markt befindlichen VoIP-Dienste und zugleich „Regel"-Überwachungsgegenstand der Quellen-TKÜ – lässt die Definition des § 3 Nr. 24 TKG zunächst nicht ohne weiteres auf ein Vorliegen der Eigenschaft eines *Erbringers von Telekommunikationsdiensten* i. S. d. § 100b III S. 1 StPO schließen. Denn im Rahmen der „klassischen" VoIP-Telefonie-Funktion stellen Anbieter wie Skype ihren Nutzern zunächst einmal nur kostenlos[226] eine Software zur Verfügung, mit deren Hilfe der Nutzer, i. d. R. ebenfalls kostenlos, direkte/geschlossene Verbindungen („peer-to-peer") zu einem anderen Nutzer der Software herstellen und Kommunikationsinhalte (v. a. Audio- und Videoinhalte) „end-to-end"-verschlüsselt austauschen kann.[227] Die eigentliche Übertragung, d. h. den Transport der VoIP-Daten vom System des einen Nutzers zu dem des ande-

---

224 *Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie)*, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0021:DE:HTML (zuletzt aufgerufen 15.06.2012).

225 Vgl. auch *Dinger*, Das Potential von Peer-to-Peer-Netzen und -Systemen, S. 186.

226 Allein die Kostenfreiheit eines P2P-VoIP-Dienstes schließt nicht bereits die Annahme des § 3 Nr. 24 TKG aus, da einerseits die Vorschrift eben nur von „in der Regel gegen Entgelt" spricht und zudem regelmäßig auch genügend Umstände für ein Erbringen der Dienste mit Ertragserzielungsabsicht vorliegen, wie ggf. der „Hintergedanke", mit dem kostenlosen P2P-Dienst den Nutzer zum Abschluss zusätzlicher kostenpflichtiger VoIP-Dienste, wie z. B. solcher, die einen Übergang ins öffentliche Telefonnetz ermöglichen, zu motivieren, oder aber bspw. auch das Schalten von Werbung in der Benutzeroberfläche des kostenlosen P2P-VoIP-Programms, vgl. auch *Seitlinger*/*Strobl*, Voice over IP – eine rechtliche Beurteilung vom Kommunikationsdienst bis zum Netzzugang, S. 8, abrufbar unter http://www.it-law.at/uploads/tx_publications/Voice_over_IP__eine_rechtliche_Beurteilung_vom_Kommunikationsdienst_bis_zum_Netzzugang.pdf (zuletzt aufgerufen 15.06.2012).

227 Vgl. Stellungnahme Skype im Rahmen der Anhörung durch die Bundesnetzagentur im Jahr 2004, S. 1 ff., abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/

ren Nutzers, welche direkt miteinander verbunden sind, bewerkstelligen hierbei jedoch nicht die VoIP-Diensteanbieter, sondern – wie dies bei der Nutzung des Internet generell üblich und technisch bedingt ist – die jeweiligen Netzbetreiber/Provider der Gesprächsteilnehmer über ihre IP-Infrastruktur. An diesem Vorgang sind Skype und vergleichbare Dienste *jedenfalls nicht unmittelbar* beteiligt, weshalb der Schluss naheliegend ist, dass derartige Diensteanbieter, die ihre „Dienste" im Rahmen einer spezielle Kommunikationssoftware auf Anwendungsebene leisten, mangels Signalübertragung i. S.d obigen Begriffsbestimmungen insoweit keine Telekommunikationsdienste erbringen.[228]

Dieser Standpunkt, auf den sich insbesondere die marktstarken VoIP-Diensteanbieter wegen des (grds. nachvollziehbaren) Interesses[229] an der Vermeidung eines Unterfallens unter die gesetzlichen Bestimmungen und Verpflichtungen (v. a. des TKG) regelmäßig stellen[230], ist ein vertretbarer[231], jedoch kein zwingender.

VoiceOverIP/Stellungnahmen/SkypeTechnologiesId714pdf.pdf?__blob=publicationFile (zuletzt aufgerufen 15.06.2012).

228 Vgl. Stellungnahme Skype, S. 1 ff., 7, 11, 16 u. 19, abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Stellungnahmen/SkypeTechnologiesId714pdf.pdf?__blob=publicationFile (zuletzt aufgerufen 15.06.2012); hierauf abstellend auch Bundesnetzagentur, Eckpunkte zur regulatorischen Behandlung von Voice over IP, S. 6, abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Eckpunkte/EckpunktederregulatorischenId3210pdf.pdf?__blob=publicationFile (zuletzt aufgerufen 15.06.2012).

229 So führt bspw. Skype an, dass „die andauernde Verbrauchernachfrage für P2P-VoIP-Software dann ernstlich beeinträchtigt werden kann, wenn die Technologie überreguliert wird" (S. 2) und ist „besorgt darüber, dass die weitreichenden Verpflichtungen […] wichtige Verbesserungen durch VoIP hinsichtlich der Verbraucherkommunikation ernsthaft behindern könnten" (S. 2), wodurch „als eine Folge hiervon […] der Wettbewerb in diesem Sektor behindert [wird]." (S. 3), Stellungnahme Skype, abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Stellungnahmen/SkypeTechnologiesId714pdf.pdf?__blob=publicationFile (zuletzt aufgerufen 15.06.2012).

230 So zieht ein Einordnen als Telekommunikationsdienst weitreichende gesetzliche Verpflichtungen nach sich, u. a. hinsichtlich Marktregulierung (§§ 9 ff. TKG), Fernmeldegeheimnis (§§ 88 ff. TKG), Datenschutz (§§ 91 ff. TKG) und der hier gegenständlichen öffentlichen Sicherheit (§§ 108 ff. TKG).

231 So bezeichnete sich Skype jedenfalls im Jahr 2004 noch als „Software-Entwicklungsunternehmen" (S. 16), welches „tatsächlich lediglich Software an[bietet]." (S. 1), Stellungnahme Skype, abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Stellungnahmen/SkypeTechnologiesId714pdf.pdf?__blob=publicationFile (zuletzt aufgerufen 15.06.2012); auch die Bundesnetzagentur geht jedenfalls noch im

So gibt es auch eine Reihe von Anknüpfungspunkten, die dafür sprechen, dass auch VoIP-Diensteanbieter wie bspw. Skype, die ihren Nutzern über eine zur Verfügung gestellte Software Kommunikation via IP ermöglichen, relevante Beiträge leisten, die auf ein Erbringen von Telekommunikationsdiensten hindeuten. Hierfür ließe sich bspw. daran anknüpfen, dass z. B. der „Basis-Dienst“[232] von Skype (P2P-IP-Kommunikation) zwar von jedermann mit dem entsprechenden technischen Equipment kostenlos heruntergeladen und auch kostenlos genutzt werden kann, sich jeder Nutzer zum Führen von Sprach- und Videotelefonie dennoch bei Skype unter Angabe und Speicherung seiner persönlichen Daten anmelden und registrieren muss[233] sowie im Rahmen des Einrichten eines Accounts auf die Zuteilung einer persönlichen Kennung in Form einer exklusiven „Skype-Kennung“ (sog. *Skype-Name*[234]) in Kombination mit einem Kennwort zum Einloggen angewiesen ist. In diesem Zusammenhang ließe sich dann auch darauf abstellen, dass Skype und vergleichbare Dienste nach einem Teil der Stimmen aus der Literatur zwar nicht den unmittelbaren Transport der Daten über das Leitungsnetz bewerkstelligen, durch gewisse Signalisierungs- bzw. Adressierungstätigkeit dennoch einen gewissen Anteil an der Übermittlung der Kommunikationsdaten hätten (vgl. nachfolgend). Denn der einzelne Nutzer muss natürlich irgendwie erfahren, dass sein potentieller Gesprächspartner gerade online ist, es muss eine Verbindung der Gesprächspartnern zueinander hergestellt werden und auch die einzelnen Datenpakete des geführten Internettelefona-

---

Jahr 2005 davon aus, dass VoIP-Dienste, „bei denen die Übertragung der Signale durch den Anbieter des genutzten Internetzugangsdienstes erbracht wird, etwa weil der Anbieter des VoIP-Dienstes lediglich eine bestimmte Software zur Verfügung stellt“ (S. 6), nicht als Telekommunikationsdienst eingeordnet werden könnten, Bundesnetzagentur, Eckpunkte zur regulatorischen Behandlung von Voice over IP, abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Eckpunkte/EckpunktederregulatorischenId3210pdf.pdf?__blob=publicationFile (zuletzt aufgerufen 15.06.2012), wobei aber zugleich festgestellt wird, dass die „heute [2005, Anm. d. Verf.] üblicherweise als VoIP bezeichneten Dienste […] der Sache nach Angebote der Sprachübertragung über Telekommunikationsnetze“ (S. 5) seien und der „gleiche Dienst […] also lediglich mit einer anderen Technik erbracht“ (S. 5) werde. Dies gelte „insbesondere“ für „VoIP-Dienste, die den Übergang in das PSTN [das öffentliche Festnetz, Anm. d. Verf.] ermöglichen [was mittlerweile aber auch von bestimmten softwarebasierten VoIP-Diensten geleistet werden kann, vgl. z. B. *SkypeIn*/*SkypeOut*, Anm. d. Verf.]“ (S. 5).

232 P2P-Telefonie sowie Instant Messaging der Nutzer untereinander innerhalb des Skype-Netzwerkes.

233 Was i. d. R. erst nach Bestätigen eines Endbenutzer-Lizenzvertrages abgeschlossen werden kann, vgl. bspw. http://www.voip-informer.de/skype/skype-erster-start-und-registrierung/2/ (zuletzt aufgerufen 15.06.2012).

234 https://support.skype.com/de/faq/FA94/Was-ist-ein-Skype-Name (zuletzt aufgerufen 15.06.2012).

tes müssen entsprechend adressiert sein, damit sie – sinnbildlich gesprochen – auf ihrem Weg über die Datenautobahn beim richtigen Zielort – dem hinter dem angewählten „Skype-Namen" befindlichen Empfängersystem des Gesprächspartners – abgesetzt werden können.

Hinzu kommt, dass es auch viele VoIP-Anbieter gibt, die nicht nur einen kostenlosen P2P-VoIP-Dienst anbieten, sondern wie Skype auch kostenpflichtige VoIP-Dienste, wie bspw. die oben dargestellten *SkypeIn*-/*SkypeOut*-Dienste[235] sowie den kostenpflichtigen Online-Anrufbeantworterdienst *Skype-Voicemail*[236]. Da für derartige Dienste im erstgenannten Fall („netzübergreifende VoIP-Dienste") ein Übergang ins öffentliche Telefon- oder Mobilfunknetz stattfindet bzw. im zweitgenannten Fall („Online-Anrufbeantworterdienste") die aufgezeichnete Sprachnachricht regelmäßig über einen Dienst-Server läuft[237], erschiene auch hier die Annahme einer Vermittlungs-, wenn nicht gar Übermittlungstätigkeit seitens des VoIP-Dienstesanbieters[238] und damit die Annahme eines *Erbringens von Telekommunikationsdiensten* nicht abwegig.

Stellt man für die Einordnung als Telekommunikationsdienst allein auf den *Wortlaut* der einschlägigen telekommunikationsrechtlichen Begriffsbestimmunsgen ab, so gestaltet sich die Subsumtion von VoIP-Diensten[239], die – wie Skype bei seinem „Basis-Dienst" – mit einer speziellen Software

---

235 Für Einzelheiten zum *SkypeIn*-/*SkypeOut*-Dienst, siehe 1. Teil A.I.2.c).

236 Für Einzelheiten zum *Skype-Voicemail*-Dienst, siehe 1. Teil A.I.4. sowie 3. Teil A.II.

237 Wobei für den Dienst *Skype-Voicemail* unterschiedliche Aussagen darüber existieren, ob dieser über einen Dienst-Server abgewickelt wird, vgl. einerseits bspw. http://sky2peer.com/de/article/677 (zuletzt aufgerufen 15.06.2012); in dieselbe Richtung http://www.pcwelt.de/news/Skype-Anrufbeantworter-im-Betatest-486874.html (zuletzt aufgerufen 15.06.2012); andererseits beruft sich Skype in einem Informationsblatt über die Beantwortung von Anfragen von Strafverfolgungsbehörden darauf, dass sein System so entworfen sei, dass Voicemail jedenfalls nicht zentral gespeichert werde („not centrally stored"), vgl. Skype-Informationsblatt *Responding to Law Enforcement Records Requests*, abrufbar unter http://cryptome.org/isp-spy/skype-spy.pdf (zuletzt aufgerufen 15.06.2012); in eine andere Richtung wiederum die Antwort des Parl. Staatssekretärs beim Bundesminister des Innern, *Bergner*, für die Bundesregierung im Rahmen der 135. Sitzung des Deutschen Bundestags am 26.10.2011, BT-PlPr. 17/135 16064 D.

238 Wohingegen z. B. Skype bislang die Auffassung vertrat, lediglich die erforderliche Software für VoIP-Kommunikation zur Verfügung zu stellen, vgl. Stellungnahme Skype, S. 1, abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Stellungnahmen/SkypeTechnologiesId714pdf.pdf?__blob=publicationFile (zuletzt aufgerufen 15.06.2012).

239 So gibt es auch eine Vielzahl von „Nur"-P2P-VoIP-Diensten, die keinen Übergang ins öffentliche Telefonnetz anbieten; soweit diese (so im Regelfall) eine Ver-

die Möglichkeit zu P2P-verbundener VoIP-Kommunikation anbieten, unter die gesetzlichen Begriffsbestimmungen durchaus problematisch. Ein Dienst, welcher der „Übertragung von Signalen über Telekommunikationsnetze" i. S. d. § 3 Nr. 24 TKG dienen soll, müsste unter Berücksichtigung der Legaldefinitionen in § 3 Nr. 22 TKG (Telekommunikation) und § 3 Nr. 23 TKG (Telekommunikationsanlagen) sowie auf Grundlage des physikalischen Signalbegriffs[240] die Signalübertragung zwischen physisch definierten Punkten[241] mittels technischer Einrichtungen und Systeme anbieten, wobei (begriffsbedingt) von dem Erfordernis der Überwindung einer gewissen Distanz im Sinne eines räumlichen Auseinanderfallens von Anfangs- und Endpunkt auszugehen wäre.[242] Im Umkehrschluss müsste dann auf Grundlage dieser physikalischen Begriffsbestimmung ein Dienst, der keine eigenständige unmittelbare Distanzüberwindung beim Kommunikationsakt leistet, also keine Transportdienstleistung[243] zur Übertragung von Signalen über Telekommunikationsnetze erbringt, als Telekommunikationsdienst ausscheiden.[244]

Bei softwarebasierter P2P-IP-Kommunikation, wie der hier gegenständlichen, findet der eigentliche Transport der Datenpakete auf IP-Ebene durch den jeweiligen Netzbetreiber statt. Bei Zugrundelegung dieser Sichtweise wären deshalb VoIP-Diensteanbieter wie Skype, die eine Software zur Ermöglichung von VoIP-Kommunikation in einem „P2P-System" bereitstellen, jedoch keinen unmittelbaren Beitrag zur Raumüberwindung im Sinne einer (physikalischen) Signalübertragung zwischen physisch definierten Punkten erbringen, bereits vom Wortlaut her nicht als Erbringer von Telekommunikationsdiensten zu qualifizieren.[245]

---

schlüsselung der Datenpakete vornehmen, fallen sie als verschlüsselte P2P-VoIP-Dienste in den Fokus der Quellen-TKÜ.

240 Vgl. bei *Dinger*, Das Potential von Peer-to-Peer-Netzen und -Systemen, S. 188.

241 Wobei die Signalübertragung nicht zwingend nur zwischen zwei physisch definierten Punkten stattfinden müsse, vgl. bei *Meinberg*, Voice over IP: IP-basierter Sprachdienst vor dem Hintergrund des novellierten TKG, S. 77 m. w. N.

242 Vgl. bei *Meinberg*, Voice over IP: IP-basierter Sprachdienst vor dem Hintergrund des novellierten TKG, S. 77.

243 Als zentrales Kennzeichen eines Telekommunikationsdienstes, so *Martini*/*von Zimmermann*, CR 2007, 368 (368).

244 Vgl. bei *Dinger* (i. E. aber abl.), Das Potential von Peer-to-Peer-Netzen und -Systemen, S. 188, 200; so aber *Martini*/*von Zimmermann*, CR 2007, 368 (371; 373); *dies*., CR 2007, 427 (429).

245 Vgl. *Meinberg*, Voice over IP: IP-basierter Sprachdienst vor dem Hintergrund des novellierten TKG, S. 96 m. w. N.; i. E. auch *Martini*/*von Zimmermann*, CR 2007, 368 (371; 373); vgl. bei *Dinger* (i. E. aber abl.), Das Potential von Peer-to-Peer-Netzen und -Systemen, S. 188, 200; vgl. auch bei *Seitlinger*/*Strobl* (i. E. aber abl.),

Demgegenüber ließe sich aber auch der auf *teleologischen* Überlegungen basierende Ansatz vertreten, dass ein alleiniges Abstellen auf den Wortlaut der gesetzlichen Legaldefinitionen zur Einordnung von Telekommunikationsdiensten weder zwingend veranlasst noch mit Blick auf den rasanten technischen Fortschritt im Bereich Telekommunikation sowie den *technologieneutralen Grundsatz*, welcher den europäischen Regulierungen[246] zugrunde liegt, sachgemäß ist, sondern die Beurteilung vielmehr anhand einer funktionellen Betrachtungsweise zu erfolgen hat.[247] Das Bedürfnis für eine technologieneutrale Regulierung liegt hierbei in der zunehmenden *Konvergenz*[248] der Systeme, d. h. dem Zusammenwachsen der bislang getrennten Bereiche der Telekommunikation, der Medien und der Informationstechnologien. Die fortschreitende Digitalisierung von Diensten und Infrastrukturen bewirkt in zunehmenden Maße ein Zusammenwachsen verschiedenartiger Übertragungstechniken (sog. *Konvergenz der Übertragungstechniken*), die Zusammenführung bislang getrennter Netze (sog. *Konvergenz der Netze*) sowie das Zusammenfassen bislang separater Dienste in multifunktionalen Endgeräten[249] (sog. *Konvergenz der Endgeräte*). Angesichts dieser Verschmelzung der Systeme bedarf es aber auch eines entsprechenden einheitlichen Rechtsrahmens für die zusammenwachsenden Netze und Dienste (sog. *Konvergenz des Rechts*).[250] Hintergrund der geforderten technologieneutralen Regulierung, an die letztlich auch die nationalen telekommunikationsrechtlichen Regelungen anknüpfen[251] (vgl. § 1 TKG), ist die Absicht

---

Voice over IP – eine rechtliche Beurteilung vom Kommunikationsdienst bis zum Netzzugang, S. 7, abrufbar unter http://www.it-law.at/uploads/tx_publications/Voice_over_IP__eine_rechtliche_Beurteilung_vom_Kommunikationsdienst_bis_zum_Netzzugang.pdf (zuletzt aufgerufen 15.06.2012).

246 Vgl. Erwägungsgründe 5 u. 18 sowie Art.2 u. 8 der Rahmenrichtlinie 2002/21/EG, abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0021:DE:HTML (zuletzt aufgerufen 15.06.2012); vertiefend *Meinberg*, Voice over IP: IP- basierter Sprachdienst vor dem Hintergrund des novellierten TKG, S. 81 f.

247 Vgl. *Dinger*, Das Potential von Peer-to-Peer-Netzen und -Systemen, S. 188 ff., 203.

248 Der Begriff der „Konvergenz" wurde geprägt durch die Europäische Kommission in deren „Grünbuch zur Konvergenz der Branchen Telekommunikation, Medien und Informationstechnologien und ihren ordnungspolitischen Auswirkungen, KOM (1997), 623 endg., abrufbar unter http://ec.europa.eu/avpolicy/docs/library/legal/com/greenp_97_623_de.pdf (zuletzt aufgerufen 15.06.2012).

249 Im Falle der VoIP-Technik: bspw. PCs, die mittels spezieller Software und Verbindung ins Internet Telefonie ermöglichen.

250 Vgl. *Meinberg*, Voice over IP: IP-basierter Sprachdienst vor dem Hintergrund des novellierten TKG, S. 81 f. m. w. N.

251 Vgl. *Meinberg*, Voice over IP: IP-basierter Sprachdienst vor dem Hintergrund des novellierten TKG, S. 82 f.; vgl. auch die Stellungnahme des Bundesministeriums

des Gesetzgebers, Technologien als grds. gleichberechtigt zu betrachten[252] und von der technischen Entwicklung bedingte Rechtsnormen nicht nur auf Technologien zu erstrecken, die zum Zeitpunkt ihres Erlasses bekannt sind, sondern auch solche in den Anwendungsbereich mit einzubeziehen, die sich noch in der Entwicklung befinden oder bislang völlig unbekannt sind.[253] Dies erlaubt eine entsprechende Anpassung an die technologische Entwicklung, ohne dass es zu wesentlicher Verzögerung käme oder es einer Änderung der Regulierung bedürfte. Demgemäß werden einschlägige Normtatbestände entsprechend abstrakt gefasst und entwicklungsoffen ausgelegt.

Im Bereich des nationalen Telekommunikationsgesetzes findet sich die Maßgabe technologieneutraler Regulierung in den Vorschriften zum Zweck des Gesetzes in § 1 TKG wieder. Für die Frage der Einordnung moderner VoIP-Dienste als Telekommunikationsdienste sei es hierbei unschädlich, dass VoIP-Dienste (ganz oder teilweise) über das IP-Netz erfolgen. Auf Grund des technologieneutralen Ansatzes der gesetzlichen Vorschriften komme es bei der Beurteilung von Telekommunikationsdiensten i. S. d. § 3 Nr. 24 TKG nämlich grds. nicht darauf an, ob für die Erbringung der Dienste leitungsvermittelte Netze (wie das Festnetz) oder paketvermittelte Netze (wie das IP-Netz) zum Einsatz kommen.[254] Für die Einordnung von VoIP-Diensten als *Telekommunikationsdienste* und der VoIP-Diensteanbieter als *Erbringer von Telekommunikationsdiensten* müsste damit vor dem Hintergrund der Technologieneutralität mit dem Bedürfnis der Gleichbehandlung funktional gleichgerichteter Dienste[255] statt auf den reinen Wortlaut vielmehr auf die Funktionalität der betreffenden Dienste abgestellt werden.

Zur näheren Auseinandersetzung mit diesem Ansatz und zur weiteren Beurteilung der Frage des Vorliegens eines *Erbringens von Telekommunikationsdiensten* bei Skype und vergleichbaren Anbietern bedarf es demnach einer getrennten *funktionellen Einordnung* der einzelnen vom jeweiligen

---

des Innern, S. 2, abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Stellungnahmen/BMIBundesministeriumdesInId676pdf.pdf?__blob=publicationFile (zuletzt aufgerufen 15.06.2012).

252 Insbesondere auch zur Schaffung eines Wettbewerbs zwischen den Technologien.

253 Vgl. *Meinberg*, Voice over IP: IP-basierter Sprachdienst vor dem Hintergrund des novellierten TKG, S. 80.

254 Vgl. Bundesnetzagentur, Eckpunkte der regulatorischen Behandlung von Voice over IP, S. 5, abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Eckpunkte/EckpunktederregulatorischenId3210pdf.pdf?__blob=publicationFile (zuletzt aufgerufen 15.06.2012).

255 Vgl. *Dinger*, Das Potential von Peer-to-Peer-Netzen und -Systemen, S. 203.

Anbieter offerierten VoIP-Dienste[256] – insbesondere anhand deren technischer Realisierung und der im Rahmen dieser Dienste durch den VoIP-Diensteanbieter erbrachten Leistungen. Am Beispiel des populären Anbieters Skype lässt sich eine derartige Einordnung wie folgt darstellen:

- Die von Skype angebotene kostenlose *Sprach- und Videotelefonie innerhalb des Skype-Netzwerkes* funktioniert nach dem Prinzip peer-to-peer („*P2P*")[257] vernetzter Gesprächsteilnehmer innerhalb eines „P2P-Systems", d. h. das aktive Telefongespräch läuft als spezielle Funktion im Rahmen der Anwendung des Skype-Programms („P2P-Anwendung") über eine direkte Verbindung von Rechner zu Rechner auf gleicher Ebene in einem Rechnernetz („P2P-Netzwerk") ab, ohne notwendige Vermittlung der Datenpakete über einen zwischengeschalteten Server. Auch das mit der Skype-Software mögliche *Instant Messaging innerhalb des Skype-Netzwerkes*[258] funktioniert nach diesem Prinzip.

  Bei einer technikneutralen Sichtweise muss Skype und vergleichbaren Anbietern im Rahmen solcher „P2P-Systeme" allerdings nicht zwingend nur die Rolle des bloßen Bereitstellers einer P2P-VoIP-Software[259] zukommen. Vielmehr erfüllen die VoIP-Diensteanbieter in funktioneller Hinsicht spezifische Aufgaben innerhalb des „P2P-Systems", welche die vernetzte Kommunikation der Nutzer untereinander überhaupt erst ermöglichen. Die Aufgabe des VoIP-Dienstes bestehe nach dieser Sichtweise nämlich insbesondere in der notwendigen Lokalisierung[260] der Nutzer bzw. der Endgeräte, über die sie den Zugang in das Internet herstellen und auf denen sie das Programm nutzen, womit eine Kernfunktion der Dienste in der indirekten Vermittlung von Verbindungen zu sehen sei[261].

---

256 Soweit verschiedene VoIP-Dienste angeboten werden und die angebotenen VoIP-Dienste als selbständige Dienste unterscheidbar sind; eine Beurteilung lässt sich bspw. anhand wirtschaftlicher Gesichtpunkte vornehmen; für Dienste wie Skype kann durchaus von einer Trennbarkeit und wirtschaftlichen Selbständigkeit der einzelnen Dienste ausgegangen werden, da bspw. der (kostenlose) P2P-VoIP-Dienst und die (kostenpflichtigen) VoIP-Dienste mit Übergang in das/aus dem öffentlichen Telefonnetz bei wirtschaftlicher Betrachtungsweise wohl jeweils isoliert existenzfähig sind und auch unabhängig voneinander betrieben werden, vgl. hierzu auch *Martini/von Zimmermann*, CR 2007, 427 (427; 430).

257 Für Einzelheiten zu peer-to-peer-vernetzter VoIP-Telefonie via Skype, siehe 1. Teil A.I.2.c).

258 Für Einzelheiten zur Instant Messaging Funktion, siehe 1. Teil A.I.2.f).

259 So aber bspw. *Martini/von Zimmermann*, CR 2007, 368 (370); auch *Meinberg*, Voice over IP: IP-basierter Sprachdienst vor dem Hintergrund des novellierten TKG, S. 96 m. w. N.

260 Anhand der jeweiligen Adressierung des ausgewählten „Skype-Namens".

261 Vgl. *Dinger*, Das Potential von Peer-to-Peer-Netzen und -Systemen, S. 185, 200 f.

Diese Sichtweise stützt sich hierbei auf folgende technische Abläufe und Funktionsweisen der softwarebasierten VoIP-Technik:

Ein Hauptanreiz der Internettelefonie via Skype ist die weltweite Nutzbarkeit des Dienstes, unabhängig davon, wo sich die Gesprächsteilnehmer gerade befinden. Erforderlich ist nur das Vorhandensein eines mit entsprechender Hardware (Mikrofon, Lautsprecher etc.) ausgerüsteten Computers auf dem die Software installiert ist und über den sich ein Zugang ins Internet herstellen lässt. Von jedem dieser Endgeräte kann sich der Nutzer dann in seinen Account einloggen[262] und über seinen „Skype-Namen" Internettelefonate führen. Die Nutzung des Dienstes allein über einen stationären Anschluss wie bei klassischer Festnetztelefonie ist bei derartigen VoIP-Diensten technisch nicht veranlasst und entspricht i. d. R. auch nicht dem Nutzungsverhalten eines Großteils der Nutzer, die Internetdienste in zunehmenden Maße ortsungebunden („nomadisch"[263]) benutzen.[264] Zusammen mit dem Umstand, dass im Rahmen der Vergabe sog. *dynamischer*[265] *IP-Adressen*[266] die an das Internet angeschlossenen Gerä-

---

262 Was über einen Login-Server zur Authentifizierung läuft, vgl. auch *Dinger*, Das Potential von Peer-to-Peer-Netzen und -Systemen, S. 37; vgl. auch http://www.skype.com/intl/de/support/user-guides/start-skype/ (zuletzt aufgerufen 15.06.2012).

263 Da der Nutzer nomadischer Dienste typischerweise nicht an einen festen Anschluss gebunden ist, können derartige Dienste theoretisch an jedem verfügbaren Breitbandanschluss mit der benötigten Hardware in Anspruch genommen werden, vgl. *Seitlinger*/*Strobl*, Voice over IP – eine rechtliche Beurteilung vom Kommunikationsdienst bis zum Netzzugang, S. 14, abrufbar unter http://www.it-law.at/uploads/tx_publications/Voice_over_IP__eine_rechtliche_Beurteilung_vom_Kommunikationsdienst_bis_zum_Netzzugang.pdf (zuletzt aufgerufen 15.06.2012).

264 Vgl. Bundesnetzagentur, Anhörung zu Voice over IP (VoIP) – Zusammenfassende Auswertung der jeweiligen Fragenkomplexe, S. 3, abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Auswertung/ThemenweiseAuswertungId3173pdf.pdf?__blob=publicationFile (zuletzt aufgerufen 15.06.2012); vgl. auch *Dinger*, Das Potential von Peer-to-Peer-Netzen und -Systemen, S. 185; hierzu auch *Bär*, Handbuch zur EDV-Beweissicherung, Rn. 121.

265 Anders als bei der sog. *statischen IP-Adresse*, die dauerhaft einem bestimmten Anschluss (z. B. bei Standleitungen) zugeordnet ist und daher direkt als Bestandsdatum im Wege des manuellen Auskunftsverfahrens nach §§ 161, 163 StPO i. V. m. § 113 TKG abgerufen werden kann, wird bei der sog. *dynamischen IP-Adresse* dem Anschlussinhaber bei jeder neuen Verbindung ins Internet eine neuen IP-Adresse nur speziell für den Zeitraum dieser Sitzung zugeordnet, weshalb die dynamische IP-Adresse und der Zuteilungszeitpunkt – mit Blick auf die vom BVerfG festgestellte Nichtigkeit des § 113b S. 1 HS 2 TKG (BVerfG NJW 2010, 833) – als Verkehrsdaten weiterhin nur im Wege einer Maßnahme nach § 100g StPO (bzw. als nähere Umstände der Telekommunikation auch im Rahmen einer Maßnahme nach §§ 100a, 100b StPO) ermittelbar sind; anhand der individualisierenden dynamischen IP-Adresse und der Uhrzeit lassen sich anschließend Name und Anschrift des Anschlussinhabers ebenfalls im Wege des manuellen Auskunftsverfahrens nach §§ 161, 163

te der Internetnutzer heutzutage i. d. R. nicht unter einer festen und permanent zugeordneten („statischen") IP-Adresse, sondern bei jeder Einwahl in das Internet unter einer neuen, dynamisch vergebenen zu erreichen sind, bedarf es für VoIP-Dienste eines zusätzlichen (diensteigenen) Namens- bzw. Adressierungsschemas, welches auf diese Umstände „flexibel" reagiert und die Erreichbarkeit der Nutzer gewährleistet.[267] Jeder Nutzer muss sich deshalb zunächst bei Skype unter Angabe seiner persönlichen Daten registrieren, bevor er den VoIP-Dienst nutzen kann. Hierbei findet zugleich eine Harmonisierung des Skype-eigenen Namens- und Adressierungsschemas statt.[268] Anhand eines Nutzerverzeichnisses wird bei Aktivierung des Dienstes dem jeweiligen „Skype-Namen" die aktuelle Netzwerkadresse (gerade zugeteilte IP-Adresse und Port[269]) des dahinter stehenden Nutzers bzw. dessen Endgerätes zugeordnet.[270] Hierdurch ist es möglich, zum Verbindungsaufbau eine Signalisierung des einzelnen Nutzer-Accounts vorzunehmen und für eine entsprechende Adressierung der Datenpakete im Falle eines anschließenden Kommunikationsvorgangs Sorge zu tragen. Zum Zwecke der Adressierung werden die einzelnen Kommunikationsdatenpakete mit einer Art Steuerungsinformation (sog. *header*) versehen[271], wodurch die Übermittlung der Datenpakete an den korrekten Empfänger sichergestellt wird.

Mit dieser technischen Abfolge bestehe gemäß obigem technikneutralen Ansatz eine Kernfunktion des VoIP-Dienstes zugleich in der *indirekten Vermittlung* von Verbindungen, da für das Routing bei der Übermittlung der Datenpakete auf IP-Ebene eine entsprechende Adressierung auf

---

StPO i. V. m. § 113 TKG abrufen, vgl. BT-Drs. 16/5846, S. 26, 86 u. 87; Meyer-Goßner – *Cierniak*, StPO, § 100g, Rn. 5; ebenso BeckOK – *Hegmann*, StPO, Ed. 13, § 100g, Rn. 2 u. 6 m. w. N.; aber str.

266 Sog. *Internet-Protokoll-Adresse*, eine Art „postalische" Adresse für die in einem auf dem Internetprotokoll aufbauenden Computernetz befindlichen Rechner/Geräte (Server, PCs etc.), wodurch die Rechner/Geräte adressierbar und damit erreichbar gemacht werden, vgl. BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 14; http://de.wikipedia.org/wiki/IP-Adresse (zuletzt aufgerufen 15.06.2012).

267 Vgl. *Dinger*, Das Potential von Peer-to-Peer-Netzen und -Systemen, S. 185.

268 Vgl. *Dinger*, Das Potential von Peer-to-Peer-Netzen und -Systemen, S. 200.

269 Teil einer Netzwerkadresse in Netzwerkprotokollen zur Zuordnung von Datenpaketen zu bestimmten Diensten, vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 185.

270 Vgl. *Dinger*, Das Potential von Peer-to-Peer-Netzen und -Systemen, S. 38, 185 u. 200.

271 Vgl. *Seitlinger*/*Strobl,* Voice over IP – eine rechtliche Beurteilung vom Kommunikationsdienst bis zum Netzzugang, S. 3, abrufbar unter http://www.it-law.at/uploads/tx_publications/Voice_over_IP__eine_rechtliche_Beurteilung_vom_Kommunikationsdienst_bis_zum_Netzzugang.pdf (zuletzt aufgerufen 15.06.2012).

Grundlage vorgeschalteter Adresszuweisung und -auflösung durch den VoIP-Dienst unerlässlich sei.[272]

Unter Berücksichtigung dieser technischen Abläufe stellt sich für die Einordnung der Dienste unter die telekommunikationsrechtlichen Begrifflichkeiten freilich dennoch die Frage, ob derartige „Vermittlungsdienste", wie sie softwarebasierte VoIP-P2P-Dienste bei Zugrundelegung dieser Sichtweise erbringen würden, als Telekommunikationsdienste i. S. d. obigen Begriffsbestimmungen gesehen werden können, gerade mit Blick darauf, dass dann zwar eine (indirekte) *Ver*mittlung von Verbindungen geleistet wird, aber keine eigentliche *Über*mittlung der entsprechend adressierten Datenpakete.[273]

Mit nachvollziehbaren Argumenten könnte sich demgegenüber aber auch auf den Standpunkt gestellt werden, dass die Ausstattung der Datenpakete mit den notwendigen „Steuerungsinformationen" zur Adressierung (aktuelle Netzwerkadresse eines bestimmten „Skype-Namens") eine unverzichtbare Voraussetzung für die eigentliche Datenübermittlung über das Netz darstellt, da die Verbindung der Nutzer miteinander nur durch das vorausgehende Übermitteln der genannten adressierungsrelevanten Informationen seitens des VoIP-Diensteanbieters realisiert werden kann, weil ohne das Bereitstehen eines Namens- und Adressierungsschemas schon ein Verbindungsaufbau nicht möglich wäre.[274] Auch das Routing, also die Steuerung der einzelnen Datenpakete während der eigentlichen Kommunikation auf IP-Ebene, sei letztlich ohne den vorgeschalteten Schritt der Adressvermittlung nicht möglich.[275] Insofern könne bei einem „P2P-System", welches zur Realisierung von VoIP-Kommunikation zwischen den Nutzern innerhalb des „P2P-Netzwerkes" Verbindungen anhand eines diensteigenen Names- und Adressierungsschemas vermittelt, auch das Vorliegen eines virtuellen[276] Telekommunikations-

---

272 Vgl. *Dinger*, Das Potential von Peer-to-Peer-Netzen und -Systemen, S. 185, 200 f.

273 In der Stellungnahme an die Bundesnetzagentur aus dem Jahr 2004 stellt sich bspw. Skype diesbezüglich auf den Standpunkt, dass „VoIP-Anbieter wie Skype […] nicht die Art von Diensten und Einrichtungen eines typischen Telekommunikationsanbieters an[bieten]" (S. 3) und die Software „es Konsumenten ermöglicht, direkt miteinander zu kommunizieren, ohne auf Netzressourcen von Skype zurückzugreifen" (S. 19), abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Stellungnahmen/SkypeTechnologiesId714pdf.pdf?__blob=publicationFile (zuletzt aufgerufen 15.06.2012).

274 Vgl. *Dinger*, Das Potential von Peer-to-Peer-Netzen und -Systemen, S. 38 u. 200 f.

275 Vgl. *Dinger,* Das Potential von Peer-to-Peer-Netzen und -Systemen, S. 200.

276 Im Sinne von „logisch", also nicht-physisch.

netzes[277] angenommen werden.[278] In Folge leiste ein P2P-System wie das von Skype über die Vermittlung der aktuellen Adressierungselemente[279] eine *mittelbare Steuerung* der schließlich auf IP-Ebene über den Austausch von Datenpaketen stattfindenden Kommunikation der Nutzer.[280]

Diese Sichtweise – als Gegenpol zum Wortlautargument (vgl. oben) – stützt sich letztlich auch auf den technologieneutralen Grundsatz der europäischen Rahmenrichtlinie und dem daraus resultierenden Bedürfnis nach gleichartiger Behandlung funktional gleichgerichteter Dienste in herkömmlichen und neuartigen Netzwerken.[281] Für moderne VoIP-Dienste, die wie herkömmliche Telefonie ebenfalls zum Zwecke der Kommunikation, insbesondere der Sprachkommunikation (mittlerweile wohl auch in kaum unterscheidbarer Sprachqualität[282]), zwischen Menschen genutzt werden[283], sei deshalb nach dieser Auffassung zu verlangen, dass sie auch

---

277 § 3 Nr. 27 TKG definiert Telekommunikationsnetz als „die Gesamtheit von Übertragungssystemen und gegebenenfalls Vermittlungs- und Leitwegeinrichtungen sowie anderweitige Ressourcen, die die Übertragung von Signalen […] ermöglichen […]"; nach Auffassung der EU-Kommission sowie der neuen Begriffsdefinition des elektronischen Kommunikationsnetzes (Übertragungssysteme und ggf. Vermittlungseinrichtungen) nach Art. 2 lit. a) der Rahmenrichtlinie kann ein Netz – entgegen der nationalen Begriffsbestimmung und dem bisherigen Verständnis der Bundesnetzagentur (Verbindung einer Vermittlungsstelle mit mindestens drei Übertragungswegen) – auch nur aus einem Übertragungsweg bestehen; entscheidend sei vielmehr die *Möglichkeit* der Signalübertragung, welche auch bei VoIP gegeben sei, vgl. Spindler/Schuster – *Holznagel/Ricke*, § 3 TKG, Rn. 38; nach Ansicht von *Dinger* verschließe sich die Bestimmung des Art. 2 lit. a) der Rahmenrichtlinie auch nicht dagegen, „weitere logische Netze, die auf Anwendungsschicht realisiert werden, in ihren Anwendungsbereich aufzunehmen" (*Dinger*, Das Potential von Peer-to-Peer-Netzen und -Systemen, S. 197).

278 Vgl. *Dinger*, Das Potential von Peer-to-Peer-Netzen und -Systemen, S. 200 u. 203.

279 Als Substitut zur klassischen „Steuerung des Leitweges" durch den Anbieter im Festnetz bei herkömmlicher Telefonie, so *Dinger*, Das Potential von Peer-to-Peer-Netzen und -Systemen, S. 193.

280 Vgl. *Dinger*, Das Potential von Peer-to-Peer-Netzen und -Systemen, S. 193 u. 200 f.

281 Vgl. *Dinger*, Das Potential von Peer-to-Peer-Netzen und -Systemen, S. 203.

282 Vgl. bei Bundesnetzagentur, Anhörung zu Voice over IP (VoIP) – Zusammenfassende Auswertung der jeweiligen Fragenkomplexe, S. 11, abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Auswertung/ThemenweiseAuswertungId3173pdf.pdf?__blob=publicationFile (zuletzt aufgerufen 15.06.2012).

283 So ist auch das Bundesministerium des Innern in seiner Stellungnahme an die Regulierungsbehörde anlässlich der Anhörung zum Thema „VoIP" der Auffassung, dass „im Unterschied zum bisher vorherrschenden Transport von Sprache in leitungsvermittelten Netzen […] die Übermittlung in paketvermittelten Netzen nur eine

denselben telekommunikationsrechtlichen Bestimmungen und Verpflichtungen unterliegen, wie „klassische" Telekommunikationsdienste.[284] Hierfür bedürfe es mitunter auch einer entsprechenden Neubewertung bislang herangezogener technischer Referenzmodelle[285].

Für die Annahme einer Art Vermittlungsfunktion ließe sich auch noch auf weitere „Leistungen" abstellen, die vom VoIP-Diensteanbieter im Rahmen des P2P-Netzwerks übernommen werden. So müssen Nutzer bspw. irgendwie davon Kenntnis erlangen, ob und wenn ja welche anderen Nutzer gerade online sind und somit für eine Kommunikation via Internettelefonie oder Instant Messaging zur Verfügung stehen. Bei Programmen wie Skype teilt deshalb im Regelfall der VoIP-Dienst – nach erfolgter Authentifizierung durch Einloggen in den Account mit Skype-Name und Kennwort – dem Nutzer mit, welche anderen Nutzer[286] ebenfalls eingeloggt sind und ob eine Verbindung zum gewünschten Gesprächspartner überhaupt in dem betreffenden Moment aufgebaut werden kann.

- Eine Vielzahl von VoIP-Diensteanbietern bietet neben kostenlosen VoIP-Diensten auf P2P-Ebene auch (i. d. R. kostenpflichtige) VoIP-Dienste an, die einen *Übergang in das bzw. aus dem öffentlichen Telefonnetz* ermöglichen. So bietet bspw. Skype VoIP-Dienste an, die Telefonie aus dem Skype-Netz in das öffentliche Festnetz oder Mobilfunknetz (*SkypeOut*) bzw. vom öffentlichen Festnetz oder Mobilfunknetz in das Skype-Netz

---

Änderung der Übertragungsart dar[stellt]. Die Dienstleistung dem Kunden gegenüber bleibt aber unverändert." (S. 2, abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Stellungnahmen/BMIBundesministeriumdesInId676pdf.pdf?__blob=publicationFile, zuletzt aufgerufen 15.06.2012); ähnlich auch die Begründung der Bundesregierung zum Entwurf für ein Telemediengesetz, BR-Drs. 556/06, S. 18, allerdings ohne nähere Differenzierung des Begriffs Internettelefonie (VoIP) nach einzelnen VoIP-Diensten.

284 Wobei sich gegen die Vergleichbarkeit der Dienste wiederum anführen ließe, dass der Wert eines Telefons für das Gros der Endnutzer gerade darin liegt, beliebige Inhaber anderer Telefonanschlüsse anrufen zu können, was jedenfalls bei VoIP-Diensten, die keinen Übergang ins öffentliche Telefonnetz bieten (P2P-VoIP-Dienste), nicht möglich ist, vgl. *Martini/von Zimmermann*, CR 2007, 368 (372); auch verneinen viele softwarebasierte VoIP-Diensteanbieter ausdrücklich die Tauglichkeit ihrer Dienste als Ersatz für das normale Telefon bspw. auf Grund fehlender Notruffunktionalität; so weist z. B. der Anbieter Skype bereits auf der Startseite seiner Internetpräsenz (http://www.skype.com/intl/de/home/) sowie in seinen Nutzungsbedingungen (http://www.skype.com/intl/de/legal/terms/tou/) ausdrücklich darauf hin, dass Skype kein Ersatz für ein normales Telefon sei und nicht für Notrufe verwendet werden könne, vgl. auch http://www.skype.com/intl/de/legal/emergency/ (zuletzt aufgerufen 15.06.2012).

285 Vgl. *Dinger*, Das Potential von Peer-to-Peer-Netzen und -Systemen, S. 203.

286 Bspw. aus der „Freundes-Liste" des jeweiligen Nutzers.

(*SkypeIn*) ermöglichen und kostenpflichtig in Anspruch genommen werden können.[287] Bei derartigen „Hybriddiensten"[288] gehen die Nutzer unabhängig von ihrem Access-Provider ein zusätzliches Geschäftsverhältnis mit dem VoIP-Diensteanbieter ein.[289] Ein VoIP-Diensteanbieter unterstützt in solchen Fällen – anders als bei P2P-VoIP-Diensten – das Zustandekommen von Verbindungen zwischen dem IP-Netz und dem öffentlichen Telefonnetz, indem er (i. d. R. entgeltlich) die Nutzung von (ggf. diensteigenen) Netzeinrichtungen wie insbesondere Gateways[290] als Schnittstellen zwischen den unterschiedlichen Techniken/Protokollen der beteiligten Netze ermöglicht und damit die (direkte) Vermittlung von Telefonaten aus dem IP-Netz in das öffentliche Telefonnetz und umgekehrt (direkt) gewährleistet.[291]

Der weit überwiegende Teil der Stimmen geht heute davon aus, dass jedenfalls VoIP-Dienste, welche (i. d. R. entgeltlich) einen Übergang in das öffentliche Telefonnetz ermöglichen und hierfür bspw. einen Zugang ins öffentliche Festnetz („PSTN") gewährleisten, einen Telekommunikationsdienst i. S. d. § 3 Nr. 24 TKG darstellen.[292] Denn bei derartigen Diensten könne ohne weiteres von einer Übertragung von Signalen i. S. d. § 3 Nr. 24 TKG ausgegangen werden, da ein VoIP-Dienst, der den Zugang ins öffentliche Festnetz gewährleistet, „jedenfalls für diesen Teil der Ver-

---

287 Für weitere Einzelheiten zu den *SkypeOut*-/*SkypeIn*-Diensten, siehe auch 1. Teil A.I.2.c).

288 *Seitlinger*/*Strobl*, Voice over IP – eine rechtliche Beurteilung vom Kommunikationsdienst bis zum Netzzugang, S. 13, abrufbar unter http://www.it-law.at/uploads/tx_publications/Voice_over_IP__eine_rechtliche_Beurteilung_vom_Kommunikationsdienst_bis_zum_Netzzugang.pdf (zuletzt aufgerufen 15.06.2012).

289 Vgl. *Meinberg*, Voice over IP: IP-basierter Sprachdienst vor dem Hintergrund des novellierten TKG, S. 47.

290 Engl. für „Protokollumsetzer", eine Art Schnittstelle, die es Netzen, welche auf unterschiedlichen Protokollen basieren und deshalb an sich nicht kompatibel sind, ermöglicht, miteinander zu kommunizieren, indem bspw. die ausgetauschten Sprachdaten zwischen dem paketvermittelten Internet (IP-Netz) und dem leitungsvermittelten öffentlichen Festnetz oder Mobilfunknetz „übersetzt" werden, vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 98; http://de.wikipedia.org/wiki/Gateway_%28Informatik%29 (zuletzt aufgerufen 15.06.2012).

291 Vgl. *Meinberg*, Voice over IP: IP-basierter Sprachdienst vor dem Hintergrund des novellierten TKG, S. 47.

292 So die Bundesnetzagentur, Eckpunkte der regulatorischen Behandlung von Voice over IP, S. 5 f., abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Eckpunkte/EckpunktederregulatorischenId3210pdf.pdf?__blob=publicationFile (zuletzt aufgerufen 15.06.2012); vgl. auch *Bär*, Handbuch zur EDV-Beweissicherung, Rn. 126.

bindung die Übertragung von Signalen entweder selbst [erbringt] oder […] diese zumindest [ermöglicht]“[293].

Ob dies neben anschlussbasierten[294] VoIP-Diensten auch für einen softwarebasierten VoIP-Dienst gilt, ist unter Berücksichtigung der aufgeführten Gesichtspunkte deshalb letztlich von der (auch rechtspolitischen[295]) Beurteilung der Frage abhängig, inwiefern man davon ausgeht, dass ein softwarebasierter VoIP-Diensteanbieter die Signalübertragung auf einer Teilstrecke kontrolliert[296], ob er für die Ermöglichung eines Übergangs von Gesprächen seiner Nutzer in das/aus dem öffentlichen Telefonnetz bspw. Netzeinrichtungen wie Gateways bereitstellt[297], inwiefern dann das

---

293 Bundesnetzagentur, Eckpunkte der regulatorischen Behandlung von Voice over IP, S. 6, abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Eckpunkte/EckpunktederregulatorischenId3210pdf.pdf?__blob=publicationFile (zuletzt aufgerufen 15.06.2012).

294 Für Anbieter, die ihre Dienste nicht über eine spezielle VoIP-Software, sondern (i. d. R. als Netzbetreiber/Provider) im Rahmen von VoIP über einen bestehenden DSL-Anschluss via VoIP-fähigem Router oder über ein spezielles VoIP-Telefon [siehe hierzu auch 1. Teil A.I.3.a) u. b)] erbringen und hierbei über ihre IP-Infrastruktur auch den Übergang in die öffentlichen Netze (PSTN und Mobilfunk) ermöglichen, dürfte vom Vorliegen einer Signalübertragung i. S. d. § 3 Nr. 24 TKG und mithin eines Erbringens von Telekommunikationsdiensten ohne weiteres auszugehen sein, in diese Richtung Bundesnetzagentur, Eckpunkte der regulatorischen Behandlung von Voice over IP, S. 5 f., abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Eckpunkte/EckpunktederregulatorischenId3210pdf.pdf?__blob=publicationFile (zuletzt aufgerufen 15.06.2012).

295 So zieht ein Einordnen als Telekommunikationsdienst weitreichende gesetzliche Verpflichtungen nach sich, u. a. hinsichtlich Marktregulierung (§§ 9 ff. TKG), Fernmeldegeheimnis (§§ 88 ff. TKG), Datenschutz (§§ 91 ff. TKG) und der hier gegenständlichen öffentlichen Sicherheit (§§ 108 ff. TKG).

296 Bejahend für die Signalübertragung auf der Teilstrecke im öffentlichen Telefonnetz *Martini/von Zimmermann*, CR 2007, 427 (429), da der VoIP-Anbieter entweder selbst Betreiber der Teilstrecke sei oder mit dem Betreiber entsprechende Vereinbarungen getroffen habe, „mittels derer ihm der Zugriff auf die Leitung und damit auch die Kontrolle über die Signalübertragung für die Dauer des Gesprächs übertragen wurde“ (429), nicht jedoch für die Teilstrecke im IP-Netz.

297 Skype gibt im Rahmen seiner Stellungnahme aus dem Jahr 2004 an die Bundesnetzagentur an, keine Netzelemente wie PSTN-Gateways zu haben (S. 18), „nicht die Art von […] Einrichtungen eines typischen Telekommunikationsanbieters an[zubieten]“ (S. 3), den eigenen VoIP-Dienst per Handelsvereinbarung „mit den VoIP-PSTN-Gateways der PSTN-Netzanbieter zu verbinden“ (S. 7) und „keinerlei Pläne [zu besitzen], […] leitungsvermittelte Geräte bzw. Netze einzusetzen, zu besitzen oder zu betreiben“ (S. 2), abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Stellungnahmen/SkypeTechnologiesId714pdf.pdf?__blob=publicationFile (zuletzt aufgerufen 15.06.2012).

Ermöglichen der Nutzung eines Gateways zur Übersetzung und Weiterleitung der Datenpakete zwischen den verschiedenen Netzen bereits als (überwiegender[298]) Teilbeitrag zur Übertragung von Signalen durch (zumindest) direkte Vermittlung in das/aus dem öffentlichen Telefonnetz gewertet und dem VoIP-Diensteanbieter auch zugerechnet werden kann.

- In wiederum einem anderen Lichte erscheint die Frage des Vorliegens eines Telekommunikationsdienstes in Bezug auf das Übertragen von Signalen bei der Nutzung spezieller *Online-Anrufbeantworterdienste*, welche oftmals von Anbietern softwarebasierter VoIP-Dienste (i. d. R. kostenpflichtig) bereitgehalten werden, wie bspw. der kostenpflichtige Dienst *Skype-Voicemail*[299]. Ist der angewählte Gesprächspartner aktuell nicht im System eingeloggt und die Herstellung einer direkten Verbindung zu diesem deshalb nicht möglich, besteht für den anrufenden Nutzer die Möglichkeit, eine Nachricht zu hinterlassen, die regelmäßig auf einem Server[300] des VoIP-Diensteanbieters[301] zwischengespeichert wird[302]. Die für ihn hinterlegten Nachrichten kann der Gesprächspartner – bei entspre-

---

298 Geht man mit einem Teil der Stimmen davon aus, dass der Teil der Übertragungsstrecke, die im Internet verläuft, keine Signalübertragung seitens des VoIP-Diensteanbieters darstellt, müsste der im öffentlichen Telefonnetz stattfindende Streckenteil insgesamt überwiegen, vgl. hierzu auch *Martini/von Zimmermann*, CR 2007, 427 (429) m. w. N., die unter einer „Kosten- und Preisbetrachtung" (429) dies bejahen.

299 Skype bietet seit Version 1.2 (2005) auch einen kostenpflichtigen Anrufbeantworter (*Skype-Voicemail*) an, vgl. http://www.skype.com/intl/de/features/allfeatures/voicemail/ (zuletzt aufgerufen 15.06.2012).

300 Ein („Web-)Server" ist ein Rechner, welcher Inhalte zum Abruf durch andere Rechner (sog. *Clients*) bereithält, vgl. auch *Sieber*, Stellungnahme zu dem Fragenkatalog des BVerfG in dem Verfahren 1 BvR 370/07, S. 7, abrufbar unter http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf (zuletzt aufgerufen 15.06.2012).

301 Somit dürfte bei Anrufbeantworter-Diensten nicht nur ein Login-Server und ggf. ein Vermittlungs-Server auf Ebene der Signalisierung/Adressierung involviert sein, sondern auch ein (Daten-)Server des VoIP-Diensteanbieters, über den auch die eigentlichen Kommunikationsdaten als Zwischen-Server laufen.

302 Wobei für den Dienst *Skype-Voicemail* unterschiedliche Aussagen darüber existieren, ob dieser über einen Dienst-Server abgewickelt wird, vgl. einerseits bspw. http://sky2peer.com/de/article/677 (zuletzt aufgerufen 15.06.2012); in dieselbe Richtung http://www.pcwelt.de/news/Skype-Anrufbeantworter-im-Betatest-486874.html (zuletzt aufgerufen 15.06.2012); andererseits beruft sich Skype in einem Informationsblatt über die Beantwortung von Anfragen von Strafverfolgungsbehörden darauf, dass sein System so entworfen sei, dass Voicemail jedenfalls nicht zentral gespeichert werde („not centrally stored"), vgl. Skype-Informationsblatt *Responding to Law Enforcement Records Requests*, abrufbar unter http://cryptome.org/isp-spy/skype-spy.pdf (zuletzt aufgerufen 15.06.2012); in eine andere Richtung wiederum die Antwort des Parl. Staatssekretärs beim Bundesminister des Innern, *Bergner*, für die Bundesregierung im Rahmen der 135. Sitzung des Deutschen Bundestags am 26.10.2011, BT-PlPr. 17/135 16064 D.

chend gebuchtem kostenpflichtigen VoIP-Dienst – später abrufen, online anhören und je nach Dienst und Anbieter ggf. auch auf das eigene System herunterladen. So wird bei *Skype-Voicemail* bspw. nach dem Online-Anhören der Nachricht diese automatisch durch die Software lokal auf dem System des Empfängers (ggf. zur dortigen Archivierung[303]) abgespeichert.[304] Der technische Ablauf derartiger Online-Anrufbeantworterdienste lässt hierbei durchaus den Schluss zu, dass im Rahmen einer solchen Abrufbeantworter-Funktion die Leistung des VoIP-Diensteanbieters nicht nur in einer indirekten Vermittlung von VoIP-Kommunikation liegt, sondern in diesen Fällen sogar eine direkte Mitwirkung an der Übermittlung der digitalisierten Sprachsignale über diensteigene Server gegeben ist.

Wie die geschilderten Umstände zeigen, gestaltet sich eine abschließende Einordnung softwarebasierter VoIP-Dienste als Telekommunikationsdienste durchaus schwierig. Während bei VoIP-Diensten, die einen Übergang der Kommunikationssignale in das öffentliche Festnetz (PSTN) oder Mobilfunknetz und umgekehrt ermöglichen und deren Anbieter hierfür spezielle Einrichtungen wie Gateways bereithalten, vieles auf ein Erbringen von Telekommunikationsdiensten i. S. d. § 3 Nr. 24 TKG hindeutet, ist eine Einordnung der (Quellen-TKÜ-relevanten) Dienste, die lediglich softwarebasierte VoIP-Kommunikation innerhalb eines P2P-Netzwerkes ermöglichen, unter die auch ihm Rahmen des § 100b III StPO relevante Begrifflichkeit des *Erbringens von Telekommunikationsdiensten* unter Würdigung obiger Gesichtspunkte jedenfalls nicht eindeutig möglich.

Neben dem *Erbringer von Telekommunikationsdiensten* (Alt. 1) verpflichtet § 100b III S. 1 StPO aber des Weiteren auch *denjenigen, der an der Erbringung von Telekommunikationsdiensten mitwirkt* (Alt. 2). So müsste hierfür ein Mitwirkungsbeitrag an der Übertragung der VoIP-Signale geleistet werden. Ob dies bei den Anbietern softwarebasierter P2P-VoIP-Kommunikation der Fall ist, erscheint ebenfalls fraglich. Wie der konkrete Gehalt der Tatbestandsbegrifflichkeit des „Mitwirkens" am Erbringen von Telekommunikationsdiensten – wie dies im TKG auch von § 3 Nr. 6 lit. b aufgegriffen wird – zu erfassen ist, ist noch nicht abschließend geklärt.[305] Nach der wohl h. M. hängt das Merkmal des „Mitwirkens" von der Beteiligung

---

303 Zum Schutz von nach Abschluss des Übertragungsvorgangs im Herrschaftsbereich eines Teilnehmers abgespeicherte Nachrichten durch das Grundrecht auf informationelle Selbstbestimmung, siehe BVerfG NJW 2006, 976.

304 Vgl. http://www.skype.com/intl/de/features/allfeatures/voicemail/ (zuletzt aufgerufen 15.06.2012); https://support.skype.com/de/faq/FA10473/Funktionsweise-von-Voicemail (zuletzt aufgerufen 15.06.2012).

305 Vgl. auch *Arenz*, Der Schutz der öffentlichen Sicherheit in Next Generation Networks am Beispiel von Internet-Telefonie-Diensten, S. 99 m. w. N.

an der konkreten Nachrichtenverarbeitung ab.[306] Für die hier vorliegende Konstellation von Anbietern einer Software für P2P-VoIP-Kommunikation ließe sich diesbezüglich zwar argumentieren, dass der Anbieter innerhalb solcher P2P-Netzwerke durch die von ihm erbrachten Vermittlungsdienste (Signalisierung/Adressierung, vgl. oben) eine Art Vorarbeit für das Zustandekommen einer Verbindung und der daran anknüpfenden Signalübertragung leistet. Auch wird abweichend von der h. M. vertreten, dass in den Fällen proprietärer Telefonie-Software die Wahrung und der Schutz des Fernmeldegeheimnisses aus Art. 10 I GG in besonderem Maße von der Ausarbeitung und Gestaltung der VoIP-Software abhängig sind[307], weshalb sich insoweit auch die Annahme eines Förderns des Angebots des jeweiligen Telekommunikationsdienstes vertreten ließe und der Beitrag des Softwareanbieters in Form des In-Verkehr-Bringens der Software als ein „Mitwirken" i. S. d § 3 Nr. 6 lit. b TKG eingestuft werden könnte.[308] Dennoch wirkt der Anbieter softwarebasierter P2P-VoIP-Kommunikation am eigentlichen Transportvorgang auf IP-Ebene gerade nicht mit, was unter Zugrundelegung des Begriffsverständnisses der h. M. wiederum deutlich gegen die Annahme eines „Mitwirkens" nach § 100b III S. 1 StPO spricht. Vielmehr geht das Verständnis der h. M. in Bezug auf den Begriff des „Mitwirkenden" i. S. d. § 3 Nr. 6 lit. b TKG – Beteiligung an der konkreten Nachrichtenverarbeitung – von Mitarbeitern und sonstigen Erfüllungsgehilfen des Telekommunikationsdiensteerbringers i. S. d. § 3 Nr. 24 TKG (hier: der die Datenpakete der VoIP-Kommunikation transportierende Netzbetreiber) aus.[309] Wie beim Begriffsverständnis des TKG in Bezug auf einen „an der Erbringung Mitwirkenden" i. S. d. § 3 Nr. 6 lit. b TKG dürften in Anlehnung hieran auch bei § 100b III S. 1 StPO mit der Umschreibung hauptsächlich unternehmensinterne Erfüllungsgehilfen wie bspw. Arbeitnehmer des jeweiligen Telekommunikationsdiensteerbringers, sowie externe Personen, die zur Erbringung von (technischen) Dienstleistungen herangezogen werden, wie bspw. Subunternehmer und deren Angestellte[310] gemeint sein. Im Verhältnis zu dem die Telekommunikationsdienste erbringenden Netzbetreiber ist der Anbieter von Software für P2P-VoIP-Kommunikation im Regelfall aber weder dessen Arbeitnehmer noch ein sonstiger Erfüllungsgehilfe, der im Pflichtenkreis

---

306 Vgl. bei *Arenz,* Der Schutz der öffentlichen Sicherheit in Next Generation Networks am Beispiel von Internet-Telefonie-Diensten, S. 99 m. w. N.

307 So *Arenz*, Der Schutz der öffentlichen Sicherheit in Next Generation Networks am Beispiel von Internet-Telefonie-Diensten, S. 99 f.

308 Vgl. *Arenz*, Der Schutz der öffentlichen Sicherheit in Next Generation Networks am Beispiel von Internet-Telefonie-Diensten, S. 99 m. w. N.

309 Vgl. bei *Arenz*, Der Schutz der öffentlichen Sicherheit in Next Generation Networks am Beispiel von Internet-Telefonie-Diensten, S. 99 m. w. N.

310 Vgl. insoweit Beck'scher TKG-Kommentar – *Robert*, § 91 TKG, Rn. 11.

des Netzbetreibers zur Erbringung technischer Dienste tätig wird. Ein Unterfallen der Anbieter softwarebasierter P2P-VoIP-Kommunikation unter die Tatbestandsbegrifflichkeit des *an der Erbringung von Telekommunikationsdiensten Mitwirkenden* und damit ein Unterliegen der Verpflichtungen des § 100b III S. 1 StPO erscheint somit ebenfalls fraglich.

Noch weitergehenden Mitwirkungsverpflichtungen als nach § 100b I S. 1 StPO – sofern man von einem Erbringen von Telekommunikationsdiensten ausgeht (vgl. hierzu die vorhergehenden Ausführungen) – unterläge der VoIP-Diensteanbieter, wenn er als *Betreiber einer Telekommunikationsanlage, mit der öffentlich zugängliche Telekommunikationsdienste erbracht werden* nach § 100b III S. 2 StPO i. V. m. § 110 I S. 1, II TKG, § 3 I TKÜV zu qualifizieren wäre.

Der weit auszulegende Begriff der Telekommunikationsanlage bezeichnet gemäß § 3 Nr. 23 TKG „technische Einrichtungen und Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können“ und umfasst indes sämtliche erforderlichen Komponenten eines Telekommunikationsnetzes nach § 3 Nr. 27 TKG.[311] Telekommunikationsanlagen sind demnach nicht nur Übertragungswege, sondern bspw. auch Vermittlungseinrichtungen wie Router oder Gateways als Systeme, die das Netzmanagement sicherstellen.[312]

Für die Annahme einer Betreibereigenschaft erforderlich ist das Vorliegen von *Funktionsherrschaft*, also bei der Frage des Betreibens einer Telekommunikationsanlage gemäß allgemeinem Begriffsverständnis das Innehaben tatsächlicher oder rechtlicher Kontrolle über die Gesamtheit der Funktionen der Telekommunikationsanlage[313], wobei das Ausüben der tatsächlichen Kontrolle gemäß der Legaldefinition in § 2 Nr. 4 TKÜV das charakteristische Kriterium darstellt.

Das Vorliegen dieser Voraussetzungen dürfte für VoIP-Dienste jedenfalls dann anzunehmen sein, wenn sie einen Übergang vom Datennetz in das bzw. aus dem öffentliche Festnetz oder Mobilfunknetz (und insoweit „öffentlich zugänglich“[314]) ermöglichen und hierfür Funktionsherrschaft über Telekommunikationsanlagen wie bspw. das für den Übergang benötigte

---

311 Vgl. Spindler/Schuster – *Holznagel*/*Ricke*, § 3 TKG, Rn. 34.

312 Vgl. *Katko*, CR 2005, 189 (192); Spindler/Schuster – *Holznagel*/*Ricke*, § 3 TKG, Rn. 34.

313 Vgl. auch Beck’scher TKG-Kommentar – *Bock*, § 110 TKG, Rn. 8.

314 Das Merkmal „öffentlich zugänglich“ lässt sich wie die bisherige Bezeichnung „für die Öffentlichkeit“ – da eine inhaltliche Änderung mit der neuen Begriffswahl nicht verbunden ist, vgl. BT-Drs. 17/5707, S. 91, 50 – an verschiedenen Aspekten festgemacht: am kommerziellen/gewerblichen Anbieten des VoIP-Dienstes,

Gateway innehaben.[315] Dies dürfte bei anschlussbasierten VoIP-Diensten[316] i. d. R. der Fall sein. Bei softwarebasierten VoIP-Diensten, die einen Übergang ins öffentliche Telefonnetz ermöglichen (z. B. *SkypeIn*/*SkypeOut*) ist dies von der Frage des Betreibens einer Telekommunikationsanlage einzelfallabhängig.[317] Werden von Anbietern netzübergreifender VoIP-Dienste keine Telekommunikationsanlagen für Telekommunikationsdienste betrieben, so scheidet eine Verpflichtung nach § 110 I S. 1 TKG aus.[318]

Für die (Quellen-TKÜ-relevanten) softwarebasierten P2P-VoIP-Dienste erscheint die Subsumtion der Anbieter unter den Betreiberbegriff des § 110 I S. 1 TKG – unabhängig von den oben dargestellten Schwierigkeiten der Einordnung als Erbringer von Telekommunikationsdiensten – indes fraglich[319]:

Bei derartigen IP-zu-IP-Anwendungen betreibt ein VoIP-Diensteanbieter innerhalb des „P2P-Netzwerks" zwar i. d. R. zentrale Komponenten wie bspw. den Login-Server, bei dem sich der Nutzer vor jeder Inanspruchnahme des VoIP-Dienstes zur Authentifizierung einloggen muss.[320] Dieser Umstand, wie auch die (vertretbare) Annahme eines (virtuellen) Telekommunikationsnetzes, in dessen Rahmen ein VoIP-Diensteanbieter von soft-

---

am Angebot nicht nur für geschlossene Benutzergruppen u. a., vgl. auch Beck'scher TKG-Kommentar – *Bock*, § 110 TKG, Rn. 9.

315 Vgl. auch *Katko*, CR 2005, 189 (192; 192 f.); *Holznagel*/*Bonnekoh*, MMR 2005, 585 (590).

316 Da diese Anbieter ihre Dienste nicht über eine spezielle VoIP-Software, sondern (i. d. R. als Netzbetreiber/Provider) im Rahmen von VoIP über einen bestehenden DSL-Anschluss via VoIP-fähigem Router oder über ein spezielles VoIP-Telefon [siehe hierzu auch 1. Teil A.I.3.a) u. b)] erbringen und hierbei über ihre IP-Infrastruktur auch den Übergang in die öffentlichen Netze (PSTN und Mobilfunk) ermöglichen.

317 So gibt Skype im Rahmen seiner Stellungnahme aus dem Jahr 2004 an die Bundesnetzagentur an, keine Netzelemente wie PSTN-Gateways zu haben (S. 18), „nicht die Art von […] Einrichtungen eines typischen Telekommunikationsanbieters an[zubieten]" (S. 3), den eigenen VoIP-Dienst per Handelsvereinbarung „mit den VoIP-PSTN-Gateways der PSTN-Netzanbieter zu verbinden" (S. 7) und „keinerlei Pläne [zu besitzen], […] leitungsvermittelte Geräte bzw. Netze einzusetzen, zu besitzen oder zu betreiben" (S. 2), abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Stellungnahmen/SkypeTechnologiesId714pdf.pdf?__blob=publicationFile (zuletzt aufgerufen 15.06.2012).

318 Jedoch unterliegen auch VoIP-Diensteanbieter, die keine Telekommunikationsanlage betreiben, gewissen „Vergewisserungspflichten" nach § 110 I S. 2 TKG, sofern sie öffentlich zugängliche Telekommunikationsdienste erbringen.

319 So auch *Holznagel*/*Bonnekoh*, MMR 2005, 585 (590).

320 Vgl. *Dinger*, Das Potential von Peer-to-Peer-Netzen und -Systemen, S. 37; vgl. auch http://www.skype.com/intl/de/support/user-guides/start-skype/ (zuletzt aufgerufen 15.06.2012).

warebasierter VoIP-Kommunikation durch P2P-basierte Verzeichnis- und Vermittlungsdienste eine mittelbare Steuerung[321] der auf IP-Ebene stattfindenden Kommunikation leistet, bedeutet jedoch nicht, dass es sich bei diesem zwangsläufig auch um einen *Betreiber von Telekommunikationsanlagen* i. S. d. § 3 I S. 1 i. V. m. § 2 Nr. 4 TKÜV handeln muss.[322]

Auf der einen Seite stellen Anbieter von P2P-VoIP-Diensten zur Lokalisierung der Nutzer und korrekten Adressierung der Datenpakete zwar ggf. einen Verzeichnis-Server[323] zur Verfügung[324], der als eine Art Vermittlungssystem unter den weiten Telekommunikationsanlagenbegriff fallen könnte und über den der Anbieter i. d. R. auch Funktionsherrschaft hat. Auf der anderen Seite bestehen unter Berücksichtigung obiger Gesichtpunkte zu § 3 Nr. 24 TKG aber wiederum Zweifel, ob ein solcher Verzeichnis-Server im Rahmen softwarebasierter VoIP-zu-VoIP-Kommunikation die Voraussetzung des § 110 I S. 1 TKG („Telekommunikationsanlage, *mit der* öffentlich zugängliche *Telekommunikationsdienste* erbracht werden") überhaupt erfüllen und unter dessen Anwendungsbereich fallen kann[325]. Eine Art zwischengeschalteten „Übermittlungs-Server", über den zentral die Datenpakete von Nutzer zu Nutzer geleitet werden, gibt es bei P2P-VoIP-Dienst wie Skype gerade nicht.[326]

Auch über die Telekommunikationsanlagen, mit denen bei softwarebasierter P2P-VoIP-Kommunikation der eigentliche Transport der Daten auf IP-

---

321 Vgl. *Dinger*, Das Potential von Peer-to-Peer-Netzen und -Systemen, S. 200 f.

322 Mit der Konsequenz, dass Anbieter von P2P-VoIP-Diensten auch aus dem Anwendungsbereich des neuen § 110 I S. 1 Nr. 1a TKG ausscheiden; die Gesetzesbegründung nennt hierbei als Beispiel zwar „VoIP-Telefonie" (vgl. BT-Drs. 16/2581, S. 28), jedoch ohne nähere Differenzierung der „VoIP-Telefonie" nach deren verschiedenen Erscheinungsformen und unterschiedlichen Dienstfunktionen; wie bereits unter 2. Teil A.II.6. erläutert, entfaltet die Vorschrift des § 110 I S. 1 Nr. 1a TKG ihre Relevanz v. a. im Zusammenhang mit anschlussbasierten VoIP-Diensten.

323 Ggf. mit Login-Server zu einem Server zusammengefasst.

324 Wobei Skype zwar einen zentralen Login-Server verwendet, sich offenbar – anders als andere VoIP-Programme – aber keines eigenen zentralen Verzeichnis-Servers bedient, sondern eine dezentrale, über das Internet verteilte Struktur nutzt, vgl. *Martini/von Zimmermann*, CR 2007, 368 (371), Fn. 49.

325 Womit sich § 110 I S. 1 Nr. 1a TKG bei VoIP-Kommunikation dann im Wesentlichen an den Netzbetreiber als Betreiber einer Telekommunikationsanlage, mit der öffentlich zugängliche Telekommunikationsdienste erbracht werden, an die (i. d. R. mit dem Netzbetreiber personengleichen) anlagenbetreibenden Anbieter von anschlussbasierten VoIP-Diensten (im Rahmen eines Breitbandanschlusses über den Router oder per VoIP-Telefon) sowie ggf. an Anbieter von softwarebasierten netzübergreifenden VoIP-Diensten, die ein Gateway als Übergang ins öffentliche Telefonnetz betreiben, richten würde.

326 Vgl. http://www.voip-information.de/wie-funktioniert-skype.html (zuletzt aufgerufen 15.06.2012).

Ebene realisiert wird, hat der Anbieter derartiger softwarebasierter VoIP-Kommunikation regelmäßig keinerlei tatsächliche wie rechtliche Kontrolle.

Anders als bei kostenpflichtigen VoIP-Diensten, die einen Übergang in das bzw. aus dem öffentlichen Festnetz und Mobilfunknetz ermöglichen[327], bereitet daneben aber auch die Qualifikation von Diensten, die P2P-VoIP-Kommunikation innerhalb eines „P2P-Netzwerks" ermöglichen, als *öffentlich zugängliche*[328] Telekommunikationsdienste Schwierigkeiten. In der aktuellen Fassung des TKG vom 22. Juni 2004 war das Merkmal bislang als Telekommunikationsdienste „für die Öffentlichkeit" bezeichnet. Eine Legaldefinition dieses Begriffes befand sich zwar nicht (mehr) im Gesetz, jedoch konnte hierfür weiterhin an die Begriffsbestimmung des früheren § 3 Nr. 19 TKG 1996 angeknüpft werden.[329] Dieser definierte *Telekommunikationsdienstleistungen für die Öffentlichkeit* als „das gewerbliche Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für beliebige natürliche oder juristische Personen und nicht lediglich für Teilnehmer geschlossener Benutzergruppen". Geändert durch Artikel 1 des Gesetzes vom 03.05.2012 m. W. v. 10.05.2012 spricht das TKG nunmehr zur Vereinheitlichung des Sprachgebrauchs mit den Richtlinienvorgaben durchgehend von „öffentlich zugänglichen Telekommunikationsdiensten" statt von „Telekommunikationsdiensten für die Öffentlichkeit". Die Begriffsbestimmung in § 3 Nr. 17a TKG definiert öffentlich zugängliche Telekommunikationsdienste als „der Öffentlichkeit zur Verfügung stehende Telekommunikationsdienste".[330] Da eine inhaltliche Änderung mit der neuen Begriffswahl nicht verbunden ist[331], lässt sich zur näheren Bestimmung, was unter „der Öffentlichkeit zur Verfügung stehend" zu fassen ist, ergänzend auch auf das bisherige Begriffsverständnis zu Telekommunikationsdiensten für die Öffentlichkeit zurückgreifen.

Gegen die Annahme von öffentlich zugänglichen Diensten könnte demnach angeführt werden, dass es sich bei kostenlosen VoIP-P2P-Diensten schon nicht um ein gewerbliches Angebot handelt. Andererseits baut das Konzept der P2P-Kommunikation als kostenfreier „Basis-Dienst" gerade auch auf der Überlegung auf, dass der Nutzer in Folge auch die regelmäßig angebotenen und beworbenen kostenpflichtigen Zusatz-VoIP-Dienste in Anspruch nimmt, was zumindest indirekt auch auf ein Anbieten der kostenlo-

---

327 Vgl. hierzu *Katko*, CR 2005, 189 (193); in diese Richtung auch *Holznagel*/*Bonnekoh*, MMR 2005, 585 (590).

328 Das Merkmal „öffentlich zugänglich" ist für die Verpflichtung nach § 100b III S. 1 StPO indes keine Tatbestandsvoraussetzung.

329 Vgl. Beck'scher TKG-Kommentar – *Bock*, § 110 TKG, Rn. 9.

330 Vgl. BT-Drs. 17/5707, S. 91, 50.

331 Vgl. BT-Drs. 17/5707, S. 50.

sen P2P-Dienste mit gewerblicher/kommerzieller Zielsetzung schließen ließe. Zudem haben mittlerweile viele VoIP-Diensteanbieter, darunter auch Skype[332], für Unternehmen die Möglichkeit eingerichtet, auf der Benutzeroberfläche der kostenlosen P2P-Anwendung Werbeanzeigen zu schalten. Auch dieser Umstand ließe sich für die Annahme eines ertragserzielungsorientierten gewerblichen Anbietens[333] – ein kostenpflichtiges Anbieten ist gerade nicht Voraussetzung – derartiger P2P-VoIP-Dienste heranziehen.

Während sich das Kriterium des „gewerblichen Anbietens" bei derartigen P2P-VoIP-Diensten noch mit durchaus schlüssigen Argumenten bejahen ließe, so bereitet das Merkmal des Angebotes an „beliebige natürliche oder juristische Personen und nicht lediglich für Teilnehmer geschlossener Benutzergruppen" weit größere Schwierigkeit. Einerseits stehen die P2P-VoIP-Dienste zwar in dem Sinne der Öffentlichkeit zur Verfügung, als sich i. d. R. jeder[334], der über die erforderliche Hardware verfügt, anmelden und nach Registrierung den (kostenfreien) Dienst auch grds. nutzen kann. Auf der anderen Seite eröffnet sich das eigentliche Angebot, Telekommunikation durch Nutzung des Dienstes zu führen, gerade nicht für die Öffentlichkeit, also für jede beliebige Person, sondern nur für den angemeldeten, registrierten und hierbei durch den Dienst akzeptierten[335] Personenkreis und ermöglicht dann auch nur eine Kommunikation innerhalb des Dienstnetzwerkes, also der angemeldeten Nutzer untereinander, ohne dass Personen und Anschlüsse[336] außerhalb dieses geschlossenen Netzwerks an der Telekommunikation teilnehmen könnten, weshalb in derartigen Fällen von P2P-VoIP-

---

332 Unter dem „Skype Home"-Registerreiter, vgl. http://blogs.skype.com/de/2011/03/werbung_in_skype.html (zuletzt aufgerufen 15.06.2012); vgl. https://support.skype.com/de/faq/FA10942/Warum-sehe-ich-Werbung-in-Skype (zuletzt aufgerufen 15.06.2012).

333 In die Richtung auch *Seitlinger*/*Strobl*, Voice over IP – eine rechtliche Beurteilung vom Kommunikationsdienst bis zum Netzzugang, S. 8, abrufbar unter http://www.it-law.at/uploads/tx_publications/Voice_over_IP__eine_rechtliche_Beurteilung_vom_Kommunikationsdienst_bis_zum_Netzzugang.pdf (zuletzt aufgerufen 15.06.2012).

334 Anders als bspw. bei „Corporate Networks", also bei privaten, unternehmensinternen Netzwerken.

335 I. d. R. nach Bestätigen eines Endbenutzer-Lizenzvertrages durch den Nutzer, vgl. bspw. http://www.voip-informer.de/skype/skype-erster-start-und-registrierung/2/ (zuletzt aufgerufen 15.06.2012).

336 So weist bspw. der Anbieter Skype bereits auf der Startseite seiner Internetpräsenz (http://www.skype.com/intl/de/home/) sowie in seinen Nutzungsbedingungen (http://www.skype.com/intl/de/legal/terms/tou/) auch ausdrücklich darauf hin, dass Skype kein Ersatz für ein normales Telefon sei und nicht für Notrufe verwendet werden könne, vgl. auch http://www.skype.com/intl/de/legal/emergency/ (zuletzt aufgerufen 15.06.2012).

Kommunikation durchaus auch die Annahme einer „de facto“ geschlossenen Benutzergruppe vertretbar ist.

Ein Unterfallen von Anbietern softwarebasierter P2P-VoIP-Dienste unter die weitergehenden Verpflichtungen des § 110 I S. 1 TKG ist unter diesen Gesichtspunkten ebenfalls nicht zwingend gegeben.

Für Unternehmen, die zwar *öffentlich zugängliche Telekommunikationsdienste* erbringen, hierfür aber *keine Telekommunikationsanlage* betreiben, bestehen nach § 110 I S. 2 TKG zwar dennoch bestimmte „Vergewisserungspflichten“. Diese haben sich bei der Auswahl des Betreibers der für die Dienste genutzten Telekommunikationsanlagen (i. d. R. der Betreiber des genutzten IP-Netzes und dessen Einrichtungen) zu vergewissern, dass dieser insbesondere Anordnungen zur Überwachung der Telekommunikation nach Maßgabe des § 110 II TKG i. V. m. §§ 1 ff. TKÜV unverzüglich umsetzen kann. Dieser Verpflichtung würden – bei Bejahen eines *Erbringens von öffentlich zugänglichen Telekommunikationsdiensten* – bspw. Anbieter solcher VoIP-Dienste unterliegen, die mit ihrer Software einen Übergang in das oder aus dem öffentlichen Telefonnetz ermöglichen, ohne hierfür eine Telekommunikationsanlage zu betreiben (vgl. oben).

Für P2P-VoIP-Dienste hingegen gestaltet sich – wie bereits oben im Rahmen der Ausführungen zu § 100b III S. 1 StPO und § 110 I S. 1 TKG im Einzelnen dargestellt – die Annahme eines *Erbringens von öffentlich zugänglichen Telekommunikationsdiensten* eher schwierig. Auch eine Verpflichtung der Anbieter P2P-basierter VoIP-Dienste nach § 110 I S. 2 TKG erscheint deshalb auf Grund der oben genannten Gesichtspunkte fraglich.

Als Ergebnis des Exkurses kann damit festhalten werden, dass sich die rechtliche Einordnung und Beurteilung der Frage, ob Skype und vergleichbare Anbieter von softwarebasierten VoIP-Diensten, insbesondere beim Anbieten von P2P-Kommunikation zwischen ihren Nutzern, „*Erbringer von Telekommunikationsdiensten*“ oder „*daran Mitwirkende*“ i. S. d. § 100b III S. 1 StPO darstellen oder gar nach § 100b III S. 2 StPO i. V. m. § 110 I TKG als „*Erbringer von öffentlich zugänglichen Telekommunikationsdiensten mit* (S. 1) oder *ohne* (S. 2) *Betreiben einer Telekommunikationsanlage hierfür*“ zu qualifizieren sind, angesichts der technischen Besonderheiten und Möglichkeiten moderner Internettelefonie und der hieraus hervorgegangenen Vielfalt einzelner VoIP-Funktionalitäten und -Dienste schwierig gestaltet. Bei den (Quellen-TKÜ-relevanten) softwarebasierten P2P-VoIP-Diensten wirken sich einerseits die divergierenden Ansichten hinsichtlich des Vorliegens eines *Erbringens von Telekommunikationsdiensten* unterschiedlich auf die Annahme einer Verpflichtung nach § 100b III S. 1 StPO aus, andererseits bereiten sowohl das Merkmal des Erbringens von *öffentlich zugänglichen* Telekommunikationsdiensten i. S. d. § 110 I S. 1, S. 2 TKG als auch

das Merkmal des *Betreibens einer Telekommunikationsanlage* i. S. d. § 110 I S. 1 TKG für die Annahme einer Verpflichtung nach § 100b III S. 2 StPO i. V. m § 110 I S. 1, II TKG, § 3 I S. 1 TKÜV bzw. § 100b III S. 2 StPO i. V. m. § 110 I S. 2 TKG Schwierigkeiten.

In Gesamtschau der herausgearbeiteten Aspekte und Kriterien sprechen im Rahmen einer Einzelfallbetrachtung der einzelnen softwarebasierten VoIP-Dienste unter den aufgeführten Voraussetzungen zwar gut vertretbare Gründe dafür, dass Anbieter softwarebasierter VoIP-Dienste, die einen Übergang zwischen dem IP-Netz und dem öffentlichen Fest- oder Mobilfunknetz ermöglichen und hierfür einen *Zugang in die öffentlichen Netze* gewährleisten (z. B. *SkypeIn*, *SkypeOut*), insoweit als „*Erbringer von Telekommunikationsdiensten*" i. S. d. § 100b III S. 1 StPO wie auch bei entsprechender Funktionsherrschaft über technische Einrichtungen als „*Betreiber von Telekommunikationsanlagen mit denen öffentlich zugängliche Telekommunikationsdienste erbracht werden*" i. S.d § 110 I S. 1 TKG qualifiziert werden können.[337]

Für softwarebasierte *P2P-VoIP-Dienste*, die (wie bspw. Skype mit seinem kostenlosen „Basis-VoIP-Dienst") lediglich eine geschlossene, „P2P-vernetzte" VoIP-Kommunikation innerhalb eines „P2P-Netzwerks" zwischen den Nutzern des VoIP-Programms ermöglichen[338], ist eine vergleichbare Schlussfolgerung jedoch nicht ohne weiteres möglich. Wenngleich sich nachvollziehbare Argumente dafür anführen lassen, bei P2P-VoIP-Kommunikation eine in Form von Verzeichnis- und Vermittlungsdiensten zum Zwecke der Signalisierung bzw. Adressierung geleistete mittelbare Steuerung des Datenpaketeaustauschs auf IP-Ebene durch die VoIP-Diensteanbieter als ein (ggf. auch nur Mitwirken am[339]) Erbringen von Telekommunikationsdiensten zu qualifizieren[340], ist diese Sichtweise, wie hierzu vertretenen divergierenden Ansichten zeigen, indes jedoch nicht zwingend.

---

337 In diese Richtung auch *Bär*, Handbuch zur EDV-Beweissicherung, Rn. 126, 128, *Holznagel*/*Bonnekoh*, MMR 2005, 585 (590) und *Katko*, CR 2005, 189 (193); auch *Martini*/*von Zimmermann*, CR 2007, 427 (429).

338 Und wegen der i. d. R. erfolgenden end-to-end-Verschlüsselung der TK-Daten indes das Bedürfnis einer Quellen-TKÜ begründen.

339 Vgl. zur Frage des Mitwirkens auch *Arenz*, Der Schutz der öffentlichen Sicherheit in Next Generation Networks am Beispiel von Internet-Telefonie-Diensten, S. 98 ff.

340 Vgl. *Dinger*, Das Potential von Peer-to-Peer-Netzen und -Systemen, S. 184 ff. (201); i. E. auch *Seitlinger*/*Strobl*, Voice over IP – eine rechtliche Beurteilung vom Kommunikationsdienst bis zum Netzzugang, S. 7 ff., abrufbar unter http://www.it-law.at/uploads/tx_publications/Voice_over_IP__eine_rechtliche_Beurteilung_vom_Kommunikationsdienst_bis_zum_Netzzugang.pdf (zuletzt aufgerufen 15.06.2012); pauschal für Internettelefonie auch die Begründung der Bundesregierung zum Entwurf für ein Telemediengesetz, BR-Drs. 556/06, S. 18; a. A. *Martini*/*von Zimmermann*, CR 2007, 368 (373), *dies*., CR 2007, 427 (430); ebenso *Meinberg*, Voice over

Angesichts der Tatsache, dass die spezifische Konstellation der softwarebasierten P2P-VoIP-Kommunikation über das Internet rechtlich und gesetzlich bislang nicht abschließend geklärt und die Einordnung eines Anbieters derartiger softwarebasierter VoIP-Dienste unter die gesetzlichen Begrifflichkeiten des „*Erbringers von Telekommunikationsdiensten*“, des „*an solchen Diensten Mitwirkenden*“ und des „*Betreibers einer Telekommunikationsanlage mit der öffentlich zugängliche Telekommunikationsdienste erbracht werden*“ de lege lata jedenfalls nicht bzw. nicht eindeutig möglich ist[341], stellt der Weg über die Inpflichtnahme des VoIP-Diensteanbieters gemäß § 100b III StPO[342] für die Ermöglichung eines Zugriffs auf ermittlungsrelevante Telekommunikationsinhalte einer P2P-geführten VoIP-Kommunikation gegenwärtig keine (ggf. mildere[343]) Alternative[344] zu einem Zugriff mittels Quellen-TKÜ dar.

c) Überwachung stets nur unter Mitwirkung Dritter?

Selbst wenn von einer Verpflichtung des jeweiligen VoIP-Diensteanbieters zur Mitwirkung nach § 100b III StPO ausgegangen würde[345], so ist es fraglich, ob – die Eignung deren Inpflichtnahme zum Erkenntnisgewinn einmal unterstellt[346] – Ermittlungsbehörden hierauf verpflichtend zurück-

---

IP: IP-basierter Sprachdienst vor dem Hintergrund des novellierten TKG, S. 96; auch *Bär*, Handbuch zur EDV-Beweissicherung, Rn. 126; a. A. wohl auch *Katko*, CR 2005, 189 (192) und *Holznagel*/*Bonnekoh*, MMR 2005, 585 (590).

341 Ähnlich resümierend auch die Bundesnetzagentur, Eckpunkte der regulatorischen Behandlung von Voice over IP, S. 6, abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Eckpunkte/EckpunktederregulatorischenId3210pdf.pdf?__blob=publicationFile (zuletzt aufgerufen 15.06.2012), die eine generell gültige Bewertung dieser Dienste bislang (2005, Anm. d. Verf.) nicht für möglich hielt, da die Bewertung insbesondere von der technischen Realisierung im Einzelfall abhängt.

342 Wegen der regelmäßig stattfindenden Verschlüsselung derartiger Kommunikation müsste der gesetzlichen Pflicht zum „Ermöglichen der Überwachung“ i. S. d. § 100b III S. 1 StPO dann ggf. – soweit technisch möglich und unter technologie- und wettbewerbsfördernden Aspekten sowie Belangen der IT-Sicherheit rechtspolitisch erwünscht – durch Implementieren entsprechender Komponenten in die Software bzw. in das Verschlüsselungsprotokoll (Hintertür; Schlüssel) nachgekommen werden.

343 Für Einzelheiten zur Frage der Erforderlichkeit der Quellen-TKÜ in diesem Zusammenhang, siehe 2. Teil B.III. 2.b) sowie 3. Teil A.I.1.c).

344 So aber offenbar *Buermeyer*, http://ijure.org/wp/archives/756 (zuletzt aufgerufen 15.06.2012).

345 Zur Frage des Unterfallens von VoIP-Diensteanbietern unter die Voraussetzungen des § 100b III StPO, siehe 2. Teil A.II.6.b).

346 Was wegen der end-to-end-Verschlüsselung der Datenpakete und des (bekundeten) Fehlens von entsprechenden Entschlüsselungsinstrumenten in den Händen der

greifen müssten. Denn es ist dogmatisch umstritten, ob aus der Regelung des § 100b III StPO zu folgern ist, dass die Durchführung einer Telekommunikationsüberwachungsmaßnahme *zwingend* unter Mitwirkung des daraus Verpflichteten zu erfolgen habe.

Unstreitig ergibt sich auf Grund der Regelungen des § 100b III S. 1 StPO für den jeweiligen Erbringer von TK-Diensten sowie für den, der an der Erbringung mitwirkt, eine Rechtspflicht dazu, Ermittlungsbehörden die Durchführung von Überwachungsmaßnahmen zu ermöglichen und erforderliche Auskünfte unverzüglich zu erteilen.

Über die Frage, ob die nach § 100b III StPO bestehenden Mitwirkungsverpflichtungen zwingend für Maßnahmen nach § 100a I StPO in Anspruch zu nehmen sind, herrscht jedoch Uneinigkeit:

So stellt sich ein Teil der Stimmen auf den Standpunkt, die Wahrnehmung der Eingriffsbefugnis aus § 100a I StPO hänge grds. von der Mitwirkung eines TK-Dienstleisters ab.[347] Dass die Strafverfolgungsbehörden keine Obliegenheit treffe, Überwachungsmaßnahmen stets nur unter Mitwirkung eines TK-Dienstleisters durchzuführen, ergebe sich aus dem Gesetzestext nicht.[348] Da bei den §§ 100a, 100b StPO der jeweilige Netzbetreiber die Durchführung der TKÜ-Maßnahme nach § 100b III S. 1 StPO zu ermöglichen habe, sei die Durchführung ohne Mitwirkung eines Diensteanbieters, gerade auch um die Streubreite Betroffener gering zu halten, nicht statthaft.[349]

Nach der überwiegend vertretenen Ansicht hingegen ist den Regelungen der §§ 100a I und 100b III StPO keine Obliegenheit für die Ermittlungsbehörden dergestalt zu entnehmen, dass eine Überwachung stets und nur unter Mitwirkung der nach § 100b III StPO Verpflichteten stattfinden könne.[350] Die Ermittlungsbehörden seien durchaus berechtigt, Überwachungsmaßnah-

---

VoIP-Diensteanbieter (vgl. Stellungnahme Skype im Rahmen der Anhörung durch die Bundesnetzagentur, S. 16, abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Stellungnahmen/SkypeTechnologiesId714pdf.pdf?__blob=publicationFile, zuletzt aufgerufen 15.06.2012, wie auch BT-PlPr. 17/135 16064 D) zweifelhaft ist, siehe hierzu auch 2. Teil B.III.2.b) sowie 3. Teil A.I.1.c).

347 So SK – *Wolter*, StPO, § 100a, Rn. 20.

348 Vgl. SK – *Wolter*, StPO, § 100b, Rn. 19.

349 So *Sankol*, CR 2008, 13 (17).

350 So Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 7a, 8 sowie § 100b, Rn. 7; ebenso *Bär*, TK-Überwachung, § 100a StPO, Rn. 32; *ders.*, MMR 2008, 215 (219); zust. *Gercke*/*Brunst*, Internetstrafrecht, Kap.5, S. 350, Rn. 895, Fn. 377; a.A. SK – *Wolter*, StPO, § 100a, Rn. 20 u. § 100b, Rn. 19; *Sankol*, CR 2008, 13 (17); wohl auch *Buermeyer*/*Bäcker*, HRRS 2009, 433 (440); ebenso noch LG Hamburg, MMR 2008, 423 (424); nunmehr zust. LG Hamburg, MMR 2011, 693 (696).

men eigenständig und ausschließlich *mit eigenen Mitteln* umzusetzen.[351] Denn § 100a I StPO enthalte allgemein eine Befugnis zur Überwachung und Aufzeichnung von Telekommunikation, die nicht nur auf die Durchführung unter Mitwirkung des nach § 100b III StPO Verpflichteten beschränkt sei.[352] Dies deckt sich auch mit den insoweit klaren Aussagen des Gesetzgebers im Rahmen der Gesetzesbegründung zu § 100b III StPO, wonach sich zwar „die Notwendigkeit für diese Inpflichtnahme […] daraus [ergibt], dass sich Telekommunikationsüberwachungsmaßnahmen in effizienter Weise regelmäßig nur unter Mitwirkung der Telekommunikationsdienstleister umsetzen lassen, indem diese eine Kopie der heute durchgehend digitalisierten Telekommunikationssignale an die Strafverfolgungsbehörden ausleiten“[353] – weshalb für die Inpflichtnahme des Dienstleisters nach § 100b III StPO freilich vom *Regelfall* der Maßnahmeumsetzung nach §§ 100a, 100b StPO gesprochen werden darf –, jedoch „eine Obliegenheit der Strafverfolgungsbehörden, Telekommunikationsüberwachungsmaßnahmen stets unter Mitwirkung eines Telekommunikationsdienstleisters durchzuführen, […] damit allerdings nicht begründet [wird]“[354] Die Vorschrift des § 100a I StPO enthalte vielmehr „eine nicht durch die Mitwirkung der Telekommunikationsdienstleister bedingte Befugnis […], Telekommunikation zu überwachen und aufzuzeichnen“[355], weshalb „nach Maßgabe der gerichtlichen Anordnungsentscheidung […] die Strafverfolgungsbehörden daher auch berechtigt [sind], Überwachungsmaßnahmen ausschließlich mit eigenen Mitteln durchzuführen“[356]. Dies steht auch in Einklang mit dem Wortlaut des Gesetzes, wonach zwar der zur Mitwirkung Verpflichteten gemäß § 100b III S. 1 StPO auf Grund der Anordnung Maßnahmen zu ermöglichen und erforderliche Auskünfte zu erteilen hat, eine entsprechende Verpflichtung der Ermittlungsbehörden, die gesetzlichen Mitwirkungspflichten auch konkret in Anspruch zu nehmen, aber in § 100b III StPO gerade nicht enthalten ist. Eine derartige Verpflichtung der Ermittlungsbehörden geht auch nicht als selbstverständliche Voraussetzung aus dem Sinn und Zweck der Regelung hervor[357], da diese in erster Linie nur für eine Erleichterung der Ermittlungstätigkeit sorgen will, indem sie die „Herren“ der jeweiligen Telekom-

---

351 Vgl. *Bär*, TK-Überwachung, § 100a StPO, Rn. 32; *ders.*, MMR 2008, 215 (219); auch Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 8; KK – *Nack*, StPO, § 100b, Rn. 11.

352 Vgl. *Bär*, TK-Überwachung, § 100b StPO, Rn. 13.

353 BT-Drs. 16/5846, S. 47.

354 BT-Drs. 16/5846, S. 47.

355 BT-Drs. 16/5846, S. 47.

356 BT-Drs. 16/5846, S. 47, wobei die Angaben nach § 100b II S. 2 Nr. 3 StPO in der Anordnung „auch die Art des technischen Zugriffs“ (S. 47) umfassen.

357 Vgl. auch die Begründung im Gesetzesentwurf BT-Drs. 16/5846, S. 47.

munikationsdienstleistung auf Grund deren Sachnähe und Verfügungsmöglichkeit über den jeweiligen Kommunikationsdienst zur Mitwirkung heranzieht. Die Regelung beabsichtigt jedoch nicht, durch die Mitwirkung hierzu verpflichteter Dritter den Ermittlungsbehörden zusätzliche Hürden für den Zugriff auf Telekommunikation dergestalt in den Weg zu stellen, dass diesen vorgeschrieben wäre, Maßnahmen nach § 100a I StPO stets und zwingend nur über die Inanspruchnahme der nach § 100b III StPO Verpflichteten durchzuführen.

Eine solche Verpflichtung zur (zwingenden) Einbindung und Inanspruchnahme Dritter wäre oftmals für die Erreichung des Ermittlungszweck auch wenig tauglich, wenn nicht gar kontraproduktiv – wie dies nicht zuletzt auch anhand der Umstände verschlüsselter Telekommunikation deutlich wird:

Denn bei Durchführung einer Maßnahme zum Zugriff auf verschlüsselte Telekommunikation würde die Inpflichtnahme des *Netzbetreibers*, der bei softwarebasierter P2P-VoIP[358] lediglich die verschlüsselten (Fremd-)Datenpakete über sein Leitungsnetz transportiert, für sich gesehen wenig Erkenntniswert haben. Der Netzbetreiber könnte technisch und müsste rechtlich zwar eine Kopie der übertragen VoIP-Daten an die Strafverfolgungsbehörden ausleiten, diese würden dann aber dennoch nur in verschlüsselter Form vorliegen, da der Netzbetreiber keinerlei Funktionsherrschaft über die Bearbeitung und Verschlüsselung der VoIP-Daten sowie die zugrunde liegenden (proprietären) Protokolle, Verschlüsselungsalgorithmen etc. des verwendeten VoIP-Programms hat.

Auch die Inpflichtnahme des softwarebasierten *VoIP-Diensteanbieters* (z. B. Skype) – sofern dieser von einer rechtlichen Mitwirkungsverpflichtung überhaupt betroffen ist[359] – würde die Durchführung und das Gelingen der Maßnahme kaum fördern, sondern – im Gegenteil – mitunter sogar erschweren.[360] Denn nach gegenwärtigem Kenntnisstand kann bspw. für die wohl populärste VoIP-Software „Skype“ nicht mit abschließender Gewissheit davon ausgegangen werden, dass ein (Zweit-)*Schlüssel*[361] für die Entschlüsselung der in codierter Form erlangten Daten existiert bzw. bei nur

---

358 Für Einzelheiten zu VoIP über den Computer mittels VoIP-Software, siehe 1. Teil A.I.2.c).

359 Zur umstrittenen Frage, ob und in welchem Umfang softwarebasierte VoIP-Diensteanbieter zur Mitwirkung verpflichtet sind, siehe 2. Teil A.II.6.b); für Einzelheiten zur Mitwirkung Dritter, siehe 2. Teil A.II.6.

360 Für Einzelheiten, siehe 3. Teil A.I.1.c).

361 Zeichenkette/-folge, mit der sich Daten/Dateien ver- und entschlüsseln lassen und deren Länge in Bit angegeben wird, vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 206 u. 130.

temporär gültiger end-to-end-Verschlüsselung überhaupt erlangbar ist, zu dessen Herausgabe das Unternehmen herangezogen werden könnte, noch, dass eine sog. *Backdoor*[362] in die Skype-Software besteht, deren Zugangs- und Nutzungsmöglichkeiten den Strafverfolgungsbehörden zur Verfügung gestellt werden könnte.[363] Entsprechendes sei jedenfalls bislang von Seiten des Unternehmens vorgetragen worden.[364] Diese Umstände als zutreffend unterstellt, würde die Einbindung des jeweiligen VoIP-Diensteanbieters der Sicherstellung einer Überwachbarkeit dieser Form von VoIP-Kommunikation in keiner Weise dienlich sein.

Folgt man daher den (überzeugenden) Argumenten der oben genannten mehrheitlich vertretenen Ansicht, so *können* Ermittlungsbehörden demnach die Mitwirkung der hierzu gemäß § 100b III StPO verpflichteten Dritten in Anspruch nehmen, *müssen* dies jedoch nicht und können vielmehr – soweit entsprechende technische Möglichkeiten bestehen – nach Maßgabe der gerichtlichen Anordnungsentscheidung Überwachungsmaßnahmen nach § 100a I StPO auch selbständig und ausschließlich mit eigenen Mitteln durchführen.

---

362 Eine „Hintertür" (engl. „Backdoor") im computertechnischen Sinne stellt einen (oftmals bewusst durch den Programmierer „von Haus aus" eingebauten) Bestandteil einer Software (bspw. eines Betriebssystems oder eines Anwendungsprogramms) dar, der die Möglichkeit eröffnet, unter Umgehung der normalen Zugriffssicherungen alternativ „über die Hintertür" Zugang in ein System oder in eine an sich geschützte Funktion eines Programms zu erhalten, vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 24.

363 Vgl. Anm. *Bär*, MMR 2011, 691 (691 f.); so auch die Antwort des Parl. Staatssekretärs beim Bundesminister des Innern, *Bergner*, für die Bundesregierung im Rahmen der 135. Sitzung des Deutschen Bundestags am 26.10.2011 (BT-PlPr. 17/135 16064 D), wonach es in den Fällen P2P-geführter VoIP zwischen zwei internetfähigen Endgeräten (softwarebasierte P2P-VoIP) „Skype […] nach derzeitigem Kenntnisstand der Bundesregierung schon aus technischen Gründen nicht möglich [ist], Inhaltsdaten den Justiz-, Strafvollzugs- oder Regierungsbehörden zur Verfügung zu stellen" (16064 D); a. A. hingegen *Braun*/*Roggenkamp*, K&R 2011, 681 (685) m. w. N., *Hoffmann-Riem*, JZ 2008, 1009 (1021) m. w. N. wie auch *Buermeyer*, http://ijure.org/wp/archives/756 (zuletzt aufgerufen 15.06.2012) m. w. N., regelmäßig jedoch unter der Einschränkung, dass nicht zu 100 Prozent gewiss sei, ob tatsächlich eine solche Möglichkeit konkret bestehe.

364 So bspw. *Bär*, persönliches Gespräch mit dem Verfasser, Bamberg, 09.12.2010, der in diesem Zusammenhang auch auf ein Treffen von Eurojust (*Europäische Einheit für justizielle Zusammenarbeit*) im Jahr 2006 hinweist, bei dem Skype betont habe, weder einen Schlüssel zur Entschlüsselung zu besitzen noch über eine sog. Backdoor in das Programm zu verfügen; hierauf deutet indes auch eine Stellungnahme von Skype im Rahmen der Anhörung durch die Bundesnetzagentur im Jahr 2004 hin, wonach „eine ‚Hintertür' in die Software […] zu vielen Probleme [sic] führen [würde]" (S. 16), abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Stellungnahmen/SkypeTechnologiesId714pdf.pdf?__blob=publicationFile (zuletzt aufgerufen 15.06.2012); für Einzelheiten, siehe auch 3. Teil A.I.1.c).

Zugunsten der Zulässigkeit von Quellen-TKÜ-Maßnahmen de lege lata lässt sich somit festhalten, dass die Vorschrift des § 100a I StPO – unter Berücksichtigung des der Gesetzesbegründung entnehmbaren Willens des Gesetzgebers wie auch unter grammatischen, gesetzessystematischen und teleologischen Aspekten – insoweit eine nicht durch die Mitwirkung der jeweiligen Telekommunikationsdiensteanbieter bedingte Befugnis zur Überwachung und Aufzeichnung von Telekommunikation enthält, der auch nicht die Regelung des § 100b III StPO entgegensteht.

III. Verwertbarkeit der Erkenntnisse

1. Kernbereichsschutz gemäß § 100a IV StPO

Im Rahmen seiner Grundsatzentscheidung zum „Großen Lauschangriff“[365] vom 03.03.2004 legte das BVerfG die Grundsätze zur Erhebung und Verwertung von Erkenntnissen aus dem höchstpersönlichen Bereich des Betroffenen fest, die mittels heimlicher Ermittlungsmaßnahmen erlangt worden sind. Es stellte hierzu in Einklang mit der bisherigen Rspr. des BVerfG fest, dass „zur Unantastbarkeit der Menschenwürde gem. Art. 1 I GG […] die Anerkennung eines absolut geschützten Kernbereichs privater Lebensgestaltung [gehört]“[366], in den nicht eingegriffen werden dürfe. Führt die Ermittlungsmaßnahme „gleichwohl zur Erhebung von Informationen aus dem absolut geschützten Kernbereich privater Lebensgestaltung, muss sie abgebrochen werden und Aufzeichnungen müssen gelöscht werden; jede Verwertung solcher Informationen ist ausgeschlossen“.[367] Ein Zugriff auf Daten mit entsprechenden kernbereichsrelevanten Informationen ist „insoweit nicht zu rechtfertigen“[368]. Die in Art. 1 I GG grundrechtlich garantierte Unantastbarkeit der Menschenwürde fordert hierbei „auch im Gewährleistungsbereich des Art. 10 GG Vorkehrungen zum Schutz individueller Entfaltung im Kernbereich privater Lebensgestaltung“[369], da nicht ausgeschlossen werden kann, dass bei Erfassung von Telekommunikationsinhalten auch personenbezogene Daten betroffen sind, deren Informationen dem Kernbereich der höchstpersönlichen Lebensgestaltung entstammen.[370] Eine Zuordnung zu diesem Kernbereich ist insbesondere davon abhängig, ob die jeweiligen

365 BVerfG NJW 2004, 999.

366 BVerfG NJW 2004, 999 (999); vgl. zu dessen Garantie bereits BVerfG NJW 1957, 297; BVerfG NJW 1969, 1707; BVerfG NJW 1972, 1123; BVerfG NJW 1973, 891; BVerfG NJW 1990, 563.

367 BVerfG NJW 2004, 999 (999).

368 BVerfG NJW 2009, 2431 (2437).

369 BVerfG NJW 2009, 2431 (2436).

370 Vgl. BVerfG NJW 2009, 2431 (2436).

personenbezogenen Kommunikationsdaten ihrem Inhalt nach „höchstpersönlichen Charakter“[371] aufweisen und „in welcher Art und Intensität sie aus sich heraus die Sphäre anderer oder Belange der Gemeinschaft berühr[en]“[372]. Maßgebend sind nach gefestigter Rspr. des BVerfG insoweit die „Besonderheiten des jeweiligen Einzelfalls“[373]. Nicht zu dem Kernbereich privater Lebensgestaltung gehören nach dieser Rspr. hingegen „Kommunikationsinhalte, die in unmittelbarem Bezug zu konkreten strafbaren Handlungen stehen, wie etwa Angaben über die Planung bevorstehender oder Berichte über begangene Straftaten“[374].

Der Schutz des Kernbereichs privater Lebensgestaltung ist im Rahmen des Fernmeldegeheimnisses nach Art. 10 I GG indes in anderer Weise ausgestaltet als im Rahmen des Grundrechts auf Unverletzlichkeit der Wohnung nach Art. 13 I GG.[375]

Art. 13 I GG räumt dem Verhalten in der Privatwohnung, welches der individuellen Entfaltung im höchstpersönlichen Bereich zuzurechnen ist (bspw. Empfindungen, Gefühle, Überlegungen, Ansichten, Erlebnisse etc.), absoluten Schutz ein.[376] Die Privatwohnung diene hierbei als „räumliches Substrat“[377] zur freien Entfaltung nach „selbst gesetzten Maßstäben“[378] und als letzter Rückzugs- und Zufluchtsort, der zur Wahrung der Menschenwürde genutzt werden könne, ohne befürchten zu müssen, der Überwachung durch staatliche Stellen ausgesetzt zu sein.[379]

Art. 10 I GG gewährleistet indes die freie Persönlichkeitsentfaltung des Einzelnen durch Zubilligung eines „privaten, vor der Öffentlichkeit verborgenen Austauschs von Kommunikation“[380]. Da der Bürger allerdings zur Wahrnehmung höchstpersönlicher Kommunikation nicht in der gleichen Weise auf Telekommunikation angewiesen ist, wie auf seine Wohnung, sind in Art. 10 GG, anders als in Art. 13 GG, die Voraussetzungen für Eingriffe nicht ausdrücklich normiert, sondern nur in den allgemeinen rechtsstaatlichen Anforderungen enthalten. Der Grundsatz des Art. 1 I GG erfordert

---

371 BVerfG NJW 2009, 2431 (2436).

372 BVerfG NJW 2009, 2431 (2436).

373 BVerfG NJW 2009, 2431 (2436); vgl. auch BVerfG NJW 1990, 563; BVerfG NJW 2004, 999. BVerfG NJW 2005, 2603.

374 BVerfG NJW 2009, 2431 (2436); bereits BVerfG NJW 1990, 563 (564); BVerfG NJW 2005, 2603 (2612).

375 Vgl. BVerfG NJW 2005, 2603 (2612).

376 Vgl. BVerfG NJW 2004, 999 (1002).

377 BVerfG NJW 2005, 2603 (2612).

378 BVerfG NJW 2004, 999 (1002).

379 Vgl. BVerfG NJW 2004, 999 (1002); BVerfG NJW 2005, 2603 (2612).

380 BVerfG NJW 2005, 2603 (2612).

aber auch in den Fällen des Art. 10 I GG Vorkehrungen zum Schutz der individuellen Entfaltung im höchstpersönlichen Bereich.[381]

Mit diesem verfassungsrechtlichen Hintergrund wurden vom Gesetzgeber für die in das Grundrecht auf Unverletzlichkeit der Wohnung eingreifenden Maßnahmen der akustischen Wohnraumüberwachung nach §§ 100c ff. StPO strengere Anforderungen an den Kernbereichsschutz (vgl. § 100c IV StPO) verankert als für Maßnahmen der Überwachung und Aufzeichnung von Telekommunikation nach §§ 100a, 100b StPO (vgl. § 100a IV StPO) unter Eingriff in das Fernmeldegeheimnis.

Auch für die *Quellen-TKÜ* als Maßnahme zur Überwachung und Aufzeichnung von Telekommunikation stellt sich die Frage nach dem Schutz kernbereichsrelevanter Inhalte, welche im Rahmen der Überwachung von VoIP-Kommunikation anfallen. Denn wie normale Telefongespräche über das Festnetz werden auch Gespräche, die über das Internet mittels VoIP stattfinden, zum Zwecke des Austauschs verschiedenster Arten von Informationen, insbesondere (bzw. gerade) aus dem privaten Bereich, zwischen den Gesprächsteilnehmern geführt. Bei Maßnahmen, die der Erfassung von Kommunikationsinhalten dienen, kann somit nicht ausgeschlossen werden, dass hierbei auch Daten erhoben werden, die dem Kernbereich privater Lebensgestaltung[382] entstammen.[383] Die Beurteilung, ob eine personenbezogene Kommunikation diesem unantastbaren Kernbereich zuzuordnen ist, „hängt davon ab, in welcher Art und Intensität sie aus sich heraus die Sphäre anderer oder Belange der Gemeinschaft berührt“[384], ihrem Inhalt nach also höchstpersönlichen Charakter aufweist.[385] Die Frage der Zugehörigkeit und daran anschließend der Verwertbarkeit der erlangten Erkenntnisse ist damit vom Charakter und von der Bedeutung des Inhalts der jeweiligen Kommunikation bedingt.[386] Nicht zu dem unantastbaren Kernbereich privater Lebensgestaltung zählen Kommunikationsinhalte, die einen unmittelbaren Bezug zu konkreten strafbaren Handlungen aufweisen, also z. B. Angaben über die Planung bevorstehender oder Mitteilungen über begangene Straftaten (vgl. oben).[387]

---

381 Vgl. BVerfG NJW 2005, 2603 (2612).

382 Grundsätzlich hierzu BVerfG NJW 2004, 999 (102).

383 Vgl. BVerfG NJW 2005, 2603 (2611 f.).

384 BVerfG NJW 2005, 2603 (2611 f.).

385 Vgl. bereits BVerfG NJW 1990, 563 (564); ebenso BVerfG NJW 2004, 999 (1002).

386 Vgl. BVerfG NJW 1990, 563 (564).

387 Vgl. BVerfG NJW 1990, 563 (564); BVerfG NJW 2005, 2603 (2612); BVerfG NJW 2009, 2431 (2436).

Für die Anforderungen an dem Kernbereichsschutz bei heimlichen Maßnahmen unter Zugriff auf informationstechnische Systeme hat das BVerfG im Rahmen seiner Entscheidung vom 27.02.2008 ebenfalls grundlegende Aussagen getroffen:

So haben gemäß st. Rspr. des BVerfG heimliche Überwachungsmaßnahmen staatlicher Stellen einen unantastbaren Kernbereich der privaten Lebensgestaltung, dessen Schutz sich aus Art. 1 I GG herleitet, zu wahren.[388]

Die Gefahr, dass die handelnde staatliche Stelle solche persönlichen Daten erhebt, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, besteht auch im Rahmen eines Zugriffs auf ein informationstechnisches System.[389] So könne das informationstechnische System,

> „soweit es telekommunikativen Zwecken dient, zur Übermittlung von Inhalten genutzt werden, die gleichfalls dem Kernbereich unterfallen können. Dies gilt nicht nur für Sprachtelefonate, sondern auch etwa für die Fernkommunikation mittels E-Mails oder anderer Kommunikationsdienste des Internet […]. Die absolut geschützten Daten können bei unterschiedlichen Arten von Zugriffen erhoben werden, etwa bei der Durchsicht von Speichermedien ebenso wie bei der Überwachung der laufenden Internetkommunikation oder gar einer Vollüberwachung der Nutzung des Zielsystems“[390].

Aus diesem Grunde bedürfe es bei heimlichen Zugriffen auf informationstechnische Systeme besonderer gesetzlicher Vorkehrungen, die den Kernbereich privater Lebensgestaltung schützen.[391] Die Heimlichkeit des Zugriffs verhindere es nämlich, dass der Betroffene vor oder während der Maßnahme selbst darauf hinwirken kann, dass die handelnde staatliche Stelle den Kernbereich privater Lebensgestaltung achtet. Dem daraus folgenden vollständigen Kontrollverlust sei durch solche besonderen Regelungen zu begegnen, die die Gefahr von Kernbereichsverletzungen durch geeignete Verfahrensvorkehrungen abschirmen.[392]

Hierbei können

> „die verfassungsrechtlichen Anforderungen an die konkrete Ausgestaltung des Kernbereichsschutzes […] je nach der Art der Informationserhebung und der durch sie erfassten Informationen unterschiedlich sein“[393].

---

388 Vgl. BVerfG NJW 2008, 822 (833); bereits BVerfG NJW 1957, 297; BVerfG NJW 1969, 1707; BVerfG NJW 1972, 1123; BVerfG NJW 1973, 891; BVerfG NJW 1990, 563; BVerfG NJW 2004, 999; BVerfG NJW 2005, 2603.

389 Vgl. BVerfG NJW 2008, 822 (833).

390 BVerfG NJW 2008, 822 (833).

391 Vgl. BVerfG NJW 2008, 822 (833).

392 Vgl. BVerfG NJW 2008, 822 (833).

393 BVerfG NJW 2008, 822 (834).

Eine gesetzliche Ermächtigung zu Überwachungsmaßnahmen, die den Kernbereich privater Lebensgestaltung berühren können, habe

> „so weitgehend wie möglich sicherzustellen, dass Daten mit Kernbereichsbezug nicht erhoben werden. Ist es – wie bei dem heimlichen Zugriff auf ein informationstechnisches System – praktisch unvermeidbar, Informationen zur Kenntnis zu nehmen, bevor ihr Kernbereichsbezug bewertet werden kann, muss für hinreichenden Schutz in der Auswertungsphase gesorgt sein“[394].

Insbesondere müssen hierbei gemäß wiederholter Rspr. des BVerfG gewonnene Daten mit Kernbereichsbezug unverzüglich gelöscht sowie ihre Verwertung ausgeschlossen werden.[395]

Die zumindest überwiegend erfolgende automatisierte Datenerhebung im Rahmen heimlicher Zugriffe auf informationstechnische Systeme erschwere es indes im Vergleich zu einer durch Personen durchgeführten Erhebung, Daten mit und ohne Bezug zum Kernbereich privater Lebensgestaltung schon bei deren Erhebung zu unterscheiden.[396] Doch selbst dann, wenn der Datenzugriff bspw. bei einer persönlichen Überwachung der über das Internet geführten Sprachtelefonie unmittelbar durch Personen ohne vorherige (automatisierte) technische Aufzeichnung erfolgt, stoße ein Kernbereichsschutz auf Ebene der Datenerhebung auf praktische Schwierigkeiten, da bei der Durchführung derartiger Maßnahmen (wie bei Telekommunikationsüberwachungen generell der Fall) regelmäßig nicht sicher vorhersehbar ist, welche Inhalte die erhobenen Daten haben werden bzw. eine Analyse während der Datenerhebung bspw. durch fremdsprachliche Telefongespräche erschwert werden kann.[397] In solchen Fällen sei es allerdings

> „verfassungsrechtlich nicht gefordert, den Zugriff wegen des Risikos einer Kernbereichsverletzung auf der Erhebungsebene von vornherein zu unterlassen“[398].

Vielmehr lasse sich

> „der verfassungsrechtlich gebotene Kernbereichsschutz […] im Rahmen eines zweistufigen Schutzkonzepts gewährleisten“[399].

Da sich in vielen Fällen die Kernbereichsrelevanz der erhobenen Daten vor oder bei der Erhebung der Daten nicht klären lassen wird (vgl. oben), habe

---

394 BVerfG NJW 2008, 822 (834).

395 Vgl. BVerfG NJW 2008, 822 (834); auch BVerfG NJW 2004, 999 und BVerfG NJW 2005, 2603.

396 Vgl. BVerfG NJW 2008, 822 (834).

397 Vgl. BVerfG NJW 2008, 822 (834).

398 BVerfG NJW 2008, 822 (834).

399 BVerfG NJW 2008, 822 (834).

„der Gesetzgeber […] durch geeignete Verfahrensvorschriften sicherzustellen, dass dann, wenn Daten mit Bezug zum Kernbereich privater Lebensgestaltung erhoben worden sind, die Intensität der Kernbereichsverletzung und ihre Auswirkungen für die Persönlichkeit und Entfaltung des Betroffenen so gering wie möglich bleiben“[400].

Die Telekommunikationsüberwachung nach §§ 100a, 100b StPO hat indes mit § 100a IV StPO eine gesetzliche Normierung der Kernbereichsrechtsprechung des BVerfG erfahren, die bei Überwachungsmaßnahmen (in nicht unumstrittener[401] aber – nunmehr auch höchstrichterlich festgestellter[402] – verfassungsrechtlich ausreichender Weise[403]) dafür Sorge trägt, dass Telekommunikation aus dem Kernbereich privater Lebensgestaltung vor staatlichem Zugriff angemessen geschützt ist:

Auf Grund der Regelung des § 100a IV S. 1 StPO hat ein Eingriff nach § 100a I StPO zu unterbleiben, wenn von vornherein absehbar ist, dass die Maßnahme „allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung“ liefern würde. Eine Überwachungsmaßnahme ist in diesen (eher sel-

---

400 BVerfG NJW 2008, 822 (834).

401 Zur Problematik der gesetzlichen Maßgabe „alleiniger“ Kernbereichsbetroffenheit nach § 100a IV S. 1 StPO, vgl. krit. *Puschke*/*Singelnstein*, NJW 2008, 113 (114) m. w. N.; auch Bundesrechtsanwaltskammer, Stellungnahme zum Gesetzentwurf der Bundesregierung zum Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (BR-Drucks. 275/07), S. 29 f., abrufbar unter http://www.brak.de/w/files/stellungnahmen/Stn31-2007.pdf (zuletzt aufgerufen 15.06.2012); krit. auch *Becker*/*Meinicke*, StV 2011, 50 (51) („verfassungsrechtlich höchst bedenkliche § 100a Abs. 4 StPO“); infrage stellend auch *Eckhardt*, CR 2007, 336 (336) („politisches Placebo“); zust. hingegen *Bär*, TK-Überwachung, § 100a StPO, Rn. 42 ff. m. w. N., der die Entscheidung des Gesetzgebers zur Regelung des Kernbereichsschutzes in der Weise, wie in § 100a IV StPO erfolgt, als „allein praxisgerecht“ (Rn. 42) bezeichnet; *ders*., MMR 2008, 215 (217); ebenso Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 24.

402 So hat das BVerfG in einer kürzlich ergangenen Entscheidung (BVerfG, Beschl. v. 12.10.2011, Az.: 2 BvR 236/08, 2 BvR 237/08, 2 BvR 422/08) unter Zurückweisung mehrerer Verfassungsbeschwerden bezüglich der zum 01.01.2008 in Kraft getretenen Neuregelung der strafprozessualen Telekommunikationsüberwachung (BGBl. I S. 3198) nunmehr höchstrichterlich festgestellt, dass „die durch § 100a Abs. 4 StPO geschaffenen Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung bei der Telekommunikationsüberwachung […] sowohl auf der Erhebungsebene als auch in der Auswertungsphase [= zweistufiges Schutzkonzept, Anm. d. Verf.] den verfassungsrechtlichen Anforderungen [genügen]“ (Abs.-Nr. 209).

403 Insbesondere auf Grund des in der Auswertungsphase zu beachtenden Beweisverwertungsverbotes nach § 100a IV S. 2 StPO; vgl. im Einzelnen BVerfG, Beschl. v. 12.10.2011, Az.: 2 BvR 236/08, 2 BvR 237/08, 2 BvR 422/08, Abs.-Nr. 210 ff.

tenen[404]) Fällen *ausschließlicher* Kernbereichsbetroffenheit bereits unzulässig. Es besteht insoweit ein Beweiserhebungsverbot.

In allen anderen Fällen sind kernbereichsrelevante Informationen, die im Rahmen einer zulässigen Maßnahme nach § 100a I StPO erlangt wurden, über § 100a IV S. 2 StPO von einer Verwertung ausgeschlossen. Dieser Schutz von Telekommunikationsinhalten aus dem höchstpersönlichen Bereich erst auf „zweiter Stufe" (Beweisverwertungsverbot) ist verfassungsrechtlich (ausnahmsweise) zulässig, da die erhöhten Voraussetzungen des § 100a I StPO, insbesondere das Erfordernis einer „schwere Straftat" nach § 100a I Nr. 1, II StPO, die gesteigerten Anforderungen erfüllen, für die das Risiko einer Erhebung („erste Stufe") von kernbereichsrelevanten Bestandteilen ausnahmsweise hinzunehmen ist[405] und die Vorgaben des § 100a IV S. 3 und S. 4 StPO als bereichsspezifische grundrechtssichernde Verfahrensregelungen[406] zudem sicherstellen, dass Aufzeichnungen hierüber unverzüglich gelöscht werden, soweit es zu einer Erhebung gekommen sein sollte, und die Tatsache ihrer Erlangung und Löschung aktenkundig gemacht wird.

Ob das Schutzkonzept des § 100a IV StPO in angemessener Weise auch den Gegebenheiten einer Quellen-TKÜ Rechnung trägt, ist Gegenstand der Untersuchungen in Teil 3 im Rahmen der Beurteilung und Ausarbeitung verschiedener Lösungsmodelle.[407]

2. Verwertbarkeit bei formellen oder materiellen Mängeln der Anordnung

Formelle oder materielle Mängel der *Anordnung*[408] einer (Quellen-)TKÜ-Maßnahme (*Anordnungsebene*) können Verwertungsverbote hinsichtlich der erlangten Erkenntnisse nach sich ziehen. Da Verwertungsverbote einen der wesentlichsten Grundsätze des Strafprozessrechts, nämlich die Pflicht des Gerichts, die Wahrheit zu erforschen und die hierzu erforderliche Beweisaufnahme von Amts wegen auf sämtliche Tatsachen und Beweismittel zu erstrecken, die von Bedeutung sein können, beschneiden[409], stellt ein sol-

---

404 Da Telekommunikation i. d. R. durch verschiedene Inhalte geprägt ist, wird das Beweiserhebungsverbot des § 100a IV S. 1 StPO im Gros der Fälle wohl nicht einschlägig sein, vgl. auch *Bär*, MMR 2008, 215 (217).

405 Vgl. entsprechend BVerfG NJW 2005, 2603 (2612).

406 Zu grundrechtssichernden Verfahrensregelungen im Zusammenhang mit Quellen-TKÜ-Maßnahmen, siehe 3. Teil A.I.1.d).

407 Siehe hierzu die Ausführungen unter 3. Teil B.II.2.

408 Für Einzelheiten zu den inhaltlichen Anforderungen einer Quellen-TKÜ-Anordnung, siehe 3. Teil A.I.2.; für einen Beschlussvorschlag, siehe Anhang 1.

409 Vgl. BGH NJW 1999, 959 (961).

ches Verbot stets „eine Ausnahme [dar], die nur nach ausdrücklicher gesetzlicher Vorschrift […] oder aus übergeordneten wichtigen Gründen im Einzelfall anzuerkennen ist“[410].

Als spezielles, gesetzlich ausdrücklich normiertes Verwertungsverbot schließt die Regelung des § 100a IV S. 2 StPO für Erkenntnisse aus dem Kernbereich privater Lebensgestaltung (siehe oben) jedwede Verwertung des erfassten kernbereichsrelevanten Materials – sowohl zu Beweiszwecken wie auch als Spurenansätze – aus.[411] Daneben können sich Beschränkungen in der Verwertbarkeit der mittels (Quellen-)TKÜ-Maßnahme aus der (an der Quelle) überwachten (VoIP-)Telekommunikation erlangten Erkenntnisse auch aus den allgemeinen Grundsätzen ergeben[412], sofern gegen formelle und/oder materielle Anordnungsvoraussetzungen der §§ 100a, 100b StPO verstoßen wurde.[413] Soweit der Beschuldigte entsprechende Verstöße für gegeben erachtet, die ein Verwertungsverbot begründen könnten, muss er als Angeklagter in der Hauptverhandlung rechtzeitig der Verwertung der potentiell widerrechtlich erlangten Erkenntnisse widersprechen (sog. *Widerspruchslösung*[414]).

Verstöße gegen *formelle Vorschriften* führen nicht in jedem Fall automatisch auch zu einem Verwertungsverbot für erlangte Erkenntnisse. Dies gilt vor allem für „einfache“ formelle Fehler. Hierzu zählen bspw. das Schriftformerfordernis aus § 100b II S. 1 StPO sowie die formellen Vorschriften des § 100b I StPO zur Zuständigkeit[415]:

Sofern die Überwachung *nicht schriftlich*, sondern – entgegen den formalen Vorgaben des § 100b II S. 1 StPO – nur mündlich angeordnet wurde, liegt ein Verstoß gegen gesetzliche Formvorschriften vor. Dieser an sich begründet allerdings nach Auffassung des BGH noch kein Verwertungsverbot für (im Übrigen rechtmäßig) erlangte Erkenntnisse.[416] Allein die mit einer bspw. fernmündlich erfolgten richterlichen Anordnung einhergehende unzureichende Dokumentation der richterlichen Entscheidung führt nicht zu einem Beweisverwertungsverbot.[417]

---

410 BGH NJW 1990, 1801 (1801).

411 Vgl. *Bär*, TK-Überwachung, § 100a StPO, Rn. 44 u. 63; auch BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 102; gleiches gilt demnach auch zum Schutz besonderer Vertrauensverhältnisse unter den Voraussetzungen des § 160a I S. 2 StPO für zeugnisverweigerungserhebliche Erkenntnisse aus Maßnahmen, die sich gegen die dort genannten zeugnisverweigerungsberechtigten Berufsgeheimnisträger richten.

412 Vgl. KK – *Nack*, StPO, § 100a, Rn. 53.

413 Vgl. *Bär*, TK-Überwachung, § 100a StPO, Rn. 51.

414 Vgl. BGH NJW 2006, 1361 (1361).

415 Vgl. *Bär*, TK-Überwachung, § 100a StPO, Rn. 53; BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 83.

416 Vgl. BGH NStZ 1996, 48 (48).

Bei Verstößen gegen die verfahrensmäßigen Bestimmungen des § 100b I StPO ist zu differenzieren: Nicht jeder Verstoß gegen *Zuständigkeitsvorschriften* begründet automatisch auch ein Verwertungsverbot für erlangte Erkenntnisse.[418] Ein derartiger Automatismus ist weder ausdrücklich in der StPO geregelt noch dem Strafprozessrecht als allgemeiner Grundsatz entnehmbar. Vielmehr ist auf die Umstände des Einzelfalles abzustellen.[419] Grundlegende Verfahrensverstöße bei der Maßnahmeanordnung können zur Unverwertbarkeit führen.[420] Wegen des besonderen Gewichts von Verfahrensverstößen bei Maßnahmen nach §§ 100a, 100b StPO[421] kommt ein Verwertungsverbot jedenfalls dann in Betracht, wenn die Erkenntnisse aus einer (Quellen-)TKÜ unter völliger Umgehung der Vorgaben der §§ 100a, 100b StPO ohne Anordnung durch das Gericht oder die Staatsanwaltschaft und somit auch außerhalb jeglicher richterlicher (im Rahmen der Anordnungskompetenz nach § 100b I S. 1 StPO oder zumindest durch nachträgliche Bestätigung nach § 100b I S. 3 StPO) oder staatsanwaltschaftlicher (im Rahmen der Eilkompetenz nach § 100b I S. 2 StPO) Prüfung und Legitimierung gewonnen wurden.[422] Gleiches gilt, wenn die Überwachung entgegen § 100b I S. 1 StPO durch polizeiliche Ermittlungspersonen angeordnet wurde[423]. Tritt hingegen die staatsanwaltschaftliche Eilanordnung gemäß § 100b I S. 2 StPO wegen fehlender richterlicher Bestätigung binnen drei Werktagen[424] nach § 100b I S. 3 StPO außer Kraft, so bleiben die bis dahin auf Grund der Eilanordnung rechtmäßig gewonnenen Erkenntnisse grds. verwertbar.[425]

Ein Verwertungsverbot kommt daneben – abhängig von den Umständen des Einzelfalls – auch bei einem Überschreiten der im Beschluss festge-

---

417 Vgl. BGH NJW 2005, 1060 (1061).

418 Vgl. KK – *Nack*, StPO, § 100a, Rn. 55.

419 Vgl. BGH NJW 1999, 959 (960 f.).

420 Vgl. BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 82.

421 Vgl. BGH NJW 1999, 959 (961).

422 Vgl. BGH NJW 1983, 1570 (1571); KK – *Nack*, StPO, § 100a, Rn. 55 m. w. N.; Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 35 m. w. N.

423 Vgl. BGH NJW 1983, 1570 (1571).

424 Wobei in Anlehnung an die Rspr. des BGH zu der in Ausnahmefällen nicht zwangsläufigen Annahme eines Verwertungsverbotes bei versehentlicher kurzzeitiger Lücke zwischen Erst- und Verlängerungsanordnung, BGH NJW 1999, 959 (961), Entsprechendes auch für eine nur marginale Lücke zwischen staatsanwaltschaftlicher Eilanordnung und deren richterlicher Bestätigung (§ 100b I S. 2, S. 3 StPO) angenommen wird, vgl. BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 82; auch *Bär*, TK-Überwachung, § 100a StPO, Rn. 53.

425 Vgl. zutr. *Bär*, TK-Überwachung, § 100b StPO, Rn. 4; Meyer-Goßner – *Cierniak*, StPO, § 100b, Rn. 1 m. w. N.; dies gilt jedoch nicht bei willkürlicher Annahme von Gefahr im Verzug.

legten *Befristung* der (Quellen-)TKÜ-Maßnahme[426] sowie bei einem *Wegfall* der Anordnungsvoraussetzungen nach Erlass (§ 100b IV StPO) in Betracht.[427]

Willkürlich angeordnete Maßnahmen hingegen begründen nach gefestigter höchstrichterlicher Rspr.[428] ein Verwertungsverbot für gewonnenen Erkenntnisse.[429] Dies gilt auch bei Anordnungen der Staatsanwaltschaft, wenn nach den Umständen des Einzelfalls der grundrechtssichernde Richtervorbehalt des § 100b I S. 1 StPO durch willkürliche Annahme des Vorliegens von Gefahr im Verzug umgangen wurde.[430] Hingegen ist von Unverwertbarkeit der erlangten Erkenntnisse grds. nicht auszugehen, wenn die Einschätzung der Staatsanwaltschaft, Gefahr im Verzug sei gegeben, irrtümlich erfolgte und die Annahme vertretbar war.[431]

Auch eine unzureichende *Begründung*[432] der richterlichen (§ 100b I S. 1 StPO) oder (bei Gefahr im Verzug) staatsanwaltschaftlichen (§ 100b I S. 2 StPO, ggf. nach § 100b I S. 3 StPO richterlich bestätigten) Anordnung führt nicht per se zur Unverwertbarkeit erlangter Erkenntnisse.[433] Ausschlaggebend sind nach Auffassung des BGH „vielmehr die tatsächlichen Voraussetzungen zum Zeitpunkt der Entscheidung über die Überwachung der Telekommunikation“[434]. Daher muss bspw. die ermittlungsrichterliche Verwendung ausschließlich vorgefertigter Textbausteine oder eine ergänzende Verweisung auf Bestandteile der Ermittlungsakte[435], ohne dass in der An-

---

426 Vgl. KK – *Nack*, StPO, § 100a, Rn. 55; zum Ausnahmefall des versehentlichen Unterlassens der rechtzeitigen Einholung einer (im dortigen Fall ohne weiteres erteilbaren) richterlichen Verlängerungsanordnung, wodurch während einer kurzfristigen Lücke zwischen Fristende der richterlichen Erstanordnung und Erlass der Verlängerungsanordnung eine Überwachung ohne rechtfertigende richterliche Anordnung stattgefunden hat, was nicht zwangsläufig zur Unverwertbarkeit der in dieser kurzen Zeitspanne gewonnenen Erkenntnis führen muss, BGH NJW 1999, 959 (961); vgl. hierzu auch BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 82.

427 Vgl. KK – *Nack*, StPO, § 100a, Rn. 55.

428 BGH NJW 1979, 990 (990); BGH NJW 1995, 1974 (1974 f.); BGH NJW 2007, 2269 (2272); BVerfG NJW 2005, 1917 (1923).

429 So KK – *Nack*, StPO, § 100a, Rn. 54 m. w. N.

430 Vgl. BVerfG NJW 2001, 1121 (1125); BGH NStZ 2004, 449 (450); BGH NJW 2007, 2269 (2272).

431 Vgl. BGH BeckRS 2006, 05646; KK – *Nack*, StPO, § 100a, Rn. 54; *Bär*, TK-Überwachung, § 100a StPO, Rn. 53.

432 Für Einzelheiten zur Formulierung der Begründung eines Quellen-TKÜ-Beschlusses, siehe 3. Teil A.I.2. sowie Anhang I.

433 Vgl. BGH BeckRS 2006, 05646; BGH NJW 2003, 368 (369 f.); *Bär*, TK-Überwachung, § 100a StPO, Rn. 53 sowie 58.

434 BGH BeckRS 2006, 05646.

435 Vgl. BGH NJW 1986, 390 (391); BGH NJW 2003, 368 (369 f.).

ordnungsbegründung eine nähere Unterlegung der im Beschluss getroffenen rechtlichen Feststellungen mit tatsächlichen, fallbezogenen Anhaltspunkten stattfand, nicht zwingend zu einem Verwertungsverbot für erlangte Erkenntnisse führen.[436] Vielmehr hat das erkennende Gericht eines sich anschließenden Straf- oder Revisionsverfahrens den Ermittlungsstand (Verdachts- und Beweislage) zum Zeitpunkt des ermittlungsrichterlichen Beschlusserlasses anhand der – ggf. aus einem anderen Verfahren beizuziehenden – Ermittlungsakten eigenständig zu rekonstruieren und auf dieser Grundlage die in der Anordnung getroffenen rechtlichen Feststellungen und Wertungen auf deren Vertretbarkeit hin zu untersuchen.[437] Von einem Beweisverwertungsverbot ist nur in den Fällen auszugehen, in denen trotz der Nachprüfung durch das erkennende Gericht weiterhin erhebliche Zweifel an der Vertretbarkeit der ermittlungsrichterlich getroffenen rechtlichen Würdigung der Verdachts- und Beweislage bestehen und eine Nachvollziehbarkeit der Anordnung nicht gegeben ist.[438] Gleiches dürfte auch bei rein schematisch gehaltenen Beschlüssen der Fall sei, welche bspw. durch die Polizei bereits vorgefertigt wurden und – statt der notwendigen richterlichen Einzelfallprüfung zumindest in groben Zügen – nur schematische richterliche Tätigkeit erkennen lassen.[439]

Bei Vorliegen *materieller Mängel* in der Anordnung, insbesondere bei Fehlen wesentlicher sachlicher Voraussetzungen für die Gestattung einer (Quellen-)TKÜ-Maßnahme, ist zu differenzieren[440]:

Lag die Anordnungsvoraussetzung des Verdachts einer *Katalogstraftat* (§ 100a I Nr. 1, II StPO) von vornherein nicht vor, bspw. weil die Überwa-

---

436 Vgl. BGH NJW 1986, 390 (391); BGH NJW 2003, 368 (369 f.); vgl. auch *Bär*, TK-Überwachung, § 100a StPO, Rn. 58.

437 Vgl. BGH NJW 2003, 368 (369 f.); bereits BGH NJW 1995, 1974 (1975); ebenso BGH NJW 2006, 1361 (1362); auch BGH NStZ-RR 2006, 370 (371).

438 So zutr. LG Kiel, StV 2006, 405 (406); vgl. auch *Bär*, TK-Überwachung, § 100a StPO, Rn. 58; hierauf deutet natürlich erst recht das komplette Fehlen einer Begründung hin, so auch BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 86.

439 So LG Rostock, StV 2008, 461 (461 f.) unter Bezugnahme auf die Rechtsprechung des BVerfG, wonach „es […] die Aufgabe und Pflicht des Ermittlungsrichters [ist], sich eigenverantwortlich ein Urteil zu bilden und nicht etwa die Anträge […] nach einer nur pauschalen Überprüfung einfach gegenzuzeichnen. Zur richterlichen Einzelentscheidung gehören eine sorgfältige Prüfung der Eingriffsvoraussetzungen und eine umfassende Abwägung zur Feststellung der Angemessenheit des Eingriffs im konkreten Fall. Schematisch vorgenommene Anordnungen vertragen sich mit dieser Aufgabe nicht. Die richterliche Anordnung des Eingriffs in das Fernmeldegeheimnis muss den Tatvorwurf so beschreiben, dass der äußere Rahmen abgesteckt wird, innerhalb dessen sich der Eingriff halten muss […]“ (BVerfG NJW 2003, 1787, 1792); vgl. auch *Bär*, TK-Überwachung, § 100a StPO, Rn. 58.

440 Vgl. BGH NJW 1983, 1570 (1571); BGH NJW 2003, 368 (369); KK – *Nack*, StPO, § 100a, Rn. 54.

chungsanordnung rechtsfehlerhaft auf eine Straftat gestützt wurde, die nicht zu den Katalogstraftaten des § 100a I Nr. 1, II StPO zählt[441], so sind die gewonnenen Erkenntnisse gemäß wiederholter Rspr. des BGH unverwertbar.[442]

Basierte die Annahme einer Katalogstraftat hingegen auf einer fehlerhaften Subsumtion des zugrunde liegenden Lebenssachverhaltes i. S. d. § 264 StPO und damit auf einem rechtlichen Bewertungsfehler des Anordnenden, so begründet dies jedenfalls dann kein Verwertungsverbot im weiteren Strafverfahren, wenn die Tatsachen- und Beweislage zum Zeitpunkt des Beschlusserlasses den Verdacht einer anderen Katalogstraftat des § 100a I Nr. 1, II StPO gerechtfertigt hätte.[443] Allerdings kann nur „soweit derselbe Lebenssachverhalt betroffen ist, auf den sich der Verdacht bezieht, und die Änderung der rechtlichen Grundlage für die Telefonüberwachung der damals bestehenden Ermittlungssituation nicht ein völlig anderes Gepräge geben würde“[444], ein derartiges Auswechseln der rechtlichen Begründung in Erwägung gezogen werden.[445]

Auch aus dem Umstand, dass sich der anfänglich bestehende Verdacht einer Katalogstraftat nach § 100a I Nr. 1, II StPO, welcher der Überwachungsanordnung zugrunde lag, im weiteren Verfahren (Anklageerhebung und Eröffnungsbeschluss) nicht bestätigt hat, ergibt sich ein Verwertungsverbot für gewonnene Erkenntnisse jedenfalls insoweit nicht, als die aus einer ordnungsgemäß angeordneten Überwachungsmaßnahme erlangten Erkenntnisse im Ausgangsverfahren zum Nachweis sonstiger Straftaten (Nichtkatalogstraftaten) verwendet werden, die in einem derart engen Bezug zu der ursprünglich in Verdacht stehenden Katalogstraftat stehen, dass es sich noch um dieselbe Tat im prozessualen Sinne (§ 264 StPO) handelt[446], sei es durch Vorliegen einer anderen Begehungsform der Katalogstraftat, durch Vorliegen von Tateinheit oder durch Vorliegen eines solchen Zusammenhangs mit der in der Anordnung genannten Katalogstraftat, dass Tatidentität i. S. d. § 264 StPO angenommen werden kann.[447] Es genügt insofern, dass im Anordnungszeitpunkt ein objektiver Bezug (insoweit zu unter-

441 Vgl. *Bär*, TK-Überwachung, § 100a StPO, Rn. 54.

442 Vgl. BGH NJW 1983, 1570 (1571); BGH NJW 1995, 1974 (1974).

443 Vgl. BGH NJW 2003, 1880 (1883), wonach der rechtliche Bewertungsfehler in diesen Fällen „heilbar“ sei; vgl. auch BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 84.

444 BGH NJW 2003, 1880 (1883).

445 Vgl. BGH NJW 2003, 1880 (1883).

446 Vgl. BGH NStZ 1998, 426 (427); bereits BGH NJW 1976, 1462 (1463); BGH NJW 1979, 990 (991 f.); BGH NJW 1979, 1370 (1371); BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 84; vgl. auch BT-Drs. 16/5846, S. 66.

447 Vgl. BGH NStZ 1998, 426 (427).

scheiden von den oben genannten Fällen des Ausscheidens des Verdachts einer Katalogstraftat von vornherein) auf eine Katalogstraftat bestanden hat.[448]

Bei der Prüfung des Vorliegens eines *von bestimmten Tatsachen begründeten Tatverdachts* steht dem anordnenden Gericht (bzw. der anordnenden Staatsanwaltschaft in den Fällen von Gefahr im Verzug) ein Beurteilungsspielraum zu.[449] Die Frage der Rechtswidrigkeit der Überwachungsanordnung wegen Fehlens des nötigen Verdachtsgrades sowie etwaige sich darauf gründende Verwertungsverbote bemessen sich deshalb danach, ob sich die getroffene Entscheidung innerhalb des eingeräumten Beurteilungsspielraums bewegt, oder aber diesen überschreitet und damit nicht mehr vertretbar ist.[450] Hat hingegen von vornherein kein Tatverdacht bestanden, so sind die erlangten Erkenntnisse unverwertbar.[451]

Ein Verwertungsverbot für erlangte Erkenntnisse ist auch für die Fälle anzunehmen, in denen die (Quellen-)TKÜ-Maßnahme unter Missachtung des *Subsidiaritätsgrundsatzes* aus § 100a I Nr. 3 StPO angeordnet wurde[452], wobei auch hier das Gesetz dem anordnenden Gericht bzw. (bei Gefahr im Verzug) der anordnenden Staatsanwaltschaft allerdings einen Beurteilungsspielraum einräumt.[453] Die Beurteilung der Aussichtslosigkeit oder der wesentlichen Erschwernis der Sachverhaltserforschung oder Aufenthaltsortsermittlung mit anderen Mitteln bemisst sich demnach ebenfalls am Maßstab der Vertretbarkeit.[454]

Soweit erlangte Erkenntnisse wegen einer Kernbereichsrelevanz dem gesetzlichen Beweiserhebungs- bzw. Beweisverwertungsverbot des § 100a IV S. 1 bzw. S. 2 StPO unterfallen, ist sowohl deren unmittelbare (= direkte) Verwertung zu *Beweiszwecken*[455] als auch deren mittelbare (= indirekte) Verwertung, bspw. als *Ermittlungs- oder Spurenansätze*, unzulässig.[456] In allen

---

448 So Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 32 m. w. N.; vgl. auch BGH NJW 1979, 1370 (1371).

449 Vgl. BGH NJW 1995, 1974 (1975); BGH NJW 2003, 368 (369).

450 Vgl. BGH NJW 1995, 1974 (1975); BGH NJW 2003, 368 (369).

451 So Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 35 m. w. N.

452 Vgl. BGH NJW 1995, 1974 (1974) m. w. N.

453 Was sich nach Auffassung des BGH bereits daraus ergebe, dass die Subsidiaritätsklauseln verschiedener Ermittlungsmaßnahmen unterschiedlich durch den Gesetzgeber gefasst wurden (vgl. § 100c I Nr. 4, § 100a I Nr. 3, § 100f I, § 100g I S. 1 bzw. S. 2, § 100h I S. 1 StPO), so BGH NJW 1995, 1974 (1975).

454 Vgl. BGH NJW 1995, 1974 (1975); BGH NJW 2003, 368 (369).

455 D. h. zum Zwecke des Klärens der Schuld- oder Straffrage, so Löwe-Rosenberg – *Schäfer*, StPO und GVG, Zweiter Band, § 100a StPO, Rn. 88.

456 Vgl. BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 102; auch *Bär*, TK-Überwachung, § 100a StPO, Rn. 44 u. 63.

anderen der oben genannten Fälle scheidet im Falle eines Verwertungsverbotes zwar die (direkte) Verwertung der erlangten Erkenntnisse zu Beweiszwecken aus, jedoch besteht kein Hindernis, derartige Erkenntnisse jedenfalls als Ermittlungs- oder Spurenansätze zu verwenden. Nach herrschender Rspr. des BGH besteht für Erkenntnisse aus TKÜ-Maßnahmen, bei denen wegen des Fehlens wesentlicher sachlicher Voraussetzungen ein Verwertungsverbot zu Beweiszwecken vorliegt, grds. keine sog. *Fernwirkung* des Beweisverwertungsverbots, welche auch die mittelbare Verwertung der gewonnenen Erkenntnisse als Ansatz für weitere Ermittlungen[457] sowie eine unmittelbare Verwertung etwaiger daraufhin erlangter anderer Beweismittel ausschließen würde.[458] Gleiches gilt auch für Verfahrensfehler, die ein Beweisverwertungsverbot herbeiführen.[459] Denn nach wiederholter Rspr. des BGH darf auf Grund des Interesses an effektiver Strafverfolgung „ein Verfahrensfehler, der ein Verwertungsverbot für ein Beweismittel herbeiführt, nicht ohne weiteres dazu führen, daß das gesamte Strafverfahren lahmgelegt wird“[460]. In der deutschen Strafprozessordnung gibt es demnach – jedenfalls gegenwärtig – keinen mit der sog. *fruit of the poisonous tree doctrine* des US-amerikanischen Rechtssystems vergleichbaren Rechtsgrundsatz.[461]

Über die dargestellten Folgen formeller oder materieller Mängel in der Anordnung hinaus stellt sich allerdings die Frage, welche Konsequenzen aus dem *Verstoß gegen die rechtlichen Vorgaben* einer Quellen-TKÜ-Anordnung – sei es auf Grundlage der §§ 100a, 100b StPO de lege lata[462] oder auf Grundlage einer ausdrücklichen gesetzlichen Normierung (bspw. bei gesetzlicher Klarstellung in den §§ 100a, 100b StPO) de lege ferenda[463] – *bei Umsetzung der Anordnung* (*Durchführungsebene*) zu folgern sind, insbesondere bei Verstößen gegen die Vorgaben hinsichtlich der erforderlichen Konfiguration der Überwachungssoftware und der diesbezüglich zur Verhinderung eines Missbrauchs der Software sowie zur Sicherstellung der Beweismittelauthentizität und -integrität zu ergreifenden technischen Schutzvorkehrungen:

---

457 Auch für Ermittlungen bezüglich Nichtkatalogstraftaten, vgl. BGH NJW 1978, 1390 (1390).

458 Vgl. BGH NJW 2006, 1361 (1363); bereits BGH NJW 1978, 1390 (1390); BGH NJW 1984, 2772 (2773); so auch Meyer-Goßner – *Meyer-Goßner*, StPO, Einl., Rn. 57 sowie Meyer-Goßner – *Cierniak* § 100a, Rn. 38; ebenso *Bär*, TK-Überwachung, § 100a StPO, Rn. 63 jeweils m. w. N.

459 Vgl. BGH NJW 1984, 2772 (2773).

460 BGH NJW 1984, 2772 (2773); so bereits BGH NJW 1978, 1390 (1390); auch BGH NJW 2006, 1361(1363).

461 Vgl. Meyer-Goßner – *Meyer-Goßner*, StPO, Einl., Rn. 57 m. w. N.

462 Zur Zulässigkeit der Quellen-TKÜ de lege lata, siehe 3. Teil A.

463 Zur gesetzlichen Klarstellung der Quellen-TKÜ de lege ferenda, siehe 3. Teil B.

Hierfür ist bislang bspw. nicht abschließend geklärt, ob für jedweden Verstoß gegen rechtliche Vorgaben zu technischen Schutzmaßnahmen beim Einsatz einer Überwachungssoftware ein generelles Beweisverwertungsverbot erforderlich ist, oder ob bei derartigen Verstößen – solange diese jedenfalls nicht bewusst bzw. willkürlich erfolgen – die Annahme einer automatischen Unverwertbarkeit der erlangten Erkenntnisse eher zu verneinen ist.

Hier empfiehlt sich eine differenzierende Herangehensweise, bei der verstärkt darauf abgestellt wird, ob die jeweilige rechtliche Vorgabe, gegen die im konkreten Einzelfall verstoßen wurde, gerade die Beweismittelauthentizität und -integrität der erhobenen Daten und damit die Beweissicherheit und Aussagekraft der erlangten Erkenntnisse sicherstellen soll oder aber anderen Zwecken dient. Eine vertiefte Auseinandersetzung mit dieser Fragestellung ist Gegenstand von Lösungsmodell 3 im Rahmen des 3. Teils der vorliegenden Arbeit[464], welches sich insbesondere mit den Konsequenzen aus Verstößen gegen spezifische gesetzliche Vorgaben hinsichtlich technischer Beschaffenheit und Missbrauchssicherheit der für die Realisierung der Quellen-TKÜ eingesetzten Überwachungssoftware befasst.

3. Konflikt mit computer-forensischen Grundsätzen?

Ermittlungsmaßnahmen im Zusammenhang mit Zugriffen auf informationstechnischen Systemen bauen sich regelmäßig auf besonderen technischen Vorgehensweisen der Ermittlungsbehörden auf. Im Bereich der Strafverfolgung dienen derartige Maßnahmen dem Zwecke der Erkenntnis- und Beweisgewinnung über Tatgeschehen sowie Täterperson[465] und sind an diesen Zweck grds. auch gebunden (sog. *Grundsatz der Zweckbindung*[466]). Bei Ermittlungen im Zusammenhang mit IT-Systemen bedarf es hierzu der gerichtsverwertbaren systematischen Erfassung, Untersuchung und Auswertung von Computersystemen und den darauf befindlichen digitalen Spuren und elektronisch gespeicherten Daten, um daraus die bezweckten ermittlungsrelevanten Erkenntnisse zum Nachweis von Tatgeschehen und Täterperson zu gewinnen.[467] Man spricht insoweit auch von der sog. *Computer-Forensik* (auch *IT-Forensik*):

Damit erlangte Erkenntnisse im weiteren Verfahren überhaupt gerichtliche Anerkennung finden können und zu Beweiszwecken verwertbar sind, müs-

---

464 Siehe hierzu 3. Teil B.III.5.

465 Während die Zielsetzung im präventiven Bereich dem Erkenntnisgewinn zur Abwehr von Gefahren entspringt.

466 Vgl. BVerfG NJW 2000, 55 (57).

467 Vgl. hierzu auch *Willer*/*Hoppen*, CR 2007, 610 (610).

sen die Echtheit des Beweismaterials und die vollständige Nachprüfbarkeit aller vorgenommenen Ermittlungsschritte durch eine unabhängige Stelle als „computerforensische Grundpfeiler“[468] nachvollziehbarer Untersuchungen gewährleistet sein.

Im Zusammenhang mit Erkenntnissen aus einem Zugriff auf informationstechnische Systeme ist hierfür insbesondere sicherzustellen, dass es zugunsten der Daten*authentizität*[469] und -*integrität*[470] und damit der Revisionsfestigkeit als Beweismittel eingeführter Erkenntnisse zu keiner (nachträglichen) Veränderung des untersuchungsgegenständlichen Datenbestandes kommt[471] und dieser der betreffenden Quelle zuordenbar ist. Entsprechende Vorkehrungen zum Schutz vor einer Manipulation der Daten sind daher im Sinne einer späteren gerichtlichen Verwertbarkeit und deren revisionsfesten Standhaltens gegenüber kritischer Prüfung („Revisionsfähigkeit“) zwingend angezeigt.

Bei der konventionellen („klassischen“) Computer-Forensik, d. h. Sicherstellung des Zielgerätes mitsamt seiner Datenträger und darauf befindlicher Daten im Rahmen einer herkömmlichen („Offline“-)Durchsuchung nach §§ 102 ff. StPO und anschließende Untersuchung und Auswertung der auf den sichergestellten Datenträgern befindlichen Daten und deren Informationen, wird im Rahmen systematischer computer-forensischer Vorgehensweise versucht, der Gefahr einer etwaigen Verfälschung von Daten durch einen festen Verfahrensablauf vorzubeugen:

Im ersten Schritt der *Identifizierung* muss zunächst geklärt werden, welche Informationen für die Ermittlungen relevant sind, zu denen Beweise auf dem Zielsystem gewonnen werden sollen. Hierbei erfolgt auch eine Festlegung der konkreten Vorgehensweise sowie der hierfür erforderlichen Mittel und Werkzeuge.

Im zweiten Schritt der *Sicherstellung* findet die Durchsuchung und Sicherstellung des Zielgerätes gemäß den Verfahrens- und Formvorschriften der §§ 102 ff. StPO im Rahmen einer herkömmlichen Durchsuchungsmaßnahme statt.

---

468 *Gercke*/*Brunst*, Internetstrafrecht, Kap. 5, S. 347, Rn. 881.

469 Nachweis der Echtheit und Zuordenbarkeit der Daten zur betreffenden Quelle, vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 22.

470 Nachweis der Vollständigkeit und Unverändertheit der Daten, vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 117 sowie https://www.bsi.bund.de/DE/Themen/weitereThemen/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html (zuletzt aufgerufen 15.06.2012).

471 Vgl. insoweit auch *Platz*, sic! 11/2008, 838, S. 4, abrufbar unter https://www.sic-online.ch/fileadmin/user_upload/Sic-Online/2008/documents/838.pdf (zuletzt aufgerufen 15.06.2012).

Im Rahmen des dritten Schrittes erfolgt dann zum Zwecke der Gewährleistung der Gerichtsverwertbarkeit eine *Sicherung der Datenträger* gegen nachträgliche Veränderung. Hierfür werden die Datenträger i. d. R. schreibgeschützt, mit einem kryptographischen Verfahren digital signiert[472] und verschlüsselt. Zur Absicherung wird zudem eine 1:1 Image-Kopie der gesicherten Datenträger erstellt.

Im abschließenden vierten Schritt findet die *Analyse und Aufbereitung* des auf den Datenträgern sichergestellten Datenmaterials statt. Durch anschließende *Interpretation der Daten* lassen sich dann (ggf.) ermittlungsrelevante Informationen gewinnen. Zum Schutz des Datenmaterial vor Verfälschung sollen die Untersuchungen hierbei ausschließlich anhand der Kopie und nie am Original-Datenbestand erfolgen. Um das gesamte Verfahren nachvollziehbar und einer späteren gerichtlichen Überprüfbarkeit zugänglich zu machen, sind hierbei die einzelnen Schritte der Untersuchung sowie das verwendete Auswertungsverfahren zudem durch Protokolle (im Idealfall lückenlos) zu dokumentieren.[473]

Die Umsetzung der Sorgfaltsmaßstäbe klassischer forensischer Computeruntersuchung gestaltet sich bei (heimlichen) Online-Zugriffen i. d. R. schwieriger.[474] Dies macht das Einhalten neuer computer-forensischer Verfahrensweisen erforderlich. Das Erfordernis der Einhaltung der computerforensischen Grundsätze besteht vor allem bei modernen Ermittlungsmaßnahmen wie der Online-Durchsuchung, bei der im Rahmen heimlichen staatlichen Handelns v. a. Daten von den Speichermedien betroffener informationstechnischer Systeme erhoben werden. Aber auch auf Maßnahmen der Quellen-TKÜ zum Erkenntnisgewinn aus laufenden Telekommunikationsvorgängen wirken sich diese – wenngleich in abgemilderter Form – grds. aus. Auf Grund des Umstandes, dass für deren Durchführung heimlich in das Zielsystem eingedrungen und ein Fremdprogramm in dessen Datenbe-

---

472 Kryptographisches Verfahren, mit dem sichergestellt werden kann, dass eine Datei tatsächlich von dem angegebenen Urheber bzw. Signaturersteller stammt (Authentizität) und nicht verändert wurde (Integrität), vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 67.

473 Vgl. *Hansen*/*Krause*, Sommerakademie 2007, S. 9, 10, abrufbar unter https://www.datenschutzzentrum.de/sommerakademie/2007/sak2007-hansen-krause-online-durchsuchung.pdf (zuletzt aufgerufen 15.06.2012); Arbeitskreis „Technische und organisatorische Datenschutzfragen", Technische Aspekte, S. 9, abrufbar unter http://www.lfd.m-v.de/dschutz/informat/internet/onlinedurchsuchung.pdf (zuletzt aufgerufen 15.06.2012); vgl. hierzu auch *Gercke*/*Brunst*, Internetstrafrecht, Kap. 5, S. 375, Rn. 989 ff.; zudem Bundesministerium des Innern, Fragenkatalog SPD, S. 4, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

474 Vgl. *Gercke*/*Brunst*, Internetstrafrecht, Kap. 5, S. 347, Rn. 881.

stand eingebracht werde muss, welches Daten aus dem System ausleitet, stellt sich für beide Ermittlungsmaßnahmen die Frage, ob die Beweismittelauthentizität/-integrität und mithin die Unverfälschtheit der im Rahmen heimlicher Online-Zugriffe erlangten Daten ausreichend gewährleistet werden kann[475].

Zur Klärung dieser Frage wird bereits an die Tatsache des Einsatzes staatlicher Überwachungssoftware an sich angeknüpft. So werden zum Teil Zweifel geäußert, ob der Einsatz staatlicher Fernzugriffssoftware die Authentizität der damit erlangten Informationen überhaupt ausreichend gewährleisten könne. Schon das Einbringen der Software könne die Echtheit und damit die gerichtliche Verwertbarkeit möglicher Erkenntnisse in Zweifel ziehen, da bereits dieser Schritt eine Modifizierung des Zielsystems und damit eine Veränderung des Untersuchungsgegenstandes bedeute.[476]

Bedenken gegen die Unverfälschtheit des erlangten Datenmaterials werden deshalb vor allem im Zusammenhang mit der *Online-Durchsuchung*[477] geäußert.[478] Ziel des Eingriffs bei der Online-Durchsuchung seien nämlich gerade die auf dem informationstechnischen System gespeicherten Datenbestände, in die die staatliche Überwachungssoftware eingebracht wird.[479] Der Fernmeldeverkehr diene im Rahmen einer Maßnahme der Online-Durchsuchung lediglich als Mittel für den Eingriff, das Internet sozusagen als Einfallstor in das System.[480] Bereits die Tatsache einer in den Datenbestand eingeschleusten Fremdsoftware widerspreche allen Grundsätzen konventioneller Computer-Forensik. Es könne aber auch nicht sicher ausgeschlossen werden, dass nicht mit dem Start der Überwachungssoftware

---

475 Vgl. insoweit auch *Platz*, sic! 11/2008, 838, S. 4, abrufbar unter https://www.sic-online.ch/fileadmin/user_upload/Sic-Online/2008/documents/838.pdf (zuletzt aufgerufen 15.06.2012).

476 Vgl. *Hansen*/*Krause*, Sommerakademie 2007, S. 37, abrufbar unter https://www.datenschutzzentrum.de/sommerakademie/2007/sak2007-hansen-krause-online-durchsuchung.pdf (zuletzt aufgerufen 15.06.2012); *Platz*, sic! 11/2008, 838, S. 4, abrufbar unter https://www.sic-online.ch/fileadmin/user_upload/Sic-Online/2008/documents/838.pdf (zuletzt aufgerufen 15.06.2012).

477 Für Einzelheiten zur Online-Durchsuchung, siehe 1. Teil A.II.2.a).

478 Vgl. auch *Gercke*/*Brunst*, Internetstrafrecht, Kap. 5, S. 347, Rn. 881; Arbeitskreis „Technische und organisatorische Datenschutzfragen", Technische Aspekte, S. 9, abrufbar unter http://www.lfd.m-v.de/dschutz/informat/internet/onlinedurchsuchung.pdf (zuletzt aufgerufen 15.06.2012).

479 Vgl. hierzu auch Bundesministerium des Innern, Fragenkatalog BMJ, S. 2, 7, 14 http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012).

480 Vgl. *Platz*, sic! 11/2008, 838, S. 7, abrufbar unter https://www.sic-online.ch/fileadmin/user_upload/Sic-Online/2008/documents/838.pdf (zuletzt aufgerufen 15.06.2012).

weitere Änderungen auf dem Zielsystem vorgenommen werden.[481] Hinsichtlich des Verfahrens der Ausleitung des ermittlungsrelevanten Datenmaterials erscheine es zudem fraglich, ob sich die Daten für die Übermittlung an den Behörden-Server überhaupt verlässlich gegen Verfälschung schützen lassen, da bspw. die Durchführung eines kryptographischen Verfahrens wie der digitalen Signatur auf einem (durch die Zielperson) fremdkontrollierten System nur schwer möglich sei.[482] Zudem habe der dynamische Charakter eines informationstechnischen Systems zur Folge, dass sich erneute Untersuchungen nicht unter gleichen Bedingungen wiederholen lassen, was zu zusätzlichen Schwierigkeiten hinsichtlich der Kriterien der „Nachvollziehbarkeit" und „Wiederholbarkeit" bei Online-Durchsuchungen führe.[483]

Von staatlicher Seite wird versucht diesen Bedenken durch „äußerst exakte und detaillierte"[484] Dokumentation und Protokollierung aller im Rahmen der Ermittlungsmaßnahme insbesondere durch das Einbringen der Überwachungssoftware stattgefundenen Einwirkungen auf das Zielsystem Rechnung zu tragen und bspw. auch durch die zusätzliche Hinterlegung des Quellcodes[485] (bzw. – falls der Quellcode nicht vorliegt[486] – ggf. des Binärcodes[487]) der konkreten Überwachungssoftware zu belegen (bspw. im Wege

---

481 Vgl. Arbeitskreis „Technische und organisatorische Datenschutzfragen", Technische Aspekte, S. 9, abrufbar unter http://www.lfd.m-v.de/dschutz/informat/internet/onlinedurchsuchung.pdf (zuletzt aufgerufen 15.06.2012).

482 Vgl. Arbeitskreis „Technische und organisatorische Datenschutzfragen", Technische Aspekte, S. 9, abrufbar unter http://www.lfd.m-v.de/dschutz/informat/internet/onlinedurchsuchung.pdf (zuletzt aufgerufen 15.06.2012).

483 Vgl. hierzu Frage 3, Fragenkatalog SPD, S. 4, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

484 Bundesministerium des Innern, Fragenkatalog SPD, S. 4, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

485 Auch *Quelltext*, bezeichnet den in einer Programmiersprache geschriebenen Text eines Computerprogramms, bestehend aus einer Abfolge von Befehlen, vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 192.

486 So wurde bspw. in der Vergangenheit bei der Beauftragung externer IT-Unternehmen zur Erstellung von Software (entsprechend der Beauftragung gemäß den rechtlichen Vorgaben) den Ermittlungsbehörden regelmäßig nur Binärcodes zur Verfügung gestellt, da Quellcodes vermarkteter Softwareprodukte grds. als Vermögenswert des betreffenden Unternehmens angesehen werden und dessen Bereitstellung daher i. d. R. unüblich ist, vgl. auch BT-Drs. 17/7760, S. 5.

487 Der in maschinen-lesbare Form übersetzte Quellcode, vgl. http://de.wikipedia.org/wiki/Quelltext (zuletzt aufgerufen 15.06.2012); dass auch der Binärcode jedenfalls grds. einer Analyse nicht unzugänglich ist, belegen nicht zuletzt die anhand des Binarcodes erfolgten Untersuchungen einer Überwachungssoftware, welche in einem Ermittlungsverfahren aus dem Jahre 2009 zum Einsatz kam und Gegenstand eines Beschwerdeverfahrens vor dem LG Landshut (MMR 2011, 690) war, durch den

eines Analysierungsverfahrens durch Sachverständige), dass die konkret verwendete Software keine Daten frei im Zielsystem platzieren konnte, sowie mittels entsprechender Verschlüsselungsverfahren oder digitaler Signaturen die Integrität der erlangten Daten überprüfbar zu machen.[488]

Soweit die genannten Bedenken bereits an der Infiltration des Zielsystems mit der Überwachungssoftware anknüpfen sowie den Schutz erhobener Daten vor Verfälschung bspw. bei der Ausleitung und deren Zurechenbarkeit zum betroffenen System und dessen Nutzer betreffen, wirkt sich die Diskussion auch auf Maßnahmen der *Quellen-TKÜ* aus:

Wie bei der Online-Durchsuchung erfolgt auch bei der Quellen-TKÜ die Installation einer Überwachungssoftware auf dem betroffenen informationstechnischen System, mithin findet folglich ein Eindringen und Einbringen eines Fremdprogramms in ein informationstechnisches System statt.

Anders als bei der Online-Durchsuchung ist das infiltrierte System mit seinen gespeicherten Datenbeständen bei der Quellen-TKÜ jedoch nicht das Ziel bzw. der Gegenstand des Eingriffs, sondern lediglich das Mittel, über das das eigentliche Ziel der Überwachung, nämlich die laufende IP-Telekommunikation, abgewickelt wird. Während bei der Online-Durchsuchung Überwachungsgegenstand gerade der Datenbestand ist, in den gemäß obigen Ansichten durch die Installation einer Überwachungssoftware bereits modifizierend eingegriffen würde, hat der Datenbestand des Systems für die Quellen-TKÜ keine Relevanz, da im Rahmen der Umsetzung der Maßnahme typischerweise gerade keine Daten zu strafprozessualen Zwecken erhoben werden, welche außerhalb laufender Telekommunikationsvorgänge auf dem Zielsystem gespeichert sind.[489] Eine mögliche Veränderung (Verfälschung) des (von der Quellen-TKÜ nicht erfassten) Datenbestandes auf dem informationstechnischen System durch Installation der Software bleibt daher für die Quellen-TKÜ unter dem Aspekt der Beweisverwertbarkeit und Gerichtsfestigkeit ohne Auswirkung.

Chaos Computer Club im Herbst 2011; hierfür stehen auch die unter dem Begriff des *Reverse Engineering* zusammengefassten technischen Möglichkeiten der automatischen Rückgewinnung des Quellcodes aus einem Binärcode bzw. der Rückumwandlung in eine für Menschen lesbare Form (z. B. mittels sog. Decompiler bzw. Disassembler) zur Verfügung.

488 In diese Richtung auch Bundesministerium des Innern, Fragenkatalog SPD, S. 4, 5, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

489 Vgl. Bundesministerium des Innern, Fragenkatalog BMJ, S. 2, 7, 14, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012); für Einzelheiten zur Abgrenzung von Online-Durchsuchung und Quellen-TKÜ, siehe 1. Teil A.II.2.a).

Anders gestaltet sich dies wiederum für Fragen der Beweismittelauthentizität und -integrität in Bezug auf den Schutz abgegriffener Daten aus IP-Telekommunikationen vor Verfälschung bei der Ausleitung der Daten an den Behörden-Server, die Gewährleistung der Zurechenbarkeit des gewonnenen Datenmaterials zu dem jeweiligen System und dessen Nutzer sowie den Schutz vor Veränderung und unbefugter Löschung der Daten während ihrer Speicherung für das weitere Verfahren im Zugriffsbereich der Ermittlungsbehörden. Diesbezüglich finden auch hier computer-forensische Grundsätze Anwendung. Wenngleich ein abgegriffenes IP-geführtes Sprach- und/oder Videotelefonat freilich andere Möglichkeit des Nachweises der Authentizität und Zurechenbarkeit des erlangten TK-Datenmaterials (vgl. nachfolgend unter Punkt 4), bspw. in Form von Stimm- und Bildabgleichen, eröffnet, als dies bei Maßnahmen der Online-Durchsuchung für das aus einem (modifizierbaren) Datenbestand erhobene Datenmaterial in Bezug auf Fragen der Urheberschaft und Zurechenbarkeit der Fall ist, besteht dennoch auch bei Maßnahmen der Quellen-TKÜ zum Zwecke der Beweismittelauthentizität, -integrität und damit der Gerichtverwertbarkeit das Erfordernis einer Absicherung der erhobenen Daten vor Veränderung, unbefugter (ggf. Teil-)Löschung und unbefugter Kenntnisnahme.[490]

4. Zurechenbarkeit des erfassten Datenmaterials

In Bezug auf das erhobene Datenmaterial bzw. die daraus gewonnenen Erkenntnisse und die Frage nach deren Unverfälschtheit und Zurechenbarkeit bestehen grundlegende Unterschiede zwischen einem Zugriff auf ein informationstechnisches System in Form einer Online-Durchsuchung und dem Zugriff im Rahmen einer Quellen-TKÜ-Maßnahme. Gemeinsam ist beiden Maßnahmen, dass sie auf das Abgreifen von *Daten* zu Beweiszwecken ausgerichtet sind.

Da die Strafprozessordnung keine „Daten“ als eigenständiges Beweismittel kennt, kommen daher zur Beweiseinführung im Wesentlichen der gesetzlich vorgesehene Augenscheinsbeweis (§ 86 StPO), der Urkundsbeweis (§ 249 StPO) sowie der Zeugenbeweis (§§ 48 ff, 250 ff. StPO) in Betracht.[491] Über den Beweiswert und das Ergebnis der Beweisaufnahme hat das erkennende Gericht nach seiner freien, aus dem Inbegriff der Verhandlung geschöpften Überzeugung zu entscheiden (§ 261 StPO).

Das mit Hilfe der heimlichen Ermittlungsmaßnahme erlangte Datenmaterial muss dem Handeln der Zielperson konkret zurechenbar sein, um gegen

---

490 Für Einzelheiten zur Berücksichtigung computer-forensischer Gesichtspunkte bei Quellen-TKÜ-Maßnahmen, siehe 3. Teil A.I.2. sowie 3. Teil B.III.3.

491 Vgl. *Gercke*/*Brunst*, Internetstrafrecht, Kap. 5, S. 374, Rn. 984.

diese im Rahmen eines gerichtlichen Verfahrens Verwendung zu finden. Gerade bei heimlichen bzw. verdeckten[492] Zugriffen auf informationstechnische Systeme liegt der Einwand nahe, nicht die der Straftat verdächtige Zielperson habe das Gerät benutzt, sondern bspw. ein Dritter, der Zugang dazu gehabt hat.[493] Auch werden Bedenken hinsichtlich des Beweiswertes und der Zurechenbarkeit erlangter Daten geäußert, wenn ein externer Zugriff Fremder auf ein Zielsystem erfolgt. Denn „wenn man von außen die volle Kontrolle über einen Rechner erlangen kann“[494], dann ließen „sich auch Informationen unterschieben und verändern“[495].

Für die Zurechenbarkeit des erlangten Datenmaterials im Rahmen einer *Online-Durchsuchung* zum Nachweis der Täterschaft, welches bspw. bei erlangten digitalen Dokumenten im Wege der Inaugenscheinnahme durch entsprechenden Ausdruck der Daten in die Verhandlung eingeführt werden kann[496], stellt der Umstand der möglichen Drittbeeinflussung des Datenbestandes durchaus eine besondere (maßnahmeimmanente) technische wie rechtliche Schwierigkeit dar. Denn die Überwachungssoftware kann lediglich das erfassen, was auf dem Computer geschieht, bspw. Veränderungen der Konfiguration, Abspeicherung von Daten etc. Nur teilweise lassen diese Vorgänge auch einen Schluss auf die dahinter stehende Person zu, bspw. Nutzung eines bestimmt Benutzerkontos unter Passworteingabe u. ä. Wer die Aktivitäten am Gerät letztlich tatsächlich vorgenommen oder wer eine bestimmte abgegriffene Datei tatsächlich erstellt hat, wird sich oftmals – jedenfalls bei Fehlen entsprechend belastbarer Protokollierungs- und Dokumentierungsverfahren unter Beachtung computer-forensischer Grundsätze[497] – nicht ohne weiteres mit absoluter Bestimmtheit sagen lassen.[498] Für das

---

[492] Der Begriff „verdeckt“ wird oftmals synonym mit dem Begriff „heimlich“ verwendet (i. S. v. „ohne Wissen des Betroffenen“); dies entspricht auch der üblichen Terminologie in Rspr. und Schrifttum; bei strenger Begriffsauslegung beschreibt der Begriff der „Verdecktheit“ indes eher den Umstand, dass der Betroffene zwar die (sichtbaren) Handlungen/Auswirkungen der Maßnahmeumsetzung mitbekommt, den dahinter stehenden tatsächlichen (ermittlungstaktischen) Anlass/Zweck aber nicht erkennt (bspw. durch das Handeln der Ermittlungspersonen unter einem bestimmten Vorwand und/oder Anwendung einer Legende), während der Begriff der „Heimlichkeit“ hingegen eher auf eine völlige Unkenntnis des Betroffenen vom Ablaufen einer Maßnahme ihm gegenüber überhaupt hindeutet.

[493] Vgl. *Gercke*/*Brunst*, Internetstrafrecht, Kap. 5, S. 347, Rn. 882.

[494] *Leutheusser-Schnarrenberger*, Bundesministerin der Justiz, in: „‚Schnelle Aufklärung‘“, Passauer Neue Presse vom 11.10.2011, S. 4.

[495] *Leutheusser-Schnarrenberger*, Bundesministerin der Justiz, in: „‚Schnelle Aufklärung‘“, Passauer Neue Presse vom 11.10.2011, S. 4.

[496] Vgl. *Gercke*/*Brunst*, Internetstrafrecht, Kap. 5, S. 374, Rn. 985.

[497] Siehe hierzu 2. Teil A.III.3.

[498] Vgl. *Gercke*/*Brunst*, Internetstrafrecht, Kap. 5, S. 347, Rn. 882.

Erlangen lediglich von Spurenansätzen auf dem System ist dieser Umstand freilich von geringerer Relevanz.

Für die Zurechenbarkeit im Rahmen einer *Quellen-TKÜ* stellt sich dieses Problem jedoch nicht in vergleichbarer Weise, da sich der Betroffene als Gesprächsteilnehmer im Rahmen einer Überwachung von Internettelefonie im Regelfall auf Grund des mit einer solchen Maßnahme als Zugriffsobjekt erfassten *Audio-Datenmaterials* für das Gros der Fälle wohl ohne größere Schwierigkeiten anhand der Stimme identifizieren lassen wird[499] und die erfassten Inhalte sich (beliebig oft wiederholbar) zum Zwecke der Inhaltserfassung anhören und dem betreffenden „Urheber" der jeweiligen Äußerung zuordnen lassen. Entsprechendes gilt für die Ansicht des Video-Datenmaterials (bei erfasster Video-Internettelefonie) in Form des Vorführens der Bildaufnahmen oder durch grafische Ausdrucke. Denn bei Erkenntnissen aus TKÜ-Maßnahmen im Ermittlungsverfahren ist originäres Beweismittel gerade die Inaugenscheinnahme der erstellten Ton- oder Datenträger durch das erkennende Gericht und die Verfahrensbeteiligten, welche zum Zwecke des Einführens der darauf gespeicherten Erkenntnisse in die Hauptverhandlung insbesondere abgespielt oder in sonstiger Weise wahrnehmbar gemacht werden können.[500] Die Gefahr eines „Unterschiebens" von Daten – wie bspw. bei einer Maßnahme wie der Online-Durchsuchung prinzipiell denkbar, in deren Zuge gerade auf den (modifizierbaren) Datenbestand des Zielsystems zugegriffen wird – ist bei einer Maßnahme wie der Quellen-TKÜ, die sich auf Daten aus laufenden Telekommunikationsvorgängen bezieht und ihrem Zweck entsprechend die akustischen[501] Gesprächsinhalte aufzeichnet, bereits maßnahmebedingt nicht in gleicher Weise gegeben, soweit jedenfalls der Inhalt der erfassten Daten betroffen ist. Darüber hinaus lässt sich hinsichtlich der Authentizität und Integrität der Inhalte – aber auch hinsichtlich der Authentizität und Integrität ggf. miterhobener näherer Umstände der Telekommunikation, sprich Verkehrsdaten wie bspw. Datum und Uhrzeit des Telekommunikationsvorgangs, welche als Urkundsbeweis in der Hauptverhandlung grds. zu verlesen wären[502] und welche zwar nicht Hauptgegenstand einer (Quellen-)TKÜ-Maßnahme sind, aber bei Maßnahmen nach §§ 100a, 100b StPO dennoch neben Kommunikationsinhalten grds. miterfasst werden können[503] – durch einen dem Stand der Technik entsprechende Einsatz von Verschlüsselungstechniken sowie durch sachge-

---

499 In diese Richtung auch *Gercke/Brunst*, Internetstrafrecht, Kap. 5, S. 347, Rn. 882, Fn. 366; dies gilt freilich erst recht, wenn bei einer Video-Internettelefonie auch die visuellen Inhalte der Kommunikation miterfasst wurden.

500 Vgl. *Bär*, TK-Überwachung, § 100a StPO, Rn. 50 m. w. N.

501 Bei Video-Internettelefonie ggf. zusätzlich auch die ausgetauschten visuellen Inhalte.

502 Vgl. *Bär*, TK-Überwachung, § 100a StPO, Rn. 50 m. w. N.

rechte Dokumentation und Protokollierung der Erlangung der Daten einschließlich Angaben zur Identifizierung der Daten und des betroffenen Systems sowie des weiteren Umgangs mit den gewonnenen Daten zugunsten deren Verwertbarkeit und Revisionsfestigkeit ein wirksamer Schutz vor Datenveränderung bzw. -manipulation sicherstellen. Bezieht sich die Quellen-TKÜ – ebenfalls denkbar – auf das Erfassen von Textmitteilungen nach deren Aussendung (Betätigung des „Versende-Buttons"), also bspw. auf Daten aus Instant Messaging-Diensten[504], so können auch hier die bereits oben unter Punkt 3. im Rahmen der computer-forensischen Grundsätze angesprochen strengen Dokumentations- und Protokollierungsvorkehrungen sowie effektive Verschlüsselungsweisen und digitale Signaturen wirksamen Schutz vor (ggf. nachträglicher) Veränderung der erlangten Textnachrichten bieten und die Authentizität und Integrität der gewonnenen Erkenntnisse sicherstellen.

B. Sekundärmaßnahme: Installieren der Überwachungssoftware; Entfernen der Überwachungssoftware

Wie bereits im Rahmen des 1. Teils zu den technischen Grundlagen von Quellen-TKÜ-Maßnahmen erläutert[505], handelt es sich bei den relevanten Begleitmaßnahmen (Sekundärmaßnahmen) im Zusammenhang mit einer Quellen-TKÜ um das heimlich bzw. unter einem Vorwand (verdeckt) vorgenommene *Installieren* der Überwachungssoftware auf dem Zielsystem sowie (als „actus contrarius") das spätere *Deinstallieren* der Software von dem Zielsystem.

I. Installieren der Überwachungssoftware auf dem Zielsystem

Die dem eigentlichen Überwachungs- und Aufzeichnungsvorgang bei verschlüsselt übermittelter VoIP-Kommunikation im Rahmen der Quellen-TKÜ vorgeschaltete Begleitmaßnahme ist das unbemerkte Installieren einer entsprechenden Überwachungssoftware auf dem zu überwachenden Rechner, sprich die heimliche bzw. verdeckte Infiltration des Zielsystems mit einer Fremdsoftware.[506]

---

503 Vgl. hierzu Löwe-Rosenberg – *Schäfer*, StPO und GVG, Zweiter Band, § 100a StPO, Rn. 47.

504 Für Einzelheiten zu *Instant Messaging-over-IP*, siehe 1. Teil A.I.2.f).

505 Für Einzelheiten, siehe 1. Teil A.II.1. u. 4.

506 Für Einzelheiten zur technischen Umsetzung der Sekundärmaßnahmen, siehe 1. Teil A.II.4.

Unabhängig von dem Umstand, auf welche konkrete Art und Weise die Überwachungssoftware letztlich in das betreffende Zielsystem eingebracht wird, bedarf es zunächst einer dogmatischen Auseinandersetzung mit der Frage, ob die Infiltration eines Systems mit einer Fremdsoftware zum Zwecke der Realisierung einer Überwachung der über das System verschlüsselt geführten VoIP-Kommunikation nur am Fernmeldegeheimnis aus Art. 10 I GG zu messen ist, oder ggf. auch weitere Grundrechte tangiert.

1. Grundrechtsrelevanz des Installierens der Software

a) Eingriff in IT-Grundrecht?

Es stellt sich die Frage, welche Grundrechtsrelevanz die Sekundärmaßnahme der Quellen-TKÜ, also die Installation einer Überwachungssoftware auf einem informationstechnischen System, entfaltet.

Das BVerfG hat im Rahmen seiner Grundsatzentscheidung vom 27.02.2008 zur technischen Infiltration komplexer informationstechnischer Systeme festgestellt, dass wenn

> „ein komplexes informationstechnisches System zum Zwecke der Telekommunikationsüberwachung technisch infiltriert (‚Quellen-Telekommunikationsüberwachung'), […] mit der Infiltration die entscheidende Hürde genommen [ist], um das System insgesamt auszuspähen"[507].

Insbesondere liege ein Risiko vor,

> dass „auch die auf dem Personalcomputer abgelegten Daten zur Kenntnis genommen werden, die keinen Bezug zu einer telekommunikativen Nutzung des Systems aufweisen"[508].

Somit ist auf Grund der von der Infiltration eines informationstechnischen Systems bedingten Gefährdung für betroffene Grundrechtsträger das Vorliegen eines Handelns staatlicher Stellen mit *Grundrechtsrelevanz* unschwer zu bejahen.

Für den Schutz der ungehinderten Persönlichkeitsentfaltung bei der Nutzung informationstechnischer System besteht ein grundrechtlich erhebliches Bedürfnis.[509] Diesem Schutzbedürfnis trägt das aus dem allgemeinen Persönlichkeitsrecht nach Art. 2 I i. V. m. Art. 1 I GG hergeleitete *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* Rechnung.[510]

---

507 BVerfG NJW 2008, 822 (825).
508 BVerfG NJW 2008, 822 (825).
509 Vgl. BVerfG NJW 2008, 822 (825).
510 Vgl. BVerfG NJW 2008, 822 (824 ff.).

Gemäß den Feststellungen des BVerfG unter Bezugnahme auf angehörte sachkundige Auskunftspersonen

> „kann es im Übrigen dazu kommen, dass im Anschluss an die Infiltration Daten ohne Bezug zur laufenden Telekommunikation erhoben werden, auch wenn dies nicht beabsichtigt ist. In der Folge besteht für den Betroffenen – anders als in der Regel bei der herkömmlichen netzbasierten Telekommunikationsüberwachung – stets das Risiko, dass über die Inhalte und Umstände der Telekommunikation hinaus weitere persönlichkeitsrelevante Informationen erhoben werden. Den dadurch bewirkten spezifischen Gefährdungen der Persönlichkeit kann durch Art. 10I GG nicht oder nicht hinreichend begegnet werden“[511].

Gemäß weiterer Feststellung des BVerfG ist

> „Art. 10I GG […] hingegen alleiniger grundrechtlicher Maßstab für die Beurteilung einer Ermächtigung zu einer ‚Quellen-Telekommunikationsüberwachung‘, wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt. Dies muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein“[512].

Die letztgenannte Einschränkung der – freilich auslegungsfähigen – Entscheidung des BVerfG lässt den Schluss zu, dass auch für das Installieren der Überwachungssoftware zur Telekommunikationsüberwachung auf dem informationstechnischen System das Fernmeldegeheimnis aus Art. 10 I GG den alleinigen Grundrechtsmaßstab darstellt.[513]

Denn wie das BVerfG hier feststellt ist das neu aus Art. 2 I i. V. m. Art. 1 I GG abgeleitete *IT-Grundrecht* für die Beurteilung einer Ermächtigung zu einer Quellen-TKÜ, bei der sich die Überwachung ausschließlich auf Daten aus laufenden Telekommunikationsvorgängen beschränkt[514] und dies durch

---

511 BVerfG NJW 2008, 822 (826).

512 BVerfG NJW 2008, 822 (826).

513 Anders hingegen in der Schlussfolgerung *Buermeyer*/*Bäcker*, HRRS 2009, 433 (439), wonach die Infiltration des Systems einen eigenständigen Eingriff in das IT-Grundrecht in seiner Integritätsdimension bewirke, da niemals auszuschließen sei, dass Daten des Systems erhoben oder verändert werden, weil die mit dem Einbringen verbundenen Eingriffe zugleich Veränderungen am System darstellen, die dessen Integrität verletzen; ähnlich auch *Albrecht*/*Dienst*, JurPC Web-Dok. 5/2012, Abs. 50 m. w. N., wonach Primärmaßnahme und Sekundärmaßnahme die Gewährleistungsbereiche unterschiedlicher Grundrechte beträfen und bereits die Installation der Software einen irreversiblen Eingriff in die vom IT-Grundrecht geschützte Integrität befürchten ließe.

514 Für eine entsprechende Beschränkbarkeit, vgl. bspw. die Antwort der Bundesregierung, BT-Drs. 17/7760, S. 5; in dieselbe Richtung auch die Antwort des Bayerischen Staatsministeriums des Innern, LT-Drs. 16/10082, S. 2 u. 3; auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, *Schaar*, widerspricht insoweit kritischen Stimmen, wonach der Einsatz von Überwachungsprogrammen grds. ungeeignet sei, weil diese stets die technische Möglichkeit zum Ausspähen des Systems eröffnen würden, vgl. *Höll*, „Gefährliche Grauzone“, Süd-

technische Vorkehrungen und rechtliche Vorgaben sichergestellt ist, gerade nicht grundrechtlicher Maßstab. In diesem Falle ist die jeweilige Ermächtigung allein am grundrechtlichen Maßstab des Fernmeldegeheimnisses aus Art. 10 I GG zu messen. Dass das BVerfG hierbei nur die Primärmaßnahme ansprechen wollte, also das Überwachen und Aufzeichnen der Telekommunikation mittels der Überwachungssoftware, nicht aber die hierzu zwangsläufige Installation der Software auf dem betroffenen System erschiene sachfremd und inkonsequent. Denn eine „Ermächtigung zu einer ‚Quellen-Telekommunikationsüberwachung'"[515] müsste verständlicherweise nicht nur die eigentliche Überwachung und Aufzeichnung regeln und legitimieren, sondern um überhaupt praktisch umsetzbar zu sein auch – sei es ausdrücklich oder konkludent im Wege einer Annexkompetenz – die hierfür notwendige Vorbereitungsmaßnahme im Form des Einbringens der hierfür erforderlichen Software. Hierauf deutet indes auch das in der Entscheidungsbegründung niedergelegte Begriffsverständnis des BVerfG von einer „Quellen-Telekommunikationsüberwachung" hin, nämlich als das *technische Infiltrieren* eines komplexen informationstechnischen Systems zum Zweck der Telekommunikationsüberwachung[516]. Gemäß dieser Begriffsfassung zählt das BVerfG folglich die technische Infiltration mit der Software zur „Quellen-Telekommunikationsüberwachung"[517] dazu, für deren Ermächtigung („zu einer ‚Quellen-Telekommunikationsüberwachung'"[518]) unter den genannten Voraussetzungen Art. 10 I GG der alleinige Grundrechtsmaßstab ist.

---

deutsche Zeitung vom 13.10.2011, S. 6; nach Einschätzung von *Schaar* sei „es […] durchaus möglich, Programme einzusetzen, die dem Urteil des Bundesverfassungsgerichts von 2008 entsprechen", zitiert nach *Höll*, in: „‚Gefährliche Grauzone'", Süddeutsche Zeitung vom 13.10.2011, S. 6; a.A. hingegen *Buermeyer*/*Bäcker*, HRRS 2009, 433 (439) unter Verweis auf BVerfG NJW 2008, 822 (826 u. 830) zur Auskunft der (2008) gehörten Sachverständigen, wonach – so die Interpretation von *Buermeyer*/*Bäcker* – *niemals* auszuschließen sei, dass Daten des Systems erhoben oder verändert würden; diese Interpretation ist indes nicht derart zwingend, wie es die Formulierung der Autoren vermuten ließe, da es gemäß den Feststellungen des BVerfG „nach Auskunft der […] angehörten sachkundigen Auskunftspersonen […] im Übrigen dazu kommen [*kann*, Hervorh. d. Verf.], dass im Anschluss an die Infiltration Daten ohne Bezug zur laufenden Telekommunikation erhoben werden […]" (BVerfG NJW 2008, 822, 825 f.); auch der Kontext der Entscheidung deutet darauf hin, dass das BVerfG die technische Möglichkeit zu einer entsprechenden Beschränkung der Software nicht ausgeschlossen hat, da das BVerfG andernfalls Aussagen zu einer Konstellation getroffen hätte, die sich wider seines Dafürhaltens so in der Praxis überhaupt nicht ergeben könnte; für Einzelheiten zur Erstellung und Konfiguration der Überwachungssoftware, siehe 1. Teil A.II.4.b).

515 BVerfG NJW 2008, 822 (826).

516 So BVerfG NJW 2008, 822 (825).

517 BVerfG NJW 2008, 822 (825).

518 BVerfG NJW 2008, 822 (826).

Auch die vorausgehenden Feststellungen des BVerfG zu den Risiken einer Erfassung von Daten ohne Bezug zu laufenden Telekommunikationsvorgängen stehen dem nicht entgegen. Denn wie sich den Ausführungen des BVerfG und dessen Argumentationsfolge entnehmen lässt, bezieht sich das BVerfG mit seiner Aussage, dass „stets das Risiko, dass über die Inhalte und Umstände der Telekommunikation hinaus weitere persönlichkeitsrelevante Informationen erhoben werden“[519] auf die Situation, „dass im Anschluss an die Infiltration Daten ohne Bezug zur laufenden Telekommunikation erhoben werden, auch wenn dies nicht beabsichtigt ist“[520], da *dann* („in der Folge“[521]) die genannten Risiken und die dadurch bewirkten spezifischen Gefährdungen der Persönlichkeit bestehen, denen durch Art. 10 I GG nicht oder nicht hinreichend begegnet werden kann.[522] Dies gilt nach dem Gesamtzusammenhang gerade also nicht bei entsprechend sichergestellter Überwachung ausschließlich laufender Telekommunikationsvorgänge, da dann Art. 10 I GG den alleinigen grundrechtlichen Maßstab darstellt und demnach eine das IT-Grundrecht Art. 2 I i. V. m. Art 1 I GG eröffnende Tangierung des Integritätsinteresses des Betroffenen nicht gegeben ist.

b) Eingriff in Art. 13 I GG?

Im Rahmen seiner Entscheidung vom 27.02.2008 weist das BVerfG darauf hin, dass mit Blick auf die Menschenwürde sowie im Interesse der Persönlichkeitsentfaltung das Grundrecht auf Unverletzlichkeit der Wohnung aus Art. 13 I GG für den Einzelnen einen elementaren Lebensraum gewährleistet, in den Eingriffe nur unter den besonderen Voraussetzungen von Art. 13 II bis VII GG zulässig sind.[523] In Bezug auf den Schutz informationstechnischer Systeme belässt die Garantie des Art. 13 I GG gemäß den Feststellungen des BVerfG aber Schutzlücken gegenüber Zugriffen auf diese.[524]

Zwar kann nach Auffassung des BVerfG „eine staatliche Maßnahme, die mit dem heimlichen technischen Zugriff auf ein informationstechnisches System im Zusammenhang steht, an Art. 13I GG zu messen sein“[525]. Hier-

---

519 BVerfG NJW 2008, 822 (826).

520 BVerfG NJW 2008, 822 (826).

521 BVerfG NJW 2008, 822 (826).

522 Auch in dem Einleitungssatz dieses Abschnittes seiner Entscheidung stellt das BVerfG deshalb auf die durch Art. 2 I i. V. m. Art. 1 I GG zu schließende Schutzlücke hin, „soweit der heimliche Zugriff auf ein informationstechnisches System dazu dient, Daten auch insoweit zu erheben, als Art. 10I GG nicht vor einem Zugriff schützt“ (BVerfG NJW 2008, 822, 825).

523 Vgl. BVerfG NJW 2008, 822 (826).

524 Vgl. BVerfG NJW 2008, 822 (826).

525 BVerfG NJW 2008, 822 (826).

mit bezieht sich das BVerfG allerdings im Zusammenhang mit der Überwachung laufender Telekommunikation auf den physischen Zugriff auf das System als konkrete Vorgehensweise[526] zum Einbringen der staatlichen Überwachungssoftware unter Eindringen in eine als Wohnung geschützte Räumlichkeit.[527] Einen „generellen, von den Zugriffsmodalitäten unabhängigen Schutz gegen die Infiltration seines informationstechnischen Systems“[528] als solche, vermittelt das Grundrecht aus Art. 13 I GG nach Auffassung des BVerfG dem Einzelnen hingegen nicht.[529]

Während es vor der Grundsatzentscheidung des BVerfG umstritten war, ob bei einer Infiltration eines informationstechnischen Systems, welches sich in einer Wohnung befindet[530], der Schutzbereich des Art. 13 I GG eröffnet ist, führt das BVerfG nunmehr insoweit klarstellend aus, dass die Infiltration eines informationstechnischen Systems „unabhängig vom Standort erfolgen [kann], so dass ein raumbezogener Schutz nicht in der Lage ist, die spezifische Gefährdung des informationstechnischen Systems abzuwehren“[531]. Eine Infiltration lasse zudem „die durch die Abgrenzung der Wohnung vermittelte räumliche Privatsphäre unberührt“[532], soweit sie „die Verbindung des betroffenen Rechners zu einem Rechnernetzwerk ausnutzt“[533]. Gerade mit Blick auf mobile informationstechnische Systeme wie Laptops/Notebooks, PDAs, Mobiltelefone oder Smartphones (für die ebenfalls entsprechende VoIP-Programme auf dem Markt erhältlich sind[534]) werde deutlich, dass „der Standort des Systems […] in vielen Fällen für die Ermittlungsmaßnahme ohne Belang und oftmals für die Behörde nicht einmal erkennbar sein [wird][535].

Darüber hinaus stellt das BVerfG für die im Vergleich zur Quellen-TKÜ grundrechtsintensivere Maßnahme der Online-Durchsuchung zudem fest, dass Art. 13 I GG auch nicht gegen eine „durch die Infiltration des Systems ermöglichte [und insoweit über die spezifische Maßnahme der Quellen-TKÜ hinausgehende, Anm. d. Verf.] Erhebung von Daten, die sich im Ar-

---

526 Zur Frage der Grundrechtsrelevanz einzelner Vorgehensweisen zum Einbringen der Überwachungssoftware, siehe 2. Teil B.I.2.

527 Vgl. BVerfG NJW 2008, 822 (826).

528 BVerfG NJW 2008, 822 (826).

529 Vgl. BVerfG NJW 2008, 822 (826).

530 Vgl. zum Diskussionsstand vor der Entscheidung des BVerfG Anm. *Vogel*/*Brodowski*, StV 2009,632 (633).

531 BVerfG NJW 2008, 822 (826).

532 BVerfG NJW 2008, 822 (826).

533 BVerfG NJW 2008, 822 (826).

534 Für Einzelheiten, siehe 1. Teil A.I.2.d).

535 BVerfG NJW 2008, 822 (826).

beitsspeicher oder auf den Speichermedien eines informationstechnischen Systems befinden, das in einer Wohnung steht,“[536] schützt.

Unter Beachtung der im Rahmen der Entscheidung des BVerfG vom 27.02.2008 höchstrichterlich erfolgten Klarstellung ist demnach in Bezug auf die Infiltration von informationstechnischen Systemen, welche sich in einer Wohnung befinden, ein Eingriff in den Schutzbereich der Art. 13 I GG zu verneinen.

Hinsichtlich der Sekundärmaßnahme der Infiltration des informationstechnischen Systems mit einer Überwachungssoftware zum Zwecke der ausschließlichen Überwachung laufender Telekommunikationsvorgänge ist die Ermächtigungsgrundlage zu einer Quellen-TKÜ somit weder am Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 I i. V. m. Art. 1 I GG noch am Grundrecht auf Unverletzlichkeit der Wohnung nach Art. 13 I GG, sondern allein am Fernmeldegeheimnis aus Art. 10 I GG zu messen.

2. Grundrechtsrelevanz einzelner Vorgehensweisen zum Installieren

Zur unbemerkten Installation der Überwachungssoftware auf dem Zielsystem haben sich in der Praxis für die Ermittlungsbehörden eine Vielzahl von Vorgehensweisen als tauglich erwiesen. Dies ist dem Umstand geschuldet, dass jede Quellen-TKÜ-Maßnahme speziell auf den konkreten Einzelfall zugeschnitten ist und jede Art und Weise des Einbringens der Überwachungssoftware von den konkreten Umständen abhängig ist, die sich im Zuge der Vorfeldermittlungen – oftmals auch kurzfristig – ergeben. Mögliche Vorgehensweise zum Einbringen sind hierbei in praktischer Hinsicht allein von der Kreativität der durchführenden Ermittlungsbehörden und der Realisierbarkeit im Einzelfall bedingt. Wie bereits im Rahmen der Ausführungen zur technischen Umsetzung der Sekundärmaßnahme in Teil 1 im Einzelnen dargestellt[537], stehen den Ermittlungspersonen zum heimlichen Installieren der Überwachungssoftware auf dem Zielrechner sowohl Vorgehensweise aus der Ferne, v. a. über das Internet („Online“) zur Verfügung als auch direktes Einspielen der Software im Rahmen eines physischen Zugriffs auf das Zielgerät.

Es stellt sich hierbei die Frage, ob von der im Einzelfall gewählten Vorgehensweise ggf. eigene, spezifische Grundrechtseingriffe ausgehen:

---

536 BVerfG NJW 2008, 822 (826).

537 Siehe 1. Teil A.II.4.b).

a) Online/aus der Ferne

Für Ermittlungsbehörden gibt es eine Vielzahl von möglichen Vorgehensweisen zum Einbringen der Überwachungssoftware *aus der Ferne* bzw. *online* über das weltweite Datennetz, ohne direkten physischen Zugriff auf das Zielgerät nehmen zu müssen, bspw. durch Zusenden präparierter E-Mails, Zuspielen manipulierter Datenträger (z. B. CDs, DVDs, USB-Sticks), Einrichten fingierter Internetseiten, aber auch durch Ausnutzen bestehender Sicherheitslücken im Zielsystem bzw. herstellerseits eingebauter Hintertüren in das System (sog. *Backdoors*).

Vorgehensweisen, die *ohne ein (unbewusstes) Mitwirken* des Maßnahmeadressaten auskommen, wie bspw. das Ausnutzen von allgemein bestehenden Sicherheitslücken oder Hintertüren im Zielsystem haben über die Eingriffswirkung der Sekundärmaßnahme des heimlichen Installierens der Software – als zulässige Begleitmaßnahme einer Quellen-TKÜ[538] – hinaus grds. keinen eigenständigen Eingriffscharakter, der weitere grundrechtliche Schutzbereiche tangieren würde. Zwar ist gerade ein Vorgehen bspw. über Sicherheitslücken oder Hintertüren in IT-Systemen nicht frei von jeglicher Kritik – hätte doch ein diesbezüglich in Betracht kommendes staatliches Ankaufen von Informationen bzw. von entsprechenden virtuellen Werkzeugen (sog. *Exploits*) zum Eindringen in das System über derartige systemimmanente Sicherheitslücken u. U. aus Hackerkreisen oder auch von „Informations-Brokern“ mitunter aus dem Bereich der Wirtschaftsspionage[539] hinsichtlich der Bindung staatlichen Handelns an Recht und Gesetz zumindest einen gewissen „Beigeschmack“[540], zumal ein Geheimhalten und stilles Ausnutzen derartiger Sicherheitslücken in gewisser Weise auch in Konflikt

---

538 Zur Frage, an welchen Grundrechten das heimliche/verdeckte Installieren einer Überwachungssoftware zu messen ist, siehe 2. Teil B.I.1.; zur dogmatischen Erörterung der Frage, ob das heimliche/verdeckte Installieren einer Überwachungssoftware in zulässiger Weise auf eine Annexkompetenz zu § 100a StPO gestützt werden kann, siehe 2. Teil B.III.

539 Vgl. *Sieber*, Stellungnahme zu dem Fragenkatalog des BVerfG in dem Verfahren 1 BvR 370/07, S. 6, 11, abrufbar unter http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf (zuletzt aufgerufen 15.06.2012).

540 Wobei der staatliche Ankauf von (hier zwar nicht Beweis-, aber immerhin) Ermittlungshilfen, welche aus vermeintlich illegalen bzw. strafrechtlich relevanten Handlungen Privater stammen, einer Verwendung nicht zwingend entgegenstehen muss. Hierfür lassen sich auch Parallelen zur (verwertungsfreundlichen) Linie des BVerfG in Bezug auf die Verwertbarkeit von Beweismitteln, welche aus einem „Datendiebstahl“ stammen und von Behörden angekauft wurden („Liechtensteiner Steuer-CD“) herstellen, wonach Beweismittel, die von Privaten in rechtswidriger oder gar strafbewehrter Weise erlangt wurden, grds. verwertbar sind (vgl. BVerfG NJW 2011, 2417, 2420 m. w. N.).

mit der staatlichen Zielsetzung[541] geraten könnte, Behörden, Unternehmen und Bürger gerade vor Gefahren für die Sicherheit in der Informationstechnik zu schützen[542] –, stellt ein derartiges Vorgehen an sich (insbesondere unter Berücksichtigung der Wesentlichkeitstheorie des BVerfG[543]) dennoch keinen Eingriff in grundrechtlich garantierte Rechte und Freiheiten des Adressaten einer damit in Zusammenhang stehenden (strafprozessualen) Ermittlungsmaßnahme dar. Das Beschaffen entsprechender Informationen bzw. Werkzeuge im Vorfeld lässt sich hierbei als wenig intensiv (bzw. gar nicht[544]) in die Rechte des Betroffenen eingreifende Ermittlungshandlungen[545] ohne weiteres auf die allgemeine strafprozessuale Ermittlungsgeneralklausel aus §§ 161 I S. 1, 163 I StPO stützen.[546]

---

541 Welche hauptsächlich durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) wahrgenommen wird, vgl. auch §§ 1 ff. BSIG (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, BSI-Gesetz vom 14. August 2009, BGBl. I S. 2821).

542 Vgl. *Sieber*, Stellungnahme zu dem Fragenkatalog des BVerfG in dem Verfahren 1 BvR 370/07, S. 18, abrufbar unter http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf (zuletzt aufgerufen 15.06.2012); vgl. insoweit auch § 3 I BSIG.

543 Vgl. BVerfG NJW 1998, 2515; BVerfG NJW 1979, 359; BVerfG NJW 1978, 807; BVerfG NJW 1972, 1504.

544 Für „Bagatell"-Ermittlungshandlungen (bloße Spurensuche, Erkundigungen, Nutzung allgemein zugängliche Informationen u. ä.) bedürfte es mangels entsprechender Eingriffsqualität der Vorfeldermittlungsmaßnahme mitunter nicht einmal eines Abstellens auf die Ermittlungsgeneralklausel der §§ 161 I S. 1, 163 I StPO (vergleichbar mit dem materiellrechtlichen Bagatellausschlussprinzip *minima non curat praetor*), vgl. Löwe-Rosenberg – *Schäfer*, StPO und GVG, Zweiter Band, 25. Aufl. 2004, Vor § 94 StPO, Rn. 32 u. 54 f.

545 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 161, Rn. 1.

546 Von derartigen Vorfeldermittlungen strikt abzugrenzen ist allerdings die Installation der Überwachungssoftware als Vorbereitungsmaßnahme (Sekundärmaßnahme) zur anschließenden Realisierung der Überwachung der laufenden VoIP-Telekommunikation auf dem betroffenen System (Primärmaßnahme); da es sich bei der Sekundärmaßnahme einer Quellen-TKÜ (heimliches bzw. verdecktes Installieren einer Überwachungssoftware auf einem informationstechnischen System) insbesondere unter Berücksichtigung der Feststellungen des BVerfG in seiner Entscheidung vom 27.02.2008 (BVerfG NJW 2008, 822, 825) nicht um eine weniger intensiv eingreifende Maßnahme i. S. d. § 161 I StPO (vgl. zu den Voraussetzungen insoweit Meyer-Goßner – *Cierniak*, StPO, § 161, Rn. 1) handelt, lässt sich das heimliche bzw. verdeckte Installieren der Überwachungssoftware im Rahmen der Vorbereitung von Quellen-TKÜ-Maßnahmen nicht auf die Ermittlungsgeneralklausel aus §§ 161 I S. 1, 163 I StPO als Rechtsgrundlage stützen, vgl. insoweit zutr. auch *Sankol*,CR 2008, 13 (18); zur Frage des Vorliegens der Voraussetzungen einer Annexkompetenz zu § 100a I StPO als Rechtsgrundlage für die Installation der Software, siehe 2. Teil B.III.

Soweit jedoch den einzelnen Vorgehensweisen zum Einbringen der Software aus der Ferne bzw. online über das Datennetz eine gewisse „Täuschung“ bzw. Ausnutzung einer Leichtfertigkeit oder Leichtgläubigkeit des Maßnahmeadressaten durch *Auftreten unter einer Legende und/oder einem bestimmten Vorwand* zugrunde liegt (z. B. Zusenden einer präparierten E-Mail unter einer veränderten Identität, Zuspielen eines manipulierten USB-Sticks unter einem bestimmten Vorwand, Einrichten fingierter Internetseiten), bedarf es an dieser Stelle auch einer Beschäftigung mit der Frage, wie weit Ermittlungsbehörden Zielpersonen über bestimmte Umstände im Unklaren lassen dürfen bzw. bei dieser gar gezielt Fehlvorstellungen hervorrufen dürfen.

Zur Beurteilung der Frage, ob derartiges verdecktes Vorgehen der Ermittlungsbehörde unter einer Legenden oder einem bestimmten Vorwand zum Installieren der Überwachungssoftware in Konflikt mit grundgesetzlichen Rechten und Freiheiten steht und staatliches Handeln als solches gegenüber dem Betroffenen zu erkennen gegeben werden müsste, lässt sich zunächst auf ein Meinungsbild abstellen, welches sich im Zusammenhang mit der Diskussion über staatliche Maßnahmen zur Informationsbeschaffung über personenbezogene Inhaltsdaten durch gezieltes Ersuchen des Betroffenen entwickelt hat:

Bei Fallkonstellationen, in denen ein Betroffener gezielt um seine (persönlichen) Daten ersucht wird, sei der Staat grds. gehalten, offen zu handeln. Andernfalls würde das schutzwürdige Vertrauen des Betroffenen in die Identität und die Motivation seines Kommunikationspartners ausgenützt werden. Denn persönliche Daten würde der Betroffene u. U. dann nicht preisgeben, wenn er wüsste, dass er diese an eine Ermittlungsbehörde gibt, die jene Daten mitunter gegen ihn oder Dritte verwenden könnte.[547] Auch staatliche Identitätstäuschungen im Internet sollen in diesem Zusammenhang als Eingriff in das Recht auf informationelle Selbstbestimmung aus Art. 2 I i. V. m. Art. 1 I GG gewertet werden.[548]

Dieses Meinungsbild passt jedoch bereits vom ermittlungsgegenständlichen Ausgangspunkt her nicht zu den hier vorliegenden Konstellationen des staatlichen „Täuschens“ im Rahmen von strafprozessual verankerten heimlichen Ermittlungsmaßnahmen wie der heimlichen Überwachung und Aufzeichnung von Telekommunikation. Das verdeckte staatliche Vorgehen unter einem Vorwand bzw. einer Legenden zum Zwecke des unbemerkten Installierens einer Überwachungssoftware auf dem Zielgerät, auf welchem die Quellen-TKÜ-Maßnahme realisiert werden soll, stellt kein staatliches Han-

---

547 Vgl. *Gercke*/*Brunst*, Internetstrafrecht, Kap. 5, S. 316, Rn. 786.

548 Vgl. *Gercke*/*Brunst*, Internetstrafrecht, Kap. 5, S. 317, Rn. 788.

deln von der Qualität einer eigenständigen Ermittlungsmaßnahme dar, wie dies bei dem oben beschriebenen verdeckten staatlichen Handeln zur Informationsbeschaffung über persönliche Daten des Betroffenen der Fall ist, sondern erfolgt im Rahmen der Durchführung der Begleitmaßnahme zur Umsetzung einer (im Regelfall richterlich) angeordneten *heimlichen* strafprozessualen Ermittlungsmaßnahme zur Überwachung und Aufzeichnung von Telekommunikation[549].

Bei einer solchen „Täuschung", die im Rahmen der Durchführung der Begleitmaßnahme der heimlichen Quellen-TKÜ gegenüber dem Maßnahmeadressaten angewendet wird, handelt es sich auch nicht um eine Täuschung über Identität oder Motivation der handelnden Ermittlungspersonen als Kommunikationspartner des Maßnahmeadressaten zum Zwecke der Informationspreisgabe – was dann gerade auf Grund des „Verleitens" zur Informationspreisgabe in Konflikt mit dem Grundrecht auf informationelle Selbstbestimmung stehen könnte.[550] Die ermittlungsgegenständlichen Informationen gibt der Maßnahmeadressat hier vielmehr erst später auf Grund freier Willensentscheidung im Rahmen eines VoIP-Telefonates gegenüber seinem Gesprächspartner preis, ohne – jedenfalls von staatlicher Seite – über dessen Identität oder Motivation „getäuscht" worden zu sein.[551] Die (überwachte) Telekommunikation mit dem Gesprächspartner und die in diesem Rahmen stattgefundene Preisgabe von Daten und Informationen hat der Maßnahmeadressat ohne Einfluss und Bezug zur verdeckten staatlichen Vorgehensweise zum Zwecke des Aufspielens der Überwachungssoftware geführt und hätte dies auch ohne das hiervon unabhängige staatliche Handeln im Vorfeld getan. Dies stellt gerade den Unterschied zu obiger Konstellation des gezielten Ersuchen des Betroffenen um seine Daten dar. Das verdeckte Agieren der Ermittlungspersonen im Rahmen der vorliegend thematisierten Begleitmaßnahme einer Ermittlungsmaßnahme der (Quellen-) TKÜ dient hierbei gerade dem Ermöglichen der anschließenden Überwachung und Aufzeichnung einer („sowieso") geführten (VoIP-)Telekommuni-

---

549 Die Heimlichkeit bzw. Verdecktheit des Vorgehens ist hier gerade maßnahmetypisch und der StPO auch nicht unbekannt.

550 Nach Auffassung des BVerfG liegt ein Eingriff in das Recht auf informationelle Selbstbestimmung aus Art. 2 I i. V. m. Art. 1 I GG indes „nicht schon dann vor, wenn eine staatliche Stelle sich unter einer Legende in eine Kommunikationsbeziehung zu einem Grundrechtsträger begibt" (836), solange dabei „ein schutzwürdiges Vertrauen des Betroffenen in die Identität und in die Motivation seines Kommunikationspartners" (836) nicht ausgenutzt wird, vgl. BVerfG NJW 2008, 822 (836).

551 Zumal nach Auffassung des BVerfG bei Kommunikation im Internet „das Vertrauen eines Kommunikationsteilnehmers in die Identität und Wahrhaftigkeit seiner Kommunikationspartner nicht schutzwürdig" (836) sei, da „keinerlei Überprüfungsmechanismen" (836) (hinsichtlich der tatsächlichen Person hinter der virtuellen Identität) bereitstünden, vgl. BVerfG NJW 2008, 822 (836).

kation „ohne Wissen der Betroffenen“ i. S. d. § 100a I StPO. Der Maßnahmeadressat soll hier nicht durch die verdeckte Vorgehensweise zur Informationspreisgabe veranlasst werden, sondern lediglich von der heimlichen Installation der Software nichts mitbekommen und den Installationsvorgang unbewusst zulassen bzw. durch eigenes Handeln (mit-)initiieren. Das verdeckte Vorgehen im Rahmen der Begleitmaßnahme dient hierbei allein der Wahrung der Heimlichkeit der Maßnahme insgesamt.

Überdies ist es staatlichen Stellen in bestimmten Fällen gerade gestattet, heimlich bzw. verdeckt zu agieren.[552] Insbesondere aus den strafprozessualen heimlichen Ermittlungsmaßnahmen der §§ 100a ff. StPO wie auch aus Vorschriften wie der des § 110a StPO zum Einsatz sog. *verdeckter Ermittler*[553] wird deutlich, dass sowohl heimliche Ermittlungen als auch verdecktes Ermittlungshandeln, also Ermitteln unter bestimmten Vorwänden und Legenden, der StPO nicht unbekannt sind. Dies steht auch in Einklang mit grundsätzlichen Feststellungen des BGH, wonach die Heimlichkeit staatlicher Ermittlungstätigkeit „kein Umstand [ist], der für sich allein schon die Unzulässigkeit […] begründet“[554], weil es „weder rechtsstaatliche Grundsätze noch strafprozessuale Bestimmungen [aus]schließen […], im Rahmen der Aufklärung von Straftaten Methoden und Mittel anzuwenden, deren Gebrauch für den Tatverdächtigen nicht als polizeiliches Handeln erkennbar ist“[555]. Bei den strafprozessualen Eingriffsbefugnissen der §§ 100a ff. StPO handelt es sich gerade um Rechtsgrundlagen, die ihrer gesetzgeberischen Intention sowie ihrem Normzweck nach als strafprozessuale heimliche Ermittlungsmaßnahmen in die StPO eingefügt worden sind und in ihrem zulässigen Eingriffsbereich zu heimlichem bzw. verdecktem staatlichen Handeln legitimieren sollen. Diese Ermächtigungsgrundlagen erfassen hinsichtlich ihrer gesetzlichen Legitimationswirkung in Bezug auf die Heimlichkeit bzw. Verdecktheit des strafprozessualen Ermittelns notwendigerweise auch die Begleitmaßnahmen einschließlich deren konkreter Realisierungsweisen, die gerade die Heimlichkeit der Durchführung der gesetzlich legitimierten Maßnahme ermöglichen und gewährleisten sollen.

Die oben beschriebenen Vorgehensweisen zur *heimlichen bzw. verdeckten* Installation der Überwachungssoftware im Rahmen einer Quellen-TKÜ erhalten somit ihre rechtliche Legitimation direkt aus den Befugnisnormen der

---

552 Vgl. bei *Gercke*/*Brunst*, Internetstrafrecht, Kap. 5, S. 316, Rn. 786 m. w. N.

553 Verdeckte Ermittler sind gemäß der Legaldefinition in § 110a II StPO „Beamte des Polizeidienstes, die unter einer ihnen verliehenen, auf Dauer angelegten, veränderten Identität (Legende) ermitteln“.

554 BGH NJW 1994, 596 (599); ebenso BGH NJW 1996, 2940 (2942).

555 BGH NJW 1994, 596 (599), wenngleich Heimlichkeit staatlicher Eingriffsmaßnahmen in einem Rechtsstaat (zu Recht) die Ausnahme darstellt und besonderer Rechtfertigung bedarf, vgl. BVerfG NJW 2008, 822 (830) m. w. N.

§§ 100a, 100b StPO und den diesen zugrunde liegenden verfassungsrechtlichen Beschränkungen des Fernmeldegeheimnisses nach Art. 10 II GG, welches den alleinigen Grundrechtsmaßstab einer Quellen-TKÜ darstellt, wenn sich die Maßnahme allein auf Daten aus laufenden Telekommunikationsvorgängen beschränkt[556].

b) Direkter Zugriff

Des Weiteren besteht für die durchführenden Ermittlungsbehörden auch die Möglichkeit, das Einbringen der Software im Wege des direkten *physischen Zugriffs* auf das Gerät zu realisieren. Wie in Teil 1 im Rahmen der Ausführungen zu den *technischen Grundlagen* im Detail dargestellt[557], kommt als konkrete Vorgehensweise hierfür in der Praxis nicht nur das heimliche Verschaffen physischen Zugriffs auf das Zielgerät (in Abwesenheit des Betroffenen) in Betracht, sondern auch das Auftreten diesem gegenüber unter einem bestimmten Vorwand, um die Möglichkeit zu einem physischen Zugriff auf das Zielgerät zu erhalten und hierdurch die Überwachungssoftware direkt am Gerät einspielen zu können.

Diesbezüglich stellt es in der Praxis einen gangbaren Weg zum Einbringen der Software dar, dass *verdeckt physischer Zugriff* auf ein (mobiles) Zielgerät (i. d. R. Laptops/Notebooks) außerhalb grundrechtlich geschützter Räumlichkeiten des Maßnahmeadressaten bei (sich i. d. R. zufällig bzw. kurzfristig ergebender) *besonderer Gelegenheit* oder auch im Rahmen *ausgenutzter Situationen* erfolgt. Denkbar ist hier bspw. ein Zugriff im Rahmen einer durchgeführten Zollkontrolle[558] unter dem Vorwand das Gerät bspw. zum Zwecke der Feststellung des Gerätezustandes oder des Gerätewertes (außerhalb der Sichtweite des Betroffenen) kurzfristig „untersuchen“ zu müssen, wobei der Betroffene sich zwar darüber bewusst ist, dass sich das Gerät (bspw. das Notebook) gerade in staatlichen Händen befindet, jedoch nicht weiß, dass gelegentlich des staatlichen Handelns eine Überwachungssoftware aufgespielt wird. Zur Frage, inwieweit der Zulässigkeit solcher Vorgehensweisen deren „täuschender“ Charakter gegenüber dem Maßnahmeadressaten entgegensteht, kann auf die Ausführungen unter Punkt a) zum verdeckten Installieren der Software Online/aus der Ferne verwiesen werden. Auch beim direkten physischen Zugriff auf das Gerät dient die verdeckte Vorgehensweise nicht dem „Verleiten“ des Maßnahmeadressaten zur

---

556 Vgl. BVerfG NJW 2008, 822 (826).

557 Für Einzelheiten, siehe 1. Teil A.II.4.b)bb).

558 Vgl. für solch eine Vorgehensweise auch das der Entscheidung des LG Landshut vom 20.01.2011 (MMR 2011, 690) zugrunde gelegene Ermittlungsverfahren; hierzu auch BT-PlPr. 17/132 15597 A.

Informationspreisgabe, die er ohne staatliche „Täuschung“ nicht preisgegeben hätte, sondern erfolgt allein zum Zwecke des unbemerkten Installierens einer Überwachungssoftware, um die – gesetzlich zulässige – heimliche Überwachung und Aufzeichnung von Telekommunikation (hier in Form verschlüsselt übermittelter Internettelefonie) realisieren zu können. Darüber hinaus findet das begleitende heimliche Einschleusen der Überwachungssoftware hier regelmäßig unter Ausnutzung einer konkret, sich mitunter kurzfristig ergebenden Zugriffsmöglichkeit statt, also *gelegentlich* einer bestimmten Situation. So stehen bspw. dem kurzzeitigen Anhalten des Betroffenen im Rahmen einer zollrechtlichen Kontrolle und dem hierbei stattfindenden Verbringen des Gerätes „außer Blickweite“ des Betroffenen zum Ermöglichen eines unbemerkten Installierens der Überwachungssoftware auch weder die von Art. 2 I GG gewährleistete allgemeine Handlungsfreiheit noch die durch Art. 14 I GG geschützten Eigentumsfreiheit entgegen, da das kurzzeitige Anhalten und Entfernen des Gerätes aus dem unmittelbaren Sachherrschaftsbereich des Betroffenen – freilich unter dem Eindruck einer verpflichtenden Kontrolle – mit „Billigung“, jedenfalls aber in Kenntnis des Betroffenen und im Rahmen der Wahrnehmung zollrechtlicher Befugnisse geschieht. Der Umstand der Heimlichkeit der Einbringung der Software an sich ist hierbei wiederum gemäß obiger Ausführungen von der dem Handeln zugrunde liegenden (primären) Ermittlungsmaßnahme zur heimlichen Überwachung und Aufzeichnung von Telekommunikation mitumfasst[559].

Soweit sich den Ermittlungspersonen hingegen die Möglichkeit eröffnet, *heimlich*, also ohne Kenntnis des Maßnahmeadressaten vom deren Handeln überhaupt (in dessen Abwesenheit), *direkt auf das Gerät zuzugreifen* und die Überwachungssoftware zu installieren – bspw. denkbar anlässlich einer Reparatur oder während sich das Zielgerät (kurzzeitig) öffentlich zugänglich und unbeaufsichtigt außerhalb grundrechtlich geschützter Räume des Maßnahmeadressaten befindet – entfaltet dieses Handeln – unter Berücksichtigung der Feststellungen des BVerfG[560] – neben den von der zugrunde liegenden Befugnisnorm zur heimlichen Überwachung und Aufzeichnung der Telekommunikation gestatteten Primär- und Sekundäreingriffen in Art. 10 I GG keine weitere Grundrechtsrelevanz.

Als weitere heimliche Methode im Rahmen der direkten Zugriffnahme auf das Zielgerät kommt auch das Verschaffen physischen Zugriffs durch *heimliches Eindringen* in von der Zielperson genutzte Räume, in denen sich das Zielgerät befindet, in Betracht, um dort die Überwachungssoftware di-

---

559 Zur Frage, ob das heimliche Einbringen der Software als Annexkompetenz von § 100a I StPO mitumfasst ist, siehe hierzu 2. Teil B.III.

560 Vgl. BVerfG NJW 2008, 822 (825 f.).

rekt am Gerät einzuspielen. Es stellt sich hierbei die Frage, ob eine an Art. 10 I GG ausgerichtete Ermächtigungsnorm zu Maßnahmen der Quellen-TKÜ auch zu solch einer Vorgehensweise legitimieren kann, oder ob darüber hinaus ggf. wegen Tangierung des Schutzbereichs des Art. 13 I GG hierzu ein spezielles *Betretungsrecht* erforderlich wäre. Wie das BVerfG in seiner Grundsatzentscheidung vom 27.02.2008 festgestellt hat, kann der heimliche technische Zugriff auf ein informationstechnisches System, mit dem eine staatliche Maßnahme in Zusammenhang steht, indes an der grundrechtlichen Gewährleistung des Art. 13 I GG zu messen sein, wenn z. B. Ermittlungspersonen in als Wohnung geschützte Räumlichkeiten eindringen, um auf ein sich dort befindendes informationstechnisches System physisch einzuwirken[561]:

aa) Eingriff in Art. 13 I GG?

Für die Beantwortung der Frage, ob ein manuelles Einbringen der Software in das System durch direktes physisches Einwirken auf das Zielgerät unter Zugangverschaffen zu dessen Standort einen eigenständigen Eingriff in Art. 13 I GG darstellt, kommt es entscheidend darauf an, wo es sich befindet:

Außerhalb einer durch Art. 13 I GG geschützten Räumlichkeit (Wohnräume sowie nicht allgemein zugängliche Betriebs-/Geschäftsräume[562]) der Zielperson einer Quellen-TKÜ-Maßnahme stellt ein direkter (heimlich bzw. unter einem bestimmten Vorwand stattfindender) Zugriff auf das jeweilige Zielgerät zum Zwecke des Einspielens der Überwachungssoftware mangels staatlichen Eindringens in dessen räumlich geschützte Sphäre privaten Lebens und Wirkens *keinen* Eingriff dar, der an Art. 13 I GG zu messen wäre. Auch ein direkter Zugriff auf das Gerät in Räumen, die zwar dem sachlichen Schutzbereich des Art. 13 I GG unterfallen, aber nicht in einer derartigen persönlichen Beziehung zum Adressaten der Quellen-TKÜ-Maßnahme stehen, wie es die Eröffnung des persönlichen Schutzbereiches für diesen erfordern würde (also in öffentlich zugänglichen Räumen bzw. Räumen Dritter mit deren Einverständnis), bewirkt keinen Eingriff in dessen Grundrechtspositionen aus Art. 13 I GG. Die Vorgehensweise des Einbringens der Überwachungssoftware durch direkten physischen Zugriff am Zielgerät steht den Ermittlungsbehörden deshalb in den Fällen offen, in denen mit dem Zugriff kein Eingriff in Art. 13 I GG verbunden ist.[563] Das

---

561 Vgl. BVerfG NJW 2008, 822 (826).

562 Für Einzelheiten zum sachlichen Schutzbereich des Art. 13 I GG, siehe 1. Teil B.II.1.

563 So i. E. auch *Käß*, BayVBl. 2010, 1 (13).

Erfordernis eines Betretungsrechts stellt sich für diese Konstellationen mithin nicht.

Anders stellt sich dies wiederum dar, wenn sich das Zielgerät *innerhalb einer durch Art. 13 I GG geschützten Räumlichkeit des Adressaten befindet*.

Zur Frage des Online-Einbringens der Software in ein System, welches sich in Wohnräumen oder nicht allgemein zugänglichen Betriebs-/Geschäftsräume des Maßnahmeadressaten befindet, hat das BVerfG – wie oben näher ausgeführt – festgestellt, dass „Art. 13I GG […] dem Einzelnen […] keinen generellen, von den Zugriffsmodalitäten unabhängigen Schutz gegen die Infiltration seines informationstechnischen Systems [vermittelt]“[564] und zwar auch dann nicht, „wenn sich dieses System in einer Wohnung befindet“[565]. Soweit deshalb „die Infiltration die Verbindung des betroffenen Rechners zu einem Rechnernetzwerk ausnutzt, lässt sie die durch die Abgrenzung der Wohnung vermittelte räumliche Privatsphäre unberührt“[566].

Für die hier gegenständliche Frage des direkten (physischen) Zugriffs auf das Zielgerät innerhalb einer durch Art. 13 I GG geschützten Räumlichkeit des Adressaten zum Zwecke des Installierens der Überwachungssoftware hingegen hat das BVerfG festgestellt, dass „eine staatliche Maßnahme, die mit dem heimlichen technischen Zugriff auf ein informationstechnisches System im Zusammenhang steht, an Art. 13I GG zu messen“[567] ist, „wenn und soweit Mitarbeiter der Ermittlungsbehörde in eine als Wohnung geschützte Räumlichkeit eindringen, um ein dort befindliches informationstechnisches System physisch zu manipulieren“[568].

Dies ist in der vorliegenden Konstellation der Fall, da sich hier Ermittlungspersonen heimlichen Zutritt zu geschützten Räumlichkeiten verschaffen, um die Überwachungssoftware im Wege direkten physischen Zugriffs auf das Zielgerät in das System einzuspielen. Dies bewirkt einen spezifischen Eingriff in die nach Art. 13 I GG geschützte Privatheit der Wohnung als elementarer Lebensraum[569], in deren räumlicher Sphäre die freie Persönlichkeitsentfaltung des Einzelnen stattfindet[570] und in die nur unter den Voraussetzungen des Art. 13 II bis VII GG eingegriffen werden darf.

---

564 BVerfG NJW 2008, 822 (826).

565 BVerfG NJW 2008, 822 (826).

566 BVerfG NJW 2008, 822 (826); anders noch LG Hamburg, MMR 2008, 423 (424).

567 BVerfG NJW 2008, 822 (826).

568 BVerfG NJW 2008, 822 (826).

569 Vgl. BVerfG NJW 2008, 822 (826); BVerfG NJW 1979, 1539 (1540); bereits BVerfG NJW 1976, 1735 (1735) m. w. N.

570 Vgl. Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 1; *Epping*, Grundrechte, Kap. 17, S. 339, Rn. 716; S. 340, Rn. 720.

Mithin ist das heimliche Betreten grundrechtlich geschützter Räumlichkeiten des Maßnahmeadressaten zum Zwecke des Einspielens der Software am Grundrecht auf Unverletzlichkeit der Wohnung nach Art. 13 I GG zu messen[571], für das es eines entsprechenden verfassungsrechtlich legitimierten *Rechts zum Betreten* bedürfte.

bb) Problem: Betretungsrecht

Um den technischen und praktischen Schwierigkeiten des Aufspielens der Überwachungssoftware aus der Ferne bzw. des direkten Aufspielens im Rahmen regelmäßig von Zufällen abhängiger Situationen oder verdeckter Vorgehensweisen außerhalb der Wohnung zu begegnen, wird mitunter das Schaffen der Voraussetzungen für ein physisches Betreten der Wohnung des Betroffenen zum Zwecke des Einspielens[572] der Software[573] auf informationstechnischen Systemen, welche sich in nach Art. 13 I GG geschützten Räumlichkeit befinden, in Betracht gezogen.[574]

Für ein solches heimliches Sich-Zugang-Verschaffen wäre – wie bspw. bei Maßnahmen zur akustischen Wohnraumüberwachung nach §§ 100c ff. StPO in Art. 13 III GG – das Bestehen eines verfassungsrechtlich verankerten Betretungsrechts erforderlich. Denn ein mit dem heimlichen Aufspielen der Überwachungssoftware mittels direkten Zugriffs am Zielrechner in der Wohnung des Betroffenen verbundenes *heimliches*[575] physisches Betreten der Wohnung greift – wie bereits oben erläutert – in die räumliche (Privat-) Sphäre der Wohnung und mithin in den sachlichen Schutzbereich des Art. 13 I GG ein.[576]

---

571 Vgl. auch BVerfG NJW 2008, 822 (826); so auch *Käß*, BayVbl. 2010, 1 (6).

572 Bzw. entspr. auch zum Zwecke des Entfernens nach Abschluss der Überwachung, soweit dies manuell durch physischen Zugriff auf das System und nicht automatisiert durch entsprechende Softwarekonfiguration erfolgen soll.

573 Zum heimlichen/verdeckten Einbringen und Entfernen der Überwachungssoftware durch physisches Betreten, siehe auch 1. Teil A.II.4.b)bb) und c)bb).

574 In diese Richtung bspw. *Thönnes*, LKA Rheinland-Pfalz, schriftliche Befragung vom 26.10.2010, für Ausnahmefälle; vgl. zur Parallelproblematik im BayPAG auch *Käß*, BayVBl. 2010, 1 (13) m. w. N.; ein solches Betretungsrecht war bspw. für präventive Telekommunikationsüberwachungsmaßnahmen nach Art. 34a BayPAG in Art. 34e BayPAG vorgesehen gewesen, welcher jedoch durch Gesetz vom 27.07.2009 (GVBl. S. 380) wieder aufgehoben wurde, hierzu näher *Käß*, BayVBl. 2010, 1 (13).

575 Ein Betreten der Wohnung mit Einverständnis des Grundrechtsträgers hingegen lässt einen Eingriff in Art. 13 I GG entfallen; dies ist auch für den Fall anzunehmen, dass das Einverständnis unter einem Vorwand erwirkt wurde, vgl. hierzu auch die nachfolgenden Ausführung im Rahmen dieses Punktes weiter unten.

576 Während Art. 13 I GG des Weiteren auch dann betroffen sein kann, wenn durch heimlichen Zugriff auf Systemgeräte des Rechners (bspw. heimliches Aktiv-

Ein derartiges Betretungsrecht zum heimlichen Eindringen in eine Wohnung im Rahmen der Vorbereitung von TKÜ-Maßnahmen unter Eingriff in die Unverletzlichkeit der Wohnung ist gegenwärtig jedoch weder in Art. 13 GG verfassungsrechtlich verankert noch von den Vorschriften der §§ 100a, 100b StPO und der von ihnen vermittelten Annexkompetenz zum Zwecke der Vor- bzw. Nachbereitung[577] von (Quellen-)Telekommunikationsüberwachungsmaßnahmen umfasst.[578]

Auf die vorhandenen Grundrechtsschranken des Art. 13 GG kann ein heimliches Betreten geschützter Räumlichkeiten zum Zwecke der Umsetzung von Maßnahmen der Telekommunikationsüberwachung de lege lata indes nicht gestützt werden:

Bei einem heimlichen Betreten von Wohnräumen oder sonstigen durch Art. 13 I GG geschützten Räumlichkeiten (der allgemeinen Zugänglichkeit entzogene Betriebs-/Geschäftsräume)[579] ohne Einverständnis des jeweiligen persönlich geschützten Inhabers zum Zwecke der Ermöglichung einer Telekommunikationsüberwachung – sei es bspw. durch Präparieren eines dort befindlichen Telefonendgerätes mit einer entsprechenden Überwachungsvorrichtung[580] oder dem heimlichen Aufspielen einer Überwachungssoftware auf ein dort befindliches informationstechnisches System (i. d. R. den Computer) als Zielgerät im Rahmen einer Quellen-TKÜ – handelt es sich weder nach dem Maßnahmezweck um ein „ziel- und zweckgerichtete[s] Suchen staatlicher Organe“[581] noch nach dem Maßnahmecharakter um einen offenen Eingriff und damit nicht um eine *Durchsuchung*, anlässlich derer ein Betreten geschützter Räumlichkeiten gegen/ohne den Willen des Grund-

---

schalten einer angeschlossenen Webcam) eine Überwachung der Vorgänge in der Wohnung ermöglicht wird (vgl. BVerfG NJW 2008, 822, 826) – wie dies bei Maßnahmen der Online-Überwachung denkbar ist, hierzu 1. Teil A.II.2.a) – liegt ein solcher Fall bei Maßnahmen der Quellen-TKÜ nicht vor, da hier der überwachte Computer nicht wie eine Abhöranlage i. S. v. Art. 13 III S. 1 GG/§ 100c I StPO zielgerichtet oder ohne/gegen den Willen des Betroffenen in Betrieb genommen wird, sondern der betroffene Rechner bewusst vom Betroffenen zum Führen softwarebasierter Internettelefonie benutzt wird, vgl. auch *Bär*, TK-Überwachung, § 100a StPO, Rn. 32; a. A. *Sankol*, CR 2008, 13 (15).

577 Das heimliche Betreten unter Eingriff in Art. 13 I GG würde auf Grund des damit verbundenen erheblichen Eingriffs in die Unverletzlichkeit der Wohnung bereits keine *verhältnismäßig geringfügige Beeinträchtigung* im Vergleich zum Primäreingriff des § 100a I GG in das Fernmeldegeheimnis darstellen.

578 In diese Richtung auch *Bär*, persönliches Gespräch mit dem Verfasser, Bamberg, 09.12.2010; ebenso Anm. *Bär*, MMR 2011, 691 (692 f.); zutr. insoweit auch *Braun*, jurisPR-ITR 3/2011 Anm. 3.

579 Für Einzelheiten zum Schutzbereich des Art. 13 I GG, siehe 1. Teil B.II.1.

580 Letztlich zwar auch eine Telekommunikationsüberwachung „an der Quelle“, aber keine „Quellen-TKÜ“ i. S. d. terminus technicus.

581 BVerwG NJW 1975, 130 (131).

rechtsträgers seine verfassungsrechtliche Legitimation in *Art. 13 II GG* finden könnte. Fragen wirft in diesem Zusammenhang auch die Situation auf, wenn gelegentlich einer angeordneten, offen durchgeführten Durchsuchung gemäß §§ 102 ff. StPO die Überwachungssoftware in ein Gerät, welches sich in den durchsuchten Räumlichkeiten befindet, heimlich eingespielt wird. Hier ließe sich einerseits vertreten, dass das Betreten und der Aufenthalt der Ermittlungspersonen in den Räumlichkeiten des Betroffenen durch die auf den §§ 102 ff. StPO beruhende Durchsuchungsanordnung legitimiert ist und das heimliche Einspielen der Software als Begleitmaßnahme der gestatteten heimlichen Überwachung und Aufzeichnung der IP-Telekommunikation durch den jeweiligen Quellen-TKÜ-Beschluss[582]. Andererseits erscheint diese Vorgehensweise im Lichte des Art. 13 I GG problematisch, wenn die Durchsuchung letztlich nur zu dem Zwecke durchgeführt wurde, um die Software aufspielen zu können. Lässt man diesbezüglich Ähnliches gelten wie bei der „gezielten Suche nach Zufallsfunden"[583], so dürfte die Zulässigkeit einer derartigen Vorgehensweise in Frage stehen[584].

Auch handelt es sich hierbei nicht um eine Maßnahme zur Ermöglichung einer (heimlichen) *akustischen Überwachung des Wohnraums i. S. d. Art. 13 III GG*[585], weshalb ein heimliches Betreten der Wohnung zum Zwecke der Ermöglichung der Telekommunikationsüberwachung und der damit einhergehende Eingriff in Art. 13 I GG auch nicht auf diese verfassungsrechtliche Grundlage gestützt werden können. Die Schranke aus Art. 13 III GG, die in den §§ 100c ff. StPO einfachgesetzlich für das Strafprozessrecht umgesetzt wurde und repressive Eingriffe in Art. 13 I GG sowohl für die (Primärmaßnahme der) akustischen Überwachung des nichtöffentlich gesprochenen Wortes in Wohnungen mit technischen Mitteln als auch für das vorherige

---

582 In diese Richtung die Antwort des Bayerischen Staatsministeriums des Innern, LT-Drs. 16/8881, S. 7.

583 Zur Thematik der gezielten Suche nach Zufallsfunden, siehe BeckOK – *Hegmann*, StPO, Ed. 13, § 108, Rn. 4 f.; zur Verwertbarkeit gezielt gesuchter Zufallsfunde, siehe BVerfG NJW 2005, 1917.

584 Von der Unzulässigkeit einer solchen Vorgehensweise gehen bspw. *Braun*/*Roggenkamp*, K&R 2011, 681 (684) aus.

585 Da insoweit nicht die akustischen Geschehnisse innerhalb der Wohnung, sondern die mittels Telekommunikationsanlagen ausgetauschten Telekommunikationssprachsignale Anknüpfungspunkt einer TKÜ-Maßnahme sind – obgleich zulässigerweise eine Maßnahme der akustischen Wohnraumüberwachung auch die (einseitigen bzw. bei einem „Lautschalten" des Telefons zweiseitigen) Sprachsignale eines innerhalb der überwachten Wohnung stattfindenden Telefonates erfassen kann, während es wiederum bei einer Maßnahme der Telekommunikationsüberwachung auch zu einer Überwachung und Aufzeichnung von Hintergrundgeräuschen kommen kann, vgl. bezüglich letzterem auch BGH NStZ 2008, 473 (474); auch BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 92; Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 2; für Einzelheiten, siehe auch 1. Teil A.II.2.b).

heimliche Betreten der Wohnung zum Zwecke des Anbringens entsprechender Überwachungsvorrichtungen[586] („Wanzen“) als notwendigerweise damit verbundene Begleitmaßnahme (Sekundärmaßnahme) zur eigentlichen Überwachung verfassungsrechtlich gestattet[587], ist auf die Fälle des heimlichen Betretens von Wohnungen zur Ermöglichung von Telekommunikationsüberwachungen nicht anwendbar.

Des Weiteren handelt es sich beim Betreten der Wohnung zur Ermöglichung von Maßnahmen der Telekommunikationsüberwachung zu Zwecken der Verfolgung und Aufklärung von Straftaten um repressive Maßnahmen, weshalb auch die für die Einschlägigkeit des *Art. 13 VII GG* erforderlichen (präventiven) Voraussetzungen eines Eingriffs oder einer Beschränkung zur Abwehr oder Verhütung einer Gefahr im Rahmen sonstiger Maßnahmen i. S. d. Art. 13 VII GG nicht vorliegen.

Auch ein Betreten zur bloßen Nachschau im Rahmen der Überprüfung gesetzlicher Bestimmungen (bspw. Einhaltung von Hygienevorschriften), die nach überwiegender Auffassung bereits das Vorliegen eines Eingriffes in Art. 13 I GG[588] entfallen lassen würde[589], liegt in diesen Fällen ebenso wenig vor.

Eine entsprechende Einschränkung des Rechts auf Unverletzlichkeit der Wohnung zum heimlichen Betreten von Wohnungen im Rahmen von TKÜ-Maßnahmen – wie dies in Art. 13 III GG für Maßnahmen der repressiven akustischen Wohnraumüberwachung verankert ist – findet gegenwärtig weder in den Bestimmungen des Art. 13 GG eine verfassungsrechtliche Grundlage noch ist ein solches Betretungsrecht den einfachgesetzlichen Vorschriften der §§ 100a, 100b StPO zur Telekommunikationsüberwachung zugrunde gelegt.

Aus diesem Grunde kommt es in der Praxis für das Installieren der Überwachungssoftware durch direkten physischen Zugriff in entscheidender Weise darauf an, wo sich das Zielgerät befindet und ob es (frei) zugänglich ist[590]:

---

586 Vgl. BVerfG NJW 1984, 419 (421).

587 Vgl. BT-Drucks. 13/8651, S. 13; auch Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 79; Meyer-Goßner – *Cierniak*, StPO, § 100c, Rn. 7.

588 Für Einzelheiten zu Eingriffen in Art. 13 I GG, vgl. 1. Teil B.II.2.

589 Unter bestimmten Voraussetzungen soll ein Betreten von Betriebs- und Geschäftsräumen auf Grund besonderer Befugnisnormen (z. B. § 17 HandwO oder § 22 GastG) zur Nachschau, ob bestimmte gesetzliche Bestimmungen eingehalten werden (z. B. Hygienevorschriften), schon gar keinen Eingriff in Art. 13 GG darstellen, vgl. hierzu im Einzelnen *Epping*, Grundrechte, Kap. 17, S. 343 f., Rn. 723 f. sowie BVerfG NJW 1971, 2299 (2301); vertieft auch bei Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 141 ff.

590 In diese Richtung auch *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11.2010.

Befindet sich das Zielgerät in Wohnräumen bzw. sonstigen von Art. 13 I GG geschützten Räumlichkeiten[591] des Maßnahmeadressaten und ist deshalb für den heimlichen Zugang zum Gerät ein Betretungsrecht erforderlich, so kann der physische Zugriff zur Installation der Überwachungssoftware in den geschützten Räumen ohne Einverständnis des Grundrechtsträgers zum Betreten nicht stattfinden, da ein entsprechendes Betretungsrecht für Maßnahmen der (Quellen-)Telekommunikationsüberwachung – wie erläutert – in Art. 13 GG (gegenwärtig) keine verfassungsrechtliche Grundlage findet.

Befindet sich das Gerät hingegen außerhalb der Wohnung oder in sonstigen, nicht der Privatsphäre des Maßnahmeadressaten dienenden Räumlichkeiten, bspw. in öffentlich zugänglichen Räumen oder in Räumen Dritter, die ihr Einverständnis in das staatliche Betreten erteilt haben, verhält es sich anders. In diesen Fälle ist ein Betretungsrecht wegen des öffentlichen Charakters der Räume bzw. wegen des Einverständnisses des Inhabers nicht erforderlich und – bei Bestehen der praktischen Möglichkeit hierzu – ein physischer Zugriff auf das Zielgerät zum direkten Einspielen der Überwachungssoftware unter Art. 13 I GG-Gesichtspunkten zulässig.

Dies heißt jedoch nicht, dass innerhalb der Wohnung oder einer sonstigen von Art. 13 I GG geschützten Räumlichkeit des Maßnahmeadressaten ein jedes Betreten zum Zwecke des Erlangens direkten physischen Zugriffs auf das Zielgerät mangels Bestehens eines entsprechenden Betretungsrechts für Ermittlungsbehörden zwangsläufig ausscheiden muss. Denn ein Betreten der Wohnung mit Einverständnis des betroffenen Grundrechtsträgers lässt einen Eingriff in Art. 13 I GG entfallen.[592] Hieran ändert sich auch nichts, wenn das Einverständnis auf Grund eines Vorwandes erwirkt wurde, da der Schutzbereich des Art. 13 I GG nach überzeugender Auffassung nicht das Vertrauen des Grundrechtsträgers in die Redlichkeit von Personen, die er freiwillig in seine Wohnung eintreten lässt, erfasst.[593] Somit stellt auch ein Betreten der Wohnung mit dem Einverständnis des Grundrechtsträgers, welches zum Erlangen der direkten Zugriffsmöglichkeit auf das Zielgerät in der geschützten Räumlichkeit unter einem bestimmten Vorwand erwirkt wurde (denkbar ist bspw. ein Auftreten als Computerreparaturdienst u. ä.), keinen Eingriff in das Grundrecht des Art. 13 I GG auf Unverletzlichkeit der Wohnung dar.[594] Entsprechend bedarf es für eine derartige Vorgehensweise im

---

591 Für Einzelheiten zum Schutzbereich des Art. 13 I GG, siehe 1. Teil B.II.1.

592 Vgl. auch BeckOK – *Fink*, GG, Ed. 13, Art. 13, Rn. 11.

593 Vgl. insoweit BeckOK – *Fink*, GG, Ed. 13, Art. 13, Rn. 11 m. w. N.

594 Freilich ist hier das Gelingen des unbemerkten Einbringens zu einem Großteil abhängig von Unwägbar- und Zufälligkeiten, weshalb in der Praxis hier in besonderer Weise das Risiko einer Entdeckung und damit Gefährdung der Ermittlungen mit anderen Vorgehensweisen zum Einbringen abgewogen werden müsste.

Rahmen des Einbringens der Überwachungssoftware auch keines Betretungsrechts.

Es lässt sich somit als Ergebnis festhalten, dass einem (heimlichen oder unter einem bestimmten Vorwand stattfindenden) direkten Zugriff durch Ermittlungspersonen auf Zielgeräte 1. in öffentlich zugänglichen Räumen oder Räumen Dritter mit deren Einverständnis sowie 2. in Wohnräumen und sonstigen geschützten Räumlichkeiten des Maßnahmeadressaten mit dessen (wenn auch ggf. unter einem Vorwand erwirkten) Einverständnis nicht entgegengehalten werden kann, dass ein Recht zum heimlichen Betreten der Räume nicht bestünde. Ein direkter physischer Zugriff auf das Zielgerät zum Zwecke des Einspielens der für eine Quellen-TKÜ-Maßnahme notwendigen Überwachungssoftware kann deshalb in diesen Fällen – jedenfalls unter Art. 13 I GG-Gesichtspunkten[595] – ohne weiteres in zulässiger Weise erfolgen.

Für das heimliche Betreten bzw. Sich-Zutritt-Verschaffen zur Wohnung oder zu sonstigen geschützten Räumlichkeiten des Maßnahmeadressaten zum Zwecke des direkten physischen Zugriffs auf das Zielgerät, bedürfte es hingegen der Normierung einer entsprechenden Schranke in Art. 13 I GG, die den mit dem heimlichen Betreten der geschützten Räumlichkeiten zur Realisierung von strafprozessualen Maßnahmen der Überwachung und Aufzeichnung von Telekommunikation verbundenen Eingriff in das Grundrecht auf Unverletzlichkeit der Wohnung verfassungsrechtlich legitimiert. Der Verankerung eines Rechts zum heimlichen Betreten von nach Art. 13 I GG geschützten Räumen auch im Rahmen von strafprozessualen Maßnahmen der (Quellen-)Telekommunikationsüberwachung notwendig vorgeschaltet wäre freilich eine entsprechende rechtspolitische Willensbildung und ein Tätigwerden des Gesetzgebers zur Ergänzung des Art. 13 GG um eine weitere Schranke, wie dies für die strafprozessuale akustische Wohnraumüberwachung in Art. 13 III GG geschehen ist.

II. Entfernen der Überwachungssoftware vom Zielsystem

Wie das heimliche bzw. verdeckte Installieren der Überwachungssoftware zu Beginn der Maßnahme ist auch das heimliche bzw. verdeckte (automatisiert oder manuell erfolgende) Entfernen der Überwachungssoftware vom überwachten Zielsystem nach Abschluss der Überwachungsmaßnahme (als „*actus contrarius*“) ein Vorgang, der im Zusammenhang mit der technischen Überwachung von verschlüsselt übermittelter IP-Kommunikation am jewei-

---

595 Für Einzelheiten zum Grundrecht auf Unverletzlichkeit der Wohnung, Art. 13 I GG, siehe 1. Teil B.II.

ligen Endgerät im Rahmen der Durchführung von Quellen-TKÜ-Maßnahmen Relevanz entfaltet.

Ob sich das Entfernen der Software als typische und verhältnismäßige Begleitmaßnahme in rechtlicher Hinsicht auf eine Annexkompetenz zu § 100a I StPO stützen lässt, ist Gegenstand der Ausführungen zu *Typizität* und *Verhältnismäßigkeit* der Begleitmaßnahmen unter Punkt III. dieses Abschnitts.

Zuvor bedarf es jedoch auch hier einer näheren Auseinandersetzung mit der Frage, ob und welche, ggf. eigenständige, grundrechtliche Relevanz die (heimliche bzw. verdeckte) Deinstallation der Überwachungssoftware vom überwachten Zielsystem („Deinfiltration des Systems") entfaltet. Die in der Praxis in Frage kommenden Vorgehensweisen zum Entfernen der Software sind – wie im Rahmen des 1. Teils im Einzelnen dargestellt[596] – der Zugriff *über das Leitungsnetz* von außen („Online"), der *direkte Zugriff* am Gerät sowie die *automatisierte Löschung*.

Als gegensätzlicher Akt zum Installieren der Überwachungssoftware auf dem überwachten informationstechnischen System in Vorbereitung der eigentlichen Überwachung (Infiltration des Systems), ist das Entfernen der Software nach Abschluss der Ermittlungsmaßnahme in „Nachbereitung" grds. an denselben grundrechtlichen Maßstäben auszurichten. Die Deinstallation einer Überwachungssoftware, welche zum Zwecke der Überwachung und Aufzeichnung von laufender Telekommunikation in ein informationstechnisches System eingebracht worden ist, bemisst sich unter Zugrundelegung der Feststellungen des BVerfG für die „Beurteilung einer Ermächtigung zu einer ‚Quellen-Telekommunikationsüberwachung'"[597] – die konsequenterweise nicht nur das Einbringen als vorbereitende Maßnahme, sondern auch das Entfernen nach Abschluss als nachbereitende Maßnahme umfassen muss – wie die vorbereitende technische Infiltration des informationstechnischen Systems, also als nachbereitende „technische Deinfiltration" des Systems, unter Berücksichtigung des Sachzusammenhangs ebenfalls anhand des grundrechtlichen Maßstabs aus Art. 10 I GG.

Auch hier würde deshalb ein heimliches Betreten von Wohnräumen zum Zwecke des Entfernens der Software durch direkten Zugriff am Gerät einen Eingriff in Art. 13 I GG darstellen[598], der mangels eines entsprechenden Betretungsrechts von einer Ermächtigungsgrundlage, wie sie in den §§ 100a, 100b StPO enthalten ist und lediglich Eingriffe in das Fernmeldegeheimnis

---

596 Für Einzelheiten zu den Vorgehensweisen zum Entfernen der Software, siehe 1. Teil A.II.4.c).

597 BVerfG NJW 2008, 822 (826).

598 Vgl. auch BVerfG NJW 2008, 822 (826).

aus Art. 10 I GG, nicht jedoch in das Grundrecht auf Unverletzlichkeit der Wohnung gestattet, verfassungsrechtlich nicht gedeckt wäre.[599]

Es stellt sich hierbei aber die Frage, ob sich eventuell eine zusätzliche Grundrechtsrelevanz aus einer Tangierung der Rechtsschutzgarantie aus Art. 19 IV GG auf Grund der mitunter (bzw. wohl im Regelfall[600]) erfolgenden Heimlichkeit bzw. Verdecktheit des Entfernens und damit zusammenhängend auch des Zeitpunkts der Deinstallation der Software ergeben könnte:

Findet die Deinstallation offen und möglichst zeitnah nach dem in § 101 V S. 1 StPO bestimmten Bekanntgabezeitpunkt statt, sprich dann, wenn die Benachrichtigung insbesondere ohne Gefährdung des Untersuchungszwecks möglich ist, so kann sich der Betroffene, auf dessen Gerät die Überwachung realisiert wurde, gegen den bis zur Entfernung der Software andauernden Eingriff dadurch zur Wehr setzen, dass er gegen die gerichtlich angeordnete – insoweit noch nicht abschließend vollzogene – Maßnahme das Rechtsmittel der Beschwerde (§§ 304 ff. StPO)[601] einlegt.[602] Diese Möglichkeit der Erlangung gerichtlichen Rechtsschutzes gegen die Vornahme von nachbereitenden Maßnahmen steht dem Betroffenen aber dann nicht zur Verfügung, wenn die durchführende Ermittlungsbehörde die Überwachungssoftware vor dem in § 101 V S. 1 StPO normierten Zeitpunkt von dem System – dementsprechend heimlich bzw. verdeckt – entfernt.[603]

Dieser Umstand steht der Einordnung des heimlichen Entfernens der Software als zulässige (Nachbereitungs-)Maßnahme jedoch nicht zwingend entgegen. Denn auch bei der Beurteilung von nachbereitenden Begleitmaßnahmen ist vielmehr auf den Gesamtcharakter der Ermittlungsmaßnahme abzustellen.[604] Maßnahmen der Überwachung und Aufzeichnung von Tele-

---

599 Vgl. hierzu die entsprechenden Ausführungen zum Installieren der Software unter 2. Teil B.I.2.b).

600 So wird eine kriminaltaktische Notwendigkeit für ein heimliches bzw. verdecktes Entfernen der Software vom Zielsystem i. d. R. dann bestehen, wenn sich aus der überwachten Kommunikation erkennen lässt, dass durch ein offenes Vorgehen bspw. noch andauernde Ermittlungen, bei denen ein ermittlungstaktisches Interesse an der noch zeitweisen Aufrechterhaltung der Geheimhaltung fortbesteht, gefährdet werden könnten, vgl. in diese Richtung auch *Schneider*, NStZ 1999, 388 (390) zum Ausbau von in einen PKW eingebauten Abhörvorrichtungen im Rahmen von Maßnahmen nach § 100c I Nr. 2 StPO a. F. (§ 100f I StPO n. F.).

601 Eilanordnungen der Staatsanwaltschaft sind gemäß § 98 II S. 2 StPO analog angreifbar, vgl. *Bär*, TK-Überwachung, § 100b StPO, Rn. 27.

602 Vgl. *Schneider*, NStZ 1999, 388 (390) zu Maßnahmen nach § 100c I Nr. 2 StPO a. F. (§ 100f I StPO n. F.).

603 Vgl. *Schneider*, NStZ 1999, 388 (391) zu Maßnahmen nach § 100c I Nr. 2 StPO a. F. (§ 100f I StPO n. F.).

604 Vgl. zutr. *Schneider*, NStZ 1999, 388 (391) zu Maßnahmen nach § 100c I Nr. 2 StPO a. F. (§ 100f I StPO n. F.).

kommunikation (repressiv nach §§ 100a, 100b StPO) sind in ihrer Gesamtheit gerade durch eine heimliche Vorgehensweise – sei es bei einem „klassischen" Abfangen von Daten auf der Transportstrecke oder bei einem Zugriff am Endgerät – charakterisiert.[605] Aus diesem Grunde spricht die – auch bei anderen heimlichen Ermittlungsmaßnahmen relevante – Tatsache *zeitlich aufgeschobenen Rechtsschutzes* wohl kaum gegen die Zulässigkeit der heimlichen bzw. verdeckten Deinstallation der Software.[606] Zu berücksichtigen ist hierbei insbesondere auch die gesetzgeberische Wertung aus § 101 V S. 1 StPO, wonach die (zeitweise) Geheimhaltung der Maßnahme zur Vermeidung einer Gefährdung des Untersuchungszwecks ein legitimes Anliegen der Ermittlungsbehörden darstellt.[607] Das berechtigte Interesse an vorübergehender Aufrechterhaltung der Geheimhaltung rechtfertigt es indes, individuelle Rechtsschutzbelange des Betroffenen jedenfalls zeitweise zu verkürzen.[608] Dem Umstand, dass bei Maßnahmen der Quellen-TKÜ als technisches Mittel zur Überwachung eine komplexe Überwachungssoftware verwendet wird, bei deren heimlicher Entfernung es dem Betroffenen – gerade im Hinblick auf die Abgrenzung zu Maßnahmen der Online-Durchsuchung – erschwert werden könnte, eventuelle, über die (von der Anordnung gestattete) bloße Überwachung laufender Telekommunikationsvorgänge hinausgehende Funktionalitäten nachzuweisen, lässt sich durch eine angemessene Dokumentation und ggf. Hinterlegung einer Kopie der verwendeten Software wie auch durch eine lückenlose Dokumentation und Protokollierung deren Einsatzes Rechnung tragen. Die hierdurch eröffneten Möglichkeiten zur späteren Überprüfung der verwendeten Überwachungssoftware – einerseits ggf. im Rahmen eines gerichtlichen Nachprüfungsverfahrens der Rechtmäßigkeit der konkreten Ermittlungsmaßnahme (§ 101 VII S. 2 StPO), andererseits auch im Rahmen der Prüfung der Gerichtsverwertbarkeit erlangter Erkenntnisse im Rahmen des Hauptverfahrens – erscheint mit Blick

---

605 Vgl. hierzu auch BT-Drs. 16/5846, S. 39.

606 Vgl. *Schneider*, NStZ 1999, 388 (391) zu Maßnahmen nach § 100c I Nr. 2 StPO a. F. (§ 100f I StPO n. F.); dies steht auch in Einklang mit den grundsätzlichen Feststellungen des BGH (BGH NJW 1994, 596, 599), wonach die Heimlichkeit staatlicher Ermittlungstätigkeit „kein Umstand [ist], der für sich allein schon die Unzulässigkeit eines solchen Verfahrens begründet" (599), da es „weder rechtsstaatliche Grundsätze noch strafprozessuale Bestimmungen [aus]schließen […], im Rahmen der Aufklärung von Straftaten Methoden und Mittel anzuwenden, deren Gebrauch für den Tatverdächtigen nicht als polizeiliches Handeln erkennbar ist" (599); ebenso BGH NJW 1996, 2940 (2942).

607 Vgl. *Schneider*, NStZ 1999, 388 (391) zu Maßnahmen nach § 100c I Nr. 2 StPO a. F. (§ 100f I StPO n. F.).

608 Vgl. *Schneider*, NStZ 1999, 388 (391) zu Maßnahmen nach § 100c I Nr. 2 StPO a. F. (§ 100f I StPO n. F.); vgl. insoweit auch BVerfG NJW 2000, 55 (57).

auf das berechtigte Interesse an (vorübergehendem) Aufrechterhalten der Geheimhaltung sachgerecht.

Mit Blick auf den grundsätzlichen Charakter von Telekommunikationsüberwachungen als heimliche Ermittlungsmaßnahmen und die gesetzgeberische Wertung aus § 101 V S. 1 StPO stehen daher dem heimlichen bzw. verdeckten Entfernen der Software noch vor Benachrichtigung des Betroffenen keine durchgreifenden verfassungsrechtlichen Bedenken aus Art. 19 IV GG entgegen. Unberührt hiervon steht dem Betroffenen zudem nach Beendigung der Maßnahme die genannte Rechtsschutzmöglichkeit offen, bis zu zwei Wochen nach erfolgter Benachrichtigung Antrag auf gerichtliche Überprüfung der Rechtmäßigkeit der Maßnahme und der Art und Weise ihres Vollzuges nach § 101 VII S. 2 StPO zu stellen, wobei es in diesem Zusammenhang zu Recht aus Gründen der Rücksichtnahme auf die Belange des Betroffenen angezeigt ist[609], im Rahmen der Benachrichtigung nach § 101 IV StPO den Betroffenen auch über die insoweit durchgeführten Begleitmaßnahmen in Kenntnis zu setzen.

III. Rechtsgrundlage: Annexkompetenz zu § 100a StPO?

Der mit der Installation der Überwachungssoftware (aber auch mit deren Deinstallation) auf dem Zielsystem verbundene Eingriff in die Rechtsposition des Betroffenen (Infiltration eines informationstechnischen Systems) ist in den gesetzlichen Befugnisnormen der §§ 100a, 100b StPO zur (primären) Überwachung und Aufzeichnung der Telekommunikation[610] *nicht ausdrücklich geregelt*. Wie die Abgrenzung zu anderen Ermittlungsmaßnahmen gezeigt hat[611], legitimieren auch sonstige Ermittlungsbefugnisse der StPO zu heimlichen strafprozessualen Ermittlungen die hier erfolgende heimliche Infiltration des Zielsystems mit einer Überwachungssoftware zum Zwecke des Abgreifens laufender Kommunikation an der Quelle nicht.

Zur Beurteilung der Zulässigkeit des Ermittlungsinstruments der Quellen-TKÜ stellt sich deshalb die Frage, ob ergänzende Maßnahmen wie das heimliche Installieren bzw. Deinstallieren der Überwachungssoftware auf einem informationstechnischen System unter Berücksichtigung des Gesetzesvorbehaltes in Art. 10 II S. 1 GG dennoch von den §§ 100a, 100b StPO

---

609 Vgl. *Schneider*, NStZ 1999, 388 (391) zu Maßnahmen nach § 100c I Nr. 2 StPO a. F. (§ 100f I StPO n. F.).

610 Für Einzelheiten zu Fragen der Primärmaßnahme, siehe 2. Teil A.II sowie 3. Teil A.I.1.

611 Für Einzelheiten zur Abgrenzung der Quellen-TKÜ zu sonstigen heimlichen Ermittlungsmaßnahmen, siehe 1. Teil A.II.2.

gedeckt sein können. Dies wäre dann der Fall, wenn sich die Maßnahmen auf eine sog. *Annexkompetenz zu § 100a StPO* stützen lassen:

Der qua (höchst-)richterlicher Rechtsfortbildung wie auch durch das Schrifttum entwickelten[612] Annahme des Bestehens von sog. *Annexkompetenzen* für gesetzlich (in der StPO regelmäßig[613]) in den jeweiligen Befugnisnormen nicht ausdrücklich geregelte Begleiteingriffe in die Rechte Betroffener, welche im Rahmen der Durchführung von im Übrigen, sprich in ihrem primären Eingriff, auf Grundlage der gesetzlichen Regelungen zulässigen strafprozessualen Ermittlungsmaßnahmen erfolgen, liegt der Gedanke zugrunde, dass es dem parlamentarischen Gesetzgeber bei der Schaffung von strafprozessualen Eingriffstatbeständen – insbesondere solchen, die wie §§ 100a, 100b StPO von der technischen Entwicklung beeinflusst und deshalb entwicklungsoffen und technologieneutral formuliert sind[614] – gerade auf Grund der „Vielgestaltigkeit möglicher Sachverhalte“[615] nicht möglich ist, sämtliche Einzelheiten der – vor allem technischen – Realisierung der von der Eingriffsbefugnis gestatteten Eingriffe ausdrücklich zu regeln und er deshalb auf Grund einer konkludent erteilten Ermächtigung auch solche Begleiteingriffe als von der Befugnisnorm mit umfasst und damit als zulässig ansieht, die notwendig sind, um die gesetzlich geregelte Primärmaßnahme nicht gänzlich oder im Wesentlichen ins Leere laufen zu lassen.[616] Denn die strikte Ablehnung gesetzlich nicht ausdrücklich geregelter Begleitmaßnahmen mit dem Argument der fehlenden Ermächtigungsgrundlage würde zwar ggf. zu klaren (bzw. klareren), zugleich aber mitunter lebensfernen und inakzeptablen Lösungen der Begleitmaßnahmenproblematik führen.[617]

Die Annahme von Annexkompetenzen ist allerdings nicht schrankenlos.[618] Um in den Fällen der Annahme einer Annexkompetenz dem verfassungsrechtlichen Grundsatz vom Vorbehalt des Gesetzes aus Art. 20 III GG gerecht zu werden[619], muss es sich bei der in Frage stehenden – gesetzlich

---

612 Vgl. BGH-Ermittlungsrichter NStZ 1998, 157; BGH NJW 2001, 1658; BGH-Ermittlungsrichter NStZ 2005, 278; vgl. auch BT-Drs. 13/8651, S. 13.

613 Vgl. hierzu *Henrichs*, Kriminalistik 2008, 438 (440).

614 Vgl. BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 2 u. 6; vgl. auch *Kudlich*, JuS 2001, 1165 (1166) m. w. N.; *ders*., JA 2010, 310 (312).

615 BVerfG NJW 2009, 2431 (2434) zu §§ 94 ff. StPO, trifft insoweit auf § 100a I StPO gleichfalls zu.

616 Vgl. BGH-Ermittlungsrichter NStZ 2005, 278 (278); bereits BGH-Ermittlungsrichter NStZ 1998, 157 (157); so zutr. auch LG Hamburg, MMR 2011, 693 (694).

617 So zutr. *Schneider*, NStZ 1999, 388 (388) m. w. N.

618 Vgl. BGH-Ermittlungsrichter NStZ 2005, 278 (278); vgl. auch *Schneider*, NStZ 1999, 388 (388).

619 Vgl. insoweit *Schneider*, NStZ 1999, 388 (388) m. w. N.

nicht ausdrücklich geregelten – Begleitmaßnahme (= Sekundärmaßnahme) zunächst um eine Maßnahme handeln, welche mit der von der gesetzlichen Eingriffsbefugnis ausdrücklich gestatteten Primärmaßnahme *typischerweise verbunden* ist.[620]

Des Weiteren wird regelmäßig verlangt, dass Begleitmaßnahmen, bei denen Typizität mit dem Primäreingriff gegeben ist, als weiteres Kriterium auch dem *Verhältnismäßigkeitsgrundsatz* gerecht werden und deshalb neben der Eignung und Erforderlichkeit zur Erreichung des damit verfolgten Zwecks auch angemessen, also verhältnismäßig i. e. S. in Bezug auf den damit verbundenen Grundrechtseingriff sein müssen. Letzteres ist jedenfalls regelmäßig dann der Fall, wenn die Begleitmaßnahme nur verhältnismäßig geringfügig in die Rechte des betroffenen Nutzers eingreift.[621] Einer Entscheidung darüber, ob für die Annahme einer Annexkompetenz beide Kriterien kumulativ vorliegen müssen[622], oder ob auch das (alternative) Vorliegen eines der beiden Kriterien genügt[623], bedarf es an dieser Stelle nicht, soweit für die hier thematisierten Begleitmaßnahmen einer Quellen-TKÜ beide Kriterien erfüllt sein sollten.

1. Typizität

a) Typische Begleitmaßnahmen einer TKÜ?

Erste Voraussetzung für die Annahme einer Annexkompetenz zu § 100a I StPO für die Begleitmaßnahmen des heimlichen Installierens der Überwachungssoftware auf dem Zielsystem (Infiltration eines informationstechnischen Systems) sowie des heimlichen Deinstallierens der Software ist das Vorliegen von *Typizität* mit der gesetzlich zulässigen Primärmaßnahme des Überwachens und Aufzeichnens von Telekommunikation.

---

620 Vgl. LG Hamburg, MMR 2011, 693 (694); bereits BGH-Ermittlungsrichter NStZ 1998, 157 (157 f.); auch Meyer-Goßner – *Cierniak*, StPO, § 100f, Rn. 4 u. § 100a, Rn. 7a.

621 Vgl. insoweit LG Hamburg, MMR 2008, 423 (424 f.); i. E. auch LG Hamburg, MMR 2011, 693 (694), wobei die Kammer auch Ansatzpunkte dafür sieht, die *verhältnismäßig geringfügige Beeinträchtigung* als Kriterium für die Bejahung einer Annexkompetenz in Frage zu stellen, siehe hierzu auch 2. Teil B.III.2.c); vgl. zum Verhältnismäßigkeitskriterium bereits BGH-Ermittlungsrichter NStZ 1998, 157 (157 f.), der allerdings insoweit nicht von einem kumulativen, sondern von einem alternativen Verhältnis beider Kriterien („neben“) ausgeht, krit. AG Hamburg, CR 2010, 249 (250); krit. auch *Schneider*, NStZ 1999, 388 (389); vgl. zum Kriterium des Verhältnismäßigkeitsgrundsatzes auch BGH NJW 2001, 1658 (1659).

622 Hierzu vertiefend AG Hamburg, CR 2010, 249 (250).

623 Vgl. insoweit BGH-Ermittlungsrichter NStZ 1998, 157 (157 f.); krit. *Schneider*, NStZ 1999, 388 (389).

Um dem Grundsatz des Vorbehalts des Gesetzes aus Art. 20 III GG[624] und den hieraus von der Rspr. des BVerfG entwickelten Grundsätzen der Wesentlichkeitstheorie[625] gerecht zu werden, wird generell unter das Kriterium der Typizität in Bezug auf die Beurteilung des Vorliegens von Annexkompetenzen die Voraussetzung gefasst, dass eine die gesetzlich ausdrücklich geregelte Primärmaßnahme ergänzende Begleitmaßnahme typischerweise und damit durch Sachzusammenhang[626] mit dem primären Eingriff in Verbindung stehen muss, da nur dann davon ausgegangen werden kann, dass der Gesetzgeber die gesetzlich nicht ausdrücklich geregelte Begleitmaßnahme bei der abstrakten Erfassung der mit der geschaffenen Norm verbundenen Zielvorstellung von der gesetzlichen Regelung der Primärmaßnahme mit umfasst wissen wollte, zumindest in Form von „sachgedanklichem Mitbewusstsein" jedenfalls billigend in Betracht gezogen hat.[627]

Das Vorliegen von Typizität für den die eigentliche Überwachung und Aufzeichnung der Telekommunikation begleitenden Eingriff der Infiltration des Zielsystems wird in Rspr. und Literatur zum Teil bezweifelt und deshalb das Vorliegen einer Annexkompetenz zu § 100a StPO als Rechtsgrundlage für den Eingriff verneint. So vertritt das *AG Hamburg* – insoweit in Einklang mit einer früheren Entscheidung des LG Hamburg[628] – im Rahmen seines Beschlusses vom 28.08.2009[629] die Auffassung, dass „das Typizitätskriterium […] nicht erfüllt [ist], wenn zur Umsetzung einer Maßnahme der Telekommunikationsüberwachung das Infiltrieren eines informationstechnischen Systems des Beschuldigten erfolgen soll"[630]. Denn Maßstab der Ty-

---

624 Grundlegend BVerfG NJW 1976, 34 (34 f.).

625 Vgl. BVerfG NJW 1998, 2515; BVerfG NJW 1979, 359; BVerfG NJW 1978, 807; BVerfG NJW 1972, 1504.

626 Vgl. *Schneider*, NStZ 1999, 388 (388) m. w. N.

627 Vgl. LG Hamburg, MMR 2011, 693 (694); insoweit auch AG Hamburg, CR 2010, 249 (250); BGH Ermittlungsrichter NStZ 1998, 157 spricht insofern von „konkludent erteilten Ermächtigungen" (157).

628 Vgl. insoweit noch LG Hamburg, 29. Große Strafkammer, Beschluss vom 01.10.2007, MMR 2008, 423 (425), als eine der ersten zur Frage der Zulässigkeit von Quellen-TKÜ-Maßnahmen veröffentlichten Entscheidungen.

629 AG Hamburg, CR 2010, 249, speziell zur Frage des Zugriffs mittels Überwachungssoftware im Zusammenhang mit der Nutzung eines Anonymisierungsdienstes, wobei diesbezüglich zu Recht bezweifelt wird, ob in solchen Fällen, also zur bloßen Ermöglichung der Feststellung einer dynamischen IP-Adresse als Verkehrsdatum vor deren Anonymisierung, überhaupt ein Zugriff auf Daten aus einem laufenden Telekommunikationsvorgang vorliegt und ein Fall der *Quellen-TKÜ* überhaupt gegeben ist, vgl. hierzu BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 107c und *Spoenle*, jurisPR-ITR 6/2010 Anm. 5; im Rahmen seiner Entscheidung nimmt das AG aber in weiten Teilen auch zu Fragen der Quellen-TKÜ zum Zwecke der Überwachung von verschlüsselter Kommunikation über das Internet Stellung.

630 AG Hamburg, CR 2010, 249 (251).

pizität müsse „regelmäßig die gesamte Breite der Anwendungsmöglichkeiten der den Primäreingriff rechtfertigenden Norm sein“[631]. Nur „wenn für (nahezu) alle Anwendungsfälle eines Primäreingriffs eine bestimmte Vorfeld- oder Begleitmaßnahme notwendig oder typisch ist“[632] könne „sicher davon ausgegangen werden, dass die Anwendung derselben durch den Gesetzgeber gebilligt ist“[633]. Eine „Prüfung der Typizität am konkreten Einzelfall“[634] sei „dagegen unzulässig“[635]. Die Infiltration stelle daher schon auf Grund dieser Bedingung „keine typische Begleitmaßnahme“[636] dar, da „Telekommunikation […] auf vielfältige Weise überwacht und aufgezeichnet werden [kann]“[637] und „die Infiltration […] hierzu regelmäßig nicht notwendig [ist]“[638], weil „im Regelfall […] die zu überwachenden Daten vom Telekommunikationsdienstleister zur Verfügung gestellt [werden]“[639]. Zwar könne dennoch „im Einzelfall eine Verengung des Maßstabs für die Prüfung der Typizität auf Fallgruppen angezeigt sein“, was voraussetze, „dass Anhaltspunkte dafür bestehen, dass die entsprechende Fallgruppe entweder ausdrücklich oder aufgrund ihrer herausragenden Bedeutung jedenfalls in Form sachgedanklichen Mitbewusstseins Berücksichtigung bei der Entscheidungsfindung im parlamentarischen Gesetzgebungsverfahren gefunden hat“[640]. Dies liege hier nach Auffassung des AG Hamburg jedoch nicht vor, da „der Gesetzgeber […] die […] Fälle verschlüsselter Kommunikation, z. B. bei bestimmten Formen computergestützter Telefonie […] nicht gesehen [hat]“[641], weshalb „gerade nicht von einem sachgedanklichen Mitbewusstsein der Notwendigkeit von Infiltrationsmaßnahmen zur Vorbereitung einer Telekommunikationsüberwachung ausgegangen werden [kann]“[642].

In Abkehr von dieser Sichtweise geht nunmehr die *8. Große Strafkammer des LG Hamburg* in ihrer Entscheidung vom 13.09.2010[643] zusammen mit einem wesentlichen Teil in Rspr. und Schrifttum[644] davon aus, dass in den

---

631 AG Hamburg, CR 2010, 249 (250).
632 AG Hamburg, CR 2010, 249 (250).
633 AG Hamburg, CR 2010, 249 (250).
634 AG Hamburg, CR 2010, 249 (250).
635 AG Hamburg, CR 2010, 249 (250).
636 AG Hamburg, CR 2010, 249 (251).
637 AG Hamburg, CR 2010, 249 (251).
638 AG Hamburg, CR 2010, 249 (251); so i. E. auch *Sankol*, CR 2008, 13 (17).
639 AG Hamburg, CR 2010, 249 (251).
640 AG Hamburg, CR 2010, 249 (251).
641 AG Hamburg, CR 2010, 249 (251).
642 AG Hamburg, CR 2010, 249 (251).
643 LG Hamburg, MMR 2011, 693.
644 Vgl. BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 107f; *Bär*, TK-Überwachung, § 100a StPO, Rn. 33; AG Bayreuth, MMR 2010, 266 (267); LG Landshut, MMR

Fällen der Quellen-TKÜ die Voraussetzung der Typizität der heimlichen Infiltration mit dem Primäreingriff erfüllt sei. Im Rahmen von Maßnahmen nach §§ 100a, 100b StPO sei es wegen des „umfassenden und technisch vielfältigen Charakters der überwachungsfähigen Telekommunikationsvorgänge“[645] für die Annahme von Typizität mit der Primärmaßnahme ausreichend, wenn die Überwachung und Aufzeichnung „in einem wesentlichen Teil des Anwendungsbereiches der Vorschrift ohne das heimliche Einspielen eines Computerprogramms in das informationstechnische System des Überwachten undurchführbar wäre“[646]. Dies ist nach Auffassung der Kammer für den Zugriff auf verschlüsselt übermittelte Internettelefonie, welche einer herkömmlichen Überwachung auf dem Übermittlungswege nicht zugänglich ist, zu bejahen. Denn die „‚Internet-Telefonie‘ in ihren verschiedenen technischen Ausformungen“[647] stelle „eine wesentliche Fallgruppe innerhalb des Anwendungsbereiches des § 100a StPO“[648] dar, welche insbesondere auf Grund der starken Verbreitung und des preisgünstigen Erwerbs des hierfür notwendigen technischen Equipments wie auch der i. d. R. kostenlosen Verfüg- und Nutzbarkeit der für die Internettelefonie erforderlichen Software seit Jahren in der Praxis häufig vorkomme.[649] Gerade mit Blick auf „die Verwendung des inhaltlich weitreichenden Begriffs der ‚Telekommunikation‘ in § 100a Abs. 1 StPO“[650] seien keine Anhaltspunkte dafür erkennbar, „dass der Gesetzgeber diesen Anwendungsbereich [Internettelefonie, Anm. d. Verf.] trotz seiner erheblichen Verbreitung übersehen haben könnte“[651], wie dies teilweise von der Gegenansicht[652] geschlussfolgert wird.[653]

Zur Klärung der strittigen Frage, ob im Falle der Quellen-TKÜ das heimliche Installieren (wie auch das Deinstallieren) der Überwachungssoftware ein die Typizitätsanforderungen erfüllendes Vorbereitungs- bzw. Nachbereitungshandeln darstellt, empfiehlt sich ein Vergleich mit anerkannten Begleitmaßnahmen anderer strafprozessualer Befugnisnormen.

2011, 690 (691); vgl. in diesem Zusammenhang auch *Kudlich*, JA 2010, 310 (312), der unter Bezugnahme auf die Entscheidung des AG Hamburg zum Vorliegen der Voraussetzungen einer Annexkompetenz zu Recht darauf hinweist, dass „dieses restriktive Auslegungsergebnis nicht als das einzig vertretbare [erscheint]“ (312); *ders*. auch GA 2011, 193 (207).

645 LG Hamburg, MMR 2011, 693 (694).

646 LG Hamburg, MMR 2011, 693 (694).

647 LG Hamburg, MMR 2011, 693 (694).

648 LG Hamburg, MMR 2011, 693 (694).

649 So LG Hamburg, MMR 2011, 693 (694).

650 LG Hamburg, MMR 2011, 693 (694).

651 LG Hamburg, MMR 2011, 693 (694).

652 So bspw. AG Hamburg, CR 2010, 249 (251).

653 Vgl. LG Hamburg, MMR 2011, 693 (694 f.).

b) Vergleich mit Begleitmaßnahmen anderer Befugnisnormen

Zur Feststellung der Typizität der heimlichen Installation einer Überwachungssoftware als vorbereitende Begleitmaßnahme für die Umsetzung der späteren TKÜ-Maßnahme ermöglicht der Vergleich zu anderen heimlichen Ermittlungsmaßnahmen und deren typischen Begleitmaßnahmen eine nähere Einordnung. Hierfür lässt sich insbesondere auf die *verdeckte Installation von GPS-Empfängern* an Kraftfahrzeugen zur späteren Standortbestimmung des Zielfahrzeugs durch GPS im Rahmen von Maßnahmen nach § 100h I S. 1 Nr. 2 StPO („Einsatz sonstiger technischer Mittel") sowie auf das *heimliche Anbringen von Wanzen* als Abhörgeräte in Wohnräumen zur Ermöglichung anschließender Maßnahmen der akustischer Wohnraumüberwachung nach § 100c I StPO abstellen[654]:

- Ein Vergleich lässt sich hierbei zunächst zu *Maßnahmen der akustischen Überwachung außerhalb von Wohnungen nach § 100f StPO* und deren Begleitmaßnahmen ziehen. Ein Abstellen auf die Regelungen zu § 100f StPO ist auch aus dem Grunde naheliegend, da Maßnahmen der akustischen Überwachung außerhalb von Wohnungen hinsichtlich ihrer Eingriffstiefe mit Überwachungsmaßnahmen nach §§ 100a, 100b StPO vergleichbar sind und vom Gesetzgeber deshalb auch in Bezug auf die Eingriffsvoraussetzungen weitgehend angeglichen wurden[655].

  Im Rahmen der Beurteilung des Vorliegens von Annexkompetenzen in Bezug auf die Zulässigkeit von Begleitmaßnahmen für das Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes in einem PKW[656] hat der *BGH-Ermittlungsrichter* im Jahre 1997 – noch zur früheren Rechtsgrundlage des *§ 100c I Nr. 2 StPO a. F.* (dessen Regelungsgegenstand nunmehr in § 100f StPO zu finden ist) entschieden, dass das *heimliche Öffnen eines PKWs* zum Zwecke des Einbaus der für die Überwachungsmaßnahme notwendigen technischen Vorrichtungen rechtmäßig sei und auf eine im Rahmen der Normierung des *§ 100c I Nr. 2 StPO a. F.* durch den Gesetzgeber konkludent erteilte Ermächtigung gestützt werden

---

654 Vgl. auch *Bär*, MMR 2008, 215 (219); *Gercke*/*Brunst*, Internetstrafrecht, Kap. 5, S. 350, Rn. 895, Fn. 377.

655 Vgl. BT-Drs. 16/5846, S. 49; vgl. auch Meyer-Goßner – *Cierniak*, StPO, § 100f, Rn. 2; ebenso *Bär*, TK-Überwachung, § 100f StPO, Rn. 1; siehe hierzu auch 1. Teil A.II.2.c).

656 Welcher naturgemäß der Fortbewegung des Menschen dient, nicht seiner „Behausung", seinem Aufenthalt und seinem Wirken und deshalb nicht dem Begriff der „Wohnung" und dem Schutzbereich des Art. 13 I GG unterfällt, vgl. BGH-Ermittlungsrichter NStZ 1998, 157 (157) m. w. N.; hierzu auch Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 10.

könne. Nicht hiervon umfasst sei hingegen das vorübergehende heimliche Verbringen des PKW in eine Werkstatt.[657]

Die Einordnung des heimlichen Öffnens des PKW als zulässige Begleitmaßnahme erfolgte hier allerdings nicht auf Grund von *Typizität* – deren Vorliegen der BGH-Ermittlungsrichter sowohl für das Öffnen als auch für das Verbringen des Fahrzeugs in eine Werkstatt im vorliegenden Beschluss verneinte – sondern auf Grund eines mit dem heimlichen Öffnen (an Ort und Stelle) verbundenen nur *geringfügigen Eingriffs* in den Rechtskreis des Betroffenen; insofern ging der BGH-Ermittlungsrichter in seiner Entscheidung von einem alternativen Verhältnis beider Kriterien aus.[658] Typizität sei dessen Auffassung nach in diesem Falle weder für das heimliche Öffnen eines PKW noch für dessen heimliches Verbringen in eine Werkstatt gegeben gewesen, da ein Abhören nach *§ 100c I Nr. 2 StPO a. F.* (§ 100f I StPO n. F.) nicht typischerweise derartige Vorbereitungsmaßnahmen erfordere.[659] Denn abgehört werden könne „auf vielfältige Weise, beispielsweise durch Richtmikrophone Gespräche auf Wegen, Straßen und Plätzen, durch sogenannte ‚Wanzen' auf Parkbänken usw."[660], weshalb „das Abhören von Gesprächen in einem Pkw […] nur eine von mehreren Möglichkeiten"[661] sei. Die Eingriffsnorm „‚liefe nicht leer', wenn mangels zulässiger Vorbereitungsmaßnahmen das Abhören von im Pkw geführten Gesprächen ausscheiden müßte"[662].

Diese Sichtweise in Bezug auf das Kriterium der *Typizität* ist indes nicht zwingend. So führt das *AG Hamburg* „für die häufig diskutierte Frage, ob § 100f StPO […] als Begleitmaßnahme auch das Öffnen eines Fahrzeugs zum Anbringen der Abhöreinrichtung umfasst"[663] in Bezug auf eine Eingrenzung des Prüfungsmaßstabs der Typizität auf entsprechende Fallgruppen abweichend hierzu aus, dass „aufgrund der Allgegenwärtigkeit von Kraftfahrzeugen, ihrer herausgehobenen Bedeutung bei der Alltagsgestaltung und der daraus folgenden Bedeutung für strafrechtliche Ermittlungsverfahren, davon ausgegangen werden [muss], dass der Gesetzgeber den Einsatz technischer Abhöranlagen auch in Fahrzeugen hat

---

657 Vgl. BGH-Ermittlungsrichter NStZ 1998, 157 (157 f.); anders in Bezug auf das kurzzeitige Verbringen in eine Werkstatt hingegen BGH NJW 2001, 1658 (1659), hier zu § 100c I Nr. 1 lit. b StPO a. F. (§ 100h I S. 1 Nr. 2 StPO n. F.); a. A. auch *Schneider*, NStZ 1999, 388 (389 f.); Meyer-Goßner – *Cierniak*, StPO, § 100f, Rn. 4.

658 Vgl. BGH-Ermittlungsrichter NStZ 1998, 157 (158) („neben"); krit. AG Hamburg, CR 2010, 249 (250).

659 So BGH-Ermittlungsrichter NStZ 1998, 157 (157).

660 BGH-Ermittlungsrichter NStZ 1998, 157 (157).

661 BGH-Ermittlungsrichter NStZ 1998, 157 (157).

662 BGH-Ermittlungsrichter NStZ 1998, 157 (157).

663 AG Hamburg, CR 2010, 249 (251).

erfassen wollen“[664]. Da „zum Einbau solcher Anlagen in Fahrzeuge […] es typischerweise notwendig [ist], das Fahrzeug zu öffnen“[665], sei das Öffnen des betreffenden Fahrzeugs als Begleitmaßnahme zu § 100f StPO erlaubt.[666]

Auch von Seiten des Schrifttums erfährt die Sichtweise des BGH-Ermittlungsrichters zur Typizität der genannten Begleitmaßnahmen Kritik. So überzeuge einerseits nicht das dieser Entscheidung zugrunde gelegte Verständnis eines alternativen Verhältnisses von Typizitätskriterium und Verhältnismäßigkeitskriterium, als ein solcher Ansatz darauf hinausliefe, „den Verhältnismäßigkeitsgrundsatz zu einer Ermächtigungsgrundlage für grundrechtsbeeinträchtigende Maßnahmen hochzustilisieren“[667]. Da der Verhältnismäßigkeitsgrundsatz aber „seinem Regelungsinhalt nach keine staatlichen Eingriffsbefugnisse [schafft], sondern […] lediglich anderwärts legitimiertes staatliches Vorgehen [begrenzt]“[668], sei an der Voraussetzung des kumulativen Vorliegens der Kriterien festzuhalten, nämlich „dass Begleitmaßnahmen zu strafprozessualen Grundrechtseingriffen nur vorgenommen werden dürfen, wenn sie mit diesen typischerweise verbunden sind und zusätzlich den Betroffenen nicht übermäßig stark belasten“[669].

Zum anderen könne entgegen den Schlussfolgerungen des BGH-Ermittlungsrichters auch das Vorliegen von *Typizität* in diesen Fällen angenommen werden. Mit dem Abstellen auf das gesamte Spektrum aller nach *§ 100c I Nr. 2 StPO a. F.* (§ 100f I StPO n. F.) denkbaren Abhörmaßnahmen als Maßstab für die Beurteilung des Vorliegens von Typizität ziehe der BGH-Ermittlungsrichter mit dem Ziel der Festschreibung möglichst einzelfallübergreifender Charakteristika den Typizitätsmaßstab zu eng[670], da „das damit angesteuerte Abstraktionsniveau […] angesichts der Vielfalt der einschlägigen Sachverhalte viel zu hoch angesetzt [ist], um operationabel zu sein“[671]. Deshalb sei in Bezug auf die Frage des Typizitätsmaßstabs ein Ansatz rechtlich handhabbarer, der „die Komplexität der […] erfassten Lebenssachverhalte durch Bildung von Fallgruppen reduziert“[672]. So sei es – insofern unter dogmatischer Weiterentwicklung der grundsätzlichen Feststellungen des BGH-Ermittlungsrichters zu Annexkompetenzen – mit

664 AG Hamburg, CR 2010, 249 (251).
665 AG Hamburg, CR 2010, 249 (251).
666 So AG Hamburg, CR 2010, 249 (251).
667 *Schneider*, NStZ 1999, 388 (389).
668 *Schneider*, NStZ 1999, 388 (389).
669 *Schneider*, NStZ 1999, 388 (389).
670 So *Schneider*, NStZ 1999, 388 (389).
671 *Schneider*, NStZ 1999, 388 (389).
672 *Schneider*, NStZ 1999, 388 (389).

Blick auf die „herausgehobene […] Bedeutung von Kraftfahrzeugen im Lebensalltag“[673] und die „daraus resultierende […] kriminaltaktische […] Notwendigkeit“[674] der Überwachbarkeit darin geführter Gespräche angezeigt, hierin eine „separate normative Fallgruppe“[675] zu sehen, womit es für die Beurteilung der Typizität von Begleitmaßnahmen darauf ankomme, was die Ermittlungsbehörde „normalerweise unternehmen muß, um die im Wagen geführten Gespräche abhören und aufzeichnen zu können“[676]. Anhand dieses Maßstabes erweise sich sowohl das Öffnen des KFZs als auch bspw. der Anschluss an die KFZ-eigene Stromversorgung als unerlässlich, um die Abhörvorrichtung im Fahrzeug zu installieren und – regelmäßig über einen längeren Zeitraum – in Betrieb halten zu können.[677] Aber auch für das kurzzeitige *Verbringen des Fahrzeugs in eine Werkstatt* ließe sich demgemäß das Vorliegen einer typischerweise mit dem Primäreingriff verbundenen Begleitmaßnahme bejahen, da „zur Gewährleistung der Energieversorgung […] handwerkliche Maßnahmen erforderlich [sind], die sachgerecht nicht am Abstellplatz des Fahrzeuges, sondern nur in einer Werkstatt durchgeführt werden können“[678].

- Des Weiteren lässt sich auch auf die von einer anerkannten Annexkompetenz gedeckten Begleitmaßnahmen in Zusammenhang mit dem *Einsatz sonstiger technischer Mittel gemäß § 100h I S. 1 Nr. 2 StPO* abstellen.

  So hat der BGH im Rahmen einer Entscheidung noch zum früheren (nunmehr in § 100h I S. 1 Nr. 2 StPO n. F. geregelten) *§ 100c I Nr. 1 lit. b StPO a. F.* festgestellt, dass bei einer Maßnahme zum Zwecke der Beweisgewinnung unter Verwendung des satellitengestützten GPS-Navigationssystems („Global Positioning System“) zur Ortung und Verfolgung der Bewegungen eines PKWs die mit „dem Einbau des Empfängers und der Gewinnung der Daten durchgeführten Maßnahmen“ wie insbesondere das *heimliche Öffnen des Kraftfahrzeugs* sowie die *Benutzung dessen Fahrzeugbatterie* als Stromquelle „zur Verwendung der ‚GPS‘-Technik [gehören] und […] daher ebenfalls gem. § 100c I Nr. 1 lit.b StPO rechtmäßig [sind]“[679]. Unter Beachtung des Verhältnismäßigkeitsgrundsatzes gestatte

673 *Schneider*, NStZ 1999, 388 (389).

674 *Schneider*, NStZ 1999, 388 (389).

675 *Schneider*, NStZ 1999, 388 (389).

676 *Schneider*, NStZ 1999, 388 (389).

677 So *Schneider*, NStZ 1999, 388 (389).

678 *Schneider*, NStZ 1999, 388 (389); so i. E. auch BGH, NJW 2001, 1658 (1659) zu Maßnahmen nach § 100c I Nr. 1 lit. b StPO a. F. (§ 100h I S. 1 Nr. 2 StPO n. F.); auch Meyer-Goßner – *Cierniak*, StPO, § 100f, Rn. 4; a. A. noch BGH-Ermittlungsrichter NStZ 1998, 157 (157 f.).

679 BGH NJW 2001, 1658 (1659).

die Vorschrift „im Wege der Annexkompetenz […] die Vornahme der für den Einsatz des technischen Mittels notwendigen Begleitmaßnahmen“[680], wozu im Einzelfall auch die *kurzzeitige Verbringung des KFZs in eine Werkstatt* zum Zwecke des Anbringens des GPS-Empfängers, welcher den ermittelten Standort überträgt, gehören kann.[681]

Dies trifft insoweit auch auf Zustimmung in der Literatur, als „der Ein- und Ausbau von GPS-Empfängern und Sendern […] in Autos […] bei dem heutigen Stand der Technik der Fahrzeugsicherung idR die heimliche Verbringung des Fahrzeuges in eine Werkstatt [erfordert]“[682]. Solche für den Einsatz des technischen Mittels notwendigen Begleitmaßnahmen wie auch die mit dem heimlichen Ein- und Ausbau *verbundenen Täuschungen* des Betroffenen seien von einer Annexkompetenz zu § 100h I S. 1 Nr. 2 StPO jedenfalls dann gedeckt, wenn Verhältnismäßigkeit gegeben ist.[683]

- Hinsichtlich der Beurteilung des Vorliegens von *Typizität* sind aber auch die Vorschriften der *akustischen Wohnraumüberwachung gemäß §§ 100c ff. StPO* einem Vergleich zugänglich.

  Hier stellt nach vorherrschender Auffassung das im Regelfall erfolgende *heimliche Eindringen* von Ermittlungspersonen in die überwachten Wohnräume zum Zwecke des dortigen *Anbringens* der technischen Vorrichtungen (v. a. Wanzen) eine mit der in § 100c I StPO gesetzlich geregelten *Überwachung des nicht öffentlich gesprochenen Wortes in Wohnräumen* typischerweise verbundene Begleitmaßnahme dar, deren Zulässigkeit der Gesetzgeber – auch wenn es an einer ausdrücklichen Befugnis in den §§ 100c ff. StPO hierfür fehlt – in Betracht gezogen und vorausgesetzt hat[684], da eine Maßnahme der Wohnraumüberwachung auf anderem Wege kaum bzw. gar nicht technisch realisiert werden könnte.[685]

Die *vergleichende Heranziehung* der in Rspr. und Lit. anerkannten typischen Begleitmaßnahmen heimlicher strafprozessualer Ermittlungsmaßnahmen lässt indes den Schluss darauf zu, dass auch für die Frage der heimlichen Installation einer Überwachungssoftware (Infiltration des Zielsystems) wie auch heimlichen Deinstallation der Software nach Beendigung einer Maßnahme zum Überwachen und Aufzeichnen von (verschlüsselt übermit-

---

680 BGH NJW 2001, 1658 (1659).

681 So BGH NJW 2001, 1658 (1659); vgl. auch KK – *Nack*, StPO, § 100h, Rn. 9.

682 KK – *Nack*, StPO, § 100h, Rn. 9.

683 So KK – *Nack*, StPO, § 100h, Rn. 9; vgl. auch *Bär*, TK-Überwachung, § 100h StPO, Rn. 8.

684 Vgl. BT-Drs. 13/8651, S. 13.

685 Vgl. LG Hamburg, MMR 2011, 693 (694); ebenso Meyer-Goßner – *Cierniak*, StPO, § 100c, Rn. 7 m. w. N.; auch *Bär*, TK-Überwachung, § 100c StPO, Rn. 8 m. w. N.

telter) VoIP-Kommunikation, hier durch Zugriff auf dem dafür genutzten informationstechnischen System („an der Quelle"), das Kriterium der *Typizität* erfüllt ist:

Angesichts der Vielfältigkeit und Vielgestaltigkeit möglicher Lebenssachverhalte, die einer strafprozessualen Eingriffsbefugnis mitunter zugrunde liegen können, ist die Fassung einer umfassenden, allen denkbaren Konstellationen und Erfordernissen – insbesondere bezüglich Vorbereitung und Durchführung der von der Gesetzesnorm ausdrücklich gestatteten Eingriffe – genügenden gesetzlichen Regelung oftmals kaum möglich.[686] Dies gilt gerade für eine Befugnisnorm wie in §§ 100a, 100b StPO zur Überwachung und Aufzeichnung von Telekommunikation, welche in besonderer Weise von den technischen Entwicklungen und dem Kommunikationsverhalten der Nutzer bestimmt und zugleich auch abhängig ist. Aus diesem Grunde hat der Gesetzgeber Regelung des § 100a I StPO bewusst entwicklungsoffen und technologieneutral formuliert, um auch neuartige, zum Zeitpunkt der Normierung noch nicht bekannte technische Kommunikationsformen, in deren Anwendungsbereich mit einzuschließen.[687]

Dass der Gesetzgeber den sich gegenwärtig wie auch in Zukunft immer stärker etablierenden Bereich der Kommunikation via Internetprotokoll über informationstechnische System beim Einfügen der §§ 100a, 100b StPO in die Strafprozessordnung im Jahre 1968[688] zwar noch nicht konkret bzw. bei Ersetzung des Begriffs *Fernmeldeverkehr* durch *Telekommunikation* im Jahre 1997[689] noch nicht in seinen ganzen technischen Einzelheiten vorhergesehen haben dürfte, aber doch eine solche moderne technische Kommunikationsform nicht von dem Anwendungsbereich der §§ 100a, 100b StPO ohne weiteres ausgeschlossen wissen wollte, ist – gerade mit Blick auf eine konsequente Berücksichtigung der entwicklungsoffenen und technologieneutralen Zielsetzung der Vorschrift und der hierdurch vom Gesetzgeber getroffenen Wert- und zum Ausdruck gebrachten Willensentscheidung – naheliegend.

Als *Maßstab für die Beurteilung der Typizität* von Begleitmaßnahmen zur Primärmaßnahme einer Quellen-TKÜ ist es deshalb auch nicht erforderlich,

---

686 Vgl. BGH-Ermittlungsrichter NStZ 2005, 278 (278).

687 So hat der Gesetzgeber insbesondere durch die Ersetzung des Begriffs des „Fernmeldeverkehrs" durch den inhaltlich weitreichenden Begriff der „Telekommunikation" im Jahr 1997 (BGBl. I S. 3108) gezielt eine weite, gegenüber der technischen Entwicklung offene Fassung gewählt, vgl. *Kudlich*, JuS 2001, 1165 (1166) m. w. N.; ebenso LG Hamburg, MMR 2011, 693 (694); vgl. auch BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 2 u. 6.

688 Mit Gesetz vom 13.08.1968 (BGBl. I S. 949).

689 Mit Gesetz vom 17.12.1997 (BGBl. I S. 3108).

dass das heimliche Installieren (Infiltration des Zielsystem) und Deinstallieren der Überwachungssoftware (vgl. unten) mit der gesamte Bandbreite der Anwendungsmöglichkeiten des § 100a I StPO[690] typischerweise verbunden sein muss.

Angesichts des bewusst entwicklungsoffenen und technologieneutralen Charakters des § 100a I StPO, der mit seinem Anwendungsbereich vielfältige, technisch unterschiedlich ablaufende – und davon bedingt auch an die Art und Weise der Überwachungsumsetzung unterschiedliche Anforderungen stellende – Kommunikationsformen erfasst, genügt es vielmehr, wenn die Begleitmaßnahmen mit einem *wesentlichen Teil der Anwendungsmöglichkeiten* des § 100a I StPO typischerweise verbunden ist.[691] Wie dies angesichts der Komplexität möglicher Sachverhalte aus Gründen der rechtlichen Handhabbarkeit für Begleiteingriffe von Maßnahmen der akustischen Überwachung außerhalb der Wohnung nach § 100f I StPO zu Recht vertreten wird[692], ist auch in Bezug auf den Anwendungsbereich der Telekommunikationsüberwachung das Abstellen auf *normative Fallgruppen*[693] als Typizitätsmaßstab angezeigt, welche einen wesentlichen Teil innerhalb des Anwendungsbereichs darstellen. Der Aspekt der „Wesentlichkeit" ist hierbei nicht allein an der Relation zur Gesamtzahl der geführten Telekommunikation in der Praxis festzumachen, sondern vielmehr danach zu beurteilen, ob der relevanten Fallgruppe generell eine herausgehobene, mithin nicht nur nebensächliche, Bedeutung innerhalb des Anwendungsbereichs des § 100a I StPO zukommt, die sich auf das Gelingen strafrechtlicher Ermittlungsverfahren auswirken kann und damit insbesondere auch kriminalistisch ausweisbar ist[694]. Ebenso wie für die spezielle Fallgruppe des Abhörens und Aufzeichnens des nichtöffentlich gesprochenen Wortes in PKWs in Bezug auf Maßnahmen nach § 100f I StPO[695], lässt sich dies auch für die Überwachung und Aufzeichnung von Internettelefonie in Bezug auf § 100a I StPO bejahen. Auf Grund der zunehmenden Etablierung der Internettelefo-

---

690 Wie dies bspw. AG Hamburg, CR 2010, 249 (250) vertritt.

691 Vgl. zutr. LG Hamburg, MMR 2011, 693 (694).

692 Vgl. *Schneider*, NStZ 1999, 388 (389); so i. E. aber auch BGH NJW 2001, 1658 (1659) zur Verwendung der GPS-Technik zur Positionsbestimmung eines PKW auf Grundlage des § 100c I Nr. 1 lit. b StPO a. F. (§ 100h I S. 1 Nr. 2 StPO n. F.), wonach für die Frage der Typizität („gehören zur") des Öffnens des PKWs zum Einbau des Empfängers, des Benutzens der PKW-Batterie zur Stromversorgung sowie hierfür ggf. des kurzzeitigen Verbringens in eine Werkstatt nicht auf alle Anwendungsfälle der Vorschrift abgestellt wird, sondern insoweit auf die spezifische Verwendung von GPS-Technik.

693 Vgl. *Schneider*, NStZ 1999, 388 (389).

694 Vgl. hierzu auch *Schneider*, NStZ 1999, 388 (389 f.).

695 Vgl. *Schneider*, NStZ 1999, 388 (389), wonach Kraftfahrzeugen im Lebensalltag eine herausgehobene Bedeutung zukommt.

nie, welche eine moderne Form von Telekommunikation i. S. d. § 100a I StPO darstellt[696], der kontinuierlich steigenden Nutzungszahlen[697], ihrer Bedeutung insbesondere für die Individualkommunikation[698] sowie der maßgeblichen Beeinflussung des Kommunikationsverhaltens des Einzelnen durch die (i.d.R) kostenlos und bei Vorhandensein entsprechenden technischen Equipments unter den Kommunikationsteilnehmern weltweit nutz- und abrufbaren Dienste, stellt die Internettelefonie eine wesentliche – d. h. nicht nur nebensächliche – Fallgruppe innerhalb des Anwendungsbereichs des § 100a I StPO dar[699].

Die Zulässigkeit der Begleitmaßnahmen einer Quellen-TKÜ bemisst sich anhand dieser Sichtweise folglich daran, ob das heimliche Installieren der Überwachungssoftware in das Zielsystem (wie auch deren heimliches Entfernen nach Beendigung der Maßnahme) ein typischerweise, mithin kraft Natur der Sache mit der Überwachung und Aufzeichnung von Internettelefonie verbundener Eingriff ist, und nicht daran, ob diese Maßnahmen für sämtliche Anwendungsfälle des § 100a I StPO typische Begleiteingriffe darstellen:

Auf Grund der mit IP-basierter Kommunikation verbundenen technischen Möglichkeiten – insbesondere auch Schutzmöglichkeiten – läuft der Datenaustausch bei dieser Telekommunikationsform häufig verschlüsselt ab. Dies lässt die Möglichkeit eines Abgreifens der Daten während der Übermittlung durch den Netzbetreiber entfallen, da hierüber nur Datenkopien in codierter Form gewonnen würden. Mit Blick auf die sich daraus ergebende (technische) Notwendigkeit des Abgreifens des laufenden IP-Kommunikationsvorgangs auf dem hierfür genutzten informationstechnischen System (i. d. R. Computer), also „an der Quelle", bevor die Daten ver- bzw. nachdem die Daten entschlüsselt sind, stellen die begleitenden Maßnahmen einer Quellen-TKÜ in Bezug auf die von § 100a I StPO gestattete Primärmaßnahme, also

---

696 Vgl. statt vieler BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 7 u. 31; Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 7a.

697 So benutzten laut Statistischem Bundesamt im Berichtszeitraum 1. Quartal 2011 bereits 22 Prozent der Internetnutzer in Deutschland das Internet zum Telefonieren und Führen von Video-/Telefonaten, vgl. Statistisches Bundesamt, Wirtschaftsrechnungen 2011, Internetaktivitäten zu privaten Zwecken in den letzten drei Monaten – Telefonieren/Videotelefonate (mit Webcam), S. 27, abrufbar unter https://www.destatis.de/DE/Publikationen/Thematisch/EinkommenKonsumLebensbedingungen/PrivateHaushalte/PrivateHaushalteIKT2150400117004.pdf?__blob=publicationFile (zuletzt aufgerufen 15.06.2012).

698 So ermöglicht IP-basierte Telefonie nicht nur Sprachtelefonie, sondern stellt – anders als die Festnetztelefonie – den technischen Standard für Videotelefonie dar; auch in Bezug auf Auslandstelefonate kommt der Internettelefonie auf Grund ihrer regelmäßigen Kostenfreiheit eine herausgehobene Bedeutung zu.

699 So auch zutr. LG Hamburg, MMR 2011, 693 (694).

das Überwachen und Aufzeichnen von (IP-)Telekommunikation – wofür nach ausdrücklichem Dafürhalten des Gesetzgebers technische Mittel eingesetzt werden dürfen[700] – typischerweise hiermit verbundene Eingriffe dar, für die anzunehmen ist, dass sie der Gesetzgeber – zumindest in Form von sachgedanklichem Mitbewusstsein – in Betracht gezogen und gebilligt hat. Die offene Formulierung des § 100a I StPO, wonach *Telekommunikation überwacht und aufgezeichnet werden darf*, legt hierbei nahe, dass der Gesetzgeber – gerade auch angesichts der Normierung einer Regelung wie der des § 100b II S. 2 Nr. 3 StPO, wonach in der gerichtlichen Anordnungsentscheidung die Art der Überwachung (auch die Art des technischen Zugriffs[701]) näher zu bestimmen ist[702] – an die jeweilige Telekommunikationsform angepasste technische Überwachungsmittel in Betracht gezogen und gebilligt hat, was zudem nicht ausschließt, dass hierfür auch am jeweiligen Endgerät angesetzt wird, welches ebenfalls technischer Anknüpfungspunkt einer TKÜ-Maßnahme sein kann[703] – zumal dieses nunmehr ausdrücklich in § 100b II S. 2 Nr. 2 StPO Berücksichtigung gefunden hat[704]. Etwas anderes ergibt sich auch nicht aus der Regelung des § 100b III StPO. Denn wie der Gesetzgeber ausdrücklich festgestellt hat, wird von dieser Vorschrift „eine Obliegenheit der Strafverfolgungsbehörden, Telekommunikationsüberwachungsmaßnahmen stets unter Mitwirkung eines Telekommunikationsdienstleisters durchzuführen, […] nicht begründet“[705]. Vielmehr ist in § 100a I StPO „eine nicht durch die Mitwirkung der Telekommunikationsdienstleister

---

700 Vgl. BT-Drs. 16/5846, S. 47; siehe auch 2. Teil A.II.5. und 3. Teil A.I.1.a)bb).

701 Vgl. BT-Drs. 16/5846, S. 47.

702 Vgl. auch BT-Drs. 16/5846, S. 47.

703 Vgl. BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 8.

704 Vgl. *Bär*, TK-Überwachung, § 100a StPO, Rn. 32; hierauf weist auch *Kudlich*, GA 2011, 193 (207) hin; die Kritik von *Klesczewski,* ZStW 2011, 737 (743), wonach der Gesetzgeber mit dieser Vorschrift lediglich die Überwachung von Mobiltelefonen auch bei wechselnden SIM-Karten ermöglichen wollte, greift im Ergebnis nicht durch, da die Neuregelung ausweislich der Gesetzesbegründung (BT-Drs. 16/5846, S. 46) dieser Konstellation zwar „Rechnung [trägt]“ (S. 46), jedoch vom Gesetzgeber so (entwicklungs-)offen formuliert wurde, dass hiervon nicht automatisch auf einen Willen des Gesetzgebers zu schließen ist, andere Kommunikationstechniken, die unter besonderer Einbindung von Endgeräten in die jeweiligen Telekommunikationsvorgänge stattfinden, von dem Geltungsbereich der Vorschrift auszunehmen; auch schließt der offene Tatbestand des § 100a I StPO es gerade nicht aus, als technischen Anknüpfungspunkt der Überwachung auch das jeweilige Endgerät heranzuziehen.

705 BT-Drs. 16/5846, S. 47; so auch Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 7a, 8 sowie § 100b, Rn. 7; ebenso *Bär*, TK-Überwachung, § 100a StPO, Rn. 32; *ders*., MMR 2008, 215 (219); zust. *Gercke*/*Brunst*, Internetstrafrecht, Kap. 5, S. 350, Rn. 895, Fn. 377; a.A. SK – *Wolter*, StPO, § 100a, Rn. 20 u. § 100b, Rn. 19; *Sankol*, CR 2008, 13 (17); *Buermeyer*/*Bäcker*, HRRS 2009, 433 (440); ebenso noch LG Hamburg, MMR 2008, 423 (424); nunmehr zust. LG Hamburg, MMR 2011, 693 (696).

bedingte Befugnis, Telekommunikation zu überwachen und aufzuzeichnen“[706] enthalten. Die im Rahmen der Durchführung einer Quellen-TKÜ zum Zwecke des Abgreifens und Ausleitens der ausgetauschten Daten in unverschlüsseltem Zustand zum Einsatz kommende Überwachungssoftware stellt ein „technisches Mittel zur Datenerhebung“[707] dar, welches verständlicherweise nicht zur Überwachung verwendet werden kann, ohne im Rahmen einer Begleitmaßnahme vorher in das betreffende Zielsystem, über das die gegenständliche Telekommunikation geführt wird, eingebracht worden zu sein. Mithin gehört die Infiltration des zum Austausch von Kommunikationsdaten genutzten Systems *zur Verwendung* einer Überwachungssoftware als technisches Mittel zur Überwachung und Aufzeichnung von (verschlüsselt übermittelten) Internettelefonaten an der Quelle.

Eine *typische Verbundenheit* des Installierens der Überwachungssoftware auf dem Zielsystem mit der anschließenden Überwachung der darüber geführten Internettelefonie zeigt gerade auch der Vergleich mit typischen Begleitmaßnahmen andere strafprozessualer heimlicher Eingriffsbefugnisse. Ebenso wie das heimliche Öffnen eines PKWs, der heimliche Einbau sowie das Anschließen an die KFZ-Batterie *zum Betrieb* einer Abhörvorrichtung[708] im Rahmen einer Maßnahme der akustischen Überwachung außerhalb der Wohnung nach § 100f I StPO zum Abhören und Aufzeichnen des in einem Kraftfahrzeug nichtöffentlich gesprochenen Wortes mittels der auf diese Weise angebrachten Abhörvorrichtung[709], bzw. eines GPS-Empfängers/-Senders im Rahmen einer Maßnahme nach § 100h I S. 1 Nr. 2 StPO zur Positionsbestimmung eines PKWs unter Verwendung der GPS-Technik[710] gehören, und ebenso wie für Maßnahmen der akustischen Wohnraumüberwachung zum Abhören und Aufzeichnen des in einer Wohnung nichtöffentlich gesprochenen Wortes nach § 100c I StPO regelmäßig das damit sachlich verbundene heimliche Eindringen in die Räumlichkeiten zum Zwecke des

---

706 BT-Drs. 16/5846, S. 47.

707 Bundesministerium des Innern, Fragenkatalog SPD, S. 6, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012), in Bezug auf *Remote Forensic Software*, gilt für Quellen-TKÜ-Software insoweit in gleicher Weise; auch gesetzlich verankerte (präventivpolizeiliche) Ermächtigungsgrundlagen zu Maßnahmen der Quellen-TKÜ (bspw. § 201 II S. 1 BKAG, § 15b I HSOG, § 31 III S. 1 POG RP) legen hier die Begrifflichkeit „technisches Mittel“ für eine Überwachungssoftware zum Ausleiten laufender Telekommunikation zugrunde; für Einzelheiten zur Überwachungssoftware als technisches Mittel i. S. d. § 100a StPO, siehe 3. Teil A.I.1.a)aa).

708 Wie auch ggf. das kurzzeitige Verbringen in eine Werkstatt zur sachgerechten Durchführung dieser Handgriffe, vgl. *Schneider*, NStZ 1999, 388 (389); auch BGH NJW 2001, 1658 (1659).

709 Vgl. *Schneider*, NStZ 1999, 388 (389).

710 Vgl. BGH NJW 2001, 1658 (1659).

Anbringens der Abhörvorrichtung naturgemäß notwendig ist[711], stellt auch das heimliche (bzw. unter einem Vorwand erfolgende) Installieren einer Überwachungssoftware auf einem zur Internettelefonie genutzten informationstechnischen System – unter Zugriff auf das System, *Integration* („*Einbettung*") *der Software* in die System- und Softwareumgebung des betroffenen Zielsystems sowie unter (Mit-)Benutzung von Systemressourcen und Systemabläufen – für die der Untersuchung zugrunde liegenden Fälle der *Quellen-TKÜ* eine mit dem primären Überwachen und Aufzeichnen von (verschlüsselt übermittelter) Telekommunikation an der Quelle mit Hilfe der auf diese Weise als technisches Mittel zur Datenerhebung aus laufenden Telekommunikationsvorgängen integrierten Software in sachlichem Zusammenhang stehende und – mangels anderweitiger Zugriffsmöglichkeiten[712] – notwendigerweise verbundene Begleitmaßnahme dar. Die genaue Vorgehensweise zur Realisierung der Softwareinstallation, also ob dies bspw. durch Zusenden einer E-Mail mit verstecktem Anhang auf elektronischem Wege[713], durch Zuspielen eines entsprechend präparierten Datenträgers oder durch direkten physischen Zugriff am Zielgerät (außerhalb von Wohnungen) geschieht[714], ist abhängig von den konkreten Umständen des Einzelfalls und liegt im Ermittlungsverfahren grds. im Ermessen der zuständigen Staatsanwaltschaft als „Herrin des Vorverfahrens" bzw. der von ihr beauftragten Ermittlungsbehörde, welche insbesondere unter Beachtung des Zweck- und Verhältnismäßigkeitsgrundsatzes über die zur Umsetzung der angeordneten Maßnahme erforderlichen Schritte zu entscheiden hat[715].

Entsprechendes kann auch für die begleitende Maßnahme des *Deinstallierens der Überwachungssoftware* vom betroffenen Zielsystem nach Abschluss der Überwachungsmaßnahme angenommen werden. Als „actus contrarius" zur Installation der Software auf einem informationstechnischen System in Vorbereitung der eigentlichen Überwachung stellt anhand obiger Voraussetzungen auch das (im Regelfall wohl ebenfalls heimlich bzw. verdeckt erfol-

---

711 Vgl. BT-Drs. 13/8651, S. 13; auch Meyer-Goßner – *Cierniak*, StPO, § 100c, Rn. 7 m. w. N.; ebenso *Bär*, TK-Überwachung, § 100c StPO, Rn. 8 m. w. N.; vgl. hierzu auch zutr. LG Hamburg, MMR 2011, 693 (694).

712 Im Einzelnen hierzu unter 2. Teil B.III.2.b).

713 So ist die heimliche Installation der Software bei einem namentlich unbekannten Nutzer wohl nur auf dem elektronischen Wege realisierbar, vgl. *Kudlich*, JA 2010, 310 (311).

714 Für Einzelheiten zu den unterschiedlichen Einbringungsmöglichkeiten, siehe 1. Teil A.II.4.b) und 2. Teil B.I.2.; unzulässig hingegen mangels Betretungsrechts ist das heimliche Eindringen in von Art. 13 I GG geschützte Räume zum direkten Einspielen der Software durch physischen Zugriff, siehe hierzu auch 2. Teil B.I.2.b)bb).

715 Vgl. BGH-Ermittlungsrichter NStZ 2005, 278 (278 f.), soweit dies im konkreten Fall nicht mit etwaigen im Beschluss enthaltenen Vorgaben hinsichtlich der Art und Weise der Durchführung in Konflikt steht.

gende[716] automatisiert oder manuell eingeleitete[717]) Entfernen der Software nach Beendigung der Überwachungsmaßnahme eine mit der Überwachung und Aufzeichnung von verschlüsselt übermittelter Internettelefonie unter Ansetzen am Endgerät als „Quelle" des Kommunikationsvorgangs mittels eines technischen Mittels zur Datenerhebung kraft Natur der Sache verbundene („nachbereitende") Begleitmaßnahme dar. Hierunter fallen all diejenigen Schritte, die notwendig sind, um die Überwachungssoftware fachgerecht von dem betroffenen Zielsystem wieder zu Entfernen und einen dem Zustand des Systems vor der Infiltration entsprechenden „uninfiltrierten" Zustand[718] – soweit nach dem Stand der Technik möglich und zur Aufhebung der beeinträchtigenden Wirkung der Infiltration nötig[719] – wiederherzustellen, wobei hier – gerade angesichts des zugleich bestehenden rechtsstaatlichen Bedürfnisses wirksamer Strafverfolgung und Straftatenaufklärung – auch von staatlichen Stellen nichts (technisch) Unmögliches und damit Unerfüllbares verlangt werden kann.

Es lässt sich damit für das Kriterium der *Typizität* festhalten, dass eine andere Sichtweise als bspw. die des AG Hamburg und ähnlicher Stimmen[720] in Bezug auf das Vorliegen von Typizität der heimlichen Infiltration eines informationstechnischen Systems mit einer Überwachungssoftware zur Ermöglichung von an der Quelle durchgeführten Überwachungsmaßnahmen bei Internettelefonie als relevanter Fallgruppe mit guten Argumenten vertret-

---

716 So wird eine kriminaltaktische Notwendigkeit für ein heimliches bzw. verdecktes Entfernen der Software vom Zielsystem i. d. R. dann bestehen, wenn sich aus der überwachten Kommunikation erkennen lässt, dass durch ein offenes Vorgehen bspw. noch andauernde Ermittlungen, bei denen ein ermittlungstaktisches Interesse an der noch zeitweisen Aufrechterhaltung der Geheimhaltung fortbesteht, gefährdet werden könnten, vgl. in diese Richtung auch *Schneider*, NStZ 1999, 388 (390) zum Ausbau von in einen PKW eingebauten Abhörvorrichtungen im Rahmen von Maßnahmen nach § 100c I Nr. 2 StPO a. F. (§ 100f I StPO n. F.); zur verfassungsrechtlichen Bewertung, siehe 2. Teil B.II.

717 Für technische Einzelheiten, siehe 1. Teil A.II.4.c).

718 Die Herstellung des exakten Zustandes wie vor der Infiltration dürfte technisch kaum möglich und müsste darüber hinaus auch nicht zwingend sachgerecht sein, da systemimmanent durch jede Benutzung des Systems regelmäßig neue Daten anfallen und Prozesse ablaufen, die das System (i. d. R. im Sinne des Nutzers) fortlaufend verändern.

719 Bleiben technisch unvermeidbar bestimmte Dateifragmente als hinterlassene „digitale Spuren" der Software trotz fachgerechter Deinstallation auf dem System zurück, die aber nicht eigenständig – insbesondere zu Lasten des Systeminhabers – nutzbar sind und – wie auch bei anderen deinstallierten Dateien – einem Durchschnittsbenutzer gar nicht zur Kenntnis gelangen, ist eine belastende Wirkung im Sinne einer Beeinträchtigung des Betroffenen eher zu verneinen.

720 So bspw. AG Hamburg, CR 2010, 249; auch LG Hamburg, MMR 2008, 423; in dieselbe Richtung *Sankol*, CR 2008, 13 (17).

bar ist. Wie dies auch von mehreren Entscheidungen aus neuerer Zeit zur Frage der Zulässigkeit von Quellen-TKÜ-Maßnahmen getragen wird, lässt sich für die spezifischen Begleitmaßnahmen der Quellen-TKÜ dogmatisch vertretbar begründen[721], dass diese mit der Durchführung der in § 100a I StPO gesetzlich geregelten Maßnahme der *Überwachung und Aufzeichnung von Telekommunikation* jedenfalls für diesen Teil des Anwendungsbereichs typischerweise verbundene Eingriffe darstellen.

2. Verhältnismäßigkeit

Als zweites Kriterium für die Annahme einer Annexkompetenz müssten die den Anforderungen der Typizität gerecht werdenden Begleitmaßnahmen des heimlichen Infiltrierens des Zielsystems mit einer Überwachungssoftware wie auch des Deinstallierens der Software nach Abschluss der Ermittlungsmaßnahme als gesetzlich nicht ausdrücklich geregelte Eingriffe des Weiteren auch dem *Verhältnismäßigkeitsgrundsatz* gerecht werden, d. h. zur Erreichung des damit verfolgten legitimen Zwecks geeignet, erforderlich wie auch angemessen sein[722]:

a) Legitimer Zweck und Geeignetheit

Neben dem Erfordernis der Typizität stellt das Erfordernis der *Verhältnismäßigkeit* des heimlichen bzw. verdeckten Einbringens der Überwachungssoftware (wie auch des anschließenden wieder heimlichen Entfernens) die zweite Voraussetzung für die Bejahung einer Annexkompetenz zu § 100a I StPO als Rechtsgrundlage zu den Begleitmaßnahmen einer Quellen-TKÜ dar.

Als *legitimer Zweck* des heimlichen Installierens der Überwachungssoftware auf dem Zielsystem kommt hierbei die Ermöglichung einer Überwachung von moderner (Voice-over-)IP-Kommunikation an der Quelle, also

---

721 Wobei hiermit aber nicht verbindlich entschieden ist, ob ganz bestimmte Vorgehensweisen zur Ermöglichung des Installierens/Deinstallierens der Überwachungssoftware (insbesondere verfassungsrechtlich) zulässig sind, wie die obigen Ausführungen zum (unzulässigen) heimlichen Betreten von Wohnräumen zum Zwecke des Einbringens der Software dies verdeutlichen, siehe 2. Teil B.I.2.b).

722 Vgl. insoweit LG Hamburg, MMR 2008, 423 (424 f.); i. E. auch LG Hamburg, MMR 2011, 693 (694); auch *Schneider*, NStZ 1999, 388 (388); vgl. bereits BGH-Ermittlungsrichter NStZ 1998, 157 (157 f.), der allerdings insoweit nicht von einem kumulativen, sondern von einem alternativen Verhältnis beider Kriterien („neben“) ausgeht, krit. AG Hamburg, CR 2010, 249 (250); krit. auch *Schneider*, NStZ 1999, 388 (389); vgl. zum Kriterium der Beachtung des Verhältnismäßigkeitsgrundsatzes auch BGH NJW 2001, 1658 (1659).

auf dem jeweiligen zur IP-basierten Kommunikation genutzten informationstechnischen System, zum Zwecke der Gewinnung von verfahrens- und beweisrelevanten Erkenntnissen in Betracht, da diese Maßnahme der Verfolgung und Aufklärung schwerer Straftaten im Zusammenhang mit der Nutzung von Telekommunikation dient.[723] Gemäß wiederholter Rspr. des BVerfG[724] stellen die „wirksame Strafverfolgung, die Verbrechensbekämpfung und das öffentliche Interesse an einer möglichst vollständigen Wahrheitsermittlung im Strafverfahren“[725] legitime Zwecke dar, welche „eine Einschränkung des Fernmeldegeheimnisses rechtfertigen können“[726].

Für die Beurteilung der *Eignung* der heimlichen Installation einer Überwachungssoftware auf dem jeweiligen Zielsystem für ein Ermöglichen der Überwachung und Aufzeichnung von (Voice-over-)IP-Kommunikation an der Quelle zum Erreichen der damit verfolgten legitimen Zwecke sind sowohl *Selbstschutzmöglichkeiten* der Nutzer gegen derartigen Zugriffe ebenso wie der *potentielle Beweiswert* der mittels eines derartigen Zugriffs erlangten Erkenntnisse in die Abwägung einzustellen:

So wird in der Literatur teilweise vorgetragen, dass der Eignung einer heimlichen Infiltration informationstechnischer Systeme für die obigen Zwecke vielfältige technische Selbstschutzmöglichkeiten zur Verfügung stünden, um einen entsprechenden Zugriff wirkungsvoll zu unterbinden. Nach *Buermeyer* liege bspw. vor allem „die Annahme nahe, dass Antiviren-Programme einen ‚Bundes-Trojaner‘ als Schädling erkennen“[727] und Anbieter von Antiviren-Software kaum Interesse haben dürften, angesichts der dann bestehenden Sicherheitslücke „bei staatlicher Überwachungssoftware ein Auge zuzudrücken“[728] und diese von der Überprüfung durch den Antiviren-Scanner auszunehmen. Auch Firewall-Programme bärgen das Risiko der Entdeckung des heimlichen staatlichen Handelns, wenn derartige Programme anschlagen, „sobald die staatliche Überwachungssoftware erfasste Daten ‚nach Hause‘ senden möchte“[729].[730] Nach *Gercke* könne sich „die zunehmende

---

723 Vgl. BVerfG NJW 2003, 1787 (1789).

724 Vgl. BVerfG NJW 1988, 329 (330); BVerfG NJW 1990, 563 (564); BVerfG NJW 2000, 55 (65); BVerfG NJW 2003, 1787 (1789); BVerfG NJW 2006, 976 (980); BVerfG NJW 2009, 2431 (2434).

725 BVerfG NJW 2009, 2431 (2434).

726 BVerfG NJW 2009, 2431 (2434).

727 *Buermeyer*, HRRS 2007, 154 (165).

728 *Buermeyer*, HRRS 2007, 154 (165); ähnlich auch *Gercke*, CR 2007, 245 (249).

729 *Buermeyer*, HRRS 2007, 154 (165).

730 Ähnlich auch *Hornung*, DuD 2007, 575 (579) in Bezug auf die Online-Durchsuchung, wonach sich „angesichts der verfügbaren Schutzinstrumente und des Fehlens von Erfolgsbeispielen“ (579) an der Eignung zweifeln lasse.

Sensibilität der Internetnutzer für die Notwendigkeit der Ergreifung von Schutzmaßnahmen […] als besonderes Problem erweisen, da diese Maßnahmen ggf. die Infiltration und Installation der Ermittlungssoftware aufdecken und verhindern“[731]. Nach *Becker/Meinicke* sei „der viel beschworene ‚Höchstgefährder‘ […] ohne größere Mühe in der Lage, erfolgreiche Angriffe auf die von ihm genutzten Systeme zu unterbinden“[732].

Des Weiteren wird von Seiten der Literatur gegen die Eignung der Installation einer Überwachungssoftware zum Erlangen von (beweissicheren) Erkenntnissen für eine effektive Strafverfolgung und Straftatenaufklärung aber auch vorgetragen, dass deren Beweiswert begrenzt sei, da eine technische Bestätigung der Echtheit, also der Authentizität des erhobenen Datenmaterials, „grundsätzlich nur verlässlich vorgenommen werden [kann], wenn eine exklusive Kontrolle über ein System vorliegt“[733], eine solche alleinige Kontrolle des Zielsystems jedoch weder beim Nutzer noch bei den Ermittlungspersonen gegeben sei[734].

Nach Auffassung des BVerfG hingegen ist der heimliche Zugriff auf informationstechnische Systeme zum Erreichen der oben genannten Zwecke geeignet.[735] Denn es könne „nicht als selbstverständlich unterstellt werden, dass jede mögliche Zielperson eines Zugriffs bestehende Schutzmöglichkeiten dagegen nutzt und tatsächlich fehlerfrei implementiert“[736]. Auch erscheine es „im Übrigen […] denkbar, dass sich im Zuge der weiteren informationstechnischen Entwicklung […] Zugriffsmöglichkeiten auftun, die sich technisch nicht mehr oder doch nur mit unverhältnismäßigem Aufwand unterbinden lassen“[737]. Hierbei sei „im Rahmen der Eignungsprüfung […] nicht zu fordern, dass Maßnahmen, welche die […] Norm erlaubt, stets oder auch nur im Regelfall Erfolg versprechen“[738], solange die Erfolgsprognose für Zugriffe im Einzelfall „zumindest nicht offensichtlich fehlsam“[739] ist. Die Eignung der heimlichen Infiltration zur Erreichung der mit der Maßnahme verbundenen Zwecke sei auch „nicht deshalb zu verneinen, weil möglicherweise der Beweiswert der Erkenntnisse, die mittels des Zugriffs gewonnen werden, begrenzt ist“[740]. Denn etwaige Schwierigkeiten der Be-

731 *Gercke*, CR 2007, 245 (249).
732 *Becker*/*Meinicke*, StV 2011, 50 (52).
733 *Hansen*/*Pfitzmann*, DRiZ 2007, 225 (228).
734 Vgl. *Hansen*/*Pfitzmann*, DRiZ 2007, 225 (228).
735 Vgl. BVerfG NJW 2008, 822 (829).
736 BVerfG NJW 2008, 822 (829).
737 BVerfG NJW 2008, 822 (829).
738 BVerfG NJW 2008, 822 (829).
739 BVerfG NJW 2008, 822 (829).
740 BVerfG NJW 2008, 822 (829).

weissicherung bewirken nach Auffassung des BVerfG „nicht, dass den erhobenen Daten kein Informationswert zukommt“[741].

Die Ausführungen des BVerfG verdeutlichen zu Recht, dass mit Blick auf die Eignung einer staatliche Infiltration von informationstechnischen Systemen (hier zum Zwecke der Überwachung verschlüsselt übermittelter VoIP-Kommunikation an der Quelle) – jedenfalls im Regelfall[742] – nicht unterstellt werden kann, dass jede in Frage kommende Zielperson eines solchen Zugriffs auch (ausreichende) technische Schutzvorkehrungen gegen einen solchen Zugriff ergreift bzw. diese technischen Schutzvorkehrungen fehlerfrei implementiert[743], ausführt und auf dem aktuellen Stand hält.[744] Insoweit ist auch nicht davon auszugehen, dass jeder Nutzer (auch künftig) das an sich notwendige Maß an Misstrauen im Umgang mit dem Internet und hierüber stattfindender virtueller Interaktion aufbringen wird. Des Weiteren ist angesichts der raschen informationstechnischen Entwicklung nicht nur zu erwarten, dass technische Schutzmechanismen verfeinert werden, sondern dass in gleicher Weise auch die den Ermittlungsbehörden zur Verfügung stehenden technischen Möglichkeiten zur Umgehung von Schutzmaßnahmen durch stetige Verbesserung der technischen Mittel und Funktionsweisen eine Infiltration zunehmend vereinfachen können. Künftig in noch stärkerem Maße wie heute wird deshalb wohl das Gelingen strafprozessaler Ermittlungsmaßnahmen auf diesem Gebiet von einem regelrechten „Wettlauf der Infiltrations- und Abwehrtechniken“ geprägt sein.[745]

---

741 BVerfG NJW 2008, 822 (829).

742 Ausnahmen wären höchstens bspw. bei technisch besonders versierten Zielpersonen denkbar, die ihre Endgeräte durch spezielle, ggf. auch selbst entworfene Schutzprogramme und Abwehrstrategien vor heimlicher Installation von Software zu schützen versuchen; einerseits stellt diese Gruppe jedoch nicht das Gros der Nutzer von Internet- und VoIP-Diensten dar und auch die technisch versierten „Experten“ sind in gewisser Weise vor menschlicher Nachlässigkeit im Umgang mit technischen Sicherungsmaßnahmen nicht gefeit, vgl. auch *Sieber*, Stellungnahme zu dem Fragenkatalog des BVerfG in dem Verfahren 1 BvR 370/07, S. 13 f., abrufbar unter http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf (zuletzt aufgerufen 15.06.2012).

743 Vgl. insoweit auch BVerfG NJW 2008, 822 (829).

744 So räumen auch *Becker*/*Meinicke*, StV 2011, 50 (52) ein, „dass etwa der Prozess um die sog. ‚Sauerland-Gruppe‘ ein beachtliches Maß an Dilettantismus in den einschlägigen terroristischen Kreisen offenbart hat“ (52).

745 Vgl. auch *Sieber*, Stellungnahme zu dem Fragenkatalog des BVerfG in dem Verfahren 1 BvR 370/07, S. 13, abrufbar unter http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf (zuletzt aufgerufen 15.06.2012), der treffend beschreibt, dass „gegen jede Angriffsform eine Abwehrtechnik und gegen jede Abwehrtechnik eine Umgehungsstrategie entwickelt werden kann.“ (S. 13).

Des Weiteren ist auch der Feststellung des BVerfG zuzustimmen, wonach die Eignung nicht aus dem Grunde zu verneinen sei, dass der Beweiswert der mittels der Überwachungssoftware erlangten Erkenntnisse mangels exklusiver Kontrolle[746] der Ermittlungspersonen über das System möglicherweise begrenzt sei, wie dies teilweise vertreten wird[747]. Schwierigkeiten der Beweissicherung auf Grund fehlender exklusiver Kontrolle im Moment der Datenerfassung lassen sich in Bezug auf die Frage der Echtheitsbestätigung der gewonnen Daten durch genaue und nachprüfbare Verfahrensvorgaben in Form von lückenlosen Dokumentations- und Protokollierungspflichten bezüglich des Einsatzes der Überwachungssoftware und der hiermit erhobenen Daten begegnen sowie durch eine vor Veränderung oder unbefugter Löschung zugriffssicher geschützte weitere Behandlung und Speicherung der erhobenen Daten gemäß dem Stand der Technik Rechnung tragen.[748] Eine Aufzeichnung von Internettelefonaten, also von akustischer IP-Kommunikation, bietet darüber hinaus freilich auch die Möglichkeit, ggf. über Stimmabgleiche u. ä. eine Zuordnung von Gesprochenem zu einer bestimmten Person vorzunehmen[749], falls die Urheberschaft von abgefangenen Telekommunikationsinhalten in Frage stehen sollte.

b) Erforderlichkeit?

Noch mehr als die Frage der Geeignetheit stehen die Frage der *Erforderlichkeit* sowie der *Angemessenheit* (vgl. unten Punkt c) der heimlichen Infiltration eines informationstechnischen Systems mit einer Überwachungssoftware zum Zwecke der Telekommunikationsüberwachung im Zentrum des Interesse der dogmatischen Diskussion.

Das heimliche Einspielen einer Überwachungssoftware wäre dann *erforderlich*, wenn keine milderen Mittel zu Verfügung stünden, welche bei gleicher Eignung den Betroffenen zur Erreichung des mit der Maßnahme verfolgten Zwecks weniger belasten würden (*Grundsatz der Erforderlichkeit*). D. h. um erforderlich zu sein, darf als Alternative zur Infiltration des

---

746 Wobei es bereits als fraglich anzusehen sein dürfte, ob eine solche nach den gegenwärtigen technischen Standards überhaupt realisierbar und damit gegenüber Ermittlungsbehörden einforderbar wäre.

747 So bspw. *Hansen*/*Pfitzmann*, DRiZ 2007, 225 (228).

748 Für Einzelheiten zu Vorgaben hinsichtlich der technisch zu ergreifenden Maßnahmen zur Gewährleistung der Beweissicherheit und Beweismittelauthentizität, insbesondere zu Dokumentations- und Protokollierungspflichten, siehe 3. Teil A.I.2. sowie 3. Teil B.III.3.

749 In diese Richtung auch *Gercke*/*Brunst*, Internetstrafrecht, Kap. 5, S. 347, Rn. 882, Fn. 366; dies gilt freilich erst recht, wenn bei einer Video-Internettelefonie auch die visuellen Inhalte der Kommunikation miterfasst wurden.

Zielsystems kein ebenso wirksamer, aber für Betroffene weniger belastender Weg vorliegen[750], um eine Überwachbarkeit von über informationstechnische Systeme geführte, verschlüsselt übermittelte VoIP-Kommunikation zu ermöglichen.

Die spezifische Vorgehensweise einer herkömmlichen („klassischen") TKÜ-Realisierung (Abfangen der Signale auf der Übertragungsstrecke durch entsprechende technische Einrichtungen) ist – wie bereits erläutert – in den Fällen verschlüsselt übertragener Internettelefonie wenig erfolgversprechend[751], da diese Umsetzungsweise den Ermittlungsbehörden zwar TK-Daten liefern würde, jedoch nur in codierter Form, und eine Entschlüsselung der Daten selbst mit einem hohen technischen Aufwand nicht, jedenfalls nicht zeitnah möglich wäre[752].

Es stellt sich daher unter dem Kriterium der *Erforderlichkeit* des heimlichen Installierens einer Überwachungssoftware zur Ausleitung der TK-Daten vor ihrer Verschlüsselung bzw. – beim Anknüpfen am Empfängersystem – nach ihrer Entschlüsselung die Frage, ob an die spezifischen technischen Besonderheiten angepasste Alternativen für den Zugriff auf (im Datennetz verschlüsselt transportierte) TK-Daten aus derartigen VoIP-Kommunikationen zur Verfügung stehen, die ein milderes aber in gleicher Weise geeignetes und erfolgversprechendes Mittel für die Realisierung einer Überwachbarkeit dieser Kommunikationsform darstellen als das heimliche Einbringen einer Überwachungssoftware.

Als denkbare Alternativen in Betracht kommen hierfür aa) das Verschaffen eines *Schlüssels* zur Entschlüsselung der codiert transportierten TK-Daten sowie bb) die Benutzung von *Hintertüren* (sog. *Backdoors*) in die jeweilige VoIP-Software:

aa) Verschaffen des Schlüssels

Eine denkbare, (möglicherweise) mildere Alternative zu einer Infiltration des informationstechnischen Systems mit einer Überwachungssoftware könnte das Verschaffen und Verwenden eines für die Verschlüsselungsart des jeweiligen VoIP-Programms passenden *Schlüssels*[753] sein. Das Verfügen über einen Schlüssel brächte hierbei den Vorteil, dass die verschlüsselt über-

---

750 Vgl. insoweit auch BVerfG NJW 2008, 822 (829).

751 In diesem Sinne auch BVerfG NJW 2008, 822 (829).

752 Vgl. BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 107a; auch LG Hamburg, MMR 2011, 693 (695).

753 Zeichenkette/-folge, mit der sich Daten/Dateien ver- und entschlüsseln lassen und deren Länge in Bit angegeben wird, vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 206 u. 130.

mittelten Daten bei ihrem Transport im Datennetz im Wege einer klassischen TKÜ abgegriffen und die dann vorliegenden Kopien der verschlüsselten TK-Daten mit Hilfe des passenden (Nach-)Schlüssels[754] zum Zweck der Kenntnisnahme und des Erkenntnisgewinns aus den darauf enthaltenen Kommunikationsinhalten decodiert werden könnten.

Zur Frage der Existenz solcher Schlüssel für die verschiedenen Verschlüsselungstechniken der auf dem Markt befindlichen VoIP-Programme – als taugliche Alternative zur Quellen-TKÜ müsste nicht nur für Skype-Kommunikation ein Schlüssel vorliegen – zur Entschlüsselung der auf dem Übertragungsweg abgefangenen, in verschlüsseltem Zustand vorliegenden TK-Daten, herrscht weitgehend Unklarheit. Insbesondere für die gegenwärtig wohl populärste VoIP-Software *Skype* ist das Vorhandenseins eines – ggf. universellen[755] – Schlüssels für dessen proprietäres Verschlüsselungsprotokoll basierend auf dem AES-Standard fraglich:

Während bspw. der Anbieter *Skype* für seine VoIP-Software damit wirbt, dass Skype „bewährte, standardbasierte Verschlüsselungsalgorithmen [verwendet], um die Kommunikationen von Skype-Nutzern davor zu schützen, dass sie in die Hände von Hackern und Kriminellen fallen“[756] und um auf diese Weise dabei zu helfen, „die Privatsphäre von Nutzern und die Integrität von Daten zu bewahren, die von einem Nutzer zu einem anderen gesendet werden“[757] – was grds. gegen die Existenz von (universellen) Schlüsseln in das Verschlüsselungsprotokoll spräche – wird von anderer Seite teilweise vorgetragen, dass sich bezüglich der „lange Zeit als abhörsicher“[758] gegoltenen Software Skype inzwischen jedoch Hinweise verdichtet hätten, „dass es einen auch hoheitlich zu nutzenden ‚Nachschlüssel‘ für das geheime Verschlüsselungsverfahren“[759] gebe[760] und die Hersteller von VoIP-Programmen „offenbar die Möglichkeit [haben], jeden Sit-

---

754 Zum „Schlüssel“ des Absenders sowie dem damit korrespondierenden „Schlüssel“ des Empfängers, mit dem der Verschlüsselungsalgorithmus der übermittelten TK-Daten wieder aufgehoben wird.

755 Passend für alle auf dem Markt befindlichen Programmversionen der VoIP-Software und alle einzelnen verschlüsselt geführten Gespräche, was bereits insoweit fraglich erscheint, als bei end-to-end-Verschlüsselung die TK-Daten i. d. R. mit einem zufälligen und nur temporär für diesen Kommunikationsvorgang gültigen Verschlüsselungsalgorithmus versehen werden, vgl. hierzu auch Anm. *Brodowski*, JR 2011, 533 (533).

756 http://www.skype.com/intl/de/security/detailed-security/ (zuletzt aufgerufen 15.06.2012).

757 http://www.skype.com/intl/de/security/detailed-security/ (zuletzt aufgerufen 15.06.2012).

758 *Hoffmann-Riem*, JZ 2008, 1009 (1021), Fn. 115.

759 *Hoffmann-Riem*, JZ 2008, 1009 (1021), Fn. 115.

760 Vgl. *Hoffmann-Riem*, JZ 2008, 1009 (1021), Fn. 115 m. w. N.

zungsschlüssel zu ermitteln, weshalb eine Entschlüsselung der durch eine herkömmliche TKÜ erlangten Daten keineswegs ausgeschlossen“[761] sei[762].

Andere Stimmen wiederum lassen darauf schließen, dass Möglichkeiten der Entschlüsselbarkeit gerade von Skype-Gesprächen bzw. der Nutzung einer technischen Hintertür (*Backdoor*) in das Skype-Programm bislang nicht bestehen[763].

Auf das gegenwärtige Fehlen technischer Entschlüsselungsmöglichkeiten für verschlüsselte VoIP-Kommunikation via Skype deuten neben den Stellungnahmen von staatlicher Seite indes auch Anhaben des Anbieters selbst hin:

Laut Stellungnahme der Bundesregierung vom 26.10.2011[764] sei es Skype in den Fällen (end-to-end) verschlüsselter P2P-VoIP zwischen zwei internetfähigen Endgeräten „nach derzeitigem Kenntnisstand der Bundesregierung schon aus technischen Gründen nicht möglich, Inhaltsdaten den Justiz-, Strafvollzugs- oder Regierungsbehörden zur Verfügung zu stellen“[765].

---

761 *Becker*/*Meinicke*, StV 2011, 50 (52).

762 Vgl. *Becker*/*Meinicke*, StV 2011, 50 (52).

763 In diese Richtung bspw. *Bär*, persönliches Gespräch mit dem Verfasser, Bamberg, 09.12.2010, unter Verweis auf ein Treffen von Eurojust (*Europäische Einheit für justizielle Zusammenarbeit*) im Jahr 2006, bei dem Skype betont habe, weder einen Schlüssel zu besitzen noch über eine sog. Backdoor in das Programm zu verfügen; hierauf deutet indes auch eine Stellungnahme von Skype im Rahmen der Anhörung durch die Bundesnetzagentur im Jahr 2004, hin, wonach „eine ‚Hintertür‘ in die Software […] zu vielen Probleme [sic] führen [würde]“ (S. 16), abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Stellungnahmen/SkypeTechnologiesId714pdf.pdf?__blob=publicationFile (zuletzt aufgerufen 15.06.2012); vgl. auch Anm. *Bär*, MMR 2011, 691 (691 f.); in diese Richtung auch *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11.2010; ebenso *Schellinger*, Inspektion Technische Einsatzunterstützung und Service, Landeskriminalamt Baden-Württemberg, schriftliche Befragung vom 03.09.2010, wonach es sich bei den dort bekannten Maßnahmen „jeweils um den einzigen Ermittlungsansatz [handelte,] die verschlüsselte Kommunikation zu überwachen“ und es „Alternativen […] hierzu nicht [gab]“.

764 Antwort des Parl. Staatssekretärs beim Bundesminister des Innern, *Bergner*, für die Bundesregierung im Rahmen der 135. Sitzung des Deutschen Bundestags am 26.10.2011 (BT-PlPr. 17/135 16064 D); in diese Richtung auch die Antwort des Parl. Staatssekretärs beim Bundesminister des Innern, *Schröder*, im Rahmen der 132. Sitzung des Deutschen Bundestages am 19.10.2011 (BT-PlPr. 17/132 15589 B), wonach es „bei der Peer-to-Peer-Kommunikation […] keine andere Möglichkeit [gibt], als an den Computer heranzugehen und die Quellen-Telekommunikationsüberwachung durchzuführen“ (15589 B).

765 Antwort des Parl. Staatssekretärs beim Bundesminister des Innern, *Bergner*, für die Bundesregierung im Rahmen der 135. Sitzung des Deutschen Bundestags am 26.10.2011 (BT-PlPr. 17/135 16064 D); in diese Richtung auch die Antwort des

Skype selbst wirbt auf seiner Internetpräsenz durchweg damit, dass der Schutz von „Informationen […] sowie der geführten Gespräche […] an erster Stelle [stehen]“[766] und „alle Sprach- und Videoanrufe und IM-Chats zwischen Skype-Nutzern […] verschlüsselt [werden]“[767], um „Nutzern Schutz vor einer großen Bandbreite möglicher Angriffe, wie z. B. Identitätswechsel, Abhören, Man-In-The-Middle-Angriffe und Datenmodifizierung während der Übertragung“[768] zu bieten und „die Privatsphäre von Nutzern und die Integrität von Daten zu bewahren, die von einem Nutzer zu einem anderen gesendet werden“[769]. Skype verweist zudem auch in einem Informationsblatt zur Beantwortung der Anfragen von Sicherheits- und Strafverfolgungsbehörden[770] darauf, dass es auf eine entsprechende Anordnung hin (technisch) nur möglich sei, bestimmte Bestands- sowie Verkehrsdaten bereitzustellen[771], was insgesamt wiederum gegen die Existenz und Nutzbarkeit eines Schlüssels zur Entschlüsselung des von Skype verwendeten Verschlüsselungsprotokolls spricht.

Doch selbst für den Fall, dass ein Schlüssels in die Skype-Verschlüsselung existieren und für strafprozessuale Zwecke zur Verfügung stehen sollte, würde dieser Umstand die Notwendigkeit zur Durchführung von Quellen-TKÜ-Maßnahmen nicht per se wegfallen lassen. Denn ein solcher „Skype-Schlüssel“ würde – sofern das Unternehmen überhaupt zur Herausgabe verpflichtet wäre[772] – dann ggf. zwar verschlüsselt abgefangene TK-In-

---

Bayerischen Staatsministeriums des Innern, LT-Drs. 16/10469, S. 2; gegen eine generelle Decodierbarkeit von Skype-Telefonaten auch *Klesczewski*, ZStW 2011, 737 (742), Fn. 25 m. w. N., wonach Skype die Parameter des Verschlüsselungscodes regelmäßig abändere.

766 http://www.skype.com/intl/de/security/#encryption (zuletzt aufgerufen 15.06. 2012).

767 https://support.skype.com/de/faq/FA31/Verwendet-Skype-Verschlusselung (zuletzt aufgerufen 15.06.2012).

768 http://www.skype.com/intl/de/security/detailed-security/ (zuletzt aufgerufen 15.06.2012).

769 http://www.skype.com/intl/de/security/detailed-security/ (zuletzt aufgerufen 15.06.2012).

770 Skype-Informationsblatt *Responding to Law Enforcement Records Requests*, abrufbar unter http://cryptome.org/isp-spy/skype-spy.pdf (zuletzt aufgerufen 15.06. 2012).

771 Vgl. Skype-Informationsblatt *Responding to Law Enforcement Records Requests*, abrufbar unter http://cryptome.org/isp-spy/skype-spy.pdf (zuletzt aufgerufen 15.06.2012).

772 Zur bislang nicht abschließend geklärten Frage, ob Anbieter softwarebasierter P2P-VoIP-Kommunikation überhaupt der Mitwirkungsverpflichtung des § 100b III StPO unterfallen, siehe 2. Teil A.II.6.b); diesen Umstand vernachlässigt bspw. *Buermeyer*, http://ijure.org/wp/archives/756 (zuletzt aufgerufen 15.06.2012), der sich als milderes Mittel (zunächst) für „eine klassische TKÜ unter Einschaltung des Provi-

haltsdaten aus P2P-Kommunikationen via Skype für Ermittlungsbehörden einsehbar machen, jedoch nicht weiterhelfen, wenn bspw. der Verdächtige ein anderes VoIP-Programm benutzt. Somit müssten Schlüssel für die Verschlüsselungsprotokolle sämtlicher in Frage kommender VoIP-Programme herangezogen werden, was sich angesichts der Vielzahl von Anbietern auf dem Markt sowie der verschiedenen digitalen Verschlüsselungsweisen neben den technischen Fragestellungen eines (universellen) „Nachschlüssels" auch organisatorisch schwierig gestalten dürfte, betrachtet man allein die Diskussionen um einen Schlüssel für das Verschlüsselungsprotokoll des einen Anbieters Skype.

Sollte es sich zudem nicht um einen universellen Schlüssel handeln, also einen Schlüssel der zu allen veröffentlichten Softwareversionen (ältere wie auch die aktuellste Version) und Softwareaktualisierungen (*Updates*) passt, sondern sollte jede Version bzw. Aktualisierung einen eigenen, speziell darauf abgestimmten Schlüssel erfordern, so würde die Durchführbarkeit strafprozessualer Ermittlungen bei verschlüsselter VoIP-Kommunikation im Ergebnis davon abhängen, ob bereits ein aktueller Schlüssel für die neueste Softwareversion bzw. noch ein gültiger Schlüssel für ältere Versionen existiert und somit jeweils ein passender Schlüssel für die passende Software den Ermittlungsbehörden zur Verfügung steht. Kommt gar für jedes einzelne Internettelefonat ein eigener Schlüssel zum Einsatz, so wäre das Gelingen strafprozessualer Ermittlungsarbeit von der wiederholten Mitwirkung des VoIP-Diensteanbieters und den technischen Möglichkeiten dazu abhängig, den konkreten Schlüssel für das konkrete Gespräch zu erlangen, was bei für Kommunikationsverschlüsselungen regelmäßig verwendeten Schlüsseln, die nur temporär gelten, automatisch generiert werden, eine große Länge und hohe Zufälligkeit aufweisen[773], mehr als fraglich ist. Dies würde zudem ein hohes Maß an Abstimmung mit den – i. d. R. mit Sitz im Ausland befindlichen und global agierenden – privaten Anbietern und deren Mitwirkungsfähigkeit sowie (bei fehlender gesetzlicher Verpflichtung) Mitwirkungsbereitschaft erfordern, was zu einem unübersehbaren – mit dem grundgesetzlichen Legalitätsprinzip und Strafanspruch des Staates kollidierenden – Abhängigkeitsverhältnis für Strafverfolgungsbehörden bei der Ermittlungstätigkeit führen würde.

Überdies kann bei der Suche nach Alternativen für die Installation einer Überwachungssoftware zur Überwachung von verschlüsselter Telekommunikation auch nicht unberücksichtigt bleiben, dass die massenhafte Existenz von Zweitschlüsseln für sämtliche VoIP-Programme und deren Verschlüsse-

---

ders – etwa Skype" als dem „in § 100b Abs. 3 StPO gesetzlich vorgesehene[n] Weg" ausspricht.

773 Vgl. Anm. *Brodowski*, JR 2011, 533 (533).

lungsprotokolle oder gar eine gesetzliche Verpflichtung (soweit praktisch wie auch technisch angesichts des weltweiten Internets überhaupt durchsetzbar) zur obligatorischen Vorhaltung solcher Schlüssel generell für Verschlüsselungsprodukte zum Zwecke des staatlichen Zugriffs wohl nicht nur ein Gefühl des generellen „Überwachtwerdens" (zumindest der erleichterten Möglichkeit hierzu) bei den Nutzern von Verschlüsselungstechnologien – mittlerweile ein Großteil der Bevölkerung – bewirken würde[774], sondern auch zu erheblichen Gefahren für den Schutz und die Vertraulichkeit codierter digitaler Informationen insgesamt führen und insbesondere für verschlüsselte Telekommunikation das Risiko unbefugter Kenntnisnahmemöglichkeit erhöhen würde, falls (universelle) Schlüssel in die Hände unbefugter Dritter gelangen sollten.

bb) Benutzen einer Hintertür (sog. *Backdoor*)

Es stellt sich die Frage, ob das Benutzen etwaiger in VoIP-Programme eingebauter *technischer Hintertüren* (sog. *Backdoors*) ein grundrechtsschonenderes[775], in gleicher Weise geeignetes Mittel als die Infiltration des Systems mit einer Überwachungssoftware darstellen könnte, um verschlüsselte Telekommunikation einer Überwachung und Aufzeichnung zugänglich zu machen. Eine Hintertür (engl. *backdoor*) im computertechnischen Sinne stellt einen (oftmals bewusst durch den Hersteller „von Haus aus" eingebauten) Bestandteil einer Software (bspw. eines Betriebssystems oder eines Anwendungsprogramms) dar, welcher die Möglichkeit eröffnet, unter Umgehung der normalen Zugriffssicherungen alternativ „über die Hintertür" Zugang in ein System oder in eine an sich geschützte Funktion eines Programms zu erlangen.[776] Eine „Backdoor" stellt damit aber als potentielles „Einfallstor" auch eine Schwachstelle in den betroffenen Systemen dar.

Um als milderes Mittel im Rahmen der Verhältnismäßigkeit (*Erforderlichkeit*) überhaupt in Betracht zu kommen, müsste solch eine Hintertür in das Programm dann aber auch vom Hersteller tatsächlich eingebaut worden sein und darüber hinaus für strafprozessuale Ermittlungszwecke zur Verfügung stehen. Ob dies bei der wohl meistverbreiteten VoIP-Software *Skype* zum Führen von P2P-geschlossener VoIP zwischen zwei Endgeräten der Fall ist bzw. überhaupt technisch möglich ist, ist weitgehend unklar.

Wie bei der Frage des Vorhandenseins eines (universellen) Schlüssels in das Verschlüsselungsprotokoll der jeweiligen VoIP-Software zur Entschlüs-

774 Vgl. hierzu auch Anm. *Brodowski*, JR 2011, 533 (534).

775 Dies bejahen bspw. *Braun*/*Roggenkamp*, K&R 2011, 681 (685).

776 Vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 24.

selung der während des Transports über das Datennetz end-to-end via AES-Algorithmus verschlüsselten TK-Daten, wird auch für die Frage des Bestehens einer technischen Hintertür in das Skype-Programm zum Teil darauf hingewiesen, dass eine solche durch den Anbieter eingerichtete und bereitgehaltene technische Eintrittsstelle in das Programm bei Skype (aber auch bei anderen Anbietern) existieren soll.[777] Die Benutzung einer solchen technischen Hintertür in das Programm soll indes nach teilweise vertretener Auffassung mit einer klassischen TKÜ vergleichbar und von § 100a StPO gedeckt sein[778] sowie im Vergleich zu einer Maßnahme der Quellen-TKÜ eine grundrechtsschonendere Maßnahme darstellen, da kein Eingriff in den Rechner der Zielperson notwendig sei[779], weshalb diese Vorgehensweise der Quellen-TKÜ vorzuziehen wäre.[780]

Von Skype selbst wurde in der Vergangenheit hingegen bereits die Befürchtung vorgetragen, dass „eine ‚Hintertür' in die Software […] zu vielen Probleme [sic] führen [würde], da dadurch sehr leicht in die Software ‚eingebrochen' werden könnte"[781]. Mit der von Skype zudem bekundeten

---

777 So bspw. *Braun*/*Roggenkamp*, K&R 2011, 681 (685) m. w. N., wonach „es schon im Jahr 2008 Hinweise darauf [gab], dass das Abhören von Skype über eine sog. ‚Backdoor' […] möglich" (685) sei, unter Hinweis auf die Datenschutzrichtlinie von Skype, wonach „Skype, der örtliche Skype-Partner oder der Betreiber bzw. Anbieter, der die Kommunikation ermöglicht, personenbezogene Daten, Kommunikationsinhalte oder Verkehrsdaten Justiz-, Strafvollzugs- oder Regierungsbehörden zur Verfügung [stellt], die derartige Informationen rechtmäßig anfordern" sowie „zur Erfüllung dieser Anforderung angemessene Unterstützung und Informationen bereitstellen [wird]" (http://www.skype.com/intl/de/legal/privacy/general/#4, zuletzt aufgerufen am 15.06.2012); hierauf Bezug nehmend auch *Stadler*, MMR 2012, 18 (19); dem lässt sich freilich entgegenhalten, dass aus der Richtlinie gerade nicht eindeutig hervorgeht, ob damit alle Inhalte, also auch die aus der end-to-end-verschlüsselt übermittelten P2P-Kommunikation gemeint sind, oder – was naheliegender ist – Inhalte, soweit Skype auf diese Zugriff hat („angemessene Unterstützung und Informationen"), in Betracht kommend bspw. bei hinterlassenen Sprachnachrichten (auf welche in der Datenschutzrichtlinie einen Absatz früher ausdrücklich Bezug genommen wird), und (technisch) zu einer Bereitstellung in der Lage ist; in diese Richtung auch die Antwort der Bundesregierung vom 26.10.2011, BT-PlPr. 17/135 16064 D.

778 Vgl. bspw. Anm. *Brodowski*, JR 2011, 533 (534); auch *Braun*/*Roggenkamp*, K&R 2011, 681 (685).

779 Wobei dem entgegenzuhalten ist, dass auch bei der Nutzung einer Hintertür im VoIP-Programm ein „Ansprechen" des Programms und mithin ein Zugriff von außen auf das informationstechnische System, auf welchem das Programm gespeichert ist und ausgeführt wird, notwendig ist.

780 So *Braun*/*Roggenkamp*, K&R 2011, 681 (685); a. A. wohl *Albrecht*, JurPC Web-Dok. 59/2011, Abs. 20.

781 Stellungnahme von Skype im Rahmen der Anhörung durch die Bundesnetzagentur im Jahr 2004, S. 16, abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/Voice

Zielsetzung, durch proprietäre Verschlüsselungstechnik „die Kommunikationen von Skype-Nutzern davor zu schützen, dass sie in die Hände von Hackern und Kriminellen fallen“[782], und „auf diese Art […] [dabei zu helfen], die Privatsphäre von Nutzern und die Integrität von Daten zu bewahren, die von einem Nutzer zu einem anderen gesendet werden“[783], spricht dies wiederum eher gegen das Vorhandensein einer bewusst von Skype in seiner Software vorgehaltenen *Backdoor*.[784]

Auch Stellungnahmen von offizieller Seite zu etwaigen Schnittpunkten für eine Zusammenarbeit mit VoIP-Diensteanbietern lassen darauf schließen, dass Hintertüren in VoIP-Programme (ebenso wie universelle Schlüssel, siehe oben) von den Anbietern nicht bereitgehalten werden und für Behörden insbesondere zu einer Nutzung zu strafprozessualen Zwecken nicht zur Verfügung stehen. So wurde seitens der Bundesregierung im Rahmen der Bundestagssitzung am 26.10.2011 mitgeteilt und zu Protokoll gegeben, dass es Skype im Falle direkter P2P-Kommunikation „nach derzeitigem Kenntnisstand der Bundesregierung schon aus technischen Gründen nicht möglich [ist], Inhaltsdaten den Justiz-, Strafvollzugs- oder Regierungsbehörden zur Verfügung zu stellen“[785]. So verweise Skype auch in seinem Informationsblatt „*Responding to Law Enforcement Records Requests*“[786] ausdrücklich darauf, dass es Skype auf entsprechende Anordnung hin ausschließlich möglich sei, bestimmte Bestandsdaten wie bspw. E-Mail-Adresse und Rufnummer des Teilnehmers[787] bereitzustellen sowie Auskunft über Verkehrs-

---

OverIP/Stellungnahmen/SkypeTechnologiesId714pdf.pdf?__blob=publicationFile (zuletzt aufgerufen 15.06.2012).

782 http://www.skype.com/intl/de/security/detailed-security/ (zuletzt aufgerufen 15.06.2012).

783 http://www.skype.com/intl/de/security/detailed-security/ (zuletzt aufgerufen 15.06.2012).

784 So auch Anm. *Bär*, MMR 2011, 691 (691 f.); in dieselbe Richtung auch Antwort der Bundesregierung vom 26.10.2011 (BT-PlPr. 17/135 16064 D); a. A. hingegen *Braun*/*Roggenkamp*, K&R 2011, 681 (685) m. w. N.; ebenso *Becker*/*Meinicke*, StV 2011, 50 (52).

785 Antwort des Parl. Staatssekretärs beim Bundesminister des Innern, *Bergner*, für die Bundesregierung im Rahmen der 135. Sitzung des Deutschen Bundestags am 26.10.2011, BT-PlPr. 17/135 16064 D; in diese Richtung bereits die Antwort des Parl. Staatssekretärs beim Bundesminister des Innern, *Schröder*, im Rahmen der 132. Sitzung des Deutschen Bundestages am 19.10.2011 (BT-PlPr. 17/132 15589 B), wonach es „bei der Peer-to-Peer-Kommunikation […] keine andere Möglichkeit [gibt], als an den Computer heranzugehen und die Quellen-Telekommunikationsüberwachung durchzuführen“ (15589 B).

786 Abrufbar unter http://cryptome.org/isp-spy/skype-spy.pdf (zuletzt aufgerufen 15.06.2012).

787 „In response to a subpoena or other court order, Skype will provide: […] Registration information provided at time of account registration […] E-mail address

daten wie bspw. Zielrufnummer für jedes Gespräch unter Beteiligung öffentlicher Telefonnetze (PSTN)[788] zu erteilen.[789] Gesprächsinhalte hingegen würden (mangels technischer Möglichkeit) von Skype in keinem Fall zur Verfügung gestellt[790], selbst dann nicht, wenn bspw. Kommunikationsinhalte als Sprachnachricht (*Voicemail*) auf Servern von Skype[791] abgelegt sind.[792] Anders stelle es sich hinsichtlich etwaiger technischer Möglichkeit zur Ausleitung lediglich für die Inhalte aus den (seltener als die P2P-Funktion genutzten) *SkypeIn* bzw. *SkypeOut*-Kommunikationen[793] dar.[794]

Als weiterer Aspekt kommt hinzu, dass selbst wenn in Skype – entgegen dem offiziellen Kenntnisstand – tatsächlich eine solche bewusst eingerichtete

---

[…] All service and account information, including any billing address(es) provided, IP address (at each transaction), and complete transactional information" (Skype-Informationsblatt *Responding to Law Enforcement Records Requests*, abrufbar unter http://cryptome.org/isp-spy/skype-spy.pdf, zuletzt aufgerufen 15.06.2012).

788 „In response to a subpoena or other court order, Skype will provide: […] IP address at the time of registration […] Destination telephone numbers for any calls placed to the public switched telephone network (PSTN)", „Skype can provide records showing account creation, financial transaction and use of PSTN interconnections" (Skype-Informationsblatt *Responding to Law Enforcement Records Requests*, abrufbar unter http://cryptome.org/isp-spy/skype-spy.pdf, zuletzt aufgerufen 15.06.2012).

789 So die Antwort des Parl. Staatssekretärs beim Bundesminister des Innern, *Bergner*, im Rahmen der 135. Sitzung des Deutschen Bundestags am 26.10.2011, BT-PlPr. 17/135 16064 D.

790 „Skype can provide records showing account creation, financial transaction and use of PSTN interconnections […]"; „Calls, IMs and other activities between Skype users do not create billing records" (Skype-Informationsblatt *Responding to Law Enforcement Records Requests*, abrufbar unter http://cryptome.org/isp-spy/skype-spy.pdf, zuletzt aufgerufen 15.01.2012).

791 Wobei für den Dienst *Skype-Voicemail* unterschiedliche Aussagen darüber existieren, ob dieser über einen Dienst-Server abgewickelt wird, vgl. einerseits http://sky2peer.com/de/article/677 (zuletzt aufgerufen 15.06.2012); in dieselbe Richtung http://www.pcwelt.de/news/Skype-Anrufbeantworter-im-Betatest-486874.html (zuletzt aufgerufen 15.06.2012); andererseits beruft sich Skype in einem Informationsblatt über die Beantwortung von Anfragen von Strafverfolgungsbehörden darauf, dass sein System so entworfen sei, dass Voicemail jedenfalls nicht zentral gespeichert werde („not centrally stored"), vgl. Skype-Informationsblatt *Responding to Law Enforcement Records Requests*, abrufbar unter http://cryptome.org/isp-spy/skype-spy.pdf (zuletzt aufgerufen 15.06.2012).

792 So die Antwort des Parl. Staatssekretärs beim Bundesminister des Innern, *Bergner*, im Rahmen der 135. Sitzung des Deutschen Bundestags am 26.10.2011, BT-PlPr. 17/135 16064 D.

793 Für Einzelheiten zu *SkypeIn* bzw. *SkypeOut* und deren Überwachbarkeit, siehe auch 1. Teil A.I.2.c).

794 So die Antwort des Parl. Staatssekretärs beim Bundesminister des Innern, *Bergner*, im Rahmen der 135. Sitzung des Deutschen Bundestags am 26.10.2011, BT-PlPr. 17/135 16064 D.

Schwachstelle im Programm in Form einer technischen Hintertür[795] vorhanden sein oder aber künftig eingebaut werden sollte, dies den Ermittlungsbehörden – wie auch bei einem Schlüssel für die Skype-Verschlüsselung – dann wenig nützen würde, wenn sich bspw. Tatverdächtige des VoIP-Programms eines der zahlreichen anderen Anbieter von (i. d. R. kostenloser) VoIP-Software bedienen, für die eine zu Strafverfolgungszwecken eingerichtete Backdoor im Zeitpunkt der Ermittlungen nicht zur Verfügung steht. Auch in diesen Fällen wäre damit eine erfolgreiche Strafverfolgung und Straftatenaufklärung letztlich von dem (zufälligen) Umstand abhängig, welche konkrete VoIP-Software die Zielperson zum Führen P2P-verbundener VoIP-Kommunikation benutzt, ob in diese eine Hintertür besteht und ob der jeweilige Anbieter auch dazu bereit ist, diese den Behörden zur Verfügung zu stellen, was jedoch wiederum gegen die Eignung einer technischen Hintertüre als gleich geeignete Alternative zu der Installation einer Überwachungssoftware für die Überwachung verschlüsselter VoIP-Kommunikation spricht[796].

Ein diesen Problemstellungen eventuell abhelfender *genereller* Einbau von staatlich nutzbaren Hintertüren – soweit technisch möglich – in Betriebssysteme, Anwendungsprogramme oder sonstige Produkte und Systeme der IT-Infrastruktur findet gegenwärtig nicht statt. Nicht zuletzt mit Blick auf (i. d. R.) weltweit agierende Anbieter derartiger Produkte und Anwendungen, erscheint es mehr als fraglich, ob ein genereller, gesetzlich vorgeschriebener Einbau technischer Hintertüren in private Softwareprodukte, also bewusst eingebaute Schwachstellen und damit potentielle Sicherheitslücken, politisch wie auch mit Blick auf entsprechende grundrechtliche Freiheiten der betroffenen Hersteller bzw. Anbieter von VoIP-Programmen – für inländische juristische Personen mithin aus Art. 19 III GG i. V. m. Art. 14 I GG[797] – rechtlich (insbesondere auch international[798]) und prak-

---

795 Vgl. auch Bundesministerium des Innern, Fragenkatalog SPD, S. 9, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

796 Zumal nach zutr. Auffassung des Bundesministeriums des Innern „das Nutzen nur einer Sicherheitslücke für alle Maßnahmen […] zudem ein stark risikobehaftetes Vorgehen [wäre], da alle Maßnahmen entdeckt würden, wenn diese Sicherheitslücke identifiziert würde“ (Fragenkatalog SPD, S. 9, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf, zuletzt aufgerufen 15.06.2012).

797 In Gestalt des *Rechtes am eingerichteten und ausgeübten Gewerbebetrieb*; auch Verfassungen und Rechtsordnungen anderer Länder werden indes vergleichbare grundrechtliche Freiheiten und Rechtsinstitute für ihrem Geltungsbereich unterfallende juristische Personen vorhalten.

798 Gerade angesichts der Tatsache, dass die gegenwärtig am Markt befindlichen Anbieter von softwarebasierter VoIP ihren Sitz regelmäßig im (nicht nur europäischen) Ausland haben.

tisch überhaupt durchsetzbar wäre[799], darüber hinaus aber auch mit Blick auf die (auch staatlich zu unterstützende und zu fördernde[800]) Software- und Systemsicherheit sinnvoll bzw. wünschenswert ist. Ein standardmäßiger Einbau von technischen Hintertüren, insbesondere in Verschlüsselungsprodukte, ist staatlichen Angaben zufolge jedenfalls derzeit politisch nicht gewollt.[801] Laut Stellungnahme des Bundesministeriums des Innern herrsche „Einigkeit darüber, dass kein Interesse daran besteht, ‚Hintertüren' in Betriebs- und Anwendungssysteme einzubauen"[802], da „solche ‚Hintertüren' beziehungsweise absichtlich eingebaute Schwachstellen in Soft- und Hardware […] nicht nur für die IT-Sicherheit, sondern auch für die deutsche IT-Wirtschaft fatale Konsequenzen [hätten]"[803]. Überdies sei „der Einbau von ‚Hintertüren' in deutsche Produkte […] schon allein aufgrund der einfachen Ausweichmöglichkeit auf ausländische Produkte, die nicht dem Einflussbereich der deutschen Gesetzgebung unterliegen, unsinnig"[804]. Auch die Anbieter betroffener Systeme und Programme stehen deshalb einer generellen Integration derartiger „Hintertüren" in ihre Software weitgehend kritisch gegenüber, als diese befürchten, dass die Einrichtung technischer Hintertüren vor allem auch zu verstärkten „Einbrüchen" in die Software durch unberechtigte Dritte führen könnte.[805] Ein solcher genereller Einbau – soweit gesetzlich überhaupt durchsetzbar – würde demnach die Sicherheit in der Informationstechnik in erheblicher Weise beeinträchtigen und den

---

799 In diese Richtung auch *Buermeyer*, HRRS 2007, 154 (163), wonach die Möglichkeit der Verpflichtung von Softwareanbietern zur Integration von Schnittstellen bspw. in Betriebssystemen zur Ermöglichung eines unerkannten staatlichen Zugriffs auf Computersysteme „praktisch kaum gangbar" (163) erscheint.

800 Vgl. insoweit auch § 3 I BSIG.

801 Vgl. Bundesministerium des Innern, Fragenkatalog BMJ, S. 19, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012); vgl. ebenso Bundesministerium des Innern, Fragenkatalog SPD, S. 9, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

802 Bundesministerium des Innern, Fragenkatalog SPD, S. 9, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

803 Bundesministerium des Innern, Fragenkatalog SPD, S. 9, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

804 Bundesministerium des Innern, Fragenkatalog SPD, S. 9, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

805 Vgl. Stellungnahme Skype im Rahmen der Anhörung durch die Bundesnetzagentur im Jahr 2004, S. 16, abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Stellungnahmen/SkypeTechnologiesId714pdf.pdf?__blob=publicationFile (zuletzt aufgerufen 15.06.2012).

Missbrauchsgefahren und Einfallsmöglichkeiten in informationstechnische System – dann gar „standardmäßig" – in einer Weise Tür und Tor öffnen, wie dies von Kritikern des staatlichen Einsatzes von Überwachungssoftware gegen den (lediglich punktuell stattfindenden) Zugriff auf informationstechnische Systeme im Rahmen derartiger staatlicher Ermittlungsmaßnahmen mitunter in regelrechten „Schreckensszenarien" skizziert wird.[806]

Unter dem Kriterium des „milderen Mittels" stellt sich damit aber auch die Frage, ob die Einrichtung und Nutzung von Hintertüren in VoIP-Programmen de facto tatsächlich zu einem wesentlich grundrechtsschonenderen Eingriff führen würde. Der Einbau von Hintertüren in Programme ist, wie oben aufgezeigt, mit deutlichen Risiken für die Sicherheit in der Informationstechnik verbunden. Mit der Installation einer VoIP-Software, welche eine solche Hintertür vorhält, wird in das jeweilige informationstechnische System ein Programm integriert, welches eine über die technische Hintertür von außen ansprech- und nutzbare Abhörschnittstelle bereithalten würde. Zur Nutzung einer solchen Abhörschnittstelle bedürfte es dann eines heimlichen „Eintretens" in das jeweilige VoIP-Programm in Form des Ansprechens und Einloggens in die auf dem Zielgerät befindliche Software von außen. Hierdurch würde jedoch auch bei der Nutzung einer technischen Hintertüre in das betroffene informationstechnische System aus der Ferne eingegriffen werden, da die über die „Backdoor" angesprochene VoIP-Software auf diesem installiert und in das System und die Systemprozesse und -abläufe integriert ist. Dieser Umstand ist im Rahmen der Beurteilung des Vorliegens etwaiger *milderer* Alternativen somit ebenfalls zu berücksichtigen, zumal eine solche „von Haus aus" eingebaute Schwachstelle in einem installierten Programm – wie sie eine generell und dauerhaft vorhandene technische Hintertür, die prinzipiell mit dem richtigen technischen Equipment und Knowhow von jedermann angesprochen werden kann, darstellt[807] – durchaus als Einfallstor in das gesamtes System ausgenutzt werden könnte, was ebenso wie die Existenz von Schlüsseln in einem Spannungsverhältnis mit den Aspekten der IT-Sicherheit und des Daten-

---

806 Ob ein genereller Einbau von Hintertüren in Softwareprodukte deshalb tatsächlich als Alternative, noch dazu als mildere, zur Quellen-TKÜ in Frage kommen und gewollt sein kann, darf bezweifelt werden; man stelle sich nur den Aufschrei vor, wenn Hersteller künftig (gesetzlich verpflichtet) tatsächlich in sämtliche Softwareprodukte (einschließlich Verschlüsselungsprogramme etc.) standardmäßig Hintertüren, also letztlich Schwachstellen und auch potentielle Einfallstore für unbefugte (kriminelle) Dritte, einbauen würden (müssten); zu den Folgefragen und insbesondere Missbrauchsgefahren eines Einbaus von Hintertüren, siehe auch die zutr. Ausführungen bei Anm. *Vogel*/*Brodowski*, StV 2011, 632 (633), Fn. 6.

807 Vgl. auch Bundesministerium des Innern, Fragenkatalog SPD, S. 9, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

schutzes stehen würde und jedenfalls kein zwingend *milderes* Mittel zur (zeitweisen) Infiltration des Zielsystem mit einer staatlichen Überwachungssoftware abgibt.

Im Ergebnis lässt sich somit bezüglich der Frage der *Erforderlichkeit* festhalten, dass für die Infiltration des Systems mit einer Überwachungssoftware zur Ermöglichung einer Überwachung und Aufzeichnung verschlüsselt übermittelter VoIP-Kommunikation demnach (jedenfalls gegenwärtig) keine gleich geeignete, den Betroffenen insgesamt weniger belastende Alternative in Form des Verschaffen eines (universellen) Schlüssels oder der Nutzung einer Hintertür in die VoIP-Software zur Verfügung steht, um derartige Telekommunikation einer staatlichen Überwachung zu strafprozessualen Zwecken zugänglich zu machen.

c) Angemessenheit?

Des Weiteren müsste die erforderliche technische Infiltration des Zielsystems mit einer Überwachungssoftware zum Zwecke der Überwachung und Aufzeichnung von (verschlüsselt übermittelter) IP-basierter Telekommunikation angemessen, also verhältnismäßig im engeren Sinne sein, um sich auf eine Annexkompetenz zur Primärbefugnis aus § 100a I StPO stützen zu können. Dies ist jedenfalls dann der Fall, wenn die Begleitmaßnahme – im Verhältnis zur Grundrechtsbeeinträchtigung, die mit der Primärmaßnahme einhergeht – nur *verhältnismäßig geringfügige Beeinträchtigungen* der Rechte des Betroffenen mit sich bringt.[808]

Das Gebot der Verhältnismäßigkeit i. e. S. verlangt, dass „die Schwere des Eingriffs bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe stehen darf“[809]. Das heimliche Installieren einer Überwachungssoftware würde jedenfalls dann ein angemessenes Mittel darstellen, wenn es sich um eine verhältnismäßig geringfügige Beeinträchtigung grundrechtlich geschützter Interessen handelt, da derartige Beeinträchtigungen dem Betroffenen mit Blick auf den hohen Stellenwert des staatlichen Strafanspruchs zugemutet werden können[810]. Die Frage der

---

[808] Vgl. zu diesem Kriterium auch BGH-Ermittlungsrichter NStZ 1998, 157 (158) sowie BGH-Ermittlungsrichter NStZ 2005, 278 (278); auch BGH NJW 2001, 1658 (1659); vgl. insoweit LG Hamburg, MMR 2008, 423 (424 f.); vgl. insoweit auch AG Hamburg, CR 2010, 249 (250); i. E. auch LG Hamburg, MMR 2011, 693 (694), wobei die Kammer auch Ansatzpunkte dafür sieht, die *verhältnismäßig geringfügige Beeinträchtigung* als Kriterium für die Bejahung einer Annexkompetenz in Frage zu stellen.

[809] BVerfG NJW 2008, 822 (829); auch BVerfG NJW 1994, 1577 (1579); BVerfG NJW 2004, 999 (1012); BVerfG NJW 2005, 2603 (2609); st. Rspr.

[810] So BGH-Ermittlungsrichter NStZ 1998, 157 (158).

„Geringfügigkeit“ ist hierbei im Zusammenhang mit der Grundrechtsbeeinträchtigung durch die Primärmaßnahme zu sehen.[811] Dies bedeutet für den hier behandelten Fall der Quellen-TKÜ, dass die für den Maßnahmebetroffenen entstehenden Nachteile des heimlichen Einbringens (wie auch späteren Entfernens) einer Überwachungssoftware in ein informationstechnisches System nicht außer Verhältnis zu den daraus resultierenden Vorteilen in Form der Ermöglichung einer Überwachung auch von verschlüsselt übermittelter Internettelefonie zum Zwecke der Strafverfolgung und Straftatenaufklärung stehen dürfen. Hierbei ist v. a. darauf abzustellen, ob die Intensität des mit der Begleitmaßnahme verbundenen Eingriffs insgesamt hinter dem Gewicht des primären Eingriffs in Form der sich anschließenden Überwachung und Aufzeichnung der geführten VoIP-Kommunikation zurückbleibt[812]:

Zur Frage, ob das heimliche Infiltrieren eines informationstechnischen Systems mit einer Überwachungssoftware zum Zwecke der Telekommunikationsüberwachung nur verhältnismäßig geringfügig in die Rechte betroffener Nutzer eingreift, werden teilweise generell zur heimlichen Installation und Verwendung von „Schadsoftware“ auf fremden Systemen durch staatliche Behörden vor allem Bedenken hinsichtlich der *Datensicherheit* und des *Missbrauchsschutzes* geäußert, die zu einer Beeinträchtigung des Betroffenen führen können:

– So wird vorgetragen, dass durch das Einbringen, das Verwenden sowie das anschließende Entfernen der Überwachungssoftware das System, sein Datenbestand, aber auch vorhandene Sicherheitsvorkehrungen (installierte Antiviren-Programme, Firewalls etc.) manipuliert würden. Hierdurch werde die Gefahr einer Veränderung von Daten[813] wie auch einer dauerhaften Schädigung bzw. Veränderung des betroffenen Zielsystems geschaffen.[814]
– Des Weiteren bestehen auch Bedenken, ob es sich ausschließen lässt, dass unbeteiligte Personen versehentlich vom Einbringen der Überwachungssoftware betroffen werden könnten.[815]

---

811 Vgl. BGH-Ermittlungsrichter NStZ 1998, 157 (158) m. w. N.

812 Vgl. auch LG Hamburg, MMR 2011, 693 (694).

813 Generell zur Frage der Verwertbarkeit von Erkenntnissen unter computerforensischen Gesichtspunkten, siehe 2. Teil A.III.3.

814 Vgl. *Buermeyer*/*Bäcker*, HRRS 2009, 433 (439) m. w. N.; vgl. hierzu auch Fragen 9 ff., 24 u. 25, Fragenkatalog SPD, S. 9 ff., 14, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012), sowie Fragenkatalog BMJ, S. 20, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012).

815 Vgl. hierzu auch Frage 37, Fragenkatalog SPD, S. 19, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

– Zudem wird auch die Gefahr des Missbrauchs einer solchen Überwachungssoftware durch Dritte gesehen. So bestehen Bedenken, ob nicht Dritte die Software isolieren und die Überwachungsmöglichkeiten für eigene Interessen zweckentfremden könnten.[816]

– Aber auch die Frage der Beschränkbarkeit des Zugriffs mittels einer solchen Software auf den in der Anordnung festgelegten Umfang, d. h. ausschließlich auf laufende Telekommunikation, wird kritisch hinterfragt, insbesondere da Überwachungsprogramme grds. auch über Nachladefunktionen verfügen können, die das Risiko in sich bergen, dass technisch jederzeit weitergehende Überwachungsfunktionen in der Software implementiert werden, die über ein Überwachen laufender Telekommunikation hinaus auch ein Ausspähen des Systems an sich und seiner Speichermedien ermöglichen.[817]

Nach Ansicht derjenigen Stimmen, die sich gegen die Annahme einer Annexkompetenz zu § 100a I StPO für das heimliche Einbringen der Überwachungssoftware aussprechen, seien deshalb derartige Beeinträchtigungen nicht mehr als verhältnismäßig geringfügig anzusehen[818], da der Begleiteingriff der Infiltration des Zielsystems bspw. nach Auffassung von *Wolter* „mit der Hauptmaßnahme von der Eingriffstiefe her auf einer Stufe stünde, wenn ihn nicht sogar überträfe“[819] sowie nach Auffassung des *AG Hamburg* als „gravierende Grenzverletzung zwischen Staat und Einzelnem zu werten“[820] sei. Hierfür ließen sich vor allem auch die Feststellungen des BVerfG im Rahmen seiner Entscheidung vom 27.02.2008 zu den mit dem Infiltrieren eines informationstechnischen Systems verbundenen Gefährdungen[821] heranziehen.[822] Nach Auffassung des *AG Hamburg* bestehe die Grenzverletzung gerade darin, „dass der Staat von außen auf ein System

---

816 In diese Richtung bspw. *Braun*/*Roggenkamp*, K&R 2011, 681 (682); vgl. hierzu auch Fragen 16 ff., Fragenkatalog SPD, S. 11 f., abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012), sowie Fragenkatalog BMJ, S. 21, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012).

817 Vgl. hierzu *Braun*/*Roggenkamp*, K&R 2011, 681 (682); auch *Buermeyer*, http://ijure.org/wp/archives/756 (zuletzt aufgerufen 15.06.2012); wohl auch Anm. *Brodowski*, JR 2011, 533 (536).

818 So i. E. SK – *Wolter*, StPO, § 100a, Rn. 29; *Buermeyer*/*Bäcker*, HRRS 2009, 433 (439); AG Hamburg, CR 2010, 249 (251); i. E. auch LG Hamburg, MMR 2008, 423 (425); a. A. mittlerweile jedoch LG Hamburg, MMR 2011, 693 (695).

819 SK – *Wolter*, StPO, § 100a, Rn. 29.

820 AG Hamburg, CR 2010, 249 (251).

821 Vgl. hierzu BVerfG NJW 2008, 822 (825 f.).

822 Vgl. bspw. *Buermeyer*, http://ijure.org/wp/archives/756 (zuletzt aufgerufen 15.06.2012).

zugreift, auf dem sich eine Vielzahl von Daten mit Bezug zu den persönlichen Verhältnissen, den sozialen Kontakten und ausgeübten Tätigkeiten des Nutzers finden können“[823]. Der Nutzer eines komplexen informationstechnischen Systems habe „daher einen Anspruch auf Achtung der Vertraulichkeit und Integrität des von ihm genutzten Systems“[824]. Wenngleich die Quellen-TKÜ das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht unmittelbar betreffe, so sei dennoch „das Schutzinteresse an der Unverletzlichkeit des genutzten Systems zu berücksichtigen“.[825] Gerade „angesichts der Sensibilität und Fülle, die der Datenbestand […] aufweisen kann und angesichts der weitreichenden Rückschlüsse auf die Persönlichkeit seines Nutzers, die dieser Datenbestand ermöglichen kann“, sei bereits das Infiltrieren des Systems als ein schwerwiegender Grundrechtseingriff zu werten.[826] Daher scheitere die Zulässigkeit der Infiltration des Systems „unabhängig von der Frage der Typizität jedenfalls an der zusätzlich erforderlichen Verhältnismäßigkeitsprüfung“[827].

Derartige Bedenken werden von gegenläufigen Auffassungen v. a. in der Rspr.[828] wie auch von offizieller Seite damit zurückgewiesen, dass Überwachungsprogramme – unabhängig davon, ob diese nun zum Zwecke der Online-Durchsuchung oder der Quellen-TKÜ hergestellt werden[829] – generell so entwickelt werden können, dass vor allem durch aufgestellte *Designkriterien* und dem Stand der Technik entsprechende *Sicherheitsstandards* sowohl die Vorgaben in der Anordnung in Bezug auf die Reichweite des Zugriffs eingehalten als auch die genannten Risiken möglicher Beeinträchtigungen für Betroffene wie auch unbeteiligte Dritte bereits im Vorfeld weitestgehend ausgeschlossen werden[830]:

– Eine Betroffenheit unbeteiligter Personen könne bei staatlicher Überwachungssoftware durch „die Rückmeldung einer eindeutigen Identifikation

---

823 AG Hamburg, CR 2010, 249 (251).

824 AG Hamburg, CR 2010, 249 (251).

825 AG Hamburg, CR 2010, 249 (252); zur Grundrechtsrelevanz der Sekundärmaßnahmen, siehe 2. Teil B.I.1. u. II.

826 So AG Hamburg, CR 2010, 249 (252); ebenso LG Hamburg, MMR 2008, 423 (425); a. A. nunmehr LG Hamburg, MMR 2011, 693 (695).

827 AG Hamburg, CR 2010, 249 (251).

828 Vgl. bspw. LG Hamburg, MMR 2011, 693 (695).

829 Da die Programme grds. auf vergleichbaren Programmierungskomponenten und Designkriterien aufbauen und sich insoweit dieselben Anforderungen an Datensicherheit und Missbrauchsschutz stellen, siehe hierzu auch 1. Teil A.II.2.a).

830 Vgl. Bundesministerium des Innern, Fragenkatalog BMJ, S. 20, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012).

des Zielsystems“[831] und einen „in der Regel erfolgenden Abgleich der Aktivitäten des Zielsystems durch eine flankierende [„klassische“[832], Anm. d. Verf.] Telekommunikationsüberwachung“[833] ausgeschlossen werden. Überwachungssoftware identifiziere das Zielsystem durch Verifizierung der technischen Systemparameter[834], anhand derer die Software bereits im Vorfeld „maßgeschneidert“ für den Einsatz auf dem konkreten Zielsystem angefertigt wurde[835]. Durch derartige Maßnahmen werde der Einsatz der Überwachungssoftware „auf dem ‚richtigen‘ Zielsystem gewährleistet“[836].

– Des Weiteren lasse sich Überwachungssoftware auf ihre Fähigkeit zur Überwindung der auf dem jeweiligen System installierten Sicherheitseinrichtungen hin überprüfen und ggf. entsprechend modifizieren.[837] Staatlichen Angaben zufolge sei bei der Verwendung von Überwachungssoftware auch „nicht vorgesehen, die auf dem System befindlichen Sicherheitssysteme auszuschalten“[838], sodass dieses wegen der heimlich eingeschleusten Überwachungssoftware bspw. gegenüber den allgemeinen Gefahren des Internets schutzlos wäre. Derartige Überwachungssoftware ziele auf ein Überwinden der Sicherheitseinrichtungen ab, mit ihr würden aber keine zusätzlichen (Einfalls-)Tore für Schad-/Spionageprogramme

---

831 Bundesministerium des Innern, Fragenkatalog SPD, S. 19, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012) zu *Remote Forensic Software*, gilt für Quellen-TKÜ-Software insoweit entsprechend.

832 Auch zur Vorbereitung von Maßnahmen der Quellen-TKÜ; hier bedarf es i. d. R. einer gewissen Vorlaufzeit zur Durchführung von Ermittlungen insbesondere zum Zwecke der Erhebung der technischen Parameter des Zielsystems; siehe hierzu auch 1. Teil A.II.4.a)aa).

833 Bundesministerium des Innern, Fragenkatalog SPD, S. 19, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

834 Vgl. Antwort des Bayerischen Staatsministeriums des Innern, LT-Drs. 16/10469, S. 2, zu bislang durch das BayLKA eingesetzter Quellen-TKÜ-Software.

835 Für Einzelheiten hierzu, siehe 1. Teil A.II.3.b) u. 4.a)aa).

836 Bundesministerium des Innern, Fragenkatalog SPD, S. 19, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

837 Vgl.Bundesministerium des Innern, Fragenkatalog SPD, S. 12, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012); in diese Richtung auch *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11.2010; vgl. auch die Antwort des Bayerischen Staatsministeriums des Innern, LT-Drs. 16/10082, S. 8.

838 Bundesministerium des Innern, Fragenkatalog SPD, S. 12, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

Dritter geöffnet.[839] Die Software lasse sich so entwickelt, „dass von ihr nach dem aktuellen Stand der Technik keine Schadfunktionen ausgehen“[840]. Zwar nehme „jedes Programm, das in eine Systemumgebung eingebracht wird, […] Änderungen an der Systemkonfiguration vor“[841], diese könnten jedoch durch „Deinstallationsroutinen beim Löschvorgang rückgängig gemacht [werden]“[842]. Auch Instabilitäten auf dem Zielsystem müssen staatlichen Angaben zufolge durch den Einsatz von Überwachungssoftware nicht zwingend verursacht werden.[843]

– Ebenso würden sich bei der Verwendung von Überwachungssoftware etwaige Beeinträchtigungen der Rechen- und Speicherkapazität des betroffenen Zielsystems sowie etwaige Verlangsamungen der Datenverbindung über das Internet in einer für den betroffenen Nutzer kaum wahrnehmbaren Größenordnung bewegen, da sich diese im Wesentlichen lediglich auf den Bedienungskomfort des Zielsystems auswirken.[844]

– Ein über die Überwachung laufender Telekommunikationsvorgänge hinausgehender (bewusster oder versehentlicher) Zugriff auf sonstige auf den Speichermedien des Systems vorhandene Dateien wie auch eine Ausforschung des Systems an sich und der dort ablaufenden Vorgänge könne ebenfalls im Vorgeld im Rahmen der Softwareerstellung verhindert werden. Die Überwachungssoftware sei so konzipierbar und konfigurierbar, dass ausschließlich Daten aus laufenden Telekommunikationsvorgängen erfasst würden.[845] Die jeweils individuellen Softwarelösungen würden vor

---

[839] Vgl. Bundesministerium des Innern, Fragenkatalog SPD, S. 12, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012); zumal die zur Infiltration (aus-)genutzten Zugriffsmöglichkeiten auch ohne die staatlichen Aktivitäten (fachkundigen) Dritten wohl gleichfalls zur Verfügung stehen dürften, vgl. auch *Sieber*, Stellungnahme zu dem Fragenkatalog des BVerfG in dem Verfahren 1 BvR 370/07, S. 18, abrufbar unter http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf (zuletzt aufgerufen 15.06.2012).

[840] Bundesministerium des Innern, Fragenkatalog SPD, S. 12, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

[841] Bundesministerium des Innern, Fragenkatalog SPD, S. 20, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

[842] Bundesministerium des Innern, Fragenkatalog SPD, S. 20, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

[843] Vgl. Bundesministerium des Innern, Fragenkatalog SPD, S. 13, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

[844] Vgl. LG Hamburg, MMR 2011, 693 (695).

der Einbringung in das System stets umfangreichen technischen Funktionsprüfungen im Rahmen eines Qualitätssicherungsprozesses in jedem Einzelfall unterzogen, wodurch sichergestellt und protokolliert werde, dass deren jeweiliger Funktionsumfang dem richterlichen Beschluss, welcher der Maßnahme zugrunde liegt, entspricht.[846]

– Soweit teilweise im Zusammenhang mit der Reichweite des technischen Zugriffs der Überwachungssoftware auch das regelmäßige Vorhandensein einer Nachladefunktion kritisiert wird, stehe dem das Bedürfnis für eine solche Funktion zum Zwecke der Sicherstellung einer verlässlichen Überwachbarkeit entgegen. Denn eine solche Nachladefunktion sei notwendig, um die Überwachungssoftware an Veränderungen des Zielsystems, wie insbesondere Systemaktualisierungen, an Versionsänderungen der jeweiligen VoIP-Software aber auch an Aktualisierungen der auf dem System vorhandenen Antiviren/Firewallprogramme u. ä. anpassen zu können.[847]

– Zudem werde der Einsatz von Überwachungssoftware entsprechend umfangreich und transparent dokumentiert, womit sich eine etwaige Manipulation des Zielsystems wie auch eine Verfälschung dessen Datenbestan-

---

[845] So *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11.2010; ebenso die Antwort der Bundesregierung, BT-Drs. 17/7760, S. 5; in dieselbe Richtung auch die Antwort des Bayerischen Staatsministeriums des Innern, LT-Drs. 16/10082, S. 2 u. 3; auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, *Schaar*, widerspricht insoweit kritischen Stimmen, wonach der Einsatz von Überwachungsprogrammen grds. ungeeignet sei, weil diese stets die technische Möglichkeit zum Ausspähen des Systems eröffnen würden, vgl. *Höll*, „Gefährliche Grauzone", Süddeutsche Zeitung vom 13.10.2011, S. 6; nach Einschätzung von *Schaar* sei „es […] durchaus möglich, Programme einzusetzen, die dem Urteil des Bundesverfassungsgerichts von 2008 entsprechen", zitiert nach *Höll*, in: „‚Gefährliche Grauzone'", Süddeutsche Zeitung vom 13.10.2011, S. 6; a. A. hingegen *Buermeyer*/*Bäcker*, HRRS 2009, 433 (439); infrage stellend auch *Albrecht*/*Dienst*, JurPC Web-Dok. 5/2012, Abs. 27 f.; für Einzelheiten zur Erstellung und Konfiguration der Überwachungssoftware, siehe 1. Teil A.II.3.b).

[846] So die Antwort des Bayerischen Staatsministeriums des Innern, LT-Drs. 16/10082, S. 8; in diese Richtung auch die Antwort der Bundesregierung, BT-Drs. 17/7760, S. 5.

[847] Vgl. Antwort der Bundesregierung, BT-Drs. 17/7760, S. 8; in dieselbe Richtung auch die Antwort des Bayerischen Staatsministeriums des Innern, LT-Drs. 16/10469, S. 2; auch *Friedrich*, Bundesminister des Innern („Wir brauchen diese Nachladefunktionen, um uns den normalen Updates auf dem Zielcomputer anpassen zu können. Aber auch hier gibt es die gleichen Sicherungen wie beim ersten Aufspielen der Software."), zitiert nach *Hoffmann*/*Tomik*, in: „‚Es gibt keine rechtliche Grauzone'", faz.net vom 15.10.2011, abrufbar unter http://www.faz.net/aktuell/politik/iminterview-bundesinnenminister-friedrich-csu-es-gibt-keine-rechtliche-grauzone-11494291.html (zuletzt aufgerufen 15.06.2012).

des durch forensische Untersuchung[848] auch noch im Nachhinein überprüfen und belegen lasse.[849] Auch durch eine Hinterlegung des Quellcodes[850] der konkret eingesetzten Überwachungssoftware, z. B. beim anordnenden Gericht, könne zusätzlich belegt werden, dass die Überwachungssoftware keine Daten im Zielsystem frei platzieren kann, wodurch sich etwaige Vorwürfe einer Manipulation von Daten auf dem Zielsystem widerlegen ließen.[851]

– Des Weiteren lasse sich im Rahmen der Designkriterien für Überwachungsprogramme zum Schutz vor Missbrauch durch (nichtstaatliche) Dritte u. a. dafür Sorge tragen, „dass die Software keine eigenen Verbreitungsroutinen […] beinhaltet“[852]. Hierzu werde insbesondere „sichergestellt, dass die Software nicht ohne erheblichen Aufwand dazu veranlasst werden kann, an einen anderen Server als den von den Sicherheitsbehörden benutzten Server zurückzumelden“[853] sowie „dass die Software weder von außen erkannt noch angesprochen werden kann“[854]. Gemäß Antwort des Bayerischen Staatsministeriums des Innern vom 17.01.2012 in Bezug auf durch das BayLKA verwendete Überwachungssoftware ist „eine Kommunikation mit der Quellen-TKÜ-Software von anderen als der in der Quellen-TKÜ-Software festgelegten IP-Adresse […] nicht möglich“[855]. Die Software sei darüber hinaus „mit einem elektronischen Fingerabdruck und mit Authentifizierungsprotokollen gegen unberechtigte Nutzung gesichert“[856]. Auch das Risiko einer Extraktion der Software durch den

---

848 Generell zur Frage der Verwertbarkeit von Erkenntnissen unter computer-forensischen Gesichtspunkten, siehe 2. Teil A.III.3.

849 Vgl. Bundesministerium des Innern, Fragenkatalog BMJ, S. 20, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012).

850 Auch *Quelltext*, bezeichnet den in einer Programmiersprache geschriebenen Text eines Computerprogramms, bestehend aus einer Abfolge von Befehlen, vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 192.

851 Vgl. Bundesministerium des Innern, Fragenkatalog SPD, S. 14, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

852 Bundesministerium des Innern, Fragenkatalog SPD, S. 6, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

853 Bundesministerium des Innern, Fragenkatalog SPD, S. 6, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

854 Bundesministerium des Innern, Fragenkatalog SPD, S. 7, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

855 Bayerisches Staatministerium des Innern, LT-Drs. 16/10607, S. 2.

856 Bayerisches Staatministerium des Innern, LT-Drs. 16/10607, S. 2.

Betroffenen zum Verwenden der Überwachungssoftware zu eigenen Zwecken könne insofern auf ein Mindestmaß begrenzt werden, als „eine Softwareextraktion […] voraussetzen [würde], dass eine Person vollumfänglich Kenntnisse über die Quellen-TKÜ-Software, ihren Funktionsumfang, ihre exakte Funktionsweise sowie ihre kryptografischen Schlüssel hat“[857]. Dem könne durch umfangreiche technische Sicherungs- und Kontrollmaßnahmen begegnet werden, welche „einem ständigen Qualitätssicherungs- und Optimierungsprozess“[858] unterliegen.[859]

Unabhängig davon, dass das Risiko eines Entdeckens/Identifizierens von Überwachungssoftware durch den Betroffenen wie auch Dritte deshalb „als gering einzustufen“[860] sei, wäre eine Analyse und Manipulation der jeweiligen Überwachungssoftware sowie deren Veränderung für eigene Zwecke aber nicht nur äußerst aufwendig, sondern zudem unnötig, da Softwareprodukte mit hohem Missbrauchspotential im Internet frei erhältlich seien.[861]

– Bei Beendigung von Überwachungsmaßnahmen ließen sich „alle Bestandteile […] restlos“[862] von dem Zielsystem wieder entfernen – auf Grund einprogrammierbarer Selbstdeinstallationsroutinen[863] sogar bei einem Kontaktabbruch mit dem Steuerungssystem der Überwachungssoftware.[864] Durch die Software selbst würden auch „keine weitergehenden Systembeeinträchtigungen“[865] erfolgen. Soweit im Zuge des Aufspielens

---

857 Bayerisches Staatministerium des Innern, LT-Drs. 16/10607, S. 2.

858 Bayerisches Staatministerium des Innern, LT-Drs. 16/10607, S. 2.

859 Vgl. Antwort des Bayerisches Staatministerium des Innern, LT-Drs. 16/10607, S. 2; in diese Richtung auch die Antwort der Bundesregierung, BT-Drs. 17/7760, S. 16.

860 Bundesministerium des Innern, Fragenkatalog SPD, S. 7, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

861 Vgl. Bundesministerium des Innern, Fragenkatalog SPD, S. 7, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012); vgl. auch Bundesministerium des Innern, Fragenkatalog BMJ, S. 21, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-online durchsuchung-BMJ.pdf (zuletzt aufgerufen 15.06.2012).

862 Bundesministerium des Innern, Fragenkatalog SPD, S. 16, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

863 Unter einer *Routine* wird im Bereich der Softwareprogrammierung eine bestimmte Programm(teil)funktion verstanden, vgl. http://www.duden.de/rechtschreibung/Routine (zuletzt aufgerufen 15.06.2012).

864 Vgl. Bundesministerium des Innern, Fragenkatalog SPD, S. 21, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

von Überwachungssoftware Änderungen an der Systemkonfiguration vorgenommen worden sein sollten, würden diese durch „Deinstallationsroutinen beim Löschvorgang rückgängig gemacht“[866]. Auch die Deinstallationsroutinen wirken sich hierbei nur auf die Überwachungssoftware selbst aus, nicht auf die Systemsicherheit.[867] Den vorgetragenen Bedenken, dass über ein während der Maßnahme generiertes *Backup*[868] des von der Überwachungssoftware kompromittierten Systems der (eigentlich schon rückgängig gemachte) „unterwanderte“ Zustand vor dem Entfernen der Software erneut hervorgerufen werden könnte[869], lasse sich durch „Einprogrammieren eines Verfalldatums und eines Zeitzählmechanismus“[870] Rechnung tragen, wodurch eine Selbstentfernung der Software „auch nach einem evt. Wiederaufsetzen des Systems“[871] eingeleitet werden könne. Derartige Mechanismen seien aber „auch der Unterbindung der Weiterverbreitung“[872] dienlich.

Nach Ansicht derjenigen Stimmen, die sich für eine Annexkompetenz des heimlichen Einbringens der Überwachungssoftware zu § 100a I StPO aussprechen, stellen die mit der vorherigen heimlichen Installation einer spezifisch auf die Überwachung laufender Telekommunikationsvorgänge ausgelegten Überwachungssoftware verbundenen Beeinträchtigungen unter Berücksichtigung der genannten Umstände im Vergleich zur Eingriffswirkung

---

865 Bundesministerium des Innern, Fragenkatalog SPD, S. 16, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

866 Bundesministerium des Innern, Fragenkatalog SPD, S. 20, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

867 Vgl. Bundesministerium des Innern, Fragenkatalog SPD, S. 18 f., abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

868 Zu Dt. „Sicherungskopie“ als Mittel zur Datensicherung und -wiederherstellung.

869 Vgl. hierzu Frage 30, Fragenkatalog SPD, S. 16, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

870 Bundesministerium des Innern, Fragenkatalog SPD, S. 16, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

871 Bundesministerium des Innern, Fragenkatalog SPD, S. 16, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

872 Bundesministerium des Innern, Fragenkatalog SPD, S. 16, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

der Primärmaßnahme deshalb keine überproportional ins Gewicht fallenden Eingriffe in die Rechte des Betroffenen dar.[873]

Nach *Bär* ließen sich die Anforderungen des BVerfG in Bezug auf den Schutz des Zielsystems durch entsprechende Maßnahmen erfüllen, und zwar „auch wenn die Installation von Fremdsoftware auf einem System zu technisch nicht vermeidbaren geringen Veränderungen im System führt“[874]. In der Praxis werde „vor einer Installation das entsprechende Zielsystem nachgestellt und durch eine Zertifizierung der eingesetzten Software sichergestellt, dass es zu keiner überschießenden Datenerhebung […] kommt“[875]. Nach Auffassung des *LG Hamburg* werde in technischer Hinsicht durch das heimliche Einschleusen einer die Überwachung und Ausleitung der TK-Daten an der Quelle durchführenden Überwachungssoftware nur eine „geringfügige Belastung der Rechen- und Speicherkapazität“[876] des betroffenen informationstechnischen Systems bewirkt. Auch deren anschließender Betrieb habe nur eine „je nach Datenmenge und Übertragungsgeschwindigkeit unterschiedlich ausfallende Verlangsamung der Internet-Datenverbindung“[877] zur Folge, was „im Wesentlichen den Bedienkomfort des genutzten Computers [betrifft] und […] sich regelmäßig in einer für den Nutzer kaum wahrnehmbaren Größenordnung [bewegt]“[878]. Auch der Auffassung, dass die heimliche Installation der Software als „gravierende Grenzverletzung zwischen Staat und Einzelnem“[879] zu einem als „schwerwiegend einzustufen[den]“[880] Eingriff führe, sei nicht zu folgen.[881] Denn gemäß den Feststellungen des BVerfG[882] sei „eine gesetzliche Ermächtigung, die sich auf eine staatliche Maßnahme beschränkt, durch welche die Inhalte und Umstände der laufenden Telekommunikation im Rechnernetz erhoben […] werden, allein an Art. 10 Abs. 1 GG zu messen ist“[883] und zwar „unabhängig davon […], ob die Maßnahme technisch auf der Übertragungsstrecke oder am Endgerät der Telekommunikation ansetzt“[884]. Die vom BVerfG

---

873 So bspw. LG Hamburg, MMR 2011, 693 (695); LG Landshut, MMR 2011, 690 (691); Anm. *Bär*, MMR 2011, 691 (692); Anm. *Bär*, MMR 2008, 425 (426 f.); BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 107 f.

874 Anm. *Bär*, MMR 2010, 267 (268).

875 Anm. *Bär*, MMR 2010, 267 (268).

876 LG Hamburg, MMR 2011, 693 (695).

877 LG Hamburg, MMR 2011, 693 (695).

878 LG Hamburg, MMR 2011, 693 (695).

879 AG Hamburg, CR 2010, 249 (251).

880 AG Hamburg, CR 2010, 249 (251).

881 So LG Hamburg, MMR 2011, 693 (695).

882 BVerfG NJW 2008, 822 (826).

883 LG Hamburg, MMR 2011, 693 (695).

884 LG Hamburg, MMR 2011, 693 (695).

hierfür neben technischen Vorkehrungen geforderten rechtlichen Vorgaben seien bereits in den strafprozessualen Vorschriften über die Telekommunikationsüberwachung enthalten, da „§ 100a StPO allein die Überwachung der ‚Telekommunikation', nicht aber sonstiger Daten für zulässig erklärt"[885], womit auch „eine den Schutzbereich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme betreffende Gefährdung"[886] ausgeschlossen sei. Hierfür seien „die entsprechenden Beschränkungen in der Funktion der eingesetzten Software […] durch zweckentsprechende Programmierung sicherzustellen"[887]. Um die Funktion der eingesetzten Computersoftware „anordnungsgemäß auf die Überwachung und Weiterleitung der von der gerichtlichen Anordnung nach § 100a StPO erfassten Telekommunikationsdaten zu beschränken"[888] und eine Erfassung sonstiger Daten oder eine sonstige unzulässige Datenmanipulation sicher auszuschließen, werde es deshalb regelmäßig angezeigt sein, „die genutzte Software entweder selbst fachkundig zu erstellen oder sie bei Ankauf von einem privaten Hersteller aus eigener technischer Sachkunde auf die Richtigkeit der Funktionsweise hin zu überprüfen"[889]. Hingegen habe die Überwachung zu unterbleiben, wenn „die Sicherstellung einer solchen Funktionsweise der eingesetzten Software nicht möglich ist"[890]. Insoweit handele es sich aber nur „um eine besondere Ausprägung des Grundsatzes, dass die Ermittlungsbehörden eine richterlich angeordnete strafprozessuale Maßnahme sorgfältig, rechtstreu und unter Beachtung der inhaltlichen Grenzen der Anordnung durchzuführen haben"[891].

Wie die Ausführungen zeigen, ist die Einordnung des Infiltrierens des Zielsystems mit einer Überwachungssoftware zum Zwecke der Überwachung von laufender Telekommunikation als *verhältnismäßig geringfügige* Begleitmaßnahme stark umstritten und im Wesentlichen von unterschiedlichen Auffassungen in Bezug auf technische Umstände und Anforderungen an das verwendete Überwachungsprogramm geprägt. Beide Ansichten argumentieren indes für „ihre Linie" mit nachvollziehbaren Gründen. Für die Beurteilung der verhältnismäßig geringfügigen Beeinträchtigung gilt es allerdings zu beachten, dass der damit verbundene Eingriff nicht an sich geringfügig sein muss, sondern im Vergleich (*verhältnismäßig* geringfügig) zur Beeinträchtigung des Betroffenen, die mit dem Primäreingriff verbunden

885 LG Hamburg, MMR 2011, 693 (696).
886 LG Hamburg, MMR 2011, 693 (696).
887 LG Hamburg, MMR 2011, 693 (696).
888 LG Hamburg, MMR 2011, 693 (696).
889 LG Hamburg, MMR 2011, 693 (696).
890 LG Hamburg, MMR 2011, 693 (696).
891 LG Hamburg, MMR 2011, 693 (696).

ist (hierzu nachfolgend). Die Einordnung als verhältnismäßig geringfügige Begleitmaßnahme im konkreten Einzelfall hängt freilich von der technischen Ausgestaltung der jeweiligen Überwachungssoftware ab. Für das Einbringen einer Überwachungssoftware, die (entsprechend der richterlichen Anordnung) indes so konfiguriert ist, dass ausschließlich laufende Telekommunikation erfasst wird, und die solche Funktionsweisen und Schutzvorkehrungen enthält, wie sie von staatlicher Seite als technisch möglich vorgetragen werden (vgl. oben), ist die Annahme des Vorliegens eines im Verhältnis zum Primäreingriff nur geringfügigen Begleiteingriffs durchaus gerechtfertigt und mithin auch das Stützen auf eine Annexkompetenz zu § 100a I StPO zulässig:

Der Annahme, wonach das heimliche Einbringen eines Programms zur Telekommunikationsüberwachung eine nicht nur verhältnismäßig geringfügige Beeinträchtigung darstellt, sondern bereits die *bloße Existenz der Software auf dem Zielsystem* als schwerwiegende Grenzverletzung anzusehen ist – wie dies von einem Teil der Stimmen geschlussfolgert wird[892] – ist in dieser Pauschalität nicht zuzustimmen.

Es trifft zwar zu, dass das BVerfG festgestellt hat, dass mit der technischen Infiltration eines komplexen informationstechnischen Systems zum Zwecke der Telekommunikationsüberwachung „mit der Infiltration die entscheidende Hürde genommen [ist], um das System insgesamt auszuspähen“[893], „den dadurch bewirkten spezifischen Gefährdungen der Persönlichkeit […] durch Art. 10I GG nicht oder nicht hinreichend begegnet werden [kann]“[894] und „soweit kein hinreichender Schutz vor Persönlichkeitsgefährdungen besteht, […] das allgemeine Persönlichkeitsrecht dem Schutzbedarf […] über seine bisher anerkannten Ausprägungen hinaus dadurch Rechnung [trägt], dass es die Integrität und Vertraulichkeit informationstechnischer Systeme gewährleistet“[895]. Darüber hinaus hat das BVerfG aber auch festgestellt, dass nicht das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 I i. V. m. Art. 1 I GG tangiert ist, sondern allein Art. 10 I GG („hingegen“[896]) den grundrechtlichen Maßstab stellt, wenn sich die Überwachung ausschließlich auf Daten aus laufenden Telekommunikationsvorgängen beschränkt.[897] Die entsprechende Beschränkung im Zugriffsumfang muss

---

892 Vgl. AG Hamburg, CR 2010, 249 (252); ebenso LG Hamburg, MMR 2008, 423 (425).

893 BVerfG NJW 2008, 822 (825).

894 BVerfG NJW 2008, 822 (826).

895 BVerfG NJW 2008, 822 (827).

896 BVerfG NJW 2008, 822 (826).

897 Vgl. BVerfG NJW 2008, 822 (826).

hierbei „durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein“[898]. Hieraus lässt sich aber auch eine Wertentscheidung des BVerfG dahingehend ableiten, dass bei einer technisch[899] wie rechtlich[900] sichergestellten reinen Überwachung laufender Telekommunikation[901] gerade keine Beeinträchtigung der Integrität des betroffenen informationstechnischen Systems wie auch dessen Vertraulichkeit gegeben ist, welche den Schutzbereich des aus Art. 2 I i. V. m. Art. 1 I GG abgeleiteten IT-Grundrechts tangiert[902], sondern Art. 10 I GG in diesen Fällen den spezifischen Gefährdungen der Persönlichkeit hinreichend begegnet.[903] Im Vergleich zu dem mit der Primärmaßnahme verbundenen intensiven Eingriff in das *Fernmeldegeheimnis* aus Art. 10 I GG, nämlich die heimliche Erfassung der Inhalte und ggf. näheren Umstände der jeweiligen überwachten Telekommu-

---

898 BVerfG NJW 2008, 822 (826).

899 Für Einzelheiten zu *technischen Vorkehrungen*, siehe die Ausführungen dieses Abschnitts sowie 3. Teil A.I.1.c).

900 Für Einzelheiten zu *rechtlichen Vorgaben*, siehe 3. Teil A.I.1.b).

901 Hierbei kann eine sorgfältige und rechtstreue Umsetzung der Maßnahme durch die Ermittlungsbehörde innerhalb der von der Anordnung gesetzten Grenzen insoweit vorausgesetzt werden, als die Ermittlungsbehörde als „an Recht und Gesetz“ gebundene staatliche Stelle durch eine anordnungsgemäße und zweckentsprechende Programmierung der Überwachungssoftware dafür Sorge zu tragen hat, dass sich der Zugriff ausschließlich auf Daten aus laufenden Telekommunikationsvorgängen beschränkt, bzw. die Durchführung der Überwachung im konkreten Fall dann zu unterlassen hat, wenn eine solche Funktions-/Einsatzweise der Software im konkreten Einzelfall nicht sichergestellt werden kann, vgl. zutr. LG Hamburg, MMR 2011, 693 (696).

902 So stellt das BVerfG fest, dass ein Eingriff in das *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* anzunehmen ist, „wenn die Integrität des geschützten informationstechnischen Systems angetastet wird, indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können; dann ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen“ (BVerfG NJW 2008, 822, 827). Hieraus lässt sich indes schließen, dass für die Fälle, in denen das BVerfG „hingegen“ Art. 10 I GG als alleinigen grundrechtlichen Maßstab für die Beurteilung einer Ermächtigung zu Quellen-TKÜ-Maßnahmen erachtet – also für die Fälle, in denen durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt ist, dass ausschließlich Daten aus laufenden Telekommunikationsvorgängen erfasst werden (vgl. BVerfG NJW 2008, 822, 826) – gerade nicht zwingend angenommen werden muss, dass jede Infiltration (generell) zu einem Zugriff auf Leistungen, Funktionen und Speicherinhalte führt. Denn dann müssten sich auch diese Fälle am Maßstab des IT-Grundrechts ausrichten, da insoweit kein hinreichender Schutz durch Art. 10 I GG gewährleistet wäre. Dies stünde jedoch wiederum im Widerspruch zur Feststellung des BVerfG, wonach Art. 10 I GG in solchen Fällen der alleinige Grundrechtsmaßstab sein soll (vgl. BVerfG NJW 2008, 822, 826).

903 In diese Richtung auch LG Hamburg, MMR 2011, 693 (695 f.).

nikation[904], stellt die Begleitmaßnahme der vorherigen heimlichen Installation der entsprechenden Telekommunikationsüberwachungssoftware auf dem überwachten Zielsystem nur eine verhältnismäßig geringfügige Beeinträchtigung der Rechte des Betroffenen dar. Denn ein noch stärkerer Eingriff in die Vertraulichkeit der individuellen Telekommunikation als durch Kenntnisnahme von dem Inhalt des jeweiligen Kommunikationsvorgangs, ist in Bezug auf das Grundrecht aus Art. 10 I GG kaum denkbar. Verglichen mit der auf die Erfassung von Telekommunikationsinhalten verbundenen Primärmaßnahme bleibt der mit der Begleitmaßnahme des Einbringens der Software verbundene Eingriff insgesamt hinter der Intensität des primären Eingriffs in die Vertraulichkeit des Fernmeldeverkehrs zurück.

Doch selbst dann, wenn – einmal ungeachtet der Feststellungen des BVerfG unterstellt – durch die bloße Infiltration mit einer Telekommunikationsüberwachungssoftware auch die *Integrität* und *Vertraulichkeit* des jeweiligen System gleichwohl betroffen wären[905], so müsste dieser Eingriff im Vergleich zu dem mit der Primärmaßnahme – in Form des (mitunter über einen längeren Zeitraum andauernden) inhaltlichen Überwachens und Aufzeichnens der über das System geführten individuellen und vertraulichen IP-Kommunikation – verbundenen intensiven Eingriff nicht zwangsläufig zu einer darüber hinausgehenden, überproportionalen Beeinträchtigung der Rechte des Betroffenen führen. Denn die Infiltration mit einer Überwachungssoftware, bei der – gemäß dem von § 100a I StPO gestatteten Überwachungsrahmen sowie den konkreten Vorgaben in der Maßnahmeanordnung – ein ausschließlicher Zugriff auf Daten aus laufenden Telekommunikationsvorgängen technisch sichergestellt ist, führt gerade – anders als bei eine Software zur Online-Durchsuchung, die gemäß den technischen Standards in der Softwareprogrammierung freilich in ihrem Aufbau auf ähnliche, teils auch gleiche Programmierungsroutinen (z. B. verstecktes Einnisten im System und Ablaufen im Hintergrund, heimliches Ausleiten abgegriffener Daten etc.) zurückgreift, aber gerade maßnahmespezifisch auf ein Ausspionieren des System bzw. dessen Speichermedien gerichtet ist – nicht zu einem weitergehenden Zugriff auf sonstige, insbesondere persönlichkeitsrelevante Datenbestände außerhalb laufender Telekommunikationsvorgänge oder eine Überwachung sonstiger auf den Zielsystem ablaufender Vorgänge. Dies gilt erst recht, wenn angemessene, dem Stand der Technik entsprechende (technische) Schutzvorkehrungen der oben genannten Art ergriffen werden. Auch das Versehen der Überwachungssoftware mit einer „Nachla-

---

904 Vgl. insoweit Löwe-Rosenberg – *Schäfer*, StPO und GVG, Zweiter Band, § 100a StPO, Rn. 47.

905 AG Hamburg, CR 2010, 249 (252), bezeichnet dies insoweit unspezifisch als „das Schutzinteresse an der Unverletzlichkeit des genutzten Systems“ (252).

defunktion“, wie dies mitunter kritisch gesehen wird, da über eine solche (theoretisch) auch das Nachladen weiterer Funktionen möglich sei, ändert hieran nichts. Denn für eine solche Nachladefunktion besteht gerade ein ermittlungstaktisches und -technisches Bedürfnis, damit die individuelle Überwachungssoftware an vorgenommene Systemaktualisierungen und Updates angepasst bleibt.[906] Das bloße Einspielen einer entsprechend auf den Primäreingriff beschränkten Telekommunikationsüberwachungssoftware in das Zielsystem muss deshalb in Bezug auf den mit der Software ermöglichten *Zugriffsumfang* zu Recht nicht bereits als ein nicht mehr geringfügiger bzw. gar „schwerwiegender Grundrechtseingriff“[907] gewertet werden.[908]

Aber auch in Bezug auf Gefahren für die *Systemsicherheit* wie auch den Schutz des Systems vor *Veränderung* wird durch die bloße Existenz der Software auf dem betroffenen System nicht zwangsläufig ein Eingriff bewirkt, welcher der Annahme des Vorliegens verhältnismäßig geringfügiger Beeinträchtigung zwingend entgegensteht. Denn wie die oben genannten technischen Schutzmöglichkeiten aufzeigen, stehen technische Vorkehrungen und Mittel zur Verfügung, um Gefahren für die Systemsicherheit wie auch des Missbrauchs durch Dritte dem Stand der Technik entsprechend jedenfalls auf ein unvermeidbares Mindestmaß abzusenken. Maßstab hierfür ist insofern der *Stand der Technik*, als – gerade auch mit Blick auf den staatlichen Strafanspruch[909] und das öffentliche Interesse an effektiver Strafverfolgung – von Ermittlungsbehörden indes nichts technisch Unmögliches verlangt werden kann. Gleiches gilt auch für mit dem Einbringen der Software (technisch) unvermeidbar erfolgende Veränderungen im System. Derartige Änderungen stehen der Annahme einer verhältnismäßig geringfügigen Beeinträchtigung aber nicht entgegen, wenn diese sich nicht bzw. kaum nachteilig auf das System bzw. den Betroffen auswirken (erforderlich ist gerade eine *Beeinträchtigung*) und sich zudem bei der Deinstallation der Software – wiederum soweit, wie nach dem Stand der Technik möglich bzw. zur Wiederherstellung des vorherigen Zustandes nötig – rückgängig machen lassen.

Auch die dann noch verbleibende Annahme, in der *Beeinträchtigung der Nutzung und Bedienung des Systems* durch die Infiltration mit einer Überwachungssoftware einen nicht mehr nur geringfügigen Eingriff zu sehen, ist abzulehnen. Denn wie dies zutreffend, insbesondere in der jüngeren Rspr., vertreten wird[910], bringen sowohl das Einschleusen der Überwachungssoftware als auch deren anschließender Betrieb im Rahmen der Durchführung

---

906 Siehe hierzu auch 3. Teil A.I.1.c).

907 AG Hamburg, CR 2010, 249 (252).

908 Vgl. zutr. LG Hamburg, MMR 2011, 693 (695).

909 Vgl. insoweit BGH-Ermittlungsrichter NStZ 1998, 157 (158).

910 Vgl. LG Hamburg, MMR 2011, 693 (695).

der Überwachung und Aufzeichnung der laufenden IP-Kommunikation (ebenso die „Wartung“ in Form von Updates über das Datennetz[911]) nur solche Belastungen der Rechenleistung und Speicherkapazität des betroffenen Systems mit sich, die sich hauptsächlich auf den Bedienkomfort des Gerätes beziehen und gerade im Vergleich zu dem mit der Primärmaßnahme verbundenen Eingriff von lediglich untergeordneter und indes verhältnismäßig geringfügiger Bedeutung sind. Aber auch für die – je nach Übertragungsmenge und -geschwindigkeit unterschiedlich ausfallende – Beeinträchtigung in Form der Verlangsamung der Internet-Datenverbindung und damit verbunden der Schnelligkeit und „Leichtigkeit“ der Internetnutzung ist bei der Frage der Geringfügigkeit der begleitenden Maßnahme im Verhältnis zum Primäreingriff zu Recht zu berücksichtigen, dass sich derartige Beeinträchtigungen anlässlich des Einbringens, Betreibens wie auch Wartens der Überwachungssoftware über die vom Nutzer jeweils hergestellte Internetverbindung gerade angesichts der heute weitverbreiteten „Highspeed“-Internetanschlüsse (DSL; VDSL) regelmäßig nur in einer für den betroffenen Nutzer kaum wahrnehmbaren Größenordnung bewegen und hinsichtlich ihrer Gewichtigkeit erst recht hinter dem mit einem (mitunter über einen längeren Zeitraum erfolgenden) heimlichen Überwachen und Aufzeichnen der über das Zielsystem geführten IP-Kommunikation verbundenen intensiven Primäreingriff in den Rechtskreis des Betroffenen zurückbleiben.

Dies ist indes nicht nur für die Vorgänge des Einbringens, Betreibens und Wartens zu bejahen, sondern gilt auch für die mit dem *Entfernen der Software* von dem überwachten Zielsystem verbundenen Vorgänge. Als „actus contrarius“ zum Einbringen der Software in das System führt die – eine Maßnahme zur Überwachung verschlüsselt übermittelter Internettelefonie mittels Überwachungssoftware *typischerweise*[912] nachbereitende – Maßnahme des (regelmäßig heimlich bzw. verdeckt ablaufenden[913] automatisiert oder manuell eingeleiteten[914]) Entfernens der Software nach Beendigung der

---

911 Insbesondere zur Anpassung der Software an etwaige System-Updates.

912 Für Einzelheiten zur Frage der Typizität des Entfernens der Software, siehe die Ausführungen unter 2. Teil B.III.1.b).

913 So wird eine kriminaltaktische Notwendigkeit für ein heimliches bzw. verdecktes Entfernen der Software vom Zielsystem i. d. R. dann bestehen, wenn sich aus der überwachten Kommunikation erkennen lässt, dass durch ein offenes Vorgehen bspw. noch andauernde Ermittlungen, bei denen ein ermittlungstaktisches Interesse an der noch zeitweisen Aufrechterhaltung der Geheimhaltung fortbesteht, gefährdet werden könnten, vgl. in diese Richtung auch *Schneider*, NStZ 1999, 388 (390) zum Ausbau von in einen PKW eingebauten Abhörvorrichtungen im Rahmen von Maßnahmen nach § 100c I Nr. 2 StPO a. F. (§ 100f I StPO n. F.); zur verfassungsrechtlichen Bewertung, siehe 2. Teil B.II.

914 Für Einzelheiten zu den technischen Deinstallationsmöglichkeiten, siehe 1. Teil A.II.4.c).

Überwachungsaktion gleichsam nur zu einer im Vergleich zum Gewicht des Primäreingriffs nach § 100a I StPO geringfügigen Beeinträchtigung, da auch hierfür regelmäßig nur eine geringfügige Inanspruchnahme von Kapazitäten des Systems sowie der Internet-Datenverbindung vonnöten sein wird. Wie die obigen Ausführungen zeigen, lassen es die technischen Möglichkeiten zu, mittels integrierter (Selbst-)Deinstallationsroutinen und einprogrammierter Verfallsdaten alle Bestandteile der eingebrachten Software vom System wieder vollständig zu entfernen, selbst wenn diese von einer Datensicherung (*Backup*) erfasst worden sein sollte. Hierbei dient die Entfernung der verwendeten Überwachungssoftware nach Abschluss der Überwachung nicht nur legitimen kriminaltaktischen Belangen[915], sondern findet gerade dazu statt, um das System insoweit von der erfolgten Infiltration wieder zu „entlastet" und in Beendigung des staatlichen Zugriffs einen entsprechend uninfiltrierten – nicht notwendig exakten[916] – Zustand wie vor dem Einschleusen herzustellen.

Auch der *Vergleich* mit zulässigen Begleitmaßnahmen anderer heimlicher Ermittlungsmaßnahmen der StPO, welche von Annexkompetenzen erfasst sind, ergibt nichts anderes. Wie bspw. das heimliche Öffnen eines PKWs, Einbauen und Anschließen einer Abhörvorrichtung an die KFZ-Batterie (mitunter hierfür auch das kurzzeitige Verbringen in eine Werkstatt[917]) im Rahmen einer Maßnahme nach § 100f I StPO bzw. eines GPS-Ortungsempfängers/-senders im Rahmen einer Maßnahme nach § 100h I S. 1 Nr. 2 StPO für das Erfassens des nichtöffentlich gesprochenen Wortes (§ 100f I StPO) bzw. die Standortbestimmung und Positionsmeldung des Zielobjekts (§ 100h I S. 1 Nr. 2 StPO) zum Zwecke der Ermöglichung des Gewinnens von Spuren und Beweismittel zur Verfolgung und Aufklärung von Straftaten als *verhältnismäßig geringfügige Begleiteingriffe* in Bezug auf den jeweiligen Primäreingriff angesehen werden[918], kann dies angesichts obiger Ausführun-

---

915 Wie insbesondere dem Interesse eines Belassens von zu staatlichen Ermittlungen herangezogenen technischen Mitteln auf Fremdsystemen nur solange, wie dies für den Untersuchungszweck erforderlich ist; vgl. auch *Schneider*, NStZ 1999, 388 (390) zu Maßnahmen nach § 100c I Nr. 2 StPO a. F. (§ 100f I StPO n. F.).

916 Die Herstellung des exakten Zustandes wie vor der Infiltration dürfte technisch kaum möglich und müsste darüber hinaus auch nicht zwingend sachgerecht sein, da systemimmanent durch jede Benutzung des Systems regelmäßig neue Daten anfallen und Prozesse ablaufen, die das System (i. d. R. im Sinne des Nutzers) fortlaufend verändern.

917 So *Schneider*, NStZ 1999, 388 (390); i. E. auch BGH, NJW 2001, 1658 (1659) zu Maßnahmen nach § 100c I Nr. 1 lit. b StPO a. F. (§ 100h I S. 1 Nr. 2 StPO n. F.); ebenso Meyer-Goßner – *Cierniak*, StPO, § 100f, Rn. 4; a. A. noch BGH-Ermittlungsrichter NStZ 1998, 157 (157 f.).

918 Vgl. BGH-Ermittlungsrichter NStZ 1998, 157 (158); BGH NJW 2001, 1658 (1659); *Schneider*, NStZ 1999, 388 (389 f.), auch der Ausbau des technischen Mit-

gen zu Recht auch für das heimliche Installieren (wie Deinstallieren nach Beendigung der Maßnahme) einer auf die ausschließliche Erfassung laufender Telekommunikation beschränkten und in ihren Schutzvorkehrungen dem technischen Stand entsprechenden Überwachungssoftware auf dem jeweiligen Zielsystem der Überwachungsmaßnahme in Bezug auf das von § 100a I StPO gestattete Überwachen und Aufzeichnen von Telekommunikation unter Zugriff am Endgerät der Kommunikation mit eigenen technischen Mitteln der Strafverfolgungsbehörden[919] angenommen werden.

Auch für Maßnahmen der akustischen Wohnraumüberwachung nach §§ 100c ff. StPO wird eine Annexkompetenz zum gesetzlich gestatteten Überwachen des Wohnraums nach § 100c I StPO für solche begleitenden Maßnahmen angenommen, die typischerweise notwendig sind, um die technische Durchführung der Überwachung zu ermöglichen. Hierzu wird selbst das heimliche Betreten der Zielwohnung durch die Ermittlungspersonen zum Installieren der Abhörvorrichtungen (v. a. Wanzen) gezählt.[920] Trotz des damit einhergehenden erheblichen Eingriffs in das Grundrecht des Betroffenen aus Art. 13 I GG auf Unverletzlichkeit der Wohnung[921], hat der Gesetzgeber dennoch von einer ausdrücklichen Normierung der typischerweise notwendigen Begleitmaßnahmen in der Ermächtigungsgrundlage abgesehen und deren Zulässigkeit (kraft Annexkompetenz) vielmehr stillschweigend[922] vorausgesetzt[923], da das gesetzlich von § 100c I StPO gestattete Abhören und Aufzeichnen des in einer Wohnung nichtöffentlich gesprochenen Wortes mit technischen Mitteln auf andere Weise kaum bzw. gar nicht realisiert werden könnte.[924]

Als Ergebnis kann damit festgehalten werden, dass sich – unter erfolgter Einzelbetrachtung der sich aus der Installation (wie auch Deinstallation)

---

tels; ebenso *Bär*, TK-Überwachung, § 100f StPO, Rn. 9 u. § 100h, Rn. 8; Meyer-Goßner – *Cierniak*, StPO, § 100f, Rn. 4 m. w. N.

919 Vgl. hierzu BT-Drs. 16/5846, S. 47; Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 7a, 8; ebenso *Bär*, TK-Überwachung, § 100a StPO, Rn. 32.

920 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100c, Rn. 7; ebenso *Bär*, TK-Überwachung, § 100c StPO, Rn. 8 m. w. N.; BT-Drs. 13/8651, S. 13.

921 Was nach Auffassung des LG Hamburg, MMR 2011, 693 (694) gar Anlass dazu gebe, das Kriterium der *verhältnismäßig geringfügigen Beeinträchtigung* für die Bejahung einer Annexkompetenz in Frage zu stellen, wobei die Kammer aber dennoch von dem Kriterium als Voraussetzung ausgeht.

922 LG Hamburg, MMR 2011, 693 (694) spricht insoweit von einer Inbetrachtziehung und Billigung derartiger ergänzender Maßnahmen in Form eines „‚sachgedanklichen Mitbewusstseins'" (694) durch den Gesetzgeber, BGH-Ermittlungsrichter NStZ 1998, 157 von „konkludent erteilten Ermächtigungen" (157).

923 Vgl. BT-Drs. 13/8651, S. 13.

924 So LG Hamburg, MMR 2011, 693 (694); vgl. auch Meyer-Goßner – *Cierniak*, StPO, § 100c, Rn. 7; ebenso *Bär*, TK-Überwachung, § 100c StPO, Rn. 8 m. w. N.

einer Überwachungssoftware auf einem informationstechnischen System zum Zwecke der Überwachung und Aufzeichnung darüber verschlüsselt geführter Internettelefonie ergebenden Beeinträchtigungen für den Maßnahmebetroffenen im Verhältnis zum Gewicht des Primäreingriffes, wie auch unter Vergleich zu anerkannten Annexkompetenzen anderer strafprozessualer Ermittlungsmaßnahmen – angesichts der genannten Aspekte möglicher technischer Schutzvorkehrungen und Softwarekonfiguration in Bezug auf die Frage des Bestehens einer Annexkompetenz für die vor- bzw. nachbereitenden Begleitmaßnahmen einer Quellen-TKÜ die von einem wesentlichen Teil des Meinungsbildes verfolgte Linie, wonach neben deren *Typizität*[925] sich diese auch auf ein *verhältnismäßig geringfügig beeinträchtigendes* Maß absenken bzw. beschränken lassen, dogmatisch gut vertreten lässt.

Bei einer entsprechend im Zugriffsumfang auf die Überwachung laufender Telekommunikation beschränkten Überwachungssoftware, welche dem Stand der Technik entsprechende Schutzvorkehrungen für die Systemsicherheit enthält, Systemveränderungen und Nutzungsbeeinträchtigungen auf ein (technisch) unvermeidbares Mindestmaß absenkt und diese bei Beendigung der Maßnahme – soweit technisch möglich und zur Aufhebung beeinträchtigender Wirkungen nötig – rückgängig macht, belastet das heimliche Installieren (wie auch Deinstallieren) der Überwachungssoftware auf dem Zielsystem den Maßnahmebetroffenen im Verhältnis zur intensiven Eingriffswirkung der Primärmaßnahme nicht überproportional und kann diesem insbesondere auch mit Blick auf den hohen Stellenwert des staatlichen Strafanspruchs gerade in Bezug auf schwere Straftaten, wie sie Maßnahmen nach §§ 100a, 100b StPO zugrunde liegen, zugemutet werden.

Wie dies von mehreren Entscheidungen in jüngerer Zeit zur Frage der Zulässigkeit von Quellen-TKÜ-Maßnahmen getragen wird, lassen sich damit die Begleitmaßnahmen einer Quellen-TKÜ – d. h. die heimliche Installation der Überwachungssoftware (Infiltration eines informationstechnischen Systems) vor Beginn der Maßnahme und die Entfernung der Überwachungssoftware vom Zielsystems nach Abschluss der Maßnahme – im Gesamtergebnis in dogmatisch gut vertretbarer Weise auf eine *Annexkompetenz* zu der Befugnis aus § 100a I StPO stützen.

---

925 Für Einzelheiten zur Typizität, siehe 2. Teil B.III.1.

C. Zusammenfassung: Dogmatische Kernfragen der Quellen-TKÜ

Nachdem im Rahmen der Ausführungen des 2. Teils die dogmatischen Aspekte der Quellen-TKÜ und der dazu vertretenen Auffassungen näher dargestellt und analysiert wurden, lassen sich nunmehr folgende Kernfragen dieses modernen Ermittlungsinstruments zur Beantwortung im Rahmen der Lösungsmodelle im nachfolgenden 3. Teil herausarbeiten:

- Mit Blick auf die spezifischen technischen Abläufe von softwarebasierter Internettelefonie und der davon bedingten technisch erforderlichen Vorgehensweise einer Quellen-TKÜ im Rahmen der Realisierung der Überwachung auf dem jeweiligen Zielsystem, stellt sich zunächst die Frage, ob es sich *im Zeitpunkt des Zugriffs* überhaupt schon bzw. noch um eine *Überwachung und Aufzeichnung von Telekommunikation i. S. d. § 100a I StPO* handelt, auf welche unter Verwendung einer speziellen *Überwachungssoftware als technisches Mittel* auf dem informationstechnischen System des Absenders oder des Empfängers zugegriffen wird. Denn wie die Entwicklungen in der Rspr. verdeutlichen – sei es zur Frage des Erfassen der visuellen Bildschirminhalte mittels sog. *Screenshots* beim Verfassen von Textnachrichten durch die jeweilige Zielperson bei der Nutzung von E-Mailing- oder Instant Messaging-Diensten[926], sei es zur Frage des Zugriffs auf nach Abschluss des Telekommunikationsvorgangs im Herrschaftsbereich des Empfängers vorhandene TK-Daten[927] – kommt es entscheidend darauf an, ab wann die telekommunikative Übertragung von Daten begonnen hat bzw. abgeschlossen ist. Dies gilt gerade bei einem Zugriff, der – wie die Quellen-TKÜ – an dem Endgerät der jeweiligen Kommunikation ansetzt.

- Im Rahmen der Bewertung möglicher Lösungsmodelle gilt es des Weiteren abzuklären, welche Anforderungen an eine Rechtsgrundlage zur Legitimation von Quellen-TKÜ-Maßnahmen und des damit verbundenen spezifischen Einsatzes von Überwachungssoftware auf informationstechnischen Systemen in Bezug auf das *Bestimmtheitsgebot* zu stellen sind und inwieweit diesem bereits auf Grundlage der *bestehenden strafprozessualen Regelungen* zur Überwachung und Aufzeichnung von Telekommunikation genügt wird, oder aber eine *eigenständige bzw. ergänzende gesetzliche Regelung* der Maßnahme der Quellen-TKÜ angezeigt ist, für die sich die Frage nach der Verortung und konkreten inhaltlichen Ausgestaltung stellt.

---

926 Vgl. insoweit LG Landshut, MMR 2011, 690.

927 Vgl. insoweit BVerfG NJW 2006, 976.

In diesem Zusammenhang ist auch zu klären, welche Anforderungen sich an die *inhaltliche Ausgestaltung von Quellen-TKÜ-Anordnungen* ergeben, die insbesondere auch die Bedenken hinsichtlich eines „überschießenden" Einsatzes der Überwachungssoftware auf dem betroffenen informationstechnischen System berücksichtigen.

- Des Weiteren gilt es abzuklären, ob und inwieweit eine Rechtsgrundlage zur Durchführung von TKÜ-Maßnahmen „an der Quelle" unter Eingriff in informationstechnische Systeme durch Einsatz einer Überwachungssoftware den *Grundsatz der Verhältnismäßigkeit* wahrt, insbesondere auch mit Blick auf die technische Beschränkbarkeit des Zugriffsumfangs der Überwachungssoftware, die Missbrauchs- und Datensicherheit eines solchen auf informationstechnischen Systemen eingesetzten Zugriffsmittels sowie die Gewährleistung ausreichender Beweismittelauthentizität durch technische wie organisatorische Vorkehrungen.
- Hieran knüpfen unmittelbar die Fragen nach dem angemessenen Schutz des Kernbereichs privater Lebensgestaltung wie auch der *sachgerechten Ausgestaltung des Verfahrens*, welches sich an die erfolgte Datenerhebung anschließt, an, in deren Rahmen es einer näheren Auseinandersetzung damit bedarf, ob die diesbezüglichen für Maßnahmen nach §§ 100a, 100b StPO geltenden Vorschriften auch für Maßnahmen der Quellen-TKÜ einen ausreichenden Maßstab darstellen.
- Als „Quintessenz" der Untersuchungen zu den sich ergebenden (rechtlichen wie technischen) Anforderungen an die Anordnung und Durchführung einer Maßnahme der Quellen-TKÜ unter Einsatz einer Überwachungssoftware auf informationstechnischen Systemen zum Zwecke des Zugriffs auf darüber geführte IP-basierte Kommunikation stellt sich abschließend die Frage, welche *Folgen aus Verstößen gegen die rechtlichen Vorgaben* hinsichtlich der technischen Ausgestaltung, Funktions- und Einsatzweise der Überwachungssoftware *bei Umsetzung* der Anordnung herzuleiten sind, und damit letztlich die Frage nach der *Verwertbarkeit* erlangter Erkenntnisse.

3. Teil

Lösungsmodelle

A. Zulässigkeit der Quellen-TKÜ de lege lata

I. Modell 1: Gesetzliche Regelung der §§ 100a, 100b StPO grds. ausreichend

1. Rechtsgrundlage §§ 100a, 100b StPO

Die Regelungen der §§ 100a, 100b StPO zur Überwachung und Aufzeichnung von Telekommunikation stellen in Verbindung mit entsprechend präzise ausgestalteten Beschlüssen und daran ausgerichteten technischen Vorkehrungen im Rahmen der Maßnahmeumsetzung nach Auffassung eines wesentlichen Teils der Stimmen aus Rechtsdogmatik und Rechtspraxis[1] *de lege lata* eine ausreichende Rechtsgrundlage für die besondere Ermittlungsmaßnahme der Quellen-TKÜ im Strafprozessrecht dar. Die Überwachung verschlüsselter VoIP-Kommunikation „an der Quelle" unter Einsatz einer speziellen Überwachungssoftware, welche im Vorfeld in das betreffende informationstechnische System eingebracht wurde, lasse sich demnach auf die §§ 100a, 100b StPO stützen.

An diese Rechtsauffassung knüpft – wie nachfolgend im Einzelnen begründet – auch die vorliegende Arbeit insoweit an, als die bestehenden Regelungen der StPO zur Telekommunikationsüberwachung für eine solche Ermittlungsmaßnahme jedenfalls als *grds. ausreichend* erachtet werden.

---

[1] So Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 7a; BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 107c; KK – *Nack*, StPO, § 100a, Rn. 27, für die Übergangszeit bis zu einer gesetzlichen Regelung; *Bär*, TK-Überwachung, § 100a StPO, Rn. 32 f.; AG Bayreuth, MMR 2010, 266 (266); LG Hamburg, MMR 2011, 693 (693); insoweit auch LG Landshut, MMR 2011, 690 (691) mit Anm. *Bär*, MMR 2011, 691 (693); a. A. noch LG Hamburg, MMR 2008, 423 (424) und AG Hamburg, CR 2010, 249 (249); a. A. auch SK – *Wolter*, StPO, § 100a, Rn. 27 ff.; *Sankol*, CR 2008, 13 (15 ff.); *Hoffmann-Riem*, JZ 2008, 1009 (1022); *Buermeyer*/*Bäcker*, HRRS 2009, 433 (440); *Becker*/*Meinicke*, StV 2011, 50 (52); Anm. *Brodowski*, JR 2011, 533 (535); *Braun*/*Roggenkamp*, K&R 2011, 681 (681); *Albrecht*/*Dienst*, JurPC Web-Dok. 5/2012, Abs. 42 ff.; (im Erscheinen) *Sieber*, Gutachten zum 69. Deutschen Juristentag 2012, D.II.1.a).

Die unter Punkt C. des 2. Teils zusammengefassten dogmatischen Kernfragen einer strafprozessualen Quellen-TKÜ-Maßnahme lassen sich hierbei wie folgt beantworten:

a) Quellen-TKÜ unter Tatbestand subsumierbar

Das moderne Ermittlungsinstrument der Quellen-TKÜ lässt sich unter die Tatbestandsvoraussetzungen des § 100a I StPO einer *Überwachung und Aufzeichnung von Telekommunikation* subsumieren. Insbesondere scheitert eine derartige Maßnahme nicht bereits daran, dass im Zeitpunkt des Zugriffs das Tatbestandsmerkmal *Telekommunikation* nicht (mehr bzw. noch nicht) vorliegen würde. Wie im 2. Teil der Arbeit im Einzelnen dargestellt[2], werden hierzu unterschiedliche Auffassungen vertreten.

Das Erfordernis, dass im Zeitpunkt des Überwachens und Aufzeichnens auf Telekommunikation, also entsprechend den auch für die StPO grds. heranziehbaren Begriffsbestimmungen in § 3 Nr. 22, 23 TKG auf den technischen Vorgang des Aussendens, Übermittelns und Empfangens von als Nachrichten identifizierbaren Signalen mittels Telekommunikationsanlagen, zugegriffen werden muss, ist auch bei der Ermittlungskonstellation der Quellen-TKÜ unter Abgreifen der Daten auf dem zum Zwecke der Kommunikation verwendeten informationstechnischen System gegeben.

Unter genauer Betrachtung der technischen Abläufe softwarebasierten P2P-IP-Kommunikation geht die vorliegende Arbeit bei der Beurteilung der Frage, ob von der *Überwachungssoftware* schon bzw. noch *Telekommunikation* abgegriffen wird, von dem Ansatz aus, dass im Zeitpunkt des Zugriffs der Quellen-TKÜ-Software auf dem überwachten Zielsystem – je nach Anknüpfen der Maßnahme am Absender- oder Empfängersystem – schon bzw. noch ein laufender Telekommunikationsvorgang gegeben ist, da die hard- und softwaregesteuerten Prozesse, an denen die Software anknüpft, spezifische Bestandteile der Aussende- bzw. Empfangsvorgänge bei verschlüsselt übermittelter P2P-IP-Kommunikation darstellen:

aa) Vorliegen von Telekommunikation im Zugriffszeitpunkt

Während das BVerfG auf verfassungsrechtlicher Ebene zur Reichweite des grundrechtlichen Schutzes durch das Fernmeldegeheimnis aus Art. 10 I GG[3] treffend festgestellt hat, dass dieses „nicht in jedem Fall am Endge-

---

[2] Siehe 2. Teil A.II.3.

[3] Für Einzelheiten zur Reichweite des Fernmeldegeheimnisses aus Art. 10 I GG, siehe 1. Teil B.I.

rät der Telekommunikationsanlage [endet]“[4], „eine Gefährdung der durch Art. 10 GG geschützten Vertraulichkeit der Telekommunikation […] auch durch einen Zugriff am Endgerät erfolgen [kann]“[5] und bei einer Überwachung des „laufende[n] Kommunikationsvorgang[s] […] ein Eingriff in das Fernmeldegeheimnis auch dann vor[liegt], wenn die Erfassung des Nachrichteninhalts am Endgerät erfolgt“[6], ist allerdings nach zuzustimmender Auffassung aus der reinen Eröffnung des Schutzbereichs des Fernmelde*geheimnisses* nicht automatisch gleich auf die Einschlägigkeit einer einfachgesetzlichen Befugnisnorm zu schließen, welche spezifische Eingriffe in dieses Grundrecht legitimiert. Vielmehr muss es sich bei einer Maßnahme, die sich auf die Befugnisnormen der §§ 100a, 100b StPO stützt, im Zugriffszeitpunkt um eine Überwachung und Aufzeichnung von Telekommunikation, also des Fernmelde*verkehrs*, handeln.[7]

Bei der spezifischen Umsetzungsweise der Quellen-TKÜ zur Überwachung und Aufzeichnung verschlüsselt übermittelter IP-Kommunikation (neben Sprachdaten auch Videodaten[8] sowie Textdaten[9] der Kommunikation als Zugriffsgegenstand einer Quellen-TKÜ prinzipiell möglich) handelt es sich – entgegen teilweise vertretener Auffassung[10] – auch im Zeitpunkt des Zugriffs auf die zwischen den Gesprächsteilnehmern mit Hilfe einer speziellen VoIP-Software ausgetauschten Daten um ein Überwachen und Aufzeichnen von (bereits bzw. noch laufender) *Telekommunikation* i. S. d. § 100a I StPO:

---

4 BVerfG NJW 2006, 976 (979); vgl. bereits BVerfG NJW 2002, 3619 (3620 f.); auch BVerfG NJW 2008, 822 (825).

5 BVerfG NJW 2006, 976 (979); vgl. bereits BVerfG NJW 2002, 3619 (3620 f.).

6 BVerfG NJW 2006, 976 (979); vgl. auch BVerfG NJW 2008, 822 (825).

7 Vgl. zur Frage des automatischen Schlusses vom Schutzbereich auf eine Eingriffsbefugnis *Kudlich*, GA 2011, 193 (201); *ders*., JuS 2001, 1165 (1167); *ders*., JA 2000, 227 (232); *ders*., JuS 1998, 209 (213); in diese Richtung auch *Böckenförde*, Die Ermittlung im Netz, S. 419, 427 u. 429; siehe hierzu auch 2. Teil A.II.2.

8 Bei Video-Internettelefonie; vgl. zutr. LG Hamburg, MMR 2011, 693 (693 f.); hiervon nicht erfasst ist allerdings das Anfertigen sog. Screenshots von der grafischen Bildschirmoberfläche, so zutr. auch LG Landshut, MMR 2011, 690 (691); zur Abgrenzung siehe 1. Teil A.I.2.e) sowie 2. Teil A.II.4.

9 Bei Instant Messaging via IP (nach Betätigung des „Versende-Buttons“); für Einzelheiten zu Instant Messaging via IP, siehe 1. Teil A.I.2.f).

10 Wonach es bereits fraglich sei, ob die bei einer Quellen-TKÜ erhobenen Daten überhaupt als „Telekommunikation“ i. S. d. § 3 Nr. 22 TKG anzusehen seien, da der Zugriff gerade vor dem Aussenden bzw. nach dem Empfang erfolge, so *Becker*/*Meinicke*, StV 2011, 50 (51); in diese Richtung, i. E. aber offengelassen, auch LG Hamburg, MMR 2008, 423 (424); dieses Problem sieht wohl auch BeckOK – *Graf*, StPO, Ed. 13, §100a, Rn. 107c, der den Zeitpunkt der Verschlüsselung aber als „Vorstufe“ dem Kommunikationsvorgang zurechnet; siehe hierzu im Einzelnen 2. Teil A.II.3.

Gemäß höchstrichterlicher Rechtsprechung hat sich die nähere Bestimmung des Begriffs „Telekommunikation“ im Rahmen der Eingriffsbefugnis des § 100a StPO am grundrechtlichen Schutz des Betroffenen durch das Fernmeldegeheimnis des Art. 10 I GG zu *orientieren*.[11] Das Grundrecht aus Art. 10 I GG „ist seinerseits gegenüber den technischen Entwicklungen […] offen und dynamisch“[12]. Dennoch heißt dies unter Berücksichtigung obiger Ausführungen jedoch nicht, dass der Schutzbereich des Art. 10 I GG und die Reichweite von *Telekommunikation* im Rahmen des § 100a I StPO zwangsläufig und stets identisch sein müssen.

Der Begriff der *Telekommunikation*, der in der Strafprozessordnung selbst nicht näher definiert ist, wurde in den Vorschriften der §§ 100a, 100b StPO durch den Gesetzgeber bewusst entwicklungsoffen gefasst, um neue, zum Zeitpunkt des Gesetzeserlasses noch unbekannte Techniken der Nachrichtenübertragung nicht auszuschließen.[13] Das Einbeziehen „neuer Formen der Telekommunikation in § 100a StPO überschreitet […] nicht die Grenzen, die der Auslegung dieser Vorschrift durch Art. 10 GG […] gezogen sind“[14].

Zur Konkretisierung des Begriffes kann hierbei ohne weiteres der Wortsinn herangezogen werden, der in den Legaldefinitionen des § 3 Nr. 22, 23 TKG gesetzlich beschrieben ist.[15] Hiernach besteht eine Telekommunikation aus den charakterisierenden Vorgängen des Aussendens, Übermittelns und Empfangens von (als Nachrichten identifizierbaren) Signalen (jeglicher Art[16]) mittels Telekommunikationsanlagen[17].

---

[11] BVerfG NJW 1978, 313 (314 f.); BVerfG NJW 2000, 55 (57); BGH NStZ 1997, 247 (247 f.); BGH NJW 2001, 1587 (1587), wonach „sich ihre [§§ 100a, 100b StPO, Anm. d. Verf.] Auslegung, insbesondere des nunmehr maßgebenden Begriffs der Telekommunikation, in erster Linie an diesem Grundrecht ausrichten [muss]“ (1587); vgl. auch *Bär*, TK-Überwachung, § 100a StPO, Rn. 10.

[12] BGH-Ermittlungsrichter NJW 2001, 1587 (1587).

[13] Vgl. *Bär*, TK-Überwachung, § 100a StPO, Rn. 10; bereits BVerfG NJW 1978, 313 (314) zu § 1 Fernmeldeanlagengesetz (FAG); vgl. zudem BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 2 u. 6; vgl. auch *Kudlich*, JuS 2001, 1165 (1166) m. w. N.; auch *Käß*, BayVBl. 2010, 1 (6).

[14] BGH-Ermittlungsrichter NJW 2001, 1587 (1587).

[15] Vgl. BGH-Ermittlungsrichter NJW 2001, 1587 (1587); vgl. auch *Bär*, TK-Überwachung, § 100a StPO, Rn. 10; siehe hierzu auch 2. Teil A.II.3.

[16] Vgl. BGH NJW 2003, 2034 (2034), hierbei aber nicht jeder technische Vorgang des Aussendens, Übermittelns und Empfangens analog oder digital codierter Daten, sondern nur ein solcher, für den sich die Person einer Telekommunikationsanlage bedient, also diese kommunikationsbezogen in Anspruch nimmt.

[17] Telekommunikationsanlagen, § 3 Nr. 23 TKG: *technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können*.

Nach diesem Begriffsverständnis sind IP-basierte Kommunikationstechniken, insbesondere auch die softwarebasierte Internettelefonie, ebenso wie die sonstigen Kommunikationsdienste des Internets (E-Mail, Instant Messaging etc.) als solche eine Form von *Telekommunikation*.[18] Dies sagt aber noch nicht zwangsläufig etwas darüber aus, ob im *Zeitpunkt des Zugriffs* auf die ausgetauschten Daten am Endgerät ein mittels solcher Telekommunikationstechniken geführter Telekommunikationsvorgang schon bzw. noch vorliegt. Dies ist vielmehr je nach verwendeter Telekommunikationstechnik und der spezifischen Zugriffsweise auf diese zu beurteilen.

Für die Frage, ob im spezifischen Zugriffszeitpunkt der Überwachungssoftware bei einer Quellen-TKÜ, die zur Überwachung und Aufzeichnung IP-basierter Internettelefonie an einem hierfür genutzten informationstechnischen System ansetzt, bereits bzw. noch *Telekommunikation* vorliegt, bedarf es einer näheren Betrachtung der Vorgänge des *Aussendens* und *Empfangens* von als Nachrichten identifizierbaren Signalen bei softwarebasierter Internettelefonie. Denn der Begriff der „Telekommunikation" umfasst in der gesetzlichen Begriffsbestimmung, die er in § 3 Nr. 22, 23 TKG erhalten hat und an die sich auch im Strafprozessrecht grds. angelehnt werden kann[19] – als der technische Vorgang des Aussendens, Übermittelns und Empfangens von als Nachrichten identifizierbaren Signalen – eben nicht nur die bloße *Übermittlung* der Signale, sondern zeitlich davor und danach auch deren *Aussenden* und *Empfangen*. Andernfalls bräuchte es einer solchen ausdifferenzierten Begriffsbestimmung nicht. Denn wäre die Reichweite von „Telekommunikation" bloß auf den technischen Vorgang des „Übermittelns" beschränkt, so hätte eine Begriffsbestimmung von *Telekommunikation* in § 3 Nr. 22 TKG auch nur als „der technische Vorgang des Übermittelns von Signalen" gefasst werden können. Vielmehr stellen aber nach der eindeutigen gesetzgeberischen Wertung auch die Vorgänge des *Aussendens* und des *Empfangens* charakteristische Bestandteile eines Telekommunikationsvorgangs dar.

Unter Abstellen auf die mit dem Aussenden und Empfangen der Signale bei softwarebasierter Internettelefonie über informationstechnische Systeme verbundenen spezifischen technischen Vorgänge und Abläufe lässt sich ein Vorliegen von Telekommunikation im Zugriffszeitpunkt der Software indes dogmatisch begründen:

---

[18] Vgl. statt vieler BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 7 u. 31; Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 6 ff.

[19] Vgl. BGH-Ermittlungsrichter NJW 2001, 1587 (1587) („wesentliche Orientierungshilfe", 1587); auch BGH NJW 2003, 2034 (2034) („insoweit inhaltsgleich mit der Legaldefinition des § 3 Nr. 16 TKG [mittlerweile § 3 Nr. 22 TKG 2004, Anm. d. Verf.]", 2034); für Einzelheiten hierzu, siehe 2. Teil A.II.3.

So kann anhand der in Teil 1 der Arbeit dargestellten spezifischen technischen Vorgänge softwaregesteuerter Kommunikation via Internetprotokoll über komplexe informationstechnische Systeme (v. a. Computer, Notebooks/Laptops etc.)[20] für die dogmatische Begründung hergeleitet werden, dass bei dieser Kommunikationstechnik bereits die Digitalisierung der in analoger Form über das Mikrofon eingefangenen Eingangssignale den Beginn einer spezifischen *Aussendephase* sowie das Bereitstellen der rückumgewandelten Sprachsignale an der Ausgabeschnittstelle das Ende einer spezifischen *Empfangsphase* darstellen[21]. Das Merkmal der *Telekommunikation* lässt sich nämlich durchaus dahingehend auslegen, dass bei softwarebasierter VoIP-Kommunikation diese spezifischen technischen Abläufe bereits die Anfangs- und Endpunkte eines gesamtheitlich zu betrachtenden Telekommunikationsvorgangs zum Austausch von Signalen i. S. d. § 3 Nr. 22 TKG darstellen. In dessen Rahmen sind die komplexen system- und softwaregesteuerten Vorgänge der Digitalisierung, Zerlegung in Datenpakete, Komprimierung, Adressierung, Verschlüsselung und Einschleusung in das Datennetz spezifische mit dem Aussenden der Daten verbundene Vorgänge und mithin Bestandteile des Aussendevorgangs, während die system- und softwaregesteuerten Abläufe der Aufnahme der Daten aus dem Datennetz, Entschlüsselung, Dekomprimierung, Zusammensetzung der einzelnen Datenpakete und Rückumwandlung in akustische (bzw. bei Videotelefonie akustische und optische) Signale spezifische mit dem Empfangen von Daten verbundene Vorgänge und damit Bestandteile des Empfangsvorgangs darstellen – und in dessen Rahmen folglich auch eine Maßnahme der Quellen-TKÜ zur Überwachung laufender Telekommunikation aktiv werden kann[22].

Zur näheren Bestimmung, ab wann bei softwarebasierter VoIP-Kommunikation das *Aussenden* beginnt bzw. das *Empfangen* abgeschlossen ist, lässt sich darüber hinaus auch der Gedanke der *Beherrschbarkeit* der technischen Abläufe, auf den zur Bestimmung der Reichweite des grundrechtlichen Schutzes durch Art. 10 I GG abgestellt wird[23], entsprechend heranziehen:

---

20 Für Einzelheiten zu den technischen Vorgängen softwarebasierter VoIP-Kommunikation, siehe 1. Teil A.I.4.

21 Für Einzelheiten zur Empfangsphase, siehe 1. Teil A.I.4.

22 In diese Richtung auch die Antwort der Bundesregierung im Rahmen einer kleinen Anfrage, vgl. BT-Drs. 16/7279, S. 1 f., die von einem Abgreifen der TK-Daten „im Moment des Versendens" (S. 2) bzw. „im Moment des Empfangens" (S. 2) spricht.

23 Vgl. BVerfG NJW 2008, 822 (825); BVerfG NJW 2006, 976 (979) und BVerfG NJW 2002, 3619 (3620 f.); auch BVerfG NJW 2009, 2431 (2432) hat im Rahmen seiner Entscheidung den Gedanken des „technisch bedingte[n] Mangel[s] an Beherrschbarkeit" (2432) als maßgebliches Abgrenzungskriterium aufgegriffen.

Gemäß der Rspr. des BVerfG ist mit der Telekommunikation, also mit der Fernkommunikation unter Verwendung technischer Hilfsmittel zwischen Personen, die sich nicht am selben Ort befinden, ein „Verlust an Privatheit“[24] verbunden, da sich die Kommunizierenden „auf die Besonderheiten eines Kommunikationsmediums einlassen und sich dem eingeschalteten Kommunikationsmittler anvertrauen [müssen]“[25], weshalb sie „nicht die Möglichkeit [haben], die Vertraulichkeit der Kommunikation sicherzustellen“[26]. Unter Berücksichtigung früherer Feststellungen des BVerfG besteht diese Gefahr indes nicht nur während der Übermittlungsphase des Telekommunikationsvorgangs auf der Transportstrecke. So kann nach Auffassung des BVerfG „eine Gefährdung der durch Art. 10 I GG geschützten Vertraulichkeit der Telekommunikation […] auch durch Zugriff am Endgerät erfolgen“[27], da „moderne Endgeräte […] eine Vielzahl von Leistungen [ermöglichen], auch solche, die untrennbar in den Übermittlungsvorgang eingebunden und dem Endteilnehmer häufig gar nicht in den Einzelheiten bekannt sind, jedenfalls nicht seiner alleinigen Einflussnahme unterliegen“[28]. Gemäß weiteren Feststellungen des BVerfG sind Telekommunikationssignale erst „mit Zugang bei dem Empfänger nicht mehr den erleichterten Zugriffsmöglichkeiten Dritter – auch des Staates – ausgesetzt, die sich aus der fehlenden Beherrschbarkeit und Überwachungsmöglichkeit des Übertragungsvorgangs durch die Kommunikationsteilnehmer ergeben“[29]. Erst in seiner Herrschaftssphäre habe der Nutzer die Möglichkeit zur Datenverarbeitung, insbesondere zur Datenlöschung.[30]

Kennzeichnend für das Befinden von Telekommunikationsdaten im Herrschaftsbereich des Nutzers sind demnach also gerade die (potentielle) Verfügungsmöglichkeiten des Nutzers über die Daten, also insbesondere die individuelle Entscheidung über deren Verarbeitung, (dauerhafte) Speicherung oder Löschung – da „die spezifischen Risiken eines der Kontroll- und Einwirkungsmöglichkeit des Teilnehmers entzogenen Übertragungsvorgangs […] dann nicht mehr [bestehen]“[31].

Die Datenverarbeitungsprozesse, die bei softwarebasierter VoIP-Kommunikation auf den informationstechnischen Systemen (v. a. Computer) softwaregesteuert und ohne Einflussmöglichkeit der Gesprächsteilnehmer (auto-

---

24 BVerfG NJW 2006, 976 (978).
25 BVerfG NJW 2006, 976 (978).
26 BVerfG NJW 2006, 976 (978).
27 BVerfG NJW 2002, 3619 (3621).
28 BVerfG NJW 2002, 3619 (3621).
29 BVerfG NJW 2006, 976 (978).
30 Vgl. BVerfG NJW 2006, 976 (979).
31 BVerfG NJW 2006, 976 (979).

matisiert) stattfinden (Digitalisierung, Komprimierung und Verschlüsselung bzw. Entschlüsselung, Dekomprimierung und Rückumwandlung) sind technisch notwendige[32] und untrennbare Bestandteile des softwaregesteuerten Aussendens und Empfangens von Signalen zur Kommunikation mittels (VoIP-Software-gesteuerter) Computer und damit unverzichtbar in den Telekommunikationsvorgang eingebunden.[33] Hierbei wird der Computer in spezifischer Weise „kommunikationsbezogen"[34] und die darauf (system- und softwaregesteuert) stattfindenden technischen Vorgänge in kommunikationserheblicher Weise gebraucht. Auf die technischen Vorgänge des Aussendens hat der Nutzer in dem Moment keinerlei Kontroll- oder Einwirkungsmöglichkeiten mehr, in welchem dieser seine Nachricht in das Mikrofon spricht und die Signale vom System erfasst werden (vergleichbar mit dem Betätigen des „Versende-Buttons" bei Textnachrichten), als von da an die weitere Signalverarbeitung automatisiert und softwaregesteuert durch die Systemprozesse bewerkstelligt wird. Eine Beherrschbarkeit der – in Sekundenbruchteilen und nur bei aktiver Verbindung zwischen den Gesprächspartnern ablaufenden – technischen Vorgänge wie auch die freie Verfügbarkeit über die Kommunikationsdaten liegt in dieser Phase nicht mehr vor, da bereits hier ein Vorgang zum Übertragen von als Nachrichten identifizierbaren Signalen unumkehrbar eingeleitet worden ist.[35]

Unter Berücksichtigung des Kriteriums der Beherrschbarkeit ist deshalb (bei Anknüpfen am Empfängersystem) von einem den Abschluss des Telekommunikationsvorgangs bewirkenden Zugang der versendeten Signale auch erst nach Ablauf der spezifischen Empfangsvorgänge – die bei dieser modernen Kommunikationsform über komplexe Endgeräte ebenfalls untrennbar in den Vorgang der Übertragung eingebunden sind – mit Rückumwandlung der digitalen Daten in Sprachsignale zum Bereitstellen an der

---

[32] In diesem Sinne auch in Einklang mit frühen Aussagen des BGH (BGH NJW 1983, 1569, 1569), wonach unter den Begriff des *Fernmeldeverkehrs* „nach dem allgemeinen Sprachgebrauch" (1569) neben dem Telefongespräch „die mit dem Telefonieren notwendigerweise verbundenen Vorgänge [fallen]" (1569).

[33] Dies steht in Einklang mit grundsätzlichen Feststellung des BGH, wonach der Eingriffsbereich des § 100a StPO „die mit dem Versenden und Empfangen von Nachrichten mittels Telekommunikationsanlagen in Zusammenhang stehenden Vorgänge" (2035) erfasst, BGH NJW 2003, 2034 (2035).

[34] Also der Nachrichtenübermittlung dienend, vgl. *Bär*, TK-Überwachung, § 100a StPO, Rn. 10.

[35] Dies steht indes in Einklang mit den Feststellungen des BVerfG zum Schutzbereich des Art. 10 I GG, wonach „moderne Endgeräte […] eine Vielzahl von Leistungen [ermöglichen], auch solche, die untrennbar in den Übermittlungsvorgang eingebunden und dem Endteilnehmer häufig gar nicht in den Einzelheiten bekannt sind, jedenfalls nicht seiner alleinigen Einflussnahme unterliegen" (BVerfG NJW 2002, 3619, 3621).

Ausgabeschnittstelle auszugehen. Denn erst nach Abschluss dieser spezifischen technischen Vorgänge steht bei softwarebasierter Internettelefonie dem Empfänger die Möglichkeit zur „Entgegennahme" der Sprachnachricht zur Verfügung.[36] Ob die Telekommunikationssignale dann von der Ausgabeschnittstelle tatsächlich hörbar in den Raum „entäußert" werden bzw. vom Empfänger gar akustisch, sprich sinnlich wahrgenommen werden, ist hierbei unerheblich.

In diesem Zusammenhang ist des Weiteren auch der Umstand mit einzubeziehen, dass die VoIP-Gesprächspartner bereits vor dem Ablauf des eigentlichen Gesprächs und während des gesamten Kommunikationsvorgangs sowohl in die verwendete VoIP-Software und damit in das jeweilige VoIP-System eingeloggt sind[37] als andererseits auch eine aktive Internetverbindung zueinander unterhalten, ohne die der in diesem Rahmen stattfindende Austausch von Kommunikationsdaten durch softwaregesteuerte automatisierte Versendung der digitalisierten Daten nicht möglich wäre. Sofern also teilweise gefolgert wird, dass zum Zeitpunkt der Verarbeitung der Sprachsignale durch eine Kommunikationssoftware noch keine Telekommunikation vorliege, da bspw. ein vorhandener Defekt es verhindern könnte, dass ein Kommunikationsvorgang „unumkehrbar" beginnt[38], lässt sich dem entgegenhalten, dass in einem solchen Falle schon keine aktive Verbindung zwischen den Gesprächsteilnehmern hergestellt werden könnte und somit schon gar keine Nutzung des VoIP-Dienstes und des informationstechnischen Systems zur (Quellen-TKÜ-relevanten) P2P-Kommunikation möglich wäre. Ist ein Einloggen in das VoIP-System durch den Nutzer jedoch erfolgt und eine aktive Verbindung zwischen den Gesprächspartnern erfolgreich aufgebaut, so wird ab Beginn des Telefonats jedes Eingangssignal durch automatisiert und softwaregesteuert ablaufende Vorgänge über das zu Telekommunikationszwecken verwendete informationstechnische System unumkehrbar versendet.

Der betroffene Nutzer bedient sich hierbei einer Telekommunikationsanlage, d. h. er nimmt Kommunikation mittels einer solchen Anlage vor[39], deren Endgerät in Form eines mit einer Kommunikationssoftware versehenen komplexen informationstechnischen Systems Leistungen erbringt, die

---

36 Da erst dann die Signale für den Empfänger zur Kenntnisnahme und zur weiteren „Verfügung" über diese (bspw. Aufzeichnen der Signale und dauerhafte Speicherung) bereitstehen.

37 Wodurch eine Adressierung der einzelnen Datenpakete stattfinden kann; für Einzelheiten, siehe 2. Teil A.II.6.b).

38 Vgl. hierzu *Gercke*/*Brunst*, Internetstrafrecht, Kap. 5, S. 349, Rn. 892, Fn. 373; *Brunst*, Anonymität im Internet, S. 267, Fn. 1399.

39 Vgl. BGH NJW 2003, 2034 (2035); BVerfG NJW 1978, 313 (314).

untrennbar in den Übermittlungsvorgang eingebunden sind[40], und hierüber als Nachrichten identifizierbare Signale sendet bzw. empfängt.

Unter Berücksichtigung obiger Ausführungen lässt sich damit auch dogmatisch begründen, dass im Zeitpunkt des Zugriffs durch die Überwachungssoftware (schon bzw. noch) *Telekommunikation* vorliegt und die Vorgehensweise ein *Überwachen und Aufzeichnen von Telekommunikation* i. S. d. § 100a I StPO darstellt. Mithin ist insoweit auch der Begriff *Quellen-TKÜ* berechtigt, als die Überwachung „an der Quelle" der Telekommunikation ansetzt.

bb) Mittels Überwachungssoftware als technisches Mittel

Wie die dogmatischen Ausführung zur Zulässigkeit der Durchführung von TKÜ-Maßnahmen auf Grundlage der §§ 100a, 100b StPO mit *technischen Mitteln*, insbesondere auch mit eigenen technischen Mitteln der Strafverfolgungsbehörden[41] im Rahmen des 2. Teils der Arbeit[42] gezeigt haben, ist – als Konsequenz aus der *technologieneutralen* und *entwicklungsoffenen* Formulierung der gesetzlichen Eingriffsbefugnis[43] und der damit getroffenen Wertentscheidung des Gesetzgebers – je nach konkret überwachter Telekommunikationsform bei der Wahl des für eine TKÜ-Maßnahme heranzuziehenden technischen Mittels ein gewisser Beurteilungsspielraum und ein gewisses Auswahlermessen einzuräumen.

Für die Fälle der verschlüsselt übermittelten VoIP-Kommunikation findet zur Gewährleistung einer Überwachbarkeit der jeweils via Internetprotokoll ausgetauschten Telekommunikationsdaten eine spezielle *Überwachungssoftware* auf dem gemäß der Anordnung zu überwachenden System Verwendung, welche die Telekommunikationsdaten zu einem Zeitpunkt abgreift, zu dem die Daten in (noch bzw. bereits wieder) unverschlüsselter Form vorliegen.

Bei solcher, im Rahmen von Maßnahmen der Quellen-TKÜ zum Zwecke des Abgreifens und Ausleitens von VoIP-basierter Telekommunikation an der Quelle zum Einsatz kommender Überwachungssoftware handelt es sich mithin um ein *technisches Mittel zum Zwecke der Datenerhebung*[44].

---

40 Vgl. BVerfG NJW 2002, 3619 (3621).

41 Vgl. auch BT-Drs. 16/5846, S. 47.

42 Siehe 2. Teil A.II.5. u. 6.c).

43 Vgl. auch BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 2 u. 6; auch *Kudlich*, JuS 2001, 1165 (1166) m. w. N.; *ders*., JA 2010, 310 (312); auch *Käß*, BayVBl. 2010, 1 (6).

44 So in Bezug auf *Remote Forensic Software* auch das Bundesministerium des Innern, Fragenkatalog SPD, S. 6, abrufbar unter http://www.netzpolitik.org/wp-up

Dieses technische Mittel ist notwendig, damit – i. S. d. Gesetzesbegründung zu den strafprozessualen Vorschriften über die Telekommunikationsüberwachung[45] – das von § 100a I StPO gestattete *Überwachen* und *Aufzeichnen* der Telekommunikation nach Maßgabe der die Maßnahme legitimierenden Anordnung[46] auch bei verschlüsselt über das Leitungsnetz transportierter Internettelefonie in technischer Hinsicht erfolgen kann. Die für Maßnahmen der Quellen-TKÜ verwendete Software stellt insoweit ein spezifisch an und spezifisch auf verschlüsselt übermittelte softwarebasierte Internettelefonie ausgerichtetes technisches Überwachungsmittel i. S. d. § 100a I StPO dar.

Wie die Untersuchungen in Teil 2 ergeben haben, kann die vorherige heimliche Installation der Überwachungssoftware auf dem Zielsystem wie auch deren spätere Deinstallation nach Beendigung der Maßnahme in zulässiger Weise auf eine Annexkompetenz zur Befugnis aus § 100a I StPO gestützt werden, da sich für diese notwendigen Begleitmaßnahmen anhand dogmatischer Erwägungen sowohl das Vorliegen von *Typizität* als auch die Wahrung der *Verhältnismäßigkeit* begründen lässt.[47]

b) Kein Verstoß gegen das Bestimmtheitsgebot

Eine Subsumtion der Quellen-TKÜ unter die bestehenden Regelungen der §§ 100a, 100b StPO ist des Weiteren ohne Verstoß gegen die *allgemeinen rechtsstaatlichen Anforderungen* an Eingriffsnormen[48], d. h. unter Einhaltung des *Bestimmtheitsgebotes* (vgl. nachfolgend) und Wahrung des *Verhältnismäßigkeitsgrundsatzes* [vgl. nachfolgend Punkt c)] möglich.

Der von einem wesentlichen Teil in Rspr. und Schrifttum verfolgten Linie, die sich für eine Zulässigkeit der Quellen-TKÜ auf Grundlage der bestehenden Regelungen der §§ 100a, 100b StPO ausspricht[49], kann darin

---

load/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012); auch gesetzlich verankerte (präventiv-polizeiliche) Ermächtigungsgrundlagen zu Maßnahmen der Quellen-TKÜ (bspw. § 20l II S. 1 BKAG, § 15b I HSOG, § 31 III S. 1 POG RP) legen hier die Begrifflichkeit „technisches Mittel" für eine Überwachungssoftware zum Ausleiten der laufenden Telekommunikation zugrunde.

45 Vgl. BT-Drs. 16/5846, S. 47.

46 Vgl. BT-Drs. 16/5846, S. 47.

47 Siehe hierzu die Ausführungen zu 2. Teil B.III.

48 Zu verfassungsrechtlichen Rahmenbedingungen des Strafverfahrensrechts, siehe *Kudlich*, GA 2011, 193 (194 ff.).

49 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 7a; BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 107c; KK – *Nack*, StPO, § 100a, Rn. 27, jedenfalls für die Übergangszeit bis zu einer gesetzlichen Regelung; *Bär*, TK-Überwachung, § 100a StPO, Rn. 32 f.; AG Bayreuth, MMR 2010, 266 (266); LG Hamburg, MMR 2011,

zugestimmt werden, dass die §§ 100a, 100b StPO für eine Maßnahme der Quellen-TKÜ – jedenfalls in noch ausreichender Weise – dem allgemeinen *Bestimmtheitsgebot* genügen. Das Ermittlungsinstrument der Quellen-TKÜ lässt sich unter die bestehenden Befugnisnormen der §§ 100a, 100b StPO über die Überwachung und Aufzeichnung von Telekommunikation ohne einen zwingenden Verstoß gegen das Bestimmtheitsgebot fassen. Die bestehende strafprozessuale Eingriffbefugnis zur Telekommunikationsüberwachung stellt auch für eine an der Quelle mittels spezieller Überwachungssoftware durchgeführte Telekommunikationsüberwachung eine noch hinreichend bestimmte Rechtsgrundlage dar:

Gesetzliche Normen bedürfen eines angemessenen Maßes an Bestimmtheit. Für die Wahrung des Bestimmtheitsgebotes bedarf es indes keiner absoluten bzw. optimalen Bestimmtheit, es genügt eine *hinreichende Bestimmtheit*. Im Ergebnis stellt das Bestimmtheitsgebot aber nur Mindestanforderungen an die Fassung einer Norm. Es genügt deshalb, wenn sich bspw. mit Hilfe juristischer Auslegungsmethodik (wie z. B. Gesetzessystematik, Normzusammenhang, Gesetzesbegründung u. ä.) eine insgesamt zuverlässige Grundlage für das Auslegen und Anwenden der Vorschrift gewinnen lässt.[50] Eingriffsnormen unterliegen hierbei tendenziell erhöhten Anforderungen. Gleichwohl ist es dem Gesetzgeber auch bei diesen gestattet, mit abstrakten und unbestimmten Rechtsbegriffen zu arbeiten.[51]

Unter verfassungsrechtlichen Gesichtspunkten ausschlaggebendes Kriterium für die hier thematisierte Konstellation ist die Beurteilung der Frage, ob die §§ 100a, 100b StPO als Ermächtigungsgrundlage hinsichtlich einer darunter subsumierten Quellen-TKÜ insgesamt dem Gebot der *Normenklarheit und Tatbestandsbestimmtheit*[52] genügen. Die Maßgaben, welche das BVerfG im Rahmen seines *Volkszählungsurteils*[53] insoweit für das Grundrecht auf informationelle Selbstbestimmung aus den Art. 2 I i. V. m. Art. 1 I GG hergeleitet hat, sind im Grundsatz auch auf Eingriffe in die speziellere Garan-

---

693 (693); insoweit auch LG Landshut, MMR 2011, 690 (691) mit Anm. *Bär*, MMR 2011, 691 (693); a. A. noch LG Hamburg, MMR 2008, 423 (424) und AG Hamburg, CR 2010, 249 (249); a. A. auch SK – *Wolter*, StPO, § 100a, Rn. 27 ff.; *Sankol*, CR 2008, 13 (15 ff.); *Hoffmann-Riem*, JZ 2008, 1009 (1022); *Buermeyer*/*Bäcker*, HRRS 2009, 433 (440); *Becker*/*Meinicke*, StV 2011, 50 (52); Anm. *Brodowski*, JR 2011, 533 (535); *Braun*/*Roggenkamp*, K&R 2011, 681 (681); *Albrecht*/*Dienst*, JurPC WebDok. 5/2012, Abs. 42 ff.; (im Erscheinen) *Sieber*, Gutachten zum 69. Deutschen Juristentag 2012, D.II.1.a).

[50] Vgl. Maunz/Dürig – *Grzeszick*, GG, Art. 20, Abschnitt VII, 63. EL 2011, Rn. 58, 61; siehe hierzu im Einzelnen auch 2. Teil A.II.1.

[51] Vgl. Maunz/Dürig – *Grzeszick*, GG, Art. 20, Abschnitt VII, 63. EL 2011, Rn. 65.

[52] Vgl. hierzu die Ausführungen unter 2. Teil A.II.1.

[53] BVerfG NJW 1984, 419.

tie aus Art. 10 I GG zu übertragen.[54] Gemäß st. Rspr. des BVerfG gehört hierzu, dass sich die Voraussetzungen sowie der Umfang der grundrechtlichen Beschränkungen aus den gesetzlichen Regelungen klar und für den Bürger erkennbar ergeben. Anlass, Zweck und Grenzen des grundrechtlichen Eingriffs müssen in der Ermächtigungsgrundlage bereichsspezifisch und präzise bestimmt sein.[55]

Für Ermächtigungen zu Überwachungsmaßnahmen fordert das Bestimmtheitsgebot indes nicht, dass die konkrete Maßnahme vorhersehbar sein muss, wohl aber, dass der Betroffene „grundsätzlich erkennen kann, bei welchen Anlässen und unter welchen Voraussetzungen ein Verhalten mit dem Risiko der Überwachung verbunden ist“[56].

Die §§ 100a, 100b StPO erfassen die Überwachung und Aufzeichnung sämtlicher Erscheinungsformen von Telekommunikation, deren Inhalte und näheren Umstände als Beweismittel oder zumindest als Spurenansätze für die Untersuchungen im Rahmen strafprozessualer Ermittlungsverfahren für die Verfolgung und Aufklärung von Straftaten von Bedeutung sein können.

Für den verständigen Durchschnittsbürger als (potentiellem) Nutzer eines VoIP-Dienstes, der mittels eines Computers über das Internet verschlüsselte Telefongespräche mit einem anderen Nutzer des Dienstes führt, kann es grds. als noch hinreichend erkennbar erachten werden, dass die repressiven Vorschriften über die Überwachung von Telekommunikation nach §§ 100a, 100b StPO auch eine heimliche Überwachung und Aufzeichnung von Telefongesprächen erfassen, welche mittels spezieller VoIP-Software über den Computer geführt werden. Diesbezüglich lässt sich den Regelungen der §§ 100a, 100b StPO in hinreichend klarer und für den verständigen Durchschnittsbürger hinreichend erkennbarer Weise entnehmen, welche *Voraussetzungen* für den mit der Überwachung und Aufzeichnung von Telekommunikation – gilt insoweit auch für ein Anknüpfen „an der Quelle“ – verbundenen grundrechtlichen Eingriff vorliegen müssen.

Die *Primärmaßnahme* einer Quellen-TKÜ in Gestalt des Überwachens und Aufzeichnens von verschlüsselt übermittelter VoIP-Kommunikation durch Anknüpfen der TKÜ an dem zu Telekommunikationszwecken genutzten informationstechnischen System des Betroffenen wird mit Blick auf die hierfür erforderlichen Eingriffsvoraussetzungen von den Vorschriften der §§ 100a, 100b StPO in einer dem Bestimmtheitsgrundsatz noch gerecht

---

[54] Vgl. BVerfG NJW 2004, 2213 (2215); BVerfG NJW 2009, 2431 (2434).

[55] Vgl. bereits BVerfG NJW 2000, 55 (57); ebenso BVerfG NJW 2004, 2213 (2215); BVerfG NJW 2009, 2431 (2434); vgl. auch Maunz/Dürig – *Grzeszick*, GG, Art. 20, Abschnitt VII, 63. EL 2011, Rn. 58 ff.

[56] BVerfG NJW 2005, 2603 (2607).

werdenden Weise erfasst – auch wenn hierfür als spezifisches technisches Mittel eine Überwachungssoftware Verwendung findet:

So lässt sich ohne weiteres annehmen, dass ein verständiger Durchschnittsbürger als (potentieller) Nutzer von IP-basierter Kommunikationstechnik – ohne in Konflikt hinsichtlich einer Erkennbarkeit für ihn zu geraten – das Kommunizieren via VoIP-Telefonie (sei es nun innerhalb des P2P-Netzwerkes oder unter Beteiligung des öffentlichen Festnetzes oder Mobilfunknetzes) grundsätzlich – ohne hierbei die näheren technischen Details und Abläufe vor Augen haben zu müssen – als eine Form des *Telekommunizierens*, also als eine Methode zum Nachrichtenaustausch via hierfür verwendeter technischer Einrichtungen und Systeme einstuft. Denn aus durchschnittlicher Nutzersicht, sowohl des Anrufenden als auch des Angerufenen, handelt es sich bei VoIP-Telefonie um eine Dienstleistung, die in der „möglichst echtzeitnahen, zielgenauen und wechselseitigen Übertragung seiner gesendeten Sprachsignale an den jeweils anderen Gesprächspartner“[57] besteht. Hierbei ist auch nicht davon auszugehend, dass ein verständiger Telekommunikationsteilnehmer bei der Nutzung von Internettelefonie das Angebot in dem Bewusstsein in Anspruch nimmt, es handele sich bloß um einen Dienst der elektronischen Informations*medien*, mit dem lediglich Inhalte einseitig abgefragt oder redaktionell bearbeitet würden. Vielmehr geht es den Nutzern von VoIP-Diensten schlicht und einfach darum, auf elektronischem Wege über die Ferne zu kommunizieren.[58]

Weder die bei softwarebasierter VoIP von Computer zu Computer zur Anwendung kommende peer-to-peer-Technik noch die geschlossene end-to-end-Verschlüsselung der Gesprächsdaten, geben einem verständigen Durchschnittnutzer Anlass zur Annahme, dass es sich bei derartiger VoIP-Telefonie um eine Kommunikationsform handeln könnte, in die wegen der Verschlüsselung der Kommunikationsdaten durch eine Maßnahme zur Überwachung und Aufzeichnung von Telekommunikation nicht eingegriffen werden dürfte und damit letztlich von Überwachungsmaßnahmen staatlicher Stellen generell ausgenommen wäre.

Wie der Begriff der Telekommunikation sind auch die gesetzlichen Begrifflichkeiten der *Überwachung* und *Aufzeichnung* zum Zwecke einer praktikablen Ausgestaltung einer Rechtnorm wie § 100a I StPO, die in be-

---

57 *Seitlinger*/*Strobl*, Voice over IP – eine rechtliche Beurteilung vom Kommunikationsdienst bis zum Netzzugang, S. 8, abrufbar unter http://www.it-law.at/uploads/tx_publications/Voice_over_IP__eine_rechtliche_Beurteilung_vom_Kommunikationsdienst_bis_zum_Netzzugang.pdf (zuletzt aufgerufen 15.06.2012).

58 Vgl. *Seitlinger*/*Strobl*, Voice over IP – eine rechtliche Beurteilung vom Kommunikationsdienst bis zum Netzzugang, S. 8, abrufbar unter http://www.it-law.at/uploads/tx_publications/Voice_over_IP__eine_rechtliche_Beurteilung_vom_Kommunikationsdienst_bis_zum_Netzzugang.pdf (zuletzt aufgerufen 15.06.2012).

sonderer Weise technischen Entwicklungen und geändertem Kommunikationsverhalten unterworfen ist, in Anpassung an den rasanten technischen Fortschritt im Bereich der Telekommunikationstechniken entwicklungsoffen gehalten[59] und benötigen daher auch auf Rechtsanwendungsebene entsprechender entwicklungsneutraler Auslegung.[60] Im Zusammenhang mit der Datenerhebung aus Telekommunikationsvorgängen ist unter einem *Überwachen* grds. das zielgerichtete Abfangen, technische Aufbereiten und (v. a. akustische) Wahrnehmen der Telekommunikationsdaten zu verstehen[61], unter *Aufzeichnen* grds. das Kopieren, Mitschneiden, Aufnehmen der Daten (v. a. Gesprächsinhalte) zur stofflichen Fixierung in einer speicherbaren (damit auswertbaren) und in die spätere Hauptverhandlung i. d. R. als Augenscheinsobjekt einführbaren Form.[62] Von der Datenerhebung durch Überwachung und Aufzeichnung mit umfasst ist zudem auch das Wahrnehmbarmachen und Auswerten der erlangten Daten.[63]

Das Überwachen und Aufzeichnen im Rahmen von TKÜ-Maßnahmen kann hierbei auch unter Verwendung *technischer Mittel* erfolgen. Dass zur Überwachung und Aufzeichnung der Telekommunikation technische Mittel eingesetzt werden dürfen, ist in der Gesetzesnorm zwar nicht ausdrücklich genannt, ergibt sich jedoch nach der Auffassung des Gesetzgeber insofern bereits aus § 100a I StPO selbst[64], als „das dort ausdrücklich erlaubte Überwachen und Aufzeichnen von Telekommunikation regelmäßig nur unter Einsatz technischer Mittel erfolgen kann“[65]. Zur Auslegung von Normen ist insbesondere auch die jeweilige Gesetzesbegründung des normerlassenden parlamentarischen Gesetzgebers heranzuziehen.[66] Wie auch die vorausgegangenen dogmatischen Untersuchungen der vorliegenden Arbeit ge-

---

[59] Insbesondere der Begriff des Überwachens, vgl. *Berner*/*Köhler*/*Käß*, BayPAG, Art. 34a, Rn. 8.

[60] Gerade auch die (bewusste) Verwendung moderner Telekommunikationstechniken als „Gegenmechanismen“ potentiell überwachter Straftäter zur Erschwerung bzw. Verhinderung einer Überwachbarkeit der geführten Kommunikation rechtfertigt zur Wahrung einer effektiven Strafrechtspflege und Herstellung von „Waffengleichheit“ eine entsprechend weite Auslegung der Tatbestandsbegrifflichkeiten.

[61] Vgl. *Berner*/*Köhler*/*Käß*, BayPAG, Art. 34a, Rn. 8.

[62] Vgl. *Bär*, TK-Überwachung, § 100a StPO, Rn. 15; *Berner*/*Köhler*/*Käß*, BayPAG, Art. 34a, Rn. 8; in diese Richtung auch SK – *Wolter*, StPO, § 100a, Rn. 19; aus diesem Grunde muss bei einem Zugriff auf Fern*sprech*verkehr beides – sowohl Überwachung als auch Aufzeichnung – für sich angeordnet werden, vgl. Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 8, § 100b, Rn. 4.

[63] Vgl. *Berner*/*Köhler*/*Käß*, BayPAG, Art. 34a, Rn. 8.

[64] Vgl. BT-Drs. 16/5846, S. 47.

[65] BT-Drs. 16/5846, S. 47.

[66] Vgl. Maunz/Dürig – *Grzeszick*, GG, Art. 20, Abschnitt VII, 63. EL 2011, Rn. 61.

zeigt haben, lässt sich – bezogen auf die spezielle Konstellation einer Quellen-TKÜ – das Abgreifen eines VoIP-Gesprächs am Endgerät der Kommunikation („an der Quelle“) – hier auf dem zu Telekommunikationszwecken genutzten informationstechnischen System des Absenders bzw. des Empfängers – und Ausleiten der Daten an die Ermittlungsbehörden mittels voher heimlich bzw. verdeckt eingebrachter Überwachungssoftware als „technisches Mittel zur Datenerhebung“[67] mit Blick auf die Gesetzesbegründung wie auch unter grammatischer, teleologischer und gesetzessystematischer Auslegung unter den Tatbestand einer *Überwachung und Aufzeichnung von Telekommunikation* i. S. d. § 100a I StPO subsumieren, ohne dass es hierfür etwa gar der Ziehung einer (ggf. unzulässigen[68]) Rechtsanalogie bedürfte.

Dem stehen auch die Anforderungen des Bestimmtheitsgebotes grds. nicht entgegen. Denn eine Vorhersehbarkeit der *konkreten* Maßnahme und deren (technischer) Realisierungsweise, hier also v. a. das Verwenden einer Überwachungssoftware und deren einzelne technische Abläufe zum Abgreifen der Daten, verlangt das Bestimmtheitsgebot indes nicht.[69] Die ausdrückliche Verankerung einer jeden Maßnahmekonstellationen im Gesetz wäre auch kaum möglich und jedenfalls dem Gebot der Normenklarheit und damit verbunden auch der Übersichtlichkeit gesetzlicher Regelungen wenig dienlich. Vielmehr genügt für die Wahrung des Bestimmtheitsgebotes die grundsätzliche Erkennbarkeit der Anlässe und Voraussetzungen, mit denen ein Verhalten mit dem Risiko einer Überwachung verbunden ist.[70]

Hierbei ist der Tatbestand der §§ 100a, 100b StPO – ggf. unter Heranziehung von Gesetzesmaterialien, juristischer Auslegungsmethodik u. ä. – hinreichend dahingehend auslegbar, dass sich der Staat zum Zugriff auf Telekommunikation (an die jeweilige Telekommunikationsform angepasster) technischer Mittel bedienen kann – sei es nun unmittelbar über eigene technische Mittel oder mittelbar über die eines hierzu verpflichteten Netzbetreibers. Des Weiteren ist angesichts der Offenheit der Tatbestandsformulierung des § 100a I StPO auch nicht ausgeschlossen, dass ein Abgreifen der

---

67 Bundesministerium des Innern, Fragenkatalog SPD, S. 6, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012), in Bezug auf *Remote Forensic Software*, gilt für Quellen-TKÜ-Software insoweit in gleicher Weise; auch gesetzlich verankerte (präventivpolizeiliche) Ermächtigungsgrundlagen zu Maßnahmen der Quellen-TKÜ (bspw. § 20l II S. 1 BKAG, § 15b I HSOG, § 31 III S. 1 POG RP) legen hier die Begrifflichkeit „technisches Mittel“ für eine Überwachungssoftware zum Ausleiten der laufenden Telekommunikation zugrunde.

68 Siehe hierzu die Ausführungen unter 2. Teil A.II.1.a).

69 Vgl. BVerfG NJW 2005, 2603 (2607).

70 Vgl. BVerfG NJW 2005, 2603 (2607).

Telekommunikationsdaten statt auf der Übermittlungsstrecke auch am jeweiligen Endgerät der verwendeten Telekommunikationsanlage erfolgen kann. Denn weder dem Gesetzeswortlaut noch der Gesetzesbegründung[71] lässt sich entnehmen, dass die Überwachung nur durch den Netzbetreiber und nur auf der Übermittlungsstrecke erfolgen darf. Wenngleich freilich die „klassische" Realisierungsweise einer Telekommunikationsüberwachung im Abgreifen und Ausleiten durch den verpflichteten Netzbetreiber zu sehen ist, so schließt sowohl der Wortlaut des § 100b III StPO als auch der des § 100a I StPO ein Anknüpfen am Endgerät nicht aus.[72] Ein grundsätzliches Bewusstsein dahingehend, dass sein Verhalten mit dem Risiko einer Überwachung verbunden ist, ist dem Nutzer einer solchen Telekommunikationsform jedenfalls zuzurechen. Denn dieser ist sich (zumindest abstrakt) bewusst, dass er sich unter Verwendung seines onlinegeschalteten und mit einer VoIP-Software versehenen Computers zum Zwecke des Telekommunizierens einer Telekommunikationsanlage bedient, d. h. mittels einer solchen Kommunikation betreibt, welche unter Beachtung der Zielsetzung des § 100a I StPO einer staatlichen Überwachung zugänglich ist. Auch der Umstand, dass der Nutzer in den Fällen der Quellen-TKÜ VoIP-Dienste nutzt, bei denen die Telekommunikationsdaten verschlüsselt übermittelt werden, ändert hieran nichts. Dem Nutzer verschlüsselter Telekommunikationstechniken dürfte angesichts der von ihm damit getroffenen Sicherheitsvorkehrungen gegen unerwünschte Kenntnisnahme zwar durchaus ein grds. höheres Vertrauen in die Sicherheit seines Kommunikationsmittels zuzubilligen sein, als dies bei unverschlüsselter Kommunikation über das Internet der Fall wäre.[73] Dieses Vertrauen findet jedoch seine Grenzen in den technischen Möglichkeiten, die denjenigen, welche das informationstechnische System „angreifen", zur Verfügung stehen, um die Sicherung am Endgerät zu überwinden[74], da gerade bei Verschlüsselungstechniken die Daten irgendwann zwangsläufig wieder „im Klarzustand" vorliegen.[75]

---

71 Vgl. BT-Drs. 16/5846, S. 47.

72 Dass der technische Anknüpfungspunkt der Maßnahme das Endgerät ist, steht dem Zugriff nach §§ 100a, 100b StPO nicht entgegen (vgl. BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 8), zumal nunmehr auch in der Vorschrift des § 100b II S. 2 Nr. 2 StPO das Endgerät erwähnt wird, vgl. auch *Bär*, TK-Überwachung, § 100a StPO, Rn. 32; Rn. 8; hierauf weist auch *Kudlich*, GA 2011, 193 (207) hin.

73 Vgl. auch *Sieber,* Stellungnahme zu dem Fragenkatalog des BVerfG in dem Verfahren 1 BvR 370/07, S. 5, abrufbar unter http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf (zuletzt aufgerufen 15.06.2012).

74 Vgl. *Sieber*, Stellungnahme zu dem Fragenkatalog des BVerfG in dem Verfahren 1 BvR 370/07, S. 5, abrufbar unter http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf (zuletzt aufgerufen 15.06.2012).

75 Freilich wäre hier auch ein Anknüpfungspunkt für eine etwaige Klarstellung im Gesetz gegeben, um diesbezüglich für endgültige Klarheit und Erkennbarkeit

Der hinreichenden Bestimmtheit der §§ 100a, 100b StPO für Maßnahmen der Quellen-TKÜ steht deshalb auch nicht zwingend entgegen, dass das hier zum Einsatz kommende spezifische technische Mittel in Gestalt einer *Überwachungssoftware* nicht ausdrücklich im Wortlaut geregelt ist.[76] Wenngleich sich aus dem Bestimmtheitsgebot grds. auch ein Bedürfnis zu hinreichend genauer Bezeichnung technischer Eingriffsinstrumente ergibt, verlangt dieses aber keine derartigen gesetzlichen Formulierungen, die jede Einbeziehung von kriminaltechnischen Neuerungen ausschließen.[77] Maßstab ist auch hier die (hinreichende) Erkennbarkeit. So kann dem verständigen Durchschnittsbürger bei Ausrichtung seines kommunikativen Handelns durchaus das Bewusstsein zugeschrieben werden, dass in der modernen Kommunikationswelt vielfältige Arten von Telekommunikationstechnologien existieren und dass darauf zugreifende Maßnahmen und technische Mittel im Rahmen (moderner) Ermittlungstätigkeit auch an die jeweiligen technischen Eigenheiten angepasst und daran ausgerichtet sein müssen. Gerade die offenen Begrifflichkeiten des *Überwachens* und *Aufzeichnens* schließen deshalb nicht zwangsläufig eine (grundsätzliche) Erkennbarkeit dahingehend aus, dass bei softwarebasierter Telekommunikation über informationstechnische Systeme auch entsprechende technische Überwachungsmittel, die ihrerseits an dem zu Kommunikationszwecken verwendeten System anknüpfen, zur Anwendung kommen.[78]

Denn die Quellen-TKÜ stellt sich nach vorzugswürdiger Ansicht als eine besondere Weise der Realisierung einer Telekommunikationsüberwachung nach §§ 100a, 100b StPO dar, nämlich als eine Überwachung und Aufzeichnung verschlüsselt übermittelter Telekommunikation „an der Quelle" mittels spezifischen technischen Mittels, das seine grundsätzliche Legitimation in

---

(qua ausdrücklicher Regelung) zu sorgen; für Einzelheiten hierzu, siehe 3. Teil B.I. u. III.2.

76 Anders hingegen, jedoch ohne genauere Begründung, *Albrecht*, JurPC Web-Dok. 59/2011, Abs. 14, wonach die §§ 100a, 100b StPO der Komplexität der stattfindenden Vorgänge nicht gerecht würden und zu viele Fragen von wesentlicher Bedeutung ungeklärt ließen.

77 Vgl. BVerfG NJW 2005, 1338 (1340); zumal sich auch bei einer ausdrücklichen Regelung zugunsten eines allgemein gehaltenen, auslegungsfähigen strafprozessualen Tatbestandes eine solche auch auf den abstrakten Begriff des *technischen Mittels* zu beschränken hätte, da eine genaue Bezeichnung aller in Frage kommenden technischen Mittel einer übersichtlichen, entwicklungsoffenen und praktikablen Regelung gerade abträglich wäre und auch nicht der üblichen Ausgestaltung (strafprozessualer) Eingriffsnormen entspräche.

78 Gleichwohl ergibt sich hieraus freilich ein Anknüpfungspunkt für eine etwaige gesetzliche Klarstellung, um diesbezüglich für endgültige Klarheit und Erkennbarkeit (qua ausdrücklicher Regelung) zu sorgen; für Einzelheiten hierzu, siehe 3. Teil B.I. u. III.2.

den §§ 100a, 100b StPO findet. Der Gesetzgeber hat indes mit der Normierung der §§ 100a und 100b in der Strafprozessordnung die grundsätzliche Entscheidung zur Gestattung der Überwachung und Aufzeichnung von Telekommunikation zu Zwecken der Strafverfolgung und Straftatenaufklärung getroffen und in diesen Rechtsnormen die wesentlichen Regelungen[79] und Voraussetzungen für die Zulässigkeit von Telekommunikationsüberwachungen und den damit einhergehenden Eingriff in Art. 10 I GG bestimmt. Sind die materiellen Eingriffsvoraussetzungen des *§ 100a I Nr. 1 bis Nr. 3, II, IV StPO* erfüllt und handelt es sich – was für die Einordnung der spezifischen Eingriffssituation der Quellen-TKÜ zur Überwachung von VoIP-Kommunikation anhand technischer und dogmatischer Kriterien zu bejahen ist[80] – bei dem Überwachungsgegenstand, auf den im Rahmen der Maßnahmedurchführung zugegriffen wird, zum Zeitpunkt des Zugriffs (noch bzw. bereits) um ein Überwachen und Aufzeichnen von *Telekommunikation* i. S. d. gesetzlichen Begriffsverständnisses, also des technischen Vorgangs des Aussendens, Übermittelns und Empfangens von als Nachrichten identifizierbaren Signalen mittels Telekommunikationsanlagen[81], so darf die Telekommunikation, deren Überwachung durch die Anordnung legitimiert ist (hier: Telefonie via Internetprotokoll), auch ohne Wissen des Betroffenen gemäß § 100a I StPO mit eigenen Mitteln der Ermittlungsbehörden *überwacht und aufgezeichnet* werden[82] – und zwar auch bzw. gerade mit *technischen Mitteln* zu denen sich auch eine Überwachungssoftware zählen lässt[83]. Dies ist zwar nicht ausdrücklich in § 100a I StPO genannt, ergibt sich jedoch – wie bereits oben näher erläutert – insoweit hinreichend aus der Gesetzesnorm[84], als die von § 100a I StPO ausdrücklich gestattete Überwachung und Aufzeichnung von Telekommunikation „regelmäßig nur unter Einsatz technischer Mittel erfolgen kann“[85]. Wie sich aus den Aussagen des Gesetzgebers schließen lässt, sind für die Überwachung und Aufzeichnung von Telekommunikation nach § 100a I StPO deshalb regelmäßig solche technische Mittel heranzuziehen, die – unter dem Eindruck der Ermächtigungsgrundlage – in

---

79 Zur Wesentlichkeitstheorie vgl. BVerfG NJW 1998, 2515; BVerfG NJW 1979, 359; BVerfG NJW 1978, 807; BVerfG NJW 1972, 1504; siehe hierzu auch 2. Teil A.II.1.

80 Siehe hierzu im Einzelnen 2. Teil A.II.3. und 3. Teil A.I.1.a)aa).

81 Vgl. § 3 Nr. 22 u. 23 TKG.

82 Vgl. BT-Drs. 16/5846, S. 47; auch *Bär*, TK-Überwachung, § 100a StPO, Rn. 32; *ders*., MMR 2008, 215 (219); Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 8.

83 Siehe hierzu 2. Teil A.II.5. und 3. Teil A.I.1.a)bb).

84 So auch BT-Drs. 16/5846, S. 47.

85 BT-Drs. 16/5846, S. 47; ausweislich der Gesetzesbegründung betreffen die Konkretisierungen in der Anordnung (§ 100b II S. 2 Nr. 3 StPO) „auch die Art des technischen Zugriffs auf die zu überwachende Telekommunikation“ (S. 47).

technischer Hinsicht „das dort [in § 100a I StPO, Anm. d. Verf.] ausdrücklich erlaubte Überwachen und Aufzeichnen von Telekommunikation“[86] durch die Strafverfolgungsbehörden im konkreten Fall ermöglichen. Eine alleinige bzw. zwingende Realisierung von TKÜ-Maßnahmen nur unter Mitwirkung des jeweiligen Telekommunikationsdienstleisters nach § 100b III StPO ist gerade nicht gesetzlich vorgeben. Denn nach dem ausdrücklichen Willen des Gesetzgebers wird durch § 100b III StPO „eine Obliegenheit der Strafverfolgungsbehörden, Telekommunikationsüberwachungsmaßnahmen stets unter Mitwirkung eines Telekommunikationsdienstleisters durchzuführen, […] nicht begründet“[87]. Vielmehr sei in § 100a I StPO „eine nicht durch die Mitwirkung der Telekommunikationsdienstleister bedingte Befugnis, Telekommunikation zu überwachen und aufzuzeichnen“[88] enthalten. Beschränkt werde „diese Befugnis lediglich durch die in der gerichtlichen Anordnungsentscheidung näher zu bestimmende Art der Überwachung (vgl. § 100b Abs. 2 Satz 2 Nr. 3 StPO-E)“[89].

Einem verständigen Durchschnittsbürger als (potentiellem) Nutzer ist deshalb durchaus auch ein grundsätzliches Bewusstsein hinsichtlich des Umstandes zuzurechnen, dass auf spezielle Formen von Telekommunikation (hier softwarebasierte P2P-VoIP-Kommunikation) über eine Befugnisnorm, die generell zur heimlichen „Überwachung und Aufzeichnung von Telekommunikation“ legitimiert, in jeweils einer auf die jeweilige Kommunikationstechnik abgestimmten Vorgehensweise von staatlicher Seite zugegriffen wird. Der Tatbestand des § 100a I StPO ist vom Gesetzgeber bewusst entwicklungsoffen gehalten und eine nähere gesetzliche Eingrenzung bzw. Darstellung der einzelnen in Betracht kommenden bzw. Anwendung findenden technischen Mittel (wie im vorliegenden Fall der Überwachungssoftware im Rahmen einer TKÜ an der Quelle) wegen der „Vielgestaltigkeit möglicher Sachverhalte“[90] nicht zwingend[91] erforderlich. Wie auch höchst-

---

[86] BT-Drs. 16/5846, S. 47.

[87] BT-Drs. 16/5846, S. 47; so auch Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 7a, 8 sowie § 100b, Rn. 7; ebenso *Bär*, TK-Überwachung, § 100a StPO, Rn. 32; *ders*., MMR 2008, 215 (219); zust. *Gercke*/*Brunst*, Internetstrafrecht, Kap. 5, S. 350, Rn. 895, Fn. 377; a. A. SK – *Wolter*, StPO, § 100a, Rn. 20 u. § 100b, Rn. 19; *Sankol*, CR 2008, 13 (17); *Buermeyer*/*Bäcker*, HRRS 2009, 433 (440); ebenso noch LG Hamburg, MMR 2008, 423 (424); nunmehr zust. LG Hamburg, MMR 2011, 693 (696).

[88] BT-Drs. 16/5846, S. 47.

[89] BT-Drs. 16/5846, S. 47.

[90] BVerfG NJW 2009, 2431 (2434) zu §§ 94 ff. StPO, trifft insoweit auf § 100a I StPO gleichfalls zu.

[91] Wenngleich eine gesetzliche Klarstellung – wie von Modell 3 näher thematisiert – i. S. größtmöglicher Rechtssicherheit und -klarheit dennoch wünschenswert ist, siehe hierzu 3. Teil B.III.

richterlich mehrfach bestätigt, können nicht stets alle Konstellationen möglicher Sachverhalte – gerade auch wie hier mit Blick auf die rasante technische Entwicklung – ausdrücklich in den Wortlaut einer Rechtsnorm aufgenommen werden.[92] Eine zu detaillierte Regelung diverser Einzelkonstellationen in einer Rechtsnorm könnte ganz im Gegenteil einer übersichtlichen und normenklaren Ausgestaltung auch abträglich sein. Das Erfordernis der Zusammenfassung einer Vielzahl von Einzelkonstellationen unter einen allgemein gehaltenen auslegungsfähigen Tatbestand einer Rechtnorm ist daher auch im Strafprozessrecht grds. unvermeidbares gesetzesgeberisches Element. Dabei bildet auf Rechtsanwendungsebene der „mögliche Wortsinn des Gesetzes […] die äußerste Grenze zulässiger richterlicher Interpretation“[93]. Solange die Grenze zur (belastenden) Rechtsanalogie und der Umgehung des Gesetzesvorbehaltes nicht überschritten sind, entspricht die Zusammenfassung einer Vielzahl von Einzelkonstellation unter dem (abstrakten) Tatbestand einer auslegungsfähigen Rechtsnorm gerade üblicher Gesetzgebungstechnik und steht damit – wenngleich in einem Spannungsverhältnis mit dem Erfordernis hinreichend klarer und bestimmter Ausgestaltung – nicht automatisch im Widerspruch mit den obigen Geboten von Normenklarheit und Tatbestandsbestimmtheit.

Für den heimlichen strafprozessualen Zugriff auf Telekommunikation überschreitet die Einbeziehung neuer Telekommunikationsformen hierbei nicht die Grenzen der Auslegung des § 100a I StPO, die durch das Grundrecht des Fernmeldegeheimnisses (Telekommunikationsgeheimnisses) aus Art. 10 I GG gezogen sind.[94] Denn die Vorschrift ist – wie auch das hiervon eingeschränkte Fernmeldegeheimnis aus Art. 10 I GG – mit ihren Tatbestandsmerkmalen *Überwachung und Aufzeichnung* von *Telekommunikation* vom Gesetzgeber bewusst entwicklungsoffen formuliert worden[95], um neue Techniken und Formen der Nachrichtenübertragung, wie bspw. die hier gegenständliche Sprachkommunikation über Computer via Internetprotokoll (IP), die zum Zeitpunkt des Einfügens der §§ 100a, 100b StPO in die Strafprozessordnung im Jahre 1968[96] technisch noch nicht entwickelt waren, in deren Anwendungsbereich einbeziehen zu können und damit auch auf

---

92 Vgl. BGH-Ermittlungsrichter NStZ 2005, 278 (278); vgl. insoweit auch BVerfG NJW 2009, 2431 (2434); BVerfG NJW 2008, 3627 (3627).

93 Vgl. BVerfG NJW 2008, 3627 (3627); siehe hierzu auch 2. Teil A.II.1.b).

94 Vgl. auch BGH NStZ 1997, 247 (247).

95 Vgl. BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 2 u. 6; vgl. auch *Kudlich*, JuS 2001, 1165 (1166) m. w. N.; *ders*., JA 2010, 310 (312); auch *Käß*, BayVBl. 2010, 1 (6).

96 Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (= G 10) v. 13.08.1968 (BGBl. I S. 949), seitdem vielfach geändert, in jüngerer Zeit insb. durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung und ande-

Rechtsanwendungsebene dem rasanten technischen Entwicklungsfortschritt des Telekommunikationsmarktes gerecht zu werden.

Probates Mittel hierfür kann ohne weiteres eine entwicklungsoffene Eingriffsbefugnis sein, die in Form einer abstrakt gehaltenen Regelung zur „Überwachung und Aufzeichnung von Telekommunikation", mit den gleichfalls entsprechend entwicklungsoffen auszulegenden Eingriffsbefugnissen des *Überwachens* und *Aufzeichnens*, eine individuelle, an die jeweilige Technik angepasste Vorgehensweisen im Einzelfall zulässt, solange diese auf den Zugriff auf Telekommunikation gerichtet ist.

Die Primärmaßnahme einer Quellen-TKÜ ist indes unter den Wortsinn der tatbestandlichen Begrifflichkeiten des § 100a I StPO, sprich eines *Überwachens* und *Aufzeichnens* von *Telekommunikation* mit Hilfe *technischer Mittel,* subsumierbar (vgl. oben) und bewegt sich damit noch im Rahmen zulässiger Gesetzesauslegung.

Auch die *Sekundärmaßnahmen* des heimlichen bzw. verdeckten Einbringens sowie Entfernens der Überwachungssoftware sind vom gesetzlichen Kontext eines Überwachens und Aufzeichnens von Telekommunikation mit Hilfe technischer Mittel i. S. d. § 100a I StPO als für die Realisierung der Maßnahme typische und verhältnismäßige Begleitmaßnahmen ebenfalls mit erfasst.[97] Denn das Bestimmtheitsgebot und der Parlamentsvorbehalt sind gewahrt, wenn begleitende Maßnahmen, die selbst nicht ausdrücklich geregelt sind, aber mit der Durchführbarkeit der im Gesetz vorgesehenen primären Befugnis notwendigerweise verbunden sind, den Kriterien der *Typizität* und *Verhältnismäßigkeit* entsprechen und damit ebenfalls einer gewissen Erkennbarkeit unterliegen.

Eine weitergehende gesetzliche Eingrenzung und Konkretisierung der Primär- und Sekundärmaßnahmen einer Quellen-TKÜ ist deshalb nicht zwingend geboten. Die verfahrensbezogene Konkretisierung des Tatbestandes hat – gerade bei entwicklungsoffen formulierten Befugnisnormen – von Verfassungs wegen vielmehr der Ermittlungsrichter im jeweiligen Überwachungsbeschluss zu leisten.[98] Gemäß der Gesetzesbegründung enthält § 100a I StPO eine Befugnis, Telekommunikation zu überwachen und aufzuzeichnen, welche „lediglich durch die in der gerichtlichen Anordnungsentscheidung näher zu bestimmende Art der Überwachung"[99] beschränkt werde. Denn die Konkretisierungen des § 100b II S. 2 Nr. 3 StPO sollen nach dem

---

rer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der RL 2006/24/EG v. 21.12.2007 (BGBl. I S. 3198).

97 Siehe im Einzelnen 2. Teil B.III.

98 Vgl. auch BVerfG NJW 2009, 2431 (2434); BVerfG NJW 2005, 1917 (1920); BVerfG NJW 1977, 1489 (1490); BVerfG NJW 1976, 1735 (1735).

99 BT-Drs. 16/5846, S. 47.

Willen des Gesetzgebers auch „die Art des technischen Zugriffs auf die zu überwachende Telekommunikation“[100] betreffen, um einen zielgerichteten Einsatz der Maßnahme zu erreichen.[101] So obliegt es insbesondere auch den Gerichten, vom technischen Fortschritt bedingte und ermöglichte neuartige Ermittlungsmaßnahmen, die sich ggf. auch in den Randbereichen der Tatbestandlichkeit befinden, in das bestehende System strafprozessualer Befugnisse und deren Eingriffsvoraussetzungen einzupassen[102].

Die bestehenden strafprozessualen Regelungen über die Überwachung und Aufzeichnung von Telekommunikation genügen indes auch den Anforderungen des Bestimmtheitsgebotes, wonach *Anlass* und *Zweck* des Eingriffs sowie der Verwendungszweck der erhobenen Daten durch den Gesetzgeber bereichsspezifisch und präzise bestimmt worden sein müssen.

Aus den Vorschriften des § 100a I Nr. 1 bis 3, 100b StPO geht präzise hervor, dass der Anlass für eine strafprozessuale Überwachung und Aufzeichnung von Telekommunikation der Umstand ist, dass sich die in § 100a III StPO genannten Maßnahmeadressaten einer Telekommunikationstechnik bedienen und hierbei ggf. ermittlungsrelevante Informationen austauschen. Aus diesem Grunde besteht ein (ermittlungstaktisches) Erfordernis für den heimlichen Zugriff auf räumlich distanzierte Kommunikation, um so eine in Verdacht stehende „schwere Straftat“ nach § 100a II StPO (sog. *Katalogstraftat*), welche im Einzelfall auch schwer wiegt und deren Aufklärung andernfalls erheblich erschwert oder aussichtslos ist, verfolgen und (möglicherweise) aufklären zu können. Diesem bereichsspezifisch niedergelegten Anlass unterliegt auch die Quellen-TKÜ zur Überwachung und Aufzeichnung verschlüsselter Internettelefonie.

Auch der mit einer Maßnahme der Quellen-TKÜ verbundene Zweck des Eingriffs in das Fernmeldegeheimnis sowie der Zweck der Verwendung der mittels der Maßnahme erhobenen Daten geht bereichsspezifisch und präzise aus den Regelungen der §§ 100a, 100b StPO hervor. Gemäß höchstrichterlicher Rspr. ist diesbezüglich von hinreichender Bestimmtheit einer Gesetzesnorm auszugehen, wenn ihr „Zweck aus dem Gesetzestext in Verbindung mit den Materialien deutlich wird […]; dabei reicht es aus, wenn sich der Gesetzeszweck aus dem Zusammenhang ergibt, in dem der Text des Gesetzes zu dem zu regelnden Lebensbereich steht […]“[103]. Zieht man den der Regelung in §§ 100a, 100b StPO zugrunde liegenden Lebensbereich, also den Informationenaustausch zwischen Menschen mittels Telekommunika-

100 BT-Drs. 16/5846, S. 47.

101 Vgl. BT-Drs. 16/5846, S. 47.

102 Vgl. hierzu Anm. *Jahn*, JuS 2009, 1048 (1048).

103 BVerfG NJW 1984, 419 (424).

tionsanlagen, heran, so ergibt sich hieraus deutlich der Zweck des mit TKÜ-Maßnahmen verbundenen Eingriffs in Art. 10 I GG, nämlich der Erkenntnisgewinn aus dem Inhalt und den näheren Umständen von Telekommunikationsvorgängen, bei denen der Verdacht besteht, dass sie im Zusammenhang mit der Begehung, dem Versuch der Begehung oder dem Vorbereiten von schweren Straftaten nach § 100a I Nr. 1, II StPO geführt werden, zur Verwendung zu Beweiszwecken oder als Spurenansätze im Strafverfahren. Dem Verfolgen und Aufklären von (schweren) Straftaten unter Zugriff auf und Erkenntnisgewinn aus Telekommunikationsvorgängen dient auch der Maßnahmezweck der Quellen-TKÜ.

Somit geht auch der *Verwendungszweck* der im Rahmen einer auf §§ 100a, 100b StPO gestützten Quellen-TKÜ-Maßnahme gewonnenen Daten bereichsspezifisch und präzise aus den bestehenden Regelungen hervor. Einerseits sind die Ermittlungsmethoden der Strafprozessordnung hinsichtlich Datenerhebung und Datenumfang zwar (grds.) weit gefasst.[104] Andererseits wird der Datenzugriff durch den Verwendungszweck begrenzt, der unter Berücksichtigung des Normzusammenhangs, in welchen die Ermittlungsbefugnisse des *Achten Abschnitts des Ersten Buches* der StPO eingebettet sind, zu beurteilen ist.[105] Als heimliche Ermittlungsmaßnahmen stehen die §§ 100a, 100b StPO hierbei (erst recht) unter der „strengen Begrenzung auf den Ermittlungszweck“[106], der in der Verwendung der gewonnenen Erkenntnisse als Beweise bzw. Spurenansätzen zur Aufklärung von Straftaten liegt. Gemäß dem Grundsatz der Zweckbindung[107], der (unmittelbar oder mittelbar) zahlreichen Bestimmungen der Strafprozessordnung zu entnehmen ist (vgl. §§ 152 II, 155 I, 160, 161 I 1, 163 I 2, 170, 244 II, 244 III 2 Alt. 2, 264 I, 483 StPO[108]), sind strafprozessuale Ermittlungsmaßnahmen „nur zulässig, soweit dies zur Vorbereitung der anstehenden Entscheidungen im Hinblick auf die in Frage stehende Straftat nötig ist“[109]. Auf die Ermittlung „anderer Lebenssachverhalte und Verhältnisse“[110] hingegen erstrecken sich die strafprozessualen Eingriffsbefugnisse nicht.[111] Diesen Vorgaben unterliegt auch die Verwendung der gewonnenen Erkenntnisse im Rahmen von TKÜ-Maßnahmen zur Aufklärung der ermittlungsgegenständlichen

---

104 Vgl. BVerfG NJW 2009, 2431 (2434); bereits BVerfG NJW 2005, 1917 (1920).

105 Vgl. entsprechend BVerfG NJW 2009, 2431 (2434).

106 BVerfG NJW 2009, 2431 (2434).

107 Vgl. BVerfG NJW 2000, 55 (57).

108 Vgl. BVerfG NJW 2009, 2431 (2434); BVerfG NJW 2005, 1917 (1920).

109 BVerfG NJW 2009, 2431 (2434).

110 BVerfG NJW 2009, 2431 (2434).

111 Vgl. BVerfG NJW 2009, 2431 (2434); bereits BVerfG NJW 2005, 1917 (1920); auch BVerfG NJW 2006, 976 (980).

Straftaten im jeweiligen Strafverfahren (Ausgangsverfahren) bzw. nach Maßgabe des § 477 II S. 2 StPO[112] als Zufallserkenntnisse in anderen Strafverfahren[113].

Als weitere Anforderung an gesetzliche Ermächtigungsgrundlagen verlangt das Bestimmtheitsgebot, dass auch die *Grenzen* des grundrechtlichen Eingriffs bereichsspezifisch und präzise bestimmt sind. Auf die hier vorliegende Konstellation bezogen bedeutet dies, dass die in den §§ 100a, 100b StPO enthaltenen Regelungen die Grenzen des mit einer Quellen-TKÜ zulässigen Eingriffs aufzeigen müssen.

Von einem Teil der vertretenen Stimmen wird das Vorhandensein von eingriffsspezifischen Beschränkungen, wie sie das BVerfG in seiner Entscheidung vom 27.02.2008 für die Frage des grundrechtlichen Maßstabs festgelegt hat, in den bestehenden Regelungen der §§ 100a, 100b StPO verneint. Denn den vom BVerfG festgelegten Anforderungen, wonach Art. 10 I GG der alleinige grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zu einer Quellen-Telekommunikationsüberwachung ist, wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt und dies durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt ist[114], würden die §§ 100a, 100b StPO nicht gerecht, da darin keine derartigen Vorgaben enthalten seien.[115]

---

112 Gemäß § 477 II S. 2 StPO dürfen personenbezogene Daten, die auf Grund einer Maßnahme, welche nach der Strafprozessordnung nur bei Verdacht bestimmter Straftaten – wie bspw. die TKÜ nach §§ 100a I Nr. 1, II StPO nur bei Verdacht einer Katalogstraftat – zulässig ist, erlangt wurden, ohne Einwilligung der von der Maßnahme betroffenen Personen zu Beweiszwecken in anderen Strafverfahren nur zur Aufklärung solcher Straftaten verwendet werden, zu deren Aufklärung eine solche Maßnahme nach der StPO hätte angeordnet werden dürfen. Die Verwertung derartiger Zufallserkenntnisse zu Beweiszwecken ist somit nur zulässig, wenn die Eingriffsvoraussetzungen der jeweiligen Maßnahme (bei mittels einer TKÜ-Maßnahme erlangten Erkenntnissen die Voraussetzungen des § 100a StPO) also auch in dem anderen Verfahren erfüllt sind, sodass auch dort eine solche Maßnahme hätte angeordnet werden dürfen. Der Vorschrift des § 477 II S. 2 StPO liegt hierbei der Gedanke des sog. *hypothetischen Ersatzeingriffs* zugrunde, hierzu BT-Drs. 16/5846, S. 66; vgl. auch *Bär*, TK-Überwachung, § 100a StPO, Rn. 60; als Grundlage für weitere Ermittlungen bzw. als Spurenansatz können derartige Zufallserkenntnisse hingegen unabhängig von den Beschränkungen des § 477 II S. 2 herangezogen werden, vgl. BVerfG NJW 2005, 2766 (2766); ebenso BT-Drs. 16/5846, S. 64.

113 *Anderes* Strafverfahren bedeutet in diesem Kontext ein Verfahren wegen einer anderen prozessualen Tat i. S. d. § 264 StPO, vgl. Löwe-Rosenberg – *Schäfer*, StPO und GVG, Zweiter Band, § 100a StPO, Rn. 88 m. w. N.

114 Vgl. BVerfG NJW 2008, 822 (826).

115 Vgl. *Braun*/*Roggenkamp*, K&R 2011, 681 (683); auch *Albrecht*, JurPC Web-Dok. 59/2011, Abs. 14 u. 15; i. E. auch Anm. *Brodowski*, JR 2011, 533 (536).

Dem ist jedoch insoweit zu widersprechen, als sich in Einklang mit der Rspr. des BVerfG[116] durchaus entsprechend beschränkende Vorgaben für Eingriffe mittels TKÜ-Maßnahmen in Form der Quellen-TKÜ in den §§ 100a, 100b StPO feststellen lassen, welche auch im Rahmen der Beurteilung der Bestimmtheit der Ermächtigungsgrundlage die Grenzen des grundrechtlichen Eingriffs mittels Quellen-TKÜ hinreichend aufzeigen:

Die Regelung des § 100a I StPO lässt in hinreichend bestimmter Weise die Grenzen von Quellen-TKÜ-Maßnahmen erkennen, die unter Verwendung einer Überwachungssoftware auf einem zur Telekommunikation genutzten informationstechnischen System realisiert werden. Grenze einer Quellen-TKÜ ist das ausschließliche Erfassen von Daten aus laufenden Telekommunikationsvorgängen – in Abgrenzung zu Maßnahmen der Online-Durchsuchung. Diese Grenze wird von § 100a I StPO erkennbar aufgezeigt. Denn bei Vorliegen der Voraussetzungen der § 100a I Nr. 1 bis 3, II, IV StPO gestattet die strafprozessuale Befugnisnorm des § 100a I StPO mit der Rechtsfolge der Überwachung und Aufzeichnung von Telekommunikation *nur* den Zugriff auf *Telekommunikation*, sprich auf Daten aus laufenden technischen Aussende-, Übermittlungs- und Empfangsvorgängen von als Nachrichten identifizierbaren Signalen mittels Telekommunikationsanlagen (§ 3 Nr. 22, 23 TKG). Bereits aus der gesetzlichen Vorschrift des § 100a I StPO selbst geht damit eindeutig hervor, dass nur solche Daten Gegenstand einer auf § 100a I StPO gestützten Quellen-TKÜ sein dürfen und nicht sonstige Daten, welche außerhalb laufender Telekommunikation auf dem Zielsystem vorhanden sind, da diese mit einer auf die Eingriffsbefugnis der §§ 100a, 100b StPO gestützten Maßnahme schon der ausdrücklichen gesetzlichen Eingriffsbefugnis nach nicht erfasst werden dürfen.[117] Denn hierbei würde es sich nicht mehr um eine Maßnahme zur Überwachung und Aufzeichnung von Telekommunikation handeln, sondern vielmehr um eine Maßnahme von der Eingriffsqualität einer Online-Durchsuchung[118], was jedoch keine Quellen-*Telekommunikations*überwachung mehr darstellen würde und nicht mehr von der Legitimationswirkung der §§ 100a, 100b StPO umfasst wäre. Die in § 100a I StPO enthaltene Begrenzung auf *Telekommunikation* stellt insoweit eine auch Maßnahmen der Quellen-TKÜ begrenzende rechtliche Vorgabe dar und steht damit in Einklang mit der Maßgabe, welche durch das BVerfG in seiner Entscheidung vom

---

116 Vgl. BVerfG NJW 2005, 2603 (2607).

117 So zutr. auch LG Hamburg, MMR 2011, 693 (696), wonach die Vorschrift „allein die Überwachung der ‚Telekommunikation', nicht aber sonstiger Daten für zulässig erklärt" (696), womit „der von der Vorschrift gestattete Überwachungsrahmen […] hinreichend deutlich abgegrenzt [ist]" (696); a. A. hingegen *Hoffmann-Riem*, JZ 2008, 1009 (1022) sowie *Becker*/*Meinicke*, StV 2011, 50 (51).

118 Für Einzelheiten zur sog. *Online-Durchsuchung*, siehe 1. Teil A.II.2.a).

27.02.2008[119] für eine alleinige Grundrechtsbetroffenheit des Art. 10 I GG und zur Abgrenzung der Quellen-TKÜ von Maßnahmen der Online-Durchsuchung zugrunde gelegt wurde, nämlich dass Quellen-TKÜ-Maßnahmen durch rechtliche Vorgaben ausschließlich auf Daten aus laufenden Telekommunikationsvorgängen beschränkt sein müssen.

Der hinreichenden Bestimmtheit der Grenzen des Eingriffs einer Quellen-TKÜ in den §§ 100a, 100b StPO steht auch nicht entgegen, dass die vom BVerfG für die Frage des grundrechtlichen Maßstab aufgestellte Maßgabe, wonach die ausschließliche Erfassung von Daten aus laufenden Telekommunikationsvorgängen neben rechtlichen Vorgaben auch durch technische Vorkehrungen sichergestellt sein muss[120], nicht in den §§ 100a, 100b StPO ausdrücklich geregelt ist. Die Aufnahme von Vorgaben zu technischen Vorkehrungen ist nicht zwingend erforderlich. Denn die Sicherstellung entsprechender technischer Vorkehrungen zur Umsetzung der (auf Grundlage der § 100a I StPO angeordneten) ausschließlichen Erfassung von Daten aus laufender Telekommunikation (und nicht sonstiger Daten) ist grds. Sache der Staatsanwaltschaft (bzw. der von ihr beauftragten Ermittlungspersonen), die im Ermittlungsverfahren über das „Ob" und „Wie" der Durchführung einer angeordneten Maßnahme zu entscheiden hat (§ 36 II S. 1 StPO)[121]. Etwas anderes ergibt sich indes auch nicht aus den Feststellungen des BVerfG zum grundrechtlichen Maßstab. Denn das BVerfG verlangt diesbezüglich, dass die ausschließliche Erfassung von Daten aus laufenden Telekommunikationsvorgängen durch rechtliche Vorgaben *und* technische Vorkehrungen sichergestellt sein muss, und nicht etwa, dass dies durch rechtliche Vorgaben *zu* technischen Vorkehrungen erfolgen müsse.[122] Die Anforderungen der Normenklarheit dienen zwar grds. auch dazu, dass der Verwaltung für ihr Handeln hinreichend klare Maßstäbe bereitgestellt werden. In den Fällen von TKÜ-Maßnahmen erfolgt die Umsetzung der jeweiligen Maßnahme jedoch nach § 100b I S. 1, II S. 2 Nr. 3 StPO auf Grundlage einer (i. d. R. richterlichen) Anordnungsentscheidung, nach deren Maßgaben die Strafverfolgungsbehörden Überwachungsmaßnahmen durchführen dürfen. Dem Gericht ist es indes unbenommen, „zur Begrenzung des

---

119 BVerfG NJW 2008, 822.

120 Vgl. BVerfG NJW 2008, 822 (826).

121 Vgl. BGH-Ermittlungsrichter NStZ 2005, 278 (279); vertiefend zur Umsetzung der Anordnung durch die Ermittlungsbehörden bei Maßnahmen der Quellen-TKÜ, LG Hamburg, MMR 2011, 693 (696).

122 Freilich empfiehlt es sich gleichwohl zur Sicherstellung einer revisionsfesten Verwendung der Software im konkreten Fall entsprechende Vorgaben in den anordnenden Beschluss mit aufzunehmen, siehe hierzu 3. Teil A.I.2.; die Aspekte der Revisionsfestigkeit und Rechtssicherheit geben indes auch für eine gesetzliche Klarstellung Anknüpfungspunkte, siehe 3. Teil A.III.2. u. 3.

Eingriffs im Einzelfall schon im Beschluss zur Gestattung einer unter Richtervorbehalt stehenden Maßnahme Einzelheiten der Art und Weise von deren Durchführung zu regeln“[123].

In der Regelung des § 100b II S. 2 Nr. 3 StPO ist ausdrücklich vorgesehen, dass die Maßnahme in der Anordnung durch das erlassende Gericht näher konkretisiert wird. Dies trägt dem Umstand Rechnung, dass es nach gefestigter Rspr. des BVerfG[124] gerade auch „Aufgabe des Richters ist, von vornherein für eine angemessene Begrenzung der Zwangsmaßnahme Sorge zu tragen. Da die Ermächtigung der Exekutive, […] in den grundrechtlich geschützten Bereich des Betroffenen einzugreifen, regelmäßig dem Richter vorbehalten ist, trifft ihn als Kontrollorgan der Strafverfolgungsbehörden zugleich die Pflicht, durch eine geeignete Formulierung […] [des Beschlusses] im Rahmen des Möglichen und Zumutbaren sicherzustellen, daß der Eingriff in die Grundrechte meßbar und kontrollierbar bleibt […]“[125].

Die Verankerung entsprechender eingriffsbegrenzender Vorgaben für die Umsetzung von Quellen-TKÜ-Maßnahmen in der jeweiligen Anordnung widerspricht aber auch insoweit nicht den Feststellungen des BVerfG, als dieses in seiner Entscheidung vom 27.02.2008 indes von „rechtlichen Vorgaben“ spricht, und nicht etwa allein von „*gesetzlichen* Vorgaben“.[126] Rechtliche Vorgaben sind aber neben den Vorgaben, welche die jeweilige Befugnisnorm auf gesetzlicher Ebene festlegt, in gleicher Weise auch die Vorgaben, welche das erlassende Organ in der jeweiligen Anordnung für die Umsetzung der angeordneten Maßnahme festsetzt.[127]

---

123 BGH-Ermittlungsrichter NStZ 2005, 278 (279).

124 Vgl. BVerfG NJW 1976, 1735 (1735 f.); BVerfG NJW 1999, 2176 (2176); BVerfG NStZ 2000, 601 (601); BVerfG BeckRS 2005, 24601, BVerfG NJW 2009, 2431 (2436).

125 BVerfG NJW 1976, 1735 (1735 f.); hierfür kann sich das Gericht bei fehlender eigener (technischer) Kenntnis bspw. auch externen Sachverstandes u. ä. bedienen, siehe hierzu im Einzelnen 3. Teil A.I.2.

126 Deshalb ist *Braun*, jurisPR-ITR 3/2011 Anm. 3 und auch *Buermeyer*, http://ijure.org/wp/archives/756 (zuletzt aufgerufen 15.06.2012) zu widersprechen, wenn diese dahingehend argumentieren, dass aus den Feststellungen des BVerfG (BVerfG NJW 2008, 822, 826) allein zu folgern sei, dass zur Schaffung „rechtlicher Vorgaben“ i. S. d. Entscheidung des BVerfG nur der Gesetzgeber berufen sein kann (vgl. *Braun*, jurisPR-ITR 3/2011 Anm. 3).

127 Vgl. auch Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 7a; in diese Richtung, i. E. aber offengelassen auch *Henrichs*, Kriminalistik 2008, 438 (439).

c) Wahrung des Verhältnismäßigkeitsgrundsatzes

Die §§ 100a, 100b StPO und darauf gestützte Maßnahmen der Quellen-TKÜ werden hinsichtlich einer Überwachung und Aufzeichnung von Telekommunikation „an der Quelle" unter Einsatz einer Überwachungssoftware auch dem zu beachtenden allgemeinen *Grundsatz der Verhältnismäßigkeit* gerecht, wonach Grundrechtseingriffe einem legitimen Zweck dienen und als Mittel zu diesem Zweck geeignet, erforderlich und angemessen sein müssen[128]:

aa) Legitimer Zweck

Die Befugnis zur Überwachung und Aufzeichnung von Telekommunikation nach §§ 100a, 100b StPO und eine darauf gestützte Quellen-TKÜ verfolgen den legitimen öffentlichen Zweck der Verfolgung und Aufklärung schwerer Straftaten im Zusammenhang mit der Nutzung von Telekommunikation.[129] Das BVerfG[130] hat im Rahmen seiner Rspr. wiederholt hervorgehoben, dass die „wirksame Strafverfolgung, die Verbrechensbekämpfung und das öffentliche Interesse an einer möglichst vollständigen Wahrheitsermittlung im Strafverfahren"[131] legitime Zwecke darstellen, welche „eine Einschränkung des Fernmeldegeheimnisses rechtfertigen können"[132]. Denn „die Aufklärung von Straftaten, die Ermittlung des Täters, die Feststellung seiner Schuld und seine Bestrafung wie auch der Freispruch des Unschuldigen"[133] stellen „die wesentlichen Aufgaben der Strafrechtspflege"[134] dar, welche „zum Schutz der Bürger den staatlichen Strafanspruch in einem justizförmigen und auf die Ermittlung der Wahrheit ausgerichteten Verfahren in gleichförmiger Weise durchsetzen soll"[135]. Die ansteigende Nutzung von elektronischen oder digitalen Kommunikationsmitteln verbunden mit entsprechenden Möglichkeiten zur Verschlüsselung und Verschleierung sowie deren Ausbreitung auf nahezu sämtliche Lebensbereiche[136] er-

---

128 Vgl. BVerfG NJW 2008, 822 (828); BVerfG NJW 2004, 999 (1008); BVerfG NJW 2007, 2464 (2468); st. Rspr.

129 Vgl. BVerfG NJW 2003, 1787 (1789).

130 Vgl. BVerfG NJW 1988, 329 (330); BVerfG NJW 1990, 563 (564); BVerfG NJW 2000, 55 (65); BVerfG NJW 2003, 1787 (1789); BVerfG NJW 2006, 976 (980); BVerfG NJW 2009, 2431 (2434).

131 BVerfG NJW 2009, 2431 (2434).

132 BVerfG NJW 2009, 2431 (2434).

133 BVerfG NJW 2006, 976 (980).

134 BVerfG NJW 2006, 976 (980).

135 BVerfG NJW 2006, 976 (980).

136 So auch BVerfG NJW 2008, 822 (829).

schwert es den Strafverfolgungsbehörden in zunehmendem Maße, die ihnen obliegenden Aufgaben der Strafverfolgung und Straftatenaufklärung wirkungsvoll wahrzunehmen.[137] Die konkrete Maßnahme der strafprozessualen Quellen-TKÜ dient hierbei dem legitimen Zweck des Auffindens verfahrenserheblicher Daten, welche im Rahmen von (verschlüsselt übermittelter) softwarebasierter P2P-Internetkommunikation anfallen, und mithin – i. S. d. verfassungsrechtlichen Zielvorgabe „möglichst vollständige[r] Wahrheitsermittlung im Strafverfahren“[138] – dem Erlangen von Beweismitteln zur Verfolgung und Aufklärung von damit in Zusammenhang stehenden (schweren) Straftaten.

Die §§ 100a, 100b StPO als Ermächtigungsgrundlage und darauf gestützt die ermittlungstechnische Möglichkeit, mittels einer Maßnahme der Quellen-TKÜ auf die Sprachdaten (und/oder Videodaten) einer geführte P2P-VoIP-Telefonie vor der Verschlüsselung auf dem System des Absenders bzw. nach der Entschlüsselung auf dem System des Empfängers zuzugreifen, ist zur Erreichung der genannten Zwecke zudem auch geeignet und erforderlich sowie verhältnismäßig i. e. S.:

bb) Geeignetheit

Die in den §§ 100a, 100b StPO verankerte Möglichkeit, Telekommunikation zu überwachen und aufzuzeichnen, ist dazu geeignet, Erkenntnisse zum Zwecke der Strafverfolgung, Verbrechensbekämpfung und Wahrheitsermittlung zu gewinnen. Ebenso ist eine darauf gestützte konkrete Ermittlungsmaßnahme der Quellen-TKÜ als Maßnahme zur Erlangung gerade von Daten aus softwarebasierten P2P-Internettelefonaten und den darin enthaltenen Informationen in unverschlüsselter und damit in für Ermittlungsbehörden einsehbarer Form ein geeignetes Mittel zum Erkenntnisgewinn für die Verfolgung und Aufklärung von Straftaten. Als Maßnahme, die unmittelbar durch die Ermittlungsbehörden selbst durchgeführt wird, eignet sich die Quellen-TKÜ hierbei für einen insgesamt zuverlässigen und (in gewissen Grenzen) planbaren Zugriff, ohne dem Risiko der effektiven Durchsetzbarkeit bei einer Mitwirkung privater, oftmals im Ausland ansässiger Unternehmen (VoIP-Diensteanbieter) an der Durchführung von Ermittlungen zu unterliegen, wie bspw. dem Risiko zeitlicher Verzögerung, fehlender Informationen oder (bei ggf. schon fehlender gesetzlichen Verpflichtung zum Mitwirken[139]) u. U. auch

---

137 Vgl. BVerfG NJW 2008, 822 (829) für den präventiven Bereich.

138 BVerfG NJW 2000, 55 (65).

139 Ob Anbieter von P2P-VoIP-Diensten überhaupt unter die Verpflichtung des § 100b StPO fallen, ist indes fraglich, siehe hierzu 2. Teil A.II.6.b).

mangelnder Kooperationsbereitschaft[140], z. B. zu einem Bereitstellen – soweit überhaupt verfügbar (vgl. unten) – von Zweitschlüsseln oder technischen Hintertüren in Verschlüsselungsprodukten[141].

Die Eignung der auf die §§ 100a, 100b StPO gestützten Maßnahme der Quellen-TKÜ wird auch nicht dadurch tangiert, dass Nutzern von VoIP-Kommunikations-diensten über informationstechnische Systeme durchaus technische Möglichkeiten des Selbstschutzes zur Verfügung stehen, um Zugriffe in Form der technischen Infiltration ihres Systems mit einer Überwachungssoftware wirkungsvoll zu verhindern.[142] Denn nach überzeugender Auffassung des BVerfG ist „im Rahmen der Eignungsprüfung […] nicht zu fordern, dass Maßnahmen, welche die […] Norm erlaubt, stets oder auch nur im Regelfall Erfolg versprechen“[143], solange die Erfolgsprognose für Zugriffe im Einzelfall „zumindest nicht offensichtlich fehlsam“[144] ist. Dies ist auch bei Maßnahmen der Quellen-TKÜ der Fall. Zwar kann ein Nutzer durch vielfältige technische Abwehrmaßnahmen, bspw. durch Installation von Antiviren-Software oder/und Firewall-Programmen u. ä. versuchen, sich nach dem Stand der Technik gegen heimliche Zugriffe auf sein System zu schützen. Mit Blick auf das heimliche Einbringen und Verwenden einer Überwachungssoftware auf einem informationstechnischen System wie hier zum Zwecke der Überwachung verschlüsselt übermittelter VoIP-Kommunikation an der Quelle kann aber – jedenfalls im Regelfall[145] – nicht davon ausgegangen bzw. unterstellt werden, dass jede in Frage kommende Zielperson einer derartigen Maßnahme auch (ausreichende) technische Schutzvorkehrungen gegen solche Zugriffe ergreift bzw. diese technischen Schutzvor-

---

140 So werben Anbieter von VoIP-Diensten i. d. R. gerade mit der besonderen Vertraulichkeit der Verschlüsselungstechniken ihrer VoIP-Programme, die Dritte von einer Kenntnisnahme der Kommunikationsinhalte ausschließen sollen.

141 Da Anbieter sich im Falle einer freiwilligen Kooperation, also ohne gesetzliche Verpflichtung zu einem Vorhalten derartiger Zugriffsmöglichkeiten, ihren Kunden gegenüber möglicherweise in zivilrechtlicher Hinsicht pflichtwidrig verhalten könnten, vgl. auch Anm. *Brodowski*, JR 2011, 533 (534), Fn. 20.

142 Vgl. insoweit auch BVerfG NJW 2008, 822 (829).

143 BVerfG NJW 2008, 822 (829).

144 BVerfG NJW 2008, 822 (829).

145 Ausnahmen wären höchstens z. B. bei technisch besonders versierten Zielpersonen denkbar, die ihre Endgeräte durch spezielle, ggf. auch selbst entworfene Schutzprogramme und Abwehrstrategien vor heimlicher Installation von Software zu schützen versuchen; einerseits stellt diese Gruppe jedoch nicht das Gros der Nutzer von Internet- und VoIP-Diensten dar und auch die technisch versierten „Experten“ sind in gewisser Weise vor menschlicher Nachlässigkeit im Umgang mit technischen Sicherungsmaßnahmen nicht gefeit, so auch *Sieber*, Stellungnahme zu dem Fragenkatalog des BVerfG in dem Verfahren 1 BvR 370/07, S. 13 f., abrufbar unter http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf (zuletzt aufgerufen 15.06.2012).

kehrungen fehlerfrei in sein System implementiert[146], ausführt und auf dem aktuellen Stand hält bzw. das an sich notwendige Maß an vernünftigem Misstrauen im Umgang mit dem Internet und hierüber stattfindender virtueller Interaktion aufbringt. Auch ist angesichts der informationstechnischen Entwicklung zu erwarten, dass derartige Schutzmaßnahmen des Nutzers wiederum durch spezifische staatliche Vorgehensweisen und weiter optimierte technische Möglichkeiten zum heimlichen Einbringen von Überwachungsprogrammen auf informationstechnischen Systemen[147] umgangen werden können[148], was im Einzelfall gar auf einen regelrechten „Wettlauf der Infiltrations- und Abwehrtechniken" hinauslaufen kann.[149] Mithin machen auch die mitunter intensiven Vorermittlungen und -arbeiten zur Ermöglichung eines heimlichen bzw. verdeckten Einschleusens der Überwachungssoftware die Maßnahme nicht insgesamt ungeeignet, da dies – wie die in der Praxis bislang durchgeführten Quellen-TKÜ-Maßnahmen belegen – erfolgreich gelingen kann. Daher stellt auch die bislang vergleichsweise geringe Zahl an Quellen-TKÜ-Maßnahmen[150] in der Praxis kein durchgreifendes Argument gegen die Eignung der Maßnahme dar.

Die Maßnahme der Quellen-TKÜ in der technischen Art ihrer Realisierung ist zudem geeignet, sowohl Spurenansätze als auch revisionsfeste Erkenntnisse zur Verfolgung und Aufklärung schwerer Straftaten zu liefern. Durch entsprechende technische wie auch organisatorische Vorkehrungen kann einer Manipulation der abgegriffenen Daten vorgebeugt werden. So lässt sich bspw. durch eine dem Stand der Technik entsprechende, von der Überwachungssoftware automatisch vorgenommene Verschlüsselung der in Echtzeit abgegriffenen und ausgeleiteten TK-Daten während der Übermittlung zum Behörden-Server zugunsten der Beweismittelauthentizität und Beweismittelintegrität und damit der Beweissicherheit wirksam dafür Sorge tragen, dass eine Manipulation der Daten durch den Betroffenen oder Dritte nicht stattfindet, da diese hierzu sowohl Kenntnis der IP-Adresse des Ziel-Servers als auch des Übertragungsprotokolls, des Verschlüsselungsverfahrens

---

146 Vgl. insoweit auch BVerfG NJW 2008, 822 (829).

147 Für Einzelheiten zu den gegenwärtigen technischen Möglichkeiten des Einbringens, siehe 1. Teil A.II.4.b).

148 Vgl. insoweit auch BVerfG NJW 2008, 822 (829).

149 Vgl. auch *Sieber*, Stellungnahme zu dem Fragenkatalog des BVerfG in dem Verfahren 1 BvR 370/07, S. 13, abrufbar unter http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf (zuletzt aufgerufen 15.06.2012), der treffend beschreibt, dass „gegen jede Angriffsform eine Abwehrtechnik und gegen jede Abwehrtechnik eine Umgehungsstrategie entwickelt werden kann." (S. 13); siehe hierzu auch die Ausführungen unter 2. Teil B.III.2.a).

150 Siehe hierzu 1. Teil A.II.1.; für konkrete Zahlen zur Anwendung von Quellen-TKÜ-Software in Bayern, siehe auch die Antwort des Bayerischen Staatsministeriums des Innern, LT-Drs. 16/10082, S. 2 und LT-Drs. 16/10469, S. 2, 4 ff.

sowie des eingesetzten Schlüssels haben müssten.[151] Dem lässt sich bspw. durch einen fortlaufenden Qualitätssicherungs- und Optimierungsprozess[152] der Kontroll- und Sicherungsmaßnahmen zusätzlich Rechnung tragen. Des Weiteren greift gegenüber der Eignung einer Maßnahme der Quellen-TKÜ im Ergebnis auch nicht der Einwand durch, dass der Beweiswert der mittels der Überwachungssoftware erlangten Erkenntnisse möglicherweise begrenzt sei, weil – wie dies teilweise vertreten wird – eine technische Bestätigung der Authentizität der gewonnenen Daten grds. eine nicht vorhandene exklusive Kontrolle des überwachten Systems durch die Ermittlungspersonen im relevanten Zeitpunkt voraussetze[153]. Eine solche ist zur Erlangung von gerichtsverwertbaren Beweismitteln auch nicht zwingend notwendig. Denn einerseits bedeutet eine fehlende Exklusive Kontrolle nicht, dass den erhobenen Daten kein Informationswert zukommt.[154] Zum anderen lässt sich zur gerichtsverwertbaren Beweismittelgewinnung diesem Umstand durch genaue und lückenlose Dokumentation und Protokollierung des Überwachungssoftwareeinsatzes und der hierüber erhobenen Daten wie auch durch eine vor Veränderung oder unbefugter Löschung zugriffssicher geschützte anschließende weitere Behandlung und Speicherung der erhobenen Daten gemäß dem Stand der Technik Rechnung tragen. Darüber hinaus bietet die Aufzeichnung von Internettelefonaten, also von akustischer und ggf. auch visueller IP-Kommunikation, zugunsten der Feststellung der Authentizität der abgegriffenen Daten – anders als dies bei elektronischer Kommunikation in Schriftform (E-Mail, Instant Messaging) gegeben ist – zusätzlich die Möglichkeit, ggf. Stimmabgleiche u. ä. für eine Zuordnung des Gesprochenen zu einer bestimmten Person vorzunehmen bzw. visuelles Datenmaterial in Augenschein zu nehmen[155], falls die Urheberschaft abgefangener Telekommunikationsinhalte in Frage stehen sollte.

cc) Erforderlichkeit

Eine Befugnisnorm wie die §§ 100a, 100b StPO zur Überwachung und Aufzeichnung von Telekommunikation ist für einen Erkenntnisgewinn aus via Telekommunikationsanlagen geführter Fernkommunikation erforderlich, da insoweit kein milderes Mittel besteht, um auf die Gespräche und deren oftmals flüchtige Inhalte (vollständig) zuzugreifen. Eine auf die §§ 100a,

---

151 Vgl. insoweit auch die Antwort der Bundesregierung, BT-Drs. 17/7760, S. 16.

152 Vgl. hierzu die Antwort des Bayerischen Staatsministeriums des Innern, LT-Drs. 16/10607, S. 2.

153 Vgl. bspw. *Hansen*/*Pfitzmann*, DRiZ 2007, 225 (228).

154 Vgl. BVerfG NJW 2008, 822 (829).

155 In diese Richtung auch *Gercke*/*Brunst*, Internetstrafrecht, Kap. 5, S. 347, Rn. 882, Fn. 366.

100b StPO gestützte Überwachungsmaßnahme in Form der Quellen-TKÜ ist hierbei zur Ermöglichung einer Einsichtnahme in verschlüsselt übermittelte Internettelefonie im Rahmen strafprozessualer Ermittlungen erforderlich:

- Die Durchführung einer TKÜ in der „klassischen" Weise, also unter Abgreifen der Daten auf dem Übertragungsweg, wäre bei der spezifischen Situation der peer-to-peer VoIP-Telefonie für den Zugriff auf Telekommunikationsinhalte ungeeignet und als Alternative für eine Quellen-TKÜ nicht erfolgversprechend, da eine solche – wie bereits eingangs geschildert – nur verschlüsselte Daten liefern würde. Eine Entschlüsselung dieser codiert abgefangenen Daten wäre wohl selbst mit hohem technischen Aufwand kaum bzw. jedenfalls nicht zeitnah möglich[156], da bei den regelmäßig für P2P-Kommunikation zum Einsatz kommenden Verschlüsselungstechniken (bei Skype bspw. ein proprietärer Verschlüsselungsalgorithmus nach dem AES-Standard) Schlüssel mit großer Länge und hoher Zufälligkeit verwendet werden, welche automatisch generiert werden und nur temporär gültig sind.[157]

  Auf Grund des Umstandes, dass es – wie im 2. Teil der Arbeit bereits näher ausgeführt[158] – darüber hinaus für die P2P-Software von Skype und vergleichbaren VoIP-Diensteanbietern gegenwärtig wohl weder einen *Schlüssel* für die Aufhebung der Codierung der Daten gibt noch für Ermittlungsbehörden eine *Hintertür* (*Backdoor*) in das Programm zur Verfügung steht[159], ist ein milderes, in gleicher Weise geeignetes und erfolgversprechendes Mittel für den Zugriff auf verschlüsselte Internettelefonie als das Anknüpfen am Absender- oder Empfängersystem mittels vorher heimlich installierter Überwachungssoftware nicht ersichtlich.

---

156 Vgl. BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 107a.; auch LG Hamburg, MMR 2011, 693 (695).

157 Vgl. Anm. *Brodowski*, JR 2011, 533 (533).

158 Für Einzelheiten zur Erforderlichkeit und der Frage des Bestehens eines Schlüssels oder einer Backdoor, siehe 2. Teil B.III.2.b)aa) u. bb).

159 Vgl. Anm. *Bär*, MMR 2011, 691 (691 f.); so auch die Antwort des Parl. Staatssekretärs beim Bundesminister des Innern, *Bergner*, für die Bundesregierung im Rahmen der 135. Sitzung des Deutschen Bundestags am 26.10.2011 (BT-PlPr. 17/135 16064 D), wonach es in den Fällen P2P-geführter VoIP zwischen zwei internetfähigen Endgeräten (softwarebasierte P2P-VoIP) „Skype […] nach derzeitigem Kenntnisstand der Bundesregierung schon aus technischen Gründen nicht möglich [ist], Inhaltsdaten den Justiz-, Strafvollzugs- oder Regierungsbehörden zur Verfügung zu stellen" (16064 D); anders hingegen *Braun*/*Roggenkamp*, K&R 2011, 681 (685) m. w. N., *Hoffmann-Riem*, JZ 2008, 1009 (1021), m. w. N. wie auch *Buermeyer*, http://ijure.org/wp/archives/756 (zuletzt aufgerufen 15.06.2012) m. w. N., regelmäßig jedoch unter der Einschränkung, dass nicht zu 100 Prozent gewiss sei, ob tatsächlich eine solche Möglichkeit konkret bestehe.

Doch selbst wenn ein Schlüssel oder eine „Backdoor" existieren würden, so müsste einer Vorgehensweise über eine dieser beiden Möglichkeiten nicht zwangsläufig auch ein vergleichbar geeignetes und dabei zugleich milderes Mittel wie das Vorgehen über eine Quellen-TKÜ darstellen:

Für die Erlangung eines passenden Schlüssels zur Decodierung der (mittels klassischer TKÜ) in verschlüsselter Form abgefangenen TK-Daten wären die Ermittlungsbehörden zunächst auf die Mitarbeit des jeweiligen VoIP-Diensteanbieters[160] angewiesen, soweit dieser im Besitz der technischen Details der VoIP-Software und des verwendeten Verschlüsselungsalgorithmus ist, um hierüber eine Schlüssel zu erstellen. Handelt es sich nicht um einen universellen Schlüssel, sondern ist z. B. für jede Softwareversion oder Softwareaktualisierung ein eigener bzw. neuer Schlüssel nötig oder kommt gar für jedes einzelne Internettelefonat ein eigener Schlüssel temporär zum Einsatz[161], so wären die Behörden auf die wiederholte Mitwirkung (privater) Dritter angewiesen und das Gelingen strafprozessualer Ermittlungen nicht nur von deren Mitwirkungsfähigkeit und -bereitschaft[162] zu einer Entschlüsselbarkeit der – regelmäßig als vertraulich und mithörsicher beworbenen[163] – P2P-VoIP-Kommunikation

---

160 Hingegen kann der jeweilige Netzbetreiber/Provider hierzu nichts beitragen, da über dessen Leitungen nur der Transport der Daten stattfindet, die nötige Kenntnis bzw. die Verfügungsgewalt über ggf. bestehende Entschlüsselungsmöglichkeiten („Schlüssel") bzw. versteckte Zugangsmöglichkeiten in das VoIP-Programm („Backdoor") hingegen beim jeweiligen VoIP- Diensteanbieter liegt.

161 So bspw. Anm. *Brodowski*, JR 2011, 533 (533), wonach „für die Kommunikationsverschlüsselung […] zumeist automatisch generierte, temporäre Schlüssel mit großer Länge und hoher Zufälligkeit verwendet [werden]" (533).

162 Hierzu bspw. das Skype-Informationsblatt *Responding zu Law Enforcement Records Requests*: „In response to a subpoena or other court order, Skype will provide: [.] Registration information provided at time of account registration [.] E-mail address [.] IP address at the time of registration [.] Financial transactions […] Destination telephone numbers for any calls placed to the public switched telephone network (PSTN) [.] All service and account information, including any billing address(es) provided, IP address (at each transaction), and complete transactional information"; „Skype can provide records showing account creation, financial transaction and use of PSTN interconnections [.] Due to the way by which Skype works, Skype does NOT have any records of user ‚logins', ‚log offs' or other general online/offline status [.] The Skype system is designed in such a way that voicemail is not centrally stored [.] Calls, IMs and other activities between Skype users do not create billing records […]" (http://cryptome.org/isp-spy/skype-spy.pdf, zuletzt aufgerufen 15.06.2012); zur umstrittenen Frage, ob und in welchem Umfang softwarebasierte VoIP-Diensteanbieter überhaupt zur Mitwirkung gesetzlich verpflichtet sind, siehe 2. Teil A.II.6.b); für Einzelheiten zur Mitwirkung Dritter, siehe 2. Teil A.II.6.

163 So wirbt bspw. Skype auf seiner Internetpräsenz damit, dass „der Schutz Ihrer Informationen […] sowie der geführten Gespräche bei uns an erster Stelle

abhängig, sondern auch von den Zufälligkeiten des Vorhandenseins des „richtigen" Schlüssels für die „richtige" Software, nämlich dass für das seitens des überwachten Nutzers gerade verwendete VoIP-Programm und der konkreten Programmversion ein passender Schlüssels vorliegt, womit der Erfolg oder Misserfolg strafprozessualer Ermittlungen – zugespitzt formuliert – letztlich vom gerade aktuellen Softwarestand des vom Nutzer verwendeten VoIP-Programms abhängig wäre. Überdies birgt die Existenz von Schlüsseln in Verschlüsselungsprodukte und -verfahren Gefahren für den Schutz und die Vertraulichkeit codierter digitaler Informationen insgesamt und erhöht insbesondere für verschlüsselte Telekommunikation auch das Risiko unbefugter Kenntnisnahmemöglichkeit, falls diese Schlüssel in die Hände unbefugter Dritter gelangen sollten.

Auch für die Nutzung einer Hintertür (*Backdoor*) in das jeweilige VoIP-Programm wären Ermittlungsbehörden von der (technischen Möglichkeit wie auch Bereitschaft zur) Mitarbeit der VoIP-Diensteanbieter abhängig[164], welche – wie bereits oben angesprochen – oftmals gerade mit der Vertraulichkeit und Zugriffssicherheit ihrer VoIP-Programme werben und hierfür Hintertüren, also potentielle Schwachstellen, in ihr Programm bewusst einbauen müssten[165] bzw. sofern eine solche Hintertür doch bereits herstellerseits vorhanden sein sollte, die für die Nutzung erforderlichen, zu den jeweiligen Softwareversionen passenden technischen Konfigurationen und Zugangsmöglichkeiten zum „Eintreten" in das VoIP-Programm durch die Hintertür gegenüber den Ermittlungsbehörden offen legen müssten.

Der Eingriff müsste bei der Vorgehensweise über eine solche „Backdoor" darüber hinaus auch nicht unbedingt vergleichsweise milder aus-

---

[stehen]" (http://www.skype.com/intl/de/security/#encryption, aufgerufen 12.01.2012), „alle Sprach- und Videoanrufe und IM-Chats zwischen Skype-Nutzern […] verschlüsselt [werden]" (https://support.skype.com/de/faq/FA31/Verwendet-Skype-Verschlusselung, zuletzt aufgerufen 15.06.2012) und dass „Skype […] seinen Nutzern Schutz vor einer großen Bandbreite möglicher Angriffe, wie z. B. Identitätswechsel, Abhören, Man-In-The-Middle-Angriffe und Datenmodifizierung während der Übertragung [bietet]" (http://www.skype.com/intl/de/security/detailed-security/, zuletzt aufgerufen 15.06.2012).

164 Zur noch nicht abschließend geklärten Frage, ob Anbieter softwarebasierter VoIP-Dienste überhaupt den Verpflichtungen des § 100b III StPO unterfallen, siehe 2. Teil A.II.6.b).

165 Wohingegen Skype nach eigenen Angaben seine Verschlüsselungsalgorithmen gerade dazu verwendet, „die Kommunikationen von Skype-Nutzern davor zu schützen, dass sie in die Hände von Hackern und Kriminellen fallen", um dabei zu helfen, „die Privatsphäre von Nutzern und die Integrität von Daten zu bewahren, die von einem Nutzer zu einem anderen gesendet werden" (http://www.skype.com/intl/de/security/detailed-security/, zuletzt aufgerufen 15.06.2012).

fallen, als dies beim heimlichen Einsatz einer staatlichen Überwachungssoftware im Rahmen der Durchführung von Quellen-TKÜ-Maßnahmen der Fall ist. Auch hier würde heimlich am System des Betroffenen angesetzt werden, indem sich „über die Hintertür" in das dort installierte VoIP-Programm unbemerkt eingeklinkt wird, um auf diese Weise auf die Kommunikationsdaten in unverschlüsselter Form zugreifen zu können.[166] Insofern fände hier letztlich ebenfalls ein Abgreifen der Daten „an der Quelle" statt, nur ohne Infiltration mit einer (gesonderten) Überwachungssoftware, als deren „Funktion" bereits von der VoIP-Software selbst erfüllt würde. Überdies entstünden durch das (ggf. standardmäßige) Einrichten von Backdoors unter den Kriterien der IT-Sicherheit und des Datenschutzes weitergehende Gefahren für den Schutz informationstechnischer Systeme im Allgemeinen, da solche technischen Hintertüren Schwachstellen im Programm darstellen und somit als potentielle Einfallstore für den missbräuchlichen Zugriff Dritter auf das Programm wie darüber auch auf das System, in dessen Systemprozesse es integriert ist, insgesamt, fungieren können[167].

In der Gesamtschau stehen somit – insbesondere auch angesichts der vielen divergierenden Informationen hinsichtlich der Existenz oder Nichtexistenz von (universellen) Schlüsseln oder technischen Hintertüren (*Backdoors*) in den gegenwärtig auf dem Markt befindlichen unzähligen (kostenfreien) VoIP-Programmen[168] – im Vergleich zur punktuellen Installation einer Überwachungssoftware und anschließenden Überwachung der unverschlüsselten Kommunikationsdaten durch die Ermittlungsbehörden nicht ohne weiteres mildere, gleich geeignete Mittel zur Verfügung. Zwar würden – die technische und rechtspolitische Umsetzbarkeit dieser Möglichkeiten einmal unterstellt – die Benutzung eines (aktuellen) Schlüssels zur Entschlüsselung abgefangener codierter Daten oder der Zugriff auf uncodierte Daten über eine „Backdoor" in das VoIP-Programm für die Ermittlungsbehörden die mithin intensive Vorarbeit zum verdeckten Einspielen einer Überwachungssoftware auf das Zielsystem sowie für den Betroffenen die mit dieser Sekundärmaßnahme verbundenen Beeinträchtigungen im Idealfall entfallen lassen. Jedoch wäre für die Verwirklichung einzelner Überwachungen dann das (wiederholte und kontinuier-

---

166 Und deren Verwendung sich nach Anm. *Brodowski*, JR 2011, 533 (534; 537) auf die §§ 100a, 100b StPO stützen lasse.

167 Vgl. insoweit auch die Stellungnahme von Skype im Rahmen der Anhörung durch die Bundesnetzagentur im Jahr 2004, S. 16, abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Stellungnahmen/SkypeTechnologiesId714pdf.pdf?__blob=publicationFile (zuletzt aufgerufen 15.06.2012).

168 Siehe hierzu auch 2. Teil B.III.2.b).

liche) Mitwirken des VoIP-Diensteanbieters zwingend notwendig und einziges Mittel, was – wie oben dargelegt – auch deutliche Risiken hinsichtlich der faktischen Gewährleistbarkeit einer Überwachung verschlüsselter Internettelefonie (Risiko zeitlicher Verzögerung, stetiges Erfordernis des Vorliegens des aktuellsten Schlüssels angepasst an die jeweilige Programmversion bzw. des temporären Schlüssels für jeden konkreten Gesprächsvorgang, Abhängigkeit von Kooperationsbereitschaft und technischen Möglichkeiten über den Globus verstreuter Hersteller/Anbieter u. ä.) allein auf Grundlage etwaiger[169] Mitwirkungsverpflichtungen in sich birgt. Überdies ist den §§ 100a, 100b III StPO – wie oben bereits ausführlich geschildert[170] – nach dem ausdrücklichen Willen des Gesetzgebers gerade keine Pflicht oder Obliegenheit für die Ermittlungsbehörden zu entnehmen, eine Überwachung stets nur unter Mitwirkung verpflichteter Dritter durchzuführen[171].

- Auch Maßnahmen der akustischen Wohnraumüberwachung nach § 100c I StPO stellen für die Überwachung von in Wohnräumen mittels verschlüsselter Telekommunikationstechniken geführter Telefonate keine Alternative zu einer Maßnahme der Quellen-TKÜ dar.[172] Zwar kann in zulässiger Weise im Rahmen einer Maßnahme der akustischen Wohnraumüberwachung auch das nichtöffentlich gesprochene Wort der Zielperson (bzw. bei einem zufälligen Lautschalten auch des Gesprächspartners) im Rahmen eines dort ablaufenden Telefongesprächs erfasst werden.[173] Daraus ist jedoch nicht zu schließen, dass Maßnahmen nach § 100c StPO damit als (gleich geeignete) Alternative zur Quellen-TKÜ, noch dazu als mildere, in Betracht kommen. Bereits der Normzweck des § 100c StPO ist nicht vorrangig auf eine Überwachung und Aufzeichnung von Telekommunikation gerichtet. Auch weist eine akustische Wohnraumüberwachung keine vergleichbare Eignung mit einer (Quellen-)TKÜ-Maßnahme zum Erhalt eines umfassenden Einblicks in die geführte Telekommunikation auf, da hierbei im Regelfall (anders nur bei

---

169 So ist bislang nicht abschließend geklärten, ob Anbieter von softwarebasierten P2P-VoIP-Diensten überhaupt nach § 100b III StPO verpflichtet sind, siehe 2. Teil A.II.6.b); diesen Umstand vernachlässigt *Buermeyer*, http://ijure.org/wp/archives/756 (zuletzt aufgerufen 15.06.2012), der sich als milderes Mittel für „eine klassische TKÜ unter Einschaltung des Providers – etwa Skype“ ausspricht, zumal Skype gerade nicht „Provider“ i. S. d. üblichen Begriffsverständnisses ist, da dieser weder den Zugang ins Internet vermittelt noch Datenpakete über das Datennetz transportiert.

170 Für Einzelheiten zur Frage der Inanspruchnahme der Mitwirkung Dritter, siehe 2. Teil A.II.6.c).

171 Vgl. BT-Drs. 16/5846, S. 47.

172 In diese Richtung offenbar Anm. *Brodowski*, JR 2011, 533 (534 f.).

173 Für Einzelheiten, siehe auch 1. Teil A.II.2.b).

einem zufälligen „Lautschalten“ des Gesprächs) lediglich ein Teil des Telefongesprächs, nämlich die gesprochenen Worte der Zielperson, erfasst werden könnte. Zudem gelten Maßnahmen der akustischen Wohnraumüberwachung zu Recht als „ultima ratio der Strafverfolgung“[174] und stellen als gegenwärtig grundrechtsintensivste heimliche Ermittlungsmaßnahme auch kein „milderes“ Mittel dar.

- Entsprechendes gilt auch für akustische Überwachungsmaßnahmen außerhalb von Wohnungen nach § 100f StPO. Auch im Rahmen von Maßnahmen nach § 100f I StPO kann das außerhalb von Wohnungen im Rahmen von Telefongesprächen nichtöffentlich gesprochene Wort zwar in zulässiger Weise (mit-)erfasst werden.[175] Hieraus jedoch den Schluss zu ziehen, dass außerhalb des räumlichen Schutzbereiches des Art. 13 I GG deshalb ein „probates technisches Mittel“[176] zum Abhören von verschlüsselten IP-Telefonaten „an der Quelle“ (über mobile Endgeräte) zur Verfügung stünde und eine Quellen-TKÜ damit nicht erforderlich sei[177], greift zu kurz, da Maßnahmen nach § 100f I StPO bereits vom Regelungszweck her nicht vorrangig auf – erst recht nicht als Ersatz für – eine Überwachung und Aufzeichnung von Telekommunikation ausgerichtet und ausgelegt sind (vgl. bspw. auch das Fehlen entsprechender Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung). Darüber hinaus wäre in einem solchen Falle das Erfassen der begehrten Kommunikation von erheblichen Zufälligkeiten abhängig (z. B. Abhör- und Aufzeichnungsqualität bei Einsatz von Richtmikrofonen, Aufrechterhalten der Überwachung bei einem Fortbewegen der Zielperson etc.) und würde zudem im Regelfall mitunter nur einen Teil des Telefonates für Ermittlungspersonen erfassbar machen, nämlich nur das gesprochene Wort der Zielperson, da ein Lautschalten von Gesprächen im Außenbereich eher den Ausnahmefall darstellen dürfte. Maßnahmen nach § 100f I StPO stellen somit weder ein geeignetes technisches Mittel zum Abhören verschlüsselter Telefonate noch eine vergleichbar geeignete Alternative zu einer Maßnahme der Quellen-TKÜ dar. Lediglich für den (ermittlungspraktisch wohl eher seltenen) Fall, dass es für die Ermittlungen im konkret gegenständlichen Ermittlungsverfahren zur Erforschung des Sachverhaltes eines Zugriff auf das gesamte Telefonat nicht bedürfte und der Strafverfolgungsbehörde allein die Erfassung des im Rahmen des Telefonates gesprochenen Wortes der Zielperson genügt, wäre eine Maßnahme nach § 100f StPO als Alternative im Einzelfall denkbar.

---

174 Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 74.

175 Für Einzelheiten, siehe auch 1. Teil A.II.2.c).

176 Anm. *Brodowski*, JR 2011, 533 (534).

177 So Anm. *Brodowski*, JR 2011, 533 (534 f.).

Eine Quellen-TKÜ auf Grundlage der §§ 100a, 100b StPO ist deshalb auch nicht mit dem Argument mangelnder Erforderlichkeit abzulehnen.

dd) Angemessenheit

Die §§ 100a, 100b StPO und hierauf gestützte Maßnahmen der Quellen-TKÜ werden darüber hinaus auch den Anforderungen der Verhältnismäßigkeit im engeren Sinne (Angemessenheit) gerecht. Nach st. Rspr. des BVerfG[178] verlangt das Gebot der Verhältnismäßigkeit i. e. S., „dass die Schwere des Eingriffs bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe stehen darf“[179]. Hierfür ist auf Seiten des Gemeinwohlinteresses das Gewicht derjenigen Ziele und Belange einzubeziehen, denen der Eingriff dient.[180] Dies ist unter anderem davon abhängig, „wie bedeutsam die Rechtsgüter sind, die mit Hilfe der Maßnahme geschützt werden sollen, und wie wahrscheinlich der Eintritt einer Rechtsverletzung ist“[181]. Hierbei erfährt das Allgemeininteresse durch die Kriterien der Tatverdachtsstärke und der Schwere des Tatvorwurfs sein konkretes Gewicht.[182] Demgegenüber ist auf Seiten des Individualinteresses zu berücksichtigen, „unter welchen Voraussetzungen welche und wie viele Grundrechtsträger wie intensiven Beeinträchtigungen ausgesetzt sind“[183]. Die Schwere des Eingriffs erhöht sich insbesondere dann, wenn eine Maßnahme heimlich erfolgt.[184] Im Bereich der Strafverfolgung sind daher bei heimlichen Eingriffen in das Grundrecht des Fernmeldegeheimnisses aus Art. 10 I GG „besonders hohe Anforderungen an die Bedeutung der zu verfolgenden Straftat und den für den Zugriff erforderlichen Grad des Tatverdachts zu stellen“[185].

Bei der Abwägung zwischen Gemeinwohlinteresse und Individualinteresse ist in Bezug auf die Schwere des Eingriffs auf Seiten des *Individualin-*

---

178 Bereits BVerfG NJW 1970, 555 (555); fortführend BVerfG NJW 1984, 419 (424); BVerfG NJW 1994, 1577 (1579); BVerfG NJW 2005, 2603 (2609); BVerfG NJW 2008, 822 (829).

179 BVerfG NJW 2008, 822 (829); vgl. auch BVerfG NJW 1994, 1577 (1579); BVerfG NJW 2000, 55 (61); BVerfG NJW 2004, 999 (1012); BVerfG NJW 2005, 2603 (2609); BVerfG NJW 2009, 2431 (2434).

180 Vgl. BVerfG NJW 2000, 55 (61); BVerfG NJW 2009, 2431 (2434).

181 BVerfG NJW 2005, 2603 (2609); auch BVerfG NJW 2009, 2431 (2434).

182 Vgl. hierzu Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 34 f. m. w. N.; BVerfG NJW 1999, 2176 (2176).

183 BVerfG NJW 2000, 55 (61).

184 Vgl. BVerfG NJW 2005, 2603 (2609 f.); BVerfG NJW 2006, 976 (981); BVerfG NJW 2008, 822 (830); BVerfG NJW 2009, 2431 (2434).

185 BVerfG NJW 2009, 2431 (2434).

teresses zunächst zu berücksichtigen, dass Maßnahmen der Quellen-TKÜ *heimlich* ablaufen. Denn Ermittlungsmaßnahmen mit heimlichen Eingriffen in die Kommunikationsfreiheit bergen „spezifische Risiken für die Rechte der Betroffenen“[186]. Hierzu zählt insbesondere der Umstand, dass Betroffene – anders als bei offenen Maßnahmen – sich der heimlichen bzw. verdeckten Eingriffe regelmäßig erst dann mit rechtlichen Mittel erwehren können, wenn diese bereits durchgeführt sind – und auch nur dann, wenn sie über die Maßnahme informiert wurden oder auf andere Weise Kenntnis erlangt haben.[187] Die Möglichkeit, der konkreten Maßnahme bei Nichtvorliegen der Eingriffsvoraussetzungen bereits vor oder bei ihrer Durchführung entgegenzutreten bzw. zumindest die Einhaltung der im richterlichen Beschluss festgesetzten Grenzen beim Vollzug der richterlichen Anordnungen selbst zu überwachen und ggf. Ausuferungen entgegenzutreten, besteht – anders als bei offenen Maßnahmen – bei heimlich ablaufenden Ermittlungsmaßnahmen wie der Quellen-TKÜ gerade nicht.[188] Der Ausschluss derartiger Einflussmöglichkeiten auf den Gang der Ermittlung verstärkt indes das Gewicht des grundrechtlichen Eingriffs.[189] Aus diesem Grunde stellt in einem Rechtsstaat Heimlichkeit staatlicher Eingriffsmaßnahmen die Ausnahme dar und bedarf einer besonderen Rechtfertigung.[190] In diesem Zusammenhang ist für die konkrete Maßnahme der Quellen-TKÜ zudem zu berücksichtigen, dass der mit der Maßnahme verbundene Eingriff – gerade auch zur Wahrung der Heimlichkeit der Überwachung – darauf ausgerichtet und technisch dazu geeignet ist, die Verwendung von Verschlüsselungstechnologie zu umgehen und damit vom Betroffenen ergriffene Vorkehrungen

---

186 BVerfG NJW 2009, 2431 (2435).

187 Vgl. BVerfG NJW 2009, 2431 (2435); BVerfG NJW 2005, 2603 (2609).

188 Vgl. BVerfG NJW 2009, 2431 (2435); BVerfG NJW 2008, 822 (830); BVerfG NJW 2006, 976 (981).

189 Vgl. BVerfG NJW 2008, 822 (830); zum Element der Heimlichkeit von Ermittlungsmaßnahmen auch *Kudlich*, HFR 2007, S. 208.

190 Vgl. BVerfG NJW 2008, 822 (830) m. w. N.; gleichwohl stellt die Heimlichkeit staatlicher Ermittlungstätigkeit grds. aber keinen Umstand dar, der für sich betrachtet die Unzulässigkeit der Maßnahmen begründet, da es „weder rechtsstaatliche Grundsätze noch strafprozessuale Bestimmungen [aus]schließen […], im Rahmen der Aufklärung von Straftaten Methoden und Mittel anzuwenden, deren Gebrauch für den Tatverdächtigen nicht als polizeiliches Handeln erkennbar ist“ (BGH NJW 1996, 2940, 2942); ebenso BGH NJW 1996, 2940 (2942); in diese Richtung auch *Kudlich*, HFR 2007, S. 210, der zu Recht feststellt, dass nicht-offene Ermittlungsmethoden der StPO nicht grds. wesensfremd sein müssen, da „der verdeckte Charakter von Maßnahmen […] Bestandteil einer Reihe strafprozessualer Ermittlungsbefugnisse [ist]“ (210), deren besondere Eingriffsintensität allerdings besondere materielle (bspw. Katalogtaten, Subsidiaritätsklausel) und formelle (Richterzuständigkeit) Sicherungen erfordert (208).

zum „informationellen Selbstschutz […]“[191] zu unterlaufen. Derartiges erhöht ebenfalls das Gewicht des grundrechtlichen Eingriffs.[192]

Weiterhin ist in die Abwägung der Umstand mit einzustellen, dass die Überwachung und Aufzeichnung der geführten Telekommunikation des Betroffenen mitunter über einen *längeren Zeitraum* erfolgen kann[193]. Der Umfang der erfassten TK-Daten (und damit auch der Grundrechtseingriff) ist hierbei noch erheblich größer als bei einmaligen Zugriffen, zumal längerfristige Überwachung auch ein Risiko von Profilbildungen u. ä. in Bezug auf das Kommunikationsverhalten des Betroffenen in sich birgt.[194]

Außerdem ist mit Blick auf das Kriterium der Streubreite der Maßnahme und damit der Zahl möglicher Betroffener eingriffserhöhend auch der Umstand mit einzubeziehen, dass neben dem Nutzer des überwachten Zielgerätes zwangsläufig auch dessen *Kommunikationspartner* und deren Interesse an der Wahrung der Vertraulichkeit räumlich distanzierter Kommunikation von der Überwachung und Aufzeichnung der ausgetauschten Informationen betroffen sind.[195] Unter dem Aspekt der Zahl möglicher Grundrechtsbetroffener ist daher auch für die Maßnahme der Quellen-TKÜ in die Abwägung mit einzustellen, dass prinzipiell sämtliche Nutzer einschlägiger TK-Dienste Betroffene einer solchen Überwachungsmaßnahme werden können. Bereits aber die Befürchtung einer Überwachung und Aufzeichnung von Telekommunikation, deren Auswertung, Verwendung und ggf. Übermittlung an anderen Behörden kann „schon im Vorfeld zu einer Befangenheit in der Kommunikation, zu Kommunikationsstörungen und zu Verhaltensanpassungen […] führen“[196].

Daneben tritt auf Seiten des Individualinteresses des Weiteren hinzu, dass die *Inhalte* von Kommunikation – die gerade primärer Ermittlungsgegenstand von Maßnahmen der Quellen-TKÜ sind – in höherem Maße schutzwürdig sind, als sonstige Kommunikationsdaten.[197] Hierbei kann es auch nicht ausgeschlossen werden, dass bei der Erfassung diesbezüglicher Kommunikationsinhalte personenbezogene Daten betroffen sind, deren Informationen dem Kernbereich der höchstpersönlichen Lebensgestaltung[198] zuzu-

---

191 BVerfG NJW 2008, 822 (830).

192 Vgl. BVerfG NJW 2008, 822 (830).

193 Vgl. insoweit § 100b I S. 4 und S. 5 StPO zu Erst- und Verlängerungsanordnungen.

194 Vgl. insoweit auch BVerfG NJW 2008, 822 (830).

195 Vgl. auch BVerfG NJW 2008, 822 (830) m. w. N.

196 BVerfG NJW 2000, 55 (63).

197 Vgl. BVerfG NJW 2009, 2431 (2435).

198 Ob personenbezogene Daten diesem Kernbereich entstammen, ist insbesondere davon abhängig, ob die Kommunikation ihrem Inhalt nach „höchstpersönlichen

ordnen sind. Die Menschenwürdegarantie aus Art. 1 I GG verlangt deshalb auch im Gewährleistungsbereich des Art. 10 I GG Vorkehrungen zum Schutz der individuellen Entfaltung im Kernbereich privater Lebensgestaltung.[199]

Für die Maßnahme der Quellen-TKÜ ist ferner zu berücksichtigen, dass die Verwendung der als Mittel zur Datenerhebung eingebrachten Überwachungssoftware auf einem zu Telekommunikationszwecken genutzten informationstechnischen System stattfindet, welches regelmäßig eine Vielzahl von *sonstigen Daten* enthalten kann, die ohne Bezug zu laufender Telekommunikation stehen und deren Informationen weitreichende Schlüsse auf den Nutzer und dessen Privatleben zulassen können.

Auf Seiten des *Allgemeininteresses* hingegen ist das Gewicht des verfassungsrechtlich anerkannten und in der Rspr. des BVerfG wiederholt hervorgehobenen Bedürfnisses effektiver Strafverfolgung und wirksamer Verbrechensbekämpfung[200] bei der Beurteilung der Verhältnismäßigkeit i. e. S. zu berücksichtigen. Hierbei liegt gerade eine „möglichst vollständige Wahrheitsermittlung im Strafverfahren – zur Überführung von Straftätern ebenso wie zur Entlastung Unschuldiger – "[201] im öffentlichen Interesse.[202] Denn „der […] Aufklärung von Straftaten kommt nach dem Grundgesetz hohe Bedeutung zu"[203]. Mit Blick auf den technischen Fortschritt ist hierbei dem Umstand Rechnung zu tragen, dass die gestiegene Nutzung moderner elektronischer und digitaler Telekommunikationsmittel und deren Vordringen in nahezu sämtliche Lebensbereiche die Strafverfolgung erschweren.[204] Der zunehmende Einsatz der neuen Kommunikationstechniken bei der Begehung von Straftaten und die damit verbundene „Effektivierung krimineller Handlungen"[205] führen insgesamt zu einer Erschwerung der Ermittlungstätigkeit bei der Verfolgung von Straftaten und machen ein „Schritthalten der Strafverfolgungsbehörden mit der technischen Entwicklung"[206] erforder-

---

Charakter" (2436) aufweist und „in welcher Art und Intensität sie aus sich heraus die Sphäre anderer oder Belange der Gemeinschaft berührt" (2436); nicht zu dem absolut geschützten Kernbereich privater Lebensgestaltung gehören jedenfalls „Kommunikationsinhalte, die in unmittelbarem Bezug zu konkreten strafbaren Handlungen stehen, wie etwa Angaben über die Planung bevorstehender oder Berichte über begangene Straftaten" (BVerfG NJW 2009, 2431, 2436); zu den Grundsätzen des Kernbereichs privater Lebensgestaltung, siehe grundlegend auch BVerfG NJW 2004, 999 (999) sowie die Ausführungen unter 2. Teil A.III.1.

199 Vgl. BVerfG NJW 2009, 2431 (2436).

200 Vgl. BVerfG NJW 2000, 55 (65) m. w. N.

201 BVerfG NJW 2000, 55 (65).

202 Vgl. BVerfG NJW 2000, 55 (65) m. w. N.

203 BVerfG NJW 2000, 55 (65); vgl. auch BVerfG NJW 2006, 976 (980).

204 Vgl. BVerfG NJW 2009, 2431 (2435); bereits BVerfG NJW 2006, 976 (981).

205 BVerfG NJW 2009, 2431 (2435).

206 BVerfG NJW 2009, 2431 (2435).

lich.[207] Gerade die neuartigen Kommunikationsformen über das Internet mit weltweiter, rund um die Uhr verfügbarer, i. d. R. kostenloser und leicht einzurichtender Nutzbarkeit erfordern neue, an die technischen Entwicklungen angepasste Ermittlungsweisen. Im besonderen Interesse der Allgemeinheit liegt hierbei, dass auch die verschlüsselte Internettelefonie keinen „rechtsfreien Raum" bildet, sondern den Ermittlungsbehörden wirkungsvolle Instrumente zu Seite gestellt werden, die im Verdachtsfall die Überwachbarkeit derartiger Telekommunikation ermöglichen und hierdurch die effektive Verfolgung und Aufklärung von Straftaten sicherstellen.

Bei *Gegenüberstellung der Individual- und Gemeinwohlinteressen* rechtfertigt die in den §§ 100a, 100b StPO verankerte Eingriffsschwelle, insbesondere die für das Gewicht des Strafverfolgungsinteresses maßgebliche Schwere der verfolgten Straftat sowie der notwendige Tatverdachtsgrad, den mit einer Quellen-TKÜ verbundenen Eingriff. Gerade die Eingriffsvoraussetzungen einer *schweren Straftat* bezüglich derer ein erhöhter Verdachtsgrad in Form eines *von Tatsachen begründeten Verdachts* vorliegen muss, tragen der Verhältnismäßigkeit i. e. S. auch bei Maßnahmen der Quellen-TKÜ Rechnung:

Die in § 100a I Nr. 1 StPO enthaltene Bezugnahme und zugleich Beschränkung von Maßnahmen auf die im Straftatenkatalog des § 100a II StPO aufgezählten *schweren Straftaten* und deren erhöhten Unrechtsgehalt kompensiert in angemessener Weise die Heimlichkeit der Maßnahme und wird zugleich aber dem Bedürfnis nach effektiver Strafverfolgung und möglichst vollständiger Wahrheitsermittlung gerecht.[208] Nach wiederholter Rspr. des BVerfG stellt gerade „die wirksame Aufklärung […] schwerer Straftaten […] einen wesentlichen Auftrag eines rechtsstaatlichen Gemeinwesens"[209] dar. Angesichts des Gewichts des Strafverfolgungsinteresses ist unter dem Gesichtspunkt des Übermaßverbotes staatlicher Eingriffe eine weitere Anhebung der ohnehin schon hohen Voraussetzungen für eine Telekommunikationsüberwachung in §§ 100a, 100b StPO auch in den

---

[207] Vgl. BVerfG NJW 2009, 2431 (2435); bereits BVerfG NJW 2006, 976 (981).

[208] Dies bestätigt nunmehr auch die kürzlich ergangene Entscheidung des BVerfG zur gegenwärtigen Regelung der strafprozessualen Telekommunikationsüberwachung (BVerfG, Beschl. v. 12.10.2011, Az.: 2 BvR 236/08, 2 BvR 237/08, 2 BvR 422/08), wonach die anlässlich der Neuregelung zum 01.01.2008 (BGBl. I S. 3198) durch den Gesetzgeber vorgenommene Erweiterung des Straftatenkatalogs in § 100a II StPO in der gegenwärtig gültigen Fassung den Verhältnismäßigkeitsgrundsatz wahre (Abs.-Nr. 203), da „die gesetzgeberische Einstufung der in § 100a Abs. 2 StPO aufgenommenen Straftatbestände als ‚schwer' bei einer Gesamtschau vertretbar" (Abs.-Nr. 205) sei.

[209] BVerfG NJW 2000, 55 (65); vgl. bereits BVerfG NJW 1988, 329; BVerfG NJW 1990, 563.

Fällen der speziellen TKÜ-Maßnahme der Quellen-TKÜ nicht veranlasst. Denn eine Quellen-*TKÜ*, die (schon ihrem Maßnahmezweck gemäß) allein auf die Erfassung von Daten aus laufenden Telekommunikationsvorgängen ausgerichtet ist, weist in Bezug auf das erlangte Datenmaterial insoweit kein im Vergleich zu herkömmlichen TKÜ-Maßnahmen gesteigertes Eingriffspotential auf. Insofern ist für die Frage der Angemessenheit zu berücksichtigen, dass bei der Überwachung und Aufzeichnung im Rahmen einer Quellen-TKÜ – anders als dies das BVerfG für die Maßnahme der Online-Durchsuchung festgestellt hat – keine derartige „staatliche Datenerhebung aus komplexen informationstechnischen Systemen“[210] stattfindet, welche „ein beträchtliches Potenzial für die Ausforschung der Persönlichkeit des Betroffenen“[211] aufweisen würde. Denn eine Maßnahme der Quellen-TKÜ hat weder den vom BVerfG in diesem Zusammenhang ausdrücklich genannten einmaligen noch den punktuellen Zugriff „wie bspw. die Beschlagnahme oder Kopie von Speichermedien solcher Systeme“[212] zum Gegenstand. Die Überwachungs- und Aufzeichnungsmaßnahme der Quellen-TKÜ richtet sich maßnahmetypisch weder auf das Erfassen eines Datenbestandes, „der herkömmliche Informationsquellen an Umfang und Vielfältigkeit bei Weitem übertreffen kann“[213] und mit dem Risiko verbunden ist, „dass die erhobenen Daten in einer Gesamtschau weitreichende Rückschlüsse auf die Persönlichkeit des Betroffenen […] ermöglichen“[214], da komplexe informationstechnische Geräte „nach den gegenwärtigen Nutzungsgepflogenheiten typischerweise bewusst zum Speichern auch persönlicher Daten von gesteigerter Sensibilität, etwa in Form privater Text-, Bild- oder Tondateien, genutzt [werden]“[215], noch auf eine umfassende „längerfristige Überwachung der Nutzung des Systems“[216] als solches, welche mit dem laufenden Erfassen des oben genannten Datenbestandes, von dem auch „lediglich im Arbeitsspeicher gehaltene flüchtige oder nur temporäre auf den Speichermedien des Zielsystems abgelegte Daten“[217] betroffen sein können, verbunden ist. Des Weiteren erfüllt die Maßnahme der Überwachung und Aufzeichnung im Rahmen einer Quellen-TKÜ aber auch nicht den Zweck, den Ermittlungsbehörden einen Zugang zu etwaigen Telekommunikationsdaten zu ermöglichen, die sich nach Abschluss des Telekommunikationsvorgangs auf den Speichermedien des Zielsystems im Herrschaftsbereich des Nutzers

210 BVerfG NJW 2008, 822 (829).
211 BVerfG NJW 2008, 822 (829).
212 BVerfG NJW 2008, 822 (829).
213 BVerfG NJW 2008, 822 (829).
214 BVerfG NJW 2008, 822 (830).
215 BVerfG NJW 2008, 822 (830).
216 BVerfG NJW 2008, 822 (830).
217 BVerfG NJW 2008, 822 (830).

befinden[218] oder gar das System und die daran angeschlossenen Geräte (Webcam etc.) in eine Abhörvorrichtung i. S. d. § 100c StPO umzufunktionieren, da die Quellen-*TKÜ* sich maßnahmetypisch allein auf den Zugriff auf Daten aus (bewusst geführten) laufenden Telekommunikationsvorgängen beschränkt. Zudem ist bei der Quellen-TKÜ die Gefahr, dass am vorhandenen Datenbestand Schäden verursacht werden, nicht in gleicher Weise gegeben, wie bei Maßnahmen der Online-Durchsuchung. Denn anders als bei der Online-Durchsuchung, die gerade maßnahmespezifisch vor allem den Zugriff auf die Datenbestände der Speichermedien des betroffenen Systems zum Gegenstand hat, ist das Risiko einer Veränderung, Beschädigung oder Löschung von bestehenden, oder auch der Anlegung von neuen Datenbeständen auf dem Zielsystem bei der Durchführung einer Maßnahme der Quellen-TKÜ, die das Abgreifen laufender (flüchtiger) Internettelefonie zum Gegenstand hat, in weit geringerem Maße gegeben. Mangels entsprechender Wechselwirkungen mit dem Betriebssystem und den damit verbundenen Speichermedien wie dies bei einer Online-Durchsuchung zur Durchsicht der Datenbestände der Fall ist und was ggf. zu Datenverlusten führen kann[219], ist die Gefahr einer Veränderung oder eines Verlustes des auf dem System vorhandenen Datenbestandes bei der reinen Überwachung und Aufzeichnung laufender Telekommunikationsvorgängen als vergleichsweise gering einzustufen.

Eines Anknüpfens der Maßnahme an dem (potentiellen) Maßstab einer Online-Durchsuchung[220] bzw. an die erhöhte Anforderung der *besonders schweren Straftat* i. S. d. § 100c II StPO[221] bedarf es deshalb zum Herstellen eines angemessenen Ausgleichs nicht.

In gleicher Weise rechtfertigen auch die erhöhten Anforderungen an den notwendigen *Tatverdacht* (§ 100a I Nr. 1 StPO), der *von bestimmten Tatsa-*

---

218 Was ebenfalls die Eingriffsqualität einer Online-Durchsuchung aufweisen würde, vgl. insoweit auch BVerfG NJW 2008, 822 (830) („[…] Überwachung, auch wenn diese erst nachträglich einsetzt […]").

219 Vgl. BVerfG NJW 2008, 822 (830).

220 A. A. hingegen *Becker*/*Meinicke*, StV 2011, 50 (51), nach deren Auffassung der „großzügige […] Straftatenkatalog des § 100a StPO" dem Eingriff der Quellen-TKÜ nicht gerecht werde; deren Begründung unter Verweis auf die Feststellungen des BVerfG zur präventiven Online-Durchsuchung, welche nur bei Gefahren für ein überragend wichtiges Rechtsgut zulässig ist (BVerfG NJW 2008, 822, 830 f.), überzeugt indes nicht, da eine ausschließlich auf laufende Telekommunikationsvorgänge beschränkte Quellen-TKÜ-Maßnahme eine geringere Eingriffsintensität aufweist als eine Maßnahme der Online-Durchsuchung; für einen solchen Zugriff stellt die Begrenzung auf den in § 100a II StPO enthaltenen Katalog schwerer Straftaten eine insgesamt angemessene Eingriffsschwelle dar, dessen geschützte Rechtsgüter und deren Bedeutung für die Gemeinschaft Maßnahmen der Quellen-TKÜ rechtfertigen.

221 Siehe hierzu auch 3. Teil B.II.2.

chen konkretisiert sein muss[222] – d. h. ein Vorliegen von Umständen, die auf Grund „hinreichend sichere[r] Tatsachenbasis“[223] mit hinreichender Wahrscheinlichkeit auf die Täter- oder Teilnehmerschaft der Zielperson an einer begangenen oder (bei Versuchsstrafbarkeit) versuchten Katalogstraftat des § 100a II StPO hindeuten – wie auch das Erfordernis des *Schwerwiegens der Tat im Einzelfall* nach § 100a I Nr. 2 StPO und der *Subsidiaritätsgrundsatz* aus § 100a I Nr. 3 StPO die Maßnahme der Quellen-TKÜ und sorgen für einen angemessenen Ausgleich zwischen den Individualinteressen des Betroffenen vor übermäßigem staatlichen Zugriff einerseits und dem Allgemeininteresse an der Gewährleistung effektiver Strafverfolgung auch bei Verwendung moderner Telekommunikationsformen wie der Kommunikation via Internetprotokoll, welche auf der Übermittlungsstrecke verschlüsselt transportiert wird, andererseits.

Der mit dem Zugriff auf Kommunikationsinhalte einhergehenden Einbuße an Privatheit wird durch die Anwendung der *Kernbereichsregelungen* des § 100a IV StPO im Rahmen von Maßnahmen nach den §§ 100a, 100b StPO in angemessener Weise Rechnung getragen. Die Regelungen des § 100a IV StPO sorgen in einer angemessenen und den verfassungsrechtlichen Anforderungen insgesamt gerecht werdenden Weise[224] dafür, dass eine Erhebung

---

[222] Mit Blick auf die Eingriffsintensität einer Quellen-TKÜ-Maßnahme bedarf es zur Wahrung der Verhältnismäßigkeit weder des Vorliegens eines „dringenden Tatverdachts“ i. S. d. § 112 I S. 1 StPO noch eines „hinreichenden Tatverdachts“ i. S. d. § 203 StPO; denn den Anforderungen an einen verhältnismäßigen Eingriff wird in ausreichender und angemessener Weise auch ein „einfacher“ Tatverdacht (Anfangsverdacht, §§ 152 II, 160 I StPO) gerecht, der allerdings von bestimmten Tatsachen begründet sein muss, wie dies § 100a I Nr. 1 StPO voraussetzt; hierfür muss sich der Verdacht auf eine hinreichend sichere Tatsachenbasis stützen, durch schlüssiges Beweismaterial bereits ein gewisses Maß an Konkretisierung erreicht haben und nicht nur unerheblich sein, vgl. BGH NJW 1995, 1974 (1975); BGH NJW 2001, 2266 (2268); BVerfG NJW 2000, 55 (66); BVerfG NJW 2003, 1787 (1791); Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 9 m. w. N.; *Bär*, TK-Überwachung, § 100a StPO, Rn. 17 m. w. N.

[223] BVerfG NJW 2003, 1787 (1791).

[224] Vgl. *Bär*, TK-Überwachung, § 100a StPO, Rn. 42 ff. m. w. N., der die Entscheidung des Gesetzgebers zur Regelung des Kernbereichsschutzes in der Weise, wie in § 100a IV StPO erfolgt, als „allein praxisgerecht“ (Rn. 42) bezeichnet; ebenso Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 24; a. A. *Becker*/*Meinicke*, StV 2011, 50 (51) („verfassungsrechtlich höchst bedenkliche § 100a Abs. 4 StPO“); krit. auch Bundesrechtsanwaltskammer, Stellungnahme zum Gesetzentwurf der Bundesregierung zum Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (BR-Drucks. 275/07), S. 29 f., abrufbar unter http://www.brak.de/w/files/stellungnahmen/Stn31-2007.pdf (zuletzt aufgerufen 15.06.2012), für Einzelheiten zur Kernbereichsregelung in § 100a IV StPO, siehe 2. Teil A.III.1.; die Verfassungsmäßigkeit der Kernbereichsregelung in § 100a IV StPO wurde indes höchst-

von Erkenntnissen, die allein dem Kernbereich privater Lebensgestaltung zuzuordnen sind, unterbleibt (§ 100a IV S. 1 StPO) bzw. derartige Erkenntnisse nicht gespeichert und verwertet (§ 100a IV S. 2 StPO), sondern unverzüglich gelöscht werden, falls es dennoch zu deren Erhebung gekommen sein sollte[225] (§ 100a IV S. 3 StPO). Diese Regelung führt auch für den im Rahmen einer Maßnahmen der Quellen-TKÜ stattfindenden Zugriff auf Inhalte einer Internettelefonie[226], mit dem letztlich die gleichen (möglicherweise kernbereichsrelevanten) Erkenntnisse wie bspw. bei einer Überwachung eines Festnetztelefonates erfasst werden, zu einem angemessenen Ausgleich mit dem Schutzinteresse höchstpersönlicher Kommunikation.

Auch hinsichtlich der regelmäßigen Erfassung (an der Straftat ggf. unbeteiligter) Dritter in Gestalt der von der Maßnahme mitbetroffenen Gesprächspartner der Zielperson oder der Personen, die das überwachte Zielgerät (mit-)benutzen, werden die Vorschriften der §§ 100a, 100b StPO, insbesondere auch mit Blick auf die für derartige Maßnahmen gültigen Regelung hinsichtlich der Verwendung von Zufallserkenntnissen in anderen Strafverfahren nach § 477 II S. 2 StPO, einer die beteiligten Interessen insgesamt in einen angemessenen Ausgleich bringenden Regelung gerecht. Durch das Miterfassen ihrer Kommunikationsanteile sind Gesprächspartner zwar ebenfalls in ihrem Grundrecht aus Art. 10 I GG beeinträchtigt. Wenngleich nicht ausdrücklich gesetzlich klargestellt, wird eine solche Mitbetroffenheit im Rahmen von Maßnahmen nach §§ 100a, 100b StPO jedoch als unvermeidbar angesehen.[227] Auch unvermeidbar mitbetroffenen Dritten gegenüber gestatten die §§ 100a, 100b StPO einen Eingriff in deren grundrechtlich geschützten Anspruch auf Unverletzlichkeit des Fernmeldegeheimnisses aus Art. 10 I GG[228], welcher insoweit zurückstehen muss, wenn deren Äußerungen zur Verfolgung und Aufklärung der jeweiligen Katalogstraftat von Bedeutung sind.[229] Anders als bei Maßnahmen mit großer Breitenwirkung – wie dies bspw. bei der Erfassung einer Vielzahl von Betroffenen im Rahmen einer Funkzellenabfrage nach § 100g II S. 2 StPO[230] der Fall und deshalb nur unter den Anforderungen des § 100g I S. 1 Nr. 1 StPO bei Straftaten von erheblicher Bedeutung zulässig ist – sind bei einer

---

richterlich bestätigt durch BVerfG, Beschluss vom 12.10.2011, Az.: 2 BvR 236/08, 2 BvR 237/08, 2 BvR 422/08, Abs.-Nr. 209.

225 Vgl. insoweit BVerfG NJW 2009, 2431 (2437).

226 Sowohl auf Sprachinhalte als auch bei einer Überwachung der audiovisuellen Inhalte einer Video-Internettelefonie auf Videoinhalte, so auch LG Hamburg, MMR 2011, 693 (694).

227 Vgl. BGH NJW 1980, 67 (68).

228 Vgl. BGH NJW 1980, 67 (68) m. w. N.

229 Vgl. KK – *Nack*, StPO, § 100a, Rn. 65.

230 Für Einzelheiten zur Befugnisnorm des § 100g StPO, siehe 1. Teil A.II.2.d).

TKÜ-Maßnahme regelmäßig „nur“ zwei Personen in ihrem Grundrecht aus Art. 10 I GG betroffen, und zwar neben der Zielperson noch dessen Gesprächspartner[231], weshalb die Drittbetroffenheit auch im Rahmen einer Maßnahme der Quellen-TKÜ kein Kriterium darstellt, welches zu einer Unangemessenheit des Eingriffs führen müsste. Dem Schutzinteresse unvermeidbar mitbetroffener Dritter wird zudem im Wege der für eine auf die §§ 100a, 100b StPO gestützte Quellen-TKÜ ebenfalls gültigen Regelungen des § 477 II StPO über die *Verwertbarkeit* der im Rahmen einer TKÜ-Maßnahme erlangten Zufallserkenntnissen in anderen Strafverfahren Rechnung getragen wie auch über die *Benachrichtigungspflichten* des § 101 IV S. 1 Nr. 3 StPO[232] und die Pflicht des § 101 VIII S. 1 StPO zum *unverzüglichen Löschen* der erlangten Daten, sobald sie zur Strafverfolgung oder für eine gerichtliche Prüfung nicht mehr erforderlich sind[233].

Auch der Umstand, dass bei Maßnahmen der Quellen-TKÜ als spezifisches technisches Mittel zum Zwecke der Telekommunikationsüberwachung eine *Überwachungssoftware* zum Einsatz kommt, steht der Verhältnismäßigkeit i. e. S. nicht entgegen.

Wie die einleitend dargestellte, teils äußerst emotional geführte öffentliche Debatte zum Einsatz von Überwachungsprogrammen seitens staatlicher Behörden verdeutlicht, handelt es sich bei einer solchen Vorgehensweise – zu Recht – um ein sensibles Thema, welches jedoch mit der nötigen Sachlichkeit und Differenziertheit betrachtet werden muss. Nicht jeder Einsatz staatlicher Überwachungssoftware muss per se unzulässig sein. In die Beurteilung der Verhältnismäßigkeit eines solchen technischen Mittels im Rahmen von TKÜ-Maßnahmen ist deshalb einerseits einzustellen, dass sich die Fremdsoftware auf einem informationstechnischen System befindet, auf dem sich gespeicherten Daten mit ggf. weitreichenden persönlichkeitsrelevanten Informationen befinden können. So hat das BVerfG in Bezug auf den Grundrechtsmaßstab zweifellos festgestellt, dass mit der technischen Infiltration

---

231 Selbst bei einer von manchen VoIP-Diensten angebotenen Konferenzschaltung mehrerer Gesprächsteilnehmer miteinander, wäre die dennoch begrenzte Zahl der Teilnehmer und damit die Zahl der von der Überwachungsmaßnahme Betroffenen doch deutlich überschaubarer als bei Maßnahmen, die auf eine breitenwirksame Erfassung ausgelegt sind.

232 Wie das BVerfG auch in einer kürzlich ergangenen Entscheidung (BVerfG, Beschl. v. 12.10.2011, Az.: 2 BvR 236/08, 2 BvR 237/08, 2 BvR 422/08) unter Zurückweisung mehrerer Verfassungsbeschwerden bezüglich der zum 01.01.2008 in Kraft getretenen Neuregelung der strafprozessualen Telekommunikationsüberwachung (BGBl. I S. 3198) nunmehr höchstrichterlich festgestellt hat, sind auch die Regelungen über die Benachrichtigungspflichten in § 101 IV bis VI StPO nicht zu beanstanden, welche „einer verfassungsrechtlichen Prüfung stand[halten]“ (Abs.-Nr. 228).

233 Vgl. BGH NJW 1980, 67 (68), noch zu § 100b V StPO a. F.

eines komplexen informationstechnischen Systems zum Zwecke der Telekommunikationsüberwachung „die entscheidende Hürde genommen [ist], um das System insgesamt auszuspähen“[234]. Im „gleichen Atemzug“ hat das BVerfG aber auch festgestellt, dass weder das neue Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 I i. V. m. Art. 1 I GG noch das Grundrecht auf Unverletzlichkeit der Wohnung aus Art. 13 I GG, sondern das Fernmeldegeheimnis (Telekommunikationsgeheimnis) aus Art. 10 I GG „der alleinige grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zu einer ‚Quellen-Telekommunikationsüberwachung‘ [ist], wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt“[235] und dies „durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt“[236] ist. Somit ist die spezifische Vorgehensweise einer solchen Maßnahme, bei der eine Überwachungssoftware auf informationstechnischen Systemen zum Einsatz kommt, unter verfassungsrechtlichen Kriterien eben nicht generell als unzulässig anzusehen, sondern vielmehr nach der damit realisierten konkreten Ermittlungsmaßnahme und deren Eingriffsumfang zwingend zu differenzieren. In Bezug auf den Schutz des Betroffenen vor einer (von § 100a I StPO nicht mehr gedeckten) überschießenden Erfassung von Daten, welche sich außerhalb laufender Telekommunikationsvorgänge auf dem System befinden, sind bei der Verwendung eines solchen technischen Mittels zur Telekommunikationsüberwachung die Grenzen der Angemessenheit jedenfalls dann nicht überschritten, wenn eine Überwachungssoftware entsprechend auf den von § 100a I StPO vermittelten Eingriffsumfang beschränkt ist. Denn soweit eine zum Einsatz kommende Überwachungssoftware gemäß der Anforderung der ausschließlichen Telekommunikationsbezogenheit ausgestaltet ist, stellt diese ein technisches Mittel dar, welches – wie auch sonstige technische Mittel zur Realisierung von TKÜ-Maßnahmen – unter Berücksichtigung des erhöhten öffentlichen Interesses an der Verfolgung und Aufklärung schwerer Straftaten eine Überwachbarkeit von Telekommunikation ermöglicht, gleichzeitig aber den Individualinteressen des jeweiligen Betroffenen Rechnung trägt, indem es sicherstellt, dass die TKÜ-Maßnahme von ihrer Eingriffswirkung her nicht einer Online-Durchsuchung gleichkommt. Auch *Bär* weist zu Recht darauf hin, dass „der Begriff Quellen-TKÜ berechtigt und eine klare Grenze zur Onlinedurchsuchung gezogen [ist]“[237], wenn „durch die eingesetzte Software eine Beschränkung auf die ‚reine‘ Überwachung der jeweiligen Telekommunikation […] sichergestellt wird“[238].

---

234 BVerfG NJW 2008, 822 (825).
235 BVerfG NJW 2008, 822 (826).
236 BVerfG NJW 2008, 822 (826).
237 Anm. *Bär*, MMR 2011, 691 (692).
238 Anm. *Bär*, MMR 2011, 691 (692).

Freilich muss eine solche Einsatzweise von Überwachungssoftware im Rahmen einer Quellen-TKÜ-Maßnahme nach §§ 100a, 100b StPO für konkrete Anwendungsfälle auch möglich sein, d. h. ein solches technisches Mittel dann auch entsprechend auf laufende Telekommunikation als Zugriffsgegenstand technisch beschränkbar sein. Entgegen einer Vielzahl von Kommentaren v. a. aus den Medien, die bisweilen den Eindruck vermitteln, „der" Staatstrojaner, würde bei jeder denkbaren Einsatzform das betroffene System bis in den kleinsten Sektor seiner Speichermedien durchforsten und sämtliche darauf befindlichen Daten mit den darin gespeicherten persönlichen Informationen des Betroffenen ausspionieren[239], ist eine entsprechende Konfiguration und damit *Beschränkbarkeit* des Überwachungspotentials der Überwachungssoftware von vornherein nur auf Daten aus laufenden Telekommunikationsvorgängen auch in der Praxis durchaus technisch möglich.[240] Denn wenn eine Überwachungssoftware prinzipiell um verschiede-

---

239 Vgl. hierzu den Auszug der Presseberichterstattung über den im Oktober 2011 durch den *Chaos Computer Club* veröffentlichten Staatstrojaner im Rahmen der Einleitung der vorliegenden Arbeit zum „Überwachungsgegenstand Internettelefonie".

240 Vgl. bspw. die Antwort der Bundesregierung, BT-Drs. 17/7760, S. 5; in dieselbe Richtung auch die Antwort des Bayerischen Staatsministeriums des Innern, LT-Drs. 16/10082, S. 2 u. 3; auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, *Schaar*, widerspricht insoweit kritischen Stimmen, wonach der Einsatz von Überwachungsprogrammen grds. ungeeignet sei, weil diese stets die technische Möglichkeit zum Ausspähen des Systems eröffnen würden, vgl. *Höll*, „Gefährliche Grauzone", Süddeutsche Zeitung vom 13.10.2011, S. 6; nach Einschätzung von *Schaar* sei „es […] durchaus möglich, Programme einzusetzen, die dem Urteil des Bundesverfassungsgerichts von 2008 entsprechen", zitiert nach *Höll*, in: „‚Gefährliche Grauzone'", Süddeutsche Zeitung vom 13.10.2011, S. 6; a. A. hingegen *Buermeyer*/*Bäcker*, HRRS 2009, 433 (439) unter Verweis auf BVerfG NJW 2008, 822 (826 u. 830) zur Auskunft der (2008) gehörten Sachverständigen, wonach – so die Interpretation von *Buermeyer*/*Bäcker* – *niemals* auszuschließen sei, dass Daten des Systems erhoben oder verändert würden; diese Interpretation ist indes nicht derart zwingend, wie es die Formulierung der Autoren vermuten ließe, da es gemäß den Feststellungen des BVerfG „nach Auskunft der […] angehörten sachkundigen Auskunftspersonen […] im Übrigen dazu kommen [*kann*, Hervorh. d. Verf.], dass im Anschluss an die Infiltration Daten ohne Bezug zur laufenden Telekommunikation erhoben werden […]" (BVerfG NJW 2008, 822, 825 f.); in diese Richtung aber auch *Albrecht*/*Dienst*, JurPC Web-Dok. 5/2012, Abs. 27 f.; der Aufbau der Entscheidung lässt demgegenüber aber auch den Schluss zu, dass das BVerfG dies für die Fälle festgestellt hat, in denen den dadurch bewirkten Gefährdungen „durch Art. 10I GG nicht oder nicht hinreichend begegnet werden" (826) kann, also in denen die Beschränkung ausschließlich auf laufende Telekommunikationsvorgänge nicht durch technische Vorkehrungen sichergestellt werden kann; im Umkehrschluss muss dann aber davon ausgegangen werden, dass das BVerfG für die Konstellation der alleinigen Grundrechtsrelevanz des Art. 10 I GG, sprich „wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt" (826), die technische Möglichkeit hierzu gerade nicht ausgeschlossen

ne Eingriffskomponenten/-funktionen erweitert werden kann (vgl. unten), dann ist diese konsequenterweise auch auf bestimmte Eingriffskomponenten/-funktionen beschränkbar. Dass eine Überwachungssoftware so konfiguriert werden kann, dass sie technisch dazu in der Lage ist, IP-Telekommunikation an der Quelle abzugreifen, belegen die bislang in der Praxis durchgeführten Quellen-TKÜ-Maßnahmen. Denkbar bzw. zum erleichterten Nachweis einer angemessenen Einsatzweise sinnvoll (zur Rechtfertigung des Eingriffs aber nicht zwingend notwendig) wäre es in diesem Zusammenhang allerdings, künftig eine Art Zertifizierung, bspw. durch das Bundesamt für Sicherheit in der Informationstechnik (BSI)[241], für staatliche Überwachungsprogramme einzuführen („Staatstrojaner-TÜV"), welche eine – ggf. auch durch unabhängige Experten im Vorfeld zusätzlich geprüfte – mit dem Erfordernis der Beschränkung auf laufende Telekommunikationsvorgänge in Einklang stehende Konfiguration der Software entsprechend bescheinigt (vgl. § 9 BSIG[242], § 2 VII BSIG).[243]

---

hat, da das BVerfG andernfalls Aussagen zu einer Konstellation getroffen hätte, die sich wider seines Dafürhaltens so in der Praxis überhaupt nicht ergeben könnte; für Einzelheiten zur Erstellung und Konfiguration der Überwachungssoftware, siehe 1. Teil A.II.4.b).

241 Gemäß § 3 Nr. 13 lit. a BSIG zählt zu den Aufgaben des BSI insbesondere auch die Unterstützung der Polizeien und Strafverfolgungsbehörden bei der Wahrnehmung ihrer gesetzlichen Aufgaben. Anders hingegen *Braun*/*Roggenkamp*, K&R 2011, 681 (685), denen eine Ansiedlung der Überprüfung bei den Datenschutzbeauftragten des Bundes und der Länder sachgerechter erscheint, da es sich bei dem BSI um eine dem Bundesministerium des Innern nachgeordnete Behörde handelt, weshalb fraglich sei, ob diese „die für die Akzeptanz in der öffentlichen Wahrnehmung notwendige Unabhängigkeit besitzt" (685). Ob ein solcher „Misstrauensvorschuss" dem BSI indes gerecht wird, darf bezweifelt werden; das BSI ist zentrale sachverständige Stelle für sämtliche Belange der Sicherheit in der Informationstechnik und gerade als staatliche Behörde in besonderer Weise an Recht und Gesetz gebunden; auch nach dem Selbstverständnis der Behörde wird „die Objektivität und Einheitlichkeit der Prüfungen sowie die Unparteilichkeit […] durch das BSI gewährleistet. Als unparteiliche Stelle ist diese Maxime, auch bei Interessenskonflikten, Leitlinie für unsere tägliche Arbeit […]" (https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/zertifizierungundanerkennung_node.html, zuletzt aufgerufen 15.06.2012).

242 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) vom 14. August 2009 (BGBl. I S. 2821).

243 In diese Richtung auch der Vorsitzende der Deutschen Polizeigewerkschaft, *Wendt*, in der Neuen Osnabrücker Zeitung vom 11.10.2011, abrufbar unter http://www.noz.de/deutschland-und-welt/gut-zu-wissen/computer/57839915/bayern-wegen-trojaner-einsatzes-unter-druck (zuletzt aufgerufen 15.06.2012); ebenso der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, *Schaar*, sowie die Bundesministerin der Justiz, *Leutheusser-Schnarrenberger*, nach *Höll*, „‚Gefährliche Grauzone'", Süddeutsche Zeitung vom 13.10.2011, S. 6; in diese Richtung bereits Anm. *Vogel*/*Brodowski*, StV 2009, 632 (634).

Bei der Verwendung einer Überwachungssoftware müssen aber auch ggf. zusätzlich vorhandene Komponenten nicht auf einen zwingend unangemessenen Gebrauch des technischen Mittels hindeuten. Selbst dann, wenn eine Überwachungssoftware mittel einer eingebauten *Fernsteuerungsfunktion* jederzeit um weitere Komponenten nach- bzw. aufrüstbar ist – wie dies vielfach im Medienecho zu dem im Oktober 2011 veröffentlichten „Staatstrojaner" kritisiert wurde – oder gar bereits entsprechende Komponenten für eine weitergehende Erfassung von Daten enthält, muss dieser Umstand ein Infiltrieren des Zielsystems mit einer Überwachungssoftware und deren Verwendung zur Telekommunikationsüberwachung nicht zwangsläufig unverhältnismäßig machen[244], solange jedenfalls von im Einzelfall ggf. technisch möglichen aber rechtlich nicht gedeckten zusätzlichen Komponenten kein Gebrauch gemacht wird.[245] Allein das Potential zu einem, von der Maßnahme nicht mehr gedeckten Gebrauch eines verwendeten technischen Mittels (hier Erfassen sonstiger auf dem Zielsystem gespeicherter Daten; Anfertigen von Screenshots etc.) muss im Rahmen der Abwägung zwischen dem wirksamen Grundrechtsschutz Betroffener und dem Bedürfnis effektiver Strafverfolgung nicht zwingend dazu führen, dass die Ermittlungsmaßnahme, die sich in den Grenzen des rechtlich Zulässigen bewegt (Überwachung ausschließlich von Daten aus laufenden Telekommunikationsvorgängen), zu Lasten der Verfolgung und Aufklärung schwerer Straftaten generell ausgeschlossen bzw. unzulässig ist.[246] Anhand eines Vergleichs zum Fußballsport versinnbildlicht: Beim Angriff eines Fußballers zum Zwecke der

---

[244] Mit der Folge der Unzulässigkeit der Maßnahme und Unverwertbarkeit der erlangten Erkenntnisse; in diese Richtung wohl *Braun*/*Roggenkamp*, K&R 2011, 681 (683) sowie *Stadler*, MMR 2012, 18 (19); für Einzelheiten zur Frage des Bestehens von Verwertungsverboten, siehe 3. Teil B.III.5.

[245] In diese Richtung auch BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 107g; a.A. *Braun*/*Roggenkamp*, K&R 2011, 681 (682), welche in Bezug auf die konkret durch den *Chaos Computer Club* untersuchte Software es bemängeln, dass die durchgeführte Quellen-TKÜ „gewissermaßen per Mausklick" (682) zu einer (von der Anordnung nicht gedeckten) Online-Durchsuchung oder einer Maßnahmen der akustischen Wohnraumüberwachung hätte ausgeweitet werden könnte; für die unzulässige Ausweitung der Maßnahme durch einen „Mausklick" bedürfte es damit aber auch erst der Ausführung eines entsprechenden computertechnischen Befehls durch die maßnahmedurchführenden Ermittlungsbehörden, welche aber bei der Maßnahmeumsetzung an die Vorgaben der zugrunde liegenden Anordnung gebunden sind.

[246] Deshalb kann durchaus auch der erst durch entsprechende (zugriffsgesicherte) Eingabe eines Befehls erweiterbare Zugriffsumfang eine technische Schutzvorkehrung darstellen; eine entsprechend auf die Vorgaben der Anordnung beschränkte Benutzung der Software und damit „rechtstreue" Umsetzung der angeordneten Überwachungsmaßnahme durch die Ermittlungsbehörde als an Recht und Gesetz gebundene staatliche Stelle (vgl. auch LG Hamburg, MMR 2011, 693, 696) kann bzw. muss in einem Rechtsstaat als selbstverständlich vorausgesetzt werden und ist überdies angesichts der dann im Raum stehenden Verwertungsverbote für unrechtmäßig

Ballabnahme entspricht das Grätschen des im Ballbesitz befindlichen Gegenspielers einer regelkonformen Spielweise, solange ausschließlich der Ball gespielt, die Grätsche kontrolliert ausgeführt und keine Verletzung des Gegenspielers in Kauf genommen wird. Regelwidrig hingegen ist die sog. Blutgrätsche, also das bewusste Treten des Gegenspielers statt des Balles.[247] Die Spielweise des Grätschens führt somit zu einer erhöhten Gefährdung für die Spieler. Die Ballabnahme mittels einer regelkonform durchgeführten Grätsche ist aber nicht automatisch deshalb unzulässig, weil die Gefahr besteht, dass ein Spieler eine regelwidrige Blutgrätsche durchführen könnte.

Auch ein Blick auf andere strafprozessuale Zwangsmaßnahmen steht dieser Sichtweise nicht entgegen: So könnte es auch im Rahmen einer angeordneten Durchsuchung beim Verdächtigen nach §§ 102 ff. StPO, bei deren Durchführung Ermittlungspersonen grds. ungehinderten Zugang zu allen in der Wohnung befindlichen Gegenständen haben, im Einzelfall z. B. zu einer rechtswidrigen Beschlagnahme von der Beschlagnahme nach § 97 StPO nicht unterliegenden Gegenständen kommen. Allein wegen eines solchen nicht gänzlich ausschließbaren (ggf. Missbrauchs-)Risikos, wäre es jedoch kaum statthaft, bereits die Ermittlungsmaßnahme der Durchsuchung generell für unzulässig zu erklären.[248]

Dies gilt grds. für jede strafprozessuale Zwangsmaßnahme, welche die Rechte und Interessen davon Betroffener tangiert. Hierbei ist im Rahmen der Beurteilung der Angemessenheit einer staatlichen Ermittlungsmaßnahme gerade auch darauf zu achten, dass an staatliche Ermittlungstätigkeit zur Erfüllung des öffentlichen Strafverfolgungs- und Straftatenaufklärungsauftrags verhältnismäßige, mithin also auch zumutbare und erfüllbare Anforderungen gestellt werden.

Deshalb weist auch eine etwa enthaltene *Nachladefunktion* nicht zwangsläufig auf einen unangemessenen Gebrauch staatlicher Überwachungssoftware hin. Denn eine Nachladefunktion kann – wie dies vorgetragen wird[249] –

---

erlangtes Datenmaterial im zwingenden Interesse effektiver Strafverfolgung; in diese Richtung auch BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 107g.

247 Vgl. http://de.wikipedia.org/wiki/Gr%C3%A4tsche_%28Fu%C3%9Fball%29 (zuletzt aufgerufen 15.06.2012); vgl. insoweit auch die Fußball-Regeln 2011/2012 des DFB, S. 89 f., abrufbar unter http://www.dfb.de/fileadmin/user_upload/2011/08/DFB_Umbr_Fussballregeln_2011_2012_low_01.pdf (zuletzt aufgerufen 15.06.2012).

248 Vgl. in diesem Sinne auch die zutr. Ausführungen von *Kudlich,* HFR 2007, S. 213, zu Maßnahmen der Blutentnahme zum Zwecke der Aufklärung von Bagatellstraftaten im Bereich des Straßenverkehrs.

249 Vgl. Antwort der Bundesregierung, BT-Drs. 17/7760, S. 8; in dieselbe Richtung auch die Antwort des Bayerischen Staatsministeriums des Innern, LT-Drs. 16/10469, S. 2; auch *Friedrich*, Bundesminister des Innern („Wir brauchen diese

gerade dafür notwendig sein, dass die individuelle Überwachungssoftware an die auf dem Zielgerät vorgenommenen Systemaktualisierungen und VoIP-Software-Updates angepasst bleibt.[250] Insofern besteht ein berechtigtes ermittlungstaktisches Interesse und Bedürfnis an der Verankerung einer Nachladefunktion in der Überwachungssoftware, als diese für die Realisierung eines praktikablen und durchführbaren Einsatzes der Software im Rahmen einer Maßnahme der Quellen-TKÜ erforderlich ist. Das Bestehen einer Nachladefunktion bedeutet gerade nicht, dass – als zweiter Schritt – darüber zwangsläufig weitere, ggf. nicht mehr von der Anordnung gedeckte Funktionalitäten des Überwachungsprogramms eingespielt werden bzw. werden können, bspw. soweit die Software technisch so konfiguriert ist, dass die Nachladefunktion nur zur Anpassung der Software an Systemveränderungen genutzt werden kann.[251] Dieser Umstand ist ebenfalls in die Beurteilung der Angemessenheit des heimlichen staatlichen Einsatzes einer Überwachungssoftware miteinzubeziehen. Die Nachladefunktion zur regelmäßigen Anpassung der Überwachung an den aktuellen Stand des Zielsystems und/oder der VoIP-Software führt insbesondere auch zu keiner Erhöhung der Eingriffswirkung für den Betroffenen. Vielmehr würde die Konsequenz einer fehlenden Nachladefunktion, nämlich das dann erforderliche stets neue Einschleusen einer wieder aktualisierten Software verbunden mit entsprechenden Vorfeldermittlungen zu einer bloßen Erschwerung der Ermittlungstätigkeit für die Strafverfolgungsbehörden führen. Das Ziel einer bloßen Erschwernis der Durchführung von Ermittlungsmaßnahmen stellt aber kein sachgerechtes und durchgreifendes Kriterium für die Beurteilung der Angemessenheit dar.

Soweit teilweise kritisiert wird, dass bei dem Einsatz einer staatlichen Überwachungssoftware auf einem fremden Zielsystem ein *Risiko* bestehe, dass diese von Dritten gezielt aus dem betroffenen Zielsystem isoliert, analysiert und zu eigenen (ggf. unlauteren) Zwecken *missbraucht* werden könnte, muss dies ebenfalls nicht generell gegen eine angemessene Verwen-

---

Nachladefunktionen, um uns den normalen Updates auf dem Zielcomputer anpassen zu können. Aber auch hier gibt es die gleichen Sicherungen wie beim ersten Aufspielen der Software."), zitiert nach *Hoffmann/Tomik*, in: „‚Es gibt keine rechtliche Grauzone'", faz.net vom 15.10.2011, abrufbar unter http://www.faz.net/aktuell/politik/iminterview-bundesinnenminister-friedrich-csu-es-gibt-keine-rechtliche-grauzone-11494291.html (zuletzt aufgerufen 15.06.2012).

250 Auch der normale Computer und Internetnutzer wird bestätigen können, dass vorhandene Software regelmäßig an durchgeführte Updates etc. angepasst werden muss.

251 A.A. offenbar Anm. *Brodowski*, JR 2011, 533 (536), der sich gegen die Integration einer Aktualisierungsfunktion ausspricht; krit. auch *Buermeyer*, http://ijure.org/wp/archives/756 (zuletzt aufgerufen 15.06.2012) sowie *Braun/Roggenkamp*, K&R 2011, 681 (682).

dung einer solchen sprechen. Eine absolute Missbrauchssicherheit ist im Rahmen einer sachgerechten Beurteilung der Angemessenheit des technischen Mittels „Überwachungssoftware" nicht zu verlangen. Denn eine garantiert, also zu 100 Prozent „missbrauchssichere" Software wird es wohl faktisch schon nicht geben, wie es auch kein zu 100 Prozent fremdzugriffssicheres informationstechnisches System gibt. Ein absoluter Schutz vor Missbrauchsgefahren ist für eine angemessene Berücksichtigung der Individualinteressen des Betroffenen aber auch nicht notwendig. Hierbei ist zu berücksichtigen, dass auch staatlichen Behörden zur Wahrnehmung ihrer verfassungsmäßigen Aufgaben und Pflichten nichts zur Bedingung gesetzt werden kann, was mitunter unmöglich und deshalb unleistbar ist. Denn das Verlangen von etwas Unmöglichem wird schwerlich dem Verhältnismäßigkeitsgrundsatz gerecht werden. Im Gegenteil, vielmehr wäre gerade das Verlangen einhundertprozentiger „Knacksicherkeit" einer staatlichen Überwachungssoftware zur Bejahung der Zulässigkeit einer Maßnahme der Quellen-TKÜ mit Blick auf das verfassungsrechtliche Bedürfnis der Effektivität der Strafverfolgung und Straftatenaufklärung, insbesondere bei schweren Straftaten, unverhältnismäßig und ginge an der Realität vorbei. Zudem kann für die Beurteilung der Missbrauchsgefahr und Gefährdung der IT-Sicherheit durch die Existenz und den Einsatz einer staatlichen Überwachungssoftware auch nicht außer Acht gelassen werden, dass es zahlreiche vergleichbare Programme gibt, die einen Zugriff bzw. ein Überwachen von Vorgängen auf informationstechnischen Systemen ermöglichen und für jedermann auf dem Markt frei erhältlich sind, sodass Dritte für missbräuchliche Zwecke nicht auf die Erlangung staatlicher Überwachungssoftware angewiesen sind. Überdies dürfte es für fachkundige Personen, die dazu in der Lage sind, eine auf einem infiltrierten System befindliche staatliche Überwachungssoftware zu isolieren und für eigene Zwecke zu verwenden, wohl ein Leichtes sein, eine solche auch selbst zu erstellen.[252] Mithin ist das Verlangen einer absolut unknackbaren Software für einen angemessenen Schutz vor missbräuchlichem Zugriff nicht veranlasst. Für einen Schutz vor unbefugten Zugriffen Dritter stehen nach dem gegenwärtigen Stand der Technik[253] indes wirksame technische Schutzvorkehrungen zur Verfü-

---

252 Zumal es sich bei der durch den *Chaos Computer Club* entdeckten „Malware" um eine nicht besonders anspruchsvoll programmierte Software handeln soll, vgl. *Reißmann*/*Stöcker*/*Lischka*, http://www.spiegel.de/netzwelt/web/0,1518,790931,00.html (zuletzt aufgerufen 15.06.2012).

253 Gemäß dem allgemeinen Begriffsverständnis von *Stand der Technik* ist demnach der Entwicklungsstand fortschrittlicher Verfahren zur Software-, Daten- und Systemsicherheit (hier bspw. proprietäre Protokolle, Verschlüsselung nach dem *Advanced Encryption Standard* etc.) heranzuziehen, der die praktische Eignung gegen Missbrauch, insbesondere unbefugte Nutzung, gesichert erscheinen lässt, vgl. hierzu

gung[254], welche zur Eindämmung derartiger Risiken in die jeweilige Software integriert werden können, um eine Isolierung, Analyse und missbräuchliche Nutzung der Software zu verhindern.

Auch die vorgetragenen Bedenken, dass durch die für die Realisierung des Eingriffs geschaffene *Lücke im System* die Sicherheit des infiltrierten Zielsystems gefährdet werde und diese auch für Zugriffe Dritter offen stehe[255], führen deshalb in der Gesamtabwägung der Umstände nicht zu einer generellen Unverhältnismäßigkeit einer solchen Maßnahme. Hierbei ist zum einen der Umstand zu berücksichtigen, dass kein informationstechnisches System „lückenlos" oder gar „uninfiltrierbar" ist. Auch im modernen Zeitalter der hochtechnologisierten IT-Gesellschaft gibt es keinen absoluten Schutz für informationstechnische Systeme vor Angriffen von außen – selbst wenn mit Antivirensoftware, Firewall u. ä. zur Verfügung stehende Gegenmaßnahmen ergriffen werden. So können fachkundige Personen jederzeit eigene Spionagesoftware entwerfen, die ein heimliches Einfallen in das System ermöglicht. Ebenso sind virtuelle Werkzeuge, welche Schutzlücken in Systemen ausnutzen (sog. *Exploits*), zuhauf im Internet erhältlich, ohne dass es für den Verwender einer gesteigerten Expertise bedürfte. Insofern gibt es eine „heile Welt der IT-Systeme", die erst durch den staatlichen Einsatz von Überwachungssoftware gefährdet würde, in diesem Sinne nicht. Auch das Vertrauen in die Sicherheit von Endgeräte ist dementsprechend von den technischen Möglichkeiten des Eindringens in diese begrenzt.[256] Einen solchen Idealtypus eines absolut sicheren Internets und dessen Kommunikationsmittel der Prüfung der Verhältnismäßigkeit als Maßstab zugrunde zu legen und mithin zu Lasten des Strafverfolgungsinteresses bei der Überwachung verschlüsselter VoIP-Kommunikation zu werten, würde des-

---

auch entsprechende Legaldefinitionen in § 3 VI Bundesimmissionsschutzgesetz oder in § 2 XI Gefahrstoffverordnung.

254 Vgl. hierzu 2. Teil B.III.2.c).

255 „‚Offen wie ein Scheunentor'", so der *Chaos Computer Club*, zitiert nach *Schulz*, in: „Staatstrojaner: Der Computer steht offen wie ein Scheunentor", faz.net vom 26.10.2011, abrufbar unter http://www.faz.net/aktuell/feuilleton/debatten/staatstrojaner/staatstrojaner-der-computer-steht-offen-wie-ein-scheunentor-11505829.html (zuletzt aufgerufen 15.06.2012); „‚Vergleichbar mit einer Hausdurchsuchung'", bei der „‚hinterher die Wohnungstür offen bleibe'", so der frühere FDP-Generalsekretär *Lindner*, zitiert nach spiegel.de vom 11.10.2011, in: „Koalitionsstreit um Spähprogramme: Trojaner infiziert Schwarz-Gelb", abrufbar unter http://www.spiegel.de/politik/deutschland/0,1518,791234,00.html (zuletzt aufgerufen 15.06.2012).

256 Insoweit auch *Sieber*, Stellungnahme zu dem Fragenkatalog des BVerfG in dem Verfahren 1 BvR 370/07, S. 5, abrufbar unter http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf (zuletzt aufgerufen 15.06.2012), wonach „das Vertrauen in die Sicherung des Endgeräts […] jedoch durch die technischen Möglichkeiten begrenzt [ist], die Angreifern zur Verfügung stehen, um diese Sicherungen am Endgerät zu brechen" (S. 5).

halb an den tatsächlichen Gegebenheiten vorbeigehen und auch einem angemessenen Ausgleich der beteiligten Interessen nicht gerecht werden. Auch hier ist zu berücksichtigen, dass es nach dem gegenwärtigen Stand der Technik zahlreiche technische Schutzvorkehrungen gibt, mit denen sich die mit einer Überwachungssoftware im System geschaffene Lücke wirksam vor unbefugten Zugriffen Dritter absichern lässt.[257] Deshalb steht es einer angemessene Verwendungsweise staatlicher Überwachungssoftware jedenfalls nicht entgegen, wenn die „Einbettung" des Überwachungsprogramms in das infiltrierte System und die Nutzung der eingerichteten Lücke zum Ausschleusen der Daten nur – wie bei TKÜ-Maßnahmen gemäß § 100b I S. 4, S. 5 StPO der Fall – für einen bestimmten (richterlich festgesetzten) Zeitraum stattfindet und während des Laufens der Maßnahme die Lücke nach dem Stand der Technik vor einem unbefugten Zugriff Dritter gesichert ist. Auch unvermeidbar mit dem Einsatz staatlicher Software verbundene *Veränderungen am System* führen deshalb nicht zur Unverhältnismäßigkeit im Vergleich zu den mit der Maßnahme verfolgten Gemeinwohlinteressen. Das Gewicht des staatlichen Strafverfolgungsinteresses bei schweren Straftaten rechtfertigt es indes, technisch unvermeidbare (zeitweise) Veränderungen am System vorzunehmen, solange sich diese jedenfalls auf die Ermöglichung des Maßnahmezwecks beschränken und vergleichsweise geringfügiger Natur sind. Dem Betroffenen sind geringfügige Veränderungen am System wie bspw. die zeitweise Integration der Software selbst, das von Sicherheitseinrichtungen des Systems unbemerkte Mitlaufen der Überwachungssoftware im Hintergrund etc. angesichts des Gemeinwohlinteresses zumutbar, zumal sich diese i. d. R. auf einer für den betroffenen Nutzer nicht wahrnehmbaren Ebene abspielen. Den Anforderungen an die Verhältnismäßigkeit i. e. S. entspricht es deshalb erst recht, wenn nach Beendigung der Maßnahme die Software (automatisch oder manuell) – soweit technisch möglich und zur Aufhebung einer eingreifenden Wirkung erforderlich – vollständig entfernt, die Lücke im System geschlossen und die Veränderungen im System wieder rückgängig gemacht werden.

ee) Zusammenfassung

Zusammenfassend lässt sich somit festhalten, dass die §§ 100a, 100b StPO und darauf gestützte Maßnahmen der Quellen-TKÜ auch hinsichtlich der Überwachung und Aufzeichnung von Telekommunikation „an der Quelle" zum Zugriff auf verschlüsselte IP-Kommunikation den Grundsatz der Verhältnismäßigkeit wahren. Hierbei dient die Quellen-TKÜ dem legitimen öffentlichen Zweck des Zugriffs auf Telekommunikation zur Verfolgung und

---

257 Vgl. hierzu 2. Teil B.III.2.c).

Aufklärung schwerer Straftaten auch bei der Nutzung verschlüsselter Kommunikationstechniken über informationstechnische Systeme. Die Quellen-TKÜ ist hierzu auch eine geeignete und erforderliche Maßnahme, da sie vor der Ver- bzw. nach der Entschlüsselung der TK-Inhalte ansetzt und gegenwärtig kein anderes (milderes) Mittel mit gleicher Eignung für einen Zugriff auf derartige Kommunikation zur Verfügung steht. Zudem ist die Verwendung der bei Quellen-TKÜ-Maßnahmen zum Einsatz kommenden Überwachungssoftware auch in angemessener Weise möglich. Die von §§ 100a, 100b StPO gesetzten hohen Eingriffsvoraussetzungen stellen hierbei eine angemessene Eingriffsschwelle auf, um die betroffenen Individualinteressen in einen gerechten Ausgleich mit den Allgemeininteressen zu bringen. Das Gewicht des öffentlichen Interesses an der Verfolgung und Aufklärung schwerer Straftaten rechtfertigt hierbei auch eine Telekommunikationsüberwachung, welche mittels Überwachungssoftware an einem zu Kommunikationszwecken verwendeten informationstechnischen System ansetzt. Dem angemessenen und hiefür streng auf den Ermittlungszweck begrenzten Einsatz der jeweiligen Überwachungssoftware ist bereits in der Überwachungsanordnung durch entsprechende Vorgaben Rechnung zu tragen. Zur Absicherung des technischen Mittels gegen missbräuchliche Nutzung und zum Schutz der Systemsicherheit bei Umsetzung der Anordnung lassen sich entsprechende technische Schutzvorkehrungen in die Software integrieren. Hierfür stellen die nach dem gegenwärtigen Stand der Technik zur Verfügung stehenden technischen Möglichkeiten angemessene Mittel dar. Denn in diesem Zusammenhang ist zu beachten, dass auch der Verhältnismäßigkeitsgrundsatz nichts (technisch) Unmögliches verlangt, weshalb von den Ermittlungsbehörden – insbesondere angesichts des gewichtigen öffentlichen Interesses an effektiver Verfolgung und Aufklärung schwerer Straftaten – ein zu 100 Prozent missbrauchssicheres technisches Mittel nicht gefordert werden kann. Eine Annahme dahingehend, dass Ermittlungsbehörden eine Überwachungssoftware, sobald sie nur die (technischen) Möglichkeiten dazu haben, umfassend und unter Missachtung jeglicher Vorgaben des zugrunde liegenden (i. d. R. richterlicher) Beschlusses verwenden, würde einer sachlichen Auseinandersetzung wenig gerecht werden. Denn wer überall Gefahren und staatliche Missbräuche sieht, wird immer „ein Haar in der Suppe“ finden[258]. Ein regelrechter „Misstrauensvorschuss“, wie ihn die Ermittlungsbehörden im Rahmen der Diskussionen über staatliche Überwachungssoftware mitunter erhalten, wird den tatsächlichen rechtsstaatlichen Verhältnissen in Deutschland und dem relativ hohen grundrechtlichen Schutzniveau insgesamt nicht gerecht. Auch die bislang vergleichsweise geringe Zahl an

[258] So auch zutr. *Kudlich*, HFR 2007, S. 213, zu Maßnahmen der Blutentnahme zum Zwecke der Aufklärung von Bagatellstraftaten im Bereich des Straßenverkehrs.

Quellen-TKÜ-Maßnahmen[259] in der Praxis mindert indes in keinster Weise das kriminalistische Bedürfnis nach einer solchen Maßnahme und stellt im Rahmen der Verhältnismäßigkeitsprüfung auch kein durchgreifendes Argument gegen deren Eignung und Angemessenheit dar. Ganz im Gegenteil lässt sich die bislang geringe Zahl an Quellen-TKÜ-Maßnahmen in der Praxis gerade auch als ein Indiz dafür heranziehen, dass über die §§ 100a, 100b StPO und deren Eingriffsschwelle insgesamt ein verantwortungsvoller und zurückhaltenden Gebrauch der Maßnahme der Quellen-TKÜ sichergestellt werden kann.

d) Sachgerechte Ausgestaltung des Verfahrens

Für strafprozessuale Befugnisnormen, die in materielle Grundrechte wie dem Fernmeldegeheimnis aus Art. 10 I GG eingreifen, bedarf es neben der Wahrung des Verhältnismäßigkeitsgrundsatzes für einen effektiven Grundrechtsschutz auch „einer den sachlichen Erfordernissen entsprechenden Ausgestaltung des Verfahrens“[260], insbesondere desjenigen, das sich an die erfolgte Datenerhebung anschließt. Gerade bei heimlicher Ermittlungstätigkeit des Staates gilt es zu beachten, dass dem Gewicht des grundrechtlichen Eingriffs durch geeignete Verfahrensvorkehrungen Rechnung getragen wird.[261]

Der Anspruch auf Gewährleistung effektiven Grundrechtsschutzes ergibt sich hierbei unmittelbar aus dem jeweils betroffenen Grundrecht[262], bei Maßnahmen zur Überwachung der Telekommunikation somit aus Art. 10 I GG. Die bestehenden *grundrechtssichernden Verfahrensregelungen*, wie sie für herkömmliche Telekommunikationsüberwachungen nach §§ 100a, 100b StPO Geltung entfalten, finden auch auf Maßnahmen der Quellen-TKÜ Anwendung, sofern diese Form der Telekommunikationsüberwachung auf die Befugnisnormen der §§ 100a, 100b StPO gestützt wird. Insgesamt entsprechen deren grundrechtssichernde Verfahrensregelungen auch für die Quellen-TKÜ einem nach sachlichen Erfordernissen ausgestalteten Verfahren zur Wahrung der Grundrechte der Betroffenen:

Zu den verfahrensrechtlichen Vorkehrungen, durch welche bei heimlichen Überwachungsmaßnahmen unter Zugriff auf informationstechnische Syste-

---

259 Siehe hierzu 1. Teil A.II.1.; für konkrete Zahlen zur Anwendung von Quellen-TKÜ-Software in Bayern, siehe auch die Antwort des Bayerischen Staatsministeriums des Innern, LT-Drs. 16/10082, S. 2 und LT-Drs. 16/10469, S. 2, 4 ff.

260 BVerfG NJW 2009, 2431 (2437).

261 Vgl. BVerfG NJW 2008, 822 (832) m. w. N.

262 Vgl. BVerfG NJW 2000, 55 (57); *Bär*, TK-Überwachung, § 101 StPO, Rn. 3 u. 4.

me dem Gewicht des grundrechtlichen Eingriffs Rechnung zu tragen ist[263], zählt insbesondere, den „Zugriff grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen“[264]. Ein *richterlicher Vorbehalt* ermöglicht es, eine geplante heimliche Ermittlungsmaßnahme durch eine unabhängige, neutrale Instanz vorbeugend kontrollieren zu lassen[265], weshalb eine solche *Kontrolle* „bedeutsames Element eines effektiven Grundrechtsschutzes“[266] sein kann, da der Richtervorbehalt insbesondere auch einer „‚kompensatorischen Repräsentation‘ der Interessen des Betroffenen“[267] dient. Diesen verfassungsrechtlichen Anforderung trägt die Regelung in § 100b I S. 1 StPO insoweit Rechnung, als Überwachungsmaßnahmen nach § 100a StPO grds. einer gerichtlichen Anordnung bedürfen. Dem steht auch nicht entgegen, dass nach § 100b I S. 2 StPO die Anordnung im Rahmen einer Eilkompetenz auch durch die Staatsanwaltschaft getroffen werden kann, wenn Gefahr im Verzug[268] vorliegt. Denn auch bei Zugriffen auf informationstechnische Systeme darf vom „Erfordernis einer vorherigen Kontrolle der Maßnahme durch eine dafür geeignete neutrale Stelle […] eine Ausnahme für Eilfälle […] vorgesehen werden, wenn für eine anschließende Überprüfung durch die neutrale Stelle gesorgt ist“[269]. Diesen vom BVerfG entwickelten Anforderungen wird die Regelung des § 100b I S. 3 StPO insoweit gerecht, als eine staatsanwaltschaftliche Eilanordnung binnen drei Tagen gerichtlich zu bestätigen ist. Wie jüngst durch das BVerfG bestätigt, ist durch die Vorbefassung eines Richters bei der Telekommunikationsüberwachung aber auch in Bezug auf den Schutz des Kernbereichs privater Lebensgestaltung „sichergestellt, dass der Kernbereichsschutz bereits im Vorfeld von einer unabhängigen Instanz in den Blick genommen wird und Beachtung findet“[270]. Zudem ist das anordnende Gericht gemäß der Verfahrensvorschrift des § 100b IV S. 2 StPO nach Beendigung der Maßnahme über deren Ergebnisse zu unterrichten. In Bezug auf den Kernbereichsschutz eröffnen die bestehenden Verfahrensregelungen daneben aber auch die Mög-

---

263 Vgl. BVerfG NJW 2008, 822 (832).

264 BVerfG NJW 2008, 822 (832).

265 So BVerfG NJW 2008, 822 (832).

266 BVerfG NJW 2008, 822 (832).

267 BVerfG NJW 2008, 822 (832).

268 *Gefahr im Verzug* liegt grds. dann vor, wenn das vorherige Einholen der richterlichen Anordnung den Erfolg der Maßnahme gefährden würde, vgl. BVerfG NJW 1979, 1539 (1540); bei strafprozessualen Maßnahmen ist dies regelmäßig dann der Fall, wenn ein Verlust von Beweismitteln droht, der allerdings nicht von den Ermittlungsbehörden selbst herbeigeführt worden sein darf, vgl. BVerfG NJW 2001, 1121 (1123).

269 BVerfG NJW 2008, 822 (832).

270 BVerfG, Beschluss vom 12.10.2011, Az.: 2 BvR 236/08, 2 BvR 237/08, 2 BvR 422/08, Abs.-Nr. 223.

lichkeit einer gerichtlichen Überprüfung nach § 101 VII S. 2 bis S. 4 StPO für die Fälle, bei denen die Ermittlungsbehörde im Einzelfall das Vorliegen eines Verwertungsverbotes verneint, weil die gewonnenen Daten ihrer Einschätzung nach nicht zum Kernbereich privater Lebensgestaltung gehören.[271]

Bei Eingriffen, die – wie bei der (Quellen-)Telekommunikationsüberwachung – der Erlangung von Informationen dienen, deren Vertraulichkeit grundrechtlich speziell geschützt ist, wird „den Verfahrensgarantien seit jeher ein hoher Stellenwert eingeräumt“[272]. Zu den verfahrensrechtlichen Schutzvorkehrungen zählen nach st. Rspr. des BVerfG „insbesondere Unterrichtungs-, Auskunfts-, Löschungs- und Kennzeichnungspflichten, Teilnahmerechte und Verwertungsverbote“[273].

Für Maßnahmen der Telekommunikationsüberwachung nach § 100a StPO sind gemäß § 101 I StPO die grundrechtssichernden Verfahrensregelungen (neben den spezifischen Verfahrensregelungen zum Kernbereichsschutz in § 100a IV S. 3 u. S. 4 StPO) der Vorschriften des (für die in Abs. 1 aufgezählten heimlichen Ermittlungsmaßnahmen einschlägigen) § 101 StPO gültig.[274] Für Maßnahmen nach § 100a StPO enthält § 101 StPO hierbei einfachgesetzliche Umsetzungen folgender verfassungsrechtlicher Vorgaben hinsichtlich grundrechtssichernder Verfahrensregelungen:

Gemäß höchstrichterlicher Rechtsprechung lässt sich die verfassungsrechtlich gebotene (grundsätzliche[275]) Bindung des erhobenen Datenmaterials an den Eingriffs- und Ermittlungszweck „nur gewährleisten, wenn auch nach der Erfassung erkennbar bleibt, dass es sich um Daten handelt, die aus Eingriffen in das Fernmeldegeheimnis stammen“[276], weshalb „eine entsprechende Kennzeichnung […] daher von Verfassungs wegen geboten [ist]“[277]. Bezogen auf Telekommunikationsüberwachung sind entsprechende Schutzvorkehrungen einfachgesetzlich in § 101 III S. 1 StPO verankert, wonach

---

271 Vgl. BVerfG, Beschluss vom 12.10.2011, Az.: 2 BvR 236/08, 2 BvR 237/08, 2 BvR 422/08, Abs.-Nr. 223.

272 BVerfG NJW 2009, 2431 (2437).

273 BVerfG NJW 2009, 2431 (2437).

274 Wie das BVerfG in einer kürzlich ergangenen Entscheidung (BVerfG, Beschl. v. 12.10.2011, Az.: 2 BvR 236/08, 2 BvR 237/08, 2 BvR 422/08) unter Zurückweisung mehrerer Verfassungsbeschwerden bezüglich der zum 01.01.2008 in Kraft getretenen Neuregelung der strafprozessualen Telekommunikationsüberwachung (BGBl. I S. 3198) nunmehr höchstrichterlich festgestellt hat, sind die Regelungen über die Benachrichtigungspflichten in § 101 IV bis VI StPO nicht zu beanstanden, welche „einer verfassungsrechtlichen Prüfung stand[halten]“ (Abs.-Nr. 228).

275 Für „nicht rundweg“ (57) ausgeschlossene Zweckänderungen, siehe BVerfG NJW 2000, 55 (57).

276 BVerfG NJW 2000, 55 (57).

277 BVerfG NJW 2000, 55 (57).

personenbezogene Daten[278], die durch eine der in § 101 I StPO genannten Maßnahme (hier einer TKÜ-Maßnahme nach § 100a StPO) erhoben wurden, durch die datenerhebende Stelle entsprechend zu *kennzeichnen* sind und die Kennzeichnung auch nach einer Übermittlung an eine andere Stelle durch diese gemäß S. 2 aufrechtzuerhalten ist. Wie die Daten genau zu kennzeichnen sind, ist gesetzlich nicht geregelt. Es muss jedenfalls die Herkunft der Daten zu erkennen sein. Mit Blick auf die Bindung erlangter personenbezogener Daten an den Zweck der Ermittlungen reicht es bei TKÜ-Maßnahmen daher aus, wenn deren Herkunft aus einer Telekommunikationsüberwachung aus dem Zusammenhang ersichtlich ist.[279]

Das Grundrecht des Fernmeldegeheimnisses aus Art. 10 I GG vermittelt den betroffenen Grundrechtsträgern ein Recht auf (spätere) Kenntnis von Datenerhebungen, die sie betreffen.[280] Wie die Kenntnisgewährung im Einzelnen auszugestalten ist, geht aus dem Grundgesetz allerdings nicht hervor[281] und obliegt somit dem Gesetzgeber, der bei nicht ausdrücklich in der Verfassung vorgeschriebenen Verfahrensregelungen in der Wahl der ihm geeignet erscheinenden Form insoweit frei ist, als sie „nur hinreichend wirksam“[282] sein muss.[283] Soweit allerdings die Kenntnis von dem Eingriff in Art. 10 I GG „dazu führen würde, dass dieser seinen Zweck verfehlt, ist es daher von Verfassungs wegen nicht zu beanstanden, die Kenntnisgewährung entsprechend einzugrenzen“[284], weshalb es „unter Umständen genügt […], den Betroffenen erst später von dem Eingriff zu benachrichtigen“[285]. Für Maßnahmen der Telekommunikationsüberwachung trägt diesem verfassungsrechtlichen Anspruch auf Kenntnisgewährung einfachgesetzlich die Verfahrensvorschrift des § 101 IV S. 1 Nr. 3 StPO in geeigneter Weise Rechnung. Die Regelung verpflichtet zur *Benachrichtigung* der Beteiligten der überwachten Telekommunikation, was regelmäßig[286] den Inhaber des

---

278 Personenbezogene Daten, § 3 BDSG: „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person […]“.

279 Vgl. BeckOK – *Hegmann*, StPO, Ed. 13, § 101, Rn. 8, bspw. durch die Aktendeckelkennzeichnung als „TKÜ-Sonderheft“.

280 Vgl. BVerfG NJW 2009, 2431 (2437); BVerfG NJW 2000, 55 (57); *Bär*, TK-Überwachung, § 101 StPO, Rn. 4.

281 Vgl. BVerfG NJW 2009, 2431 (2437).

282 BVerfG NJW 2000, 55 (57).

283 Vgl. BVerfG NJW 2000, 55 (57).

284 BVerfG NJW 2000, 55 (57).

285 BVerfG NJW 2000, 55 (57).

286 Aber nicht ausnahmslos: Sind der Inhaber des überwachten Anschlusses oder der Beschuldigte an der überwachten Telekommunikation nicht beteiligt gewesen (bspw. der Inhaber, weil er den Anschluss einer anderen Person überlassen hat oder der Beschuldigte, weil nur eine Telekommunikation des Nachrichtenmittlers mit einem Dritten überwacht wurde), so besteht eine Benachrichtigungspflicht diesen ge-

überwachten Anschlusses und (bei Personenverschiedenheit) den telekommunizierenden Beschuldigten, wie aber auch alle Anrufer und die hierüber Angerufenen[287] betrifft. Sie hat zu unterbleiben, wenn der Benachrichtigung eines Betroffenen überwiegende schutzwürdige Belange einer (anderen) betroffenen Person entgegenstehen, § 101 IV S. 3 StPO[288], bzw. kann unterbleiben, wenn es sich um eine Person handelt, die zwar von der Maßnahme betroffen ist, gegen die sich die Maßnahme aber nicht gerichtet hat (also ein Betroffener, der keine Person i. S.d § 100a III StPO ist[289], bspw. der Gesprächspartner), wenn diese von der Maßnahme nur unerheblich betroffen wurde und anzunehmen ist, dass sie kein Interesse an einer Benachrichtigung hat[290], § 101 IV S. 4 StPO. Bei TKÜ-Maßnahmen wird deshalb regelmäßig nur der Beschuldigte[291] und (bei Personenverschiedenheit) der Inhaber des überwachten Anschlusses, sofern er den Anschluss selbst benutzt, zu benachrichtigen sein.[292] Der jeweilige Diensteanbieter hingegen ist kein Beteiligter.[293]

Steht die Identität einer nach § 101 IV S. 1 StPO zu benachrichtigenden Person nicht fest (denkbar in den Fällen von Internettelefonie bspw. bei dem Gesprächspartner, der vom Ausland aus und ggf. unter einem anonymen Benutzernamen an dem Gespräch teilnimmt), so sind Nachforschungen nur nach Maßgabe einer Interessenabwägung nach § 101 IV S. 5 StPO vorzunehmen.[294]

Zuständig für die Benachrichtigung ist die Staatsanwaltschaft.[295] Gemäß § 101 V S. 1 StPO erfolgt die Benachrichtigung allerdings erst dann, „so-

---

genüber nicht, vgl. BT-Drs. 16/5846, S. 58; ebenso *Bär*, TK-Überwachung, § 101 StPO, Rn. 15.

287 Da auch in deren Rechte aus Art. 10 I GG durch die Maßnahme eingegriffen wurde, auch wenn das jeweilige Gespräch nicht entscheidungserheblich gewesen sein sollte, vgl. BeckOK – *Hegmann*, StPO, Ed. 13, § 101, Rn. 14.

288 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 101, Rn. 16.

289 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 101, Rn. 17.

290 Bspw. wenn das überwachte Telefongespräch nur die Besorgung von alltäglichen Geschäften betroffen hat, vgl. Meyer-Goßner – *Cierniak*, StPO, § 101, Rn. 17.

291 Eine Benachrichtigung an den Beschuldigten entfällt allerdings, wenn die Kommunikation eines Nachrichtenmittlers mit einer dritten Person überwacht wurde, vgl. *Bär*, TK-Überwachung, § 101 StPO, Rn. 15.

292 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 101, Rn. 9; BeckOK – *Hegmann*, StPO, Ed. 13, § 101, Rn. 13.

293 Vgl. BeckOK – *Hegmann*, StPO, Ed. 13, § 101, Rn. 13.

294 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 101, Rn. 18 m. w. N., wonach eine Identitätsfeststellung aber dann nicht erforderlich sei, wenn die Daten nach den speziellen Vorschriften zum Kernbereichsschutz nach § 100a IV S. 3 StPO zu löschen sind.

295 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 101, Rn. 5.

bald dies ohne Gefährdung des Untersuchungszwecks, des Lebens, der körperlichen Unversehrtheit und der persönlichen Freiheit einer Person und von bedeutenden Vermögenswerten“ möglich ist. Eine Benachrichtigung kommt hiernach also solange nicht in Betracht, wie noch damit gerechnet werden kann, dass mittels der heimlich ablaufenden Maßnahme noch Beweismittel erlangt werden können.[296] Wird die Benachrichtigung – solange die Gründe des § 101 V S. 1 StPO bestehen, ohne gerichtliche Zustimmung aber maximal für 12 Monate (§ 101 VI S. 1 StPO) – zurückgestellt, sind die Gründe für die Zurückstellung nach § 101 V S. 2 StPO aktenkundig zu machen. Weitergehende Vorschriften zur Zurückstellung und zum endgültigen Absehen von einer Benachrichtigung sind den Regelungen des § 101 VI StPO sowie § 101 VII S. 1 StPO zu entnehmen.

Die Pflicht zur Benachrichtigung besteht unabhängig davon, ob die Maßnahme erfolgreich verlaufen ist und unabhängig davon, ob die gewonnenen Erkenntnisse verwertet worden sind oder nicht.[297] Denn die gesetzliche Benachrichtigungspflicht dient der Gewährleistung effektiven Rechtsschutzes und eröffnet nachträglich rechtliches Gehör (Art. 103 I GG), um sich gegen die Maßnahme an sich und die Art und Weise ihrer Durchführung zur Wehr zu setzen.[298]

Inhaltlich ist in der nach § 101 IV S. 1 Nr. 3 StPO durchzuführenden Benachrichtigung auf die in § 101 VII S. 2 bis S. 4 StPO verankerte Möglichkeit nachträglichen Rechtsschutzes und die dafür vorgesehene Frist von zwei Wochen ab dem Benachrichtigungszeitpunkt *hinzuweisen*, § 101 IV S. 2 StPO. Zur Wahrnehmung ihrer berechtigten Interessen sind die Beteiligten notwendigerweise daneben auch über die (gerichtlich oder nichtgerichtlich per Eilkompetenz erfolgte) Anordnung der heimlichen Maßnahme und deren Durchführung (einschließlich der vorgenommenen Begleitmaßnahmen[299]), die jeweiligen Überwachungszeiträume und ggf. den Umfang der Überwachung[300] sowie rein formal-informatorisch über das Verfahren, in dem die Daten erhoben wurden, in Kenntnis zu setzen.[301]

Des Weiteren erfordern die verfassungsrechtlichen Anforderungen aus Art. 10 GG (ebenso wie die Rechtsweggarantie aus Art. 19 IV GG) für die Gewährleistung effektiven Rechtsschutzes eine Kontrolle durch unabhängige

---

296 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 101, Rn. 19.

297 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 101, Rn. 6.

298 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 101, Rn. 6.

299 Zur heimlichen Deinstallation der Software vor Benachrichtigung des Betroffenen, siehe 2. Teil B.II.

300 Vgl. bspw. BGH NJW 1990, 584; BGH NJW 2007, 2753.

301 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 101, Rn. 15 m. w. N.; *Bär*, TK-Überwachung, § 101 StPO, Rn. 23.

und weisungsungebundene staatliche Organe und Hilfsorgane.[302] Mangels konkreter Regelung in der Verfassung steht es dem Gesetzgeber hierbei frei, für die Ausgestaltung der Kontrolle „die ihm geeignet erscheinende Form zu wählen, wenn sie nur hinreichend wirksam ist“[303]. Gemäß der Rspr. des BVerfG gehört hierzu, „dass sich die Kontrolle auf alle Schritte des Prozesses der Fernmeldeüberwachung erstreckt“[304], wobei „kontrollbedürftig […] sowohl die Rechtmäßigkeit der Eingriffe als auch die Einhaltung der gesetzlichen Vorkehrungen zum Schutze des Fernmeldegeheimnisses [ist][305]“.

Diesen Anforderungen wird für TKÜ-Maßnahmen nach §§ 100a, 100b StPO in der Weise Rechnung getragen, dass die Beteiligten der überwachten Telekommunikation gemäß §§ 101 VII S. 2, IV S. 1 Nr. 3 StPO bei dem nach § 101 VII S. 1 StPO zuständigen Gericht (i. d. R. der Ermittlungsrichter am Sitz der Staatsanwaltschaft, § 162 I S. 1 StPO[306]) „auch nach Beendigung der Maßnahme bis zu zwei Wochen nach ihrer Benachrichtigung“ eine *gerichtliche Überprüfung* der „Rechtmäßigkeit der Maßnahme sowie der Art und Weise ihres Vollzugs“ *beantragen* können.[307] Gegen die Entscheidung des Gerichts über den Antrag nach § 101 VII S. 2 StPO ist sofortige Beschwerde statthaft, § 101 VII S. 3 StPO. In diesem Rahmen bestehen i. d. R. auch *Akteneinsichtsrechte* nach den besonderen Regelungen über Auskünfte und Akteneinsicht für Verfahrensbeteiligte[308] sowie für sonstige Antragsteller nach § 475 StPO.[309]

Unter verfassungsrechtlichen Gesichtspunkten verpflichtet der (begrenzte) Zweck der Datenerhebung und Datenverwendung bezogen auf Telekommunikationsüberwachungen grds. zur Rückgabe oder Löschung aller aufgezeichneten Telekommunikationsdaten, die nicht (mehr) zur Zweckerreichung oder den gerichtlichen Rechtsschutz benötigt werden.[310] Die Regelung des

---

302 Vgl. BVerfG NJW 2000, 55 (57); so auch BVerfG NJW 1971, 275; BVerfG NJW 1984, 419; BVerfG NJW 1985, 121.

303 BVerfG NJW 2000, 55 (57).

304 BVerfG NJW 2000, 55 (57).

305 BVerfG NJW 2000, 55 (57).

306 Solange die öffentliche Klage noch nicht erhoben wurde bzw. auch danach, sofern eine Benachrichtigung des Angeklagten noch nicht erfolgt ist; nach Erhebung der öffentlichen Klage und Benachrichtigung des Angeklagten das erkennende Gericht, vgl. im Einzelnen Meyer-Goßner – *Cierniak*, StPO, § 101, Rn. 25a, 25c m. w. N.

307 Zur str. Frage, ob diese Rechtsschutzmöglichkeit eine abschließende Sonderregelung darstellt, vgl. Meyer-Goßner – *Cierniak*, StPO, § 101, Rn. 26a m. w. N.

308 Zu den einzelnen Regelungen, siehe Meyer-Goßner – *Cierniak*, StPO, § 101, Rn. 25d m. w. N.

309 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 101, Rn. 25d m. w. N.

310 Vgl. BVerfG NJW 2009, 2431 (2438); BVerfG NJW 2000, 55 (57).

§ 101 VIII S. 1 StPO trägt dem Rechnung und schreibt die Pflicht zur *unverzüglichen Löschung* der „durch die Maßnahme erlangten personenbezogenen Daten" vor, sobald sie „zur Strafverfolgung und für eine etwaige gerichtliche Überprüfung der Maßnahme nicht mehr erforderlich" sind. Erlangte Zufallsfunde, deren Verwendung zu Beweiszwecken in anderen Strafverfahren nach § 477 II S. 2 StPO bei Vorliegen der Voraussetzungen der jeweiligen Eingriffsbefugnis zulässig ist, sind allerdings (vorerst) nicht zu löschen, da sie für Strafverfolgungszwecke weiterhin erforderlich sind.[311] Die Löschung nach § 101 VIII S. 1 StPO ist gemäß § 101 VIII S. 2 StPO *aktenkundig* zu machen. Bei TKÜ-Maßnahmen ist nicht nur die jeweilige Aufzeichnung zu vernichten, sondern auch etwaige Niederschriften über die Aufzeichnung.[312] Soweit die Löschung der personenbezogenen Daten „lediglich für eine etwaige gerichtliche Überprüfung der Maßnahme zurückgestellt ist", dürfen diese „ohne Einwilligung des Betroffenen nur zu diesem Zweck verwendet werden", § 101 VIII S. 3 HS 1, und sind gemäß § 101 VIII S. 3 HS 2 StPO „entsprechend zu sperren".

Die bestehenden grundrechtssichernden Regelungen des § 101 StPO, wie sie auf TKÜ-Maßnahmen i. S. d. §§ 100a, 100b StPO generell Anwendung finden, geben damit auch für die spezielle TKÜ-Maßnahme der Quellen-TKÜ eine nach sachlichen Erfordernissen ausgestaltete Verfahrensregelung zur Hand. Diese gewährleisten auch bei der Überwachung von Internettelefonie einen effektiven grundrechtlichen Schutz in Bezug auf das sich an die erfolgte Datenerhebung anschließende weitere Verfahren und ermöglicht Betroffenen die Inanspruchnahme gerichtlichen Rechtsschutzes.

2. Inhaltliche Anforderungen an den gerichtlichen Beschluss, § 100b I, II StPO

Gemäß obiger Ausführungen rechtfertigen die §§ 100a, 100b StPO bei Vorliegen ihrer Tatbestandvoraussetzungen als verfassungsrechtlich zulässige Schranken nach Art. 10 II 1 GG in noch hinreichend bestimmter und verhältnismäßiger Weise die im Zuge einer spezifischen Maßnahme der Quellen-TKÜ stattfindenden Eingriffe in das Grundrecht aus Art. 10 I GG der an dem jeweiligen überwachten P2P-Internettelefonat beteiligten Grundrechtsträger.

Im Rahmen seiner Grundsatzentscheidung zur (präventiven) Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalen vom 27.02. 2008 hat das BVerfG für die Quellen-TKÜ festgestellt, dass die gesetzliche

311 Vgl. *Bär*, TK-Überwachung, § 101 StPO, Rn. 40.

312 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 101, Rn. 28.

Ermächtigung zu einer Quellen-TKÜ allein an Art. 10 I GG zu messen ist, wenn sich „die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt“[313] und „dies […] durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt“[314] ist. Für das Messen einer solchen Maßnahme allein am Grundrecht des Fernmeldegeheimnisses aus Art. 10 I GG kommt damit der Begrenzung von Maßnahmen der Quellen-TKÜ entsprechend den Vorgaben des BVerfG auf derartige Daten entscheidende Bedeutung zu:

Hinsichtlich der geforderten „technischen Vorkehrungen“ zur Sicherstellung einer ausschließlichen Erfassung von Daten aus laufenden TK-Vorgängen ist dies weniger eine Frage der rechtlichen Normierung als der Umsetzung der Maßnahme in der Praxis.[315] Die hierfür eingesetzten technischen Mittel und Vorgehensweisen müssen so abgestimmt und konfiguriert sein, dass ein Zugriff auf Daten außerhalb laufender Telekommunikationsvorgänge unterbleibt, um nicht die Grenze zur „Online-Durchsuchung“ zu überschreiten. Sofern die Überwachungssoftware diese Anforderungen erfüllt und – was von staatlicher Seite bestätigt wird[316] – so konfigurierbar ist, dass derartige Beschränkungen im Zugriffsumfang wirksam umgesetzt werden können, bestehen mit Blick auf die vom BVerfG aufgestellten Anforderung keine Bedenken.

Bezüglich den vom BVerfG geforderten „rechtlichen Vorgaben“ – ebenfalls zur Sicherstellung, dass ein Zugriffs auf sonstige, bspw. auf dem Zielsystem abgespeicherte Daten ausgeschlossen und damit letztlich eine Abgrenzung zur Online-Durchsuchung gewährleistet ist – enthält bereits die Ermächtigung in § 100a I StPO eine ausschließliche Beschränkung auf Telekommunikation, also auf die technischen Vorgänge des Aussendens, Übermittelns und Empfangens von Signalen mittels TK-Anlagen.[317] Dies ist für den konkreten Einzelfall in der Quellen-TKÜ-Anordnung in Bezug auf den Umfang der Maßnahme auch nochmals ausdrücklich anzugeben (§ 100b II S. 2 Nr. 3 StPO). Für die Umsetzung einer konkreten Maßnahme der Quellen-TKÜ stellt eine richterliche Anordnung mit für die einzelne Maßnahme

---

313 BVerfG NJW 2008, 822 (826).

314 BVerfG NJW 2008, 822 (826).

315 So auch zutr. LG Hamburg, MMR 2011, 693 (696).

316 *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11.2010; so auch die Antwort der Bundesregierung, BT-Drs. 17/7760, S. 5; in dieselbe Richtung die Antwort des Bayerischen Staatsministeriums des Innern, LT-Drs. 16/10082, S. 2 u. 3.

317 So zutr. auch LG Hamburg, MMR 2011, 693 (696), wonach die Vorschrift „allein die Überwachung der ‚Telekommunikation‘, nicht aber sonstiger Daten für zulässig erklärt“, womit „der von der Vorschrift gestattete Überwachungsrahmen […] hinreichend deutlich abgegrenzt [ist]“ (696).

konkretisierenden Begrenzungen[318] bindende rechtliche Vorgaben hinsichtlich des Umfangs des Datenzugriffs und der technischen Umsetzung der Maßnahme dar, für deren Einhaltung die maßnahmedurchführende Ermittlungsbehörde Sorge zu tragen hat. Eine verfassungsgemäße Begrenzung des Eingriffsumfangs auf Ebene der Maßnahmeanordnung durch entsprechend ausgestaltete richterliche Beschlüsse ist der Rspr. des BVerfG auch bei eingriffsintensiven Ermittlungsmaßnahmen nicht unbekannt[319]. Hiernach ist es gerade auch „Aufgabe des Richters, von vornherein für eine angemessene Begrenzung der Zwangsmaßnahme Sorge zu tragen"[320].

Die bisweilen vorgetragenen Bedenken[321], wonach es fraglich sei, ob das die Maßnahme anordnende Gericht die Funktionsweise von Überwachungsprogrammen beurteilen könne bzw. bei Vorlage des Quellcodes[322] (oder ggf. des Binärcodes[323]) der für eine konkrete Quellen-TKÜ-Maßnahme bereits entworfenen Überwachungssoftware bei Antragstellung auch tatsächlich in der Lage sei zu beurteilen, ob dieser programmiersprachliche Code in seinen Textbausteinen entsprechende technische Einschränkungen in den Zugriffsmöglichkeiten der Software ausschließlich auf Daten aus laufenden TK-Vorgängen enthält, mögen zwar der – zugegebenermaßen[324] – mitunter

---

318 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 7a.

319 Vgl. BVerfG NJW 1976, 1735 (1735 f.); BVerfG NJW 1999, 2176 (2176); BVerfG NStZ 2000, 601 (601); BVerfG BeckRS 2005, 24601; BVerfG NJW 2009, 2431 (2436).

320 BVerfG NJW 1976, 1735 (1735); unter dem Begriff der strafprozessualen „Zwangsmaßnahmen" werden eingriffsintensive strafprozessuale Ermittlungsmaßnahmen verstanden, vgl. BT-Drs. 12/989, S. 39.

321 So bspw. *Eckhardt*, CR 2007, 336 (338 f.), der gar von einer „unzumutbare[n] Entscheidung" (338) spricht, die dem Richter aufgebürdet würde, und diesen, ebenso wie den antragstellenden Staatsanwalt, überfordere.

322 Auch *Quelltext*, bezeichnet den in einer Programmiersprache geschriebenen Text eines Computerprogramms, bestehend aus einer Abfolge von Befehlen, vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 192.

323 Der in maschinen-lesbare Form übersetzte Quellcode, vgl. http://de.wikipedia.org/wiki/Quelltext (zuletzt aufgerufen 15.06.2012); da dieser in Maschinensprache gehalten ist, bedürfte es einer entsprechend präzisierten Erläuterung; dass auch der Binärcode jedenfalls grds. einer Analyse nicht unzugänglich ist, belegen nicht zuletzt die anhand des Binarcodes erfolgten Untersuchungen einer Überwachungssoftware, welche in einem Ermittlungsverfahren aus dem Jahre 2009 zum Einsatz kam und Gegenstand eines Beschwerdeverfahrens vor dem LG Landshut (MMR 2011, 690) war, durch den *Chaos Computer Club* im Herbst 2011; hierfür stehen auch die unter dem Begriff des *Reverse Engineering* zusammengefassten technischen Möglichkeiten der automatischen Rückgewinnung des Quellcodes aus einem Binärcode bzw. der Rückumwandlung in eine für Menschen lesbare Form (z. B. mittels sog. Decompiler bzw. Disassembler) zur Verfügung.

324 Ohne hier verallgemeinernd sprechen zu wollen.

nicht selten anzutreffenden begrenzten Begabung juristisch versierter Personen auf dem Gebiete der (informations-)technischen Künste geschuldet sein, greifen jedoch im Bezug auf die Unzulässigkeit einer Quellen-TKÜ wegen fehlender Begrenzung des Eingriffsumfangs nicht durch. Denn den Gerichten ist es bei ggf. fehlenden Fachkenntnissen unbenommen, sich bspw. unabhängigen Sachverstandes zu bedienen[325]. Auch lässt sich durch organisatorische Vorkehrungen dafür Sorge tragen, dass den Gerichten entsprechende Informationen – z. B. in Form von Erläuterungsblättern[326] oder durch Einholen von Sachverständigenauskünften[327] – vorliegen, die eine Beurteilung des Quellcodes und vor allem dessen unverzichtbarer Bestandteile hinsichtlich der wirksamen Beschränkung des Zugriff mittels der Software ermöglichen.[328] Sofern die im Zuge der öffentlichen Diskussion über den Einsatz staatlicher Trojaner im Oktober 2011 ins Gespräch gebrachte vorherige Überprüfung staatlicher Überwachungsprogramme im Rahmen eines „Staatstrojaner-TÜV" mit anschließender Zertifizierung bspw. durch das Bundesamt für Sicherheit in der Informationstechnik (BSI)[329], welche die Vereinbarkeit der Software mit den Vorgaben des BVerfG bescheinigt (vgl. § 9 BSIG, § 2 VII BSIG)[330], politisch wie auch rechtlich und technisch umgesetzt worden sein sollte, empfiehlt es sich an dieser Stelle auch die

---

325 In diese Richtung bereits das Bundesministerium des Innern, Fragenkatalog SPD, S. 15, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-online durchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

326 In diese Richtung auch *Buermeyer*, http://ijure.org/wp/archives/756 (zuletzt aufgerufen 15.06.2012), der das Einholen von sachverständigen Stellungnahmen der die Software prüfenden Stelle vorschlägt, die dem Richter bei der Entscheidungsfindung vorliegen, sodass dieser „Punkt für Punkt" abhaken könne, ob (von der Software) alle Voraussetzungen eingehalten werden.

327 In diese Richtung bereits das Bundesministerium des Innern, Fragenkatalog SPD, S. 15, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-online durchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

328 Dass die Festlegung der Art des technischen Zugriffs dem Richter eine gar „unzumutbare Entscheidung" (*Eckhardt*, CR 2007, 336, 338; in diese Richtung auch SK – *Wolter*, StPO, § 100b, Rn. 19) aufbürde, ist unter diesen Umständen nicht zu erkennen.

329 Gemäß § 3 Nr. 13 lit. a BSIG zählt zu den Aufgaben des BSI insbesondere auch die Unterstützung der Polizeien und Strafverfolgungsbehörden bei der Wahrnehmung ihrer gesetzlichen Aufgaben.

330 In diese Richtung auch der Vorsitzende der Deutschen Polizeigewerkschaft, *Wendt*, in der Neuen Osnabrücker Zeitung vom 11.10.2011, abrufbar unter http://www.noz.de/deutschland-und-welt/gut-zu-wissen/computer/57839915/bayern-wegen-trojaner-einsatzes-unter-druck (zuletzt aufgerufen 15.06.2012); ebenso der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, *Schaar*, sowie die Bundesministerin der Justiz, *Leutheusser-Schnarrenberger*, nach *Höll*, „‚Gefährliche Grauzone'", Süddeutsche Zeitung vom 13.10.2011, S. 6; in diese Richtung bereits Anm. *Vogel*/*Brodowski*, StV 2009, 632 (634).

entsprechenden Angaben zu etwaigen Softwareversionen und Zertifizierungsnummern etc. in den anordnenden Beschluss mit aufzunehmen.

Doch auch dann, wenn eine Vorlage des genauen Quellcodes oder des Binärcodes der Überwachungssoftware im Zuge der Beantragung einer Maßnahme der Quellen-TKÜ nicht erfolgt (bspw. weil diese sich noch in der Erstellung befindet oder erst nach Beschlusserlass speziell für das Zielsystem entworfen wird[331]), ist eine solche Maßnahme nicht wegen fehlender Sicherstellung einer ausreichenden Begrenzung unzulässig. Es genügen insoweit die gerichtlichen Vorgaben im Beschluss, dass eine Überwachung der verschlüsselt übermittelten Telekommunikation unter Einsatz einer Überwachungssoftware angeordnet wird, sich die Überwachungsmaßnahme im Rahmen ihrer Umsetzung ausschließlich auf Daten aus laufenden Telekommunikationsvorgängen zu beschränken hat und sonstige auf dem System gespeicherte Daten sowie Datenverarbeitungsvorgänge (bspw. Screenshots von grafischen Bildschirminhalten, Officeanwendungen, Grafik- und Multimediaanwendungen etc.) von der Software nicht erfasst werden dürfen. Im Ermittlungsverfahren ist es grds. Sache der Staatsanwaltschaft („Herrin des Vorverfahrens“) und deren Ermittlungspersonen – insbesondere unter Beachtung des Grundsatzes der Zweck- und Verhältnismäßigkeit – darüber zu entscheiden, ob und wie ein richterlich gestatteter Eingriff vollzogen wird[332], solange hierbei die im Beschluss gesetzten Grenzen nicht überschritten werden. Dem Gericht ist es indes unbenommen[333], „zur Begrenzung des Eingriffs im Einzelfall schon im Beschluss zur Gestattung einer unter Richtervorbehalt stehenden Maßnahme Einzelheiten der Art und Weise von deren Durchführung zu regeln“[334]. Insoweit ist, nach Übergabe des Beschlusses an die Staatsanwaltschaft zur Vollstreckung (§ 36 II S. 1 StPO), die mit der Durchführung beauftragte Behörde (i. d. R. sog. TKÜ-Kompetenzzentren bei den jeweiligen Landeskriminalämtern[335]) bei der Erstellung der individuell an das Zielsystem angepassten Überwachungssoftware, bei deren heimlicher Einbringung in das Zielsystem sowie bei der anschließenden Durchführung der Maßnahme an entsprechende gerichtliche Vorgaben gebunden. Die Annahme, dass sich staatliche Behörden in einem Rechtsstaat an rechtliche

---

331 Wie dies bei TKÜ-Fällen in der Vergangenheit offenbar übliche Verfahrensweise war, vgl. Antworten des Bayerischen Staatsministeriums des Innern, LT-Drs. 16/10082, S. 1, LT-Drs. 16/10470, S. 2 und LT-Drs. 16/10607, S. 2.

332 Vgl. BGH-Ermittlungsrichter NStZ 2005, 278 (278 f.).

333 Bzw. das Gericht wird bei entsprechender Beantragung durch die Staatsanwaltschaft darüber zu befinden haben, vgl. BGH-Ermittlungsrichter NStZ 2005, 278 (279).

334 BGH-Ermittlungsrichter NStZ 2005, 278 (279).

335 Vgl. hierzu bspw. die Antwort des Bayerischen Staatsministeriums des Innern, LT-Drs. 16/10607, S. 2; für Einzelheiten, siehe auch 1. Teil A.II.1.

Vorgaben, insbesondere an gerichtliche Anordnungen zu halten haben und auch halten, ist Grundvoraussetzung des legislativen, judikativen und exekutiven Zusammenspiels und tragende Säule jeglichen staatlichen Handelns[336].

Bei Maßnahmen der Quellen-TKÜ ist deshalb durch eine *präzise Formulierung* der gerichtlichen Anordnung im Rahmen des Möglichen und Zumutbaren dafür Sorge zu tragen, dass der mit einer Quellen-TKÜ verbundene Eingriff angemessen begrenzt wird sowie „meßbar und kontrollierbar“[337] bleibt.

An die *Ausgestaltung des gerichtlichen Beschlusses*[338], mit dem eine heimliche Maßnahme („ohne Wissen der Betroffenen“[339]) zur Überwachung und Aufzeichnung von softwarebasierter P2P-Internettelefonie mittels der spezifischen Maßnahme der Quellen-TKÜ angeordnet wird, sind daher neben dem allgemeinen Inhalt eines gerichtlichen TKÜ-Beschlusses auch besondere („Quellen-TKÜ-spezifische“) inhaltliche Anforderungen zu stellen:

- Der Beschluss hat nach § 100b II S. 1 StPO schriftlich zu ergehen[340] und muss gemäß den allgemeinen Anforderungen die *erlassende Stelle* erkennen lassen:

---

336 Gegenteiliges würde insbesondere den durchführenden Ermittlungsbehörden unterstellen, dass sie sich nicht an die Inhalte von Beschlüssen halten würden; nicht nur unter Beweisverwertungsaspekten, sondern vor allem unter rechtsstaatlichen Gesichtspunkten wie auch mit Blick auf das Selbstverständnis staatlicher Behörden wären Maßnahmen unter bewusstem Missachten richterlicher Anordnungen unzulässige Ermittlungsmaßnahmen und ein regelrechter „Super-Gau“, in diese Richtung *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11.2010.

337 BVerfG NJW 1976, 1735 (1735 f.); auch BVerfG NJW 1997, 2165 (2166); BVerfG NJW 2004, 1517 (1518); st. Rspr.; entschieden für Durchsuchungsbeschlüsse, kann die Kernaussage hinsichtlich der Ver-pflichtung zur Sicherstellung einer Messbarkeit und Kontrollierbarkeit von schwerwiegenden Grundrechtseingriffen in den anordnenden Beschlüssen zum Zwecke einer angemessenen Begrenzung von Maßnahmen insoweit als genereller Maßstab herangezogen werden, vgl. auch BT-Drs. 16/5846, S. 46 zu den Inhalten der Begründung.

338 Für den vollständigen Beschlussvorschlag der richterlichen Anordnung einer strafprozessualen Überwachung der Telekommunikation einschließlich der Überwachung verschlüsselt geführter VoIP-Telekommunikation, siehe Anhang 1.

339 Wobei die gesetzliche Formulierung „auch ohne Wissen der Betroffenen“ verdeutlicht, dass die Anordnung weder unzulässig noch überflüssig ist, wenn ein Betroffener die ohne sein Einverständnis vorgenommene Überwachungsmaßnahme bemerkt hat, vgl. insoweit entspr. Meyer-Goßner – *Cierniak*, StPO, § 100f, Rn. 1.

340 Wie auch jede Verlängerungsanordnung nach § 100b I S. 5 StPO; Verstöße gegen das Schriftformerfordernis begründen aber nicht automatisch ein Verwertungsverbot für erlangte Erkenntnisse, vgl. BGH NStZ 1996, 48 (48) m. w. N.; *Bär*, TK-Überwachung, § 100a StPO, Rn. 53; für Einzelheiten zur Verwertbarkeit bei formellen oder materiellen Mängeln, siehe 2. Teil A.III.2.

Amtsgericht Musterstadt

– Ermittlungsrichter –

Az. …Gs…/…

Hinsichtlich der Frage der Zuständigkeit für die Anordnung von Maßnahmen der (Quellen-)Telekommunikationsüberwachung gelten die formellen Vorschriften des § 100b I StPO. Zuständig für die Anordnung von Maßnahmen nach § 100a I StPO ist gemäß § 100b I S. 1 StPO in erster Linie das Gericht, d. h. im Ermittlungsverfahren der Ermittlungsrichter nach §§ 162 I S. 1, 169 StPO (i. d. R. der Ermittlungsrichter beim Amtsgericht, in den Fällen des § 169 I StPO i. V. m. § 120 GVG der Ermittlungsrichter beim OLG bzw. beim BGH) am Sitz der Staatsanwaltschaft, nach Erhebung der öffentlichen Klage das mit der Sache befasste Gericht (§ 162 III StPO).[341] Erforderlich ist gemäß § 100b I S. 1 StPO stets ein Antrag der Staatsanwaltschaft. Nur bei Gefahr im Verzug[342] kann nach § 100b I S. 2 StPO eine TKÜ-Maßnahme durch die Staatsanwaltschaft selbst angeordnet werden[343], wobei die staatsanwaltliche Eilanordnung nach § 100b I S. 3 StPO außer Kraft tritt[344], wenn sie nicht binnen drei Werktagen gerichtlich bestätigt wird.[345] Eine solche Regelung, wie sie in § 100b I S. 1 bis S. 3 StPO ver-

---

341 Zu den Folgen von Verstößen gegen die Verfahrensvorschriften des § 100b I StPO in Bezug auf die Verwertbarkeit erlangter Erkenntnisse, siehe 2. Teil A.III.2.

342 *Gefahr im Verzug* liegt grds. dann vor, wenn das vorherige Einholen der richterlichen Anordnung den Erfolg der Maßnahme gefährden würde, vgl. BVerfG NJW 1979, 1539 (1540); bei strafprozessualen Maßnahmen ist dies regelmäßig dann der Fall, wenn ein Verlust von Beweismitteln droht, der allerdings nicht von den Ermittlungsbehörden selbst herbeigeführt worden sein darf, vgl. BVerfG NJW 2001, 1121 (1123).

343 Wobei für Maßnahmen der Quellen-TKÜ auf Grund der regelmäßig erforderlichen Vorbereitungszeit die Zahl von Eilfällen in der Praxis eher gering ausfallen dürfte; auch eine solche Eilanordnung durch die Staatsanwaltschaft nach § 100b I S. 2 StPO hat dann schriftlich zu ergehen (§ 100b II S. 1 StPO) und muss dieselben inhaltlichen Anforderungen erfüllen, wie die Anordnung durch das Gericht nach § 100b I S. 1 StPO; wegen der fehlenden Prüfung durch ein unabhängiges Gericht empfiehlt sich hierbei eine besonders präzise Darlegung der einzelnen Prüfungsschritte im Rahmen der Beschlussgründe; die Staatsanwaltschaft muss zudem die tatsächlichen Grundlagen für die Annahme des (gerichtlich voll nachprüfbaren) Vorliegens von Gefahr im Verzug zeitnah dokumentieren, vgl. Meyer-Goßner – *Cierniak*, StPO, § 100b, Rn. 3 m. w. N.

344 Tritt die staatsanwaltschaftliche Anordnung wegen fehlender richterlicher Bestätigung innerhalb von drei Werktagen außer Kraft, so bleiben die bis dahin auf Grund der Eilanordnung rechtmäßig gewonnenen Erkenntnisse verwertbar, vgl. hierzu *Bär*, TK-Überwachung, § 100b StPO, Rn. 3 f.; Meyer-Goßner – *Cierniak*, StPO, § 100b, Rn. 1 m. w. N.; zur Unverwertbarkeit bei willkürlicher Annahme von Gefahr im Verzug, siehe 2. Teil A.III.2.

345 Vgl. *Bär*, TK-Überwachung, § 100b StPO, Rn. 3; Meyer-Goßner – *Cierniak*, StPO, § 100b, Rn. 1.

ankert ist, wird hierbei auch heimlichen Überwachungsmaßnahmen auf informationstechnischen Systemen verfassungsrechtlich gerecht, da ein solcher Zugriff „grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen [ist]“[346] und vom „Erfordernis einer vorherigen Kontrolle der Maßnahme durch eine dafür geeignete neutrale Stelle […] eine Ausnahme für Eilfälle, etwa bei Gefahr im Verzug, vorgesehen werden [darf], wenn für eine anschließende Überprüfung durch die neutrale Stelle gesorgt ist“[347].

B e s c h l u s s[348]

In dem Ermittlungsverfahren gegen

[*Name*], [*Vorname*], geb. [*Geburtsname*], geboren am [*Geburtsdatum*], in [*Geburtsort*], [*Staatsangehörigkeit*], [*Familienstand*], [*Beruf*], wohnhaft [*Straße mit Hausnummer, PLZ mit Ort*],

wegen [*Tatvorwurf*]

wird …

- Gemäß den allgemeinen Anforderungen an die formelle Ausgestaltung von Anordnungen im strafprozessualen Ermittlungsverfahren sind in den Kopf des *Beschlusses* (bei staatsanwaltschaftlicher Eilanordnung: *Verfügung*) – soweit entsprechende Informationen vorliegen – zunächst die Angaben zur Person des Beschuldigten als desjenigen, gegen den als Tatverdächtiger das Ermittlungsverfahren, in welchem die (richterliche bzw. bei Gefahr im Verzug staatsanwaltliche und richterlich bestätigte Anordnung ergeht, betrieben wird[349], aufzunehmen und der Tatvorwurf in Form der Straftat, deren Begehung oder (bei entsprechender Versuchsstrafbarkeit) deren Versuch der Beschuldigte verdächtig ist, zu nennen. Wie auch aus der Regelung des § 100b II Nr. 1 StPO hervor geht, muss die genaue Identität des Beschuldigten allerdings noch nicht bekannt sein, weshalb der Beschluss insofern auch gegen Personen mit unvollständigen Angaben oder „gegen Unbekannt“ ergehen kann.[350]

---

346 BVerfG NJW 2008, 822 (832).

347 BVerfG NJW 2008, 822 (832).

348 Unter Einbeziehung der Entwürfe nach BeckOK – *Graf*, StPO, Ed. 13, Formulare zum Strafprozessrecht, III., Quellen-TKUE, und *Bär*, TK-Überwachung, § 100a StPO, Rn. 73 für die nachfolgenden Beschlussbestandteile; für den vollständigen Beschlussvorschlag der richterliche Anordnung einer strafprozessualen Überwachung der Telekommunikation einschließlich der Überwachung verschlüsselt geführter VoIP-Telekommunikation, siehe Anhang 1.

349 Gemäß dem materiellen oder formellen Beschuldigtenbegriff, vgl. Meyer-Goßner – *Meyer-Goßner*, StPO, Einl., Rn. 76 m. w. N.; aber auch, sofern ein Ermittlungsverfahren noch nicht eingeleitet ist, derjenige, der entsprechend verdächtig ist und gegen den Ermittlungen erst mit der Überwachungsmaßnahme beginnen, vgl. *Bär*, TK-Überwachung, § 100a StPO, Rn. 38.

- Von Gesetzes wegen hat die sich hieran anschließende *Entscheidungsformel* der nach § 100b II S. 1 StPO schriftlich zu ergehenden Anordnung gemäß § 100b II S. 2 StPO bestimmte Angaben zu enthalten:

  In der Entscheidungsformel des Beschlusses sind – neben der konkreten Maßnahmeanordnung – gemäß § 100b II S. 2 Nr. 1 StPO zunächst „soweit wie möglich" der Name und die Anschrift des Betroffenen anzugeben, gegen den sich die Maßnahme richtet. Dies wird im Regelfall ebenfalls der Beschuldigte als Anschlussinhaber sein, kann aber auch einen der in § 100a III StPO neben dem Beschuldigten aufgezählten Dritten als Anschlussinhaber betreffen. Mit einer solchen Formulierung („soweit möglich") stellt der Gesetzgeber klar, dass die Anordnung einer TKÜ-Maßnahme auch gegen Personen ergehen kann, deren (wahre) Identität (bspw. wegen der Nutzung von Alias- oder Decknamen) (noch) nicht oder (noch) nicht vollständig bekannt ist und ggf. durch die Überwachung erst zu ermitteln ist.[351]

  Gemäß § 100b II S. 2 Nr. 2 StPO muss in der Entscheidungsformel des Weiteren die Rufnummer oder einer andere Kennung des/der zu überwachenden Anschlusses/Anschlüsse oder des Endgerätes angegeben werden.

  Ferner sind gemäß *§ 100b II S. 2 Nr. 3 StPO* die Art, der Umfang und die Dauer der TKÜ-Maßnahme unter Benennung des Endzeitpunktes[352] in der Entscheidungsformel zu bezeichnen. Die gemäß dieser Vorschrift zu treffenden konkretisierenden Angaben dienen hierbei der Sicherstellung, „dass die Maßnahme zielgerichtet eingesetzt und der Richtervorbehalt im Sinne einer umfassenden Prüfung aller eingriffsrelevanten Aspekte ausgeübt wird"[353].

  Bei TKÜ-Beschlüssen, deren Entscheidungsformel einem Telekommunikationsunternehmen (Netzbetreiber/Access-Provider) auf Grund der Inanspruchnahme dessen gesetzlicher Verpflichtung zur Mitwirkung an der Überwachungsmaßnahme (§ 100b III StPO) nach § 12 TKÜV übermittelt wird – wie dies bei Beschlüssen zur Durchführung klassischer TKÜ sowie bei „kombinierten Beschlüssen", die sowohl klassische TKÜ als auch Quellen-TKÜ anordnen, regelmäßig der Fall ist –, sah der Gesetzgeber bei Maßnahmen der Telekommunikationsüberwachung nach § 100a I

---

350 Vgl. KK – *Nack*, StPO, § 100a, Rn. 37; ebenso *Bär*, TK-Überwachung, § 100a StPO, Rn. 38; BT-Drs. 16/5846, S. 46.

351 Vgl. BT-Drs. 16/5846, S. 46; Meyer-Goßner – *Cierniak*, StPO, § 100b, Rn. 4; *Bär*, TK-Überwachung, § 100b StPO, Rn. 8, § 100f StPO, Rn. 17.

352 Zur Vermeidung von Ungewissheiten über den spätesten Beendigungszeitpunkt, vgl. BT-Drs. 16/5846, S. 47.

353 BT-Drs. 16/5846, S. 47.

StPO – anders als bei der akustischen Wohnraumüberwachung nach § 100c I, § 100d II S. 2 Nr. 2 StPO – für den gesetzlich vorgeschriebenen Inhalt nach § 100b II S. 2 StPO von der Angabe des Tatvorwurfs in der Entscheidungsformel aus Datenschutzgründen ab.[354] Es empfiehlt sich daher auch für die Praxis, bei derartigen Beschlüssen auf die Angabe des Tatvorwurfes in Beschlussbestandteilen, die an Dritte übermittelten werden, zu verzichten und für eine entsprechende Gewährleistung des Datenschutzes Sorge zu tragen. In den – Dritten nicht übermittelten – Gründen des Beschlusses ist die Anlasstat (Katalogstraftat nach § 100a I Nr. 1, II StPO) allerdings i. S. d. Sicherstellung einer Mess- und Kontrollierbarkeit des mit der angeordneten Maßnahme verbundenen Grundrechtseingriffs[355] näher auszuführen.[356]

Der jeweilige Umfang der Entscheidungsformel des konkreten TKÜ-Beschlusses hängt davon ab, ob die Überwachung nur unverschlüsselte Telekommunikation, nur verschlüsselte IP-Kommunikation oder beides erfassen soll. Im Regelfall wird in der Praxis ein „kombinierter Beschluss" ergehen, der die umfassende Überwachung jeglicher über den betroffenen Anschluss des Adressaten der Maßnahme geführten Telekommunikation anordnet.

In Ziff. I der Entscheidungsformel wird daher regelmäßig zunächst die Anordnung der „klassischen" TKÜ zur Überwachung herkömmlicher (unverschlüsselter) Telekommunikation (insb. Festnetztelefonie) über den/die Anschluss/Anschlüsse des Maßnahmeadressaten erfolgen:

I. nach §§ 100a I, 100b StPO auf Antrag der Staatsanwaltschaft gemäß § 33 IV StPO ohne vorherige Anhörung die Überwachung und Aufzeichnung[357] der Telekommunikation (Inhaltsdaten und Verkehrsdaten) für die Telekommunikationsanschlüsse

Anschluss 1: [*Rufnummer/andere Anschlusskennung*]
[*ggf. zusätzlich: zugeordneter DSL-Anschluss*]
[*Name Anschlussinhaber/Anschlussnutzer*]
[*Anschrift Anschlussinhaber/Anschlussnutzer*]

Anschluss 2: […]

durch

---

354 Vgl. BT-Drs. 16/5846, S. 46.

355 Vgl. BVerfG NJW 1976, 1735 (1735 f.); auch BVerfG NJW 1997, 2165 (2166); BVerfG NJW 2004, 1517 (1518); st. Rspr.

356 Vgl. *Bär*, TK-Überwachung, § 100b StPO, Rn. 8.

357 Bei einem Zugriff auf Fern*sprech*verkehr muss beides – sowohl Überwachung als auch Aufzeichnung – für sich angeordnet werden, vgl. Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 8, § 100b, Rn. 4.

[*Name des nach § 100b III StPO verpflichteten Netzbetreibers/ Providers*[358]]

[*Anschrift Netzbetreiber/Provider*]

für die Zeit vom [*Datum Beginn*] bis zum [*Datum Ende*, *max. 3 Monate*] angeordnet.

- Die von den vorliegenden Untersuchungen behandelten *Quellen-TKÜ-spezifischen Inhalte* einer Überwachungsanordnung nach §§ 100a, 100b StPO sind bei ausschließlichen Quellen-TKÜ-Beschlüssen, d. h. bei Quellen-TKÜ als alleinigem Anordnungsgegenstand, bereits als Ziff. I aufzunehmen. Bei den regelmäßigen auftretenden „kombinierten Beschlüssen" empfiehlt es sich die Quellen-TKÜ als Maßnahme zur Überwachung der über den Zielanschluss verschlüsselt geführten Internettelefonie als eigenen Anordnungspunkt in der Entscheidungsformel aufzuführen. Inhaltlich ergeben sich für die Quellen-TKÜ folgende Anforderungen:

  II. nach §§ 100a I, 100b StPO auf Antrag der Staatsanwaltschaft gemäß § 33 IV StPO ohne vorherige Anhörung[359] die Überwachung und Aufzeichnung[360] der über

  Anschluss: [*Rufnummer/andere Anschlusskennung*]
  [*ggf. zusätzlich: zugeordneter DSL-Anschluss*]
  [*Name Anschlussinhaber/Anschlussnutzer*]
  [*Anschrift Anschlussinhaber/Anschlussnutzer*]

  Endgerät: [Gerätekennung/Seriennummer; nähere Bezeichnung]

  geführten, …

  Bei einer Überwachung von verschlüsselter Internettelefonie handelt es sich bei der nach § 100b II S. 2 Nr. 2 StPO in der Entscheidungsformel anzugebenden Rufnummer oder anderen Kennung des zu überwachenden Anschlusses oder des Endgerätes im Regelfall um die Kennung des/der

---

358 Soweit bei der Überwachung der über den betroffenen Zielanschluss geführten herkömmlichen (unverschlüsselten) Telekommunikation die Verpflichtungen des § 100b III S. 1 und S. 2 i. V. m. §§ 1 ff. TKÜV zu entsprechenden Mitwirkung in Anspruch genommen und das jeweils verpflichtete Telekommunikationsunternehmen an der Durchführung der Überwachung auf der Netzstrecke beteiligt wird, ist eine entsprechende Vorgabe in die Anordnung aufzunehmen und die Entscheidungsformel dem verpflichteten Telekommunikationsunternehmen gemäß den Regelungen des § 12 TKÜV zu übermitteln.

359 Die Anordnung erfolgt ohne vorherige Anhörung der/des Beschuldigten und der sonstigen Betroffenen, um den Zweck der Ermittlungsmaßnahme nicht zu gefährden, vgl. Meyer-Goßner – *Cierniak*, StPO, § 100b, Rn. 3.

360 Bei einem Zugriff auf Fern*sprech*verkehr muss beides – sowohl Überwachung als auch Aufzeichnung – für sich angeordnet werden, vgl. Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 8, § 100b, Rn. 4.

für die VoIP-Kommunikation genutzten Telefonanschlusses/-anschlüsse, über den/die der Zugang in das Internet erfolgt, einschließlich eines dem Telefonanschluss zugeordneten DSL-Anschlusses, sofern die Internetverbindung über einen DSL-Zugang (mittlerweile wohl der Regelfall) realisiert wird. Die Regelung des § 100b II S. 2 Nr. 2 StPO sieht auch die Angabe der Rufnummer oder einer sonstigen Kennung (z. B. Hardwarekennung) des Endgerätes der überwachten Telekommunikation vor. Dies wird bei der Quellen-TKÜ vor allem in den Fällen relevant werden, in denen die IP-Kommmunikation nicht über ein stationäres System, welches an einem festen Telekommunikationsanschluss des Maßnahmeadressaten „hängt" (i. d. R. ein Personal Computer), geführt wird, sondern über ein mobiles System (z. B. Laptop/Notebook) ortsungebunden erfolgen kann, und bei denen daher nicht auszuschließen ist, dass es im Überwachungszeitraum zu verschiedenen Standorten verbracht wird und sich unter Verwendung der jeweils vor Ort vorhandenen Anschlüsse (z. B. WLAN-Hotspots etc.) im Rahmen der nomadischen Nutzung von IP-Diensten ins Internet einloggt.[361] Soweit entsprechende Informationen bei Anordnungserlass vorliegen, sorgt hierbei die (zusätzliche[362]) Angabe einer zuordenbaren Kennung des überwachten Endgerätes (Seriennummer) in der Anordnung für eine Flexibilität und Unabhängigkeit bei spontanen Ortswechseln.[363]

Darüber hinaus ist das informationstechnische System, in das zum Zwecke der Telekommunikationsüberwachung eingegriffen wird, auch aus Gründen der Klarheit und Bestimmtheit der Anordnung sowie zur Konkretisierung des Eingriffs möglichst genau zu bezeichnen, d. h. soweit entsprechende Angaben bei Anordnungserlass vorliegen (bspw. auf Grund einer im Vorfeld stattgefundenen herkömmlichen TKÜ-Maßnahme, in deren Rahmen sowohl der Umstand der Nutzung verschlüsselter Telekommunikationsformen festgestellt als auch die technischen Parameter des genutzten Systems erhoben wurden[364]). Zu nennen ist hierbei bspw.

---

361 Für die praktische Ermittlungsarbeit ist zudem zu beachten, dass für den Fall, dass sich das mobile Gerät zum Zeitpunkt der Überwachung im europäischen Ausland befinden bzw. im Zeitraum der Überwachung dorthin verbracht werden sollte, gemäß Art. 20 des *Übereinkommen gemäß Artikel 34 des Vertrags über die Europäische Union über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union* (EU-RhÜbk) der betreffende Mitgliedstaat von der Überwachung zu unterrichten ist.

362 Da auch bei mobilen informationstechnischen Systemen regelmäßig ein „Heim"-Internetanschluss des Maßnahmeadressaten, über den das System zu Telekommunikationszwecken benutzt wird, gegeben ist.

363 Vgl. bspw. LG Hamburg, BeckRS 2011, 06733.

364 Vgl. hierzu auch die Antwort des Bayerischen Staatsministeriums des Innern, LT-Drs. 16/10469, S. 2 f.

die Geräteart (Personal Computer, Laptop, aber bspw. auch internetfähige mobile Endgeräte wie Smartphones[365]) sowie ggf. auch nähere Gerätespezifizierung des betroffenen informationstechnischen Systems.

> … verschlüsselten Telekommunikation sowie die Vornahme der hierzu erforderlichen Maßnahmen, um die Telekommunikationsdaten [Sprachdaten; *bei Video-Internettelefonie zusätzlich:* einschließlich Videodaten[366]; bei *Instant Messaging via IP zusätzlich:* einschließlich Textdaten[367]] vor deren Verschlüsselung und nach deren Entschlüsselung im Wege des Einsatzes einer speziellen [*ggf.*: bei Gericht hinterlegten[368]] Überwachungssoftware (*soweit bekannt*: *Bezeichnung*, *Versionsnummer*, *Zertifizierungsnummer des Bundesamtes für Sicherheit in der Informationstechnik*[369]) auf dem zur Telekommunikation gebrauchten *Endgerät* [*möglichst genaue Bezeichnung: bspw. Geräteart, Gerätekennung/Seriennummer, Betriebssystem/-version etc.*] überwachen zu können, …

Mit einer derartigen Beschreibung der angeordneten Quellen-Telekommunikationsüberwachung wird der gemäß § 100b II S. 2 Nr. 3 StPO in der Entscheidungsformel anzugebenden Art der Maßnahme und des damit verbundenen spezifischen technischen Zugriffs in hinreichend präziser,

---

365 Verschlüsselte softwarebasierte VoIP-Kommunikation, die die besondere Maßnahme der Quellen-TKÜ erforderlich macht, kann nicht nur über Computer stattfinden, sondern mittlerweile auch über entsprechende *softwarebasierte* Nutzung mobiler internetfähiger Endgeräte wie insbesondere moderner Smartphones, siehe auch 1. Teil A.I.2.d).

366 Vgl. insoweit zutr. LG Hamburg, MMR 2011, 693 (693 f.); hiervon nicht erfasst ist allerdings das Anfertigen sog. Screenshots von der grafischen Bildschirmoberfläche, so zutr. auch LG Landshut, MMR 2011, 690 (691); zur Abgrenzung siehe 1. Teil A.I.2.e) sowie 2. Teil A.II.4.

367 Für Einzelheiten zu Instant Messaging via IP, siehe 1. Teil A.I.2.f).

368 Durch Hinterlegung des Quellcodes der eingesetzten Überwachungssoftware beim anordnenden Gericht (soweit bereits verfügbar und vorliegend) ließe sich eine entsprechende Nachprüfbarkeit im Rahmen des sich anschließenden Strafverfahrens zusätzlich dahingehend sicherstellen, dass die Überwachungssoftware weder sonstige auf dem Zielsystem gespeicherte Daten außerhalb laufender Telekommunikationsvorgänge erfassen konnte noch unter dem Gesichtspunkt der Datenmanipulation dazu in der Lage war, Daten frei auf dem Zielsystem zu platzieren, vgl. hierzu auch die Ausführungen unter 2. Teil A.III.3. und 2. Teil B.III.2.c). Die Vorlage und Hinterlegung des Quellcodes bei Beantragung der Maßnahme gibt dem Gericht aber zudem auch die Möglichkeit sicherzugehen, dass die zum Einsatz kommende Überwachungssoftware auch die erforderlichen Beschränkungen hinsichtlich des Eingriffsumfangs einhält; durch entsprechende organisatorische Vorkehrungen, bspw. in Form von Erläuterungsblättern oder durch Heranziehen unabhängigen Sachverstandes, lässt sich dafür Sorge tragen, dass den Gerichten eine Nachvollziehbarkeit des Quellcodes ermöglicht wird.

369 Soweit entsprechende Schritte zur Überprüfung und Zertifizierung „verfassungsrechtlich zulässiger" Überwachungsprogramme bereits umgesetzt wurden; zur erwogenen Einführung eines sog. „Staatstrojaner-TÜVs", siehe 3. Teil A.I.1.c) und 3. Teil B.III.3.c).

nachvollziehbarer und für die durchführenden Behörden umsetzbarer Weise Rechnung getragen, um die TKÜ-Maßnahme zielgerichtet einsetzen[370] zu können. Nach Maßgabe einer solchen Bestimmung hinsichtlich der Art des technischen Zugriffs in der gerichtlichen Anordnung, ist die über §§ 100a, 100b StPO vermittelte Eingriffsbefugnis nach zutreffender Auffassung auch nicht an die Mitwirkung eines TK-Dienstleisters zwingend gebunden. Denn gemäß der gesetzgeberischen Intention des § 100b III StPO besteht zwar eine Verpflichtung des jeweiligen TK-Dienstleisters zur Ermöglichung und ggf. Umsetzung von Überwachungsmaßnahmen gemäß den Vorgaben des § 100b III S. 1, S. 2 StPO i. V. m. §§ 1 ff. TKÜV, jedoch sind die Ermittlungsbehörden auch berechtigt, die Überwachung und Aufzeichnung ausschließlich mit eigenen Mitteln (und somit eigenständig) durchzuführen.[371] Dementsprechend bedarf es allein bei der Anordnung einer Quellen-TKÜ auch nicht der Aufnahme eines TK-Dienstleisters zur Ermöglichung oder Umsetzung der angeordneten Überwachung und Aufzeichnung. Die Anordnung betrifft hierbei auch die notwendigen *Vorbereitungs- und Begleitmaßnahmen*, d. h. bei einer Maßnahme der Quellen-TKÜ die Maßnahmen zur heimlichen bzw. verdeckten Einbringung der Überwachungssoftware in das Zielsystem, was sich auf Grundlage obiger dogmatischer Ausführungen[372] auf eine Annexkompetenz zu § 100a I StPO stützen lässt. Zudem ist es dem Gericht unbenommen, Regelungen hinsichtlich der Art und Weise der technischen Durchführung zu treffen, was ebenfalls von der Anordnungskompetenz umfasst ist.[373]

> … für die Zeit vom [*Datum Beginn*] bis zum [*Datum Ende*, *max. 3 Monate*] angeordnet.

---

370 Vgl. BT-Drs. 16/5846, S. 46.

371 So BT-Drs. 16/5846, S. 47, wonach „eine Obliegenheit der Strafverfolgungsbehörden, Telekommunikationsüberwachungsmaßnahmen stets unter Mitwirkung eines Telekommunikationsdienstleisters durchzuführen, […] nicht begründet [wird]. Vielmehr enthält § 100a Abs. 1 Satz 1 StPO-E eine nicht durch die Mitwirkung der Telekommunikationsdienstleister bedingte Befugnis, Telekommunikation zu überwachen und aufzuzeichnen“ (S. 47); zust. Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 7a, 8; *Bär*, TK-Überwachung, § 100a StPO, Rn. 32; a. A. SK – *Wolter*, StPO, § 100a, Rn. 20 u. § 100b, Rn. 19; *Sankol*, CR 2008, 13 (17); krit. auch *Eckhardt*, CR 2007, 336 (338); für Einzelheiten zur Mitwirkungspflicht Dritter, siehe auch 2. Teil A.II.6.

372 Siehe hierzu im Einzelnen 2. Teil B.III.

373 Vgl. BVerfG NJW 2004, 999, 1014 (hier zu Maßnahmen der akustischen Wohnraumüberwachung), wonach das Gericht „je nach den Umständen des Einzelfalls auch Regelungen zu Art und Weise des Vollzugs zu treffen haben [wird], darunter auch zu Vorbereitungs- und Begleitmaßnahmen sowie gegebenenfalls zur technischen Durchführung“ (1014); vgl. des Weiteren BGH-Ermittlungsrichter NStZ 2005, 278 (278 f.).

Gemäß § 100b II S. 2 Nr. 3 StPO ist in der Entscheidungsformel ferner die Dauer der Maßnahme anzugeben sowie der (konkrete) Endzeitpunkt zu benennen – auch dann, wenn die Höchstdauer von 3 Monaten nach § 100a I S. 4, 5 StPO angeordnet wird[374]. Die Höchstdauer kann in der Anordnung verkürzt oder auch voll ausgeschöpft werden. Für die Fristberechnung finden die §§ 42 ff. StPO Anwendung. Für die Umsetzung der gerichtlichen Anordnung ist hierbei zu beachten, dass die festgesetzte Frist nicht erst mit dem Vollzug der TKÜ-Maßnahme beginnt, sondern bereits mit Erlass der (Erst- oder Verlängerungs-)Anordnung.[375] Soweit die Voraussetzungen für die Anordnung der TKÜ-Maßnahme nach § 100a I StPO unter Berücksichtigung der bislang gewonnenen Ermittlungsergebnisse[376] fortbestehen, kann sie gemäß § 100a I S. 5 StPO durch das Gericht mehrmals verlängert werden[377], stets jedoch nur um höchstens weitere 3 Monate. Zur Beurteilung, ob die Voraussetzungen des § 100a StPO fortbestehen, muss das Gericht durch die durchführenden Ermittlungsbehörden entsprechend über den Ermittlungsstand informiert werden. Findet eine Verlängerung der Frist nicht statt, so tritt die Anordnung mit Erreichen des in der Entscheidungsformel festgesetzten Endzeitpunktes automatisch außer Kraft.[378]

Innerhalb des angeordneten Überwachungszeitraums dauert die TKÜ-Maßnahme so lange an, wie die Eingriffsvoraussetzungen des § 100a I StPO fortbestehen. Während der Durchführung der konkreten TKÜ-Maßnahme muss daher durch die Ermittlungsbehörden[379] ständig im

---

374 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100b, Rn. 4; das Fehlen einer ausdrücklichen Befristung nach § 100b I S. 4, II S. 2 Nr. 3 StPO in der Anordnung ist mit Blick auf die Revisibilität eines Verstoßes unschädlich, wenn die durchgeführte Überwachung die Dauer von 3 Monaten als zeitliche Obergrenze der Erstanordnung nicht überschritten hat, vgl. BGH NJW 2009, 2463 (2464).

375 Vgl. BT-Drs. 16/5846, S. 46; bereits BGH NJW 1999, 959 (960); *Bär*, TK-Überwachung, § 100b StPO, Rn. 6, wobei der Tag des Erlasses nach §§ 43 I, 42 StPO nicht mitgerechnet wird.

376 Aus sämtlichen in der Sache durchgeführten Ermittlungsmaßnahmen, nicht nur aus der Überwachung und Aufzeichnung der Telekommunikation, vgl. Meyer-Goßner – *Cierniak*, StPO, § 100b, Rn. 2.

377 Ohne gesetzlich bestimmte absolute Höchstgrenze für die Zahl der Verlängerungsanordnungen, vgl. auch *Bär*, TK-Überwachung, § 100b StPO, Rn. 5; gesetzgeberische Bestrebungen (BT-Drs. 16/5846, S. 45 f.), wonach Anordnungs- und Verlängerungszeiträume auf 2 Monate verkürzt werden sollten und Verlängerungsanordnungen über 6 Monate hinaus – vorbehaltlich des § 169 StPO – nur durch das Landgericht hätten angeordnet werden dürfen, wurden in den endgültigen Gesetzesentwurf mangels Erforderlichkeit nicht übernommen, vgl. BT-Drs. 16/6979, S. 43.

378 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100b, Rn. 2.

379 Die Entscheidung über die Beendigung der Maßnahme nach § 100b IV S. 1 StPO obliegt im Ermittlungsverfahren i. d. R. dem Staatsanwalt, dem Richter nur bei

Auge behalten werden, ob insbesondere der erforderliche Tatverdacht noch besteht, die weiteren Ermittlungen auch ohne die grundrechtsintensive Maßnahme der Telekommunikationsüberwachung fortgeführt werden können, der Aufenthalt des Beschuldigten ermittelt wurde, oder die Erfolgsaussichten der Maßnahme entfallen sind.[380] Gemäß § 100b IV S. 1 StPO ist bei Wegfall der Anordnungsvoraussetzungen – auch bei Unverhältnismäßigkeit im Einzelfall[381] – eine auf Grund der Anordnung ergriffene Maßnahme unverzüglich, also ohne schuldhafte Verzögerung, zu beenden[382]. Gemäß § 100b IV S. 2 StPO ist das anordnende Gericht[383] über die Ergebnisse[384] der beendeten Maßnahme zu unterrichten[385].

> Zulässig sind hierbei aber nur solche Maßnahmen, die der Überwachung und Aufzeichnung von Daten aus laufenden Telekommunikationsvorgängen dienen und die für deren Umsetzung zwingend erforderlich sind.
>
> Unzulässig sind insbesondere
>
> 1. die Durchsuchung der Speichermedien des fremden *Endgerätes* nach bestimmten gespeicherten Daten und Dateien sowie das Übertragen und Kopieren solcher Daten und Dateien außerhalb eines Telekommunikationsvorgangs sowie
> 2. die Überwachung von Datenverarbeitungsvorgängen, die nicht der Telekommunikation dienen (z. B. sog. Screenshots von grafischen Bildschirminhalten, Office- und Textverarbeitungsanwendungen, Grafik- und Multimediaanwendungen, Spiele u. ä.).

Über eine derartige Formulierung kann in Bezug auf den nach § 100b II S. 2 Nr. 3 StPO in der Entscheidungsformel anzugebenden Umfang der

---

einer Überwachung zum Zweck der Aufenthaltsermittlung in einem anhängigen Verfahren, vgl. Meyer-Goßner – *Cierniak*, StPO, § 100b, Rn. 9.

380 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100b, Rn. 2 u. 9.

381 So auch *Bär*, TK-Überwachung, § 100b StPO, Rn. 22.

382 Ein Wegfall der Voraussetzungen des § 100a StPO liegt jedoch nicht vor, wenn zwar der Beschuldigte verhaftet wurde, ein Nachrichtenmittler (§ 100a III Var. 2 StPO) von dem überwachten Anschluss aber weiterhin Gebrauch macht und durch das Fortführen der Überwachung weitere Aufklärung in der Sache zu erwarten ist, vgl. BGH NJW 1994, 2904 (2907).

383 Auch dann, wenn das anordnende Gericht nicht mit dem weiteren Verfahrensablauf betraut ist, vgl. *Bär*, TK-Überwachung, § 100b StPO, Rn. 23.

384 Anders als gemäß § 100d IV S. 1 StPO bei der akustischen Wohnraumüberwachung ist eine Unterrichtung des Gerichts neben den Ergebnissen auch über den Verlauf der Maßnahme bei Telekommunikationsüberwachungen gesetzlich nicht vorgegeben.

385 Die Unterrichtung dient hierbei der Stärkung der mit dem Richtervorbehalt vorgesehenen rechtsstaatlichen Kontrolle sowie der Ermöglichung einer Erfolgskontrolle, vgl. BT-Drs. 16/5846, S. 47 f. Konkrete Inhalte für die Unterrichtung sind von Gesetzes wegen nicht vorgeschrieben; in der Praxis dürfte eine kurze schriftliche Mitteilung ausreichen, vgl. *Bär*, TK-Überwachung, § 100b StPO, Rn. 23.

Maßnahme für eine wirkungsvolle Begrenzung einer Maßnahme der Quellen-TKÜ bei der Umsetzung Sorge getragen werden. Durch die auf diese Weise in der gerichtlichen Anordnung niedergelegten, die Bestimmung des § 100b II S. 2 Nr. 3 StPO konkretisierenden Begrenzungen des Maßnahmeumfangs lässt sich den vom BVerfG für eine alleinige Grundrechtsbetroffenheit des Fernmeldegeheimnisses aus Art. 10 I GG geforderten rechtlichen Vorgaben[386] Rechnung tragen.[387] Durch die ausdrückliche ausschließliche Legitimierung von Maßnahmen, die der Überwachung und Aufzeichnung von Daten aus laufenden Telekommunikationsvorgängen dienen sowie für die Umsetzung der Überwachung und Aufzeichnung erforderlich sind, werden Maßnahmen mit weitergehenden Wirkungen in ihrer Eingriffsreichweite, wie bspw. eine Online-Durchsuchung, auf Anordnungsebene der Quellen-TKÜ durch gerichtliche Entscheidung für unzulässig erklärt und der Zugriff demgemäß auf den zulässigen Umfang einer Quellen-TKÜ begrenzt. An diese gerichtliche Begrenzung sind die Ermittlungsbehörden bei der anschließenden Umsetzung der angeordneten Maßnahme gebunden. Durch den Ausschluss („Unzulässig sind insbesondere …“) werden – neben dem positiv formulierten zulässigen Umfang der angeordneten Quellen-TKÜ („Zulässig sind hierbei aber nur …“) – zusätzlich und in nicht abschließender Weise („insbesondere“) die beiden wesentlichen Konstellationen einer (unzulässigen) Online-Durchsuchung, die hinsichtlich der technischen Vorgehensweise (Einsatz einer sog. *Remote Forensic Software*[388]) ähnlich der Quellen-TKÜ realisiert wird[389], nämlich die Durchsuchung von Speichermedien des fremden Endgerätes (i. d. R. Computer) nach darauf gespeicherten Daten außerhalb laufender Telekommunikationsvorgänge (Nr. 1) sowie die Überwachung von Datenverarbeitungsvorgängen, die nicht der Telekommunikation dienen (Nr. 2)[390], als unzulässige Maßnahmen ausdrücklich hervorgehoben.

---

386 Vgl. BVerfG NJW 2008, 822 (826).

387 So auch Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 7a.

388 Vom BKA entwickelte Software für verdeckte Eingriffe in informationstechnische Systeme zum Zwecke der Online-Durchsuchung, vgl. auch BT-Drs. 17/7760, S. 10.

389 Für Einzelheiten zu Online-Durchsuchung mit Online-Durchsicht und Online-Überwachung, siehe 1. Teil A.II.2.a).

390 So stellte auch das LG Landshut, MMR 2011, 690 (691) mit Beschluss vom 20.01.2011 fest, dass beim Vollzug eines Quellen-TKÜ-Beschlusses ein Erfassen von grafischen Bildschirminhalten durch Fertigung sog. Screenshots („Ablichtungen“ der Bildschirmanzeigen) mangels Rechtsgrundlage rechtswidrig sei, da zum Zeitpunkt einer derartigen Maßnahme kein Telekommunikationsvorgang stattfinde; nicht zu beanstanden sei nach Auffassung des LG allerdings die Anordnung und Durchführung der Überwachung und Aufzeichnung laufender verschlüsselter Tele-

III. Bei der Durchführung der Maßnahmen nach Ziff. II. ist[391]

1. technisch sicherzustellen, dass an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden,

2. das eingesetzte Mittel nach dem Stand der Technik gegen unbefugte Nutzung zu schützen,

3. kopiertes Datenmaterial nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen,

4. bei jedem Einsatz des technischen Mittels die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes, die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen, die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und die Organisationseinheit, die die Maßnahme durchführt, zu protokollieren, wobei das Protokolldatenmaterial nur dazu zu verwenden ist, um dem Betroffenen oder einer dazu befugten öffentlichen Stelle die Prüfung zu ermöglichen, ob die Maßnahme nach Ziff. II rechtmäßig durchgeführt worden ist, und unverzüglich zu löschen ist, soweit es für diesen Zweck nicht mehr erforderlich ist.

Zum Zwecke der Begrenzung des Eingriffs mittels einer Überwachungssoftware in Bezug auf ihr technisches Überwachungspotential wie auch zum Zwecke der Nachprüfbarkeit des Verfahrens und der Beweissicherheit erlangter Erkenntnisse ist der Einsatz einer Überwachungssoftware im Rahmen einer Maßnahme der Quellen-TKÜ möglichst transparent zu halten. Zwar ist es im Ermittlungsverfahren grds. Sache der mit der Durchführung der Ermittlungen betrauten Staatsanwaltschaft und der von ihr beauftragten Ermittlungspersonen darüber zu entscheiden, wie eine angeordnete Maßnahme durchgeführt wird (vgl. § 36 II S. 1 StPO). Dem

---

kommunikation sowie der hierzu erforderlichen technischen Maßnahmen im Wege einer auf §§ 100a, 100b StPO gestützten Quellen-TKÜ; die Feststellungen des LG Landshut erfolgen zu Recht, da es sich bei einem Kopieren und Speichern von grafischen Bildschirminhalten (nicht gemeint ist hiermit das Überwachen und Aufzeichnen von Videosignalen im Rahmen eines laufenden Videotelefonates) nicht um eine Quellen-TKÜ, sondern um eine (gegenwärtig unzulässige) strafprozessuale Online-Durchsuchung in Form der Online-Überwachung handelt [vgl. 1. Teil A. II.2.a)], die auch maßnahmetypisch nicht auf die bloße Überwachung und Aufzeichnung laufender Telekommunikationsvorgänge ausgerichtet ist; für weitergehende Einzelheiten zum Anfertigen von Screenshots, siehe auch 2. Teil A.II.4.

391 In Anlehnung an die in §§ 20l II S. 2, 20k II, III BKAG bzw. § 31c IV S. 3 POG RP gewählten Formulierungen.

Gericht ist es jedoch unbenommen, gerade in Fällen wie der Quellen-TKÜ, bei denen dies aus den oben genannten Gründen in besonderer Weise geboten erscheint, zum Zwecke der Begrenzung des Eingriffs im konkreten Fall bereits im Beschluss, mit dem eine unter dem Richtervorbehalt stehende Ermittlungsmaßnahme angeordnet wird, Einzelheiten zur Art und Weise des Vollzugs, insbesondere deren (technischer) Durchführung, festzulegen.[392] Aus diesem Grunde empfiehlt es sich hier, neben den Auflagen zur Konfiguration und Wirkungsweise der Software (Ziff. II) auch den wesentlichen technischen Umgang mit dem infiltrierten System und der darauf eingesetzten Überwachungssoftware sowie die Protokollierung der verfahrensmäßigen Schritte hinsichtlich des Einsatz der Software auf dem informationstechnischen System (Ziff. III) im Wege der richterlichen Anordnung im Beschluss vorzugeben und hierüber einen revisionsfesten Einsatz der Überwachungssoftware abzusichern.

Die in Ziff. III Nr. 1 der Entscheidungsformel enthaltene Verpflichtung zur technischen Sicherstellung der ausschließlichen Vornahme solcher Veränderungen am Zielsystem, die für die Erhebung von Daten aus laufenden Telekommunikationsvorgängen unerlässlich sind, sowie zur – soweit technisch möglich automatisierten – Rückgängigmachung der vorgenommenen Veränderungen bei Beendigung der Maßnahme, tragen hierbei dem Umstand Rechnung, dass im Zuge der Realisierung der Quellen-TKÜ-Maßnahme auf ein informationstechnisches System zugegriffen wird, welches außerhalb der ausschließlichen Überwachung laufender Telekommunikationsvorgänge unter dem Schutz des Grundesrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 I i. V. m. Art. 1 I GG steht[393]. Zugunsten der Verhältnismäßigkeit ist hierdurch ein Ergreifen solcher technischer Vorkehrungen bei Durchführung der Maßnahme richterlich vorgegeben, die einerseits durch die Begrenzung der Systemveränderungen auf das für die Datenerhebung unerlässliche Mindestmaß geäußerten Bedenken[394] hinsichtlich Beschränkbarkeit und Nachladbarkeit der Überwachungssoftware Rechnung tragen, andererseits in angemessener Weise dem Ermittlungs- und Aufklärungsinteresse gerecht werden. Dies lässt sich bspw. über eine elektronische Signatur des technischen Mittels erreichen, welche sowohl die Software als auch deren Funktionsumfang identifiziert.[395]

---

392 Vgl. BGH-Ermittlungsrichter NStZ 2005, 278 (278 f.); auch BVerfG NJW 2004, 999 (1014).

393 Vgl. BVerfG NJW 2008, 822 (825 f.).

394 Zu den Kritikpunkten im Einzelnen, siehe 2. Teil B.III.2.c) sowie 3. Teil A.I.1.c).

395 Vgl. insoweit LT RP-Drs. 15/4879, S. 37 zu § 31c II POG RP.

Auf Grund der Verpflichtung zum Rückgängigmachen der Veränderungen bei Beendigung der Maßnahmen sind sämtliche Veränderungen an Systemdateien rückgängig zu machen und insbesondere die in das System eingebrachte Überwachungssoftware vollständig zu löschen. Dies hat aus Gründen der Zuverlässigkeit und Einfachheit der Abwicklung[396] grds. automatisiert zu erfolgen, jedoch mit der Einschränkung, „soweit" die automatisierte Rückgängigmachung technisch möglich ist. Im Falle der technischen Unmöglichkeit sind die Veränderungen hingegen – soweit die Möglichkeit besteht[397] – manuell rückgängig zu machen.

Die richterliche Vorgabe der Ziff. III Nr. 2 trägt geäußerten Bedenken hinsichtlich des Systemschutzes vor einem unbefugten Eindringen Dritter über den zum Zwecke des Ausleitens der Daten im infiltrierten System geschaffenen Zu- bzw. Ausgang („Systemlücke") sowie hinsichtlich der Gefahr des Verschaffens und Verwendens der Software durch Dritte zu missbräuchlichen Zwecken Rechnung, indem das eingesetzte technische Mittel gegen unbefugte Nutzung zu schützen ist. Die technischen Schutzvorkehrungen zur Verhinderung einer missbräuchlichen Nutzung der Software durch Dritte umfasst hierbei insbesondere den Schutz vor dem Ausleiten der Daten an einen anderen als den von staatlichen Behörden zum Zwecke der Maßnahmedurchführung eingerichteten Server sowie vor einem Identifizieren und Ansprechen der Überwachungssoftware auf dem infiltrierten System durch Dritte.[398] Die den Ermittlungsbehörden auferlegten technischen Schutzmechanismen sind hierbei allein nach dem jeweiligen Stand der Technik vorzunehmen, da ein gerechter Ausgleich der betroffenen Interessen[399] keinen unverhältnismäßig hohen, gar unerfüllbaren Maßstab hinsichtlich der technischen Schutzmöglichkeiten verlangt.[400] Eine zu einhundert Prozent sichere Software gibt es ebenso wenig, wie

---

396 Vgl. insoweit auch BT-Drs. 16/10121, S. 29 zu § 20k II BKAG.

397 Vgl. insoweit LT RP-Drs. 15/4879, S. 37 zu § 31c II POG RP.

398 Vgl. insoweit auch BT-Drs. 16/10121, S. 29 zu § 20k II BKAG.

399 Für Einzelheiten zur Verhältnismäßigkeit, siehe 2. Teil B.III.2. sowie 3. Teil A.I.1.c).

400 Dies steht auch in Einklang mit den Feststellungen des BVerfG im Rahmen der verfassungsrechtlichen Bewertung der Vorschriften zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten (BVerfG NJW 2010, 833), wonach „die Verfassung […] nicht detailgenau vor[gibt], welche Sicherheitsmaßgaben im Einzelnen geboten sind" (840), „im Ergebnis […] jedoch ein Standard gewährleistet werden [muss], der unter spezifischer Berücksichtigung der Besonderheiten der […] geschaffenen Datenbestände ein besonders hohes Maß an Sicherheit gewährleistet" (840), wobei „sicherzustellen [ist], dass sich dieser Standard – etwa unter Rückgriff auf einfachgesetzliche Rechtsfiguren wie den Stand der Technik […] – an dem Entwicklungsstand der Fachdiskussion orientiert und neue Erkenntnisse und Einsichten fortlaufend aufnimmt" (840).

ein uninfiltrierbares System. Etwas Unmögliches kann aber nicht Bedingung für die Zulässigkeit einer Maßnahme sein, die im Rahmen der Beurteilung der Verhältnismäßigkeit einer Seite auferlegt wird. Im Sinne des allgemeinen Begriffsverständnisses von *Stand der Technik*[401] ist sich demnach bei den zu ergreifenden technischen Schutzvorkehrungen vielmehr eines technischen Verfahrens zu bedienen, welches auf gesicherten Erkenntnissen von Wissenschaft und Technik basiert und mithin der Entwicklungsstand fortschrittlicher Verfahren zur Software-, Daten- und Systemsicherheit (hier bspw. proprietäre Protokolle, Verschlüsselung nach dem *Advanced Encryption Standard* etc.) heranzuziehen, der die praktische Eignung gegen Missbrauch, insbesondere unbefugte Nutzung, gesichert erscheinen lässt. Gerade auch mit Blick auf die spezifischen Besonderheiten der Kommunikation über das Internet und der nur begrenzten Vertraulichkeit in die Sicherheit der Systeme wird ein dem Stand der Technik entsprechender Schutz den Anforderungen an eine angemessene Handhabung des Einsatzes der Überwachungssoftware im Rahmen einer Quellen-TKÜ-Maßnahme gerecht.

Werden – wie zuletzt im Rahmen der Diskussion über eine durch den *Chaos Computer Club* im Oktober 2011 veröffentliche sog. „Regierungs-Malware“[402] – Bedenken auch dahingehend geäußert, ob im Rahmen des Einsatzes einer Überwachungssoftware ein ausreichender Schutz für die abgefangenen, ausgeleiteten und kopierten Daten vor Kenntnisnahme und ggf. Veränderung durch Dritte gewährleistet wird, so kann den Erfordernissen der Integrität, d. h. Vollständigkeit und Unverfälschtheit des erlangten Datenmaterials, sowie der Wahrung des Datenschutzes in der Anordnung durch Vorgaben hinsichtlich des weiteren Umgangs mit den Daten nach deren Abgreifen Rechnung getragen werden. In Umsetzung der Vorgabe der Ziff. III Nr. 3 ist die Software daher so zu konfigurieren, dass die ausgeleiteten Daten auf dem Weg über das Datennetz zum sog. „Recording-Server“[403] vor einer Veränderung, unbefugten Löschung oder unbefugten Kenntnisnahme durch technische Maßnahmen nach dem Stand der Technik (bspw. durch Datenverschlüsselungen, Signaturverfahren etc.), geschützt sind und die erstellten Datenkopien auch während der anschließenden Speicherung bei den Ermittlungsbehörden entsprechend

---

401 Vgl. hierzu bspw. die Legaldefinitionen in § 3 VI Bundesimmissionsschutzgesetz oder in § 2 XI Gefahrstoffverordnung.

402 Bericht „Analyse einer Regierungs-Malware“ vom 08.10.2011, abrufbar unter http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf (zuletzt aufgerufen 15.06.2012).

403 Für Einzelheiten zum technischen Ablauf des Abfangens, Ausleitens und Aufzeichnens, siehe 1. Teil A.II.3.

zugangsgeschützt und beweissicher (bspw. mit elektronischer Signatur[404] und elektronischem Zeitstempel[405]) verwahrt sind.

Über die richterlichen Vorgaben nach Ziff. III Nr. 4 zur Protokollierung der Maßnahme sowie zur Verwendung und den weiteren Umgang mit den Protokolldaten lassen sich neben der Gewährleistung effektiven Grundrechts- und Datenschutzes auch die Gerichts- und Revisionsfestigkeit der erlangten Daten als Beweismittel rechtlich absichern. Hierbei ermöglicht die Protokollierung in der nach Ziff. III Nr. 4 festgelegten Weise für die anschließende gerichtliche Würdigung bzw. eine etwaige spätere gerichtliche Nachprüfung im Rahmen der Rechtsmittelinstanz den Nachweis dafür, dass die – auf Grund der Angaben im Protokoll festgestellten – Daten, welche von der im Protokoll vermerkten durchführenden Organisationseinheit der Ermittlungsbehörde mit der im Protokoll bezeichneten Überwachungssoftware im dokumentierten Überwachungszeitraum gewonnenen wurden, tatsächlich von dem – auf Grund der Angaben im Protokoll identifizierten – überwachten informationstechnischen System stammen, vollständig vorliegen und nicht verändert wurden[406], d. h. als Beweismittel authentisch und integer sind.

- Im Hinblick auf den mit einer (Quellen-)TKÜ-Anordnung regelmäßig und naturgemäß verbundenen intensiven Eingriff in das Fernmeldegeheimnis aus Art. 10 I GG sind unter entsprechender Anwendung der für Durchsuchungsanordnungen entwickelten Grundsätze bei den gerichtlichen Beschlüssen – wie bereits oben geschildert – bestimmte verfassungsrechtliche Anforderungen zu beachten.[407] Durch geeignete Formulierungen des (Quellen-)TKÜ-Beschlusses – d. h. der Entscheidungsformel und der diese erläuternden Gründe – hat das Gericht deshalb „im Rahmen des Möglichen und Zumutbaren“[408] insbesondere dafür Sorge zu tragen, dass

---

404 Mit Hilfe kryptographischer Verfahren wird durch eine elektronische Signatur jede Manipulation oder Verfälschung an Originaldaten sofort erkennbar gemacht; zudem lässt sich durch eine sichere Zuordnung der verwendeten kryptographischen Schlüssel der Signaturersteller/Urheber signierter Daten zweifelsfrei feststellen, vgl. https://www.bsi.bund.de/ContentBSI/Publikationen/Faltblaetter/F10ElektronischeSignatur.html (zuletzt aufgerufen 20.05.2012); durch das Verwenden von Prüfsummen (engl. *checksum*) lässt sich bspw. die Integrität von Daten bei Übermittlung und -speicherung gewährleisten, vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 45 u. 190; durch ein Hashverfahren lässt sich mittels eines sog. *Hashwertes* („digitaler Fingerabdruck“) bspw. auch die Authentizität einer Datei überprüfen, vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 105.

405 So bspw. auch BT-Drs. 16/10121, S. 29 zu § 20k II BKAG.

406 Vgl. insoweit auch BT-Drs. 16/10121, S. 30 zu § 20k III BKAG.

407 Vgl. hierzu auch BT-Drs. 16/5846, S. 46.

408 BVerfG NJW 1976, 1735 (1735).

der Grundrechtseingriff in Art. 10 I GG „meßbar und kontrollierbar bleibt“[409]. Dies folgt aus den tangierten Grundrechtspositionen sowie aus dem Rechtsstaatsprinzip.[410] Im Rahmen der Entscheidung über die Anordnung hat das Gericht das Vorliegen der einzelnen Eingriffsvoraussetzungen eigenständig zu prüfen.[411] Hinsichtlich der Anforderungen an die *Begründung* des anordnenden Beschlusses sind qualifizierte Begründungspflichten – wie bspw. in § 100d III StPO[412] für Maßnahmen der akustischen Wohnraumüberwachung nach § 100c StPO verankert – für Maßnahmen der Telekommunikationsüberwachung nach §§ 100a, 100b StPO gesetzlich zwar nicht speziell vorgeschrieben. Aus dem allgemeinen Grundsatz des § 34 StPO ergibt sich aber die Pflicht zu einer angemessenen Begründung, die neben der richterlichen Eigenkontrolle insbesondere der Nachvollziehbarkeit und Überprüfbarkeit der Entscheidung[413] dient[414]:

---

409 BVerfG NJW 1976, 1735 (1735 f.); auch BVerfG NJW 1997, 2165 (2166); BVerfG NJW 2004, 1517 (1518); st. Rspr.; entschieden für Durchsuchungsbeschlüsse, kann die Kernaussage hinsichtlich der Verpflichtung zur Sicherstellung einer Messbarkeit und Kontrollierbarkeit von schwerwiegenden Grundrechtseingriffen in den anordnenden Beschlüssen zum Zwecke einer angemessenen Begrenzung von Maßnahmen insoweit als genereller Maßstab herangezogen werden, vgl. auch BT-Drs. 16/5846, S. 46 zu den Inhalten der Begründung.

410 Vgl. Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 25 f.

411 Vgl. BGH NJW 2010, 1297 (1298); so auch BVerfG NJW 2003, 1787 (1792), wonach „es […] die Aufgabe und Pflicht des Ermittlungsrichters [ist], sich eigenverantwortlich ein Urteil zu bilden und nicht etwa die Anträge […] nach einer nur pauschalen Überprüfung einfach gegenzuzeichnen. Zur richterlichen Einzelentscheidung gehören eine sorgfältige Prüfung der Eingriffsvoraussetzungen und eine umfassende Abwägung zur Feststellung der Angemessenheit des Eingriffs im konkreten Fall. Schematisch vorgenommene Anordnungen vertragen sich mit dieser Aufgabe nicht.“ (1792).

412 Insbesondere hinsichtlich der bestimmten Tatsachen, die den Verdacht begründen (§ 100d III S. 2 Nr. 1 StPO), die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme (§ 100d III S. 2 Nr. 2 StPO) sowie die tatsächlichen Anhaltspunkte i. S. d. § 100c IV S. 1 StPO (§ 100d III S. 2 Nr. 3 StPO).

413 Dies erfordert zumindest eine knappe Darstellung der Tatsachen, die den Tatverdacht begründen sowie der jeweiligen Beweislage; die Darstellung soll sich hierbei nicht nur in der Wiedergabe des Gesetzestextes oder vorgefertigter Textbausteine erschöpfen, sondern mit tatsächlichen, auf den konkreten Fall bezogenen Anhaltspunkten unterlegt werden, wobei die Bezugnahme auf Aktenteile im Einzelfall genügen kann, so BGH NJW 2003, 368 (369); BGH NJW 1986, 390 (391); ebenso *Bär*, TK-Überwachung, § 100a StPO, Rn. 58, § 100b StPO, Rn. 7; zur Frage der Verwertbarkeit erlangter Erkenntnisse bei Vorliegen von Defiziten in der Begründung, siehe 2. Teil. A.III. 2.

414 Vgl. BGH NJW 2003, 368 (369); BT-Drs. 16/5846, S. 46; *Bär*, TK-Überwachung, § 100b StPO, Rn. 7; zudem kann die zu den notwendigen Begründungsinhal-

Gründe

1. Der/Die Beschuldigte ist auf Grund bestimmter Tatsachen verdächtig, Täter oder Teilnehmer einer [*Katalogstraftat*] nach § 100a I Nr. 1 i. V. m. § 100a II Nr. [*einschlägige Nummer*] StPO (sog. Katalogstraftat) zu sein.

Auf Grund der bisherigen Ermittlungen liegt dem/der Beschuldigte/-n zur Last,

[*Tatbeschreibung*]

begangen zu haben.

Dies ist strafbar als [*Straftatbestimmung*]

gemäß §§ [*Strafvorschriften*].

Unter Berücksichtigung der verfassungsrechtlichen Anforderungen an die Messbarkeit und Kontrollierbarkeit des Grundrechtseingriffs muss der Beschluss im Rahmen des Möglichen und Zumutbaren tatsächliche Angaben über die mit der strafprozessualen Ermittlungsmaßnahme aufzuklärenden Straftaten bzw. den *Inhalt des jeweiligen Tatvorwurfs* enthalten, sodass klar erkennbar ist, worauf die Überwachungsmaßnahme abzielt.[415] Bei der gemäß obiger Darstellung einzufügenden Tatbeschreibung ist für die praktische Anwendung im Einzelfall zu beachten, dass eine bloße schlagwortartige Bezeichnung der mutmaßlichen Straftat nach gefestigter Rspr. des BVerfG für eine den rechtstaatlichen Erfordernissen gerecht werdende Begründung nicht genügt.[416] Zum Abstecken des äußeren Rahmens, innerhalb dessen die Maßnahme durchzuführen ist, ist es vielmehr notwendig, den Tatvorwurf konkret zu beschreiben[417] und die Tathandlung in sachlicher wie zeitlicher Hinsicht derart zu konkretisieren, dass – sowohl für die Durchführung der (Quellen-)TKÜ-Maßnahme als auch für eine etwaige spätere gerichtliche Nachprüfung deren Rechtmäßigkeit im Rahmen des nachträglichen Rechtsschutzes nach § 101 VII S. 2 StPO – feststeht, was dem Beschuldigten konkret vorgeworfen wird/wurde[418] und hierdurch darzulegen, dass es tatsächliche Anhaltspunkte für das Vorlie-

---

ten von Durchsuchungsbeschlüssen ergangene Rechtsprechung entsprechend herangezogen werden, vgl. BT-Drs. 16/5846, S. 46.

415 Vgl. BVerfG NJW 1976, 1735 (1736); Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 26 u. 28; so auch BVerfG NJW 2003, 1787 (1792), wonach „die richterliche Anordnung des Eingriffs in das Fernmeldegeheimnis […] den Tatvorwurf so beschreiben [muss], dass der äußere Rahmen abgesteckt wird, innerhalb dessen sich der Eingriff halten muss […]“ (1792).

416 Vgl. BVerfG NJW 1976, 1735 (1736); BVerfG NJW 1992, 551 (552).

417 Vgl. BVerfG NJW 1976, 1735 (1736); BVerfG NJW 1999, 2176 (2176).

418 Entsprechend der Konkretisierung der Tathandlung bei (offen vollzogenen) Durchsuchungsbeschlüssen, welche den Beschuldigten darüber in Kenntnis setzen soll, was ihm vorgeworfen wird, vgl. LG Mönchengladbach, StV 1986, 246; hierauf verweisend auch Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 28.

gen der Straftat/-en, deren Begehung der Beschuldigte verdächtigt wird, gibt/gab.

2. Der Tatverdacht beruht auf

   □ den Angaben des/der …

   □ [*sonstige bestimmte Tatsachen*].

   [*ggf:* Ergänzend wird auf den Zwischenbericht der mit den Ermittlungen betrauten bzw. sachbearbeitenden Dienststelle [*Angabe der Dienststelle*] vom [*Datum*], Bl. [*Blattzahl*] der Ermittlungsakten Bezug genommen.]

3. Die Tat wiegt auch im vorliegenden Fall schwer (§ 100a I Nr. 2 StPO), weil [*nähere Ausführungen*].

Da für die Frage der Verhältnismäßigkeit i. e. S. (Angemessenheit) das Gewicht des Strafverfolgungsinteresses maßgeblich anhand der Stärke des Tatverdachts sowie der Schwere der Straftat zu beurteilen ist[419], ist in dem Beschluss – zur Gewährleistung seiner Messbarkeit und Kontrollierbarkeit – einerseits darzulegen, auf welchen Tatsachen und Fakten (konkrete Sachverhaltsmomente[420]) der zum Zeitpunkt der Anordnung vorliegende konkrete *Tatverdacht* für die Begehung der unter Punkt 1. der Beschlussgründe vorgenommenen Beschreibung des Tatvorwurfs basiert.[421] Nur wenn und soweit entsprechende tatsächliche Angaben zur notwendigen Verdachtslage[422] im Beschluss vorhanden sind[423], ist auch eine Nachprüfung (Art. 19 IV GG) der Angemessenheit der jeweiligen (Quellen-)TKÜ-Maßnahme möglich. Mithin handelt es sich bei dem Bestehen eines (konkreten) Tatverdachts bereits um ein verfassungsrechtliches Erfordernis zur Beurteilung der Angemessenheit des Eingriffs.[424] Entsprechende Angaben zum Tatverdacht sind im Rahmen von (Quellen-) TKÜ-Beschlüssen ohne weiteres auch möglich und zumutbar, da das Vorliegen eines von *bestimmten Tatsachen begründeten Verdachtes*[425] der

---

419 Vgl. insoweit Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 34 f.; für Einzelheiten zur Verhältnismäßigkeit i. e. S., siehe auch 3. Teil A.I.1.c).

420 Ein abstrakter Verdacht genügt lediglich für die Eröffnung des repressiven Aufgabenbereichs nach §§ 152 II, 163 I StPO, vgl. insoweit Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 37 m. w. N.

421 Vgl. insoweit Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 30.

422 Bei Maßnahmen nach § 100a I StPO: ein *von bestimmten Tatsachen begründeter Verdacht*, § 100a I Nr. 1 StPO.

423 Vgl. insoweit Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 27.

424 Vgl. insoweit Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 37.

425 Es bedarf hierfür weder eines „dringenden Tatverdachts" i. S. d. § 112 I S. 1 StPO noch eines „hinreichenden Tatverdachts" i. S. d. § 203 StPO; sog. „einfacher" Tatverdacht (Anfangsverdacht, §§ 152 II, 160 I StPO) ist ausreichend, soweit dieser auf bestimmten Tatsachen beruht; hierfür ist erforderlich, dass sich der Verdacht auf

Täter- oder Teilnehmerschaft an einer begangenen oder versuchten Katalogstraftat gemäß § 100a I Nr. 1 StPO für TKÜ-Maßnahmen nach §§ 100a, 100b StPO qualifiziertes Tatbestandsmerkmal ist, welches das Gericht im Rahmen seiner Entscheidung über den Antrag auf Anordnung der Maßnahme eigenständig zu prüfen hat. Diesbezüglich steht dem anordnenden Gericht (bzw. der anordnenden Staatsanwaltschaft in den Fällen von Gefahr im Verzug) ein Beurteilungsspielraum zu.[426] Die gerichtliche Anordnung muss hierbei zwar nicht alle Erwägungen darlegen, jedoch müssen aus dieser die wesentlichen Grundlagen der Entscheidung hervorgehen.[427] Im Rahmen der Darlegung der verdachtsbegründenden Tatsachen, welche der Entscheidung zugrunde liegen, kann auch auf einzelne Aktenteile der Ermittlungsakte konkret Bezug genommen werden.[428]

Des Weiteren kommt zur Beurteilung des Gewichts des Strafverfolgungsinteresses der *Schwere der aufzuklärenden Straftat*, welche anhand ihres Unrechtsgehaltes zu bestimmen ist[429], bei Maßnahmen der (Quellen-) TKÜ maßgebliche Bedeutung zu. Das Vorliegen einer schweren Straftat i. S. d. § 100a I Nr. 1, II StPO, welche nach § 100a I Nr. 2 StPO auch im konkreten Einzelfall schwer wiegen muss, ist nicht nur gemäß § 100a I Nr. 1 StPO Tatbestandsvoraussetzung einer (Quellen-)TKÜ-Maßnahme nach §§ 100a, 100b StPO auf Ebene des einfachen Gesetzes, sondern auch maßgebliches Kriterium zur Prüfung und Beurteilung der Verhältnismäßigkeit i. e. S.[430]. Neben der Darlegung des Tatverdachts sind deshalb zum Zwecke der Mess- und Kontrollierbarkeit des Beschlusses auch tatsächliche Angaben zur Schwere der Straftat im konkret vorliegenden Fall in die Gründe mit aufzunehmen.

---

eine hinreichend sichere Tatsachenbasis stützt, durch schlüssiges Beweismaterial bereits ein gewisses Maß an Konkretisierung erreicht hat und nicht nur unerheblich ist. Nicht ausreichend wären bspw. nur vage Anhaltspunkte, nicht nachgeprüfte Gerüchte oder bloße Vermutungen. Vgl. BGH NJW 1995, 1974 (1975); BGH NJW 2001, 2266 (2268); BVerfG NJW 2000, 55 (66); BVerfG NJW 2003, 1787 (1791); Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 9 m. w. N.; *Bär*, TK-Überwachung, § 100a StPO, Rn. 17 m. w. N.

426 Vgl. BGH NJW 2010, 1297 (1298); demgemäß ist die Nachprüfung der Rechtmäßigkeit der angeordneten Überwachungsmaßnahme sowie etwaiger Verwertungsverbote erlangter Erkenntnisse nur daran auszurichten, ob die Entscheidung vertretbar war, vgl. BGH NJW 1995, 1974 (1975); ebenso BGH NJW 2003, 368 (369); für Einzelheiten zur Frage der Verwertbarkeit bei materiellen Mängeln der Anordnung, siehe 2. Teil A.III.2.

427 Vgl. BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 37.

428 Vgl. BGH NJW 2003, 368 (369); Meyer-Goßner – *Cierniak*, StPO, § 100b, Rn. 5 m. w. N.

429 Vgl. insoweit Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 41.

430 Vgl. insoweit Maunz/Dürig – *Papier*, GG, Art. 13, 61. EL 2011, Rn. 34 f.

4. Inhaber des/der oben genannten Telekommunikationsanschlusses/-anschlüsse ist (§ 100a III StPO)

   □ der/die Beschuldigte.

   □ eine Person, von der auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den/die Beschuldigte/-n bestimmte oder von ihm herrührende Mitteilungen entgegennimmt oder weitergibt.

   □ eine sonstige Person, von der auf Grund bestimmter Tatsachen anzunehmen ist, dass der/die Beschuldigte ihren/ihre Anschluss/Anschlüsse benutzt.

   [*nähere Ausführung der Tatsachen*]

Adressat einer (Quellen-)TKÜ-Maßnahme kann gemäß § 100a III StPO neben dem Beschuldigten auch ein Dritter sein, der Nachrichten von dem Beschuldigten entgegennimmt oder an diesen weiterleitet (sog. *Nachrichtenmittler*) oder dessen Anschluss der Beschuldigte benutzt. Die Anordnung kann im Falle der beabsichtigten Maßnahmerichtung gegen einen solchen Dritten nur dann ergehen, wenn sich dessen Nachrichtenmittlereigenschaft oder der Umstand der Benutzung dessen Anschlusses durch den Beschuldigten auf eine hinreichend sichere Tatsachenbasis gründet.[431] Die Tatsachen, auf Grund derer das Vorliegen einer Beziehung i. S. d. § 100a III StPO zum Beschuldigten anzunehmen ist, sind deshalb – zur Sicherstellung der Mess- und Kontrollierbarkeit der Anordnung – ebenfalls in den Gründen näher auszuführen.

5. Die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Beschuldigten wäre auf andere Weise wesentlich erschwert oder aussichtslos (§ 100a I Nr. 3 StPO), weil

   □ andere Aufklärungsmittel einen erheblich größeren Zeitaufwand erfordern und deshalb zu einer wesentlichen Verfahrensverzögerung führen würden.

   □ andere Aufklärungsmittel zu wesentlich schlechteren Erkenntnissen führen würden.

   □ andere Aufklärungsmittel mit hoher Wahrscheinlichkeit keinen Erfolg versprechen.

   □ andere erfolgversprechende Aufklärungsmittel nicht vorhanden sind oder nicht zur Verfügung stehen.

   [*nähere Ausführungen*]

Auch die im Rahmen der Entscheidung zu prüfenden Umstände[432], ob die in § 100a I Nr. 3 StPO enthaltene *qualifizierte Subsidiaritätsklausel*, dass

---

431 Vgl. BVerfG NJW 2005, 2603 (2610).

432 Wie bei der Beurteilung des Tatverdachtes wird auch hier dem anordnenden Gericht oder StA (Eilanordnung) ein Beurteilungsspielraum zugestanden, vgl. BVerfG NJW 1995, 1974 (1975).

die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise als durch die Überwachung und Aufzeichnung von Telekommunikation wesentlich erschwert oder aussichtslos sein müssen, erfüllt ist, sind zum Zwecke der Messbarkeit und Kontrollierbarkeit der Anordnung in den Beschlussgründen näher auszuführen. Auch hinsichtlich der Beurteilung der Aussichtlosigkeit oder wesentlichen Erschwernis steht dem anordnenden Gericht (bzw. der anordnenden Staatsanwaltschaft in den Fällen von Gefahr im Verzug) ein Beurteilungsspielraum zu.[433]

6. [bei Quellen-TKÜ zusätzlich:]

Der [*Adressat der Maßnahme*] bedient sich nach den bisherigen Ermittlungen für seine Kommunikation der Sprachübertragung [*bei Video-Internettelefonie zusätzlich*: Bildübertragung; *bei Instant Messaging via IP zusätzlich:* Textübertragung] in Echtzeit mittels Internetprotokoll (sog. Voice-over-IP). Dabei wird für die Kommunikation eine Software [*soweit vorliegend: Bezeichnung VoIP-Software*] benutzt, mittels derer die Telekommunikationsdaten bei der Übermittlung verschlüsselt werden und deshalb für die Ermittlungsbehörden im Rahmen einer herkömmlichen Telekommunikationsüberwachungsmaßnahme nicht einsehbar und für das Ermittlungsverfahren nicht verwendbar sind, da die Daten nur in der verschlüsselten Form vorlägen. Zur technischen Umsetzung der Überwachungsmaßnahme ist es daher zwingend erforderlich, auf dem für die Kommunikation verwendeten [*Endgerät*] eine spezielle Überwachungssoftware zu installieren, die ein Abgreifen und Ausleiten der noch unverschlüsselten Telekommunikationsdaten vor der Verschlüsselung (ausgehende Daten) bzw. nach der Entschlüsselung (eingehende Daten) an die Ermittlungsbehörden vornimmt und hierdurch die Überwachung und Aufzeichnung der Telekommunikationsdaten ermöglicht. Der mit der heimlichen/verdeckten Installation sowie Deinstallation der Überwachungssoftware verbundene ausschließliche Eingriff in das Fernmeldegeheimnis aus Art. 10 I GG (vgl. BVerfG NJW 2008, 822, 826) ist als typische und verhältnismäßige Begleitmaßnahme zur Umsetzung der Überwachung und Aufzeichnung nach § 100a I StPO im Wege der Annexkompetenz zulässig, weil ein Sachzusammenhang gegeben ist, andere mildere Mittel nicht zur Verfügung stehen und der Maßnahmeadressat nicht unverhältnismäßig belastet wird (vgl. BGH NJW 2001, 1658, 1659 zu § 100c I S. 1 Nr. 1b StPO a. F.; zustimmend auch AG Bayreuth, Beschluss vom 17.09.2009 – Gs 911/09, MMR 2010, 266, 267; LG Hamburg, Beschluss vom 13.09.2010 – 608 Qs 17/10, MMR 2011, 693, 694; LG Landshut, Beschluss vom 20.01.2011 – 4 Qs 346/10, MMR 2011, 690, 691). Mit den in der Entscheidungsformel unter Ziff. II aufgeführten und bei der Konfiguration der Überwachungssoftware zu beachtenden Einschränkungen wird durch rechtliche Vorgaben und technische

433 Demgemäß sei die Nachprüfung der Rechtmäßigkeit der angeordneten Überwachungsmaßnahme sowie etwaiger Verwertungsverbote erlangter Erkenntnisse nur daran auszurichten, ob die Entscheidung vertretbar war, vgl. BGH NJW 1995, 1974 (1975); ebenso BGH NJW 2003, 368 (369); für Einzelheiten zur Frage der Verwertbarkeit bei materiellen Mängeln der Anordnung, siehe 2. Teil A.III.2.

> Vorkehrungen sichergestellt, dass sich die Überwachung ausschließlich auf Daten eines laufenden Telekommunikationsvorganges beschränkt, so dass es nicht zu einem Zugriff auf sonstige auf dem betroffenen [*Endgerät*] gespeicherte Daten und Dateien oder zu einer Überwachung von Datenverarbeitungsvorgängen, die nicht der Telekommunikation dienen (z. B. sog. Screenshots von grafischen Bildschirminhalten, Office- und Textverarbeitungsanwendungen, Grafik- und Multimediaanwendungen, Spiele u. ä.), kommt und keine Maßnahme von der Wirkung einer Online-Durchsuchung vorgenommen wird (vgl. BVerfG NJW 2008, 822, 826). [*Soweit der Quellcode der Überwachungssoftware dem Gericht bei Antragstellung vorgelegt wurde*: Die in vorliegender Sache zum Einsatz kommende Überwachungssoftware (*Bezeichnung, Softwareversion, Zertifizierungsnummer etc.*) stellt auf Grund der gewählten Textbausteine (*Textbausteinnummern u. ä.*) des bei Beantragung vorgelegten und bei Gericht hinterlegten Quellcodes eine entsprechende technische Beschränkung der Software sicher.] Entsprechend den spezifischen Besonderheiten des Einbringens einer Fremdsoftware in ein informationstechnisches System dienen die Vorgaben der Ziff. III der Entscheidungsformel durch Gewährleistung eines transparenten und – in den Grenzen des nach dem technischen Stand Möglichen und Zumutbaren – sicheren Einsatzes des technischen Mittels der Sicherstellung einer insgesamt verhältnismäßigen Handhabe der Ermittlungsmaßnahme in Bezug auf die technische Vorgehensweise und deren verfahrensmäßige Ausgestaltung, der Datenschutzkontrolle sowie der Beweismittelauthentizität und -integrität des erlangten Datenmaterials.
>
> Die Überwachungsmaßnahme ist im vorliegenden Fall verhältnismäßig, da das Abgreifen der Telekommunikationsdaten auf dem zur verschlüsselten Telekommunikation genutzten [*Endgerät*] geeignet, erforderlich und angemessen ist, um den der Anordnung zugrunde liegenden, unter Punkt 1. näher beschriebenen Tatvorwurf aufzuklären und den Tatnachweis gegen den Beschuldigten zu führen. [*ggf. nähere Ausführungen*]

Eine solche Begründung der angeordneten Quellen-TKÜ-Maßnahme nennt hierbei die ermittlungsspezifische Situation und den Anlass für die Durchführung der Maßnahme (Verwendung verschlüsselter Telekommunikationstechniken) sowie das aus diesem Grund bestehende ermittlungstaktische und -technische Erfordernis dieser besondere TKÜ-Maßnahme als entsprechende Notwendigkeit zur Sicherstellung einer strafprozessualen Überwachbarkeit auch von Telekommunikationsformen wie der IP-Kommunikation, bei der TK-Daten verschlüsselt übermittelt werden. Die Begründung enthält hierbei insbesondere auch grundsätzliche Ausführungen zur in Ziff. II der Entscheidungsformel angeordneten Überwachung und Aufzeichnung der IP-Telekommunikation durch Abgreifen „an der Quelle“ mittels Überwachungssoftware und der damit typischerweise (durch Sachzusammenhang)[434] sowie – mangels milderer Mittel zur Realisie-

[434] Für Einzelheiten zur Typizität des Installierens einer Überwachungssoftware, siehe 2. Teil B.III.1.

rung der Überwachung – notwendigerweise[435] verbundenen Installation/Deinstallation einer Überwachungssoftware auf dem Zielsystem als zulässige Begleitmaßnahmen. Zur Begründung der richterlichen Vorgaben in Ziff. III der Entscheidungsformel hinsichtlich Art und Weise der (technischen) Umsetzung der Maßnahme in Bezug auf die Umgangsweise mit dem betroffenen System, der darauf zum Einsatz kommenden Überwachungssoftware sowie die Verpflichtung zur Protokollierung der wesentlichen technischen und organisatorischen Schritte, ist die damit verfolgte Transparenz des Eingriffs und die Sicherstellung einer insgesamt verhältnismäßigen Vorgehensweise bei Durchführung der Ermittlungsmaßnahme auszuführen. Durch derartige Angaben in der Begründung wird in messbarer und kontrollierbarer Weise dafür Sorge getragen, dass sich insbesondere das Ausmaß des (technischen) Zugriffs bei Umsetzung der Quellen-TKÜ auf die gerichtliche Anordnung zurückführen lässt und den (verfassungs-)rechtlichen Anforderungen entspricht.

Sofern dem Gericht der Quellcode[436] (oder der Binärcode[437]) der konkret zum Einsatz kommenden Überwachungssoftware bereits zusammen mit dem Antrag vorgelegt worden sein sollte und es sich – ggf. unter Zuhilfenahme entsprechender Erläuterungsblättern oder durch Heranziehen externen Sachverstandes[438] – bereits bei Anordnungserlass davon überzeugen konnten, dass die Software so konfiguriert ist, dass keine sonstigen Daten außer Daten aus laufenden Telekommunikationsvorgängen erfasst werden, empfiehlt es sich, den im Rahmen der Prüfung der rechtlichen Voraussetzungen einer (Quellen-)TKÜ-Maßnahme stattgefundenen

---

435 Für Einzelheiten zur Erforderlichkeit des Installierens einer Überwachungssoftware, siehe auch 2. Teil B.III.2.b).

436 Auch *Quelltext*, bezeichnet den in einer Programmiersprache geschriebenen Text eines Computerprogramms, bestehend aus einer Abfolge von Befehlen, vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 192.

437 Der in maschinen-lesbare Form übersetzte Quellcode, vgl. http://de.wikipedia.org/wiki/Quelltext (zuletzt aufgerufen 15.06.2012); da dieser in Maschinensprache gehalten ist, bedürfte es einer entsprechend präzisierten Erläuterung; dass auch der Binärcode jedenfalls grds. einer Analyse nicht unzugänglich ist, belegen nicht zuletzt die anhand des Binarcodes erfolgten Untersuchungen einer Überwachungssoftware, welche in einem Ermittlungsverfahren aus dem Jahre 2009 zum Einsatz kam und Gegenstand eines Beschwerdeverfahrens vor dem LG Landshut (MMR 2011, 690) war, durch den *Chaos Computer Club* im Herbst 2011; hierfür stehen auch die unter dem Begriff des *Reverse Engineering* zusammengefassten technischen Möglichkeiten der automatischen Rückgewinnung des Quellcodes aus einem Binärcode bzw. der Rückumwandlung in eine für Menschen lesbare Form (z. B. mittels sog. Decompiler bzw. Disassembler) zur Verfügung.

438 In diese Richtung bereits das Bundesministerium des Innern, Fragenkatalog SPD, S. 15, abrufbar unter http://www.netzpolitik.org/wp-upload/fragen-online durchsuchung-SPD.pdf (zuletzt aufgerufen 15.06.2012).

(für die rechtmäßige Anordnung einer Quellen-TKÜ aber nicht zwingend erforderlichen[439]) „Vergewisserungsvorgang" des Gerichts hinsichtlich der technischen Wirkungsweise des vorgelegten und ggf. bei Gericht hinterlegten Quellcodes ebenfalls in die Begründung mit einzustellen.

In die Ausführungen zur Verhältnismäßigkeit der Maßnahme im konkret vorliegenden Fall ist insbesondere auch mit aufzunehmen, dass keine anderen gleich geeigneten (milderen) Mittel als die Quellen-TKÜ zur Verfügung steht, um die verschlüsselte Telekommunikation zum Zwecke der Erlangung von Beweismitteln einsehbar zu machen, da bspw. eine Maßnahme nach § 100f I StPO[440] für den vorliegenden Fall ggf. kein erfolgversprechendes Mittel darstellt bzw. zu wesentlich schlechteren Erkenntnissen führen würde[441], eine „herkömmliche" TKÜ-Maßnahme unter Abgreifen der Daten auf der Übermittlungsstrecke wegen deren Codierung mit hoher Wahrscheinlichkeit keinen Erfolg verspricht bzw. einen erheblich größeren Zeitaufwand erfordert und die Verwendung eines Schlüssels oder einer Hintertüre (sog. *Backdoor*) nicht vorhanden ist bzw. nicht zur Verfügung steht.[442]

7. Auf Grund der bisherigen Ermittlungen liegen keine tatsächlichen Anhaltspunkte dafür vor, dass durch die vorliegende/-n Anordnung/-en der Überwachung der Telekommunikation allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden (§ 100a IV S. 1 StPO).

   [*nähere Ausführungen*]

Auf Grund des gesetzlich angeordneten Beweiserhebungsverbotes gemäß § 100a IV S. 1 StPO bei der Annahme einer alleinigen Betroffenheit des *Kernbereichs privater Lebensgestaltung* durch die (Quellen-)TKÜ-Maßnahme ist auch der Prüfungs- und Entscheidungsvorgang des Gerichts hinsichtlich der Beurteilung des Vorliegens tatsächlicher Anhaltspunkte hierfür in den Beschlussgründen nachvollziehbar darzulegen.

8. Die Anordnung/-en war/-en gemäß § 33 IV StPO ohne vorherige Anhörung des/der Beschuldigten und der sonstigen Betroffenen zu treffen, um den Zweck der Ermittlungsmaßnahme nicht zu gefährden.

---

439 Da bereits eine entsprechende einschränkende Anordnung des Gerichts hinsichtlich des Zugriffsumfangs der Überwachungsmaßnahme als rechtliche Vorgabe für eine wirksame Begrenzung der Maßnahme genügt, weil die maßnahmeumsetzende Ermittlungsbehörde hieran gebunden ist.

440 Siehe hierzu auch 1. Teil A.II.2.c).

441 Siehe hierzu auch die Ausführungen zur Erforderlichkeit der Quellen-TKÜ unter 3. Teil A.I.1.c).

442 Siehe hierzu auch die Ausführungen zur Erforderlichkeit der Quellen-TKÜ unter 3. Teil A.I.1.c).

Bei heimlichen Ermittlungsmaßnahmen wie der (Quellen-)TKÜ-Maßnahmen nach §§ 100a, 100b StPO handelt es sich um notwendigerweise überraschende Maßnahmen.[443] Da die vorherige Anhörung des Beschuldigten oder sonstiger Personen, gegen die sich die Maßnahme richtet, nach § 33 III StPO den Zweck der Anordnung einer heimlichen Überwachung und Aufzeichnung der von den Betroffenen geführten Internettelefonie gefährden würde, ist von einer *vorherigen Anhörung gemäß § 33 IV StPO abzusehen*. In entsprechender Anwendung der Vorschrift des § 33 IV StPO ist auch die Anhörung sonstiger Betroffener wie der ebenfalls in ihrem Grundrecht auf Fernmeldegeheimnis aus Art. 10 I GG tangierten Gesprächspartner[444] des Maßnahmeadressaten ausgeschlossen, da mangels vorheriger Kenntnis der Gesprächspartner eine Anhörung bereits aus tatsächlichen Gründen nicht realisierbar wäre.[445] Näherer Ausführungen zu den Umständen, die zur Anwendung des § 33 IV StPO geführt haben, bedarf es in Fällen wie der (Quellen-)TKÜ in den Beschlussgründen nicht, da die Gefährdung des Zwecks der Anordnung durch vorherige Anhörung der Beteiligten offensichtlich ist.[446] Die (nachträgliche) Anhörung der Beteiligten erfolgt deshalb in diesen Fällen (erst) im Rechtsmittelzug.[447] Bei Maßnahmen nach §§ 100a, 100b StPO wird den Beteiligten der überwachten Telekommunikation[448] gemäß § 101 VII S. 2, IV S. 1 Nr. 3 StPO nachträglicher Rechtsschutz zur Überprüfung der Rechtmäßigkeit der Maßnahme sowie der Art und Weise ihrer Durchführung gewährt, in dessen Rahmen die Anhörung der Beteiligten nachträglich erfolgt. Eine Entscheidung des Gerichtes im Rahmen der vorliegenden Entscheidung zur Frage der Zurückstellung der Benachrichtigung nach § 101 IV S. 1

---

443 Vgl. Meyer-Goßner – *Meyer-Goßner*, StPO, § 33, Rn. 15.

444 Wobei das Miterfassen auch von Telefongesprächen ggf. unbeteiligter Dritter – wie bspw. der Gesprächspartner der Zielperson oder von Personen, die den Anschluss des Überwachten (mit-)benutzen – im Rahmen von TKÜ-Maßnahmen nach §§ 100a, 100b StPO unvermeidbar ist, vgl. BGH NJW 1980, 67 (68).

445 Vgl. Meyer-Goßner – *Meyer-Goßner*, StPO, § 33, Rn. 17.

446 Vgl. Meyer-Goßner – *Meyer-Goßner*, StPO, § 33, Rn. 16.

447 Vgl. Meyer-Goßner – *Meyer-Goßner*, StPO, § 33, Rn. 18.

448 Regelmäßig der Inhaber des betreffenden Anschlusses und der Beschuldigte, aber nicht ausnahmslos; sind der Inhaber des überwachten Anschlusses oder der Beschuldigte an der überwachten Telekommunikation nicht beteiligt gewesen (bspw. der Inhaber, weil er den Anschluss einer anderen Person überlassen hat oder der Beschuldigte, weil nur eine Telekommunikation des Nachrichtenmittlers mit einem Dritten überwacht wurde), so besteht eine Benachrichtigungspflicht diesen gegenüber nicht, vgl. BT-Drs. 16/5846, S. 58; des Weiteren Beteiligte sind alle Anrufer und Angerufenen des überwachten Anschlusses, in deren Rechte aus Art. 10 I GG durch die Maßnahme eingegriffen wurde, auch wenn das jeweilige Gespräch nicht entscheidungserheblich gewesen sein sollte, vgl. BeckOK – *Hegmann*, StPO, Ed. 13, § 101, Rn. 14.

Nr. 3, V S. 1 StPO[449] erfolgt nicht, da die Entscheidung darüber, ob und wie lange gemäß § 101 V S. 1 StPO die Benachrichtigung des Betroffenen nach § 101 IV S. 1 Nr. 3 StPO vorläufig unterbleibt, der Staatsanwaltschaft als hierfür zuständige Strafverfolgungsbehörde obliegt.[450]

Ort, Datum

[*Unterschrift*]

Richter/-in am Amtsgericht

II. Zusammenfassung

Die dogmatische Auseinandersetzung im Rahmen von Modell 1 zur Frage der Zulässigkeit der Quellen-TKÜ de lege lata zeigt auf, dass die von einem wesentlichen Teil in Rechtspraxis und der Kommentarliteratur befürwortete Lösung auf Grundlage der §§ 100a, 100b StPO einer (verfassungs-)rechtlichen Prüfung standhält und sich mit guten Gründen vertreten lässt. Eine solche moderne Form der Telekommunikationsüberwachung ist unter den entwicklungsoffenen Tatbestand des § 100a I StPO subsumierbar, hält sich hierbei noch im Rahmen des Wortsinns der Tatbestandsbegrifflichkeiten als Grenze der Auslegung und ist unter Heranziehung entsprechender Auslegungsmethodik für Normadressaten in Bezug auf Anlass, Zweck und Grenzen des Eingriffs hinreichend bestimmt. Auch wahren die §§ 100a, 100b StPO mit der dort verankerten Eingriffsschwelle angesichts des hohen Gewichtes des Strafverfolgungsinteresses zur Aufklärung schwerer Straftaten, für die ein von bestimmten Tatsachen begründeter Verdacht besteht, den Grundsatz der Verhältnismäßigkeit für ein Abgreifen der Telekommunikation „an der Quelle“ mittels einer hierauf beschränkten Überwachungssoftware und stellen der Ermittlungsmaßnahme ein sachgerechtes Verfahren insbesondere auch nach erfolgter Datenerhebung zur Seite. Durch entspre-

---

449 Soweit eine Benachrichtigung nach § 101 IV S. 1 StPO erforderlich ist und kein Fall des ausnahmsweisen Absehens nach § 101 IV S. 3 bis 5 StPO vorliegt, erfolgt gemäß § 101 V S. 1 StPO die Benachrichtigung erst dann, wenn die Inkenntnissetzung der Beteiligten über Art und Zeitraum der Durchführung der angeordneten Überwachungsmaßnahme v. a. den Untersuchungszweck nicht (mehr) gefährdet. Dies wird in der Praxis bei der Anordnung und Durchführung einer TKÜ-Maßnahme nach §§ 100a, 100b StPO jedenfalls solange nicht der Fall sein, wie durch die heimliche Maßnahme versucht wird, (weitere) Beweismittel zu erlangen und die strafprozessualen Ermittlungen noch andauern, vgl. *Bär*, TK-Überwachung, § 101 StPO, Rn. 28.

450 Vgl. AG Bayreuth, MMR 2010, 266 (267); Meyer-Goßner – *Cierniak*, StPO, § 101, Rn. 5; hierzu auch BGH NJW 1990, 584 (585); zur Verfassungsmäßigkeit der Regelung des § 101 V S. 1 StPO, siehe BVerfG, Beschl. v. 12.10.2011, Az.: 2 BvR 236/08, 2 BvR 237/08, 2 BvR 422/08, Abs.-Nr. 234.

chend präzise gefasste Beschlüsse auf Rechtsanwendungsebene lässt sich der Zugriff mittels Überwachungssoftware für den konkreten Einzelfall entsprechend auf das rechtlich zulässige Maß beschränken und durch Vorgaben hinsichtlich der (technischen) Durchführung der Maßnahme zugunsten der Revisionsfestigkeit der Vorgehensweise und der Beweissicherheit erlangter Erkenntnisse absichern. Gleichwohl ergeben sich auch berechtigte Anknüpfungspunkt für eine entsprechende Klarstellung der Quellen-TKÜ im Gesetz.

B. Gesetzliche Klarstellung der Quellen-TKÜ de lege ferenda

I. Bedürfnis nach einer gesetzlichen Klarstellung

Wie bereits im Rahmen der obigen Ausführungen zu Modell 1 dargelegt, wird seitens des Verfasser der von einem wesentlichen Teil der Stimmen aus der Rechtspraxis und Kommentarliteratur verfolgten Linie[451] – die insbesondere mit den jüngeren Tendenzen in der Rspr.[452] erneuten Aufwind erhalten hat – jedenfalls im Grundsatz beigepflichtet, wonach die Regelungen der *§§ 100a, 100b StPO* über die Überwachung und Aufzeichnung von Telekommunikation in Verbindung mit entsprechend konkret und präzise ausgestalteten Beschlüssen[453] *grds. eine ausreichende Rechtsgrundlage* für die strafprozessuale Anordnung von Quellen-TKÜ-Maßnahmen darstellen.

Legt man diese Rechtsauffassung zugrunde, so bedarf es für die Zulässigkeit der Anordnung und Durchführung von Maßnahmen der Quellen-TKÜ de lege lata ein Tätigwerden des Gesetzgebers nicht zwingend.

Dennoch gibt es auch Ansatzpunkte, die Anlass zur Empfehlung einer gesetzliche Klarstellung geben, handelt es sich doch bei der Quellen-TKÜ

---

451 So Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 7a; BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 107c; KK – *Nack*, StPO, § 100a, Rn. 27, für die Übergangszeit bis zu einer gesetzlichen Regelung; *Bär*, TK-Überwachung, § 100a StPO, Rn. 32 f.; AG Bayreuth, MMR 2010, 266; LG Hamburg, MMR 2011, 693; insoweit auch LG Landshut, MMR 2011, 690.

452 Nunmehr auch LG Hamburg, Beschluss vom 13.09.2010, Az. 608 Qs 17/10 (MMR 2011, 693) unter Abkehr von der bisher in den „Hamburger Entscheidungen" vertretenen Linie (anders noch LG Hamburg, MMR 2008, 423 sowie AG Hamburg, CR 2010, 249); ebenso AG Bayreuth, MMR 2010, 266; jüngst insoweit auch LG Landshut, MMR 2011, 690.

453 Für Einzelheiten zur inhaltlichen Ausgestaltung der Anordnung und Begründung einer Quellen-TKÜ und für einen Beschlussvorschlag, siehe 3. Teil A.I.2. sowie Anhang 1.

und dem hierbei stattfindenden strafprozessualen Einsatz einer Überwachungssoftware, welche zur Realisierung der Überwachung verschlüsselter VoIP-Kommunikation „an der Quelle" in ein komplexes informationstechnisches System (i. d. R. Computer) eingebracht wird und dort bei jeder Nutzung des jeweiligen VoIP-Dienstes zum Abgreifen von Daten aus laufenden TK-Vorgängen aktiv wird, um ein neuartiges Ermittlungsinstrument, das auf Grund seiner (technischen) Nähe zur (gegenwärtig strafprozessual unzulässigen) Online-Durchsuchung und den mit einer technischen Infiltration einhergehenden potentiellen Gefahren für das betroffene System von heftigen Lagerkämpfen in Rspr. und Lit. begleitet wird.

Um hieraus resultierenden Unsicherheiten beim strafprozessualen Einsatz eines komplexen technischen Mittels wie einer Überwachungssoftware auf einem informationstechnischen System zum Zwecke der Ermöglichung einer Überwachung und Aufzeichnung verschlüsselter Telekommunikation über informationstechnische Systeme Rechnung zu tragen, empfiehlt es sich – wenngleich unter Berücksichtigung von Modell 1 für die rechtmäßige Anordnung und Durchführung von Quellen-TKÜ-Maßnahmen de lege lata nicht zwingend notwendig –, eine *Klarstellung der Quellen-TKÜ im Gesetz* vorzunehmen.[454] Eine entsprechend ausgestaltete gesetzliche Klarstellung könnte hierbei sowohl für das maßnahmeanordnende Organ als auch für die Ermittlungspersonen, welche die angeordneten Maßnahmen umzusetzen haben, insgesamt zu einem Mehr an *Rechtssicherheit* und *Rechtseinheitlichkeit* führen.[455] Eine gesetzliche Klarstellung wäre aber nicht nur den staatlichen Organen bei der rechtssicheren Handhabe dieses Ermittlungsinstruments dienlich, sondern würde auch beim Bürger als betroffenem Grundrechtsträger ein Mehr an *Rechtsklarheit* und *Transparenz* staatlichen Handelns bei Zugriffen auf informationstechnische Systeme zur Folge haben.

II. Modell 2: Normierung einer eigenständigen Befugnisnorm („§ 100j StPO")

Eine Möglichkeit der gesetzlichen Klarstellung wäre hierbei die Schaffung einer eigenständigen Befugnisnorm für die Ermittlungsmaßnahme der Quellen-TKÜ in der StPO. Als stärkste Form der Konstituierung einer sol-

---

454 In diese Richtung auch Anm. *Bär*, MMR 2011, 691 (693) sowie KK – *Nack*, StPO, § 100a, Rn. 27.

455 In diese Richtung auch der Bayerische Landesbeauftragte für den Datenschutz, *Petri*, der sich für „Rechtsklarheit für Bürger, aber auch für die Ermittlungsbehörden" ausspricht, zitiert nach Welt am Sonntag vom 16.10.2011, „Kontrolle in der Grauzone", S. BY 1.

chen Ermittlungsmaßnahme im Konstrukt strafprozessualer Befugnisnormen wird diese Möglichkeit insbesondere von Vertretern der Auffassung herangezogen, die die Tauglichkeit der §§ 100a, 100b StPO als Rechtsgrundlage verneint und mithin von einer Unzulässigkeit der Quellen-TKÜ auf Grundlage der bestehenden Regelungen der StPO ausgeht.

Integriert man die Quellen-TKÜ als eine neue Befugnisnorm in die StPO, so wäre eine solche als grds. heimliche strafprozessuale Ermittlungsmaßnahme bei den §§ 100a ff. StPO im *Achten Abschnitt des Ersten Buches* der Strafprozessordnung zu verorten. Wie die Nummerierungen der §§ 100a–100i StPO verdeutlichen, handelte es sich bei diesen (modernen) Eingriffsbefugnissen um nachträglich in die StPO eingefügte Normen. Aus Gründen der Übersichtlichkeit wie auch der Beibehaltung der weitgehend etablierten bestehenden Paragraphennummern der einzelnen Ermittlungsmaßnahmen nach erfolgter systematischer Neuordnung der §§ 100a–100i StPO zum 01.01.2008[456], empfiehlt es sich für ein solches Modell, trotz der thematischen Nähe zu den §§ 100a, 100b StPO, die neue Befugnisnorm der Quellen-TKÜ „hinten anzustellen" und nach der Befugnisnorm des § 100i StPO (Maßnahmen bei Mobilfunkendgeräten) als „*§ 100j StPO*" einzufügen.

1. Vorschlag nach Brodowski/Freiling

Von den Vertretern der Auffassung, die eine auf §§ 100a, 100b StPO gestützte Quellen-TKÜ de lege lata ablehnen und de lege ferenda das Bedürfnis nach einer (erstmaligen) Regelung der Quellen-TKÜ in der StPO sehen, werden zahlreiche Anforderungen an die Ausgestaltung einer eigenständigen strafprozessualen Eingriffsbefugnis gestellt.[457]

Ein im Schrifttum entwickeltes Modell für die Ausgestaltung einer solchen eigenständigen Befugnisnorm der Quellen-TKÜ lässt sich dem Vorschlag nach *Brodowski/Freiling*[458] entnehmen:

---

456 Durch Gesetz vom 21.12.2007 (BGBl. I S. 3198).

457 Vgl. bspw. *Brodowski*/*Freiling*, Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, S. 144 f., abrufbar unter http://www.sicherheit-forschung.de/schriftenreihe/sr_v_v/sr_4.pdf (zuletzt aufgerufen 15.06.2012); bereits Anm. *Vogel*/*Brodowski*, StV 2009, 632 (634 f.); *Braun*/*Roggenkamp*, K&R 2011, 681 (685).

458 *Brodowski*/*Freiling*, Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, S. 144 f., abrufbar unter http://www.sicherheit-forschung.de/schriftenreihe/sr_v_v/sr_4.pdf (zuletzt aufgerufen 15.06.2012) unter Anknüpfung an Anm. *Vogel*/*Brodowski*, StV 2009, 632 (634 f.).

§ 100j [Quellen-Telekommunikationsüberwachung]

(1) Auch ohne Wissen der Betroffenen darf die Telekommunikation in der Weise überwacht und aufgezeichnet werden, dass mit technischen Mitteln in vom Betroffenen ausschließlich oder überwiegend genutzte informationstechnische Systeme eingegriffen wird, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in § 100c Absatz 2 bezeichnete besonders schwere Straftat begangen oder in Fällen, in denen der Versuchstrafbar ist, zu begehen versucht hat,
2. die Tat auch im Einzelfall besonders schwer wiegt,
3. auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass durch die Überwachung Äußerungen des Beschuldigten erfasst werden, die für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Mitbeschuldigten von Bedeutung sind,
4. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Mitbeschuldigten auf andere Weise unverhältnismäßig erschwert oder aussichtslos wäre, und
5. durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird.

(2) Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, 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 überwiegend ihren Anschluss benutzt.

(3) §§ 100c Absatz 4 bis 7, 100d und 100e finden entsprechende Anwendung.

(4) Für Maßnahmen nach Absatz 1 dürfen nur vom Bundesamt für Sicherheit in der Informationstechnik im Hinblick auf Absatz 1 Nr. 5 zertifizierte technische Mittel eingesetzt werden.

Untersucht man in Analyse dieses Vorschlages die einzelnen Normbestandteile auf ihren Regelungsinhalt und Regelungszweck hin, so lässt sich Folgendes feststellen[459]:

a) § 100j I StPO-E

Nachdem der Entwurf in Absatz 1 zunächst wie § 100a I StPO mit der Vorgabe beginnt, dass *auch ohne Wissen der Betroffenen die Telekommunikation überwacht und aufgezeichnet werden darf*, nennt der dargestellte § 100j StPO-E in Abgrenzung zu § 100a I StPO ausdrücklich den Einsatz *technischer Mittel,* mittels derer eine Überwachung und Aufzeichnung *in*

[459] Für eine Bewertung des an §§ 100c ff. StPO angeglichenen Vorschlages, siehe 3. Teil B.II.2.

der Weise realisiert werden darf, dass *in informationstechnische Systeme eingegriffen wird*. Als weitergehende Einschränkung sieht der Vorschlag nach Brodowski/Freiling in Absatz 1 hierbei allerdings vor, dass es sich bei den informationstechnischen Systemen nur um solche handeln darf, die *vom Betroffenen ausschließlich oder überwiegend genutzt* werden.

Absatz 1 schafft mit einer solchen Formulierung die eigenständige Rechtsgrundlage für einen heimlichen Eingriff in informationstechnische Systeme mit technischen Mitteln zum Zwecke der Telekommunikationsüberwachung (Quellen-TKÜ). Hierbei legt sich der Vorschlag nicht etwa durch Verwendung des Begriffs „Überwachungssoftware" bereits im Wortlaut auf ein bestimmtes Mittel fest, sondern wählt in Sinne einer entwicklungsoffenen Formulierung diesbezüglich die auslegungsfähige Bezeichnung des *technischen Mittels*. Die Eingrenzung auf solche informationstechnischen Systeme, die *ausschließlich oder überwiegend vom Betroffenen genutzt* werden, soll hierbei dem Umstand Rechnung tragen, dass bei einer Anknüpfung der Maßnahme nur an einem (ggf. auch nur einmaligen) Benutzen des informationstechnischen Mittels durch den Betroffenen, eine „unabsehbare Ausweitung"[460] der Quellen-TKÜ – bspw. auf sämtliche, verschlüsselte VoIP-Telefonie anbietende Telefon- und Internetshops – drohen würde.[461]

Als Voraussetzung für die Quellen-TKÜ nennt Absatz 1 Nr. 1 des Normvorschlags hierbei zunächst – wie § 100a I StPO in dessen Nr. 1 – das notwendige Vorliegen *bestimmter Tatsachen, die den Verdacht einer Täterschaft oder Teilnahme bzw. in den Fällen einer Versuchsstrafbarkeit der Versuchsbegehung begründen*, wobei nach dem Vorschlag von Brodowski/Freiling allerdings im Unterschied zu § 100a I Nr. 1 StPO und in Anlehnung an § 100c I StPO die bloße Vorbereitung einer späteren Anlasstat durch eine andere (Nichtkatalog-)Straftat ausgenommen ist und sich der Verdacht auch nur auf eine *in § 100c II StPO bezeichnete besonders schwere Straftat* beziehen soll. Mit dem an das Vorliegen bestimmter Tatsachen geknüpften konkretisierten Tatverdacht zieht der Vorschlag nach Brodowski/Freiling zunächst hinsichtlich der Eingriffsvoraussetzungen in Absatz 1 Nr. 1 mit den Regelungen des § 100a I Nr. 1 StPO bis auf die bloße Vorbereitungstat gleich. Allerdings soll hierbei „angesichts der Eingriffstiefe"[462] einer Quellen-TKÜ ein Anknüpfen an den Straftatenkatalog des § 100c II StPO (*be-*

460 Anm. *Vogel*/*Brodowski*, StV 2009, 632 (634).

461 So Anm. *Vogel*/*Brodowski*, StV 2009, 632 (634).

462 *Brodowski*/*Freiling*, Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, S. 144, abrufbar unter http://www.sicherheit-forschung.de/schriftenreihe/sr_v_v/sr_4.pdf (zuletzt aufgerufen 15.06.2012) unter Anknüpfung an Anm. *Vogel*/*Brodowski*, StV 2009, 632 (634 f.).

sonders schwere Straftaten) und nicht an den des § 100a II StPO (*schwere Straftaten*) veranlasst sein.[463]

Wie § 100a I Nr. 2 StPO bezüglich eines *Schwerwiegens der Tat im Einzelfall*, verlangt auch der Vorschlag nach Brodowski/Freiling in Absatz 1 Nr. 2 zusätzlich zum Verdacht einer abstrakt vorliegenden besonders schweren Straftat, dass die Straftat nach Absatz 1 Nr. 1, Absatz 2 *auch im Einzelfall besonders schwer wiegt*. Hierüber ist auch für eine eigenständige Befugnisnorm der Quellen-TKÜ unter dem Aspekt der Verhältnismäßigkeit sichergestellt, dass im Rahmen einer Einzelfallprüfung solche Fälle herausfallen, die zwar eine Anlasstat nach § 100c II StPO zum Gegenstand haben, aber im konkreten Einzelfall keine hinreichende *besondere Schwere* aufweisen.

Als im Vergleich zu § 100a I StPO zusätzliche und weitergehende, ebenfalls an die §§ 100c ff. StPO angelehnte Voraussetzung ist in Absatz 1 Nr. 3 die gesetzliche Vorgabe enthalten, wonach *auf Grund tatsächlicher Anhaltspunkte die Annahme bestehen muss, dass durch die Überwachung Äußerungen des Beschuldigten erfasst werden, die für die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes eines Mitbeschuldigten von Bedeutung sind*. Mit dieser an § 100c I Nr. 3 StPO angelehnten Eingriffsvoraussetzung werden in dem Normvorschlag nach Brodowski/Freiling die Vorgaben des BVerfG zur akustischen Wohnraumüberwachung[464] auf die Fälle der Telekommunikationsüberwachung an der Quelle übertragen. Demnach läge dieser Sichtweise die Annahme zugrunde, dass die Angemessenheit der Quellen-TKÜ mit Blick auf deren Eingriffstiefe nur dann gewahrt sei, wenn die Quellen-TKÜ-Maßnahme – i. S. d. Entscheidung des BVerfG zur akustischen Wohnraumüberwachung – von vornherein ausschließlich auf IP-Telefongespräche des Beschuldigten gerichtet ist, weil nur insoweit angenommen werden könnte, dass die Telefongespräche einen hinreichenden Bezug zur verfolgten Straftat aufweisen[465] und damit Anhaltspunkte für die Erfassung bedeutsamer, also insbesondere beweisrelevanter Informationen für die Sachverhaltserforschung oder die Aufenthaltsermittlung gegeben sind[466].

---

463 Zur Frage, ob ein Bedürfnis für eine derartige Angleichung der Quellen-TKÜ-Befugnisnorm an die Regelungen der akustischen Wohnraumüberwachung nach §§ 100c ff. StPO besteht, siehe 3. Teil B.II.2.

464 Vgl. BVerfG NJW 2004, 999 (1013).

465 Vgl. BVerfG NJW 2004, 999 (1013) zur akustischen Wohnraumüberwachung; zur Frage, ob ein Bedürfnis für eine derartige Angleichung der Quellen-TKÜ-Befugnisnorm an die Regelungen der akustischen Wohnraumüberwachung nach §§ 100c ff. StPO besteht, siehe 3. Teil B.II.2.

466 Vgl. *Bär*, TK-Überwachung, § 100c StPO, Rn. 14.

Auch hinsichtlich der in Absatz 1 Nr. 4 enthaltenen qualifizierten Subsidiaritätsklausel, wonach *die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes eines Mitbeschuldigten auf andere Weise unverhältnismäßig erschwert oder aussichtslos sein muss*, sieht der Vorschlag nach Brodowski/Freiling eine an § 100c I Nr. 4 StPO angelehnte, gegenüber § 100a I Nr. 3 StPO nochmals verschärfte Regelung vor, da hiernach nicht nur eine *wesentliche* Erschwernis oder Aussichtslosigkeit, sondern gar eine *unverhältnismäßige* Erschwernis oder Aussichtslosigkeit der Ermittlungsarbeit mit anderen Mitteln vorliegen muss, bevor auf das Mittel der Quellen-TKÜ zurückgegriffen werden darf. Der Normvorschlag legt damit in Anlehnung an § 100c I Nr. 4 StPO eine Subsidiaritätsklausel fest, auf Grund derer die ermittlungstechnischen Notwendigkeiten gegen das Gewicht der Rechtsgutsbeeinträchtigung in besonderer Weise abzuwägen sind[467]. Brodowski/Freiling ordnen der Quellen-TKÜ damit einen Eingriffsgrad zu, der diese Ermittlungsmaßnahme neben der akustischen Wohraumüberwachung als schwersten strafprozessualen Eingriff stehen lässt. Die hierdurch festgelegte Rangfolge der strafprozessualen Ermittlungsmaßnahmen ließe die Quellen-TKÜ damit neben der akustischen Wohnraumüberwachung als ultima ratio hinter anderen Ermittlungsmaßnahmen zurücktreten.[468]

Als spezifische Voraussetzung dieser neuen Befugnisnorm knüpft die Vorgabe des Absatzes 1 Nr. 5, wonach *durch technische Maßnahmen sicherzustellen ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird,* an den Feststellungen des BVerfG[469] hinsichtlich des grundrechtlichen Maßstabs der Quellen-TKÜ an. So stellt diese Formulierung eine Möglichkeit dar, wie die vom BVerfG für eine alleinige Grundrechtsrelevanz des Art. 10 I GG geforderte Beschränkung des Überwachungsumfangs einer Quellen-TKÜ ausschließlich auf Daten aus laufenden Telekommunikationsvorgängen – was durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein muss[470] – in ausdrücklicher Weise im Gesetzestext verankert werden kann und so auch in neueren präventiven Rechtsgrundlagen wie bspw. § 20l II S. 1 Nr. 1 BKAG oder § 15b I Nr. 1 HSOG enthalten ist.

---

467 Vgl. BT-Drs. 13/8650, S. 5 und BVerfG NJW 2004, 999 (1010) zur akustischen Wohnraumüberwachung.

468 Vgl. BVerfG NJW 2004, 999 (1010) zur akustischen Wohnraumüberwachung; ebenso BT-Drs. 15/4533, S. 12 f.; zur Frage, ob ein Bedürfnis für eine derartige Angleichung der Quellen-TKÜ-Befugnisnorm an die Regelungen der akustischen Wohnraumüberwachung nach §§ 100c ff. StPO besteht, siehe 3. Teil B.II.2.

469 Vgl. BVerfG NJW 2008, 822 (826).

470 So BVerfG NJW 2008, 822 (826).

b) § 100j II StPO-E

Die Regelung des Absatzes 2, wonach *sich die Anordnung nur gegen den Beschuldigten oder gegen Personen richten darf, 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 überwiegend ihren Anschluss benutzt* entspricht hierbei weitgehend der Regelung des § 100a III StPO hinsichtlich der zulässigen Adressaten einer Quellen-TKÜ-Maßnahme, nämlich Beschuldigte, aktive/passive Nachrichtenmittler sowie Dritte, deren Anschluss der Beschuldigte benutzt, wobei die weitergehende Einschränkung des *überwiegenden* Benutzens des Anschlusses eines Dritten mit der Formulierung in Absatz 1 des Normvorschlags korreliert.

c) § 100j III StPO-E

Gemäß der Regelung des Absatzes 3 finden – in weiterer Abgrenzung zu §§ 100a, 100b StPO – nach dem Vorschlag von Brodowski/Freiling die Vorschriften des § 100c IV, V StPO zum Kernbereichsschutz und des § 100c VII StPO zur gerichtlichen Entscheidung über die Verwertung in den Fällen des § 100c V, die Vorschriften des § 100c VI StPO hinsichtlich des Schutzes zeugnisverweigerungsberechtigter Personen, des § 100d StPO zu Zuständigkeit und Verfahren sowie des § 100e StPO hinsichtlich der Berichtspflichten auf die Quellen-TKÜ entsprechende Anwendung:

Mit der Verweisung in Absatz 3 auf die Vorschriften des § 100c IV und V StPO unterwirft der Normvorschlag nach Brodowski/Freiling die Quellen-TKÜ in Bezug auf den Schutz des Kernbereichs privater Lebensgestaltung nach § 100j III StPO-E i.V.m. § 100c IV S. 1 StPO entspr. als zusätzliche Eingriffsvoraussetzung einer negativen Prognoseentscheidung, welche vom anordnenden Organ zu treffen ist. Die Anordnung einer Quellen-TKÜ wäre demnach nur zulässig, wenn auf Grund tatsächlicher Anhaltspunkte mit einem Erfassen von kernbereichsrelevanten Äußerungen im Rahmen der überwachten Telefongespräche nicht zu rechnen ist (*negative Kernbereichsprognose*).[471] Hierfür müsste nach der subjektiven Einschätzung des die Maßnahme anordnenden Gerichts eine gewisse Wahrscheinlichkeit dafür bestehen, dass es nicht zu einem Eingriff in den Kernbereich privater Lebensgestaltung kommen wird.[472] Durch die entsprechende Anwendung der Sät-

---

[471] Zur Frage, ob ein Bedürfnis für eine derartige Angleichung der Quellen-TKÜ-Befugnisnorm an die Regelungen der akustischen Wohnraumüberwachung nach §§ 100c ff. StPO besteht, siehe 3. Teil B.II.2.

[472] Vgl. *Löffelmann*, NJW 2005, 2033 (2033) m.w.N.

ze 2 und 3 des § 100c IV StPO würden folglich für die Kernbereichsprognose zusätzlich gesetzliche Vermutungen dahingehend erhoben, dass Telefongespräche in Betriebs- oder Geschäftsräumen (S. 2) oder über begangene Straftaten und Äußerungen, mittels derer Straftaten begangen werden (S. 3) dem Kernbereich privater Lebensgestaltung i. d. R. nicht zuzuordnen sind.

Sofern kein genereller Ausschluss der Überwachung nach § 100j III StPO-E i. V. m. § 100c IV StPO entspr. auf Grund fehlender negativer Kernbereichsprognose vorliegt, müsste das Überwachen und Aufzeichnen von Internettelefonaten im Rahmen von Quellen-TKÜ-Maßnahmen gemäß § 100j III StPO-E i. V.m § 100c V S. 1 StPO entspr. dann unverzüglich unterbrochen werden, soweit sich während einer Quellen-TKÜ Anhaltspunkte dafür ergeben, dass kernbereichrelevante Äußerungen erfasst werden. Sofern Aufzeichnungen über Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, angefertigt worden sein sollten, wären diese nach § 100j III StPO-E i. V. m. § 100c V S. 2 StPO entspr. unverzüglich zu löschen und die Tatsache der Erfassung der Daten und ihrer Löschung nach § 100c V S. 4 StPO entspr. zu dokumentieren. Hinsichtlich solcher Erkenntnisse, die unter Verletzung des Kernbereichs erlangt wurden, normiert § 100j III StPO-E i. V. m. § 100c V S. 3 StPO entspr. darüber hinaus ein umfassendes Beweisverwertungsverbot.[473] Soweit ein Beweisverwertungsverbot hiernach in Betracht kommt, hätte die Staatsanwaltschaft nach § 100j III StPO-E i. V. m. § 100c VII S. 1 StPO entspr. aus Gründen der hinreichenden Gewährleistung des Schutzes kernbereichsrelevanter Kommunikation eine Entscheidung des anordnenden Gerichts über die Verwertbarkeit der erlangten Erkenntnisse herbeizuführen, welche – in Einschränkung der Sachentscheidungsbefugnis für das erkennende Gericht[474] – bei Verneinung der Verwertbarkeit für das weitere Verfahren gemäß S. 2 bindend ist. Ferner gelten nach § 100j III StPO-E auch die Vorschriften des § 100c V S. 5 und S. 6 StPO zur Fortführung der Maßnahme nach Unterbrechung entsprechend.

Mit der über § 100j III StPO-E gesetzlich angeordneten entsprechenden Anwendung des § 100c VI StPO trägt der Normvorschlag des Weiteren den Interessen zeugnisverweigerungsberechtigter Personen dadurch Rechnung, dass er – wie bei der akustischen Wohnraumüberwachung in abgestufter Weise – in den Fällen des § 53 I StPO (Berufsgeheimnisträger) ein absolutes Überwachungs- und Erhebungsverbot vorschreibt (§ 100c VI S. 1 StPO entspr.)[475], während in den Fällen des § 52 StPO (Angehörige) und § 53a

---

473 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100c, Rn. 17 m. w. N.

474 Vgl. *Bär*, TK-Überwachung, § 100c StPO, Rn. 40.

475 Im Unterschied zur allgemeinen Regelung in § 160a StPO, welche in Abs. 1 S. 1 für die Berufsgruppen des § 53 I S. 1 Nr. 1 (Geistliche), Nr. 2 (Verteidiger) und Nr. 4 (Abgeordnete) ein (absolutes) Beweiserhebungsverbot festlegt, während in

StPO (Berufshelfer) nur ein eingeschränktes Beweisverwertungsverbot besteht (§ 100c VI S. 2 StPO entspr.). Über die Verweisung in § 100c VI S. 3 StPO finden ferner die Verstrickungsregelungen des § 160a IV StPO entsprechende Anwendung.[476]

Hinsichtlich Zuständigkeit und Verfahren ordnet § 100j III StPO-E die entsprechende Anwendung der Vorschriften des § 100d StPO an. Demnach dürfte eine Anordnung der Quellen-TKÜ im Ermittlungsverfahren nicht durch den Ermittlungsrichter nach §§ 162 I S. 1, 169 StPO am Sitz der jeweiligen Staatsanwaltschaft, wie dies gemäß § 100b I S. 1 StPO für TKÜ-Maßnahmen nach § 100a I StPO der Fall ist, getroffen werden, sondern nur durch die in § 74a IV GVG genannte, allein hierfür einzurichtende Kammer bei demjenigen Landgericht, in dessen Bezirk das jeweilige OLG seinen Sitz hat, für den gesamten OLG-Bezirk (§ 100d I S. 1 StPO, § 74a IV GVG). Eine Eilanordnungskompetenz für die Quellen-TKÜ bei Gefahr im Verzug bestünde entspr. § 100d I S. 2 StPO nur für den Vorsitzenden der Kammer, nicht mehr jedoch wie bei § 100b I S. 2 StPO für die Staatsanwaltschaft.[477] Gegen die richterliche Anordnung wäre als Rechtsmittel – neben[478] dem befristeten Rechtsbehelf nach § 101 VII S. 2–4 StPO für die in §101 IV S. 1 Nr. 4 StPO genannten Personen[479] und des Rechtsschutzes nach § 98 II S. 2 analog – dann insbesondere die Möglichkeit der Beschwerde gemäß § 304 StPO zu einem nicht mit der Hauptsache befassten Senat des OLG, in dessen Bezirk die jeweilige Landesregierung ihren Sitz hat, nach § 120 IV, I GVG gegeben.[480]

Abs. 2 S. 1 für die Berufsgruppen der Nr. 3-3b (Beratungs- und Heilberufe) und Nr. 5 (Medien)„nur“ ein relatives Beweiserhebungsverbot vorgesehen ist, vgl. auch Meyer-Goßner – *Cierniak*, StPO, § 160a, Rn. 9.

476 Zur Frage, ob ein Bedürfnis für eine derartige Angleichung der Quellen-TKÜ-Befugnisnorm an die Regelungen der akustischen Wohnraumüberwachung nach §§ 100c ff. StPO besteht, siehe 3. Teil B.II.2.

477 Zur Frage, ob ein Bedürfnis für eine derartige Angleichung der Quellen-TKÜ Befugnisnorm an die Regelungen der akustischen Wohnraumüberwachung nach §§ 100c ff. StPO besteht, siehe 3. Teil B.II.2.

478 Vgl. BT-Drs. 16/5846, S. 62 m. w. N.; a. A. aber BGH NJW 2009, 454 (454), wonach es sich bei § 101 VII S. 2 StPO jedenfalls für bereits beendete Maßnahmen um eine die allgemeinen Rechtsbehelfe der Beschwerde sowie des § 98 II S. 2 StPO analog verdrängende abschließende Sonderregelung handele; vgl. zum Meinungsstreit auch Meyer-Goßner – *Cierniak*, StPO, § 101, Rn. 26a m. w. N.

479 Für die nicht in § 101 IV S. 1 Nr. 4 StPO genannten Personen richtet sich der Rechtsschutz hingegen nach den allgemeinen Vorschriften (§ 304 StPO; § 98 II S. 2 StPO analog), vgl. Meyer-Goßner – *Cierniak*, StPO, § 101, Rn. 26a; *Bär*, TK-Überwachung, § 101 StPO, Rn. 35.

480 Vgl. Anm. *Vogel*/*Brodowski*, StV 2009, 632 (635); allgemein zum Rechtsschutz bei Maßnahmen nach § 100a StPO, siehe *Bär*, TK-Überwachung, § 100b

Im Vergleich zu § 100b II S. 2 StPO wären in formeller Hinsicht des Weiteren in die Entscheidungsformel der schriftlichen Anordnung zusätzlich der Tatvorwurf, auf Grund dessen die Quellen-TKÜ angeordnet wird (§ 100d II S. 2 Nr. 2 StPO entspr.) sowie die Art der durch die Quellen-TKÜ zu erhebenden Informationen und deren Bedeutung für das Strafverfahren (§ 100d II S. 2 Nr. 5 StPO) mit aufzunehmen.

Mit der Anlehnung an die gesetzlichen Vorschriften über die akustische Wohnraumüberwachung nach §§ 100c ff. StPO hätte die Anordnung der Quellen-TKÜ nach diesem Normvorschlag aber nicht nur die zusätzliche Angaben nach § 100d II S. 2 Nr. 2 und Nr. 5 StPO zu enthalten. Auf Grund der umfassenden Verweisung des § 100j III StPO-E auf die Vorschriften des § 100d StPO unterläge die Anordnung der Quellen-TKÜ darüber hinaus auch einer qualifizierten Begründungspflicht nach § 100d III StPO entspr., statt lediglich der allgemeinen Pflicht zu angemessener und nachvollziehbarer Begründung nach § 34 StPO genügen zu müssen, wie dies bei § 100b II StPO der Fall ist.

Zudem fänden über die Verweisungsvorschrift des § 100j III StPO-E die Regelungen des § 100d V StPO über die Weiterverwendung der durch die Maßnahme erhobenen personenbezogenen Daten zu anderen Zwecken entsprechende Anwendung, die als leges speciales den allgemeinen Verwendungsvorschriften des § 477 II StPO vorgehen (§ 477 II S. 4 StPO). Für die Weiterverwendung der erlangten verwertbaren personenbezogenen Daten in anderen Strafverfahren[481] stellt § 100j III StPO-E i. V. m. § 100d V Nr. 1 StPO entspr. als Sonderregel zu § 477 II S. 2 StPO durch den Begriff „verwertbar“ klar, dass die für die Weiterverwendung in anderen Strafverfahren zur Disposition stehenden Daten auch im Ausgangsverfahren verwertbar sein müssen. Die Verwendung in anderen Strafverfahren unterliegt damit ebenfalls den strafprozessualen Erhebungs- und Verwertungsverboten aus §§ 100c IV–VI StPO[482]. Nach den Vorgaben des BVerfG zur akustischen Wohnraumüberwachung, welche § 100d V Nr. 1 StPO umsetzt, genügt für die Verwendung der gewonnenen Erkenntnisse in anderen Strafverfahren nicht allein das Vorliegen einer Katalogstraftat. Wie deshalb auch aus der Formulierung „zur Aufklärung einer Straftat, auf Grund derer die Maßnahme nach § 100c StPO angeordnet werden könnte“ deutlich wird, müssen darüber hinaus auch eine konkretisierte Verdachtslage gegeben und die

---

StPO, Rn. 27 f., bei Maßnahmen nach § 100c StPO, *ders*., TK-Überwachung, § 100d StPO, Rn. 22 f.

481 Verwendung der erlangten Daten in Verfahren, denen eine andere prozessuale Taten als die Anlasstat zugrunde liegt, vgl. Meyer-Goßner – *Cierniak*, StPO, § 477, Rn. 5, 5a.

482 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100d, Rn. 6 m. w. N.

Subsidiaritätsklausel des § 100c I Nr. 3 StPO beachtet sein.[483] Zudem gelten mangels Begrenzung auf die Verwendung „zu Beweiszwecken" die gesetzlichen Verwendungseinschränkungen des § 100d V Nr. 1 StPO im Sinne eines umfassenden Verwendungsverbotes auch für die Weiterverwendung der gewonnenen Erkenntnisse als Spurenansätze in anderen Strafverfahren, wobei ein Verstoß gegen ein Verwendungsverbot als Spurenansatz keine Fernwirkung, sprich kein Verbot der daraus gewonnenen Erkenntnisse begründet.[484]

Über die Verweisung in § 100j III StPO-E finden ferner auch die Berichtspflichten nach § 100e StPO auf die Quellen-TKÜ entsprechende Anwendung.

d) § 100j IV StPO-E

Als spezifische Vorgabe für eine im Rahmen der Quellen-TKÜ zum Einsatz kommende spezielle Überwachungssoftware verankern Brodowski/Freiling in ihrem Vorschlag eines „§ 100j StPO-E" zusätzlich als weiteren Absatz 4 in der Befugnisnorm, dass *für Maßnahmen nach Absatz 1 nur vom Bundesamt für Sicherheit in der Informationstechnik im Hinblick auf Absatz 1 Nr. 5 zertifizierte technische Mittel eingesetzt werden dürfen*. Die Aufnahme einer solche Vorschrift trägt damit dem Umstand Rechnung, dass eine Zugriffssoftware je nach Konfiguration und Aufbau prinzipiell *technisch* dazu in der Lage sein kann, nicht nur laufende Telekommunikation zu erfassen, sondern ein informationstechnisches System auch im Übrigen auszuforschen. In Anbetracht der für eine ausschließliche Betroffenheit des Art. 10 I GG erforderlichen Ausgestaltung einer Quellen-TKÜ-Überwachungssoftware stellt die Verpflichtung zur Verwendung einer durch das BSI zertifizierten Software (vgl. § 9 BSIG, § 2 VII BSIG)[485], welche auf das

---

483 Vgl. BT-Drs. 15/4533, S. 18.

484 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100d, Rn. 7 m. w. N.; *Löffelmann*, ZIS 2006, 87 (96).

485 Gemäß § 3 Nr. 13 lit. a BSIG zählt zu den Aufgaben des BSI insbesondere auch die Unterstützung der Polizeien und Strafverfolgungsbehörden bei der Wahrnehmung ihrer gesetzlichen Aufgaben. Anders hingegen *Braun*/*Roggenkamp*, K&R 2011, 681 (685), denen eine Ansiedlung der Überprüfung bei den Datenschutzbeauftragten des Bundes und der Länder sachgerechter erscheint, da es sich bei dem BSI um eine dem Bundesministerium des Innern nachgeordnete Behörde handelt, weshalb fraglich sei, ob diese „die für die Akzeptanz in der öffentlichen Wahrnehmung notwendige Unabhängigkeit besitzt" (685). Ob ein solcher „Misstrauensvorschuss" dem BSI indes gerecht wird, darf bezweifelt werden; das BSI ist zentrale sachverständige Stelle für sämtliche Belange der Sicherheit in der Informationstechnik und gerade als staatliche Behörde in besonderer Weise an Recht und Gesetz gebunden; auch nach dem Selbstverständnis der Behörde wird „die Objektivität und Einheitlichkeit der Prüfungen

Einhalten der Anforderungen des § 100j I Nr. 5 StPO-E im Vorfeld durch unabhängige Prüfstellen[486] geprüft und bewertet wurde, eine Möglichkeit dar, durch Begleitbestimmungen abzusichern, dass keine über die abzugreifende Telekommunikation hinausgehenden Daten abgegriffen werden[487], und hierüber den Anforderungen des BVerfG[488] Rechnung zu tragen.[489]

Die unter Punkt C des 2. Teils der vorliegenden Arbeit herausgearbeiteten Kernfragen einer Quellen-TKÜ werden unter Gesamtbetrachtung des Normvorschlags eines „§ 100j StPO-E" im Rahmen von Modell 2 damit wie folgt berücksichtigt:

Für die Frage der *Tatbestandsbestimmtheit und Normenklarheit* einer solchen Ermittlungsmaßnahme stellen die Eingriffsbeschreibung in Absatz 1 sowie die Beschränkung des Eingriffsumfangs in Absatz 1 Nr. 5 des Normvorschlags nach Brodowski/Freiling gesetzlich fest, dass auf laufende Telekommunikation auch durch Eingriff in informationstechnische Systeme mit Hilfe technischer Mittel zugegriffen werden darf, die technisch hierauf begrenzt sein müssen. Diese gesetzliche Vorgabe zur Begrenzung des Eingriffsumfangs dient hierbei – insbesondere im Zusammenspiel mit den Vorgaben des Absatzes 4 zur Heranziehung nur durch das BSI zertifizierter technischer Mittel – der Sicherstellung der Einhaltung der durch das BVerfG aufgestellten Anforderungen für eine alleinige Grundrechtsbetroffenheit des Fernmeldegeheimnisses aus Art. 10 I GG. Auf Grund der von dem Vorschlag angenommenen Nähe der Quellen-TKÜ zu Maßnahmen der akustischen Wohnraumüberwachung in Bezug auf deren Eingriffsintensität sind die Eingriffsvoraussetzungen des § 100j StPO-E an der im Vergleich zu den §§ 100a, 100b StPO erhöhten Schwelle der §§ 100c ff. StPO ausgerichtet

---

sowie die Unparteilichkeit […] durch das BSI gewährleistet. Als unparteiliche Stelle ist diese Maxime, auch bei Interessenskonflikten, Leitlinie für unsere tägliche Arbeit […]" (https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/zertifizierungundanerkennung_node.html, zuletzt aufgerufen 15.06.2012).

486 Vgl. https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/zertifizierungundanerkennung_node.html (zuletzt aufgerufen 15.06.2012).

487 Vgl. *Brodowski*/*Freiling*, Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, S. 144, abrufbar unter http://www.sicherheit-forschung.de/schriftenreihe/sr_v_v/sr_4.pdf (zuletzt aufgerufen 15.06.2012).

488 Vgl. BVerfG NJW 2008, 822 (826).

489 In diese Richtung auch der Vorsitzende der Deutschen Polizeigewerkschaft, *Wendt*, in der Neuen Osnabrücker Zeitung vom 11.10.2011, abrufbar unter http://www.noz.de/deutschland-und-welt/gut-zu-wissen/computer/57839915/bayern-wegen-trojaner-einsatzes-unter-druck (zuletzt aufgerufen 15.06.2012); ebenso der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, *Schaar*, sowie die Bundesministerin der Justiz, *Leutheusser-Schnarrenberger*, nach *Höll*, „‚Gefährliche Grauzone'", Süddeutsche Zeitung vom 13.10.2011, S. 6; in diese Richtung bereits Anm. *Vogel*/*Brodowski*, StV 2009, 632 (634).

und die *Verhältnismäßigkeit* des Eingriffs durch Anknüpfen an einer besonders schweren Straftat nach § 100c II StPO gewahrt. Die Regelung des Absatzes 4 trägt schließlich auch der erleichterten *Nachweisbarkeit* einer rechtmäßigen Funktions- und Verwendungsweise der Überwachungssoftware durch Vorweisbarkeit einer staatlichen Zertifizierung Rechnung.

2. Bedürfnis nach einer Angleichung an §§ 100c ff. StPO?

Es stellt sich die Frage, ob eine gesetzliche Normierung der Quellen-TKÜ – wie dies von obigem Normvorschlag nach Brodowski/Freiling angenommen wird – an der Eingriffsschwelle der akustischen Wohnraumüberwachung auszurichten und damit an die Eingriffsvoraussetzungen der §§ 100c ff. StPO anzugleichen wäre.

Unter Bewertung des von Brodowski/Freiling vorgeschlagenen Regelungsmodells ist zunächst die festgelegte Beschränkung der Überwachung auf vom Betroffenen *ausschließlich oder überwiegend genutzte* informationstechnische Systeme voranzustellen. Gegen eine solche Eingrenzung der überwachbaren Systeme spricht bereits, dass hierdurch nicht nur zwei neue, der StPO bislang unbekannte auslegungsbedürftige Begrifflichkeiten, nämlich die der *ausschließlichen Nutzung* sowie der *überwiegenden Nutzung* eingefügt werden, die bei jeder Anordnung und Durchführung einer Quellen-TKÜ eine Ermessenentscheidung dahingehend erforderlich machen, ob eine ausschließliche oder überwiegende Nutzung bereits bzw. noch gegeben ist – wobei schon eine taugliche Definition, ab bzw. bis zu welchem (Fremd-) Nutzungsgrad gerade eine *überwiegende* Nutzung des Betroffenen überhaupt anzunehmen ist, schwer fallen dürfte – und Ermittlungstätigkeit damit letztlich von der im Einzelfall mitunter äußerst schwierigen Feststellung abhängig gemacht wird, welchen Grad die Nutzung des informationstechnischen Systems durch den Betroffenen im relevanten Überwachungszeitraum gerade erreicht hat. Darüber hinaus würde eine solche Einschränkung letztlich zu einem – auch unter dem Aspekt des effektiven Schutzes der Rechte unbeteiligter Dritter – kaum zu rechtfertigenden rechtsfreien Raum für verschlüsselte Internettelefonie, welche über nicht ausschließlich oder nicht überwiegend vom Betroffenen genutzte Systeme realisiert wird, führen und zur Folge haben, dass Straftäter verstärkt über entsprechend von einer Vielzahl von Personen bzw. öffentlich nutzbaren und damit nach dieser Bestimmung nicht überwachbaren VoIP-Einrichtungen, bspw. in Internetcafés, Universitäten etc., aber auch ggf. über Systeme von Verwandten oder Bekannten kommunizieren.[490]

---

[490] Entgegen Anm.*Vogel*/*Brodowski*, StV 2009, 632 (634), welche von einer „unabsehbare[n] Ausweitung“ (634) auf Telefon- und Internetshops mit verschlüssel-

Wie oben im Detail dargestellt, legt der Normvorschlag nach Brodowski/Freiling in § 100j I Nr. 1 und Nr. 2 StPO-E als Anlasstaten den Katalog der *besonders schweren Straftaten* aus § 100c II StPO zugrunde, welche auch *im Einzelfall besonders schwer wiegen* müssen. Für eine derartige Anhebung der Anlasstatenqualität/-schwere besteht jedoch bei einer Maßnahme, die ausschließlich IP-Telekommunikation überwacht und aufzeichnet, keine Veranlassung. Denn die Überwachung und Aufzeichnung derartiger Telekommunikation mit Hilfe der besonderen Ermittlungsmaßnahme der Quellen-TKÜ weist unter Berücksichtigung der oben zu Modell 1 angestellten Untersuchungen keine mit der akustischen Wohnraumüberwachung vergleichbare Eingriffsintensität auf, wie sich dies bspw. für die eingriffsintensivere *Online-Durchsuchung* annehmen lässt. Der strafprozessuale Zugriff auf Daten aus IP-Telekommunikationsvorgängen an der Quelle stellt – wenngleich eine vom (technischen) Grundprinzip ähnliche, in der Konfiguration- und Anwendungsweise aber unterschiedliche Überwachungssoftware zum Einsatz kommt – insgesamt dennoch einen niedrigerer Grundrechtseingriff dar, als die umfassende Ausforschung des Zielsystems ohne Bezug zu laufenden Telekommunikationsvorgängen, welche am neuen IT-Grundrecht aus Art. 2 I i. V. m. Art. 1 I GG zu messen ist. Auch im Vergleich zu der an Art. 13 GG zu messenden *akustischen Wohnraumüberwachung* weist der Eingriff im Rahmen einer Quellen-TKÜ, der sich bei ausschließlicher Erfassung laufender Telekommunikationsvorgänge allein am Maßstab des Art. 10 GG ausrichtet, eine geringere Grundrechtsrelevanz auf. Eine entsprechende Vorgabe zur Beschränkung von Eingriffen nur auf besonders schwere Straftaten wie in Art. 13 III S. 1 GG enthält die verfassungsrechtliche Legitimationsgrundlage in Art. 10 II S. 1 GG für Einschränkungen des Fernmeldegeheimnisses indes nicht.

Bereits die Art der zu erlangenden Erkenntnisse (Inhalte aus Telekommunikationen) unterscheidet sich qualitativ. Diese unterliegen nicht einem gleich hohen Schutzniveau, wie bspw. Gespräche in der Wohnung als Refugium des privaten Lebens. Dem Umstand der geringeren Grundrechtsintensität einer streng auf den Ermittlungszweck begrenzten Quellen-TKÜ

---

ter VoIP-Telefonie sprechen, steht eine derartige Beschränkung der zugreifbaren Systeme unter dem Kriterium der ausschließlichen oder überwiegenden Nutzung im Widerspruch zu dem eindeutigen Willen des Gesetzgebers, der in § 100a III Alt. 3 StPO trotz des Miterfassens (ggf. auch einer Vielzahl) unverdächtiger Nutzer das grundsätzliche Bedürfnis für eine Überwachbarkeit auch von Anschlüssen Dritter in den Fällen der Fremdanschlussbenutzung durch den Betroffenen gesetzlich normiert hat. Auch für Maßnahmen der akustischen Wohnraumüberwachung ist ein entsprechender Gedanke des Gesetzgebers in den Bestimmungen des § 100c III S. 2 StPO enthalten, der eine Überwachung von Wohnungen anderer Personen, also von Räumlichkeiten, die nicht ausschließlich oder überwiegend von dem Beschuldigten genutzt werden, unter den dort genannten Voraussetzungen gestattet.

schließt sich damit zudem eine im Vergleich zu Maßnahmen nach §§ 100c ff. StPO abgesenkte Schutzbedürftigkeit des Betroffenen an, da der Nutzer von (gerade auch Internet-)Telekommunikationsformen bewusst Kommunikationsinhalte aus seiner Sphäre in ein fremdbeherrschtes Datennetz entäußern, welches sich seinem Zugriff entzieht und von Dritten betrieben wird. Der Eingriff mittels Quellen-TKÜ weist darüber hinaus keine Eingriffsqualität von dem Gewicht auf, dass ein Beschränken der Maßnahme nur auf solche Straftatbestände, die mit einer Höchststrafe von mehr als fünf Jahren Freiheitsstrafe bewehrt sind und besonders schweres Tatunrecht in sich tragen[491], veranlasst wäre, wie es bei akustischen Wohnraumüberwachungen der Fall ist. Eine Beschränkung nur auf Straftaten aus dem Bereich der organisierten Kriminalität, des Terrorismus sowie anderer Formen besonders schwerer Kriminalität[492] erscheint in Bezug auf die anhand der Eingriffintensität unterhalb der akustischen Wohnraumüberwachung anzusiedelnden Quellen-TKÜ wenig sachgerecht. Hier empfiehlt sich – insbesondere auf Grund desselben Grundrechtsmaßstabs (Art. 10 GG) und derselben Erkenntnismöglichkeiten (Informationen aus Telekommunikationsvorgängen) wie bei herkömmlichen TKÜ-Maßnahmen – vielmehr eine Ausrichtung der für eine Quellen-TKÜ erforderlichen Anlasstat an der Begrifflichkeit der *schweren Straftat* mit einer Höchststrafe von i. d. R. mindestens fünf Jahren[493], auf jeden Fall über einem Jahr Freiheitsstrafe[494]. Unter Abwägung der tangierten Grundrechte und der Art der zu erlangenden Erkenntnisse stellt sich das Anknüpfen der Maßnahme der Quellen-TKÜ in Bezug auf das Gewicht der Anlasstat an das Vorliegen einer *schweren Straftat* für den damit verbundenen Eingriff in Art. 10 I GG als sachgerecht dar. Durch das Anknüpfen auch der Quellen-TKÜ an den Anlasstatenkatalog des § 100a II StPO gelingt es für die Überwachbarkeit verschlüsselter VoIP-Kommunikation in angemessener Weise, den Strafverfolgungsbehörden auch für diese moderne Telekommunikationsform die notwendigen Mittel bei der Verfolgung schwe-

---

491 Vgl. insoweit BT-Drs. 16/5846, S. 39; *Bär*, TK-Überwachung, § 100c StPO, Rn. 11.

492 Vgl. BT-Drs. 15/4533, S. 10; BVerfG NJW 2004, 999 (1002).

493 In einer kürzlich ergangenen Entscheidung (BVerfG, Beschl. v. 12.10.2011, Az.: 2 BvR 236/08, 2 BvR 237/08, 2 BvR 422/08) hat das BVerfG unter Zurückweisung mehrerer Verfassungsbeschwerden bezüglich der zum 01.01.2008 in Kraft getretenen Neuregelung der strafprozessualen Telekommunikationsüberwachung (BGBl. I S. 3198) nunmehr höchstrichterlich festgestellt, dass die durch den Gesetzgeber vorgenommene Erweiterung des Straftatenkatalogs in § 100a II StPO in der gegenwärtig gültigen Fassung den Verhältnismäßigkeitsgrundsatz wahre (Abs.-Nr. 203), da „die gesetzgeberische Einstufung der in § 100a Abs. 2 StPO aufgenommenen Straftatbestände als ‚schwer' bei einer Gesamtschau vertretbar" (Abs.-Nr. 205) sei.

494 Vgl. BT-Drs. 16/5846, S. 40; Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 10 m. w. N.

rer und schwer ermittelbarer Kriminalität an die Hand zu geben, zugleich aber die Überwachung und Aufzeichnung von Telekommunikation – was regelmäßig einen erheblichen Eingriff in die Rechte der Betroffenen darstellt – für solche Fälle auszuschließen[495], „in denen die Bedeutung des zu schützenden Rechtsguts und das öffentliche Interesse an der Strafverfolgung nicht so gewichtig erscheinen, dass der von der Maßnahme zu erwartende Nutzen die mit ihr verbundenen Beeinträchtigungen überwiegen würde.“[496] Hierdurch kann dem Grundsatz Rechnung getragen werden, „dass auch im Strafverfahren die Wahrheit nicht ‚um jeden Preis‘ erforscht werden darf“[497].

Auch einer gesetzlichen Vorgabe in der Weise des § 100j I Nr. 3 StPO-E hinsichtlich der Annahme des Erfassens beweisrelevanter Informationen auf Grund tatsächlicher Anhaltspunkte bedarf es unter Verhältnismäßigkeitsaspekten bei einer Maßnahme der Quellen-TKÜ nicht. Mit dieser zusätzlichen, an die Regelung des § 100c I Nr. 3 StPO angelehnt Eingriffsvoraussetzung übertragen Brodowski/Freiling die Vorgaben des BVerfG zur akustischen Wohnraumüberwachung[498] auf die Fälle der an der Quelle realisierten Telekommunikationsüberwachung. Unter entsprechender Anwendung der Argumentation des BVerfG auf die Ermittlungsmaßnahme der Quellen-TKÜ müsste dieser Sichtweise demnach konsequenterweise die Annahme zugrunde liegen, dass die Angemessenheit der Quellen-TKÜ mit Blick auf deren Eingriffstiefe nur dann gewahrt sein kann, wenn die Quellen-TKÜ-Maßnahme von vornherein ausschließlich auf VoIP-Telefongespräche des Beschuldigten gerichtet ist, weil nur insoweit angenommen werden könnte, dass die VoIP-Telefongespräche einen hinreichenden Bezug zur verfolgten Straftat aufweisen.[499] Eine solche von der akustischen Wohnraumüberwachung auf die Ermittlungsmaßnahme der Quellen-TKÜ übertragene Vorgabe würde dann aber zugleich auch bedeuten, dass die Quellen-TKÜ nur bei einer aktuellen, wenn auch ggf. nur vermuteten Teilnahme des Beschuldigten an dem zu überwachenden VoIP-Telefongespräch zulässig wäre.[500] Eine solche Vorgabe stünde bereits im Widerspruch zum erklärten Willen des Gesetzgeber, bei einer Überwachung und Aufzeichnung von Telekommunikation die Anordnung auch bspw. gegen (auf Grund bestimmter Tatsachen angenommene) aktive und passive Nachrichtenmittler als Adressaten des Eingriffs richten zu dürfen (vgl. § 100a III StPO) und damit grds. auch Telekommu-

---

495 Vgl. BT-Drs. 16/5846, S. 40.

496 BT-Drs. 16/5846, S. 40.

497 BT-Drs. 16/5846, S. 40 m. w. N.

498 Vgl. BVerfG NJW 2004, 999 (1013).

499 Vgl. entspr. BVerfG NJW 2004, 999 (1013) zur akustischen Wohnraumüberwachung.

500 Vgl. entspr. BVerfG NJW 2004, 999 (1013) zur akustischen Wohnraumüberwachung; ebenso BT-Drs. 15/4533, S. 12.

nikation Dritter ohne direkte Teilnahme des Beschuldigten überwachbar zu machen, welche ggf. nur mittelbar verwertbare Erkenntnisse gegen den Beschuldigten liefert, aber keine unmittelbaren Äußerungen des Beschuldigten erfasst. Darüber hinaus wird bei Telefonaten naturgemäß nicht nur Beweisrelevantes besprochen, sondern eine Vielzahl, gerade auch alltäglicher Dinge. Mangels vergleichbarer Eingriffstiefe der Quellen-TKÜ mit der akustischen Wohnraumüberwachung (geringere Grundrechtsintensität sowie niedrigere Schutzbedürftigkeit des Betroffenen, der bewusst im Rahmen der Nutzung von Telekommunikationsdiensten Sprache in ein fremdbeherrschtes Datennetz entäußert) ist eine Regelung in Form des § 100j I Nr. 3 StPO-E auch nicht zur Gewährleistung eines insgesamt verhältnismäßigen Eingriffs erforderlich (vgl. oben). Wie die Untersuchungen der vorliegenden Arbeit zu Modell 1 gezeigt haben, ist bereits über die gegenwärtige Rechtslage nach §§ 100a, 100b StPO in Verbindung mit entsprechend ausgestalteten Beschlüssen auch ohne eine solche zusätzliche Eingriffsvoraussetzung eine Überwachung und Aufzeichnung von (VoIP-)Telekommunikation an der Quelle in geeigneter, erforderlicher und insbesondere angemessener Weise mit dem Instrument der Quellen-TKÜ realisierbar.[501] Auch die verfassungsrechtliche Ermächtigungsgrundlage in Art. 10 II GG für Eingriffe in das Fernmeldegeheimnis legt die Normierung einer solchen zusätzlichen Eingriffsvoraussetzung in einfachgesetzlichen Rechtsgrundlagen indes nicht nahe. Denn anders als die Formulierung des Art. 13 III GG, die mit der Anknüpfung an Wohnungen, in denen sich der Beschuldigte vermutlich aufhält, eine Teilnahme des Beschuldigten an den überwachten Gesprächen impliziert, enthält Art. 10 II GG keine entsprechende Vorgabe auf Verfassungsebene.

Mit der Verankerung einer an § 100c I Nr. 4 StPO angelehnten und damit im Vergleich zu § 100a I Nr. 3 StPO verschärften Subsidiaritätsklausel in § 100j I Nr. 4 StPO-E müsste auf Grund der Anknüpfung an der Eingriffsschwelle der akustischen Wohnraumüberwachung einer derart ausgestalteten Quellen-TKÜ-Befugnisnorm ebenfalls der Gedanke zugrunde liegen, dass die Quellen-TKÜ im Vergleich zu anderen Maßnahmen nur ultima ratio, also allerletztes Mittel der Strafverfolgung sein könne und demgemäß als – neben der akustischen Wohnraumüberwachung – schwerstes Eingriffsmittel hinter allen anderen strafprozessualen heimlichen Ermittlungsmaßnahmen zurückzutreten habe.[502] Eine solche implizierte Rangfolge des strafprozessualen Maßnahmeninstrumentariums wäre mit Blick auf die Eingriffs-

[501] Für Einzelheiten zur Wahrung des Verhältnismäßigkeitsgrundsatzes, siehe 3. Teil A.I.1.c).

[502] Vgl. entspr. BT-Drs. 13/8650, S. 5 sowie BT-Drs. 15/4533, S. 13, jeweils zur akustischen Wohnraumüberwachung.

qualität der Quellen-TKÜ aber unverhältnismäßig. Denn die Quellen-TKÜ, deren Überwachungsgegenstand softwarebasierte VoIP-Telekommunikation ist, stellt angesichts der akustischen Wohnraumüberwachung nach §§ 100c ff. StPO und der – strafprozessual bislang noch nicht normierten – Online-Durchsuchung gerade nicht das schwerste strafprozessuale Eingriffsmittel dar. Denn die Quellen-TKÜ weist im Vergleich zur akustischen Wohnraumüberwachung, welche in die Unverletzlichkeit der Wohnung als das „letztes Refugium“[503] des Einzelnen zur Wahrung seiner Menschenwürde eingreift, sowie zur Online-Durchsuchung, welche auf die Durchsicht bzw. Überwachung des gesamten Systems ausgerichtet ist und damit in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme eingreift, eine deutlich abgesenkte Eingriffsintensität auf. Die Verhängung der strengsten Subsidiaritätsklausel (*unverhältnismäßig erschwert oder aussichtslos*) in gleicher Weise auch für die Quellen-TKÜ „ohne Luft nach oben“ würde jedoch diesen unterschiedlichen Eingriffsqualitäten nicht gerecht werden. Aber auch für die praktische Folge einer solchen verschärften Subsidiaritätsklausel, nämlich dass Erschwernisse in der Ermittlungsarbeit bis zum Grad der Unverhältnismäßigkeit hingenommen werden müssten, ehe auf das Mittel der Quellen-TKÜ zurückgegriffen werden dürfte[504], besteht mit Blick auf die Schaffung eines angemessenen Ausgleichs zwischen dem Strafverfolgungsinteresse und dem Bedürfnis nach einer Überwachbarkeit verschlüsselt übermittelter VoIP-Kommunikation einerseits sowie dem tangierten Grundrecht des Fernmeldegeheimnisses und der Schutzbedürftigkeit des Betroffenen andererseits, keine durchgreifende sachliche Rechtfertigung. Da der Eingriff im Rahmen einer Quellen-TKÜ insgesamt unter der Eingriffsqualität einer akustischen Wohraumüberwachung oder einer Online-Durchsuchung zurückbleibt, besteht kein vergleichbares Erfordernis – wie es der Gesetzgeber für die Ermittlungsmaßnahme der akustischen Wohnraumüberwachung gesehen hat –, die ermittlungstaktischen Notwendigkeiten der Maßnahme im Rahmen einer strengen Subsidiaritätsklausel gegen das Gewicht der Rechtsgutsbeeinträchtigung in besonderer Weise abzuwägen[505].

Auch einer Angleichung an die Vorgaben der §§ 100c IV–VII, 100d und 100e StPO, auf deren entsprechende Anwendung der Normvorschlag nach Brodowski/Freiling in § 100j III StPO-E verweist, bedarf es im Wesentlichen nicht:

---

503 BVerfG NJW 2004, 999 (1002).

504 Vgl. entspr. BVerfG NJW 2004, 999 (1010) zur akustischen Wohnraumüberwachung.

505 Vgl. entspr. BVerfG NJW 2004, 999 (1010) zur akustischen Wohnraumüberwachung.

Hinsichtlich des Schutzes des Kernbereichs privater Lebensgestaltung würde eine entsprechende Anwendung des § 100c IV S. 1 StPO der Anordnung einer Quellen-TKÜ als zusätzliche Eingriffsvoraussetzung eine zwingend erforderliche negative Kernbereichsprognose auferlegen. Dies würde bedeuten, dass eine Quellen-TKÜ-Maßnahme von vornherein nur dann angeordnet werden dürfte, soweit auf Grund tatsächlicher Anhaltspunkte ein Erfassen von kerbereichsrelevanten Äußerungen nicht anzunehmen ist. Das Abhängigmachen der Zulässigkeit einer jeden Quellen-TKÜ-Maßnahme von einer solchen negativen Kernbereichsprognoseentscheidung in gleicher Weise wie für Maßnahmen der akustischen Wohnraumüberwachung würde mit Blick auf die abgestufte Eingriffsqualität beider Maßnahmen sowie die unterschiedliche Schutzbedürftigkeit der Betroffenen jedoch dem Verhältnismäßigkeitsgrundsatz nicht gerecht werden. Denn Maßnahmen der akustischen Wohnraumüberwachung greifen in das Grundrecht auf Unverletzlichkeit der Wohnung aus Art. 13 I GG ein, welches in engem Bezug zum Schutz der Menschenwürde (Art. 1 I GG) steht und diesen in spezifischer Weise konkretisiert. Die Unverletzlichkeit der Wohnung steht hierbei „im nahen Zusammenhang mit dem verfassungsrechtlichen Gebot unbedingter Achtung einer Sphäre des Bürger für eine ausschließliche private – eine ‚höchstpersönliche' – Entfaltung"[506]. Das Recht, in Ruhe gelassen zu werden, soll nach ständiger Rspr. des BVerfG dem Einzelnen gerade in seiner Wohnung gesichert sein.[507] Zur Entfaltung der Persönlichkeit im Kernbereich der privaten Lebensgestaltung bedarf es eines dafür geeignet Freiraums, sprich eines „räumliche[n] Substrat[s]"[508], in dem der Einzelne „für sich sein und sich nach selbst gesetzten Maßstäben frei entfalten [kann]"[509]. Als ein solches räumliches Substrat fungieren regelmäßig die privaten Wohnräume, da diese für andere verschlossen werden können. Die Privatwohnung stellt damit „als ‚letztes Refugium' ein Mittel zur Wahrung der Menschenwürde"[510] dar, was „zwar nicht einen absoluten Schutz der Räume der Privatwohnung [verlangt], wohl aber absoluten Schutz des Verhaltens in diesen Räumen"[511], soweit es sich hierbei um individuelle Entfaltung im Kernbereich der privaten Lebensgestaltung handelt.[512] Dieser absolute Schutz des Verhaltens in Wohnräumen durch Art. 13 I GG lässt sich aber nicht 1:1 auf den Schutz der individuellen Kommunikation durch das Fernmeldegeheimnis aus Art. 10 I GG übertragen. Das in Art. 10 I GG verbürg-

506 BVerfG NJW 2004, 999 (1002).
507 Vgl. BVerfG NJW 2004, 999 (1002) m. w. N.
508 BVerfG NJW 2004, 999 (1002).
509 BVerfG NJW 2004, 999 (1002).
510 BVerfG NJW 2004, 999 (1002).
511 BVerfG NJW 2004, 999 (1002).
512 So BVerfG NJW 2004, 999 (1002).

te Fernmeldegeheimnis gewährleistet zwar „die freie Entfaltung der Persönlichkeit durch einen privaten, vor der Öffentlichkeit verborgenen Austausch von Kommunikation und schützt damit zugleich die Würde des Menschen“[513]. Auch kann nicht bestritten werden, dass ebenso am Telefon höchstpersönliche Dinge besprochen werden können, deren Erfassen im Rahmen einer TKÜ-Maßnahme in die nach Art. 1 I GG garantierte Unantastbarkeit der Menschenwürde eingreift. Deshalb müssen nach Auffassung des BVerfG gerade auch für den Gewährleistungsbereich des Art. 10 I GG einfachgesetzliche Vorkehrungen zum Schutz der individuellen Entfaltung im Kernbereich der privaten Lebensgestaltung getroffen sein.[514] Dieser Schutz ist jedoch im Gewährleistungsbereich des Fernmeldegeheimnisses nach Art. 10 I GG anders ausgestaltet, als bei dem Grundrecht auf Unverletzlichkeit der Wohnung nach Art. 13 I GG.[515] Anders als das Grundrecht aus Art. 13 I GG weist das Fernmeldegeheimnis aus Art. 10 I GG keinen derart engen Bezug zur Menschenwürde auf, dass für das Telekommunizieren ein absoluter Schutz wie für das höchstpersönliche Verhalten in privaten Wohnräumen veranlasst wäre.[516] Denn nach überzeugender Auffassung des BVerfG sind „Bürger […] zur höchstpersönlichen Kommunikation nicht in gleicher Weise auf Telekommunikation angewiesen wie auf eine Wohnung“[517]. Bei der Nutzung von Telekommunikationsmedien, welche „auf die Entfernung der Kommunizierenden voneinander angelegt [sind] und typischerweise nicht in vergleichbarer Weise wie bei der Nutzung einer Wohnung den Rahmen für den Austausch höchstpersönlicher Informationen biete[n], […] besteht in ungleich geringerem Maße als bei der akustischen Wohnraumüberwachung, durch die unmittelbar in den ‚letzten Rückzugsbereich‘ […] des Bürgers eingegriffen wird, die Gefahr der Erfassung von Gesprächen, die dem Kernbereich privater Lebensgestaltung zuzuordnen [sind] und daher am unantastbaren Schutz der Menschenwürde des Betroffenen teilhaben.“[518] Hierbei ist insbesondere auch zu berücksichtigen, dass deren „Nutzung nicht nur die Inanspruchnahme der Dienste Dritter – der Telekommunikationsdiensteanbieter – erfordert, sondern auch [bspw., Anm. d. Verf.] im Bereich des Mobilfunks vielfach in der Öffentlichkeit stattfindet“[519].

---

513 BVerfG NJW 2005, 2603 (2612); krit. *Löffelmann*, AnwBl 2006, 598 (601).

514 Vgl. BVerfG NJW 2005, 2603 (2612); Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 23.

515 So auch BVerfG NJW 2005, 2603 (2612).

516 Vgl. BVerfG NJW 2005, 2603 (2612); auch *Löffelmann*, AnwBl 2006, 598 (599).

517 BVerfG NJW 2005, 2603 (2612).

518 BT-Drs. 16/5846, S. 43.

519 BT-Drs. 16/5846, S. 43.

Die in § 100a IV StPO verankerte Kernbereichsregelung für Maßnahmen der Telekommunikationsüberwachung wird den im Vergleich zu Eingriffen in Art. 13 I GG niedrigeren Schutzanforderungen bei Eingriffen in Art. 10 I GG mit der Normierung eines Beweiserhebungsverbotes in § 100a IV S. 1 StPO bereits auf Anordnungsebene (für den Fall des Bestehens tatsächlicher Anhaltspunkte für die Annahme, dass allein kernbereichsrelevante Erkenntnisse erlangt würden) sowie eines Beweisverwertungsverbotes in § 100a IV S. 2 StPO (für den Fall, dass dennoch kernbereichsrelevante Erkenntnisse erlangt wurden) daher insofern eher gerecht, als diese Regelung in angemessener Weise wirksame, an dem niedrigeren Bezug des Fernmeldegeheimnisses zur Menschenwürde ausgerichtete einfachgesetzliche Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung vorhält, die zugleich die effektive Durchführung von TKÜ-Maßnahmen zur Verfolgung schwerer Straftaten gewährleisten.[520] Nichts anderes als für die Überwachung und Aufzeichnung „normaler“ unverschlüsselter Telekommunikation (sei es unter Mitwirkung des jeweiligen Providers, sei es durch die Strafverfolgungsbehörden mit eigenen Mitteln) gilt für die Fälle der Überwachung verschlüsselt übermittelter VoIP-Telekommunikation an der Quelle, da es hinsichtlich des Schutzes von Gesprächsinhalten mit kernbereichsrelevantem Bezug unerheblich ist, ob diese im Rahmen der Überwachung leitungsvermittelter oder paketvermittelter Telekommunikation erfasst werden und ein Unterschied für das Erlangen etwaiger kernbereichsrelevanter Erkenntnisse hinsichtlich deren Erkenntnisgehaltes sowie deren Schutzbedürftigkeit nicht besteht. Nur weil eine Maßnahme der Quellen-TKÜ die VoIP-Telekommunikation bereits an der Quelle der Kommunikation erfasst, heißt dies nicht, dass Art. 10 I GG hinsichtlich des Schutzes kernbereichsrelevanter Gesprächsinhalte deshalb einen vergleichbar engen Bezug zur Menschenwürde entfalten würde, wie dies bei Art. 13 I GG und der akustischen Wohnraumüberwachung nach §§ 100c ff. StPO der Fall ist. Übertragen auf die Fälle der Überwachung von (VoIP-)Telekommunikation lässt sich daraus der Schluss ziehen, dass der Einzelne nicht auf höchstpersönliche Kommunikation via VoIP-Dienste in gleicher Weise angewiesen, wie auf private Wohnräume. VoIP-Telekommunikation stellt auch kein „letztes Refugium“ wie die private Wohnung dar, in welchem der Einzelne – wie für das Grundrecht aus Art. 13 I GG festgestellt – für sich sein und sich nach selbst gesetzten Maßstäben frei entfalten kann. Hieran ändert auch die Tatsache nichts, dass die Überwachung in den Fällen der Quellen-TKÜ an informationstechnischen Systemen ansetzt, welche auch eine Fülle von abgespeicherten Daten höchstpersönlicher Natur enthalten können. Denn eine

---

520 Vgl. vertiefend BT-Drs. 16/5846, S. 44; nunmehr höchstrichterlich bestätigt durch BVerfG, Beschl. v. 12.10.2011, Az.: 2 BvR 236/08, 2 BvR 237/08, 2 BvR 422/08.

Maßnahme, welche auf diese Daten zugreift, wäre als unzulässige Online-Durchsuchung bereits vom Maßnahmezweck wie auch von der zugrunde liegenden Anordnung über die Gestattung der Überwachung und Aufzeichnung von Telekommunikation nicht gedeckt.[521] Höhere Vorkehrungen zum Schutz kernbereichsrelevanter Inhalte bei der Überwachung von VoIP-Kommunikation an der Quelle sind daher nicht geboten. Anders ausgedrückt, kernbereichsrelevante Inhalte eines Telekommunikationsvorgangs verdienen bei einer Telekommunikation via Internetprotokoll keinen höheren Schutz, als dies bei einer Telekommunikation via Fest- oder Mobilfunknetz der Fall ist. Es würde eine – sachlich nicht gerechtfertigte – Besserstellung von moderner Telekommunikation via Internetprotokoll darstellen, wenn eine Überwachung dieser neuen Telekommunikationsform nur unter den strengeren Voraussetzungen des § 100c IV StPO zum Schutz des Kernbereichs privater Lebensgestaltung möglich wäre, während für die Überwachung sonstiger Telekommunikationsformen die Regelung des § 100a IV StPO Anwendung findet. Eine entsprechende Anwendung der Regelungen des § 100c IV StPO auf die Fälle der Quellen-TKÜ ist daher unter verfassungsrechtlichen Gesichtspunkten nicht geboten[522].

Überdies würde die Auferlegung einer derart verschärften Kernbereichsregelung, welche dazu verpflichten würde, vor Anordnung und Durchführung der Quellen-TKÜ eine mögliche Kernbereichsrelevanz der zu überwachenden Gespräche prognostisch zu prüfen[523], eine weder sach- noch praxisgerecht Lösung darstellen. Die entsprechende Anwendung der Regelungen des § 100c IV StPO auf Maßnahmen der Quellen-TKÜ wäre angesichts des dringenden strafprozessualen Bedürfnisses nach einer Überwachbarkeit der in der Popularität stetig zunehmenden verschlüsselten VoIP-Dienste und der Gleichbehandlung mit anderen Formen der Telekommunikation, insbesondere auch zur Verhinderung des Entstehens von „rechtsfreien Räume“, nicht sachgerecht, da dies den Anwendungsbereich der Quellen-TKÜ auf ein ab-

---

521 Bei einem heimlichen Zugriff im Rahmen einer sog. Online-Durchsuchung, in deren Rahmen das gesamte informationstechnische System durchsucht oder das Eingabeverhalten mitprotokolliert wird, ließen sich hinsichtlich des Menschenwürdebezuges durchaus Parallelen zur Privatsphäre der Wohnung ziehen, da bspw. auf einem Computer im Rahmen der individuellen Entfaltung persönlichste Daten gespeichert werden und private, für andere nicht einsehbare Aktivitäten stattfinden; dies hat nicht zuletzt auch Ausdruck im neuen Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 I i. V. m. 1 I GG gefunden, dessen Schutzbereich nach zutr. Rspr. des BVerfG (BVerfG NJW 2008, 822, 826) bei ausschließlicher Erfassung laufender Telekommunikation im Rahmen der Quellen-TKÜ jedoch nicht eröffnet ist.

522 Vgl. auch zutr. *Bär*, TK-Überwachung, § 100a StPO, Rn. 42, generell zu § 100a IV StPO.

523 Vgl. insoweit BT-Drs. 16/5846, S. 43.

solutes Minimum absenken würde, wie es bereits jetzt schon bei der akustischen Wohnraumüberwachung festgestellt werden kann[524]. Denn in entsprechender Anwendung des § 100c IV S. 2 StPO, wonach (Telefon-)Gespräche in Betriebs- und Geschäftsräumen i. d. R. nicht dem Kernbereich privater Lebensgestaltung zuzurechnen sind, müsste für VoIP-Telefonate in Privatwohnungen dann konsequenterweise die gegenteilige Vermutung des § 100c IV S. 2 StPO Wirkung entfalten, sodass Äußerungen im Rahmen von Telefonaten in Privatwohnungen folglich dem Kernbereich privater Lebensgestaltung i. d. R. zuzurechnen seien.[525] Es ist daher als sachgerechter zu erachten, auch bei der Überwachung verschlüsselter Internettelefonie eine Kernbereichsregelung wie in § 100a IV StPO vorzuhalten, welche ein Beweiserhebungsverbot wie in § 100a IV S. 1 StPO bei (positivem) Vorliegen tatsächlicher Anhaltspunkte für die Annahme eines alleinigen[526] Erlangens von Erkenntnissen aus dem Kernbereich privater Lebensgestaltung vorsieht und flankierend („auf zweiter Stufe") ein Beweisverwertungsverbot wie in § 100a IV S. 2 StPO für bei Durchführung der Maßnahme erlangte kernbereichsrelevante Erkenntnisse festlegt. Dies wird auch den Bedürfnissen der Praxis insoweit gerecht, als Telekommunikation im geschäftlichen wie auch im privaten Bereich i. d. R. durch verschiedenste Inhalte geprägt sein kann. Da sich Anhaltspunkte für eine Kernbereichsrelevanz bei Telekommunika-

---

524 Vgl. hierzu auch BT-Drs. 16/5846, S. 43.

525 Vgl. BVerfG NJW 2004, 999 (1004) zur akustischen Wohnraumüberwachung; Meyer-Goßner – *Cierniak*, StPO, § 100c, Rn. 14 m. w. N.

526 Ob hierbei letztlich die Lösung wie vom Gesetzgeber gewählt, dass sich die Annahme darauf beziehen muss, dass „allein" Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, oder stattdessen eine Lösung wie z. T. im Schrifttum vorgeschlagen (vgl. bspw. Stellungnahme der Bundesrechtsanwaltskammer zum Gesetzentwurf der Bundesregierung zum Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (BR-Drucks. 275/07), S. 29 f., abrufbar unter http://www.brak.de/w/files/stellungnahmen/Stn31-2007.pdf (zuletzt aufgerufen 15.06.2012), dass für die Annahme eines Beweiserhebungsverbots es bereits genügen sollte, wenn „überwiegend" kernbereichrelevante Erkenntnisse erlangt würden, sachgerechter wäre, kann an dieser Stelle dahingestellt bleiben, da diese Frage kein spezifisches Problem der Quellen-TKÜ darstellt, sondern für TKÜ-Maßnahmen nach §§ 100a, 100b StPO generell diskutiert wird; ohnehin hat das BVerfG in einer kürzlich ergangenen Entscheidung (BVerfG, Beschl. v. 12.10.2011, Az.: 2 BvR 236/08, 2 BvR 237/08, 2 BvR 422/08) unter Zurückweisung mehrerer Verfassungsbeschwerden bezüglich der zum 01.01.2008 in Kraft getretenen Neuregelung der strafprozessualen Telekommunikationsüberwachung (BGBl. I S. 3198) nunmehr höchstrichterlich festgestellt, dass „die durch § 100a Abs. 4 StPO geschaffenen Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung bei der Telekommunikationsüberwachung […] sowohl auf der Erhebungsebene als auch in der Auswertungsphase [= zweistufiges Schutzkonzept, Anm. d. Verf.] den verfassungsrechtlichen Anforderungen [genügen]" (Abs.-Nr. 209).

tion i. d. R. erst aus dem jeweiligen Gespräch selbst ergeben[527], wäre eine verschärfte Regelung des Kernbereichschutzes in Form einer (präventiven) negativen Kernbereichsprognose – wie in § 100c IV StPO für die Fälle der akustischen Wohnraumüberwachung gesetzlich vorgeschrieben – für Maßnahmen der Quellen-TKÜ in gleicher Weise wie für sonstige TKÜ-Maßnahmen nicht praktikabel. Dies wird insoweit auch daraus deutlich, als über die entsprechende Verweisung des § 100j III StPO-E auf die Regelung des § 100c V S. 1 StPO die Ermittlungsbehörden dazu verpflichten wären, das Abhören und Aufzeichnen unverzüglich zu unterbrechen, soweit sich während der Überwachung Anhaltspunkte dafür ergeben, dass kernbereichsrelevante Äußerungen erfasst werden, was zur Konsequenz hätte, dass im Einzelfall wohl auf eine automatisierte Aufzeichnung verzichtet werden müsste[528], während auch das BVerfG hingegen (zu Recht) festgestellt hat, dass im Rahmen heimlicher Zugriffe auf informationstechnische Systeme „die Datenerhebung schon aus technischen Gründen zumindest überwiegend automatisiert erfolgen [wird]“[529] und des deshalb „praktisch unvermeidbar [ist], Informationen zur Kenntnis zu nehmen, bevor ihr Kernbereichsbezug bewertet werden kann“[530], weshalb „für hinreichenden Schutz in der Auswertungsphase gesorgt sein [muss]“[531]. Dies wird durch die Kernbereichsregelung des § 100a IV StPO und das darin verankerte zweistufige Schutzkonzept in verfassungsgemäßer und praktikabler Weise sichergestellt, was durch das BVerfG für Maßnahmen nach §§ 100a, 100b StPO indes höchstrichterlich bestätigt wurde[532].

Auch für die entsprechende Anwendung einer Sonderregelung zum Schutz von Berufsgeheimnisträgern wie in § 100c VI S. 1 StPO, welche – anders als die allgemeine Regelung in § 160a I, II StPO[533] – hinsichtlich

---

527 Vgl. BT-Drs. 16/5846, S. 43; BVerfG NJW 2005, 2603 (2612).

528 Vgl. auch *Bär*, TK-Überwachung, § 100c StPO, Rn. 30.

529 BVerfG NJW 2008, 822 (834), wenngleich es den Ermittlungspersonen natürlich unbelassen bleibt, über das Internet geführte Sprachtelefonie, soweit technisch möglich, auch persönlich zu überwachen, sprich „live“ mitzuhören.

530 BVerfG NJW 2008, 822 (834).

531 BVerfG NJW 2008, 822 (834).

532 Vgl. hierzu BVerfG, Beschluss vom 12.10.2011, Az.: 2 BvR 236/08, 2 BvR 237/08, 2 BvR 422/08, wonach „die durch § 100a Abs. 4 StPO geschaffenen Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung bei der Telekommunikationsüberwachung […] sowohl auf der Erhebungsebene als auch in der Auswertungsphase [= zweistufiges Schutzkonzept, Anm. d. Verf.] den verfassungsrechtlichen Anforderungen [genügen]“ (Abs.-Nr. 209).

533 In seiner Entscheidung über die Verfassungsmäßigkeit der zum 01.01.2008 in Kraft getretenen Neuregelung der strafprozessualen Telekommunikationsüberwachung (BGBl. I S. 3198) hat das BVerfG unter Zurückweisung mehrerer Verfassungsbeschwerden (BVerfG, Beschl. v. 12.10.2011, Az.: 2 BvR 236/08, 2 BvR

der in § 53 I StPO bezeichneten Zeugnisverweigerungsberechtigten (Berufsgeheimnisträger) nicht zwischen den einzelnen Berufsgruppen unterscheidet[534], besteht insbesondere mit Blick auf die unterschiedliche Eingriffsintensität und dem Schutz besonderer Vertrauensverhältnisse für die Maßnahmen der Quellen-TKÜ kein Bedürfnis. Eine unterschiedliche Behandlung der Überwachung von unverschlüsselter (v. a. Festnetz-/Mobilfunk-)Telekommunikation und verschlüsselter (VoIP-)Telekommunikation an der Quelle in Bezug auf das Schutzniveau Zeugnisverweigerungsberechtigter wäre sachlich nicht gerechtfertigt. Überdies gehen die Regelungen des § 100c VI StPO mit der Verhängung eines generellen Überwachungs- und somit Beweiserhebungsverbotes bereits für die eingriffsintensivere Ermittlungsmaßnahme der akustischen Wohnraumüberwachung deutlich über die Vorgaben des BVerfG hinaus[535], da das BVerfG mehrfach festgestellt hat[536], dass mangels unmittelbaren Bezugs zum Kernbereich privater Lebensgestaltung[537] ein absoluter Vorrang des Schutzes der Zeugnisverweigerungsrechte von Parlamentsabgeordneten und Presseangehörigen gegenüber dem öffentlichen Interesse effektiver Strafrechtspflege von Verfassungs wegen nicht geboten ist.[538] Vielmehr enthalten die allgemeinen Regelungen in § 148 StPO und § 160a StPO sowohl für die „klassische" TKÜ als auch für die „moderne" Quellen-TKÜ angemessene und ausreichende gesetzliche Vorkehrungen zum Schutz zeugnisverweigerungsberechtigter Personen.[539]

Einer entsprechenden Anwendung des § 100c VII StPO auch auf die Fälle der Quellen-TKÜ stehen deutliche systematische Bedenken entgegen. Denn eine abschließende Entscheidung des anordnenden Gerichts über die Frage der Verwertbarkeit erlangter Erkenntnisse bereits im Ermittlungsver-

---

237/08, 2 BvR 422/08) des Weiteren höchstrichterlich festgestellt, dass auch die Regelungen über den Schutz von Zeugnisverweigerungsberechtigten in § 160a I, II StPO und die Privilegierung bestimmter Berufsgruppen in Bezug auf die Gewährung absoluten Ermittlungsschutzes verfassungsrechtlich gerechtfertigt seien (Abs.-Nr. 243 ff.).

534 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100c, Rn. 15 u. 22a.

535 Vgl. *Bär*, TK-Überwachung, § 100c StPO, Rn. 35 f. m. w. N.; *Löffelmann*, NJW 2005, 2033 (2035).

536 Vgl. insoweit BVerfG NJW 2004, 999 (1004); BVerfG NJW 2003, 1787 (1794); BVerfG NJW 2003, 3401 (3401 f.).

537 Die Zeugnisverweigerungsrechte von Parlamentsabgeordneten sowie Presseangehörigen dienen nach BVerfG NJW 2004, 999 (1004) vielmehr der Funktionsfähigkeit der jeweiligen Institution als dem Persönlichkeitsschutz des Beschuldigten.

538 Vgl. *Löffelmann*, NJW 2005, 2033 (2035).

539 Siehe hierzu allgemein *Bär*, TK-Überwachung, § 100a StPO, Rn. 41, 46 ff.; vgl. nunmehr BVerfG, Beschl. v. 12.10.2011, Az.: 2 BvR 236/08, 2 BvR 237/08, 2 BvR 422/08 zu § 160a I, II StPO.

fahren steht in klarem Kontrast zur grundsätzlichen Systematik der Strafprozessordnung, wonach die Beurteilung der Verwertbarkeit dem späteren erkennenden Gericht obliegt, dessen Entscheidung darüber hinaus der Kontrolle durch ober- bzw. höchstrichterliche Instanzen unterliegt.[540] Die hierüber besser gewährleistbare einheitliche Auslegung und Anwendung der Verwertungsregelungen ist gerade dem besonderen Interesse der Rechtssicherheit dienlich.[541]

Im Rahmen der über die Verweisung in § 100j III StPO-E auf die Vorschriften des § 100d StPO für Maßnahmen der Quellen-TKÜ entsprechende Anwendung findenden Bestimmungen des § 100d I S. 1 StPO zur Konzentration der Anordnungszuständigkeit im Ermittlungsverfahren auf einen besonderen Spruchkörper wie bei Maßnahmen der akustischen Wohnraumüberwachung (Staatsschutzkammer beim LG gemäß § 100d I S. 1 StPO, § 74a IV GVG anstelle des normalerweise nach §§ 162 I S. 1, 169 StPO zuständigen Ermittlungsrichters sowie Beschwerdemöglichkeit zum OLG, in dessen Bezirk die jeweilige Landesregierung ihren Sitz hat, § 120 IV, I GVG) sind nicht geboten. Denn mit Blick auf die niedrigere Eingriffsqualität der Quellen-TKÜ und zugleich höheren praktischen Relevanz der Telekommunikationsüberwachung im Vergleich zu Maßnahmen der akustischen Wohnraumüberwachung stellt das Belassen der Regelanordnungszuständigkeit – wie gesetzlich für die Anordnung der Überwachung und Aufzeichnung von Telekommunikation vorgesehen – beim Ermittlungsrichter des Amtsgerichts am jeweiligen Sitz der Staatsanwaltschaft (§ 100b I S. 1, § 162 I StPO) sowie der Regelzuständigkeit der Strafkammern am Landgericht im Rechtsmittelverfahren (§ 73 I GVG)[542] eine insgesamt angemessene und sachgerechtere Lösung dar. Über die Regelungen des § 162 I StPO zur Konzentration der örtlichen Regelanordnungszuständigkeit auf den Ermittlungsrichter am Sitz der jeweiligen Staatsanwaltschaft lässt sich nämlich neben der Stärkung der mit dem Richtervorbehalt bezweckten rechtsstaatlichen Kontrolle[543] zudem auch ein praktikables und zügiges Anordnungsverfahren gewährleisten. Denn die Verlagerung der Anordnungszuständigkeit vom Ermittlungsrichter am Sitz der jeweiligen Staatsanwaltschaften auf einen ggf. entfernteren (Kollegial-)Spruchkörper wie die Staatsschutzkammer bei demjenigen Landgericht, in dessen Bezirk das OLG seinen Sitz hat, für den gesamten OLG-Bezirk (§ 74a IV GVG), beinhaltet – insbesondere in Flächenstaaten – zugleich auch die Gefahr längerer Bearbeitungszeiten und

---

540 Vgl. BT-Drs. 16/5846, S. 36.

541 Vgl. BT-Drs. 16/5846, S. 36.

542 Zu den Rechtsmitteln im Einzelnen, siehe *Bär*, TK-Überwachung, § 100a StPO, Rn. 41, 46 ff.

543 Vgl. BT-Drs. 16/5846, S. 24.

erschwerter gerichtlicher Begleitung der Maßnahme auf Grund größerer räumlicher Distanz zu entfernter liegenden Ermittlungsbehörden in deren Bezirk.[544] Des Weiteren sei auch darauf hingewiesen, dass die Verlagerung der Anordnungskompetenz auf die Staatsschutzkammer beim Landgericht – sei es wie gegenwärtig bei der akustischen Wohnraumüberwachung oder bei einer möglichen Befugnisnorm zur Quellen-TKÜ – generell nicht ohne einen gewissen systematischen Wertungswiderspruch erfolgen würde, da bspw. der Erlass von Haftbefehlen vor Erhebung der öffentlichen Klage in die Zuständigkeit des Ermittlungsrichters fällt[545], hingegen im Vergleich zu dem damit verbundenen Eingriff in die persönliche Freiheit weniger massive Überwachungsmaßnahmen hiernach aber der Anordnung durch ein höherinstanzliches Gericht bedürften[546].

Auch das BVerfG verlangt unter verfassungsrechtlichen Gesichtspunkten insoweit für einen heimlichen Zugriff auf informationstechnische Systeme nur, dass „der Zugriff grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen [ist]“[547], nicht jedoch, dass die erforderliche „vorbeugende Kontrolle einer geplanten heimlichen Ermittlungsmaßnahme durch eine unabhängige und neutrale Instanz“[548] zwingend durch ein höheres Gericht als den Ermittlungsrichter bzw. durch einen besonderen Spruchkörper erfolgen müsste. Art. 10 I GG selbst – als relevanter Grundrechtsmaßstabs einer Quellen-TKÜ[549] – enthält darüber hinaus keine dem Art. 13 III S. 3 GG entsprechende Bestimmung, welche für die Telekommunikationsüberwachung von Verfassungs wegen das Erfordernis eines mit drei Richtern besetzten Spruchkörpers wie für die Anordnung technischer Mittel zur akustischen Überwachung von Wohnungen konstatiert.

---

544 In diese Richtung auch Bundesrechtsanwaltskammer, Stellungnahme zum Gesetzentwurf der Bundesregierung zum Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (BR-Drucks. 275/07), S. 51 f., abrufbar unter http://www.brak.de/w/files/stellungnahmen/Stn31-2007.pdf (zuletzt aufgerufen 15.06. 2012); vgl. insoweit auch die Antwort des Landes Brandenburg zum Fragenkatalog des BVerfG, abgedruckt bei *Vormbaum*/*Asholt*, Der Große Lauschangriff vor dem Bundesverfassungsgericht, 2. Teil, S. 236.

545 Gemäß der besonderen Zuständigkeitsregelung in § 125 I StPO, wie daneben auch gemäß der allgemeinen Zuständigkeitsregelung in § 162 I S. 2 StPO.

546 Vgl. insoweit auch die Antworten des Freistaates Bayern und des Landes Brandenburg zum Fragenkatalog des BVerfG, abgedruckt bei Vormbaum/Asholt, Der Große Lauschangriff vor dem Bundesverfassungsgericht, 2. Teil, S. 236.

547 BVerfG NJW 2008, 822 (832).

548 BVerfG NJW 2008, 822 (832), wobei hiervon „eine Ausnahme für Eilfälle, etwa bei Gefahr im Verzug, vorgesehen werden [darf]“ (832).

549 Vgl. BVerfG NJW 2008, 822 (826).

Die über die Verweisung in § 100j III StPO-E ebenso auf die Vorschriften des § 100d StPO entsprechende Anwendung findenden, im Vergleich zu § 100b II S. 2 StPO weitergehenden Anforderungen nach § 100d II S. 2 Nr. 2 (Angabe des Tatvorwurfs) und Nr. 5 StPO (Angabe der Art der durch die Maßnahme zu erhebenden Informationen und ihrer Bedeutung für das Verfahren) an den gesetzlich notwendigen Inhalt der Entscheidungsformel eines Quellen-TKÜ-Beschlusses sind sachlich nicht geboten. Anders als bei der akustischen Wohnraumüberwachung sah der Gesetzgeber bei Maßnahmen der Telekommunikationsüberwachung für den gesetzlich vorgeschriebenen Inhalt in § 100b II S. 2 StPO von der Angabe des Tatvorwurfs in der Entscheidungsformel wie bei § 100d II S. 2 Nr. 2 StPO aus Datenschutzgründen bewusst ab, da in den Fällen des § 100b III StPO, sprich der (gesetzlich nicht zwingend durch die Ermittlungsbehörden in Anspruch zu nehmenden[550]) Mitwirkung eines Telekommunikationsunternehmens an der Durchführung der TKÜ-Maßnahme, der Beschluss (genauer: die Entscheidungsformel) an dieses zu übermitteln ist.[551] Wenngleich die Entscheidungsformel eines Quellen-TKÜ-Beschlusses auf Grund der Durchführung der Maßnahme durch die Ermittlungsbehörden mit eigenen Mitteln – wozu die Ermittlungsbehörden auf Grundlage der §§ 100a, 100b StPO berechtigt sind[552] – nicht an Dritte übermittelt wird und somit die Gefahr einer Datenschutzverletzung durch Angabe des Tatvorwurfes in der Entscheidungsformel grds. nicht besteht (anders ggf. bei kombinierten Beschlüssen[553]), ist eine Angabe des Tatvorwurfs in der Entscheidungsformel – in Anlehnung an § 100d II S. 2 Nr. 2 StPO zum Zwecke des Absteckens des äußeren Rahmens, innerhalb dessen die Maßnahme durchzuführen ist[554] – bei einer Maßnahme der Quellen-TKÜ nicht zwingend erforderlich. Zum Abstecken des äußeren Rahmens wie auch zur Sicherstellung der Mess- und Kontrollierbarkeit des mit der angeordneten Maßnahme verbundenen Grundrechtseingriffs genügt die nähere Ausführung des Tatvorwurfs in den Beschlussgründen. Insoweit gilt für die mit eigenen Mitteln der Strafverfolgungsbehörden durchgeführte Quellen-TKÜ nichts anderes, als für die übrigen ohne Mitwirkung der nach § 100b III StPO Verpflichteten realisierten TKÜ-Maßnahmen.

Ebenso wenig bedarf es einer Angabe der Art der durch die Maßnahme zu erhebenden Informationen und ihrer erwarteten Bedeutung für das Ver-

---

550 Da die Eingriffsnorm des § 100a I StPO insoweit „eine nicht durch die Mitwirkung der Telekommunikationsdienstleister bedingte Befugnis, Telekommunikation zu überwachen und aufzuzeichnen [enthält]“ (BT-Drs. 16/5846, S. 47).

551 Vgl. BT-Drs. 16/5846, S. 46.

552 Vgl. BT-Drs. 16/5846, S. 47.

553 Siehe hierzu 3. Teil A.I.2.

554 So BVerfG NJW 2004, 999 (1014) zur akustischen Wohnraumüberwachung.

fahren als Erkenntnismittel[555] entsprechend § 100d II S. 2 Nr. 5 StPO bereits in der Entscheidungsformel des Quellen-TKÜ-Beschlusses. Auch hier erfordert der Verhältnismäßigkeitsgrundsatz keine unterschiedliche Behandlung von Quellen-TKÜ und übriger TKÜ-Maßnahmen, da es sich hierbei um Maßnahmen zur Erfassung von Telekommunikationsinhalten zum Zwecke der Erlangung von Beweismitteln oder Spurenansätzen handelt und sich die zu erlangenden Erkenntnisse ihrer Art nach nicht unterscheiden.

Die Verankerung einer qualifizierten Begründungspflicht wie über die Verweisung des § 100j III StPO-E auf § 100d III StPO ist unter dem Gesichtspunkt des Bemühens um eine gewisse „Grundrechtsoptimierung" des Regelungsvorschlags zwar vertretbar. Eine gesetzlich vorgeschriebene qualifizierte Begründungspflicht wie in § 100d III StPO ist für die Maßnahme der Quellen-TKÜ aber nicht zwingend erforderlich, zumal diese Vorschrift selbst für die akustische Wohnraumüberwachung über die Forderungen des BVerfG[556] hinausgeht[557]. Wie bei TKÜ-Maßnahmen im Allgemeinen würde die Aufnahme einer gesetzlich vorgeschriebenen qualifizierten Begründungspflicht wie in § 100d III StPO auch bei Maßnahmen der Quellen-TKÜ, welche hinsichtlich ihrer Eingriffsintensität unterhalb der akustischen Wohnraumüberwachung anzusiedeln sind (vgl. oben), zu einer – gesetzessystematisch nicht wünschenswerten und gesetzgeberisch wohl auch nicht gewollten – Relativierung der besonderen Anforderungen der akustischen Wohnraumüberwachung führen sowie darüber hinaus auch Fragen hinsichtlich der sich in Konsequenz hieraus ergebenden (dann möglw. niedrigeren) Anforderungen an die Begründung anderer heimlicher wie auch offener Ermittlungsmaßnahmen aufwerfen.[558] Eine entsprechende Unterwerfung der Quellen-TKÜ unter die qualifizierten Begründungspflichten des § 100d III StPO ist deshalb nicht zwingend angezeigt. Es genügt vielmehr eine den allgemeinen Anforderungen nach § 34 StPO gerecht werdende Begründung, welche für die konkrete Quellen-TKÜ-Maßnahme insbesondere die zugrunde liegende Ermittlungssituation nennt, die ermittlungstechnische Notwendigkeit des Ansetzens am Endgerät mittels spezieller Überwachungssoftware darlegt und die technischen Anforderungen an diese erläutert, womit eine Nachvollziehbarkeit und Überprüfbarkeit der Maßnahme ohne weiteres er-

---

555 Vgl. BT-Drs. 15/4533, S. 16.

556 Vgl. BVerfG NJW 2004, 999 (1014), welches lediglich feststellt, dass „die maßgeblichen Erwägungen des Gerichts […] in der Begründung der Anordnung hinreichend zu dokumentieren [sind]" und „aus § 34 i.V. mit § 100d VI S. 1 StPO [a. F., Anm. d. Verf.] folgt, dass die Anordnung schriftlich zu begründen ist", wobei es „darüber hinausgehender gesetzlicher Regelungen […] nicht [bedarf]" (BVerfG NJW 2004, 999, 1014).

557 Vgl. BT-Drs. 15/4533, S. 17.

558 Vgl. insoweit BT-Drs. 16/5846, 46.

möglicht wird. Bereits über die Einhaltung dieser allgemeinen Begründungspflicht lässt sich die Funktion des Richtervorbehaltes in sorgfältiger und verantwortungsvoller Weise[559] wahrnehmen sowie die Mess- und Kontrollierbarkeit der Entscheidung gewährleisten.[560] Ergänzend findet auch auf Maßnahmen der Quellen-TKÜ wie auf TKÜ-Maßnahmen im Allgemeinen die gefestigte Rspr. zu den notwendigen Inhalten der Begründung von Durchsuchungsbeschlüssen entsprechende Anwendung.[561]

Eine Sonderregelung wie die über § 100j III StPO-E entsprechende Anwendung findende Regelung in § 100d V Nr. 1 StPO zur Weiterverwendung erlangter *verwertbarer* (gemäß den Erhebungs- und Verwertungsverbote in § 100c IV bis VI StPO[562]) personenbezogener Daten (Zufallsfunde) in anderen Strafverfahren ohne Einwilligung der insoweit überwachten Person ist auf Grund der von vorliegender Arbeit befürworteten sachnäheren Ansiedlung der Quellen-TKÜ und deren grundrechtlicher Eingriffswirkung bei den TKÜ-Maßnahmen nach §§ 100a, 100b StPO[563] als bei Maßnahmen der akustischen Wohnraumüberwachung nicht geboten. Insofern ist die Frage der Weiterverwendung erlangter Daten in anderen Strafverfahren für TKÜ-Maßnahmen nach dem ausdrücklichen Willen des Gesetzgebers in der allgemeinen Verwendungsvorschrift des § 477 II S. 2 StPO geregelt[564]. Die Vorschrift des § 477 II S. 2 StPO[565] – welche auf die gefestigte fachgerichtliche Rspr. zur Telekommunikationsüberwachung nach §§ 100a, 100b StPO zurückgeht[566] – enthält mit der Vorgabe, dass die auf Grund einer Maßnahme, die – wie die (Quellen-)TKÜ – nur bei Verdacht bestimmter Straftaten (hier: schwere Straftaten nach § 100a I Nr. 1, II StPO) nach der StPO zulässig ist, erlangten personenbezogenen Daten ohne Einwilligung der von der Maßnahme betroffenen Personen *zu Beweiszwecken* in anderen Strafverfahren nur zur Aufklärung solcher Straftaten verwendet werden dürfen, zu deren Aufklärung eine solche Maßnahme nach diesem Gesetz hätte angeordnet werden dürfen, eine angemessene und sachgerech-

---

559 Vgl. insoweit BT-Drs. 15/4533, S. 17 zur akustischen Wohnraumüberwachung.

560 Für Einzelheiten zum Inhalt der Begründung eines Quellen-TKÜ-Beschlusses, siehe 3. Teil A.I.2. sowie Anhang 1.

561 Vgl. insoweit BT-Drs. 16/5846, S. 46 m. w. N.

562 Vgl. Meyer-Goßner – *Cierniak*, StPO, § 100d, Rn. 6 m. w. N.

563 Für Einzelheiten zur grundsätzlichen Eignung der §§ 100a, 100b StPO als Rechtsgrundlage für die strafprozessuale Maßnahme der Quellen-TKÜ, siehe 3. Teil A.I.

564 Vgl. BT-Drs. 16/5846, S. 3, 38, 45, 48 u. 66.

565 Zur Regelung des § 477 II S. 2 StPO im Einzelnen, siehe Meyer-Goßner – *Cierniak*, StPO, § 477, Rn. 5 ff.

566 Vgl. BT-Drs. 16/5846, S. 66; ebenso Meyer-Goßner – *Cierniak*, StPO, § 477, Rn. 5a.

te Regelung der Weiterverwendung von mittels einer (Quellen-)TKÜ-Maßnahme erlangten Daten (Zufallsfunde) in anderen Strafverfahren. Ein (verfassungs-)rechtliches Bedürfnis für ein Unterwerfen der Weiterverwendung ebenfalls unter die Erhebungs- und Verwertungsverbote des § 100c IV–VI StPO durch Verankerung der zusätzlichen Verwendungsvoraussetzung der *Verwertbarkeit* erlangter Daten im Ausgangsverfahren, besteht ebenso wenig, wie für das Einbeziehen auch der Weiterverwendung *als Spurenansatz* in die speziellen gesetzliche Verwendungsregelungen des § 100d V Nr. 1 StPO, da rechtmäßig gewonnene Zufallserkenntnisse, die keine Katalogtaten betreffen, nach gefestigter und vom BVerfG gebilligter fachgerichtlicher Rechtsprechung in anderen Strafverfahren zwar nicht zu Beweiszwecken verwertet werden dürfen, sie aber Anlass für weitere Ermittlungen zur Gewinnung neuer Beweismittel sein können[567]. Dies ist auch in den Fälle der Quellen-TKÜ sachgerecht, da hierüber einerseits dem Schutz des Fernmeldegeheimnisses aus Art. 10 I GG genügt wird, indem weitergehende Ermittlungen in anderen Strafverfahren auf Grund von im Ausgangsverfahren gewonnenen Zufallserkenntnissen nur für die Fälle für zulässig gehalten werden, bei denen die Maßnahme nach §§ 100a, 100b StPO rechtmäßig war[568]. Andererseits findet über eine solche Lösung auch das öffentliche Interesse an effektiver Strafverfolgung und Straftatenaufklärung angemessen Berücksichtigung.[569]

Eine Ausrichtung der Quellen-TKÜ an der Eingriffsschwelle der §§ 100c ff. StPO ist daher im Ergebnis abzulehnen.

3. Bedürfnis nach einer eigenständigen Befugnisnorm?

Dem unter Punkt 1 analysierten und unter Punkt 2 dogmatisch bewerteten Vorschlag nach *Brodowski/Freiling* für eine eigenständige Regelung der Quellen-TKÜ liegt die Annahme zugrunde, dass die Quellen-TKÜ unter Einsatz einer Überwachungssoftware auf Grund einer damit verbundenen größeren Eingriffstiefe eher eine Anlehnung der Eingriffsvoraussetzungen an den erhöhten Anforderungen der akustischen Wohnraumüberwachung nach §§ 100c ff. StPO als an §§ 100a, 100b StPO erforderlich macht.[570] Wird die Quellen-TKÜ demnach als eine von der Telekommunikationsüberwachung nach §§ 100a, 100b StPO losgelöste eigenständige Ermittlungs-

---

567 So BVerfG NJW 2005, 2766 (2766); BT-Drs. 16/5846, S. 66, 64.

568 Vgl. insoweit BT-Drs. 16/5846, S. 66, 64.

569 Vgl. insoweit BT-Drs. 16/5846, S. 66, 64.

570 Vgl. *Brodowski*/*Freiling*, Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, S. 144, abrufbar unter http://www.sicherheit-forschung.de/schriftenreihe/sr_v_v/sr_4.pdf (zuletzt aufgerufen 15.06.2012).

maßnahme betrachtet, die ihrem Regelungsinhalt und Maßnahmegegenstand nach mit dem Normengefüge heimlicher Ermittlungsmaßnahmen der StPO de lege lata nicht in Einklang zu bringen ist und vollkommen neu hinzugefügt wird, so liegt eine Regelung als eigenständige Befugnisnorm auf der Hand, erst recht, wenn diese an der Eingriffsschwelle der akustischen Wohnraumüberwachung ausgerichtet sein soll. Eine solche eigenständige Regelung kann dann detailliert die spezifischen Eingriffsvoraussetzungen einer Quellen-TKÜ ähnlich der Ausgestaltung der §§ 100c ff. StPO regeln. Auch die systematische Verortung dieser neuen Befugnisnorm als „§ 100j StPO" im Normengefüge des *Achten Abschnitts des Ersten Buches* der StPO nach der Befugnisnorm des § 100i StPO (Einsatz des IMSI-Catchers) als weitere strafprozessuale heimliche Ermittlungsmaßnahme erscheint dann ebenfalls konsequent. Als von den §§ 100a, 100b StPO unabhängige Ermittlungsmaßnahme ist ein Einfügen der neuen Befugnisnorm unmittelbar bei den §§ 100a, 100b StPO nicht zwingend angezeigt.

Geht man hingegen mit dem anderen Teil des juristischen Meinungsbildes – dem sich auch vorliegende Arbeit im Grundsatz anschließt – davon aus, dass sich die Ermittlungsmaßnahme der Quellen-TKÜ auf die bestehenden Regelungen der §§ 100a, 100b StPO zur Telekommunikationsüberwachung und entsprechend konkretisierte Beschlüsse stützen lässt, so scheidet ein Bedürfnis für die Schaffung einer eigenständigen strafprozessualen Befugnisnorm aus. Denn wie bereits vorhergehend ausgeführt, würde das Bedürfnis einer Ausgestaltung der Quellen-TKÜ als eigenständige, erstmals geschaffene Befugnisnorm zugleich bedeuten, dass die Quellen-TKÜ de lege lata von keiner der vorhandenen strafprozessualen Befugnisnormen erfasst ist. Dies lässt sich jedoch mit guten Gründen, wie das Ergebnis der Ausführungen zu Modell 1 zeigt[571], dogmatisch widerlegen. Ein Bedürfnis für eine getrennte Regelung der Überwachung und Aufzeichnung von verschlüsselter IP-Telekommunikation an der Quelle von der Überwachung und Aufzeichnung von („sonstiger") Telekommunikation nach §§ 100a, 100b StPO, welche ebenfalls am jeweiligen Endgerät ansetzen und mit eigenen Mitteln der Strafverfolgungsbehörden erfolgen kann, besteht indes nicht. Bei den §§ 100a, 100b StPO handelt es sich vielmehr um eine im Vergleich zu den sonstigen heimlichen Ermittlungsmaßnahmen der StPO, insbesondere der akustischen Wohnraumüberwachung, sachnähere Regelung, welche das Institut der Überwachung und Aufzeichnung von Telekommunikation in der StPO regelt und auch die Quellen-TKÜ im Grundsatz legitimiert. Da insbesondere die Eingriffsschwelle von Maßnahmen der Quellen-TKÜ nicht an derjenigen der akustischen Wohnraumüberwachung ausgerichtet sein

---

571 Für Einzelheiten zur grundsätzlichen Zulässigkeit der Quellen-TKÜ nach §§ 100a, 100b StPO, siehe 3. Teil A.I.

muss (vgl. oben)[572], enthalten die §§ 100a, 100b StPO die grds. erforderlichen und wesentlichen Normbestandteile, an denen auch eine Quellen-TKÜ anknüpft und die eine eigenständige Regelung in einer separaten Befugnisnorm entbehrlich machen.

Ein Bedürfnis für die Schaffung einer eigenständigen, insbesondere von den §§ 100a, 100b StPO systematisch zu trennenden Befugnisnorm für die Quellen-TKÜ besteht deshalb nicht. Soweit Ansatzpunkte für eine gesetzliche Klarstellung bestehen und eine solche trotz bzw. gerade wegen der grundsätzlichen Tauglichkeit der §§ 100a, 100b StPO als Rechtsgrundlage der Quellen-TKÜ wünschenswert ist[573], empfiehlt es sich, statt der – systematisch nicht erforderlichen – Schaffung einer eigenständigen Befugnisnorm „§ 100j StPO", welche die Quellen-TKÜ den heimlichen Ermittlungsbefugnissen der §§ 100a bis 100i StPO „hintenanhängt", die bestehenden §§ 100a, 100b StPO um die spezifischen Besonderheiten der Überwachung und Aufzeichnung von über informationstechnische Systeme geführter verschlüsselter Telekommunikation unter Verwendung einer Überwachungssoftware als spezielles technisches Mittel zu ergänzen. Die Gründe, die für eine Ergänzung der §§ 100a, 100b StPO sprechen, sind mithin keine solchen, die im Zusammenhang mit der Eingriffstiefe dieser speziellen Realisierungsweise der Telekommunikationsüberwachung „an der Quelle" stehen, sondern allein solche, die – wie dies im Rahmen der nachfolgenden Ausführungen zu Modell 3 im Einzelnen aufgezeigt wird – auf dem Aspekt umfassender und größtmöglicher Rechnungtragung der Grundsätze der Tatbestandsbestimmtheit und Normenklarheit beruhen sowie der Absicherung einer insgesamt verhältnismäßigen technischen Umsetzungsweise der Maßnahme und einer bestmöglichen Gewährleistung der Gerichtsfestigkeit und Beweissicherheit erlangter Erkenntnisse dienen.

III. Modell 3: Ergänzung der §§ 100a, 100b StPO

1. Bedürfnis nach einer Ergänzung der bestehenden Befugnisnormen

Wie bereits im Rahmen der obigen Ausführungen zu Modell 1 dargelegt, wird seitens des Verfassers der in Rechtspraxis und Kommentarliteratur verbreiteten Auffassung[574] – die insbesondere mit den jüngeren Tendenzen

---

572 Zur Frage, ob ein Bedürfnis nach einer Angleichung an §§ 100c ff. StPO besteht, siehe 3. Teil B.II.2.

573 Für Einzelheiten zu den Anknüpfungspunkten für eine gesetzliche Klarstellung, siehe 3. Teil B.I. sowie 3. Teil B.III.1.

574 So Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 7a; BeckOK – *Graf*, StPO, Ed. 13, § 100a, Rn. 107c; KK – *Nack*, StPO, § 100a, Rn. 27, für die Übergangszeit

in der Rspr.[575] erneuten Aufwind erhalten hat – jedenfalls im Grundsatz zugestimmt, wonach die Regelungen der *§§ 100a, 100b StPO* über die Überwachung und Aufzeichnung von Telekommunikation in Verbindung mit entsprechend konkret und präzise ausgestalteten Beschlüssen[576] *grds. eine ausreichende Rechtsgrundlage* für die strafprozessuale Anordnung von Maßnahmen der Quellen-TKÜ darstellen.

Legt man diese Rechtsauffassung zugrunde, so bedarf es für die zulässige Anordnung und Durchführung von Quellen-TKÜ-Maßnahmen keiner ausdrücklichen Normierung der Quellen-TKÜ in der Strafprozessordnung, insbesondere nicht in Form einer eigenständigen Befugnisnorm („§ 100j StPO"). Wie die Untersuchungen zu Modell 2 gezeigt haben, besteht diesbezüglich auch kein Bedürfnis für eine Anlehnung der Voraussetzungen dieser modernen Form der Telekommunikationsüberwachung an den nochmals erhöhten Anforderungsgrad der akustischen Wohnraumüberwachung nach §§ 100c ff. StPO.

Gleichwohl gibt es Anknüpfungspunkte für eine gesetzliche Klarstellung der Quellen-TKÜ in den bestehenden §§ 100a, 100b StPO (vgl. oben zu Punkt I.). Um den Grundsätzen der *Tatbestandsbestimmtheit und Normenklarheit* bei einem zum Zwecke der Überwachung und Aufzeichnung von Telekommunikation auf die Befugnisnormen der §§ 100a, 100b StPO gestützten Einsatz einer Überwachungssoftware auf einem informationstechnischen System im Sinne einer umfassenden und größtmöglichen Rechnungtragung zu begegnen, empfiehlt sich – wenngleich unter Berücksichtigung von Modell 1 für die rechtmäßige Anordnung und Durchführung von Quellen-TKÜ-Maßnahmen de lege lata nicht zwingend notwendig – de lege ferenda eine *Ergänzung der §§ 100a, 100b StPO*, welche bereits auf Gesetzesebene sowohl die Ermittlungs- und Eingriffssituation einer an der Quelle durchgeführten Telekommunikationsüberwachung beschreibt und den (verfassungsrechtlich zulässigen) Eingriffsumfang einer derartigen Überwachungsmaßnahme unter Einsatz technischer Mittel auf informationstechnischen Systemen für die alleinige Grundrechtsbetroffenheit des Art. 10 I GG ausdrücklich hervorhebt, als auch zur gesetzlichen Absicherung einer insge-

---

bis zu einer gesetzlichen Regelung; *Bär*, TK-Überwachung, § 100a StPO, Rn. 32 f.; AG Bayreuth, MMR 2010, 266; LG Hamburg, MMR 2011, 693; insoweit auch LG Landshut, MMR 2011, 690.

575 Nunmehr auch LG Hamburg, Beschluss vom 13.09.2010, Az. 608 Qs 17/10 (MMR 2011, 693) unter Abkehr von der bisher in den „Hamburger Entscheidungen" vertretenen Linie (anders noch LG Hamburg, MMR 2008, 423 und AG Hamburg, CR 2010, 249); ebenso AG Bayreuth, MMR 2010, 266; jüngst insoweit auch LG Landshut, MMR 2011, 690.

576 Für Einzelheiten zur inhaltlichen Ausgestaltung der Anordnung einer Quellen-TKÜ und für einen Beschlussvorschlag, siehe 3. Teil A.I.2. sowie Anhang 1.

samt *verhältnismäßigen technischen Umsetzungsweise* der Maßnahme – neben der rechtlichen Absicherung durch entsprechende Beschlussausgestaltung – eine den (verfassungsrechtlichen) Anforderungen gerecht werdende grundsätzliche technische Einsatzweise des technischen Mittels gesetzlich bestimmt und zur bestmöglichen Gewährleistung der *Gerichtsfestigkeit* und *Beweissicherheit* der über eine Maßnahme der Quellen-TKÜ erlangten Erkenntnisse den hierfür angezeigten Verfahrensablauf bereits auf Gesetzesebene in seinen wesentlichen Eckpunkten vorgibt.

Eine solche gesetzliche Klarstellung würde hierbei nicht nur für das maßnahmeanordnende Organ und die maßnahmedurchführenden Ermittlungspersonen, sondern insbesondere auch für den Bürger als betroffenem Grundrechtsträger im Sinne einer „Optimierung der Rechtslage" insgesamt zu einem Mehr an *Rechtssicherheit*, *Rechtseinheitlichkeit* und *Rechtsklarheit* führen[577] – vermittelt die gegenwärtige Situation doch den Eindruck, dass sich die Normadressaten momentan im Zentrum eines argumentatorischen Wettstreits zweier Lager innerhalb des juristischen Meinungsbildes wiederfinden, die mit divergierenden Sichtweisen und Rechtauffassungen zu einem höchstrichterlich bislang noch nicht abschließend geklärten Ermittlungsinstrument um eine regelrechte „Vorherrschaft der Argumentationsansätze" buhlen. Zur Vermeidung von Unsicherheiten bei der Anwendung dieser modernen Ermittlungsmaßnahme in der Praxis, wäre eine gesetzliche Klarstellung der §§ 100a, 100b StPO jedenfalls im Sinne einer „*integrativen Gesamtlösung*" der Quellen-TKÜ-Problematik durchaus begrüßenswert.

Im Rahmen der nachfolgend zu Modell 3 dargestellten Ergänzungsvorschläge für die §§ 100a und 100b StPO lassen sich die unter Punkt C des 2. Teils herausgearbeiteten Kernfragen der besonderen Ermittlungsmaßnahme der Quellen-TKÜ in sachgerechter und praktikabler Weise berücksichtigen.

2. Ergänzung des § 100a StPO

Für die Frage der konkreten Ausgestaltung einer solchen Ergänzung der bestehenden §§ 100a, 100b StPO de lege ferenda um die Besonderheiten der Überwachung und Aufzeichnung von Telekommunikation unter Zugriff auf zu Telekommunikationszwecken gebrauchte informationstechnische Systeme durch Verwendung einer Überwachungssoftware als spezifischem technischen Mittel zur Realisierung der Maßnahme „an der Quelle" lässt sich

---

577 In diese Richtung auch der Bayerische Landesbeauftragte für den Datenschutz, *Petri*, der sich für „Rechtsklarheit für Bürger, aber auch für die Ermittlungsbehörden" ausspricht, zitiert nach Welt am Sonntag vom 16.10.2011, „Kontrolle in der Grauzone", S. BY 1.

zum einen auf die bislang erfolgte Rspr. des BVerfG[578] zu den verfassungsrechtlichen Anforderungen an eine Quellen-TKÜ anknüpfen. Zum anderen kann hierbei auch auf entsprechende ausdrückliche Regelungen der Quellen-TKÜ in präventiv-polizeilichen Gesetzen[579] wie bspw. in § 20l II BKAG[580] oder § 15b HSOG[581] zurückgegriffen werden.

Hinsichtlich des Bestimmtheitsgebotes ist hierbei allerdings zu beachten, dass Regelungen der Gefahrenabwehr nicht zwingend an denselben Kriterien anknüpfen müssen, wie Regelungen der Strafverfolgung. So setzen präventive Maßnahmen, die in Freiheitsrechte des Bürgers eingreifen, das Bestehen einer konkreten Gefahrenlage voraus. Repressive Maßnahmen hingegen knüpfen an den Verdacht einer schon verwirklichten (bzw. versuchten) Straftat an.[582] Entsprechend dieser Kriterien sind grds. auch die Anforderungen an die Bestimmtheit auszurichten.

Auch wenn es sich bei den jeweiligen Befugnisnormen um Regelungen aus dem präventiven Bereich handelt, gibt deren konkrete Form der Ausgestaltung indes gleichwohl Anhaltspunkte für die im Raum stehenden (verfassungs-)rechtlichen und technischen Aspekte der Quellen-TKÜ, wie sie für den repressiven Bereich in vergleichbarer Weise Geltung beanspruchen. Dies gilt insbesondere in Bezug auf diejenigen Tatbestandselemente, die vergleichbare Standards[583] hinsichtlich Vorhersehbarkeit und Kontrollierbarkeit schaffen.

a) Ergänzungsvorschlag: § 100a II StPO-E

§ 100a StPO-E
[Überwachung der Telekommunikation]

(1) Auch ohne Wissen der Betroffenen darf die Telekommunikation überwacht und aufgezeichnet werden, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in *Absatz 3* bezeichnete schwere Straftat begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht, oder durch eine Straftat vorbereitet hat,

2. die Tat auch im Einzelfall schwer wiegt und

---

578 Vgl. BVerfG NJW 2008, 822 (826).

579 Für Einzelheiten zu präventiv-polizeilichen Rechtsgrundlagen der Quellen-TKÜ, siehe 2. Teil A.I.1.

580 Siehe hierzu auch 2. Teil A.I.1.a).

581 Siehe hierzu auch 2. Teil A.I.1.d).

582 Vgl. BVerfG NJW 2005, 2603 (2607).

583 Hierzu BVerfG NJW 2005, 2603 (2608).

3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

(2) Die Überwachung und Aufzeichnung der Telekommunikation darf auch ohne Wissen des Betroffenen in der Weise erfolgen, dass mit technischen Mitteln in von dem Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn

1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird, und

2. der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen.[584]

(3) Schwere Straftaten im Sinne des Absatzes 1 Nr. 1 sind: (…)

(4) Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, 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 benutzt.

(5) [1]Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach *den Absätzen 1 und 2* allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. [2]Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach *den Absätzen 1 und 2* erlangt wurden, dürfen nicht verwertet werden. [3]Aufzeichnungen hierüber sind unverzüglich zu löschen. [4]Die Tatsache ihrer Erlangung und Löschung ist aktenkundig zu machen.

b) Inhalt und Zweck der Ergänzung

Vorliegendes Modell stellt in der eingefügten Vorschrift des § 100a II StPO-E zunächst klar, dass es sich bei der Überwachung und Aufzeichnung von Telekommunikation unter Zugriff auf hierzu vom Betroffenen genutzte informationstechnische Systeme (Quellen-TKÜ) um eine besondere Weise der nach § 100a I StPO gestatteten Telekommunikationsüberwachung („darf […] in der Weise erfolgen“) handelt.

Als spezifische (verfassungsrechtliche) Anforderung an derartige Maßnahmen hebt Modell 3 unter Berücksichtigung der Feststellungen des BVerfG vom 27.02.2008 zur Differenzierung zwischen Maßnahmen der Quellen-TKÜ und der Online-Durchsuchung in Bezug auf den jeweils einschlägigen Grundrechtsmaßstab die zwingende Bindung des zum Zwecke

---

584 Unter Heranziehung der in § 20l II S. 1 und § 20k II, III BKAG gewählten Formulierungen.

der Überwachung und Aufzeichnung auf dem informationstechnischen System eingesetzten technischen Mittels an laufende Telekommunikationsvorgänge hervor (§ 100a II Nr. 1 StPO-E). Hierbei verweist die Vorschrift darauf, dass die Überwachung und Aufzeichnung ausschließlich laufender Telekommunikation durch technische Maßnahmen sichergestellt sein muss, da gemäß den Aussagen des BVerfG nur dann das Fernmeldegeheimnis aus Art. 10 I GG den alleinigen grundrechtlichen Maßstab darstellt[585].

Da alle Formen der Telekommunikationsüberwachung dem Grundsatz der Verhältnismäßigkeit unterliegen, ist vor jedem Einsatz generell zu prüfen, ob eine Alternative gegeben ist, die bei gleicher Eignung ein grundrechtsschonenderes („milderes") Mittel darstellt.[586] Diesem Umstand trägt Modell 3 bereits auf Gesetzesebene Rechnung, indem es – in besonderer Ausgestaltung des Verhältnismäßigkeitsgrundsatzes – die Vorschrift des § 100a StPO in § 100a II Nr. 2 StPO-E um die Notwendigkeit des Eingriffs in das informationstechnische System zum Zwecke der Überwachung und Aufzeichnung der Telekommunikation ergänzt und zugleich mit der Gewährleistung der Überwachung und Aufzeichnung von Telekommunikation in unverschlüsselter Form den Hauptanwendungsfall der Maßnahme nennt[587], der einen Zugriff auf informationstechnische Systeme („an der Quelle") mit technischen Mitteln zu Zwecken der Telekommunikationsüberwachung erforderlich macht. Hierdurch trägt die Formulierung des § 100a II Nr. 2 StPO-E auch einer größtmöglichen Umsetzung des Bestimmtheitsgebotes Rechnung, da für die Konstellation verschlüsselt übermittelter Telekommunikation Normadressaten konkret erkennen können, aus welchem Anlass und unter welchen Umständen ein solches Telekommunikationsverhalten mit dem Risiko einer staatlichen Überwachung und Aufzeichnung verbunden ist.[588] An das Bestimmtheitsgebot knüpft indes bereits die Formulierung in Halbsatz 1 des § 100a II StPO-E an, wodurch zum Zwecke größtmöglicher Klarheit und Erkennbarkeit für Normadressaten die (technische) Eingriffs- und Ermittlungssituation[589] der Quellen-TKÜ, nämlich dass unter den genannten Voraussetzungen zum Zwecke der Überwachung und Aufzeichnung der Telekommunikation mit *technischen Mitteln* in vom Betroffenen genutzte *informationstechnische Systeme* eingegriffen werden darf, ausdrücklich in den Gesetzestext aufgenommen wird.

---

585 Vgl. BVerfG NJW 2008, 822 (826).

586 So auch die Antwort der Bundesregierung vom 26.10.2011, BT-PlPr. 17/135 16064 C.

587 Vgl. auch BT-Drs. 16/10121, S. 31.

588 Siehe hierzu auch 3. Teil A.I.1.b).

589 Siehe hierzu 3. Teil A.I.1.b).

3. Ergänzung des § 100b StPO

a) Ergänzungsvorschlag: § 100b II S. 2 Nr. 4 StPO-E

§ 100b StPO-E
[Zuständigkeit für Anordnung der Überwachung
der Telekommunikation und Umsetzung]

(1) [1]Maßnahmen nach § 100a *Abs. 1 und 2* dürfen nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden. [2]Bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft getroffen werden. [3]Soweit die Anordnung der Staatsanwaltschaft nicht binnen drei Werktagen von dem Gericht bestätigt wird, tritt sie außer Kraft. [4]Die Anordnung ist auf höchstens drei Monate zu befristen. [5]Eine Verlängerung um jeweils nicht mehr als drei Monate ist zulässig, soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen.

(2) [1]Die Anordnung ergeht schriftlich. [2]In ihrer Entscheidungsformel sind anzugeben:

1. soweit möglich, der Name und die Anschrift des Betroffenen, gegen den sich die Maßnahme richtet,
2. die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgerätes, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist,
3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes, *und*
4. *im Falle des § 100a Abs. 2 auch eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll.*[590]

(3) [1]Auf Grund der Anordnung hat jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt, dem Gericht, der Staatsanwaltschaft und ihren im Polizeidienst tätigen Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) die Maßnahmen nach § 100a *Abs. 1* zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen. [2]Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, bestimmt sich nach dem Telekommunikationsgesetz und der Telekommunikations-Überwachungsverordnung. [3]§ 95 Abs. 2 gilt entsprechend.

---

590 Unter Heranziehung der in § 20l IV S. 1 Nr. 4 BKAG gewählten Formulierung.

b) Ergänzungsvorschlag: § 100b IV StPO-E

(4) *[1]Bei Maßnahmen nach § 100a Abs. 2 ist technisch sicherzustellen, dass*

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und

2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden.

[2]Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. [3]Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen. [4]Von dem Einhalten der technischen Anforderungen des § 100a Abs. 2 Nr. 1 sowie der Sätze 1 bis 3 ist in der Regel auszugehen, wenn ein vom Bundesamt für Sicherheit in der Informationstechnik zertifiziertes technisches Mittel eingesetzt wird. [5]Bei jedem Einsatz des technischen Mittels sind zu protokollieren

1. die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,

2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,

3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und

4. die Organisationseinheit, die die Maßnahme durchführt.

[6]Die Protokolldaten dürfen nur verwendet werden, um dem Betroffenen oder einer dazu befugten öffentlichen Stelle die Prüfung zu ermöglichen, ob die Maßnahme nach § 100a Abs. 2 rechtmäßig durchgeführt worden ist.[591] *[7]Sie sind unverzüglich zu löschen, soweit sie für den in Satz 6 genannten Zweck nicht mehr erforderlich sind.*[592]

(5) [1]Liegen die Voraussetzungen der Anordnung nicht mehr vor, so sind die auf Grund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden. [2]Nach Beendigung der Maßnahme ist das anordnende Gericht über deren Ergebnisse zu unterrichten.

(6) [1]Die Länder und der Generalbundesanwalt berichten dem Bundesamt für Justiz kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres über in ihrem Zuständigkeitsbereich angeordnete Maßnahmen nach § 100a. [2]Das Bundesamt für Justiz erstellt eine Übersicht zu den im Berichtsjahr bundesweit angeordneten Maßnahmen und veröffentlicht diese im Internet.

(7) In den Berichten nach Absatz 6 sind anzugeben:

1. die Anzahl der Verfahren, in denen Maßnahmen nach § 100a Abs. 1 *und Abs. 2* angeordnet worden sind;

---

591 Unter Heranziehung der in § 20l II S. 1 und § 20k II, III BKAG gewählten Formulierungen.

592 Unter Heranziehung der in § 31c IV S. 3 POG RP gewählten Formulierung.

2. die Anzahl der Überwachungsanordnungen nach § 100a Abs. 1 *und Abs. 2*, unterschieden nach
   a) Erst- und Verlängerungsanordnungen sowie
   b) Festnetz-, Mobilfunk- und Internettelekommunikation;
3. die jeweils zugrunde liegende Anlassstraftat nach Maßgabe der Unterteilung in § 100a *Abs. 3.*

c) Inhalt und Zweck der Ergänzung

Bei der Überwachung von Telekommunikation auf informationstechnischen Systemen mit Hilfe technischer Mittel handelt es sich – wie oben im Einzelnen erläutert – um eine spezielle Ermittlungssituation der §§ 100a, 100b StPO. Der Hauptanwendungsfall der Überwachung und Aufzeichnung verschlüsselter VoIP-Kommunikation unter Einsatz einer individuellen Überwachungssoftware im Rahmen der Quellen-TKÜ baut indes auf einem komplexen technischen Überwachungsmittel auf. Zur Gewährleistung wie auch zum Nachweis einer insgesamt verhältnismäßigen Anwendungsweise dieses komplexen technischen Mittels im Rahmen der Umsetzung von Quellen-TKÜ-Maßnahmen empfiehlt es sich – wenn auch mit Blick auf die verbindliche Wirkung entsprechender richterlicher Vorgaben im anordnenden Beschluss[593] für die Zulässigkeit nicht zwingend erforderlich – Vorgaben hinsichtlich der *grundlegenden technischen und organisatorischen Anforderungen*, insbesondere hinsichtlich der erforderlichen technischen Schutzvorkehrungen, der technischen und organisatorischen Verfahrensweise wie auch hinsichtlich der grundlegenden technischen Eigenschaften des technischen Mittels für die Maßnahmedurchführung, bereits in die gesetzliche Ermächtigungsgrundlage mit aufzunehmen, wie dies bspw. für die Umsetzung von TKÜ-Maßnahmen unter Inpflichtnahme der nach § 3 I S. 1 TKÜV verpflichteten Betreiber von Telekommunikationsanlagen (§ 2 Nr. 4 TKÜV), mit denen Telekommunikationsdienste für die Öffentlichkeit[594] erbracht werden, in der TKÜV in den §§ 6 ff., teilw. i. V. m. mit der technischen Richtlinie nach § 11 S. 1 TKÜV (TR TKÜV[595]) näher konkretisiert ist.

---

[593] Für Einzelheiten zur inhaltlichen Ausgestaltung eines Quellen-TKÜ-Beschlusses, siehe 3. Teil A.I.2.; für einen Beschlussvorschlag, siehe Anhang 1.

[594] Zur Vereinheitlichung mit der Bezeichnung in den Richtlinienvorgaben spricht das TKG in neuer Terminologie mittlerweile statt von Telekommunikationsdiensten „für die Öffentlichkeit" von „öffentlich zugänglichen" Telekommunikationsdiensten, vgl. § 110 I S. 1, S. 2 TKG i.d. ab dem 10.05.2012 geltenden Fassung (BGBl. I S. 958); eine inhaltliche Änderung ist mit der neuen Begriffswahl indes nicht verbunden, vgl. BT-Drs. 17/5707, S. 91, 50.

[595] Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation und zum Auskunftersuchen für Verkehrsdaten, abruf-

Hinsichtlich der nach § 100b II S. 2 StPO in die Entscheidungsformel der schriftlichen Anordnung zwingend aufzunehmenden Angaben ist als weitere Angaben für die Fälle der Überwachung und Aufzeichnung von Telekommunikation unter Eingriff in informationstechnische Systeme mit Hilfe technischer Mittel nach § 100a II StPO-E (Quellen-TKÜ) zur Sicherstellung eines zielgerichteten Eingriffs in das zur Telekommunikation genutzte informationstechnische System durch bestmögliche Konkretisierung der Eingriffsumstände im Rahmen präziser Beschlüsse gemäß § 100b II S. 2 Nr. 4 StPO-E auch eine möglichst genaue Bezeichnung des betroffenen informationstechnischen Systems (z. B. Geräteart, Gerätekennung/Seriennummer, Betriebssystem/-version u. ä.) vorzunehmen.

Ähnlich wie in den §§ 6 ff. TKÜV für die nach § 3 I S. 1 TKÜV zur Umsetzung von TKÜ-Maßnahmen verpflichteten Betreiber von Telekommunikationsanlagen (§ 2 Nr. 4 TKÜV), mit denen Telekommunikationsdienste für die Öffentlichkeit erbracht werden, regelt auch § 100b IV StPO-E grundlegende *technische Anforderungen* an die Umsetzung des Zugriffs auf das informationstechnische System im Rahmen von Quellen-TKÜ-Maßnahmen und die notwendige Konfiguration und Funktionsweise des hierfür zum Einsatz kommenden technischen Mittels.

Neben der technischen Sicherstellung einer ausschließlichen Erfassung laufender Telekommunikation (§ 100a II Nr. 1 StPO-E) im Rahmen der Überwachung „an der Quelle", sind für eine entsprechende Begrenzung des Eingriffs in das infiltrierte informationstechnische System auf das hierfür zwingend erforderliche Mindestmaß sowie zur Gewährleistung der Datensicherheit von den Ermittlungsbehörden gemäß § 100b IV S. 1–S. 3 StPO-E bei der Maßnahmedurchführung bestimmte weitere Schutzvorkehrungen technischer Art zu treffen[596]:

Die Vorschrift des § 100b IV S. 1 Nr. 1 StPO-E bestimmt hierfür, dass beim Einsatz des technischen Mittels (Überwachungssoftware) durch entsprechende technische Vorkehrungen sicherzustellen ist, dass an dem betroffenen informationstechnischen System bei Durchführung der Maßnahme nach § 100a II, I StPO-E nur Veränderungen dergestalt vorgenommen werden, die für die Datenerhebung aus laufenden Telekommunikationsvorgängen unerlässlich, sprich unbedingt erforderlich sind.[597] Hierbei sind nicht nur die von dem Nutzer des betroffenen informationstechnischen Systems angelegten

---

bar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/TechnischeRegulierung/TechnischeUmsetzungUeberwachung/Downloads/02_01DETRTKUEV61vom05012012pdf.pdf?__blob=publicationFile (zuletzt aufgerufen 15.06.2012).

596 Vgl. auch BT-Drs. 16/10121, S. 29 zu § 20k II BKAG.

597 Vgl. BT-Drs. 16/10121, S. 29 zu § 20k II BKAG.

Anwenderdateien vor einer nicht unbedingt erforderlichen Veränderung zu schützen, sondern auch die für die Funktionsfähigkeit des informationstechnischen Systems notwendigen Systemdateien.[598] Zudem sind auch Beeinträchtigungen der Systemleistung auf Grund des Einsatzes des technischen Mittels auf das technisch unvermeidbare Maß zu begrenzen.[599] Zum Zwecke des erleichterten Nachweises dafür, dass die technischen Anforderungen nach § 100b IV S. 1 Nr. 1 StPO-E eingehalten worden sind, empfiehlt es sich, das technische Mittel – bei der Quellen-TKÜ in Gestalt der Überwachungssoftware, welche auf dem informationstechnischen System zu Einsatz kommt – mit einer elektronischen Signatur zu versehen, über die sich das technische Mittel wie auch dessen Funktionsumfang identifizieren lässt.[600]

Des Weiteren sieht die Vorschrift des § 100b IV S. 1 Nr. 2 StPO-E vor, dass bei Beendigung der Quellen-TKÜ-Maßnahme zum Schutz der Systemintegrität alle an dem infiltrierten System vorgenommenen Veränderungen – soweit technisch möglich – rückgängig zu machen sind.[601] Dies umfasst insbesondere die vollständige Löschung der auf dem informationstechnischen System installierten Überwachungssoftware und die Rückgängigmachung der Veränderungen an den bei Installation der Überwachungssoftware vorgefundenen Systemdateien. Hierbei sind im Interesse einer zuverlässigen und einfachen Abwicklung die vorgenommenen Veränderungen grundsätzlich, d. h. soweit technisch möglich automatisiert, andernfalls manuell rückgängig zu machen.[602]

In Anlehnung an § 14 I TKÜV enthält die Regelung des § 100b IV S. 2 StPO-E eine entsprechende Verpflichtung zum Schutz des eingesetzten technischen Mittels gegen unbefugte Nutzung, welcher nach dem Stand der Technik zu erfolgen hat. Hierzu haben die Ermittlungsbehörden – durch entsprechende technische, ggf. auch organisatorische Vorkehrungen – insbesondere dafür Sorge zu tragen, dass die eingesetzte Überwachungssoftware nicht durch Dritte wie bspw. Hacker zweckentfremdet werden kann.[603] Um nicht zuletzt auch den im Zuge der Veröffentlichung einer sog. „Regierungs-Malware“[604] durch den *Chaos Computer Club* im Herbst 2011 verstärkt

---

598 Vgl. BT-Drs. 16/10121, S. 29 zu § 20k II BKAG.

599 Vgl. BT-Drs. 16/10121, S. 29 zu § 20k II BKAG.

600 Vgl. insoweit LT RP-Drs. 15/4879, S. 37, 38 zu § 31c II POG RP.

601 Vgl. BT-Drs. 16/10121, S. 29 zu § 20k II BKAG.

602 Vgl. BT-Drs. 16/10121, S. 29 zu § 20k II BKAG sowie LT RP-Drs. 15/4879, S. 37 zu § 31c II POG RP.

603 Vgl. auch BT-Drs. 16/10121, S. 29 zu § 20k II BKAG.

604 Bericht „Analyse einer Regierungs-Malware“ vom 08.10.2011, abrufbar unter http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf (zuletzt aufgerufen 15.06.2012).

geäußerten Bedenken hinsichtlich möglicher Risiken einer missbräuchlichen Erlangung und Ingebrauchnahme von staatlicher Überwachungssoftware Rechnung zu tragen, ist auf Grund dieser Vorschrift sicherzustellen, dass die Überwachungssoftware seitens Unbefugter weder erkannt noch angesprochen werden kann und insbesondere dafür Sorge zu tragen, dass die Überwachungssoftware nicht, bzw. – mit Blick auf den Umstand, dass sich gerade bei Software nie eine zu 100 Prozent „knacksichere" Lösung programmieren lässt und von staatlichen Behörden insoweit auch nichts Unmögliches verlangt werden kann – jedenfalls nicht ohne einen erheblichen Aufwand von Unbefugten dazu veranlasst werden kann, an einen anderen Server als den von der Ermittlungsbehörde genutzten, zurückzumelden.[605] Gemäß der Vorgabe in § 100b IV S. 2 StPO-E, wonach das eingesetzte Mittel „nach dem Stand der Technik" gegen unbefugte Nutzung zu schützen ist, haben die Ermittlungsbehörden sich hierbei fortschrittlicher technischer Verfahren zu bedienen, welche auf gesicherten Erkenntnissen von Wissenschaft und Technik basieren.[606] Insbesondere ist hierfür der Entwicklungsstand fortschrittlicher technischer Verfahren zur Software-, Daten- und Systemsicherheit (bspw. proprietäre Protokolle, Verschlüsselung nach dem *Advanced Encryption Standard* etc.) heranzuziehen, der die praktische Eignung gegen unbefugte Nutzung als gesichert erscheinen lässt.[607] Hierfür bedarf es regelmäßig auch einer umfassenden und sorgfältigen Beobachtung und Auswertung der einschlägigen Aktivitäten auf den Gebieten der Technik.[608] Bei der Bestimmung des Stands der Technik sind insbesondere vergleichbare Verfahren zur Software und Datensicherheit zu berücksichtigen, die mit Erfolg in der Praxis erprobt worden sind. Nicht angemessen und mit dem Strafverfolgungsinteresse schwerlich vereinbar wäre hingegen eine Verpflichtung zum Heranziehen solcher technischer Verfahren, „die nach Auffassung führender Fachleute aus Wissenschaft und Technik auf der Grundlage neuester wissenschaftlicher Erkenntnisse"[609] angezeigt sind.[610] Durch die Maß-

---

605 Vgl. auch BT-Drs. 16/10121, S. 29 zu § 20k II BKAG.

606 Vgl. LT RP-Drs. 15/4879, S. 37 zu § 31c II POG RP.

607 In Anlehnung an entsprechende Legaldefinitionen in § 3 VI Bundesimmissionsschutzgesetz oder in § 2 XI Gefahrstoffverordnung.

608 Vgl. BT-Drs. 16/10121, S. 29 zu § 20k II BKAG.

609 BT-Drs. 16/10121, S. 29; so ursprünglich in der Gesetzesbegründung zu § 20k II BKAG enthalten, in die Endfassung aber nicht übernommen.

610 Ein Anknüpfen am „Stand der Technik" ist insgesamt sachgerecht, praktikabel und unter Abwägung mit dem Strafverfolgungsinteresse angemessen; dies steht auch in Einklang mit den Feststellungen des BVerfG im Rahmen der verfassungsrechtlichen Bewertung der Vorschriften zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten (BVerfG NJW 2010, 833), wonach „die Verfassung […] nicht detailgenau vor[gibt], welche Sicherheitsmaßgaben im Einzelnen geboten sind" (840), „im Ergebnis […] jedoch ein Standard gewährleistet werden [muss], der unter

gabe „Stand der Technik“ lässt sich ein Schutzniveau erreichen, welches auch den Schutzanforderungen des § 14 I TKÜV für „herkömmliche“ TKÜ-Maßnahmen entspricht.[611]

Angelehnt an die Regelung des § 14 II S. 1 TKÜV bezweckt § 100b IV S. 3 StPO-E den Schutz der Authentizität, der Vollständigkeit bzw. Unveränderheit und der Vertraulichkeit der unter Verwendung des technischen Mittels abgefangenen Daten aus laufenden Telekommunikationsvorgängen, indem die Vorschrift dazu verpflichtet, erlangte Daten nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen. Hierfür sind regelmäßig umfassende technische Verschlüsselungsweisen, elektronische Signaturen u. ä. heranzuziehen.[612] Die Verpflichtung gilt vom Zeitpunkt des Abgreifens der Datensignale auf dem informationstechnischen Systeme an, während deren Ausleitung und Übermittlung an den/die Behörden-Server über paketvermittelte Netze sowie während der Speicherung der kopierten Daten bei der Ermittlungsbehörde. Nach ihrer verschlüsselten Übertragung an die Ermittlungsbehörde sind die kopierten Daten beweissicher und zugriffsgeschützt bei der Behörde zu speichern. Hierfür empfiehlt es sich die Daten insbesondere mit elektronischen Signaturen sowie elektronischen Zeitstempeln zu versehen.[613] Dies trägt einerseits dem Interesse des von der Maßnahmen Betroffenen Rechnung, dass die auf dem Zielsystem während eines laufenden Telekommunikationsvorgangs abgegriffenen Telekommunikationsdaten nachträglich nicht – zufällig oder bewusst – verändert werden oder unbefugten Personen zur Kenntnis gelangen, andererseits wird auch dem staatlichen Interesse an größtmöglicher Beweissicherheit durch Beweismittelauthentizität und -integrität bezüglich der gewonnenen Erkenntnisse genüge getan.[614]

Des Weiteren empfiehlt es sich – insbesondere mit Blick auf die Nachprüfbarkeit der Maßnahme – hinsichtlich der technischen Anforderungen an die Veränderungen am Zielsystem und deren Rückgängigmachung bei Beendigung der Maßnahme (§ 100b IV S. 1 StPO-E), an den Schutz der eingesetzten Mittel gegen unbefugte Benutzung (§ 100b IV S. 2 StPO-E) sowie an den Schutz der erlangten Daten gegen Veränderung, unbefugte Löschung

---

spezifischer Berücksichtigung der Besonderheiten der […] geschaffenen Datenbestände ein besonders hohes Maß an Sicherheit gewährleistet“ (840), wobei „sicherzustellen [ist], dass sich dieser Standard – etwa unter Rückgriff auf einfachgesetzliche Rechtsfiguren wie den Stand der Technik […] – an dem Entwicklungsstand der Fachdiskussion orientiert und neue Erkenntnisse und Einsichten fortlaufend aufnimmt“ (840).

611 Vgl. LT RP-Drs. 15/4879, S. 37 zu § 31c II POG RP.

612 Vgl. auch BT-Drs. 16/10121, S. 29 zu § 20k II BKAG.

613 Vgl. BT-Drs. 16/10121, S. 29 zu § 20k II BKAG.

614 Vgl. BT-Drs. 16/10121, S. 29 zu § 20k II BKAG.

und unbefugte Kenntnisnahme (§ 100b IV S. 3 StPO-E) auf von Fachstellen entsprechend geprüfte und „freigegebene" Überwachungssoftware zurückzugreifen und damit – soweit technisch möglich – einheitlich technische Maßstäbe in der Praxis zu verankern. Die Vorschrift des § 100b IV S. 4 StPO-E sieht daher vor, dass von einem Einhalten der technischen Anforderungen des § 100a II Nr. 1 StPO-E (Überwachen und Aufzeichnen ausschließlich laufender Telekommunikation) sowie der Sätze 1 bis 3 des § 100b IV StPO-E in der Regel auszugehen ist, wenn ein vom Bundesamt für Sicherheit in der Informationstechnik zertifiziertes technisches Mittel eingesetzt wird. Die Berücksichtigung der Zertifizierungsmöglichkeit der Überwachungssoftware im Gesetz unter Einbindung des BSI[615] (vgl. § 9 BSIG, § 2 VII BSIG) kommt der mit Bekanntwerden einer „Regierungs-Malware"[616] im Herbst 2011 vielfach geäußerten Forderung nach der Bindung von staatlicher Überwachungssoftware an die vorherige Prüfung durch unabhängige Experten im Rahmen von Zertifizierungsverfahren („Staatstrojaner-TÜV"), mit denen die in Einklang mit den verfassungsgerichtlichen Feststellungen[617] stehende Konfiguration der Software – jedenfalls hinsichtlich der grundsätzlichen, nicht auf den Einzelfall zugeschnittenen Softwarebestandteile – entsprechend bescheinigt wird[618], entgegen. Die Verankerung einer *gesetzlichen Regelvermutung* („in der Regel") trägt hierbei dem Umstand Rechnung, dass den Ermittlungsbehörden bei Verwenden zertifizierter Überwachungssoftware ein erleichterter Nachweis für das Einhalten der gesetzlichen sowie richterlichen Vorgaben zur Seite steht. Dies wird sowohl dem Interesse der Ermittlungsbehörden wie auch dem des Betroffenen gerecht, da die gesetzliche Vermutung bei Verwenden einer zertifizierten Software zunächst zugunsten der Rechtmäßigkeit, insbesondere der Verhältnismäßigkeit des technischen Eingriffs im Rahmen der Maßnahmedurchführung wirkt, die Vermutung aber auch widerlegt werden kann,

---

615 Gemäß § 3 Nr. 13 lit. a BSIG zählt zu den Aufgaben des BSI insbesondere auch die Unterstützung der Polizeien und Strafverfolgungsbehörden bei der Wahrnehmung ihrer gesetzlichen Aufgaben.

616 Bericht „Analyse einer Regierungs-Malware" des *Chaos Computer Clubs* vom 08.10.2011, abrufbar unter http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf (zuletzt aufgerufen 15.06.2012).

617 BVerfG NJW 2008, 822 (826).

618 In diese Richtung auch der Vorsitzende der Deutschen Polizeigewerkschaft, *Wendt*, in der Neuen Osnabrücker Zeitung vom 11.10.2011, abrufbar unter http://www.noz.de/deutschland-und-welt/gut-zu-wissen/computer/57839915/bayern-wegen-trojaner-einsatzes-unter-druck (zuletzt aufgerufen 15.06.2012); ebenso der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, *Schaar*, sowie die Bundesministerin der Justiz, *Leutheusser-Schnarrenberger*, nach *Höll*, „‚Gefährliche Grauzone'", Süddeutsche Zeitung vom 13.10.2011, S. 6; in diese Richtung bereits Anm. *Vogel*/*Brodowski*, StV 2009, 632 (634).

falls im Einzelfall bspw. eine Software verwendet worden sein sollte, die trotz Zertifizierung nicht die gesetzlich vorgeschriebenen technischen Anforderungen erfüllt hat. Unter Berücksichtigung des Umstand, dass es bislang nicht „den Staatstrojaner" gibt, sondern jeweils eine auf das konkrete technische Zielsystem individuell zugeschnittene Überwachungssoftware zum Einsatz kommt, schließt eine solche Lösung für Ermittlungsbehörden im Einzelfall – je nach Dringlichkeit, Erforderlichkeit und konkreter technischer Ausgangssituation – zudem aber auch künftig nicht aus, eigenen Überwachungssoftware zu erstellen und zu verwenden, bei der dann allerdings die Darlegung und der Nachweis des Einhalten der technischen und rechtlichen Anforderungen im Zweifelsfalle erhöhten Anforderungen und ggf. erschwerten Bedingungen unterliegt.

Zur Gewährleistung effektiven Grundrechts- sowie Datenschutzes, zur besseren Nachweisbarkeit der ausschließlichen Erfassung von Daten aus laufenden Telekommunikationsvorgängen als auch zur rechtlichen Absicherung der Gerichts- und Revisionsfestigkeit der gewonnenen Daten als Beweismittel[619] werden mit der Vorschrift des § 100b IV S. 5 StPO-E zusätzlich Regelungen zur *Protokollierung des Einsatzes des technischen Mittels* gesetzlich verankert. Auch hierfür lässt sich auf entsprechende Regelungen aus präventivpolizeilichen Normierungen der Quellen-TKÜ-Maßnahme (vgl. § 20l II S. 2 i. V. m. § 20k III BKAG; § 15b III HSOG; § 31 III S. 2 i. V. m. § 31c IV POG RP) zurückgreifen. Zwar sind an strafprozessuale Maßnahmen mit Blick auf die Revisionsfestigkeit erlangter Erkenntnisse grds. gesteigerte Anforderungen an die Beweismittelauthentizität und -integrität aufgezeichneter Telekommunikationsvorgänge zu stellen als dies schon für Maßnahmen im präventiven Bereich gilt. Jedoch heißt das nicht, dass die getroffenen Regelungen über die Protokollierung des Einsatzes des technischen Mittels (Überwachungssoftware) in den präventiv-polizeilichen Gesetzen diesen gesteigerten Anforderungen im repressiven Bereich nicht gerecht werden, da diese ein hohes Maß an – nach dem Stand der Technik möglichen – Protokollierungsvorgaben zur Sicherstellung einer nachprüfbaren Dokumentation und Zuordenbarkeit erlangter Erkenntnisse in Bezug auf die relevante(n) Frage(n) „*Wer welche Daten auf welchem informationstechnischen System wem zuordenbar mit welchem technischen Mittel wann erhoben hat*". Auch hierbei gilt es wieder zu beachten, dass von den Ermittlungsbehörden – gerade auch mit Blick auf den verfassungsrechtlich verankerten Strafanspruch – nichts (technisch) Unmögliches bzw. hinsichtlich der Effizienz staatlicher Ermittlungstätigkeit nichts Unzumutbares verlangt werden kann.[620] Vielmehr ist diesbe-

---

619 Vgl. insoweit BT-Drs. 16/10121, S. 30 zu § 20k III BKAG.

620 Auch im Vergleich zu sonstigen Ermittlungsmaßnahmen der StPO wie auch den Regeln zur richterlichen Beweiswürdigung ist eine einhundertprozentige, völlig

züglich – nicht mehr, aber auch nicht weniger – ebenfalls ein Standard zu verlangen, der dem jeweils geltenden Stand der Technik entspricht.[621] Diesen Anforderungen werden die herangezogenen Protokollierungsvorschriften insgesamt gerecht. So ermöglicht hierbei die Protokollierung nach § 100b IV S. 5 Nr. 1–4 StPO-E insbesondere den Nachweis dafür, dass die – auf Grund der Angaben im Protokoll festgestellten (§ 100b IV S. 5 Nr. 3 StPO-E) – Daten, welche von der im Protokoll vermerkten durchführenden Organisationseinheit der jeweiligen Ermittlungsbehörde (§ 100b IV S. 5 Nr. 4 StPO-E) mit der bezeichneten Überwachungssoftware im dokumentierten Überwachungszeitraum (§ 100b IV S. 5 Nr. 1 StPO-E) gewonnenen wurden, tatsächlich von dem – auf Grund der Angaben im Protokoll identifizierten (§ 100b IV S. 5 Nr. 2 StPO-E) – überwachten informationstechnischen System stammen, vollständig vorliegen und nicht verändert wurden[622], d. h. als Beweismittel authentisch sind:

Nach § 100b IV S. 5 Nr. 1 StPO-E sind zunächst die Bezeichnung des verwendeten technischen Mittels und der Zeitpunkt seines Einsatzes zu protokollieren. Hierzu zählt insbesondere die Versionsbezeichnung der verwendeten Überwachungssoftware einer Quellen-TKÜ.[623] Zur Bezeichnung der im Rahmen einer Quellen-TKÜ zum Einsatz kommenden Überwachungssoftware bedarf es indes keiner dezidierten Beschreibung der Software in all ihren technischen Details[624]. Es genügt vielmehr eine allge-

---

von Umständen des Einzelfalls losgelöste Beweissicherheit gewonnener Erkenntnisse kaum möglich und auch nicht einforderbar (Gedanke d. *impossibilium nulla obligatio est*), sondern vielmehr ein Verfahren gemäß den technischen Standards sowie eine Beweiswürdigung durch das erkennende Gericht nach dessen freier, aus dem Inbegriff der Verhandlung geschöpfter Überzeugung (§ 261 StPO), welche nicht zu 100 Prozent bestehen muss, sondern auf der Grundlage eines „nach der Lebenserfahrung ausreichende[n] Maß[es] an Sicherheit“ (BGH NStZ 1988, 236, 237; st. Rspr.).

621 Dies steht auch in Einklang mit den Feststellungen des BVerfG im Rahmen der verfassungsrechtlichen Bewertung der Vorschriften zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten (BVerfG NJW 2010, 833), wonach „die Verfassung […] nicht detailgenau vor[gibt], welche Sicherheitsmaßgaben im Einzelnen geboten sind“ (840), „im Ergebnis […] jedoch ein Standard gewährleistet werden [muss], der unter spezifischer Berücksichtigung der Besonderheiten der […] geschaffenen Datenbestände ein besonders hohes Maß an Sicherheit gewährleistet“ (840), wobei „sicherzustellen [ist], dass sich dieser Standard – etwa unter Rückgriff auf einfachgesetzliche Rechtsfiguren wie den Stand der Technik […] – an dem Entwicklungsstand der Fachdiskussion orientiert und neue Erkenntnisse und Einsichten fortlaufend aufnimmt“ (840).

622 Vgl. insoweit auch BT-Drs. 16/10121, S. 30 zu § 20k III BKAG.

623 Vgl. insoweit LT RP-Drs. 15/4879, S. 38 zu § 31c IV POG RP.

624 Wobei dennoch zu empfehlen ist, auch eine Kopie der verwendeten Überwachungssoftware beweissicher aufzubewahren bzw. die Software – soweit bei Antrag-

meinverständliche Dokumentation der Art des technischen Mittels sowie des Funktionsumfangs, sodass es einem erkennenden Gericht oder dem von der Maßnahmen Betroffenen möglich ist zu beurteilen, ob die in der Anordnung bestimmten Vorgaben hinsichtlich Art und Umfang der Überwachungsmaßnahme (§ 100b II S. 2 Nr. 3 StPO) eingehalten worden sind.[625] Hierunter fällt insbesondere auch die Dokumentation der Prüfsummen der elektronischen Signatur, mit der bspw. die eingesetzte Überwachungssoftware zum Nachweis der Sicherstellung der technischen Anforderungen nach § 100b IV S. 1 Nr. 1 StPO-E versehen worden ist (vgl. oben).[626]

Zum besseren Nachweis dafür, dass es sich bei den erlangten Daten um Daten aus laufenden Telekommunikationsvorgängen handelt, welche über das informationstechnische System geführt wurden, dessen Überwachung angeordnet wurde, sind nach § 100b IV S. 5 Nr. 2 StPO-E des Weiteren Angaben zur Identifizierung des infiltrierten informationstechnischen Systems zu protokollieren. Auf Grund des Umstandes, dass kein solitäres Merkmal ein informationstechnisches System eindeutig identifiziert, bedarf es zur konkreten Bezeichnung und Individualisierung des informationstechnischen Systems einer Dokumentation all derjenigen Informationen über die Hard- und Software des Zielsystems, welche das informationstechnische System, in das zur Datenerhebung eingegriffen werden soll, möglichst so genau beschreiben, dass keine ernstzunehmenden Zweifel daran bestehen können, dass es sich bei dem Gegenstand der Maßnahme tatsächlich um das in der Anordnung nach § 100b II S. 2 Nr. 4 StPO-E bezeichnete System handelte.[627] Des Weiteren schreibt § 100b IV S. 5 Nr. 2 StPO-E die Dokumentation aller an dem betroffenen informationstechnischen System im Zuge des Einsatzes des technischen Mittels vorgenommenen Veränderungen vor. Auf Grund des Umstandes, dass „jede aktive Software permanent eine Fülle vorübergehender Veränderungen des IT-Systems vornimmt, die für die Revisionssicherheit irrelevant sind und vielfach schon nach kurzer Zeit (z. B. beim vollständigen Herunterfahren des PC) automatisiert gelöscht werden“[628], sind jedoch flüchtige Veränderungen von der Protokollierungspflicht des § 100b IV S. 5 Nr. 2 StPO-E ausgenommen. Als flüchtige Veränderungen sind allerdings nur solche Veränderungen anzusehen, die im Arbeitsspeicher (RAM) und damit nur temporär gespeichert werden. Nach

---

stellung bereits vorhanden – zusammen mit dem Antrag vorzulegen und ggf. diese bei Gericht auch zu hinterlegen.

625 Vgl. BT-Drs. 16/10121, S. 30 zu § 20k III BKAG.

626 Vgl. insoweit LT RP-Drs. 15/4879, S. 37, 38 zu § 31c IV POG RP.

627 Vgl. BT-Drs. 16/10121, S. 30 zu § 20k III BKAG.

628 BT-Drs. 16/10121, S. 30 zu § 20k III BKAG.

dem ausdrücklichen Willen des Gesetzgeber ist der Begriff der *flüchtigen Veränderungen* hierbei entsprechend eng auszulegen.[629]

Des Weiteren sind nach § 100b IV S. 5 Nr. 3 StPO-E Angaben, die die Feststellung der erhobenen Daten ermöglichen, zu protokollieren. Von der Dokumentationspflicht erfasst sind damit allerdings nicht die aus der Überwachung und Aufzeichnung von laufenden Telekommunikationsvorgängen gewonnenen Daten selbst, sondern vielmehr nur solche Daten, die Zusatzinformationen zu deren Eigenschaften enthalten[630] und damit genauere bzw. zuverlässige Rückschlüsse auf die erlangten Telekommunikationsdaten zulassen (sog. *Metadaten*)[631]. Bezogen auf den Bereich der Telekommunikationsdaten handelt es sich bei solchen Metadaten um Dateiinformationen/-eigenschaften wie bspw. Gegenstand der Aufzeichnung (laufendes Internettelefonat), Gesprächszeitpunkt, Gesprächsdauer, verwendete VoIP-Software, Länge und Dateigröße der Aufzeichnung, Dateiart (Audiodatei/Videodatei) u. ä., die zugunsten der Beweissicherheit und Gerichtsfestigkeit wie auch zur besseren Nachweisbarkeit, dass kein Zugriff auf sonstige Daten, d. h. kein Eingriff von der Qualität einer Online-Durchsuchung stattgefunden hat[632], eine Feststellung der erhobenen Telekommunikationsdaten ermöglichen. Rückschlüsse auf die jeweiligen konkreten Inhalte der erhobenen Daten dürfen derart protokollierte Metadaten indes nicht zulassen.[633]

Abschließend verlangt § 100b IV S. 5 Nr. 4 StPO-E auch die Dokumentation derjenigen Organisationseinheiten, die die Maßnahme durchführen.

Die in § 100b IV S. 6 StPO-E enthaltenen gesetzlichen Regelungen zur Verwendung der nach § 100b IV S. 5 StPO-E vorzuhaltenden Protokolldaten binden diese streng an den Zweck der (Nach-)Prüfung der Rechtmäßigkeit der durchgeführten Maßnahme durch eine dazu befugte Behörde (z. B. Rechtsaufsichtsbehörde, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit[634]), durch ein dazu befugtes Gericht oder durch den Betroffenen – sei es für letzteren im Rahmen eines Auskunftsanspruchs[635] (§ 491 I S. 1 StPO i. V. m § 19 BDSG entspr.) wie auch im Rahmen der Inanspruchnahme nachträglichen Rechtsschutzes nach § 101 VII S. 2 StPO.

Gemäß den gesetzlichen Regelungen zur Aufbewahrung und Löschung der Protokolldaten nach § 100b IV S. 7 StPO-E dürfen diese nur für den in

---

629 Vgl. BT-Drs. 16/10121, S. 30 zu § 20k III BKAG.

630 Vgl. *Köhler*/*Kirchmann*, IT von A bis Z, S. 149.

631 Vgl. insoweit auch BT-Drs. 16/10121, S. 30 zu § 20k III BKAG.

632 Für Einzelheiten zur Online-Durchsuchung in Abgrenzung zur Quellen-TKÜ, siehe 1. Teil A.II.2.a).

633 Vgl. LT RP-Drs. 15/4879, S. 38 zu § 31c IV POG RP.

634 Vgl. BT-Drs. 16/10121, S. 30 zu § 20k III BKAG.

635 Vgl. insoweit BT-Drs. 16/10121, S. 30 zu § 20k III BKAG.

§ 100b IV S. 6 StPO-E genannten Zweck der Überprüfung der rechtmäßigen Durchführung der Maßnahme aufbewahrt werden und sind unverzüglich zu löschen, soweit sie hierfür nicht mehr erforderlich sind. Die Verankerung einer gesetzlich festgelegten (fixen) Aufbewahrungsfrist erscheint – gerade mit Blick auf die mitunter sehr lange Dauer strafprozessualer Ermittlungsverfahren bei der Verfolgung schwerer Straftaten i. S. d. Kataloges in § 100a StPO – wenig sachgerecht, da eine solche den Anforderungen des Einzelfalls nicht stets Rechnung tragen würde. Über den Verzicht auf eine gesetzlich vorgegebene Aufbewahrungsfrist lässt sich deshalb sicherstellen, dass die Protokolldaten bei einer späteren Überprüfung der Rechtmäßigkeit der Durchführung der strafprozessualen heimlichen Ermittlungsmaßnahme auch tatsächlich vorhanden sind.[636] Die Löschung der Protokolldaten bestimmt sich dann allein danach, ob diese für den in § 100b IV S. 6 StPO-E genannten Zweck nicht mehr erforderlich sind.

Alternativ wäre es aber ebenso vertretbar, die Aufbewahrung bis zur automatisierten Löschung von einer gesetzlich festgelegten Aufbewahrungsfrist abhängig zu machen – wie dies bspw. der Gesetzgeber für die Regelung in § 20k III S. 3 BKAG festgelegt hat –, wenn man die festgelegte Frist als ausreichend ansieht, um bei Bedarf eine Überprüfung der Rechtmäßigkeit einzuleiten. In Anlehnung an die Regelung in § 20k III S. 3 BKAG wären die Protokolldaten dann bis zum Ablauf des auf die Speicherung folgenden Kalenderjahres aufzubewahren und anschließend – grds. unverzüglich[637] – zu löschen, es sei denn, dass sie noch für den in § 100b IV S. 6 StPO-E genannten Zweck der Prüfung der rechtmäßigen Durchführung der Quellen-TKÜ-Maßnahme erforderlich sind. Für die Löschung der Protokolldaten nach Ablauf der Aufbewahrungsfrist empfiehlt sich unter Zweckmäßigkeitsgesichtspunkten das Festlegen einer automatisierten Durchführung, bspw. durch Einrichten einer Löschroutine. Für bereits eingeleitete Verfahren i. S. d. § 100b IV S. 6 StPO-E, in denen die Rechtmäßigkeit der Maßnahme entscheidungsrelevant ist, wären die Protokolldaten somit über die Löschfrist des § 100b IV S. 7 StPO-E hinaus zu speichern.[638]

4. Zusätzliche Normierung eines Betretungsrechts?

Wie die Ausführungen in Teil 2 der Arbeit zur Frage der Grundrechtsrelevanz einzelner Vorgehensweisen zum Installieren bzw. Deinstallieren der Überwachungssoftware gezeigt haben, besteht – verfassungsrechtlich wie

---

636 Vgl. insoweit auch LT RP-Drs. 15/4879, S. 38 zu § 31c IV POG RP.

637 Vgl. insoweit auch BT-Drs. 16/10121, S. 30 zu § 20k III BKAG.

638 Vgl. BT-Drs. 16/10121, S. 30 zu § 20k III BKAG.

einfachgesetzlich – für ein heimliches Betreten von Wohnräumen unter Eingriff in Art. 13 I GG gegenwärtig kein *Betretungsrecht*.[639]

Für die Verankerung eines solchen Betretungsrechts wird mitunter insoweit Bedarf gesehen[640], als das gegenwärtig gehandhabte Einbringen der Überwachungssoftware aus der Ferne über das Datennetz oder außerhalb von Art. 13 I GG geschützten Räumen bzw. ohne Eingriff in Art. 13 I GG (Betreten mit Einverständnis des Betroffenen bspw. unter einem Vorwand) sich je nach Einzelfall schwierig gestalten kann bzw. oftmals auch von zufälligen Gegebenheiten abhängt.

Voraussetzung für die Verankerung eines Betretungsrechts für direkte physische Zugriffe auf informationstechnische Systeme ist freilich zunächst eine entsprechende politische Willensbildung hierzu.[641]

Da sich das Betreten zum Zwecke des direkten physischen Infiltrierens informationstechnischer Systeme auf keine der in Art. 13 GG enthaltenen Schranken verfassungsrechtlich stützen lässt[642], wie dies bspw. für ein Betreten von Wohnräumen zum Zwecke der Realisierung von Maßnahmen der akustischen Wohnraumüberwachung nach §§ 100c ff. StPO auf Grundlage des Art. 13 III GG der Fall ist, bedürfte es zunächst einer Ergänzung des Art. 13 GG um eine weitere Schranke für eine derartige Eingriffskonstellation.

Im zweiten Schritt würde sich dann die Frage anschließen, ob das Betretungsrecht auf Ebene des einfachen Gesetzes ausdrücklich geregelt wird, oder auf eine (nicht ausdrücklich geregelte) Annexkompetenz gestützt werden soll bzw. kann. Letzteres erscheint für das Betreten von Wohnräumen bereits aus dem Grunde fraglich, da der damit verbundene intensive Eingriff in die Unverletzlichkeit der Wohnung schon keine *verhältnismäßig geringfügige Beeinträchtigung* im Vergleich zur primären Überwachung und Aufzeichnung der Telekommunikation darstellen dürfte.

Aber auch eine dann in Betracht zu ziehende ausdrückliche Regelung des Betretungsrechts im Gesetz bereitet Bedenken. Zum einen regelt die StPO bislang Begleiteingriffe im Regelfall nicht ausdrücklich[643], sodass eine ausdrückliche Regelung hier gesetzessystematisch einen Ausnahmefall dar-

---

639 Siehe 2. Teil B.I.2.b) und II.

640 Vgl. hierzu auch *Käß*, BayVBl. 2010, 1 (13) m. w. N.

641 Zur Aufhebung eines solchen Betretungsrechts im Bayerischen Polizeiaufgabengesetz in Gestalt des zum 01.08.2008 eingef. und zum 01.08.2009 aufgeh. Art. 34e BayPAG, siehe auch LT-Drs. 16/1271, S. 1 f.

642 Siehe hierzu 2. Teil B.I.2.b)bb).

643 Eine Ausnahme stellt bspw. § 110a III StPO dar; vgl. hierzu auch *Henrichs*, Kriminalistik 2008, 438 (440).

stellen würde. Zum anderen wäre es fraglich, ob ein solches Betretungsrecht in das Normgefüge von Maßnahmen der Überwachung und Aufzeichnung von Telekommunikation überhaupt passt und die vorhandene Eingriffsschwelle einer an §§ 100a, 100b StPO ausgerichteten Quellen-Telekommunikationsüberwachung mit der Begrenzung auf *schwere* Straftaten für den intensiven Eingriff in das Grundrecht aus Art. 13 I GG ausreicht. Angesichts der hohen Anforderungen, die bspw. § 100c StPO bzw. Art. 13 III GG für den Eingriff in die Unverletzlichkeit der Wohnung festlegen, ist dies unter Verhältnismäßigkeitsaspekten mithin zu verneinen.[644]

Von der zusätzlichen Normierung eines Betretungsrechts im Rahmen der Ergänzung der §§ 100a, 100b StPO ist demnach abzusehen.

5. Folgen von Verstößen gegen die Vorgaben der §§ 100a II Nr. 1 und 100b IV StPO-E bei Umsetzung der Anordnung

Während sich die Folgen von formellen und/oder materiellen Mängeln in der Quellen-TKÜ-Anordnung[645] unter Heranziehung der von Rspr. und Praxis entwickelten Grundsätze zur Verwertbarkeit ohne weiteres herleiten lassen, schließt sich bezüglich der in den §§ 100a II Nr. 1 und 100b IV StPO-E normierten (und im Beschluss für den konkreten Einzelfall angeordneten) Quellen-TKÜ-spezifischen Bestimmungen die noch nicht geklärte Frage an, welche Konsequenzen aus einem Verstoß gegen die rechtlichen Vorgaben hinsichtlich der sicherzustellenden technischen Vorkehrungen sowie der vorzunehmenden Protokollierungen bei der Durchführung der Quellen-TKÜ-Maßnahme zu ziehen sind.

---

644 Die Verankerung eines Betretungsrechts wäre aus Gründen der Verhältnismäßigkeit zwar bei der Ausrichtung einer Quellen-TKÜ-Regelung an der Eingriffsschwelle der §§ 100c ff. StPO (vgl. hierzu 3. Teil B.II.3.) nicht ausgeschlossen, jedoch sprechen die besseren Argumente, insbesondere auch zugunsten einer praktischen Durchführbarkeit der Maßnahme, für ein Ausrichten an §§ 100a, 100b StPO, zumal Primär- und Sekundärmaßnahmen einer Quellen-TKÜ kein Eingriffsniveau wie eine Maßnahme nach §§ 100c ff. StPO erfordern, siehe hierzu 3. Teil B.II.2.; dass Quellen-TKÜ-Maßnahmen auch ohne ein heimliches Betreten von Wohnräumen erfolgreich realisiert werden können, belegen indes die bislang in der Praxis durchgeführten Maßnahmen.

645 Zur Frage der Verwertbarkeit erlangter Erkenntnisse bei formellen oder materiellen Mängeln in der Anordnung, siehe 2. Teil A.III.2.

a) Bedürfnis nach der Normierung eines generellen Beweisverwertungsverbotes?

Zur umfassenden Absicherung der rechtlich vorgegebenen Anforderungen an die zu ergreifenden technischen Vorkehrungen wäre es eine Möglichkeit, bei jeglichen Verstößen gegen § 100a II Nr. 1 StPO-E und § 100b IV StPO-E bei der Maßnahmeumsetzung ein ausdrückliches und generelles Beweisverwertungsverbot für dadurch erlangte Erkenntnisse (auch als Spurenansätze) gesetzlich zu verankern, wie dies bislang in der Strafprozessordnung bspw. für die Fälle des § 100a IV S. 2 StPO, des § 100c V S. 3 StPO wie auch des § 136a III S. 2 StPO geregelt ist.

Damit sich ein Bedürfnis nach einer vergleichbaren Regelung für die Fälle von Verstößen gegen die rechtlichen Vorgaben hinsichtlich der zu ergreifenden technischen Vorkehrungen beim Einsatz von Überwachungssoftware im Rahmen der Umsetzung von Quellen-TKÜ-Maßnahmen bejahen lässt, müsste allerdings eine *Vergleichbarkeit in der Wertigkeit* des von den einzelnen Normen jeweils erfassten Schutzgutes gegeben sein:

Durch den generellen Ausschluss jeglicher Verwertung von erlangten Erkenntnissen, die der Entfaltung im höchstpersönlichen Bereich zuzurechnen sind, dient das Beweisverwertungsverbot in § 100a IV S. 2 StPO für Maßnahmen der Telekommunikationsüberwachung dem Schutz des Kernbereichs privater Lebensgestaltung durch Zubilligung eines von staatlicher Kenntnisnahme ausgenommenen Austauschs höchstpersönlicher Informationen mittels Telekommunikation. Die Anerkennung eines absolut geschützten Kernbereichs privater Lebensgestaltung gehört nach der grundlegenden Rspr. des BVerfG[646] zur Unantastbarkeit der Menschenwürde nach Art. 1 I GG.

Wie auch § 100a IV S. 2 StPO dient auch das Beweisverwertungsverbot in § 100c V S. 3 StPO im Rahmen von Maßnahmen der akustischen Wohnraumüberwachung dem Schutz des unantastbaren Kernbereichs privater Lebensgestaltung und mithin dem Schutz der Menschenwürde aus Art. 1 I GG durch Zubilligung eines vor staatlicher Einsichtnahme geschützten Refugiums des Einzelnen zur höchstpersönlichen Entfaltung in seinen Wohnräumen[647].

Das umfassende gesetzliche Beweisverwertungsverbot des § 136a III S. 2 StPO verbietet die (unmittelbare wie mittelbare[648]) Verwertung der Aussagen von Beschuldigten (auch von Zeugen, § 69 III i. V. m. § 136a III S. 2 StPO entspr.), die im Rahmen einer Vernehmungssituation unter Beeinträch-

---

646 BVerfG NJW 2004, 999; BVerfG NJW 2005, 2603; vgl. bereits BVerfG NJW 1990, 563; BVerfG NJW 1957, 297.

647 Vgl. hierzu BVerfG NJW 2004, 999 (1002).

648 Vgl. Meyer-Goßner – *Meyer-Goßner*, StPO, § 136a, Rn. 29 m. w. N.

tigung der Freiheit der Willensentschließung und Willensbetätigung durch verbotene Vernehmungsmethoden zustande gekommen sind. Als Norm zum Schutze der freien Willensentschließung und Willenbetätigung dient die Vorschrift neben dem Zweck der Wahrheitsfindung ebenso wie die Kernbereichsregelungen der §§ 100a IV S. 2 und 100c V S. 3 StPO der Achtung und Wahrung der Unantastbarkeit der Menschenwürde aus Art. 1 I GG[649].

Unter Berücksichtigung der Schutzgüter absoluter gesetzlicher Beweisverwertungsverbote stellt sich die generelle Einordnung von Verstößen gegen die gesetzlichen Anforderungen an die technischen Vorkehrungen sowie gegen die Protokollierungspflichten auf gleicher Wertigkeitsstufe indes als schwierig dar. Anders als die Regelungsgegenstände der §§ 100a IV, 100c V sowie 136a StPO enthalten die Bestimmungen der §§ 100a II Nr. 1 und 100b IV StPO-E keine spezielle Ausprägung des Menschenwürdegehaltes aus Art. 1 I GG. Eine vergleichbare Wertigkeit der Schutzgüter der §§ 100a II Nr. 1 und 100b IV StPO-E mit den Schutzgütern der §§ 100a IV, V wie auch 136a StPO auf einer Ebene lässt sich daher nicht konstatieren. Es besteht damit *kein Bedürfnis* nach der Normierung eines absoluten gesetzlichen Beweisverwertungsverbotes für die Fälle des Verstoßes gegen rechtliche Vorgaben über technische Vorkehrungen und Protokollierungspflichten beim Einsatz technischer Mittel im Rahmen der Umsetzung von Quellen-TKÜ-Maßnahmen.

b) Verwertbarkeit der erlangten Erkenntnisse

Besteht kein generelles Beweisverwertungsverbot bei Verstößen gegen die rechtlichen Vorgaben der §§ 100a II Nr. 1 und 100b IV StPO-E, so ist grds. je nach Verstoß für den Einzelfall zu entscheiden, ob dies zur Unverwertbarkeit der erlangten Erkenntnisse führt oder nicht.

Für die Beurteilung, ob aus dem Verstoß im Einzelfall ein Verbot der Verwertung erlangter Erkenntnisse zu folgern ist, empfiehlt sich eine *differenzierende Herangehensweise*, bei der insbesondere darauf abgestellt wird, ob die jeweilige rechtliche Vorgabe, gegen die im konkreten Einzelfall verstoßen wurde, gerade die Beweismittelauthentizität und -integrität der erhobenen Daten und damit die Beweissicherheit und Aussagekraft der erlangten Erkenntnisse sicherstellen soll – womit sich für den Fall eines Verstoßes ein Beweisverwertungsverbot begründen ließe – oder aber anderen Zwecken dient und ein Verstoß daher – abgesehen von den Fällen bloßer Willkür bzw. bewusster Missachtung der rechtlichen Vorgaben[650] –

---

649 Vgl. auch Meyer-Goßner – *Meyer-Goßner*, StPO, § 136a, Rn. 1.

650 In den Fällen von willkürlicher oder bewusster Missachtung rechtlicher Vorgaben ist nach verallgemeinerungsfähigem Rechtsgedanken regelmäßig von einem

grds. kein Beweisverwertungsverbot bedingt, sofern im Einzelfall die Rechtsstellung des Betroffenen das Interesse an effektiver Strafverfolgung und funktionstüchtiger Strafrechtspflege nicht überwiegt.

Liegen Verstöße gegen die Vorschriften der §§ 100a II Nr. 1 und 100b IV StPO-E bei der Umsetzung einer Quellen-TKÜ-Anordnung vor, so kann für die Frage der Verwertbarkeit der im Rahmen einer fehlerhaften Umsetzung erlangten Erkenntnisse wie folgt differenziert werden:

- Bei einem Verstoß gegen die gesetzlich vorgeschriebenen und im Beschluss auf den Einzelfall angewendeten Bestimmungen des § 100a II Nr. 1 StPO-E, wonach durch technische Maßnahmen sichergestellt sein muss, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird, sind grds. zwei Konstellationen zu unterscheiden:

  Sind keine ausreichenden (jedoch zumutbaren) technischen Maßnahmen für eine ausschließliche Erfassung laufender Telekommunikationsvorgänge bei der Umsetzung der Anordnung unter Verstoß gegen die rechtliche Vorgabe ergriffen worden und ist es bei der Durchführung der Maßnahme neben laufender Telekommunikation des Weiteren auch zu einem *Erfassen von sonstigen Daten oder Vorgängen* auf dem betroffenen informationstechnischen System ohne Bezug zu laufenden Telekommunikationsvorgängen gekommen, ist für solche Fälle der Durchführung einer als Quellen-TKÜ angeordneten Maßnahmen, welche in ihrer praktischen Umsetzung tatsächlich jedoch (teilweise) die Wirkung einer Online-Durchsuchung entfaltet hat, – nicht zuletzt auch zum Schutze des Richtervorbehaltes – ein *umfassendes Verwertungsverbot* jedenfalls für die erlangten, von der Anordnung *nicht gedeckten* Erkenntnisse zu bejahen[651].

Verwertungsverbot als Folge des fehlerhaften Verfahrens auszugehen, vgl. BVerfG NJW 2006, 2684 (2686); BVerfG NJW 2005, 1917 (1923); BVerfG NJW 1971, 1097 (1098); vgl. auch bei Meyer-Goßner – *Cierniak*, StPO, § 94, Rn. 21.

[651] In diese Richtung zwar auch *Albrecht*, JurPC Web-Dok. 59/2011, Abs. 21, der sich jedoch in den Fällen, in denen es bei der Maßnahmeumsetzung entgegen der Anordnung neben des zulässigen Zugriffs auf Daten aus laufenden TK-Vorgängen auch zu einem unzulässigen weiteren Zugriff auf Daten bzw. Datenverarbeitungsvorgänge außerhalb laufender Telekommunikation gekommen ist (vgl. LG Landshut, MMR 2011, 690 zu zusätzlich angefertigten Screenshots, vgl. hierzu auch 2. Teil A.II.4.), gegen eine Trennbarkeit der erhobenen Informationen ausspricht. Für ein Einbeziehen auch der gewonnenen Erkenntnisse aus laufenden TK-Vorgängen in das Verwertungsverbot besteht indes jedoch kein überzeugender Grund; insbesondere rechtfertigt das von *Albrecht* angesprochene Argument des „disziplinierenden Einwirkens auf die Ermittlungsbehörden“ (Abs. 21) – gerade auch angesichts des bedeutsamen öffentlichen Interesses an der Verfolgung und Aufklärung schwerer Straftaten – keine derart weitreichende Folge in Form eines pauschalen Verwertungsverbots für sämtliche Erkenntnisse; denn die erlangten Erkenntnisse aus laufenden Telekommunikationsvorgängen sind formell von der Anordnung und materiell von § 100a I StPO gedeckt; allein der Verstoß gegen § 100a II Nr. 1 StPO-E bei der

Denn in derartigen Fällen stellt sich die Ermittlungsmaßnahme insoweit bereits formell rechtswidrig dar, als für eine solche Maßnahme mit Wirkung einer Online-Durchsuchung schon gar keine entsprechende Anordnung und damit keine Legitimationsgrundlage für die Maßnahmedurchführung und Erhebung sonstiger Daten gegeben war.[652] Auch die §§ 100a, 100b StPO ließen sich für die Erhebung von Daten außerhalb laufender Telekommunikationsvorgänge nicht mehr als Rechtsgrundlage heranziehen, da ein solcher Eingriff nicht mehr nur am Fernmeldegeheimnis aus Art. 10 I GG zu messen wäre, sondern am neuen IT-Grundrecht aus Art. 2 I i. V. m. 1 I GG.[653]

Stellt sich hingegen im konkreten Einzelfall (nachträglich) heraus, dass die Überwachungssoftware von ihrem technischen Potential her – jedenfalls prinzipiell – dazu in der Lage gewesen bzw. über entsprechende Upgrades in die Lage versetzbar gewesen sein sollte, im Sinne einer Online-Durchsuchung das Zielsystem auch im Übrigen zu durchsuchen und auch sonstige auf dem Zielsystem gespeicherte Daten ohne Bezug zu laufenden Telekommunikationsvorgängen zu erfassen, würde ein solcher Umstand zwar grds. mit der Vorgabe des § 100a II Nr. 1 StPO-E in Konflikt geraten, wonach durch technische Maßnahmen sichergestellt sein muss, dass ausschließlich laufende Telekommunikation erfasst wird. Allein das im Einzelfall möglicherweise bestehende *technische Potential* der Software, über die Überwachung und Aufzeichnung laufender Telekommunikation hinaus auch sonstige Daten oder Vorgänge erfassen zu können, begründet jedoch *grds. noch kein Beweisverwertungsverbot*, wenn bei der Maßnahmedurchführung von der Überwachungssoftware strikt in der von der Quellen-TKÜ-Anordnung legitimierten Weise Gebrauch gemacht worden ist und eine darüber hinaus gehende Verwendung des technischen Mittels nicht stattgefunden hat. Hierbei lässt sich insbesondere auch der Gedanke des *hypothetisch rechtmäßigen Ermittlungsverlaufs*[654] heranziehen, nämlich

---

Durchführung bewirkt kein Beweisverwertungsverbot auch für diese Erkenntnisse (vergleichbar mit Verstößen gegen die nach § 81f II S. 2 StPO zu ergreifenden Vorkehrungen bei der Durchführung von DNA-Untersuchungen, vgl. Meyer-Goßner – *Cierniak*, StPO, § 81f, Rn. 9); sachgerecht wie auch verhältnismäßig ist deshalb die getrennte Beurteilung (in diese Richtung auch LG Landshut, MMR 2011, 690, 690 „soweit"); auch die Ausführungen des BVerfG, NJW 2008, 822 (826) stehen dem nicht zwingend entgegen, vgl. insoweit *Braun*, jurisPR-ITR 3/2011 Anm. 3.

652 Vgl. insoweit BGH NJW 1983, 1570 (1571); vgl. Meyer-Goßner – *Cierniak*, StPO, § 100a, Rn. 35; vgl. auch entspr. Meyer-Goßner – *Cierniak*, StPO, § 81a, Rn. 33 zu körperlichen Eingriffen ohne Anordnung sowie § 81f, Rn. 9 zur DNA-Analyse ohne Anordnung.

653 Vgl. BVerfG NJW 2008, 822 (826).

654 Auch *hypothetischer Ersatzeingriff;* vgl. hierzu BVerfG NJW 1971, 1097 (1098); BVerfG NJW 1989, 1741 (1744).

dass nach den konkreten Umständen keine anderen Erkenntnisse erhoben worden sind, als sie bei der Verwendung einer Software erhoben worden wären, deren technische Konzeption von Anfang nicht mehr als eine Überwachung und Aufzeichnung laufender Telekommunikationsvorgänge möglich gemacht hätte. Dem steht insbesondere auch nicht die Gefahr der Umgehung des Richtervorbehaltes gegenüber, da in diesen Fällen nur Daten erlangt worden sind (Daten aus laufenden Telekommunikationsvorgängen), für deren Erhebung eine entsprechende Anordnung als legitimierende Grundlage gerade gegeben war.

- Verstöße gegen die für die Umsetzung von Quellen-TKÜ-Maßnahmen beachtlichen Vorschriften des § 100b IV S. 1 Nr. 1 und Nr. 2 StPO-E begründen im Einzelfall *grds. noch kein Beweisverwertungsverbot*. Die darin enthaltenen Vorgaben an die technischen Vorkehrungen, welche sicherzustellen haben, dass im Zuge des Softwareeinsatzes nur für die Datenerhebung unerlässliche Veränderungen an dem betroffenen Zielsystem vorgenommen (Nr. 1) und diese bei Maßnahmebeendigung rückgängig gemacht werden (Nr. 2), dienen zuvörderst dem Schutz des betroffenen informationstechnischen Systems an sich, und zwar aus Gründen der Verhältnismäßigkeit und nicht zur Sicherstellung möglichst gerichtsfester und auf Authentizität und Integrität nachprüfbarer Beweismittel. Für den Fall eines Verstoßes gegen diese Vorgaben, falls es also im Zuge der Implementierung und des Einsatzes der Überwachungssoftware bspw. auch zu Veränderungen an dem betroffenen Zielsystem gekommen sein sollte, welche nicht unbedingt erforderlich für die Datenerhebung waren – was für die Praxis nicht ohne Belang ist, da ein aktiv laufendes Programm i. d. R. fortwährend eine Vielzahl von (oftmals aber nur vorübergehenden) Veränderungen an Systemeinstellungen wie auch der Systemleistung erzeugt[655] – oder auch falls vorgenommene Veränderungen entgegen § 100b IV S. 1 Nr. 2 StPO-E doch nicht bei Beendigung der Maßnahme rückgängig gemacht worden sein sollten, ist daher mit Blick auf die Verwertbarkeit der erlangten Erkenntnisse einer im Übrigen rechtmäßig durchgeführten Quellen-TKÜ-Maßnahme regelmäßig nicht von einem Überwiegen der durch den Verstoß beeinträchtigten Rechtsstellung des Beschuldigten gegenüber dem Strafverfolgungsinteresse auszugehen.
- Auch ein Verstoß gegen die Vorgabe des § 100b IV S. 2 StPO-E, wonach die im Rahmen der Durchführung einer Quellen-TKÜ-Maßnahme eingesetzte Überwachungssoftware nach dem Stand der Technik gegen unbefugte Nutzung zu schützen ist, macht die durch insoweit fehlerhafte Umsetzung der Quellen-TKÜ-Anordnung erlangten Erkenntnisse *i. d. R. nicht unverwertbar*. Die Vorschrift dient in Anlehnung an § 14 I TKÜV

655 Vgl. insoweit auch BT-Drs. 16/10121, S. 30.

zuvörderst dem Schutz vor einer Zweckentfremdung des eingesetzten technischen Mittels durch Dritte, nicht jedoch der beweissicheren Erlangung und Behandlung von Erkenntnissen zur Verfolgung und Aufklärung der maßnahmegegenständlichen Straftat. Von einem Überwiegen der Rechtsstellung des Beschuldigten gegenüber dem Interesse des Staates und der Allgemeinheit an effektiver Verfolgung und Aufklärung von Straftaten, was in dem vorliegenden Falle für die Annahme eine Beweisverwertungsverbotes erforderlich wäre, kann daher bei einem Verstoß gegen die Vorschrift des § 100b IV S. 2 StPO-E regelmäßig nicht ausgegangen werden.

- Anders als die vorhergehenden gesetzlichen Bestimmungen dient die Vorschrift des § 100b IV S. 3 StPO-E der Authentizität und Integrität der erhobenen Daten und damit der Beweissicherheit der gewonnenen Erkenntnisse, da sie vorgibt, dass erlangte Daten nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen sind. Dies allein begründet allerdings *nicht automatisch auch das Vorliegen eines Beweisverwertungsverbotes* für unter Verstoß gegen diese Vorgabe erlangte Erkenntnisse. Hierfür lässt sich insbesondere auch auf die Rspr. des BGH[656] zur Umsetzung von Maßnahmen der *DNA-Analyse* nach §§ 81e, 81f StPO zurückgreifen. Gemäß § 81e I S. 1 StPO dürfen an dem im Rahmen von körperlichen Untersuchungen des Beschuldigten nach § 81a I StPO (anderer Personen nach § 81e I S. 2 i. V. m. § 81 c I StPO) durch die Entnahme von Blut oder anderen DNA-enthaltenden natürlichen Körperbestandteilen (Zellen, Flüssigkeiten etc., z. B. Speichel) erlangten Material unter bestimmten Voraussetzungen auch molekulargenetische Untersuchungen (DNA-Analysen) durchgeführt werden. Für die Umsetzung von DNA-Analysen bestimmt § 81f II S. 2 StPO in ähnlicher Weise, dass durch technische und organisatorische Maßnahmen gewährleistet sein muss, dass unzulässige molekulargenetische Untersuchungen und unbefugte Kenntnisnahme Dritter ausgeschlossen sind. Die gesetzliche Pflicht zum Ergreifen besonderer technischer und organisatorischer Vorkehrungen gegen unzulässige DNA-Untersuchungen dient ausweislich der Gesetzesbegründung dem Schutz vor Missbräuchen bei der Durchführung von angeordneten Untersuchungen an gewonnenen DNA-Proben[657], wobei ein Missbrauch, vor dem die besonderen Vorkehrungen schützen können, auch in der Weise möglich ist, dass die jeweilige DNA-Probe verändert oder ausgetauscht wird, es sich damit nicht mehr um das nach § 81a I StPO gewonnenen DNA-Material handelt und somit letztlich der Beweiswert der Untersuchungsergebnisse verfälscht

656 BGH NStZ 1999, 209.

657 Vgl. BT-Drs. 13/667, S. 8.

bzw. aufgehoben wird. Zudem verpflichtet § 81f II S. 2 StPO dazu, die Untersuchungsbefunde, d. h. alle Ergebnisse einschließlich der bei einzelnen Untersuchungsschritten angefallenen Zwischenergebnisse, gegen eine unbefugte Kenntnisnahme Dritter zu schützen.[658] Die gesetzliche Pflicht zum Ergreifen besonderer technischer und organisatorischer Vorkehrungen umfasst hierbei alle nach dem Stand der Technik möglichen und zumutbaren Maßnahmen[659]. Darüber hinaus ist das für die Untersuchung verwendete Material (DNA-Probe) nach Maßgabe des § 81f II S. 3 StPO bereits in anonymisierter Form zur DNA-Analyse zu geben. Auch die erlangten personenbezogenen Informationen sind zu anonymisieren, sobald dies der Untersuchungszweck gestattet.[660]

Verstöße gegen die in § 81f II StPO enthaltenen Bestimmungen für die Durchführung von DNA-Analysen begründen jedoch nicht automatisch auch ein Beweisverwertungsverbot. Wie dies der BGH bereits für den Verstoß gegen das Anonymisierungsgebot des § 81f II S. 3 StPO höchstrichterlich entschieden hat[661], wird sich die *Revision* auf Verstöße gegen die Vorgaben des § 81f II StPO *regelmäßig nicht stützen lassen*.[662]

Unter Übertragung dieses Ansatzes auf die hier vorliegende Konstellation wird im Einzelfall auch bei einem Verstoß gegen die Bestimmungen des § 100b IV S. 3 StPO-E im Rahmen der Durchführung von Quellen-TKÜ-Maßnahmen nur dann ein Beweisverwertungsverbot anzunehmen sein, wenn nach den konkreten Umständen tatsächliche Anhaltspunkte für die Annahme vorliegen, dass es auf Grund des Verstoßes gegen die gesetzlichen Vorgaben zu einer Verfälschung des erlangten Datenmaterials und damit zu einem schweren Eingriff in die Integrität und Authentizität der erhobenen Daten und deren Beweiswert gekommen ist. Bei Vorliegen derartiger konkreter Bedenken hinsichtlich der Beweissicherheit und Aussagekraft der gewonnenen Erkenntnisse ist im Einzelfall *ausnahmsweise* bei Verstößen gegen die Vorgaben des § 100b IV S. 3 StPO-E das Aufklärungsbedürfnis der Allgemeinheit zurückzustellen und zum Schutze der Rechtsstellung des Betroffenen ein *Beweisverwertungsverbot* anzunehmen.

- Entsprechendes gilt auch für Verstöße gegen die Protokollierungspflichten des § 100b IV S. 5 StPO-E. Die Verfahrensvorschriften dienen in Ergänzung zu den gesetzlichen Vorgaben der Sätze 1 bis 3 insbesondere der Nachprüfbarkeit des staatlichen Eingriffs sowie der Gewährleistung der

---

658 Vgl. BT-Drs. 13/667, S. 8; Meyer-Goßner – *Cierniak*, StPO, § 81f, Rn. 5.
659 Vgl. BT-Drs. 13/667, S. 8.
660 Vgl. BT-Drs. 13/667, S. 8.
661 Vgl. BGH NStZ 1999, 209 (209).
662 Vgl. auch Meyer-Goßner – *Cierniak*, StPO, § 81f, Rn. 9.

Gerichtsfestigkeit des erlangten Datenmaterials, indem über die Protokollierung ein erleichterte Nachweis dafür eröffnet wird, dass die erhobenen Daten tatsächlich vom betroffenen Zielsystem stammen und nicht verändert worden sind[663]. Dennoch bedarf es für die Annahme eines *ausnahmsweise bestehenden Beweisverwertungsverbotes* des Vorliegens besonderer Umstände, auf Grund derer im Einzelfall wegen des Verstoßes gegen Protokollierungspflichten aus § 100b IV S. 5 StPO-E das Strafverfolgungs- und Aufklärungsinteresse hinter dem Interessen des Betroffenen an der Unversehrtheit seiner Rechtsstellung zurücktritt. Da die Protokollierungspflichten vor allem der erleichterten Nachweisbarkeit der Beweismittelauthentizität und -integrität im Rahmen des gerichtlichen Verfahrens dienen[664], wird ein schwerwiegender Eingriff in die Rechte des Betroffenen, der im Rahmen der Abwägung mit dem Aufklärungsinteresse der Allgemeinheit ein Beweisverwertungsverbot begründen könnte, jedoch bei Verstößen gegen Protokollierungspflichten *im Regelfall nicht* gegeben sein.

663 Vgl. insoweit BT-Drs. 16/10121, S. 30.

664 Worüber das erkennende Gericht nach seiner freien, aus dem Inbegriff der Verhandlung geschöpften Überzeugung (§ 261 StPO) entscheidet, und zwar auf der Grundlage eines „nach der Lebenserfahrung ausreichende[n] Maß[es] an Sicherheit“ (BGH NStZ 1988, 236, 237; st. Rspr.).

Fazit

Mit der zunehmenden Digitalisierung und Verschlüsselung von Telekommunikation wird auch die Erkenntnisgewinnung und Beweisermittlung zur Aufklärung von Straftaten technisch und kriminaltaktisch immer anspruchsvoller und schwieriger. Neue Formen der Kriminalität wie auch neue technische Möglichkeiten, die im Zusammenhang mit der Begehung von Straftaten genutzt werden, können mitunter zu erheblichen Ermittlungsproblemen für staatliche Behörden führen. Entsprechend besteht für eine wirkungsvolle Strafverfolgung und Straftatenaufklärung das Bedürfnis, neue Wege bei der Ermittlungsarbeit zu gehen und entsprechend an die technische Entwicklung angepasste Ermittlungsmaßnahmen einzusetzen.

Der Einsatz spezieller technischer Mittel ist für die Durchführung moderner Ermittlungsarbeit im Zusammenhang mit der rasanten technischen Entwicklung unverzichtbar geworden. Die Notwendigkeit eines Ermittlungsinstruments wie der *Quellen-TKÜ* zum Zugriff mittels einer Überwachungssoftware auf verschlüsselte softwarebasierte Internettelefonie, welche über zu Telekommunikationszwecken genutzte informationstechnische Systeme geführt wird, liegt angesichts der stetig zunehmenden Verbreitung von Skype und vergleichbarer Programme sowie der fortschreitenden Etablierung von VoIP in der Gesellschaft als technischer Standard für Telefonate auf der Hand. Die Weiterentwicklung der technischen Standards für die Verschlüsselung von Kommunikationsinhalten macht gegenwärtig wie auch in Zukunft einen „technischen Wettlauf“ der Strafverfolgungsbehörden mit den modernen Telekommunikationsdiensten und -formen unausweichlich. Die automatisierte, bereits auf dem System des Nutzers stattfindende Verschlüsselung von TK-Daten vor deren Übermittlung im weltweiten Datennetz, wie dies bei vielen softwaregestützten VoIP-Diensten der Fall ist, macht ein Anknüpfen der Überwachung und Aufzeichnung „an der Quelle“ der Telekommunikation erforderlich, um die TK-Daten vor ihrer Ver- bzw. nach ihrer Entschlüsselung und damit in einsehbarer Form abgreifen zu können.

Die (noch) überschaubare Anzahl von durchgeführten Quellen-TKÜs pro Jahr mag über die ermittlungstaktische Unverzichtbarkeit dieser modernen Ermittlungsmaßnahme auf den ersten Blick hinwegtäuschen. Die Bedeutung dieser Maßnahme kann jedoch nicht allein von deren (gegenwärtiger) Anordnungshäufigkeit abgeleitet werden, sondern muss im Zusammenhang mit der sich entwickelnden Technik und dem (künftigen) Kommunikations-

verhalten der Bevölkerung gesehen werden.[1] Fragen vor allem im Zusammenhang mit der zunehmenden *Konvergenz* der Systeme[2], also insbesondere der Zusammenschaltung der Netze und Verschmelzung der Übertragungstechniken, werden künftig von immer stärkerer Relevanz sein. So zeichnet sich nach Angaben der Bundesnetzagentur[3] bei den Netzstrukturen ein eindeutiger Trend weg von den leitungsvermittelten Netzen des herkömmlichen öffentlichen Festnetzes hin zu paketvermittelten Netzen ab.[4] Hieran schließen auch Medienberichte aus jüngerer Zeit an, wonach die großen deutschen Anbieter von Telekommunikationsdienstleistungen, insbesondere die Deutsche Telekom AG, das Vorhaben verfolgen, ihre bisherigen Telekommunikationsdienste in naher Zukunft vollständig auf das Internetprotokoll (IP) umzustellen, mit dem Ziel durch ein einheitlich aufgebautes und zu betreibendes IP-Netz Kosten zu reduzieren und Dienste hinsichtlich Datenmengen, Geschwindigkeit und Verfügbarkeit zu optimieren.[5] Die Kommunikation via Internetprotokoll (IP) hat daher neben dem technischen auch das wirtschaftliche Potential, die Konvergenz der Systeme weiter voranzutreiben und damit den Telekommunikationsmarkt gänzlich neu zu ordnen sowie die herkömmliche Festnetztelefonie durch moderne Internettelefonie weitgehend abzulösen.[6]

---

[1] In diese Richtung überzeugend auch *Dathe*, Präsident des BayLKA, öffentliche Anhörung im Rahmen der 14. Sitzung des Innenausschusses des Hessischen Landtags am 30.09.2009 zum Gesetzesentwurf der Fraktionen der CDU und der FDP für ein Gesetz zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung und anderer Gesetze – Drucks. 18/861 –, stenografischer Bericht, Ausschussvorlage INA/18/14, S. 54.

[2] Für Einzelheiten, siehe auch die Ausführungen hierzu unter 2. Teil A.II.6.b).

[3] Bundesagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA), vormals Regulierungsbehörde für Telekommunikation und Post (RegTP).

[4] Vgl. Bundesnetzagentur, Anhörung zu Voice over IP (VoIP) – Zusammenfassende Auswertung der jeweiligen Fragenkomplexe, S. 9, abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Auswertung/ThemenweiseAuswertungId3173pdf.pdf?__blob=publicationFile (zuletzt aufgerufen 15.06.2012).

[5] Vgl. Polizeikurier RLP Feb 08, S. 9; zum zunehmenden Ausbau der IP-Technologie: http://www.onlinekosten.de/news/artikel/14732/0/Telekom-stellt-Telefonfestnetz-bis-2012-auf-IP-Technik-um (zuletzt aufgerufen 15.06.2012); http://www.teltarif.de/arch/2008/kw10/s29168.html (zuletzt aufgerufen 15.06.2012); http://www.teltarif.de/arch/2004/kw04/s12579.html (zuletzt aufgerufen 15.06.2012); http://www.teltarif.de/arch/2004/kw24/s13978.html (zuletzt aufgerufen 15.06.2012); http://www.datentarif.de/html/internettelefonie-voip.html (zuletzt aufgerufen 15.06.2012); http://www.call-magazin.de/telefon-festnetz/telefon-festnetz-nachrichten/umstellung-des-telekom-netzes-auf-voip-hat-massive-folgen_27046.html (zuletzt aufgerufen 15.06.2012); http://www.heise.de/newsticker/meldung/BT-investiert-Milliarden-in-IP-Telefonie-99611.html (zuletzt aufgerufen 15.06.2012).

Dies wird langfristig auch zur Folge haben, dass der herkömmliche Festnetzanschluss und die klassische Festnetztelefonie mehr und mehr zugunsten IP-basierter Technologie an Bedeutung verlieren werden. Mit der Änderung des Telefoniestandards auf dem Telekommunikationsmarkt dürfte dann auch eine Übertragung von Verschlüsselungsstandards wie bei Skype & Co auf jedwede Art von IP-gestützter Telefonie zu erwarten sein, um einen ausreichenden Schutz vor unbefugten Zugriffen und Missbrauch gewährleisten zu können.

Die Quellen-TKÜ ist bereits heute ein wichtiger Baustein eines *harmonischen Gesamtkonzepts strafprozessualer heimlicher Ermittlungsmaßnahmen*[7], ohne den eine gravierende Lücke bestünde. Maßnahmen unter Einsatz staatlicher Überwachungssoftware „sind Ermittlungsmöglichkeiten, auf die der Staat nicht generell verzichten kann [und in Form der Quellen-TKÜ unter verfassungsrechtlich sowie einfachgesetzlichen Aspekten auch nicht verzichten braucht, Anm. d. Verf.], weil er sonst in einer Reihe von Verfahren gar keine Beweise mehr erheben kann“[8]. Sinnbildlich gesprochen: *Die verschiedenen Möglichkeiten strafprozessualer heimlicher Ermittlungsmaßnahmen sind „wie ein Klavier, und eine Taste ist die Quellen-TKÜ, und wenn die fehlt, dann fehlt eine Taste – dann können Sie nicht mehr spielen“*[9].

Damit den Sicherheitsbehörden bei verschlüsselten Telefonaten u. a. über den PC nicht die Hände gebunden sind, muss die Telekommunikationsüberwachung der technischen Entwicklung folgen und rechtlich so ausgestaltet sein, dass das Strafverfolgungsinteresse des Staates und das Sicherheitsinteresse der Allgemeinheit auf der einen Seite mit den Freiheits- und Grundrechte des Einzelnen auf der anderen Seite in einen gerechten Ausgleich gebracht sind. Dies kann durch einen verantwortungsbewussten und sensiblen Umgang mit dem neuen Ermittlungsinstrument der Quellen-TKÜ gewährleistet werden.

Die Regelungen der Telekommunikationsüberwachung in §§ 100a, 100b StPO stellen hierbei – wie die Untersuchungen zu *Modell 1* ergeben haben – grds. eine ausreichende Rechtsgrundlage für die mit der Quellen-TKÜ

---

6 Vgl. auch *Katko*, CR 2005, 189 (193).

7 Vgl. zu diesem angestrebten Ziel die Antwort der Bundesregierung, BT-Drs. 15/4725, S. 34; vgl. auch BT-Drs. 14/7679, S. 2; BT-Drs. 14/7008, S. 6, 8; BR-Drs. 702/01, S. 10.

8 *Bosbach*, Vorsitzender des Innenausschusses des Deutschen Bundestages, zitiert nach *Baumer*, in: „Berlin flieht vor dem Trojaner“, Nürnberger Nachrichten/Fürther Nachrichten vom 11.10.2011, S. 2.

9 *Wirth*, BayLKA, persönliches Gespräch mit dem Verfasser, München, 12.11. 2010.

verbundenen Primär- und Sekundärmaßnahmen dar und erfassen dem Wortsinn der Tatbestandsbegrifflichkeiten wie auch dem Regelungszweck (Überwachung und Aufzeichnung von Telekommunikation) nach auch den heimlichen/verdeckten Zugriff auf Internettelefonie, welche über informationstechnische Systeme als spezifische zu Telekommunikationszwecken genutzte Endgeräte stattfindet, mittels einer Überwachungssoftware als technisches Mittel zur Erhebung der TK-Daten. Den Vorgaben des BVerfG, wonach Art. 10 I GG nur dann alleiniger Grundrechtsmaßstab ist, wenn ausschließlich Daten aus laufenden Telekommunikationsvorgängen erfasst werden[10], lässt sich durch präzise und den Eingriff konkretisierende rechtliche Vorgaben in den Anordnungsbeschlüssen und durch eine streng auf den Maßnahmezweck beschränkte Vorgehensweise bei der (technischen) Umsetzung Rechnung tragen.

Wie die Untersuchungen zu *Modell 2* ergeben haben, bedarf es keiner Regelung der Quellen-TKÜ als eigenständige Befugnisnorm („§ 100j StPO-E"), welche in ihren Eingriffsvoraussetzungen an die erhöhten Bestimmungen der §§ 100c ff. StPO zur akustischen Wohnraumüberwachung angeglichen ist. Angesichts des gegenwärtig vorherrschenden „argumentatorischen Wettstreits" zweier Lager in Rechtspraxis und Schrifttum, welche mit unterschiedlichen Sichtweisen und Rechtauffassungen zu einem höchstrichterlich bislang noch nicht abschließend geklärten Ermittlungsinstrument letztlich um eine Art „Vorherrschaft der Argumentationsansätze" buhlen, empfiehlt es sich bei einem rechtlich, rechtspolitisch wie auch gesellschaftlich höchst sensiblen Thema wie der Quellen-TKÜ und dem damit verbundenen Einsatz staatlicher Überwachungssoftware dennoch, die repressive Quellen-TKÜ nur noch für einen gewissen Übergangszeitraum auf die §§ 100a, 100b StPO in ihrer gegenwärtigen Fassung zu stützen[11], *mittel- und langfristig jedoch die Quellen-TKÜ gesetzlich klarzustellen* und die für diese Ermittlungsmaßnahme als besondere Weise des Realisierens der Überwachung und Aufzeichnung von Telekommunikation einschlägigen §§ 100a und 100b StPO um die in *Modell 3* dargestellten Vorschriften zu ergänzen. Etwaigen (technischen) Unsicherheiten im Umgang mit der im Rahmen einer solchen Ermittlungsmaßnahme auf informationstechnischen Systemen zum Einsatz kommenden Überwachungssoftware lässt sich über eine Ergänzung der grundlegenden technischen Anforderungen im Gesetz begegnen. Mit Blick auf das elementare Bedürfnis der Praxis nach einer rechtlich „hieb- und stichfesten" und damit rechtssicheren und gerichtsfesten Überwachbarkeit der in der Popularität stetig wachsenden VoIP-Dienste gerade in Form softwarebasierter P2P-Internettelefonie wie auch im Sinne einer *integrativen*

---

[10] Vgl. BVerfG NJW 2008, 822 (826).

[11] In diese Richtung auch KK – *Nack*, StPO, § 100a, Rn. 27.

Gesamtlösung der zu der modernen Ermittlungsmaßnahme der Quellen-TKÜ vertretenen Rechtsansichten ist eine solche Lösung innerhalb des vom Gesetzgeber kontinuierlich angestrebten „harmonische[n] Gesamtkonzept[s] der strafprozessualen heimlichen Ermittlungsmaßnahmen“[12] jedenfalls wünschenswert.

[12] Antwort der Bundesregierung, BT-Drs. 15/4725, S. 34; vgl. auch BT-Drs. 14/7679, S. 2; BT-Drs. 14/7008, S. 6, 8; BR-Drs. 702/01, S. 10.

Anhang 1

Beschlussvorschlag für die richterliche Anordnung einer strafprozessualen Überwachung der Telekommunikation einschließlich[1] Überwachung verschlüsselt geführter VoIP-Telekommunikation (Quellen-Telekommunikationsüberwachung)[2]

Amtsgericht Musterstadt

– Ermittlungsrichter –

Az. …Gs…/…

B e s c h l u s s

In dem Ermittlungsverfahren gegen

[*Name*], [*Vorname*], geb. [*Geburtsname*], geboren am [*Geburtsdatum*], in [*Geburtsort*], [*Staatsangehörigkeit*], [*Familienstand*], [*Beruf*], wohnhaft [*Straße mit Hausnummer, PLZ mit Ort*],

wegen [*Tatvorwurf*]

wird

I. nach §§ 100a I, 100b StPO auf Antrag der Staatsanwaltschaft gemäß § 33 IV StPO ohne vorherige Anhörung die Überwachung und Aufzeichnung der Telekommunikation (Inhaltsdaten und Verkehrsdaten) für die Telekommunikationsanschlüsse

Anschluss 1: [*Rufnummer/andere Anschlusskennung*]
[*ggf. zusätzlich: zugeordneter DSL-Anschluss*]
[*Name Anschlussinhaber/Anschlussnutzer*]
[*Anschrift Anschlussinhaber/Anschlussnutzer*]

Anschluss 2: […]

---

[1] Im Regelfall wird in der Praxis neben der Überwachung und Aufzeichnung der verschlüsselt übermittelten VoIP-Kommunikation zugleich auch die Überwachung und Aufzeichnung der „normalen" über den überwachten Telekommunikationsanschluss ablaufenden Telekommunikation angeordnet.

[2] Unter Einbeziehung auch der Entwürfe nach BeckOK – *Graf*, StPO, Ed. 13, Formulare zum Strafprozessrecht, III., Quellen-TKUE, und *Bär*, TK-Überwachung, § 100a StPO, Rn. 73; für Einzelheiten zu den Quellen-TKÜ-spezifischen Besonderheiten des TKÜ-Beschlusses, siehe 3. Teil A.I.2.

durch

[*Name des nach § 100b III StPO verpflichteten Netzbetreibers/Providers*]

[*Anschrift Netzbetreiber/Provider*]

für die Zeit vom [*Datum Beginn*] bis zum *[Datum Ende*, *max. 3 Monate*] angeordnet.

II. nach §§ 100a I, 100b StPO auf Antrag der Staatsanwaltschaft gemäß § 33 IV StPO ohne vorherige Anhörung die Überwachung und Aufzeichnung der über den/die oben genannten Telekommunikationsanschluss/-anschlüsse [bzw. über das *Endgerät* (*Gerätekennung/Seriennummer*)] geführten, verschlüsselten Telekommunikation sowie die Vornahme der hierzu erforderlichen Maßnahmen, um die Telekommunikationsdaten [Sprachdaten; *bei Video-Internettelefonie zusätzlich:* einschließlich Videodaten[3]; bei *Instant Messaging via IP zusätzlich:* einschließlich Textdaten[4]] vor deren Verschlüsselung und nach deren Entschlüsselung im Wege des Einsatzes einer speziellen [*ggf.*: bei Gericht hinterlegten[5]] Überwachungssoftware (*soweit bekannt*: *Bezeichnung*, *Versionsnummer*, *Zertifizierungsnummer des Bundesamtes für Sicherheit in der Informationstechnik*[6]) auf dem zur Telekommunikation gebrauchten *Endgerät* [*möglichst genaue Bezeichnung: bspw. Geräteart, Gerätekennung/Seriennummer, Betriebssystem/-version etc.*] überwachen zu können,

für die Zeit vom [*Datum Beginn*] bis zum [*Datum Ende*, *max. 3 Monate*] angeordnet.

---

[3] Vgl. insoweit zutr. LG Hamburg, MMR 2011, 693 (693 f.); hiervon nicht erfasst ist allerdings das Anfertigen sog. Screenshots von der grafischen Bildschirmoberfläche, so zutr. auch LG Landshut, MMR 2011, 690 (691); zur Abgrenzung siehe 1. Teil A.I.2.e) sowie 2. Teil A.II.4.

[4] Für Einzelheiten zu Instant Messaging via IP, siehe 1. Teil A.I.2.f).

[5] Durch Hinterlegung des Quellcodes der eingesetzten Überwachungssoftware beim anordnenden Gericht (soweit bereits verfügbar und vorliegend) ließe sich eine entsprechende Nachprüfbarkeit im Rahmen des sich anschließenden Strafverfahrens zusätzlich dahingehend sicherstellen, dass die Überwachungssoftware weder sonstige auf dem Zielsystem gespeicherte Daten außerhalb laufender Telekommunikationsvorgänge erfassen konnte noch unter dem Gesichtspunkt der Datenmanipulation dazu in der Lage war, Daten frei auf dem Zielsystem zu platzieren, vgl. hierzu auch die Ausführungen unter 2. Teil A.III.3. und 2. Teil B.III.2.c). Die Vorlage und Hinterlegung des Quellcodes bei Beantragung der Maßnahme gibt dem Gericht aber zudem auch die Möglichkeit, sicherzugehen, dass die zum Einsatz kommende Überwachungssoftware auch die erforderlichen Beschränkungen hinsichtlich des Eingriffsumfangs einhält; durch entsprechende organisatorische Vorkehrungen, bspw. in Form von Erläuterungsblättern oder durch Heranziehen unabhängigen Sachverstandes, lässt sich dafür Sorge tragen, dass den Gerichten eine Nachvollziehbarkeit des Quellcodes ermöglicht wird.

[6] Soweit entsprechende Schritte zur Überprüfung und Zertifizierung „verfassungsrechtlich zulässiger" Überwachungsprogramme bereits umgesetzt wurden; zur erwogenen Einführung eines sog. „Staatstrojaner-TÜVs", siehe 3. Teil A.I.1.c) und 3. Teil B.III.3.c).

Zulässig sind hierbei aber nur solche Maßnahmen, die der Überwachung und Aufzeichnung von Daten aus laufenden Telekommunikationsvorgängen dienen und die für deren Umsetzung zwingend erforderlich sind.

Unzulässig sind insbesondere

1. die Durchsuchung der Speichermedien des fremden *Endgerätes* nach bestimmten gespeicherten Daten und Dateien sowie das Übertragen und Kopieren solcher Daten und Dateien außerhalb eines Telekommunikationsvorgangs sowie
2. die Überwachung von Datenverarbeitungsvorgängen, die nicht der Telekommunikation dienen (z. B. sog. Screenshots von grafischen Bildschirminhalten, Office- und Textverarbeitungsanwendungen, Grafik- und Multimediaanwendungen, Spiele u. ä.).

III. Bei der Durchführung der Maßnahmen nach Ziff. II. ist[7]

1. technisch sicherzustellen, dass an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden,
2. das eingesetzte Mittel nach dem Stand der Technik gegen unbefugte Nutzung zu schützen,
3. kopiertes Datenmaterial nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen,
4. bei jedem Einsatz des technischen Mittels die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes, die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen, die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und die Organisationseinheit, die die Maßnahme durchführt, zu protokollieren, wobei das Protokolldatenmaterial nur dazu zu verwenden ist, um dem Betroffenen oder einer dazu befugten öffentlichen Stelle die Prüfung zu ermöglichen, ob die Maßnahme nach Ziff. II rechtmäßig durchgeführt worden ist, und unverzüglich zu löschen ist, soweit es für diesen Zweck nicht mehr erforderlich ist.

Gründe:

1. Der/Die Beschuldigte ist auf Grund bestimmter Tatsachen verdächtig, Täter oder Teilnehmer einer [*Katalogstraftat*] nach § 100a I Nr. 1 i. V. m. § 100a II Nr. [*einschlägige Nummer*] StPO (sog. Katalogstraftat) zu sein.

   Auf Grund der bisherigen Ermittlungen liegt dem/der Beschuldigte/-n zur Last,

   [*Tatbeschreibung*]

   begangen zu haben.

---

[7] In Anlehnung an die in §§ 20l II S. 2, 20k II, III BKAG bzw. § 31c IV S. 3 POG RP gewählten Formulierungen.

Dies ist strafbar als [*Straftatbestimmung*]

gemäß §§ [*Strafvorschriften*].

2. Der Tatverdacht beruht auf

□ den Angaben des/der …

□ [*sonstige bestimmte Tatsachen*].

[*ggf:* Ergänzend wird auf den Zwischenbericht der mit den Ermittlungen betrauten bzw. sachbearbeitenden Dienststelle [*Angabe der Dienststelle*] vom [*Datum*], Bl. [*Blattzahl*] der Ermittlungsakten Bezug genommen.]

3. Die Tat wiegt auch im vorliegenden Fall schwer (§ 100a I Nr. 2 StPO), weil

[*nähere Ausführungen*].

4. Inhaber des/der oben genannten Telekommunikationsanschlusses/-anschlüsse ist (§ 100a III StPO)

□ der/die Beschuldigte.

□ eine Person, von der auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den/die Beschuldigte/-n bestimmte oder von ihm herrührende Mitteilungen entgegennimmt oder weitergibt.

□ eine sonstige Person, von der auf Grund bestimmter Tatsachen anzunehmen ist, dass der/die Beschuldigte ihren/ihre Anschluss/Anschlüsse benutzt.

[*nähere Ausführung der Tatsachen*]

5. Die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Beschuldigten wäre auf andere Weise wesentlich erschwert oder aussichtslos (§ 100a I Nr. 3 StPO), weil

□ andere Aufklärungsmittel einen erheblich größeren Zeitaufwand erfordern und deshalb zu einer wesentlichen Verfahrensverzögerung führen würden.

□ andere Aufklärungsmittel zu wesentlich schlechteren Erkenntnissen führen würden.

□ andere Aufklärungsmittel mit hoher Wahrscheinlichkeit keinen Erfolg versprechen.

□ andere erfolgversprechende Aufklärungsmittel nicht vorhanden sind bzw. nicht zur Verfügung stehen.

[*nähere Ausführungen*]

6. [*bei Quellen-TKÜ zusätzlich:*]

Der [*Adressat der Maßnahme*] bedient sich nach den bisherigen Ermittlungen für seine Kommunikation der Sprachübertragung [*bei Video-Internettelefonie zusätzlich*: Bildübertragung; *bei Instant Messaging via IP zusätzlich*: Textübertragung] in Echtzeit mittels Internetprotokoll (sog. Voice-over-IP). Dabei wird für die Kommunikation eine Software [*soweit vorliegend: Bezeichnung VoIP-Software*] benutzt, mittels derer die Telekommunikationsdaten bei der Übermittlung ver-

schlüsselt werden und deshalb für die Ermittlungsbehörden im Rahmen einer herkömmlichen Telekommunikationsüberwachungsmaßnahme nicht einsehbar und für das Ermittlungsverfahren nicht verwendbar sind, da die Daten nur in der verschlüsselten Form vorlägen. Zur technischen Umsetzung der Überwachungsmaßnahme ist es daher zwingend erforderlich, auf dem für die Kommunikation verwendeten [*Endgerät*] eine spezielle Überwachungssoftware zu installieren, die ein Abgreifen und Ausleiten der noch unverschlüsselten Telekommunikationsdaten vor der Verschlüsselung (ausgehende Daten) bzw. nach der Entschlüsselung (eingehende Daten) an die Ermittlungsbehörden vornimmt und hierdurch die Überwachung und Aufzeichnung der Telekommunikationsdaten ermöglicht. Der mit der heimlichen/verdeckten Installation sowie Deinstallation der Überwachungssoftware verbundene ausschließliche Eingriff in das Fernmeldegeheimnis aus Art. 10 I GG (vgl. BVerfG NJW 2008, 822, 826) ist als typische und verhältnismäßige Begleitmaßnahme zur Umsetzung der Überwachung und Aufzeichnung nach § 100a I StPO im Wege der Annexkompetenz zulässig, weil ein Sachzusammenhang gegeben ist, andere mildere Mittel nicht zur Verfügung stehen und der Maßnahmeadressat nicht unverhältnismäßig belastet wird (vgl. BGH NJW 2001, 1658, 1659 zu § 100c I S. 1 Nr. 1b StPO a. F.; zustimmend auch AG Bayreuth, Beschluss vom 17.09.2009 – Gs 911/09, MMR 2010, 266, 267; LG Hamburg, Beschluss vom 13.09.2010 – 608 Qs 17/10, MMR 2011, 693, 694; LG Landshut, Beschluss vom 20.01.2011 – 4 Qs 346/10, MMR 2011, 690, 691). Mit den in der Entscheidungsformel unter Ziff. II aufgeführten und bei der Konfiguration der Überwachungssoftware zu beachtenden Einschränkungen wird durch rechtliche Vorgaben und technische Vorkehrungen sichergestellt, dass sich die Überwachung ausschließlich auf Daten eines laufenden Telekommunikationsvorganges beschränkt, so dass es nicht zu einem Zugriff auf sonstige auf dem betroffenen [*Endgerät*] gespeicherte Daten und Dateien oder zu einer Überwachung von Datenverarbeitungsvorgängen, die nicht der Telekommunikation dienen (z. B. sog. Screenshots von grafischen Bildschirminhalten, Office- und Textverarbeitungsanwendungen, Grafik- und Multimediaanwendungen, Spiele u. ä.), kommt und keine Maßnahme von der Wirkung einer Online-Durchsuchung vorgenommen wird (vgl. BVerfG NJW 2008, 822, 826). [*Soweit der Quellcode der Überwachungssoftware dem Gericht bei Antragstellung vorgelegt wurde*: Die in vorliegender Sache zum Einsatz kommende Überwachungssoftware (*Bezeichnung, Softwareversion, Zertifizierungsnummer etc.*) stellt auf Grund der gewählten Textbausteine (*Textbausteinnummern u. ä.*) des bei Beantragung vorgelegten und bei Gericht hinterlegten Quellcodes eine entsprechende technische Beschränkung der Software sicher.] Entsprechend den spezifischen Besonderheiten des Einbringens einer Fremdsoftware in ein informationstechnisches System dienen die Vorgaben der Ziff. III der Entscheidungsformel durch Gewährleistung eines transparenten und – in den Grenzen des nach dem technischen Stand Möglichen und Zumutbaren – sicheren Einsatzes des technischen Mittels der Sicherstellung einer insgesamt verhältnismäßigen Handhabe der Ermittlungsmaßnahme in Bezug auf die technische Vorgehensweise und deren verfahrensmäßige Ausgestaltung, der Datenschutzkontrolle sowie der Beweismittelauthentizität und -integrität des erlangten Datenmaterials.

Die Überwachungsmaßnahme ist im vorliegenden Fall verhältnismäßig, da das Abgreifen der Telekommunikationsdaten auf dem zur verschlüsselten Telekommunikation genutzten [*Endgerät*] geeignet, erforderlich und angemessen ist, um den der Anordnung zugrunde liegenden, unter Punkt 1. näher beschriebenen Tatvorwurf aufzuklären und den Tatnachweis gegen den Beschuldigten zu führen. [*ggf. nähere Ausführungen*]

7. Auf Grund der bisherigen Ermittlungen liegen keine tatsächlichen Anhaltspunkte dafür vor, dass durch die vorliegende/-n Anordnung/-en der Überwachung der Telekommunikation allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden (§ 100a IV S. 1 StPO).

   [*nähere Ausführungen*]

8. Die Anordnung/-en war/-en gemäß § 33 IV StPO ohne vorherige Anhörung des/der Beschuldigten und der sonstigen Betroffenen zu treffen, um den Zweck der Ermittlungsmaßnahme nicht zu gefährden.

Ort, Datum

[*Unterschrift*]

Richter/-in am Amtsgericht

Anhang 2

Vorschlag für die Ergänzung der bestehenden strafprozessualen Regelungen der Telekommunikationsüberwachung de lege ferenda (§§ 100a, 100b StPO-E)

§ 100a StPO-E
[Überwachung der Telekommunikation]

(1) Auch ohne Wissen der Betroffenen darf die Telekommunikation überwacht und aufgezeichnet werden, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in *Absatz 3* bezeichnete schwere Straftat begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht, oder durch eine Straftat vorbereitet hat,
2. die Tat auch im Einzelfall schwer wiegt und
3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

(2) Die Überwachung und Aufzeichnung der Telekommunikation darf auch ohne Wissen des Betroffenen in der Weise erfolgen, dass mit technischen Mitteln in von dem Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn

1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird, und
2. der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen.[1]

(3) Schwere Straftaten im Sinne des Absatzes 1 Nr. 1 sind: (…)

(4) Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, 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 benutzt.

(5) [1]Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach *den Absätzen 1 und 2* allein Erkenntnisse aus dem Kernbereich

---

[1] Unter Heranziehung der in § 20l II S. 1 und § 20k II, III BKAG gewählten Formulierungen.

privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. [2]Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach *den Absätzen 1 und 2* erlangt wurden, dürfen nicht verwertet werden. [3]Aufzeichnungen hierüber sind unverzüglich zu löschen. [4]Die Tatsache ihrer Erlangung und Löschung ist aktenkundig zu machen.

§ 100b StPO-E
[Zuständigkeit für Anordnung der Überwachung der Telekommunikation und Umsetzung]

(1) [1]Maßnahmen nach § 100a *Abs. 1 und 2* dürfen nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden. [2]Bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft getroffen werden. [3]Soweit die Anordnung der Staatsanwaltschaft nicht binnen drei Werktagen von dem Gericht bestätigt wird, tritt sie außer Kraft. [4]Die Anordnung ist auf höchstens drei Monate zu befristen. [5]Eine Verlängerung um jeweils nicht mehr als drei Monate ist zulässig, soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen.

(2) [1]Die Anordnung ergeht schriftlich. [2]In ihrer Entscheidungsformel sind anzugeben:

1. soweit möglich, der Name und die Anschrift des Betroffenen, gegen den sich die Maßnahme richtet,
2. die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgerätes, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist,
3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes, *und*
4. *im Falle des § 100a Abs. 2 auch eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Datenerhebung eingegriffen werden soll.*[2]

(3) [1]Auf Grund der Anordnung hat jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt, dem Gericht, der Staatsanwaltschaft und ihren im Polizeidienst tätigen Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) die Maßnahmen nach § 100a *Abs. 1* zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen. [2]Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, bestimmt sich nach dem Telekommunikationsgesetz und der Telekommunikations-Überwachungsverordnung. [3]§ 95 Abs. 2 gilt entsprechend.

(4) [1]Bei Maßnahmen nach § 100a Abs. 2 ist technisch sicherzustellen, dass

1. *an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und*
2. *die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden.*

---

[2] Unter Heranziehung der in § 20l IV S. 1 Nr. 4 BKAG gewählten Formulierung.

[2]Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. [3]Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen. [4]Von dem Einhalten der technischen Anforderungen des § 100a Abs. 2 Nr. 1 sowie der Sätze 1 bis 3 ist in der Regel auszugehen, wenn ein vom Bundesamt für Sicherheit in der Informationstechnik zertifiziertes technisches Mittel eingesetzt wird. [5]Bei jedem Einsatz des technischen Mittels sind zu protokollieren

1. die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,

2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,

3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und

4. die Organisationseinheit, die die Maßnahme durchführt.

[6]Die Protokolldaten dürfen nur verwendet werden, um dem Betroffenen oder einer dazu befugten öffentlichen Stelle die Prüfung zu ermöglichen, ob die Maßnahme nach § 100a Abs. 2 rechtmäßig durchgeführt worden ist.[3] *[7]Sie sind unverzüglich zu löschen, soweit sie für den in Satz 6 genannten Zweck nicht mehr erforderlich sind.*[4]

(5) [1]Liegen die Voraussetzungen der Anordnung nicht mehr vor, so sind die auf Grund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden. [2]Nach Beendigung der Maßnahme ist das anordnende Gericht über deren Ergebnisse zu unterrichten.

(6) [1]Die Länder und der Generalbundesanwalt berichten dem Bundesamt für Justiz kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres über in ihrem Zuständigkeitsbereich angeordnete Maßnahmen nach § 100a. [2]Das Bundesamt für Justiz erstellt eine Übersicht zu den im Berichtsjahr bundesweit angeordneten Maßnahmen und veröffentlicht diese im Internet.

(7) In den Berichten nach Absatz 6 sind anzugeben:

1. die Anzahl der Verfahren, in denen Maßnahmen nach § 100a Abs. 1 *und Abs. 2* angeordnet worden sind;
2. die Anzahl der Überwachungsanordnungen nach § 100a Abs. 1 *und Abs. 2*, unterschieden nach
   a) Erst- und Verlängerungsanordnungen sowie
   b) Festnetz-, Mobilfunk- und Internettelekommunikation;
3. die jeweils zugrunde liegende Anlassstraftat nach Maßgabe der Unterteilung in § 100a *Abs. 3.*

---

[3] Unter Heranziehung der in § 20l II S. 1 und § 20k II, III BKAG gewählten Formulierungen.

[4] Unter Heranziehung der in § 31c IV S. 3 POG RP gewählten Formulierung.

Anhang 3

Fragenkatalog Experteninterviews

Zur Person (Behörde/Institution, Person, Funktion, Ort und Datum des Interviews)

Seit wann beschäftigen Sie sich mit dem Themengebiet der TK-Überwachung, insbesondere der sog. Quellen-TKÜ? Seit wann ist dies ein ermittlungsrelevantes Thema? Seit wann werden im Zuständigkeitsbereich Ihrer Behörde/Institution Quellen-TKÜ-Maßnahmen beantragt bzw. angeordnet bzw. durchgeführt?

Wie häufig wurden in den vergangenen Jahren im Zuständigkeitsbereich Ihrer Behörde/Institution Quellen-TKÜ-Maßnahmen beantragt bzw. angeordnet bzw. durchgeführt?

Von welchen Behörden/Institutionen wurden Quellen-TKÜ-Maßnahmen beantragt?

Welche Behörden/Institutionen greifen auf Ihre Behörde/Institution zurück, sowohl präventiv als auch repressiv gesehen?

Erfolgen die Quellen-TKÜ-Maßnahmen mehrheitlich zu präventiven Zwecken oder zu repressiven Zwecken?

Auf welche Rechtsgrundlagen werden Quellen-TKÜ-Maßnahmen hierbei jeweils gestützt?

Ist die präventive Quellen-TKÜ in Bayern gesetzlich geregelt?

Allgemein zum Begriff der „Quellen-TKÜ": Hierunter wird die Überwachung von Voice-over-IP-Kommunikation (VoIP), welche verschlüsselt über das Internet übertragen wird, verstanden. VoIP umfasst drei Konstellationen, und zwar 1. VoIP über den PC mittels spezieller Software (z. B. Skype), 2. VoIP über ein spezielles VoIP-Telefon (ohne PC) sowie 3. VoIP über ein normales Telefon mittels VoIP-fähigen Routers (ohne PC). Sind dies alles Problemfelder der Quellen-TKÜ?

Wie sieht es für VoIP über ein normales Telefon mittels VoIP-fähigen Routers (Konstellation 3) aus?

Ist die VoIP-Kommunikation mittels speziellen VoIP-Telefons bzw. mittels VoIP-fähigen Routers in einer Weise speziell verschlüsselt wie die VoIP über den PC bspw. über Skype (Konstellation 1)?

Ist Anwendungsbereich der Quellen-TKÜ nur Konstellation 1, sprich VoIP über den PC?

Ist Gegenstand der Quellen-TKÜ nur VoIP über die Kommunikationssoftware Skype oder auch anderer Anbieter?

Zur Quellen-TKÜ an sich: Die Quellen-TKÜ gliedert sich in zwei Maßnahmen. Die Primärmaßnahme, d. h. die Überwachung an sich, sowie die Sekundär-/Begleitmaßnahme, d. h. das Einbringen einer Überwachungssoftware in das Zielsystem. Es ist rechtlich umstritten, ob es für diese beiden Maßnahmen in der StPO gegenwärtig Rechtsgrundlagen gibt. Eine Ansicht hält § 100a StPO für eine ausreichende Rechtsgrundlage, sowohl für die Primärmaßnahme als auch für die Sekundärmaßnahme im Wege einer Annexkompetenz. Unter dem Eindruck der Entscheidung des BVerfG zur Online-Durchsuchung soll dies jedoch nur gelten, wenn technisch und rechtlich sichergestellt ist, dass die Überwachung auf Daten aus einem laufenden TK-Vorgang beschränkt ist. Wie fassen Sie den Begriff „laufender TK-Vorgang" auf?

Wird die Kommunikation im Zeitpunkt ihres Ablaufens überwacht?

Welche Art von Kommunikation lässt sich durch eine Quellen-TKÜ überwachen?

Wird bei einer Quellen-TKÜ nur das Tonmaterial ausgeleitet? Wird auch Bildmaterial ausgeleitet, welches bei einer Video-Telefonie bspw. über Skype ebenso anfällt, wie Tonmaterial, Stichwort „Video"-over-IP?

Weiter zur Primärmaßnahme, die auf Daten aus laufenden TK-Vorgängen beschränkt sein muss: Schwerpunkt der Kritik ist, ob es wirklich sauber gewährleistet werden kann, dass nur TK-Daten aufgezeichnet werden und nicht auch sonstige gespeicherte Daten, bspw. von der Festplatte. Ist diese Kritik gerechtfertigt?

Ist die Überwachungssoftware zur Quellen-TKÜ so konstruiert, dass keine sonstigen gespeicherten Daten, welche nicht aus einem laufenden TK-Vorgang stammen, erfasst werden?

Anknüpfungspunkt der kritischen Stimmen hierzu ist, dass trotz Beschränkungen im Beschluss sonstige Daten im Rahmen der technischen Umsetzung der Maßnahme aufgeschnappt werden könnten. Reichen allein Vorgaben im Beschluss aus, um die Tangierung sonstiger Daten zu verhindern?

Würden unzulässig gewonnene Erkenntnisse Ihrer Meinung nach in die Nähe von Beweisverwertungsverboten geraten?

Wie muss man sich die technische Umsetzung einer Quellen-TKÜ-Maßnahme vorstellen?

Welche technischen Standards werden eingesetzt?

Ist die Software immer auf den konkret vorliegenden Einzelfall zugeschnitten?

Wird die Quellen-TKÜ in der Regel mit anderen Maßnahmen verknüpft bzw. als eine Maßnahme neben anderen Maßnahmen durchgeführt?

Wird für die Anfertigung der Software im Vorfeld der Einsatz anderer Ermittlungsmaßnahmen benötigt?

Stichwort Sekundärmaßnahme, welche Sekundär-/Begleitmaßnahmen gibt es im Zusammenhang mit der Quellen-TKÜ?

Kommt auch der direkte Zugriff auf das Gerät vor Ort und ein manuelles Aufspielen der Überwachungssoftware in Betracht?

Welche Konstellationen des direkten Zugriffs sind denkbar? Wie sieht hier die Vorgehensweisen in der Praxis aus?

Wie wird verfahren, wenn sich das Gerät in Privaträumen befindet?

Wie muss man sich den Vorgang des Online-Einschleusens technisch vorstellen? Wird dem Verdächtigen die Software per E-Mail zugeschickt oder wird diese heimlich installiert während sich der Betroffene im Internet befindet?

Auf welche Rechtsgrundlage werden die Sekundärmaßnahmen gestützt? Sehen Sie diese von einer Annexkompetenz zu § 100a StPO gedeckt?

Ist die Infiltration des Systems mit der TK-Überwachungssoftware Ihrer Meinung nach eine typische sowie verhältnismäßige Sekundärmaßnahme?

Ist das Einschleusen einer Überwachungssoftware überhaupt erforderlich? Oder wäre es ein milderes Mittel, sich bei Skype bspw. einen Schlüssel zu besorgen?

Sehen Sie gesetzlichen Regelungsbedarf hinsichtlich des Ermittlungsinstruments der Quellen-TKÜ? Würden Sie es begrüßen, wenn eine Klarstellung der Quellen-TKÜ im Gesetz erfolgen würde, z. B. Ergänzung der §§ 100a, 100b StPO bzw. Schaffung einer neuen strafprozessualen Norm?

Sollte dann auch ein Betretungsrecht mitnormiert werden?

Sollte dann auch ein ausdrückliches Beweisverwertungsverbot mitnormiert werden?

Welche Bedeutung räumen Sie der Quellen-TKÜ im Vergleich zu anderen Maßnahmen, insbesondere auch zu anderen TK-Maßnahmen ein?

Wie sehen Sie die Zukunft dieser Ermittlungsmaßnahme?

Literaturverzeichnis

Albrecht, Florian: Rechtswidrige Online-Durchsuchung durch das Bayerische Landeskriminalamt. Anmerkung zu LG Landshut, Beschl. v. 20.01.2011 – 4 Qs 346/10, JurPC Web-Dok. 59/2011, Abs. 1–30

Albrecht, Florian/*Dienst*, Sebastian: Der verdeckte hoheitliche Zugriff auf informationstechnische Systeme – Rechtsfragen von Online-Durchsuchung und Quellen-TKÜ, JurPC Web-Dok. 5/2012, Abs. 1–65

Arbeitskreis „Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Technische Aspekte der Online-Durchsuchung, 21. August 2007, URL: http://www.lfd.mv.de/dschutz/informat/internet/onlinedurchsuchung.pdf [zuletzt aufgerufen 15.06.2012] (zit.: Arbeitskreis „Technische und organisatorische Datenschutzfragen, Technische Aspekte)

Arenz, Stefan: Der Schutz der öffentlichen Sicherheit in Next Generation Networks am Beispiel von Internet-Telefonie-Diensten (VoIP) – Zugleich eine Einordnung von Internet-Telefonie-Diensten in telekommunikationsrechtliche Kategorien unter Berücksichtigung europarechtlicher Vorgaben, Berlin 2010 (zit.: *Arenz*, Der Schutz der öffentlichen Sicherheit in Next Generation Networks am Beispiel von Internet-Telefonie-Diensten)

Backes, Otto/*Gusy*, Christoph: Wer kontrolliert die Telefonüberwachung? – Eine empirische Untersuchung zum Richtervorbehalt bei der Telefonüberwachung, Frankfurt am Main 2003 (zit.: *Backes*/*Gusy*, Wer kontrolliert die Telefonüberwachung?)

Bär, Wolfgang: Handbuch zur EDV-Beweissicherung im Strafverfahren, Stuttgart/München/Hannover/Berlin/Weimar/Dresden 2007 (zit.: *Bär*, Handbuch zur EDV-Beweissicherung)

– Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen – Gesetzliche Neuregelungen zum 1.1.2008, MMR 2008, 215–222

– Anmerkung zu LG Hamburg, Beschluss vom 01.10.2007 – 629 Qs 29/07, MMR 2008, 425–427

– TK-Überwachung, §§ 100a-101 StPO mit Nebengesetzen, Kommentar, Köln/München 2010 (zit.: *Bär*, TK-Überwachung)

– Anmerkung zu AG Bayreuth, Beschluss vom 17.09.2009 – Gs 911/09, MMR 2010, 267–268

– Anmerkung zu LG Landshut, Beschluss vom 20.01.2011 – 4 Qs 346/10, MMR 2011, 691–693

Basak, Denis: Strafbare Verfolger?, in: Legal Tribune ONLINE vom 13.10.2011, URL: http://www.lto.de/recht/hintergruende/h/trojaner-einsatz-strafbare-strafverfolger/ [zuletzt aufgerufen 15.06.2012]

Bayerischer Landesbeauftragter für den Datenschutz: 24. Tätigkeitsbericht, Berichtszeitraum: 2009/2010, Veröffentlichungsdatum: 01.02.2011, URL: http://www.datenschutz-bayern.de/tbs/tb24/tb24.pdf [zuletzt aufgerufen 15.06.2012] (zit.: Bayerischer Landesbeauftragter für den Datenschutz, 24. Tätigkeitsbericht)

Becker, Christian/*Meinicke*, Dirk: Die sog. Quellen-TKÜ und die StPO – Von einer „herrschenden Meinung" und ihrer fragwürdigen Entstehung –, StV 2011, 50–52

Beck'scher Online-Kommentar GG: Beck'scher Online-Kommentar zum Grundgesetz, herausgegeben von Volker Epping und Christian Hillgruber, Edition: 13, Stand: 01.01.2012, München 2012 (zit.: BeckOK – *Bearbeiter*, GG, Ed. 13)

Beck'scher Online-Kommentar StGB: Beck'scher Online-Kommentar zum Strafgesetzbuch, herausgegeben von Bernd von Heintschel-Heinegg, Edition: 17, Stand: 01.12.2011, München 2011 (zit.: BeckOK – *Bearbeiter*, StGB, Ed. 17)

Beck'scher Online-Kommentar StPO: Beck'scher Online-Kommentar zur Strafprozessordnung, herausgegeben von Jürgen Peter Graf, Edition: 13, Stand: 01.02.2012, München 2012 (zit.: BeckOK – *Bearbeiter*, StPO, Ed. 13)

Beck'scher TKG-Kommentar: Beck'scher TKG-Kommentar, herausgegeben von Martin Geppert, Hermann-Josef Piepenbrock, Raimund Schütz und Fabian Schuster, 3. Auflage, München 2006 (zit.: Beck'scher TKG-Kommentar – *Bearbeiter*)

Berner, Georg/*Köhler*, Gerd Michael/*Käß*, Robert: Polizeiaufgabengesetz, 20. Auflage, Heidelberg/München/Landsberg/Berlin 2010 (zit.: *Berner*/*Köhler*/*Käß*, BayPAG)

Böckenförde, Thomas: Die Ermittlung im Netz – Möglichkeiten und Grenzen neuer Erscheinungsformen strafprozessualer Ermittlungstätigkeit, Tübingen 2003 (zit.: *Böckenförde*, Die Ermittlung im Netz)

Braun, Frank: Unzulässige Online-Durchsuchung durch das bayerische Landeskriminalamt, jurisPR-ITR 3/2011 Anm. 3

Braun, Frank/*Roggenkamp*, Jan Dirk: Ozapftis – (Un)Zulässigkeit von „Staatstrojanern", K&R 2011, 681–686

Brodowski, Dominik: Anmerkung zu LG Landshut, Beschluss vom 20.01.2011 – 4 Qs 346/10, JR 2011, 533–538

Brodowski, Dominik/*Freiling*, Felix C.: Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, Forschungsforum Öffentliche Sicherheit, Schriftenreihe Sicherheit Nr. 4, März 2011, URL: http://www.sicherheit-forschung.de/schriftenreihe/sr_v_v/sr_4.pdf [zuletzt aufgerufen 15.06.2012] (zit.: *Brodowski*/*Freiling*, Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft)

Brunst, Phillip W.: Anonymität im Internet – rechtliche und tatsächliche Rahmenbedingungen, Berlin 2009 (zit.: *Brunst*, Anonymität im Internet)

Buermeyer, Ulf: Die „Online-Durchsuchung". Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, HRRS 2007, 154–166

– Quellen-TKÜ – ein kleines Einmaleins (nicht nur) für Ermittlungsrichter, Oktober 2011, URL: http://ijure.org/wp/archives/756 [zuletzt aufgerufen 15.06.2012]

Buermeyer, Ulf/*Bäcker*, Matthias: Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des § 100a StPO, HRRS 2009, 433–441

Bundesministerium des Innern: Stellungnahme zu VoiP, 16. Juni 2004, URL: http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Stellungnahmen/BMIBundesministeriumdesInId676pdf.pdf?__blob=publicationFile [zuletzt aufgerufen 15.06.2012]

– Fragenkatalog des Bundesministeriums der Justiz, 22. August 2007, URL: http://www.netzpolitik.org/wp-upload/fragen-online durchsuchung-BMJ.pdf [zuletzt aufgerufen 15.06.2012] (zit.: Bundesministerium des Innern, Fragenkatalog BMJ)

– Fragenkatalog der SPD-Bundestagsfraktion, AG Kultur und Medien, AG Neue Medien, 22. August 2007, URL: http://www.netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf [zuletzt aufgerufen 15.06.2012] (zit.: Bundesministerium des Innern, Fragenkatalog SPD)

Bundesministerium für Wirtschaft und Technologie: Breitbandatlas 2009_02, Teil II des Berichts zum Atlas für Breitband-Internet des Bundesministeriums für Wirtschaft und Technologie – Methodik & weitere Ergebnisse, 15. Dezember 2009, URL: http://www.zukunft-breitband.de/Dateien/BBA/PDF/breitbandatlas-bericht-2009-02-teil2,property=pdf,bereich=bba,sprache=de,rwb=true.pdf [zuletzt aufgerufen 15.06.2012] (zit.: Bundesministerium für Wirtschaft und Technologie, Breitbandatlas 2009_02)

Bundesnetzagentur: Anhörung zu Voice over IP (VoIP) – Zusammenfassende Auswertung der jeweiligen Fragenkomplexe, URL: http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Auswertung/ThemenweiseAuswertungId3173pdf.pdf?__blob=publicationFile [zuletzt aufgerufen 15.06.2012] (zit.: Bundesnetzagentur, Anhörung zu Voice over IP (VoIP) – Zusammenfassende Auswertung der jeweiligen Fragenkomplexe)

– Eckpunkte der regulatorischen Behandlung von Voice over IP (VoIP), 09.09.2005, URL: http://www.bundesnetzagentur.de/ SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Eckpunkte/EckpunktederregulatorischenId3210pdf.pdf?__blob=publicationFile [zuletzt aufgerufen 15.06.2012] (zit.: Bundesnetzagentur, Eckpunkte der regulatorischen Behandlung von Voice over IP)

Bundesrechtsanwaltskammer: Stellungnahme der Bundesrechtsanwaltskammer zum Gesetzentwurf der Bundesregierung zum Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG BR-Drucks. 275/07, August 2007, BRAK-Stellungnahme-Nr. 31/2007, URL: http://www.brak.de/w/files/stellungnahmen/Stn31-2007.pdf [zuletzt aufgerufen 15.06.2012] (zit.: Bundesrechtsan-

waltskammer, Stellungnahme zum Gesetzentwurf der Bundesregierung zum Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG)

Demko, Daniela: Die Erstellung von Bewegungsbildern mittels Mobiltelefon als neuartige strafprozessuale Observationsmaßnahme, NStZ 2004, 57–64

Dinger, Jochen: Das Potential von Peer-to-Peer-Netzen und -Systemen – Architekturen, Robustheit und rechtliche Verortung, Karlsruhe 2009 (zit.: *Dinger*, Das Potential von Peer-to-Peer-Netzen und -Systemen)

Eckhardt, Jens: Die Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen – Ein kritischer Überblick über die geplanten Änderungen in der StPO zur Umsetzung der Cybercrime Convention, CR 2007, 336–344

Epping, Volker: Grundrechte, in Zusammenarbeit mit Sebastian Lenz und Philipp Leydecker, Berlin – Heidelberg 2004 (zit.: *Epping*, Grundrechte)

Gercke, Marco: Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit – Der Einsatz softwarebasierter Ermittlungsinstrumente zum heimlichen Zugriff auf Computerdaten, CR 2007, 245–253

Gercke, Marco/*Brunst*, Phillip W.: Praxishandbuch Internetstrafrecht, Stuttgart 2009 (zit.: *Gercke*/*Brunst*, Internetstrafrecht)

Hansen, Markus/*Krause*, Christian: Heimliche Online-Durchsuchung – Wie geht's, wie schütze ich mich?, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Sommerakademie 2007-08-27, Kiel, URL: https://www.datenschutzzentrum.de/sommerakademie/2007/sak2007-hansen-krause-online-durchsuchung.pdf [zuletzt aufgerufen 15.06.2012] (zit.: *Hansen*/*Krause*, Sommerakademie 2007)

Hansen, Markus/*Pfitzmann*, Andreas: Online-Durchsuchung, Technische Grundlagen von Online-Durchsuchung und -Beschlagnahme, DRiZ 2007, 225–230

Henrichs, Axel: Zur rechtlichen Zulässigkeit der Quellen-TKÜ, Kriminalistik 2008, 438–443

Hoeren, Thomas: Das Telemediengesetz, NJW 2007, 801–806

Hoffmann-Riem, Wolfgang: Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2008, 1009–1022

Holznagel, Bernd/*Bonnekoh*, Mareike: Voice over IP – Regulierungsbedarf und erste Lösungen, MMR 2005, 585–591

Holznagel, Bernd/*Schumacher*, Pascal: Auswirkungen des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme auf RFID-Chips, MMR 2009, 3–8

Hornung, Gerrit: Ermächtigungsgrundlage für die „Online-Durchsuchung"?, DuD 2007, 575–580

Jäger, Christian: Grund und Grenzen des Gesetzlichkeitsprinzips im Strafprozessrecht, GA 2006, 615–628

Jahn, Matthias: Sicherstellung von E-Mails beim E-Mail-Provider, Anmerkung zu BGH, Beschluss vom 31.03.2009 – 1 StR 76/09, JuS 2009, 1048–1049

Jahn, Matthias/*Kudlich*, Hans: Die strafprozessuale Zulässigkeit der Online-Durchsuchung, JR 2007, 57–61

Karlsruher Kommentar zur StPO: Karlsruher Kommentar zur Strafprozessordnung mit GVG, EGGVG und EMRK, herausgegeben von Rolf Hannich, 6., neu bearbeitete Auflage, München 2008 (zit.: KK – *Bearbeiter*, StPO)

Käß, Robert: Die Befugnis zum verdeckten Zugriff auf informationstechnische Systeme im bayerischen Polizeiaufgabengesetz (sog. Online-Überwachung oder Online-Durchsuchung), BayVBl. 2010, 1–15

Katko, Peter: Voice-over-IP – Entscheidender Schritt zur Konvergenz oder nur preiswert Telefonieren?, CR 2005, 189–193

Klesczewski, Diethelm: Straftataufklärung im Internet – Technische Möglichkeiten und rechtliche Grenzen von strafprozessualen Ermittlungseingriffen im Internet, ZStW 2011, 737–766

Köhler, Thomas R./*Kirchmann*, Walter: IT von A bis Z – Das schnelle und kompakte Nachschlagewerk, Frankfurt am Main 2008 (zit.: *Köhler*/*Kirchmann*, IT von A bis Z)

Kudlich, Hans: Der heimliche Zugriff auf Daten in einer Mailbox: ein Fall der Überwachung des Fernmeldeverkehrs? – BGH, NJW 1997, 1934, JuS 1998, 209–214

– Strafprozessuale Probleme des Internets – Rechtliche Probleme der Beweisgewinnung in Computernetzen –, JA 2000, 227–234

– Mitteilung der Bewegungsdaten eines Mobiltelefons als Überwachung der Telekommunikation – BGH, NJW 2001, 1587, JuS 2001, 1165–1169

– Zur Zulässigkeit strafprozessualer Online-Durchsuchungen, HFR 2007, 202–213

– Enge Fesseln für „Landes- und Bundestrojaner" – Anforderungen an die Zulässigkeit einer (sicherheitsrechtlichen) Online-Durchsusuchung, JA 2008, 475–478

– An der Quelle angezapft – zur Zulässigkeit einer Quellen-TKÜ im Strafverfahren, JA 2010, 310–312

– Strafverfolgung im Internet – Bestandsaufnahme und aktuelle Probleme –, GA 2011, 193–208

Löffelmann, Markus: Die Neuregelung der akustischen Wohnraumüberwachung, NJW 2005, 2033–2036

– Das Gesetz zur Umsetzung des Urteils des Bundesverfassungsgerichts vom 3. März 2004 (akustische Wohnraumüberwachung), ZIS 2006, 87–98

– Aktuelle Rechtsprobleme der Telekommunikationsüberwachung, AnwBl 2006, 598–602

Löwe-Rosenberg: Die Strafprozessordnung und das Gerichtsverfassungsgesetz, Großkommentar, herausgegeben von Peter Rieß, 25., neubearbeitete Auflage,

Zweiter Band, §§ 72-136a, Berlin 2004 (zit.: Löwe-Rosenberg – *Bearbeiter*, StPO und GVG, Zweiter Band)

– Die Strafprozessordnung und das Gerichtsverfassungsgesetz, Großkommentar, herausgegeben von Volker Erb, Robert Esser, Ulrich Franke, Kirsten Graalmann-Scheerer, Hans Hilger und Alexander Ignor, 26., neu bearbeitete Auflage, Erster Band, Einleitung; §§ 1-47; Sachregister, Berlin 2006 (zit.: Löwe-Rosenberg – *Bearbeiter*, StPO und GVG, Erster Band)

Martini, Mario/*Zimmermann*, Georg von: Voice-over-IP am regulatorischen Scheideweg, CR 2007, 368–373

– E-Mail und integrierte VoIP-Services: Telekommunikationsdienste i. S. d. § 3 Nr. 24 TKG?, CR 2007, 427–431

Maunz, Theodor/*Dürig*, Günter: Grundgesetz-Kommentar, herausgegeben von Roman Herzog, Rupert Scholz, Matthias Herdegen und Hans H. Klein, 61. Ergänzungslieferung Januar 2011, München 2011 (zit.: Maunz/Dürig – *Bearbeiter*, GG)

Meinberg, Ralf: Voice over IP: IP-basierter Sprachdienst vor dem Hintergrund des novellierten TKG, Münster 2008 (zit.: *Meinberg*, Voice over IP: IP-basierter Sprachdienst vor dem Hintergrund des novellierten TKG)

Meyer-Goßner, Lutz: Strafprozessordnung mit GVG und Nebengesetzen, 53., neu bearbeitete Auflage, München 2010 (zit.: Meyer-Goßner – *Bearbeiter*, StPO)

Platz, Ernst: Rechtliche Zulässigkeit von „Remote Forensic Software“ in der Schweiz, sic! 11/2008, 838, URL: https://www.sic-online.ch/fileadmin/user_upload/Sic-Online/2008/documents/838.pdf [zuletzt aufgerufen 15.06.2012]

Puschke, Jens/*Singelnstein*, Tobias: Telekommunikationsüberwachung, Vorratsdatenspeicherung und (sonstige) heimliche Ermittlungsmaßnahmen der StPO nach der Neuregelung zum 1.1.2008, NJW 2008, 113–119

Sankol, Barry: Überwachung von Internet-Telefonie – Ein Schatten im Lichte der §§ 100a ff. StPO, CR 2008, 13–18

Schneider, Hartmut: Zur Zulässigkeit strafprozessualer Begleitmaßnahmen im Zusammenhang mit dem Abhören des nicht öffentlich gesprochenen Wortes in Kraftfahrzeugen, NStZ 1999, 388–391

Seitlinger, Michael/*Strobl*, Klaus: Voice over IP – eine rechtliche Beurteilung vom Kommunikationsdienst bis zum Netzzugang, August 2005, URL: http://www.it-law.at/uploads/tx_publications/Voice_over_IP__eine_rechtliche_Beurteilung_vom_Kommunikationsdienst_bis_zum_Netzzugang.pdf [zuletzt aufgerufen 15.06.2012] (zit.: *Seitlinger*/*Strobl*, Voice over IP – eine rechtliche Beurteilung vom Kommunikationsdienst bis zum Netzzugang)

Sieber, Ulrich: Stellungnahme zu dem Fragenkatalog des Bundesverfassungsgerichts in dem Verfahren 1 BvR 370/07 zum Thema der Online-Durchsuchungen, Version 1.0 vom 9. Oktober 2007 (endg.) zur Anhörung in der mündlichen Verhandlung am 10. Oktober 2007, Max-Planck-Institut für ausländisches und internationales Strafrecht, 2007, URL: http://www.mpicc.de/shared/data/pdf/bverfg-sieber-1-endg.pdf [zuletzt aufgerufen 15.06.2012] (zit.: *Sieber*, Stellungnahme zu dem Fragenkatalog des BVerfG in dem Verfahren 1 BvR 370/07)

– Gutachten zum 69. Deutschen Juristentag 2012 (*im Erscheinen*) (zit.: *Sieber*, Gutachten zum 69. Deutschen Juristentag 2012)

Skype Technologies S.A.: Stellungnahme an die Bundesnetzagentur, 18. Juni 2004, URL: http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/Telekommunikation/Regulierung/VoiceOverIP/Stellungnahmen/SkypeTechnologiesId714pdf.pdf?__blob=publicationFile [zuletzt aufgerufen 15.06.2012]

Spindler, Gerald/*Schuster*, Fabian: Recht der elektronischen Medien, Kommentar, herausgegeben von Gerald Spindler und Fabian Schuster, 2. Auflage, München 2011 (zit.: Spindler/Schuster – *Bearbeiter*)

Spoenle, Jan: Unzulässigkeit der Installation von Spähsoftware zu Deanonymisierungszwecken, jurisPR-ITR 6/2010 Anm. 5

Stadler, Thomas: Zulässigkeit der heimlichen Installation von Überwachungssoftware – Trennung von Online-Durchsuchung und Quellen-Telekommunikationsüberwachung möglich?, MMR 2012, 18–20

Statistisches Bundesamt: Wirtschaftsrechnungen, Private Haushalte in der Informationsgesellschaft – Nutzung von Informations- und Kommunikationstechnologien, 2011, Fachserie 15 Reihe 4, Wiesbaden 2011, URL: https://www.destatis.de/DE/Publikationen/Thematisch/EinkommenKonsumLebensbedingungen/PrivateHaushalte/PrivateHaushalteIKT2150400117004.pdf?__blob=publicationFile [zuletzt aufgerufen 15.06.2012] (zit.: Statistisches Bundesamt, Wirtschaftsrechnungen 2011)

Systematischer Kommentar StPO: SK-StPO, Systematischer Kommentar zur Strafprozessordnung mit GVG und EMRK, herausgegeben von Jürgen Wolter, Band II, §§ 94–136a StPO, 4., neu bearbeitete Auflage, Köln 2010 (zit.: SK – *Bearbeiter*, StPO)

Thüringer Landesbeauftragter für den Datenschutz: 8. Tätigkeitsbericht, Berichtszeitraum: 01.01.2008 – 31.12.2009, Veröffentlichungsdatum: 20.05.2010, URL: http://www.thueringen.de/imperia/md/content/datenschutz/taetigkeitsberichte/microsoft_word_-_tlfd08-_endfassung_stand_07.06.2010_f__r_internet.pdf [zuletzt aufgerufen 15.06.2012] (zit.: Thüringer Landesbeauftragter für den Datenschutz, 8. Tätigkeitsbericht)

Vogel, Joachim/*Brodowski*, Dominik: Unzulässigkeit einer Beschwerde durch die StA und Aufspielen von Entschlüsselungssoftware – Anmerkung zu OLG Hamburg, Beschluss vom 12.11.2007 – 6 Ws 1/07 –, StV 2009, 632–635

Vormbaum, Thomas/*Asholt*, Martin: Der Große Lauschangriff vor dem Bundesverfassungsgericht – Verfahren, Nachspiel und Presse-Echo, Münster 2005 (zit.: *Vormbaum*/*Asholt*, Der Große Lauschangriff vor dem Bundesverfassungsgericht)

Welp, Jürgen: Die Gestellung des verhandlungsunfähigen Angeklagten, JR 1991, 265–272

Willer, Christoph/*Hoppen*, Peter: Computerforensik – Technische Möglichkeiten und Grenzen, CR 2007, 610–616

Wohlers, Wolfgang/*Demko*, Daniela: Der strafprozessuale Zugriff auf Verbindungsdaten (§§ 100 g, 100 h StPO), StV 2003, 241–248

Verzeichnis Experteninterviews

Bär, Wolfgang: Richter am Oberlandesgericht Bamberg, seit 01.11.2011 Leiter Referat Internetkriminalität, Missbrauch neuer Technologien und Kriminologie im Bayerischen Staatsministerium der Justiz, persönliches Gespräch, Oberlandesgericht Bamberg, Wilhelmsplatz 1, Bamberg, 09.12.2010

Schellinger, Jürgen: Berater „Kommunikationsspuren", Inspektion 380 (TEUS) – Technische Einsatzunterstützung und Service, Landeskriminalamt Baden-Württemberg, schriftliche Befragung, Stuttgart, 03.09.2010

Thönnes, Michael: Leiter der Projektgruppe TKÜ-CC (Kompetenzzentrum für TKÜ), Landeskriminalamt Rheinland-Pfalz, schriftliche Befragung, Mainz, 26.10.2010

Wirth, Ernst: Leiter Sachgebiet 633 – Kompetenzzentrum TKÜ Bayern, Landeskriminalamt Bayern, persönliches Gespräch, Bayerisches Landeskriminalamt, Maillinger Str. 15, München, 12.11.2010

Sachregister