Dr. Matthias Krauß
Bundesanwalt b. BGH

Karlsruhe, 30. Mai 2017

Stellungnahme zum Gesetzentwurf zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze

BT-Drs. 18/112727 und Formulierungshilfe der Bundesregierung für einen Änderungsantrag der Fraktionen CDU/CSU und SPD vom 15.05.2017 – A-Drs. 18 (6) 334

hier: Öffentliche Anhörung im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages am 31.05.2017

Der Änderungsantrag betrifft die Schaffung einer Rechtsgrundlage für die Quellen-Telekommunikationsüberwachung und die sogenannte Online-Durchsuchung. Es handelt sich um Überwachungsmaßnahmen, die regelmäßig ohne Kenntnis der Betroffenen heimlich durchgeführt werden und dabei tief in die Privatsphäre eingreifen können. Betroffen ist bei der Quellen-TKÜ in erster Linie das Grundrecht aus Art. 10 Abs. 1 GG, bei der Online-Durchsuchung der Schutzbereich des neuen Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gem. Art. 2 Abs. 1 i.V.m. Art. 1 GG. Der Zugriff auf informationstechnische Systeme stellt einen erheblichen Eingriff dar. Dies gilt für die Quellen-TKÜ, weil mit der Infiltration des Systems die Hürde genommen ist, um das System insgesamt auszuspähen.[1] Noch weitergehender ist der Grundrechtseingriff bei der Online-Durchsuchung, da personenbezogene Daten des Betroffenen erfasst werden können, die allein oder in ihrer technischen Vernetzung Einblick in wesentliche Teile der Lebensgestaltung einer Person oder ein aussagekräftiges Bild der Persönlichkeit gewähren können. Das BVerfG hat deshalb hohe verfassungsrechtliche Anforderungen für diese Eingriffe in die Grundrechte gemäß Art. 10 Abs. 1 und Art. 2 Abs. 1 i.V.m. Art. 1 GG aufgestellt.[2] Die dort für die Zulässigkeit der Eingriffsmaßnahmen im präventiven Bereich aufgestellten Grundsätze sind auch Maßstab für die Beurteilung der hier gegenständlichen Regelungen im repressiven Bereich.

Gerade das Strafrecht mit seinen oft weitreichenden Folgen für den Betroffenen steht in besonderem Maße unter dem verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit. Die Einräumung der hier in Rede stehenden Befugnisse an die Strafverfolgungsbehörden muss demnach einem legitimen Ziel dienen, zu dessen Erreichung geeignet und erforderlich sowie verhältnismäßig im engeren Sinne sein, d.h. die den Eingriff rechtfertigenden Gründe müssen die Bedeutung der betroffenen Grundrechte und die Intensität seiner Eingriffe überwiegen.

[1] BVerfGE 120, 274 Rz. 170.

[2] Vgl. nur BVerfG Urteil vom 27.2.2008, 1BvR 370/07 zu § 5 Abs. 2 Nr. 11 Satz 1 Alt. 2 VSG NRW; Urteil vom 20.4.2016, 1BvR 966/09 zu §§ 20k, l BKAG.

Das Ob und Wie staatlicher Strafverfolgung muss in einem angemessenen Verhältnis zur Schwere und Bedeutung der Straftat stehen, die Intensität des Verdachts muss die jeweilige Maßnahme rechtfertigen und diese insgesamt als zumutbar erscheinen.

Unter Anlegung dieses Maßstabes bestehen gegen die vorgeschlagenen Regelungen nicht nur keine grundsätzlichen Bedenken, vielmehr kommt der Gesetzgeber mit den vorgeschlagenen Ermittlungsmaßnahmen seiner Verpflichtung nach, ein Prozessrecht zu schaffen, das zur Gewährleistung einer effektiven Strafverfolgung erforderlich ist. Die Notwendigkeit einer funktionsfähigen Strafrechtspflege gehört zum Rechtsstaatsprinzip und genießt Verfassungsrang. Es handelt sich um einen Teilaspekt der verfassungsrechtlich gewährleisteten Pflicht zur Justizgewährung. Der Rechtsstaat hat seine freiheitsverbürgende Aufgabe nicht nur dadurch zu erfüllen, dass er den Einzelnen vor unverhältnismäßigen oder den Kernbereich seiner Persönlichkeit oder der Menschenwürde verletzenden staatlichen Zugriffen schützt, sondern ihm obliegt als verfasste Friedens- und Ordnungsmacht eine durch seine Rechtsordnung zu erfüllende Schutzpflicht für das Gemeinwesen, deren wirksame Erfüllung die Voraussetzung für die Anerkennung des von ihm in Anspruch genommenen Gewaltmonopols darstellt. Um dieser Schutzpflicht Rechnung zu tragen, sind aufgrund der technischen Entwicklungen im Kommunikationsbereich Ergänzungen bei den strafprozessualen Eingriffsbefugnissen erforderlich. Aufgrund der vermehrten Nutzung elektronischer oder digitaler Kommunikationsmittel und deren Vordringen in alle Lebensbereiche und der damit einhergehenden Verschlüsselung der Daten wird es den Strafverfolgungsbehörden zunehmend erschwert, ihre gesetzlichen Aufgaben wirksam wahrzunehmen. Es besteht deshalb gesetzgeberischer Handlungsbedarf, um auch zukünftig die Sicherheit des Staates als verfasster Friedens- und Ordnungsmacht und die Sicherheit der Bevölkerung vor Gefahren für Leib, Leben, Freiheit und anderen wichtigen Rechtsgütern zu gewährleisten.

I. Eignung und Erforderlichkeit

1. Es steht außer Frage, dass die Ermittlungsinstrumente der Quellen-TKÜ und Online-Durchsuchung nicht nur geeignet sind, den Strafverfolgungsbehörden zur Erfüllung ihrer Aufgaben einer effektiven Strafverfolgung zu dienen. Die vorgesehenen Maßnahmen stellen vielmehr einen deutlichen Mehrwert für eine effiziente und effektive Strafverfolgung dar.

2. Die Quellen-TKÜ ist auch dringend erforderlich, um die Ermittlungsbefugnisse dem rasanten Fortschritt moderner Kommunikationstechnologien anzupassen. Aufgrund der Internettelefonie und der zunehmenden Kommunikation über Instant-Messenger-Gruppen wie etwa WhatsApp-Nutzergruppen, bei der die VoIP-Software automatisch eine Verschlüsselung der Daten während der Übermittlung im Datennetz vornimmt, läuft die bisherige Telekommunikationsüberwachung gem. § 100a StPO weitgehend ins Leere, weil sie den Ermittlungsbehörden nur kryptierte Daten liefert, die praktisch nicht entschlüsselt werden können. Damit ist ein Eckpfeiler erfolgreicher Ermittlungen insbesondere im Bereich der Verfolgung schwerer und organisierter Kriminalität weggefallen. Nur in einem geringen Teil der Ermittlungsverfahren wird Kommunikation noch auf bisherigem Weg, also unverschlüsselt, durchgeführt, in der Mehrzahl der Fälle führt die wachsende Rele-

vanz der Voice-over-IP-Kommunikation zu gravierenden verschlüsselungsbedingten Ausfällen bei der Überwachung. Eine zuverlässige Ermittlung von Organisationsstrukturen, arbeitsteiligem Zusammenwirken von Tätergruppierungen und gemeinsamen Absprachen im Zusammenhang mit der Planung und Vorbereitung von Straftaten, aber auch von computerspezifischen Delikten wird zunehmend erschwert. In zahlreichen Fällen ist zu beobachten, dass die Beschuldigten bewusst verschlüsselte Kommunikation zur Verschleierung ihrer Tätigkeiten einsetzen.

Zur Lösung des Problems ist es erforderlich, die VoIP-Kommunikation vor deren Verschlüsselung bzw. nach deren Entschlüsselung, mithin an der Quelle durch Installation einer speziellen Überwachungssoftware auf dem Computer des Betroffenen abzugreifen und zur Aufzeichnung an die Ermittlungsbehörde auszuleiten. Andere mildere Maßnahmen sind nicht ersichtlich. Eine theoretisch denkbare Verpflichtung der Provider zur Verfügungstellung unverschlüsselter Daten ist kein geeignetes Mittel. Zum einen werben die Anbieter von IP-Telefonie gerade damit, dass die über sie geführte Kommunikation abhörsicher sei. Zum anderen besteht auch keine rechtliche Regelung, die Softwareanbieter dazu verpflichtet, mit deutschen Ermittlungsbehörden auf dem Gebiet der Strafverfolgung zusammenzuarbeiten und in ihre verschlüsselten Kommunikationsprogramme Backdoors einzubauen, um den Strafverfolgern Zugang zu den Gesprächsinhalten zu verschaffen. Hinzu kommt, dass die entsprechenden Softwareanbieter meist im Ausland ansässig sind, weshalb deutsche Rechtsvorschriften in die Leere laufen würden.

3. Entsprechendes gilt für die Online-Durchsuchung. Die offene Beschlagnahme von Computern und Festplatten läuft gerade im Bereich hoch konspirativ arbeitender krimineller Netzwerke wegen höchst wirksamer Kryptierungsverfahren, Anonymisierung und Zugangssicherungen z.B. durch die Verschleierung von IP-Adressen oder die Verwendung von Passwörtern zunehmend ins Leere. Aufgrund der Entwicklung auf dem Gebiet der Verschlüsselungstechnik ist heute nicht mehr gewährleistet, dass die Daten bei einer Beschlagnahme noch ausgewertet werden können.

4. Eine gesetzliche Regelung der Eingriffsbefugnis der Quellen-TKÜ ist schließlich aus Gründen der Rechtssicherheit erforderlich.

   Bekanntlich ist allein Artikel 10 Abs. 1 GG der grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zu einer Quellen-TKÜ,[3] wenn sich die Quellen-TKÜ darauf beschränkt, Inhalte und Umstände der laufenden Telekommunikation im Rechnernetz zu erheben oder darauf bezogene Daten auszuwerten und diese Beschränkung durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt ist. Ausgehend von dieser Rechtsprechung wird in Teilen der Rechtsprechung und Literatur vertreten, dass die Quellen-TKÜ als Überwachung und Aufzeichnung von Telekommunikation auf der Grundlage der §§ 100a, 100b StPO rechtlich möglich sei.[4] Dass der Zugriff auf die Inhal-

[3] BVerfGE 120, 274 ff., Rz. 166, 172.

[4] Vgl. AG Bayreuth, MMR 2010, 266; LG Hamburg MMR 2011, 693; LG Landshut MMR 2011, 690 (mit zustimmender Anm. Bär, MMR 2011, 6 und abl. Anm. Brodowski, JR 2011, 533 sowie Albrecht, JurPC Web-Dok 59/2011 und Braun, jurisPR-ITR 3/2011 Anm. 3); KMR/Bär StPO § 100a Rn. 331b; Bär, MMR 2008, 315; BeckOK/Graf StPO § 100a Rn. 107c; Meyer/Goßner StPO 57. Aufl. § 100a Rn. 7a; KK/Bruns § 100a Rn. 28 (für ei-

te der Telekommunikation bei der Quellen-TKÜ gerade nicht über den Provider erfolge, sondern an ihm vorbei unmittelbar bei einem der Teilnehmer, sei unerheblich, weil aus der Tatsache, dass § 100b Abs. 3 StPO bestimmte TK-Dienstleister zur Mitwirkung an gerichtlich angeordneten Überwachungsmaßnahmen verpflichtet, sich nicht folgern lassen, dass TKÜ-Maßnahmen überhaupt nur dann erlaubt sein sollen, wenn der Provider eingebunden sei.[5] § 100a StPO sei hinsichtlich der technischen Umsetzung wegen der Vielgestaltigkeit möglicher Sachverhalte vom Gesetzgeber bewusst offen gestaltet worden, auch um neue Techniken und Formen der Nachrichtenübertragung, die zum Zeitpunkt des Einfügens der §§ 100a, 100b StPO in die StPO im Jahre 1968 technisch noch nicht entwickelt waren, in deren Anwendungsbereich einbeziehen zu können. Die Installation der benötigten Spionagesoftware sei als Sekundärmaßnahme nur eine notwendige Vorbereitung für die Umsetzung der späteren Überwachungsmaßnahme, sodass – vergleichbar der Installation von GPS-Empfängern an Kraftfahrzeugen beziehungsweise von Wanzen in Räumen – von einer Annexkompetenz der Strafverfolgungsbehörden zu §§ 100a, 100b StPO auszugehen sei, damit der Zweck des Eingriffs erreicht werden könne.[6]

Ich teile diese Rechtsauffassung zwar nicht, weil die mit der Quellen-TKÜ einhergehende spezifische Vorgehensweise von der konkreten Befugnisnorm des § 100a StPO nicht gedeckt ist. Die für die Durchführung der Quellen-TKÜ erforderliche verdeckte Installation einer Software bewirkt auf dem Endgerät des Betroffenen zwangsläufig einen Eingriff in die Integrität des Systems[7] und ist mit einer heimlichen Datenveränderung verbunden.[8] Bereits aus diesem Grund handelt es sich bei der Quellen-TKÜ um ein neuartiges Ermittlungsinstrument, dessen Einsatz auf Grund seiner technischen Nähe zur Online-Durchsuchung und der mit einer technischen Infiltration einhergehenden potentiellen Gefahren für das betroffene System ein im Vergleich zu klassischen Telekommunikationsüberwachung tiefgreifenderer Eingriff darstellt und nicht mehr als typische Begleiterscheinung einer Telekommunikationsüberwachung qualifiziert werden kann.

Ich befürchte allerdings, dass ohne baldige gesetzliche Regelung der Quellen-TKÜ nicht zuletzt wegen des hohen Handlungsdrucks in einzelnen Phänomen-Bereichen entsprechende Maßnahmen zukünftig auf der Grundlage der bisherigen Fassung des § 100a StPO durchgeführt werden und damit mangels klarer rechtlicher Vorgaben ein Weniger an Rechtssicherheit, Rechtsklarheit und Rechtsschutz die Folge sein wird.

---

ne Übergangsphase, wenn eine rechtliche Beschränkung auf ausschließlich für die Überwachung der Telekommunikation notwendige Eingriffe in den Zielcomputer erfolgt).

5 Bär, MMR 2011, 690, 692; krit. Popp, ZD 2012, 51, 54, weil die Maßnahme sich nicht mehr auf den TK-Vorgang selbst beziehe, sondern schon vor dem eigentlich technischen Vorgang des „Aussendens, Übermittelns und Empfangens von Signalen mittels TK-Anlagen“ (§ 3 Nr. 22 TKG) ansetze.

6 Vgl. AG Bayreuth, MMR 2010, 266; LG Hamburg MMR 2011, 693; LG Landshut MMR 2011, 690 mit zustimmender Anm. Bär, MMR 2011, 6 und abl. Anm. Brodowski JR 2011, 533; KMR/Bär StPO § 100a Rn. 331b; BeckOK/Graf StPO § 100a Rn. 107c; Meyer/Goßner StPO 57. Aufl. § 100a Rn. 7a; Bratke, aaO, S. 321 ff.

7 Vgl. BVerfGE 120, 274, Rz. 221 ff.

8 Satzger/Schluckebier/Widmaier/Eschelbach StPO § 100a Rn. 46; Singelnstein, NStZ 2012, 593, 599; Bode, Verdeckte strafprozessuale Ermittlungsmaßnahmen (2012), S. 368.

5. Für eine gesetzliche Regelung sowohl der repressiven Quellen-TKÜ als auch der Online-Durchsuchung streitet letztlich auch der nach gegenwärtigem Rechtszustand unbefriedigende Ausschluss der Umwidmung von Daten, die aufgrund einer präventiven Quellen-TKÜ oder Online-Durchsuchung auf der Grundlage des BKAG und der entsprechende länderpolizeilichen Regelungen erhoben worden sind, für Zwecke des Strafverfahrens. Umfangreiche Ermittlungen nach den Polizeigesetzen aufgrund Gefährdungssachverhalten (§ 4a BKAG), die später in Ermittlungsverfahren münden, sind keine Seltenheit. Aufgrund des in § 161 Abs. 2 StPO normierten Grundsatzes des hypothetischen Ersatzeingriffes dürfen aber konkrete Erkenntnisse aus einer präventiven Quellen-TKÜ oder Online-Durchsuchung, etwa dass mehrere Personen einen terroristischen Anschlag vorbereiten, im Ermittlungs- und Strafverfahren zu Beweiszwecken nach gegenwärtigem Rechtszustand nicht verwertet werden.[9] Dies ist wenig befriedigend, weshalb es sachlich gerechtfertigt ist, insoweit einen gewissen Gleichlauf zwischen präventiven und repressiven Befugnissen zu schaffen.

II. Verhältnismäßigkeit im engeren Sinne

Die Begrenzungen, die sich aus den Anforderungen der Verhältnismäßigkeit im engeren Sinne ergeben, sind in den vorgeschlagenen Regelungen eingehalten. Danach müssen die Überwachungsbefugnisse mit Blick auf das Eingriffsgewicht angemessen ausgestaltet sein. Es ist Aufgabe des Gesetzgebers, einen Ausgleich zu schaffen zwischen der Schwere der Eingriffe in die Grundrechte potenziell Betroffener auf der einen Seite und der Pflicht des Staates zum Schutz des Grundrechte und Rechtsgüter der Bürgerinnen und Bürger auf der anderen Seite. Für tief in die Privatsphäre eingreifende Ermittlungsbefugnisse, wie sie hier in Rede stehen, hat das BVerfG aus dem Verhältnismäßigkeitsgrundsatz im engeren Sinne übergreifende Anforderungen abgeleitet, denen die vorgeschlagenen Regelungen gerecht werden. Im Einzelnen:

1. Quellen-TKÜ

a) § 100a Abs. 1 Satz 2 StPO-E

§ 100a Abs. 1 Satz 2 StPO-E betrifft die Erlaubnis, die laufende Kommunikation dadurch zu überwachen, dass in ein von dem Betroffenen genutztes informationstechnisches System mit technischen Mitteln eingegriffen werden darf, um die Kommunikation in unverschlüsselter Form zu überwachen.

aa) Da sich die Maßnahme nach § 100a Abs. 1 Satz 2 StPO-E auf den laufenden Telekommunikationsvorgang beschränkt, hat sie lediglich die Aufgabe, den technischen Entwicklungen der Informationstechnik zu folgen und – ohne Zugriff auf weitere inhaltliche Informationen des informationstechnischen Systems – eine Telekommunikationsüberwachung auch dort zu ermöglichen, wo dies mittels der

[9] Vgl. Popp, ZD 2012, 51, 52; siehe auch KK-Griesbaum § 161 Rn. 35. Die Beschränkungen aus § 161 Abs. 2 StPO greifen nicht, soweit die Verwendung der Daten im Strafverfahren **nicht zu Beweiszwecken**, sondern als Ermittlungs- und Spurenansatz oder zur Ermittlung des Aufenthaltsortes des Beschuldigten erfolgen soll.

alten Überwachungstechnik nicht mehr möglich ist. Sie ist folgerichtig „nur" an Art. 10 Abs. 1 GG zu messen.

bb) Indem auf den Straftatenkatalog des § 100a Abs. 2 StPO Bezug genommen wird, ist gewährleistet, dass der gesetzlich geregelte Eingriffsanlass für eine Quellen-TKÜ ein hinreichendes Gewicht aufweist. Ein Bedürfnis für eine Ausrichtung einer Quellen-TKÜ-Regelung an dem Katalog der Taten gem. § 100c ff. StPO (Straftaten aus dem Bereich der organisierten Kriminalität, des Terrorismus sowie anderer Formen besonders schwerer Kriminalität mit einer Höchststrafe von mehr als fünf Jahren Freiheitsstrafe) besteht nicht. Eine Maßnahme, die mit Hilfe der besonderen Ermittlungsmaßnahme der Quellen-TKÜ ausschließlich IP-Telekommunikation überwacht und aufzeichnet, weist keine mit der akustischen Wohnraumüberwachung vergleichbare Eingriffsintensität auf. Es handelt sich auch im Vergleich zur umfassenden Ausforschung des Zielsystems ohne Bezug zu laufenden Telekommunikationsvorgängen im Rahmen einer Online-Durchsuchung, die am Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme zu messen ist, um einen weniger gravierenden Grundrechtseingriff. Die abgesenkte Schutzbedürftigkeit bei einer Telefonüberwachung im Vergleich zur Wohnraumüberwachung ergibt sich daraus, dass der Nutzer von (Internet-) Telekommunikationsformen bewusst Kommunikationsinhalte aus seiner Sphäre in ein fremdbeherrschtes Datennetz entäußert, welches sich seinem Zugriff entzieht und von Dritten betrieben wird, während Art. 13 GG die Wohnung als Rückzugsraum vertraulicher räumlicher Lebenssphäre schützt.

Im Hinblick auf denselben Grundrechtsmaßstab des Art. 10 GG und dieselben Erkenntnismöglichkeiten (Informationen aus Telekommunikationsvorgängen) ist es deshalb sachgerecht, sich bei der Quellen-TKÜ an dem Katalog der schweren Straftaten des § 100a Abs. 2 StPO mit einer Höchststrafe von in der Regel mindestens fünf Jahren, auf jeden Fall über einem Jahr Freiheitsstrafe, zu orientieren, zumal das BVerfG in seiner Entscheidung vom 12.10.2011 die durch den Gesetzgeber 2008 vorgenommene Erweiterung des Straftatenkatalogs in § 100a Abs. 2 StPO für verfassungsgemäß erklärt hat.[10]

cc) Die verfassungsrechtlichen Anforderungen an die tatsächlichen Voraussetzungen des Eingriffs sind mit dem Erfordernis des Vorliegens bestimmter Tatsachen, die den Verdacht einer Täterschaft oder Teilnahme an einer bestimmten Straftat begründen, gewahrt.[11] Damit ist klargestellt, dass bloße Vermutungen nicht ausreichen und der Verdacht so weit konkretisiert sein muss, dass ein Beschuldigter erkennbar und dessen Beteiligung an einer Katalogtat wahrscheinlich ist.[12]

10 BVerfGE 129, 208.

11 Vgl. BVerfGE 113, 348, 385.

12 BGH StV 2010, 553 f.

dd) Da die Quellen-TKÜ voraussetzt, dass die Straftat auch im Einzelfall schwer wiegt, ist sichergestellt, dass im Rahmen der Einzelfallprüfung solche Fälle herausfallen, die zwar eine Anlasstat der Erlaubnisnorm zum Gegenstand haben, aber im konkreten Einzelfall keine hinreichende Schwere aufweisen.

ee) Durch die Subsidiaritätsklausel wird gewährleistet, dass die Quellen-TKÜ nur dann zulässig ist, wenn keine erfolgversprechenden schonenderen Maßnahmen möglich sind (vgl. § 100a Abs. 1 Nr. 3 StPO-E). Dadurch ist sichergestellt, dass im Hinblick auf das dem „additiven“ Grundrechtseingriff innewohnende Gefährdungspotential das Ausmaß der Überwachung beschränkt bleibt.

ff) § 100a Abs. 1 Satz 3 StPO-E

Die Regelung erfasst die Überwachung von verschlüsselter Kommunikation, bei der der Übertragungsvorgang bereits abgeschlossen ist, die aber noch auf dem informationstechnischen System des Betroffenen gespeichert ist. Nach ständiger Rechtsprechung des BVerfG unterliegt solche Kommunikation, weil sie sich nunmehr im Herrschaftsbereich des Nutzers befindet, nicht mehr dem Schutzbereich des Art. 10 GG, sondern ist der Eingriff an dem Grundrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG in seiner Ausprägung als Grundrecht auf informationelle Selbstbestimmung oder als Grundrecht in die Integrität und Vertraulichkeit eigener informationstechnischer Systeme zu messen. Der Zugriff auf solche Kommunikationsinhalte findet seine Rechtsgrundlage grundsätzlich in der für die Online-Durchsuchung neu geschaffenen Ermächtigungsgrundlage des § 100b StPO-E.

§ 100a Abs. 1 Satz 3 StPO-E macht hiervon eine Ausnahme, als bereits gespeicherte Kommunikationsinhalte eines Kommunikationsdienstes ausgeleitet werden dürfen, wenn dies „ein funktionales Äquivalent zur Überwachung und Ausleitung der Nachrichten aus dem Telekommunikationsnetz darstellt“. Was darunter zu verstehen ist, ergibt sich aus § 100 Abs. 5 Nr. 1b StPO-E. Danach darf gespeicherte Kommunikation nur dann ausgeleitet werden, wenn sie nach dem Zeitpunkt der regelmäßig richterlichen Anordnung nach § 100e StPO-E gespeichert worden ist und während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten erhoben werden können. Kommunikation, die vor der richterlichen Anordnung gespeichert worden ist, wird von § 100a Abs. 1 Satz 3 StPO-E nicht erfasst; ein Zugriff kann insoweit nur unter den einschränkenden Voraussetzungen der Online-Durchsuchung erfolgen.

Ich halte diese Ausnahmeregelung für vertretbar. Die vom BVerfG zurecht aufgestellten hohen Anforderungen an die Durchführung einer Online-Durchsuchung betreffen andere Konstellationen als durch § 100a Abs. 1 Satz 3 StPO-E geregelte Sachverhalte. Hier geht es nicht um die Möglichkeit des Auslesens des gesamten informationstechnischen Systems, sondern um das Ausleiten ankom-

mender und abgesendeter Nachrichten, die nach Vorliegen eines richterlichen Beschlusses zur Quellen-TKÜ gespeichert worden sind. Solche Kommunikationsvorgänge stellen zwar rein formal betrachtet keine laufende Kommunikation mehr dar, sie sind aber der Sache nach eher dem Schutzbereich des Art. 10 GG als dem Schutzbereich des Grundrechts auf Integrität und Vertraulichkeit informationstechnischer Systeme zuzuordnen.

Soweit zum Teil kritisch angemerkt wird, dass zur Überprüfung, ob die Speicherung der Kommunikationsinhalte nach der richterlichen Anordnung erfolgte, zunächst alle gespeicherten Kommunikationsinhalte ausgelesen werden müssten, weshalb in Wahrheit eine Online-Durchsuchung vorläge, teile ich diese Bedenken nicht. Die bloß technische Überprüfung der zu den einzelnen Nachrichten hinterlegten Meta-Daten wie Absende-, Empfangs- und Lesezeitpunkte mittels der eingesetzten Software ohne automatische Ausleitung der Daten stellt m.E. noch keine Online-Durchsuchung dar. Vielmehr ist es im Rahmen anderer Überwachungsmaßnahmen durchaus nicht unüblich, zunächst den Gesamtbestand an Kommunikation zu überprüfen, um in einem weiteren Schritt nicht verwertbare Inhalte (z.B. wegen Kernbereichsschutz) auszusondern.

gg) § 100a Abs. 3 StPO-E

Die Einbeziehung von Nachrichtenmittlern und Personen, deren informationstechnisches System benutzt wird, begegnet keinen Bedenken. Die Erstreckung von heimlichen Überwachungsmaßnahmen auf Dritte steht nach der Rechtsprechung des BVerfG unter strengen Verhältnismäßigkeitsanforderungen und setzt eine spezifische Nähe der Betroffenen zu der aufzuklärenden Straftat voraus. Dazu bedarf es konkreter Anhaltspunkte, dass der Kontakt einen Bezug zum Ermittlungsziel aufweist und so eine nicht unerhebliche Wahrscheinlichkeit besteht, dass die Überwachungsmaßnahme der Aufklärung der Straftat dienlich sein kann.[13] Diese verfassungsrechtlichen Vorgaben sind hier erfüllt.

hh) § 100a Abs. 5 StPO-E

Die in § 100a Abs. 5 StPO-E aufgestellten technischen Voraussetzungen der Durchführung der Quellen-TKÜ lehnen sich an die Regelung der präventiven Quellen-TKÜ des BKAG an. Dadurch wird zunächst sichergestellt, dass eine Quellen-TKÜ nur bei einer technisch sichergestellten Begrenzung der Überwachung auf die laufende Telekommunikation bzw. auf Kommunikation, die ab dem Zeitpunkt der Anordnung nach § 100e StPO-E gespeichert und auch während des laufenden Übertragungsvorgangs hätte überwacht und aufgezeichnet werden können, durchgeführt wird. Damit wird klargestellt, dass der Einsatz multifunktionaler Programme ebenso wenig erlaubt ist wie etwa die Anfertigung von Screenshots vom Bildschirm des infiltrierten Rechners oder die Aufzeichnung der

13 BVerfG Urteil vom 20.04.2016, 1 BvR 966/09, Rz. 116.

Tastaturanschläge der Zielperson mittels eines Key-Loggers. Wie diese technischen Vorgaben im Einzelnen sicherzustellen sind, betrifft die Anwendung der Norm, nicht aber ihre Gültigkeit. Eine nähere Spezifizierung im Gesetz ist nicht erforderlich. Sollten diese Anforderungen aus technischen Gründen nicht erfüllbar sein, liefe die Vorschrift ins Leere. Sie würde dadurch aber nicht verfassungswidrig, weil nicht ausgeschlossen ist, dass die nötigen technischen Voraussetzungen in absehbarer Zukunft geschaffen werden können.[14]

Die dem BKAG nachgebildeten gesetzlichen Regelungen zur Minimierung der durch den Zugriff bedingten Veränderungen an dem informationstechnischen System, zu der Vermeidung der Nutzbarkeit durch Dritte und zur Rückgängigmachung der vorgenommenen Veränderungen hat das BVerfG bei der präventiven Quellen-TKÜ nicht beanstandet.

Soweit in der Literatur diskutiert wird, dass zur ausreichend sicheren Gestaltung der Quellen-TKÜ nur solche Überwachungssoftware zum Einsatz kommen dürfe, die durch eine unabhängige Stelle zertifiziert ist, erscheint mir dies wenig praktikabel. Im Hinblick auf die schnelle technische Entwicklung im Kommunikationsbereich ist die Gefahr, dass eine Überwachungssoftware im Zeitpunkt ihrer Zertifizierung veraltet ist und weiterentwickelte, einsatzfähige Überwachungssoftware wegen Nichtzertifizierung nicht eingesetzt werden kann, nicht von der Hand zu weisen. Außerdem gibt es nicht „den Staatstrojaner“, der als Überwachungsinstrument in allen Fällen einsetzbar ist; vielmehr wird meist eine auf das konkrete technische Zielsystem individuell zugeschnittene Überwachungssoftware zum Einsatz kommen. Je nach Dringlichkeit der Maßnahme und konkreter technischer Ausgangssituation muss es deshalb möglich sein, auch nicht zertifizierte Software einzusetzen. Ungeachtet dessen liegen Eigenentwicklungen einer Überwachungssoftware für die Quellen-TKÜ seitens des BKA vor, so dass von einem verantwortungsbewussten Umgang mit den Eingriffsgrundlagen unter der politischen Ressortverantwortung des zuständigen Ministers auszugehen ist.

2. Online-Durchsuchung (§ 100b StPO-E)

§ 100b Abs. 1 StPO-E enthält die Ermächtigungsgrundlage zur Durchführung der Online-Durchsuchung und stellt hinsichtlich der Anlasstaten auf den für die Wohnraumüberwachung geltenden Katalog des § 100c Abs. 2 StPO ab.

Ich halte die Regelung für sachgerecht.

a) Das BVerfG hat in seinen Entscheidungen zur präventiven Online-Durchsuchung die hohe Intensität des Grundrechtseingriffs ausführlich dargestellt.[15] Diese ergibt

14 BVerfG Urteil vom 20.04.2016, 1 BvR 966/09, Rz. 234.

15 BVerfGE 120, 274 Rz. 211 ff.; BVerfGE 141, 220 ff.

vor allem daraus, dass der Zugriff den Zugang zu einem Datenbestand eröffnet, der herkömmliche Informationsquellen an Umfang und Vielfältigkeit übertreffen kann, weshalb der Zugriff mit dem naheliegenden Risiko verbunden ist, dass die erhobenen Daten in einer Gesamtschau Rückschlüsse auf die Persönlichkeit des Betroffenen bis hin zu einer Bildung von Verhaltens- und Kommunikationsprofilen ermöglichen. Hinzu kommt, dass der Eingriff eine große Streubreite aufweisen kann und die Maßnahme heimlich durchgeführt wird.

Das BVerfG fordert als Voraussetzung für eine präventive Online-Durchsuchung eine konkrete Gefahr für ein überragend wichtiges Rechtsgut und nennt dazu Leib, Leben und Freiheit, aber auch wichtige Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Das Urteil enthält keine näheren Ausführungen zu den Anforderungen an eine repressive Online-Durchsuchung. Insoweit wird nur in allgemeiner Form darauf hingewiesen, dass es im Hinblick auf den Schutz hinreichend gewichtiger Rechtsgüter in erster Linie auf das Gewicht der verfolgten Taten ankommt.[16] Insoweit hat der Gesetzgeber eine Einstufung in erhebliche, schwere und besonders schwere Straftaten vorgenommen. Während die Durchführung einer Telekommunikationsüberwachung oder die Nutzung von vorsorglich erhobenen Telekommunikationsverkehrsdaten den Verdacht einer schweren Straftat voraussetzen, bedarf die Durchführung einer Wohnraumüberwachung des Verdachts einer besonders schweren Straftat. In seiner Entscheidung vom 3. März 2004 zum großen Lauschangriff hat das BVerfG gefordert, dass grundsätzlich nur Katalogtaten in Betracht kommen, deren Tatbestand eine Höchststrafe von mehr als fünf Jahren androht.[17] Während bei bestimmten Taten die besondere Schwere durch das verletzte Rechtsgut indiziert ist (Mord, Totschlag), kann – so das BVerfG – die besondere Schwere aber auch durch die faktische Verzahnung mit anderen Katalogtaten oder durch das Zusammenwirken mit anderen Straftätern begründet werden.[18] Dies sei bei einem arbeitsteiligen, gegebenenfalls auch vernetzt erfolgenden Zusammenwirken mehrerer Täter im Zuge der Verwirklichung eines komplexen, mehrere Rechtsgüter verletzenden kriminellen Geschehens gegeben, wie es etwa für die organisierte Kriminalität gelte. Entsprechendes könne für die Straftaten des Friedensverrats, des Hochverrats und bestimmter Delikte der Gefährdung des demokratischen Rechtsstaats gelten.[19]

Von der Eingriffstiefe vergleicht das BVerfG die Online-Durchsuchung mit dem Eingriff in die Unverletzlichkeit der Wohnung.[20] Meines Erachtens ist deshalb der Gesetzgeber nicht gehindert, die maßgebliche Schwelle für den Rechtsgüterschutz bei

16 BVerfG Urteil vom 20.04.2016, 1 BvR 966/06, Rn. 107.

17 BVerfG NJW 2004, 999 = BVerfGE 109, 279 Rz. 248.

18 BVerfGE 109, 279 Rz. 245.

19 Zur hohen Bedeutung der Abwehr von extremistischen und terroristischen Bestrebungen vgl. BVerfGE 120, 274 Rz. 202.

20 BVerfG Urteil vom 20.04.2016, 1 BvR 966/06, Rn. 210.

der Wohnraumüberwachung und der Online-Durchsuchung einheitlich zu bestimmen. Da zusätzlich zum Verdacht einer abstrakt vorliegenden besonders schweren Straftat gem. § 100b Abs. 1 Nr. 2 StPO-E erforderlich ist, dass die Straftat auch im Einzelfall schwer wiegt, ist sichergestellt, dass im Rahmen der Einzelfallprüfung solche Fälle herausfallen, die zwar eine Anlasstat der Erlaubnisnorm zum Gegenstand haben, aber im konkreten Einzelfall keine hinreichende besondere Schwere aufweisen.

b) Zielperson

Die Regelung des § 100b Abs. 3 StPO-E, die die Maßnahme der Online-Durchsuchung grundsätzlich auf den Beschuldigten beschränkt, ist angesichts des Eingriffsgewichts der Maßnahme zu begrüßen. Eine Erstreckung der Maßnahme auf Dritte erscheint unverhältnismäßig. Unberührt davon muss – verfassungsrechtlich unbedenklich - bleiben, dass durch die Online-Durchsuchung möglicherweise auch unbeteiligte Dritte erfasst werden. Die in § 100b Abs. 3 Satz 2 StPO-E vorgesehene Ausnahme, wonach ein Eingriff in informationstechnische Systeme Dritter zulässig ist, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass der Beschuldigte informationstechnische Systeme des Dritten benutzt, entspricht verfassungsrechtlicher Rechtsprechung.[21]

3. Kernbereichsschutz, § 100d StPO-E

Die Kernbereichsregelung des § 100d StPO-E begegnet keinen Bedenken.

Entsprechend dem zweistufigen Schutzkonzept des BVerfG[22] stellt die Regelung sicher, dass schon die Erhebung kernbereichsrelevanter Daten unterbleibt, wenn konkrete Anhaltspunkte dafür vorliegen, dass eine bestimmte Datenerhebung den Kernbereich privater Lebensgestaltung berührt. Auf der Verwertungsebene sieht § 100d Abs. 2 StPO-E ausreichende Schutzvorkehrungen vor.

Soweit in § 100d Abs. 3 StPO-E die Regelung des Kernbereichsschutzes im Rahmen der Online-Durchsuchung auf der Erhebungsebene geringere Anforderungen vorsieht als die Regelung zum Kernbereichsschutz im Rahmen der Wohnraumüberwachung, ist dies dem Charakter der Maßnahme der Online-Durchsuchung geschuldet, weil sich die Überwachung bei der Online-Durchsuchung nicht als ein zeitlich gegliedertes Geschehen an verschiedenen Orten, sondern als Zugriff mittels eines Ausforschungsprogramms auf digital vorliegende Informationen vollzieht, die in ihrer Gesamtheit typischerweise nicht schon als solche den Charakter der Privatheit wie das Verhalten oder die Kommunikation in einer Wohnung aufweisen. Die deswegen erforderlich werdende Rücknahme

21 BVerfG Urteil vom 20.04.2016, 1 BvR 966/09, Rz. 115.

22 BVerfGE 120, 274 Rz. 262.

der Anforderungen an den Kernbereichsschutz auf der Erhebungsebene ist verfassungsrechtlich unbedenklich.[23]

4. Schutz von Berufsgeheimnisträgern, § 100d Abs. 5 StPO-E

§ 100d Abs. 5 StPO überträgt die bisher in § 100c Abs. 6 StPO enthaltene Regelung zum Schutz von Zeugnisverweigerungsberechtigten, insbesondere Berufsgeheimnisträgern auf die Online-Durchsuchung. Dies ist konsequent; die Gesetzeslage bleibt damit aber weiterhin uneinheitlich. Sie statuiert Überwachungsverbote für sämtliche Berufsgeheimnisträger nur in den Fällen des großen Lauschangriffs und der Online-Durchsuchung, bei den übrigen Ermittlungsmaßnahmen aber lediglich für eine gewisse Gruppe unter ihnen und für die dieser Gruppe zuzuordnenden Berufshelfer (§ 160a Abs. 1, Abs. 3 StPO). Für alle Berechtigten der §§ 52, 53a StPO werden im Fall des großen Lauschangriffs und der Online-Durchsuchung nur relative, also richterlich abwägungsoffene Verwertungsverbote gewährt. Damit wird eine Chance vertan, die kritisierte Differenzierung bei der personellen Schutzerstreckung einem geschlossenen Konzept zuzuführen.

III. Fazit

Die vorgeschlagenen Regelungen stellen notwendige Ergänzungen der Ermittlungsbefugnisse der Strafverfolgungsbehörden dar, die der fortschreitenden technischen Entwicklung im Kommunikationsbereich und den damit einhergehenden gravierenden Überwachungsschwierigkeiten Rechnung tragen. Sie sind praxistauglich ausgestaltet und begegnen in verfassungsrechtlicher Hinsicht keinen grundsätzlichen Bedenken.

[23] BVerfG Urteil vom 20.04.2016, 1 BvR 966/09, Rz. 218.