Fachbereich Rechtswissenschaften

Prof. Dr. Arndt Sinn

Prof. h.c. (National University Kaohsiung)

Lehrstuhl für Deutsches und
Europäisches Straf- und Strafprozess-
recht, Internationales Strafrecht
sowie Strafrechtsvergleichung

Direktor des

ZEIS
ZENTRUM FÜR EUROPÄISCHE UND INTERNATIONALE STRAFRECHTSSTUDIEN

Heger-Tor-Wall 14
49069 Osnabrück
Telefon: (0541) 969-6133 DW 6135
Fax: (0541) 969-4852
LS-Sinn@uos.de
zeis@uos.de

Universität Osnabrück · FB 10 · 49069 Osnabrück

Osnabrück, den 30.05.2017

Stellungnahme zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze BT-Drucksache 18/11272 sowie zur Formulierungshilfe der Bundesregierung für einen Änderungsantrag zum o.g. Gesetzentwurf (Ausschussdrucksache 18(6)334)

I. Einleitung

Der Änderungsantrag unterscheidet zwischen der Quellentelekommunikationsüberwachung (Quellen-TKÜ) und der Online-Dursuchung. Er greift zwei eingriffsintensive Ermittlungsmaßnahmen auf, die im letzten Jahrzehnt in Wissenschaft und Praxis (vgl. *Sieber*, „Straftaten und Strafverfolgung im Internet", Gutachten zum 69. Deutschen Juristentag, 2012, C 103 ff.) stark diskutiert wurden und vor dem Hintergrund präventiv-polizeilicher Ermittlungsmaßnahmen auch Gegenstand verfassungsgerichtlicher Rechtsprechung waren.

Die Intention des Änderungsvorschlages zu verhindern, dass technische Innovationen die Strafverfolgung vor allem im Bereich schwerer Straftaten behindern, ist nachvollziehbar und entspricht bezüglich der Quellen-TKÜ auch Forderungen in der Wissenschaft (vgl. *Sieber*, „Straftaten und Strafverfolgung im Internet", Gutachten zum 69. Deutschen

Juristentag, 2012, C 105 ff.) Eine Anpassung der Maßnahmen der StPO ist im Hinblick auf den technischen Fortschritt geboten.

Die klassische Telekommunikationsüberwachung hat aufgrund der mehr und mehr verbreiteten Verschlüsselung der Daten für die Strafverfolgungsorgane an Bedeutung verloren. Die Kommunikationsinhalte können zwar ausgeleitet werden, allerdings sind diese in dieser Form unbrauchbar.

Dabei gilt es im Hinblick auf die Quellen-TKÜ zu beachten, dass es zwar einerseits „nur“ um eine Anpassung der bereits bestehenden Regelung des § 100a StPO an die technologischen Neuerungen geht, andererseits mit diesen Neuerungen aber Folgeprobleme verbunden sind, die auf verfassungsrechtlicher und einfachgesetzlicher Grundlage zu lösen sind.

Im Hinblick auf die Online-Durchsuchung (§ 100b-E) handelt es sich um eine völlig neue und eingriffsintensive Maßnahme des staatlichen Eingriffs in die Grundrechtssphäre des Bürgers im Bereich der Strafverfolgung. Nachdem im Jahr 2007 der 3. Strafsenat in seiner Entscheidung vom 31.1.2007 (BGHSt 51, 211) den Bemühungen der Praxis, die Online-Durchsuchung in der Art eines Baukastensystems auf die Ermächtigungsgrundlagen der Durchsuchung sowie der Telefon- oder Wohnraumüberwachung, zu stützen zu Recht eine Absage erteilt hat, kann nur der Gesetzgeber durch die Schaffung einer bestimmten Ermächtigungsgrundlage den Eingriff in das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme erlauben. In der Vergangenheit hat man in der Wissenschaft den Bedarf an dieser repressiven Ermittlungsmaßnahme (*Sieber*, „Straftaten und Strafverfolgung im Internet“, Gutachten zum 69. Deutschen Juristentag, 2012, C 109) und in der Praxis sogar die Möglichkeit einer Online-Durchsuchung auf der Grundlage verfassungsgerichtlicher Rechtsprechung verneint (vgl. Stadler MMR 2012, 18 (20).

Der technische Fortschritt und die Nutzung von informationstechnischen Systemen sind die entscheidenden Antriebsfaktoren für eine Ausweitung der Ermittlungsbefugnisse. Zwar können die Strafverfolgungsorgane in den Fällen der Beschlagnahme auch PC, Mobiltelefone, Tablets etc. durchsuchen, allerdings bleiben diese Maßnahmen dann erfolglos, wenn der Nutzer die Inhalte vor der Beschlagnahme verschlüsselt hat. Im Wesentlichen geht es also u.a. auch darum, durch den heimlichen Zugriff auf die Inhalte der Geräte einer Verschlüsselung zuvor zu kommen. Das Bundesverfassungsgericht hatte sich mit den Möglichkeiten einer Online-Durchsuchung im präventiv-polizeilichen Bereich zu beschäftigen und diese Maßnahme bei entsprechender Flankierung durch weitere Schutzmechanismen mit den Grundrechten des Grundgesetzes vereinbar erklärt (vgl. BVerfG v. 20.4.2016 - 1 BvR 966/09; 1 BvR 1140/09 Leitsatz 1a). Eine Online-Durchsuchung sei, so das BVerfG, seinem Gewicht nach mit einem Eingriff in die Unverletzlichkeit der Wohnung vergleichbar (BVerfG aaO, Rn. 210). Eine Maßnahme im repressiven Bereich muss sich, vorbehaltlich der Verhältnismäßigkeit der Maßnahme in der Strafverfolgung, an diesen Vorgaben messen lassen. Der verfassungsgerichtlichen Rechtsprechung kann jedenfalls nicht der Grundsatz entnommen werden, dass eine Online-Durchsuchung im Bereich der Repression generell ausgeschlossen sein soll.

Exkurs: Zur Möglichkeit der Schaffung einer General-Ermächtigungsgrundlage

Aufgrund der sich rasant entwickelten Technik, den daraus erwachsenden Möglichkeiten auch eines Missbrauchs für kriminelles Verhalten ergibt sich die Frage, ob neben den nun vorgeschlagenen drei neuen Ermächtigungsgrundlagen auch eine General-Ermächtigungsgrundlage für Eingriffe in das Grundrecht auf Gewährung der Vertraulichkeit und Integrität informationstechnischer Systeme geschaffen werden könnte.

Aus dem Gebot der Normenklarheit und Bestimmtheit folgt, dass Ermächtigungsgrundlagen grundsätzlich nicht offen gestaltet werden dürfen. Die von dem Eingriff betroffenen Grundrechte sowie die Art und Weise des Eingriffs müssen hinreichend klar in der Norm formuliert sein. Das BVerfG hat diesen Grundsatz mehrfach betont und in 1 BvR 518/02 v. 4.4.2006 (Rn. 150) wie folgt formuliert:

„Ermächtigungen zu Grundrechtseingriffen bedürfen einer gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenbestimmtheit und Normenklarheit entspricht (vgl. BVerfGE 110, 33 (53)). Bei Eingriffen in das Grundrecht auf informationelle Selbstbestimmung - wie auch in die Spezialgrundrechte der Art. 10 und 13 GG - hat der Gesetzgeber insbesondere den Verwendungszweck der Daten bereichsspezifisch und präzise zu bestimmen (vgl. BVerfGE 65, 1 (46); 110, 33 (70); 113, 29 (51)).“

Gegenstand der Ermächtigungsgrundlage wäre die Infiltration eines informationstechnischen Systems des Betroffenen, also ein hinreichend bestimmter Eingriff in den Schutzbereich des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme nach Art. 2 Absatz 1 i.V.m. Artikel 1 Absatz 1 GG. Um als „offen“ gelten zu können, würden Maßnahmen zur Umsetzung eines entsprechenden Eingriffs in einer Ermächtigungsgrundlage, die generalklauselartigen Charakter haben soll, gerade nicht beschrieben werden.

Wie sich an §§ 100c oder 100h StPO zeigt, führt dies für sich noch nicht zu einem Verstoß gegen das Gebot der Normenklarheit und Bestimmtheit, solange die übrigen Voraussetzungen ausreichend konkret formuliert sind und insbesondere der Zweck der Maßnahme hinreichend erkennbar bleibt.

Allerdings können die Zwecke, die mit einem Eingriff in das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme sehr vielfältig sein: So ist es durch Eingriffe in diese Systeme möglich, Heizungs- und Lichtanlagen, Schalter und andere Internetfähigen Geräte heimlich zu steuern; es ist möglich, Kameras und Mikrophone des entsprechenden Endgeräts mittels Software einzuschalten, und es kann sogar die Steuerung eines „Smart Car“ übernommen oder nur dessen Systeme ausgelesen werden. Die wenigen Beispiele sollen genügen, um zu zeigen, dass das Gebot der Normenklarheit und Bestimmtheit nicht ohne eine konkret zu beschreibende Zwecksetzung einzuhalten ist. Eine General-Ermächtigung zur Infiltration informationstechnischer Systeme ist demnach nicht möglich.

II. Zur Einführung einer Rechtsgrundlage für die Quellen-Telekommunikationsüberwachung, § 100a StPO-E

1. Grundfragen

§ 100a Absatz 1 Satz 2 und 3 StPO-E ordnen zwei verschiedene Fälle. Satz 2 regelt den Hauptanwendungsfall der Quellen-TKÜ, also die Ausleitung von laufender unverschlüsselter Kommunikation. Das setzt den Begleiteingriff „Einsatz technischer Mittel" zur Ausleitung der Quelldaten voraus. Die Ermächtigung zu diesem Eingriff steht im Zentrum von Satz 2. Damit wird die umstrittene Praxis einer Rechtfertigung solcher Eingriffe als „Begleiteingriff" zu § 100a StPO obsolet, was ausdrücklich zu begrüßen ist. Die Regelung setzt den Grundsatz um, dass spezielle Grundrechtseigriffe auf speziellen Ermächtigungsgrundlagen beruhen müssen. Das Aufspielen einer Software auf einem informationstechnischen Systems zu dem Zweck, die Kommunikationsinhalte vor einer Verschlüsselung auszuleiten stellt einen besonderen Eingriff in Art. 10 GG dar, weshalb § 100a StPO geltender Fassung auch nicht die Ermächtigungsgrundlage für die Quellen-TKÜ sein konnte. Art. 10 GG ist dann alleiniger Prüfungsmaßstab für die Quellen-TKÜ, „wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden TK-Vorgang beschränkt. Dies muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein." (BVerfG MMR 2008, 315 (317)). Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist aufgrund des subsidiären Charakters also nicht einschlägig.

Für die praktische Durchführung der Maßnahme sind die technischen Reglementierungen der zu installierenden Software von besonderer Bedeutung. § 100a Absatz 1 Satz 2 StPO-E ermächtigt nur zu einem Eingriff in informationstechnische Systeme zu dem Zweck, „laufende Kommunikation" unverschlüsselt auszuleiten. Soweit die technischen Anforderungen derzeit nicht umsetzbar sein sollten, würde das - wie das BVerfG in seiner Entscheidung vom 20. April 2016 deutlich gemacht hat (BVerfG v. 20.4.2016 - 1 BvR 966/09; 1 BvR 1140/09 Rn. 234) - nicht die Frage der Rechtmäßigkeit der Norm betreffen, sondern ausschließlich die Frage des Gesetzesvollzuges. Dennoch sei an dieser Stelle daran erinnert, dass die Integrität der Software und die Begrenzung ihrer Funktionen auf den in Satz 2 genannten Zweck Voraussetzung und Garant dafür sind, dass kein weiterer Grundrechtseingriff als in Art. 10 GG erfolgt und die erhobenen Beweise auch verwertet werden können. Es dürfte auf der Hand liegen, dass angesichts der noch 2016 vorhandenen Softwareschwächen die Integrität der Programme in den kommenden Jahren erhöhter Kontrolldichte durch die Strafgerichte unterliegen wird.

Im Wortlaut ungeklärt lässt der Änderungsantrag die dringende Frage, ob in den Anwendungsbereich des neuen § 100a StPO auch ein Datenaustausch zwischen digitalen Endgeräten fallen soll, insb. in Fällen des Cloud-Computings. Diese Frage zu beantworten bedürfte der Klarstellung, ob es sich in diesen Fällen um Telekommunikation handelt bzw. ob der Telekommunikationsbegriff vor dem Hintergrund technischer Innovationen nicht einer funktionalen Betrachtungsweise folgen müsste. Folgt man einer rein formalen Betrachtung der genannten besonderen Telekommunikationsvorgänge, so spricht dies für eine Einordnung als Telekomunikation und damit für die Geltung des § 100a StPO-E in diesen Fällen. Bei einer funktionalen Betrachtung gelangt man zu dem Ergebnis, dass der

Datenaustausch zwischen Endgeräten und einer Cloud durch eine Person höchstpersönlicher Natur und nicht der klassischen Kommunikation zwischen zwei Personen gleichzusetzen ist. Vielmehr werden Daten ausgelagert und bei Bedarf wird auf sie zurückgegriffen. Die Überwachung derartiger Datenströme gleicht also eher einem Eingriff in Art. 13 GG (vgl. a. *Sieber*, „Straftaten und Strafverfolgung im Internet", Gutachten zum 69. Deutschen Juristentag, 2012, C-106 ff.). Freilich spricht die systematische Auslegung der Entwurfsvorschriften § 100a StPO-E sowie § 100b StPO-E gegen die Anwendung des § 100a StPO auf die genannten Fälle, denn mit der Online-Durchsuchung sollen gerade ganze Dateninhalte erhoben werden. Es wird dennoch angeregt, in der Begründung der Gesetzesinitiative eine Formulierung aufzunehmen, mit der klar gestellt wird, dass die Überwachung und Aufzeichnung von Daten, die der Nutzer für sich selbst in einer Cloud ablegt und mit seinen Endgeräten synchronisiert, ausschließlich unter den Eingriffsvoraussetzungen des § 100b StPO-E zulässig ist. Damit ist die Kommunikation zwischen zwei Rechnern weiterhin nach § 100a StPO-E zu überwachen, während die Überwachung der „Kommunikation" einer Person mit ihren eigenen Daten dem § 100b StPO-E vorbehalten bleiben muss. Dies ist schon deshalb von herausragender Bedeutung, da die Eingriffsvoraussetzungen bei § 100a StPO-E niedriger sind als bei § 100b StPO-E, was an den unterschiedlichen Grundrechtsanknüpfungen liegt.

2. Zu § 100a Absatz 1 Satz 3 StPO-E

Die in Satz 3 geregelte Fallgestaltung stellt funktional betrachtet den Fall einer „kleinen Online-Durchsuchung" dar. Auf Grundlage dieser Norm soll sichergestellt werden, dass auch solche Inhalte und Umstände der Kommunikation mittels einer Überwachungssoftware überwacht und aufgezeichnet werden dürfen, bei denen der Übertragungsvorgang bereits abgeschlossen ist und die auf dem informationstechnischen System des Betroffenen in einer Anwendung gespeichert sind. Dies betrifft konkret die über Messenger-Dienste versandten und mittlerweile regelmäßig verschlüsselten Nachrichten, wobei die funktionale Äquivalenz zur herkömmlichen Telekommunikationsüberwachung zu gewährleisten ist. Das hat zur Folge, dass nur solche Kommunikationsinhalte und -umstände erhoben werden, die auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form erhoben werden könnten.

Die gespeicherten Inhalte fallen aus dem Grundrechtsschutz des Art. 10 GG heraus und unterfallen deshalb hinsichtlich des heimlichen Zugriffs auf die Inhalte mittels einer Überwachungssoftware dem Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme. Dies wird auch von dem Änderungsantrag vorausgesetzt. Es wird aber erwogen, dass es trotzdem „verfassungsrechtlich nicht geboten sei (…), die höheren Anforderungen des Bundesverfassungsgerichts" (S. 20) an Eingriffe in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme anzuwenden. Dies ist zu diskutieren:

Es wird argumentiert, der Eingriff weise eine eher geringe Intensität auf, weil die erhobenen Informationen nicht über diejenigen hinaus gingen, welche im Wege der herkömmlichen Telekommunikationsüberwachung ermittelt worden wären, wenn der Betroffene diesen Weg gewählt hätte (S. 20). Es wird angedeutet, dass für den Nutzer die Art und Weise der Telekommunikation im Allgemeinen ohne Relevanz sei. Dabei bleibt jedoch unterbelichtet, dass sich der mündige Nutzer bewusst gegen die herkömmliche Art der Telekommunikation entschieden und im Vertrauen auf die vermeintlich sichere Übertragung der Inhalte bewusst den Weg über eine verschlüsselte Übertragung gewählt haben kann. Insoweit lässt die Entwurfsbegründung unberücksichtigt, dass mit der Umgehung der vom Betroffenen zum Schutze seiner Inhalte ergriffenen Maßnahmen gleichzeitig die Eingriffsintensität gegenüber der herkömmlichen Telekommunikationsüberwachung deutlich erhöht wird (vgl. dazu BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 – Rn. 236).

Die Überwachungssoftware zum Zweck der Ausleitung der Quell-Daten (Quellen-TKÜ) soll tatsächlich nur gewährleisten, dass die herkömmliche TKÜ durch Verschlüsselungstechnologien nicht bedeutungslos wird. Diese Art des Eingriffs hat eine dienende Funktion: Der Eingriff in die Vertraulichkeit und Integrität informationstechnischer Systeme durch eine Überwachungssoftware dient dem Eingriff in Art. 10 GG zum Zwecke unverschlüsselter Ausleitung von Kommunikationsinhalten. Die dienende Funktion der Infiltration des Systems allein zu dem Zweck, die Quellen-TKÜ zu ermöglichen, führt dann auch dazu, die Maßnahme insgesamt an Maßstäben zu Art. 10 GG und damit zur TKÜ und den damit in Zusammenhang stehenden Folgen für eine verfassungsgemäße Ermächtigungsgrundlage zu messen.

Ob diese dienende Funktion auch bei der Ermächtigung zur kleinen Online-Durchsuchung (§ 100a Absatz 1 Satz 3 StPO-E) nachgewiesen werden kann, ist zweifelhaft. Dagegen spricht, dass es um das heimliche Ausleiten von Kommunikationsinhalten und -umständen durch die Infiltration des System des Nutzers geht, also um einen Eingriff, der gerade nicht in den Schutzbereich des Art. 10 GG fällt. Die Überwachungssoftware dient also nicht dem Zweck, die Quellen-TKÜ zu ermöglichen, sondern ist eine eigenständige Maßnahme zum heimlichen Erlangen von Informationen. Für eine dienende Funktion spricht aber, dass mit der kleinen Online-Durchsuchung nur auf die Kommunikationsinhalte und -umstände zugegriffen werden soll, die auch durch eine Quellen-TKÜ erhoben werden könnten. Im Kern geht es um die Vermeidung einer Datenlücke zwischen Anordnung der Quellen-TKÜ und der Installation der Überwachungssoftware (s.u.).

Der Wortlaut von Satz 3 lässt den Rechtsanwender im Unklaren darüber, welche Fälle der Gesetzgeber für die „kleine Onlineüberwachung“ im Auge hat. Diese sollten aber deutlich benannt werden, um den Anwendungsbereich der Vorschrift und deren Bestimmtheit zu garantieren. Wenn § 100a Absatz 1 Satz 3 StPO-E ausweislich der Entwurfsbegründung nicht die Fälle laufender Kommunikation erfasst und auch nicht Kommunikationsinhalte, die im Wege einer normalen TKÜ erlangt werden können, so bleibt die Frage zu beantworten, um welche Fälle es dann gehen soll, wenn mit § 100b StPO-E doch gerade eine Ermächtigungsgrundlage geschaffen werden soll, die u.a. die Erhebung solcher auf

Endgeräten gespeicherten Daten erlaubt. Im Kern dürfte es um die Ausleitung von Inhalten und Umständen der Kommunikation in den Fällen von verschlüsselten Telekommunikationsvorgängen gehen, die nach der Anordnung einer Quellen-TKÜ, aber vor der Installation der Überwachungssoftware stattfinden. In diesen Fällen ist eine herkömmliche TKÜ aussichtlos, da damit nur verschlüsselte Daten erhoben werden können. Die Quellen-TKÜ ist also möglich, greift aber noch nicht, weil die Software auf dem Endgerät erst noch installiert werden muss. Ein Zugriff auf das Endgerät des Nutzers, auf dem die Daten in der Anwendung unverschlüsselt liegen, würde die Heimlichkeit der Maßnahme aufheben. Deshalb soll mit § 100a Absatz 1 Satz 3 StPO-E wohl sichergestellt werden, dass heimlich auch auf die Inhalte und Umstände der Kommunikation durch eine entsprechend zu konfigurierende Software zugegriffen werden kann, die nach einer Anordnung der Maßnahme (Quellen-TKÜ) angefallen sind.

Soweit mit der kleinen Online-Durchsuchung diese Fälle erfasst werden sollen, handelt es sich also um die heimliche Ausleitung von Inhalten und Umständen der Kommunikation, also um eine Teilmenge der von der „großen Online-Durchsuchung“ erfassten Fälle (§ 100b StPO-E).

Systematisch folgerichtig und entsprechend dem betroffenen Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme müssten also die Schutzmechanismen dieses Grundrechts auch für die kleine Online-Durchsuchung greifen. Allerdings ist nicht zu übersehen, dass mit der kleinen Online-Durchsuchung nur auf die Kommunikationsinhalte und -umstände zurückgegriffen werden sollen, die mittels einer Quellen-TKÜ ab dem Zeitpunkt der richterlichen Anordnung sowieso erhoben werden könnten, aber nicht ausgeleitet werden können, weil die Software noch nicht installiert wurde. Die Vorschriften zur kleinen Online-Durchsuchung frieren also die ab dem Anordnungszeitpunkt ausgetauschten Kommunikationsinhalte und -umstände in den Schutzbereich des Art. 10 GG ein, was zur Subsidiarität des IT-Grundrechts führen würde.

Die Bemerkungen zur technischen Umsetzbarkeit und Funktionsbegrenzung der Software gelten auch hier.

Es wird eine weitere parlamentarische Diskussion zu diesem Thema angeregt.

3. Zu § 100a Absatz 3 StPO-E

Die bisherige Regelung in § 100a Abs. 3 StPO wird folgerichtig dahin gehend ergänzt, dass sich Maßnahmen auch dann gegen Dritte richten können, wenn der Beschuldigte deren informationstechnische Systeme nutzt.

4. Zu § 100a Absatz 4 StPO-E

Durch die neuen Abs. 4 und 6 wird einerseits die bisher in § 100b Abs. 4 StPO enthaltene Regelung (wegen des engen Bezugs zu dieser Maßnahme) in den § 100a StPO-E überführt. Darüber hinaus werden - vergleichbar der Regelungen in § 20l Abs. 2 bzw. 20k Abs. 2 BKAG - besondere Anforderungen an die Zulässigkeit der Maßnahme aufgestellt. Ob gerade die in Bezug auf Abs. 1 Satz 3 StPO-E aufgestellten Voraussetzungen (programm)technisch gewährleistet werden können, ist diesseits nicht bekannt und bedürfte einer Bewertung durch einen Sachverständigen. Solange die aufgestellten Anforderungen nicht erfüllbar sein sollten, wäre eine Maßnahme der Quellen-TKÜ nicht zulässig. Wie die Begründung auf Seite 22 f. zutreffend ausführt, wäre dann zu prüfen, ob eine Online-Durchsuchung in Betracht kommt.

§ 100a Abs. 4 StPO-E verpflichtet die erwähnten Dienstleister die Quellen-TKÜ zu ermöglichen sowie alle erforderlichen Auskünfte zu erteilen. Der Formulierungsvorschlag enthält keine Konkretisierung dieser Verpflichtungen sondern einen generellen Verweis auf das Telekommunikationsgesetz und die Telekommunikations-Überwachungsverordnung. Ausgeschlossen werden lediglich eine Pflicht zur Herausgabe der zur Dechiffrierung erforderlichen Schlüssel sowie das Versehen der jeweiligen Systemsoftware mit sog. „back doors“. Letzteres ist im Hinblick auf die Gefahren eines Missbrauchs durch Dritte ausdrücklich zu begrüßen.

Nach dieser Negativabgrenzung verbleibt noch ein weites Feld an Mitwirkungspflichten für die jeweiligen Anbieter. § 110 TKG verpflichtet Unternehmen, welche eine Telekommunikationsanlage betreiben, mit der öffentlich zugängliche Telekommunikationsdienste erbracht werden, an Maßnahmen zur Überwachung der Telekommunikation mitzuwirken, indem sie die technische Umsetzung gewährleisten und Auskünfte erteilen. Dies erfordert „Funktionsherrschaft“. Wer nur entsprechende Dienste erbringt, selbst aber keine Anlage betreibt ist nach Abs. 1 Nr. 2 verpflichtet sich zu vergewissern, dass der ausgewählte Betreiber die entsprechenden Verpflichtungen einhalten kann. Anbieter i.d.S. sind nur Netzwerkbetreiber, nicht jedoch die Anbieter von Messenger-Programmen oder anderen Applikationen.

Der Wortlaut von § 110 TKG könnte nahelegen, die Mitwirkungspflicht auch auf das Aufspielen des Überwachungsprogramms durch die Anbieter selbst zu erstrecken. Eine solche Interpretation ist jedoch ausgeschlossen:

1. Die Verpflichtung privater Unternehmen als Erfüllungsgehilfen der Strafverfolgungsbehörden wäre in der hier genannten Form bislang beispiellos. Sie stellte die Infiltration privater informationstechnischer Systeme im Auftrag des Staates dar. Solch ein staatlich angeordneter Eingriff nicht-staatlicher Akteure in die Grundrechte Dritter ist aus verfassungsrechtlicher Sicht, bedenklich. Im Gegensatz zur herkömmlichen TKÜ, wo ohne Zugriff auf die Systeme des Nutzers allein aus den Systemen der Telekommunikationsdienstleister ausgeleitet wird, wird bei der Quellen-TKÜ auf ein informationstechnisches System einer Person aktiv und intensiv eingegriffen. Diese Art eines Grundrechtseingriffs ist vom Staat und nicht von Privaten vorzunehmen. Der Grund, warum die TK-Anbieter Mitwirkungspflichten im Sinne des § 110 TKG haben ist der, dass es deren Systeme sind, auf die nur sie Zugriff haben. Die Mitwirkung zur TKÜ ist die

logische Konsequenz dieser Zugriffshoheit. Die gleiche Logik gilt aber nicht bei der Quellen-TKÜ.

2. Da in Zusammenhang mit der Mitwirkungspflicht das Software-Programm dem jeweiligen Dienstleister auch zugänglich gemacht werden müsste, bestünde darüber hinaus die Gefahr, dass der Quellcode zu Zwecken missbraucht wird, die nicht der Strafverfolgung dienen. Personen, welche im Rahmen ihrer Beschäftigung bei dem Telekommunikationsunternehmen selbst, oder einem von diesem beauftragten Subunternehmer, Zugang zu dem Programm haben bzw. mit dessen Aufspielen betraut sind, könnten dieses für eigene Zwecke nutzen bzw. Dritten zur Verfügung stellen. Die Vertraulichkeit der informationstechnischen Systeme der Nutzer würde dadurch erheblichen Gefahren ausgesetzt. Letztendlich kann staatlicherseits nicht gewollt sein, dass sich unkontrollierbar Schadsoftware verbreitet.

5. Praktische Umsetzung der Infiltration

Im Ergebnis muss die Software also von den Strafverfolgungsbehörden selbst aufgespielt werden.

Der Eingriff in das zu überwachende System darf nach der Formulierungshilfe „grundsätzlich nur auf technischem Wege oder mittels kriminalistischer List“ erfolgen. Ob mit dieser Formulierung auch Ausnahmen von diesem Grundsatz zugelassen sein sollen, bleibt unklar. Jedenfalls setzen das Recht auf ein faires Verfahren, der Grundsatz der Selbstbelastungsfreiheit sowie das Täuschungsverbot nach § 136a StPO der Art und Weise des Zugangs zu dem informationstechnischen System Grenzen.

Die Möglichkeit der manuellen Installation mittels CD oder USB-Sticks ist, soweit sie nicht mit einem Betreten der Wohnung des Betroffenen verbunden ist, nach der Formulierungshilfe grundsätzlich zulässig. Die praktische Umsetzung erfordert jedoch einen physischen, vom Benutzer unbemerkten Zugang zum Endgerät, sowie in den meisten Fällen die Überwindung einer Zugangssperre (v.a. Passwortsicherung). Beides dürfte in vielen Fällen kaum möglich sein.

Daneben kommt das Zusenden einer entsprechenden Datei bzw. eines Download-Links, mittels E-Mail oder als Kurznachricht, auch über ein soziales Netzwerk, in Betracht, nach deren Öffnung durch den Nutzer die Installation der Software eingeleitet wird. Ein solch „offenes“ Vorgehen wird beim verständigen und für die Gefahren von Computerviren sowie Hackerangriffen medial sensibilisierten Nutzer dazu führen, dass dieser Verdacht schöpfen und die Nachricht eines ihm unbekannten Absenders eher ungeöffnet löschen, als einen Download initiieren wird. Würde das Programm im Hinblick auf diese Bedenken als zweckdienliche Anwendung ausgegeben, ergebe sich daraus die Gefahr, dass der Beschuldigte die Software auch an Dritte weiterleiten und so unbewusste eine Infiltration dieser Systeme herbeiführen würde (vgl. BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 – Rn. 241).

Daneben ist auch zu prüfen, ob technisch sichergestellt werden kann, dass das Programm nach Beendigung der Maßnahme wieder rückstandslos vom informationstechnischen System des Betroffenen entfernt wird.

III. Zur Einführung einer Rechtsgrundlage für die Online-Durchsuchung, § 100b StPO-E

Mit dem neuen § 100b StPO-E wird erstmals eine Rechtsgrundlage für die Online-Durchsuchung geschaffen. Die Online-Durchsuchung im Sinne eines verdeckten staatlichen Zugriffs auf ein fremdes informationstechnisches System mit dem Ziel, dessen Nutzung zu überwachen und gespeicherte Inhalte aufzuzeichnen, ist derzeit zu Strafverfolgungszwecken nicht gestattet. Aus diesem Grunde sind bisher entsprechende Erkenntnisse aus präventiven Verfahren nicht verwertbar (vgl. § 161 Abs. 2 Satz 1 StPO).

Die neue strafprozessuale Befugnisnorm greift die strengen Anforderungen des BVerfG in seiner Entscheidung vom 27. Februar 2008 (MMR 2008, 315 ff.) auf.

1. Zu § 100b Absatz 1 StPO-E

Mit der Regelung wird die Online-Durchsuchung eingeführt. Damit findet eine besonders eingriffsintensive neue heimliche Ermittlungsmethode Eingang in den Kanon strafprozessualer Ermächtigungen. Die Regelung stuft entsprechend der Eingriffsintensität der Maßnahme die Anordnungsschwelle gegenüber § 100a StPO-E hoch und setzt den Verdacht einer „besonders schweren Straftat“, die in Abs. 2 in einem Katalog näher ausgeführt werden, voraus.

Mit „Eingriff“ in das informationstechnische System wird das Aufspielen einer Software zum Ausleiten aller – also auch alter, vor einer Anordnung gespeicherter Informationen – beschrieben. Damit wird es den Strafverfolgungsorganen möglich, alle auf Endgeräten und in Clouds gespeicherten Informationen auszulesen und das Nutzerverhalten am Endgerät zu überwachen, ohne dass der Betroffene davon Kenntnis erlangt. Bei der Durchführung der Maßnahme ist aber sicherzustellen, dass nicht andere Systeme des Endgerätes heimlich zur Ausleitung von Informationen genutzt werden, wie bspw. die Kamera an einem PC oder Mobiltelefon zur Überwachung des Wohnraumes. Die Gesetzesbegründung sollte klarstellen, das derartige Informationsbeschaffungen, die zu einer Rundumüberwachung führen könnten, nicht durch § 100b StPO-E gedeckt sind.

Die zahlreichen Missbrauchsmöglichkeiten, die im Zusammenhang mit dieser Software stehen können, sind bekannt. Die Formulierungshilfe lässt aber offen, wie staatlicherseits diesem Missbrauchspotential so entgegengewirkt wird, dass bspw. Manipulationen an der Software selbst, deren illegale Verbreitung, unautorisierter Einsatz durch Dritte und letztendlich der gesamten IT-Sicherheit vermieden werden können. Deshalb werden nachdrücklich Konkretisierungen angeraten, die sich auch im Gesetzeswortlaut niederschlagen müssen.

2. Zu § 100b Absatz 2 StPO-E

Angesichts der strikten Vorgaben des BVerfG ist es folgerichtig, dass die Online-Durchsuchung nur im Fall einer Straftat angeordnet werden kann, die im Straftatenkatalog des § 100c Abs. 2 StPO aufgeführt ist. Denn hinsichtlich der Eingriffsintensität ist die Online-Durchsuchung mit einer Wohnraumüberwachung vergleichbar. Der bisher in § 100c Abs. 2 StPO enthaltene Katalog wird in § 100b Abs. 2 StPO-E überführt und gilt dann sowohl für die Online-Durchsuchung, als auch (aufgrund einer Verweisung) für die akustische Wohnraumüberwachung gemäß § 100c StPO.

Zu erwähnen ist, dass der Katalog der besonders schweren Straftaten nicht den „einfachen" Wohnungseinbruchdiebstahl enthält. Sollte dieser zukünftig noch in den Katalog des § 100g Abs. 2 Satz 2 StPO aufgenommen werden, wäre zu prüfen, den Katalog des § 100b Abs. 2 StPO-E ebenfalls um diesen Straftatbestand zu erweitern. Begründen lässt sich dies damit, dass sowohl § 100b StPO-E als auch § 100g StPO auf auf denselben Typus von Straftaten abzielen: „besonders schwere Straftaten".

Bei einer ins Auge gefassten Synchronisierung der Straftatenkataloge sollte auch erwogen werden, den gegenwärtig im Katalog des § 100c Abs. 2 Nr. 1 lit. a) StPO enthaltenen Straftatbestand der Terrorismusfinanzierung im Sinne von § 89c Abs. 1 - 4 StGB in den Katalog den Katalog des § 100g Abs. 2 Satz 2 StPO aufzunehmen.

IV. Zu § 100d StPO-E

Zwar wird nun - anders als dies bisher in § 100c Abs. 4 Satz 2 und 3 der Fall ist - in § 100d Abs. 4 StPO-E nicht mehr im Detail klargestellt, wann im Regelfall kein Kernbereichsbezug gegeben ist (im Regelfall nicht bei Geschäftsräumen und nicht bei Äußerungen mit Bezug zu Straftaten). In der Gesetzesbegründung wird auf Seite 26 im 2. Absatz jedoch zutreffend ausgeführt, dass auch die bisherigen Regelungen lediglich eine besondere Ausgestaltung der umfangreichen Rechtsprechung des BVerfG darstellen und letztlich mit der Streichung keine Änderung bezweckt ist. Vor dem Hintergrund der - in der Begründung auch zitierten - Entscheidung des BVerfG vom 11. Mai 2007 (NJW 2007, 2753 ff.), wonach die Frage nach der Kernbereichsrelevanz letztlich stets eine Frage der Abwägung im Einzelfall ist, erscheint die Streichung vertretbar.

Daneben werden alle vom Bundesverfassungsgericht gestellten Anforderungen zum Kernbereichsschutz beachtet.

V. Zu § 100e StPO-E

Zu überdenken ist, ob die verfahrensrechtlichen Vorgaben für die akustische Wohnraumüberwachung im Verhältnis 1:1 auf die Online-Durchsuchung übertragen werden müssen. Gemäß § 100e Abs. 2 StPO-E soll zukünftig auch für Anordnungen nach § 100b StPO-E die Strafkammer nach § 74a Abs. 4 GVG zuständig sein. Ein entsprechendes Erfordernis kann der Entscheidung des BVerfG vom 27. Februar 2008 aber nicht entnommen werden. Dort wird nur folgendes ausgeführt (MMR 2008, 315 [322]):

„*Bei einem Grundrechtseingriff von besonders hohem Gewicht wie dem heimlichen Zugriff auf ein informationstechnisches System reduziert sich der Spielraum dahingehend, dass* *die Maßnahme grds. unter den Vorbehalt richterlicher Anordnung zu stellen ist. Richter können auf Grund ihrer persönlichen und sachlichen Unabhängigkeit und ihrer ausschließlichen Bindung an das Gesetz die Rechte des Betroffenen im Einzelfall am besten und sichersten wahren (vgl. BVerfGE 103, 142, 151; 107, 299, 325). Vorausgesetzt ist allerdings, dass sie die Rechtmäßigkeit der vorgesehenen Maßnahme eingehend prüfen und die Gründe schriftlich festhalten (zu den Anforderungen an die Anordnung einer akustischen Wohnraumüberwachung vgl. BVerfGE 109, 279, 358 ff.; zur Kritik an der Praxis der Ausübung des Richtervorbehalts bei Wohnungsdurchsuchungen vgl. BVerfGE 103, 142, 152, m.w.Nw.)*."

Dass bei der akustischen Wohnraumüberwachung eine mit drei Richtern besetzte Kammer zu befinden hat, ist verfassungsrechtlich vorgeschrieben, Art. 13 Absatz 3 Satz 3 GG. Im Fall der Online-Durchsuchung greift dieser aber gerade nicht ein. Zwar ist die Online-Durchsuchung eine sehr eingriffsintensive Maßnahme und ohne Zweifel mit einer akustischen Wohnraumüberwachung vergleichbar. Der heimliche Eingriff in das Grundrecht aus Art. 13 GG hat dennoch eine tiefere Bedeutung und betrifft den inneren Lebensbereich einer Person, der durch die akustische Wohnraumüberwachung in Echtzeit betroffen wird.

Es gehört natürlich zur Einschätzungsprärogative des Gesetzgebers, eine dem Art. 13 Absatz 3 Satz 3 entsprechende Regelung auf § 100b StPO-E zu übertragen. Zwingende Gründe sind dafür jedoch nicht ersichtlich.

VI. Ergebnis

Es bleibt festzuhalten, dass der Änderungsvorschlag nicht alle wesentlichen Fragen im Zusammenhang mit der Einführung dreier neuer, besonders eingriffsintensiver und heimlicher Ermittlungsmethoden im Bereich der Repression beantwortet.