18. Wahlperiode

Deutscher Bundestag
Ausschuss für Recht und Verbraucherschutz

Wortprotokoll
der 152. Sitzung

Ausschuss für Recht und Verbraucherschutz
Berlin, den 31. Mai 2017, 16:07 Uhr
Berlin, Paul-Löbe-Haus, Saal 2.600

Vorsitz: Renate Künast, MdB

Tagesordnung - Öffentliche Anhörung

Einziger Tagesordnungspunkt **Seite 12**

Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze

BT-Drucksache 18/11272

Federführend:
Ausschuss für Recht und Verbraucherschutz

Mitberatend:
Innenausschuss
Finanzausschuss
Ausschuss für Familie, Senioren, Frauen und Jugend
Ausschuss für Umwelt, Naturschutz, Bau und Reaktorsicherheit

Gutachtlich:
Parlamentarischer Beirat für nachhaltige Entwicklung

Berichterstatter/in:
Abg. Alexander Hoffmann [CDU/CSU]
Abg. Dr. Patrick Sensburg [CDU/CSU]
Abg. Dr. Johannes Fechner [SPD]
Abg. Jörn Wunderlich [DIE LINKE.]
Abg. Hans-Christian Ströbele [BÜNDNIS 90/DIE GRÜNEN]

Sitzung des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss)

Mittwoch, 31. Mai 2017, 16:00 Uhr

Ordentliche Mitglieder des Ausschusses	Unterschrift	Stellvertretende Mitglieder des Ausschusses	Unterschrift
CDU/CSU		CDU/CSU	
Brandt, Helmut		Bosbach, Wolfgang	
Heck Dr., Stefan		Fabritius Dr., Bernd	
Heil, Mechthild		Frieser, Michael	
Hirte Dr., Heribert		Gutting, Olav	
Hoffmann, Alexander		Harbarth Dr., Stephan	
Hoppenstedt Dr., Hendrik		Hennrich, Michael	
Launert Dr., Silke		Heveling, Ansgar	
Luczak Dr., Jan-Marco		Jörrißen, Sylvia	
Monstadt, Dietrich		Jung Dr., Franz Josef	
Ripsam, Iris	J Ripsam	Lach, Günter	
Rösel, Kathrin		Lerchenfeld, Philipp Graf	
Seif, Detlef		Maag, Karin	
Sensburg Dr., Patrick		Noll, Michaela	
Steineke, Sebastian		Schipanski, Tankred	
Sütterlin-Waack Dr., Sabine		Schnieder, Patrick	
Ullrich Dr., Volker		Stritzl, Thomas	
Wanderwitz, Marco		Weisgerber Dr., Anja	
Wellenreuther, Ingo		Woltmann, Barbara	
Winkelmeier-Becker, Elisabeth			

Referat ZT 4 - Zentrale Assistenzdienste, Tagungsbüro
Luisenstr. 32-34, Telefon: +49 30 227-32251, Fax: +49 30 227-36339

18. Wahlperiode

Sitzung des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss)
Mittwoch, 31. Mai 2017, 16:00 Uhr

Ordentliche Mitglieder des Ausschusses	Unterschrift	Stellvertretende Mitglieder des Ausschusses	Unterschrift
SPD		**SPD**	
Bähr-Losse, Bettina		Barley Dr., Katarina	
Bartke Dr., Matthias		Franke Dr., Edgar	
Brunner Dr., Karl-Heinz		Hartmann (Wackernheim), Michael	
Drobinski-Weiß, Elvira		Högl Dr., Eva	
Fechner Dr., Johannes		Lischka, Burkhard	
Flisek, Christian		Miersch Dr., Matthias	
Groß, Michael		Müller, Bettina	
Hakverdi, Metin		Müntefering, Michelle	
Jantz-Herrmann, Christina		Özdemir (Duisburg), Mahmut	
Rode-Bosse, Petra		Rohde, Dennis	
Steffen, Sonja		Schieder, Marianne	
Strässer, Christoph		Vogt, Ute	
Eslen, Saskia			
DIE LINKE.		**DIE LINKE.**	
Binder, Karin		Jelpke, Ulla	
Korte, Jan		Lay, Caren	
Wawzyniak, Halina		Pitterle, Richard	
Wunderlich, Jörn		Renner, Martina	

26. Mai 2017

Anwesenheitsliste
Referat ZT 4 - Zentrale Assistenzdienste, Tagungsbüro
Luisenstr. 32-34, Telefon: +49 30 227-32251, Fax: +49 30 227-36339

Seite 2 von 3

18. Wahlperiode

Sitzung des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss)
Mittwoch, 31. Mai 2017, 16:00 Uhr

Ordentliche Mitglieder des Ausschusses	Unterschrift	Stellvertretende Mitglieder des Ausschusses	Unterschrift
BÜ90/GR		BÜ90/GR	
Keul, Katja		Beck (Köln), Volker	
Künast, Renate		Kühn (Tübingen), Christian	
Maisch, Nicole		Mihalic, Irene	
Ströbele, Hans-Christian		Notz Dr., Konstantin von	

26. Mai 2017

Anwesenheitsliste
Referat ZT 4 - Zentrale Assistenzdienste, Tagungsbüro
Luisenstr. 32-34, Telefon: +49 30 227-32251, Fax: +49 30 227-36339

Seite 3 von 3

Sitzung des Ausschusses für Recht und Verbraucherschutz
(6. Ausschuss)
Mittwoch, 31. Mai 2017, 16:00 Uhr

	Fraktionsvorsitz	Vertreter
CDU/CSU		
SPD		
DIE LINKE.		
BÜNDNIS 90/DIE GRÜNEN		

Fraktionsmitarbeiter

Name (Bitte in Druckschrift)	Fraktion	Unterschrift
Liebs, Hartmut	Die Linke.	H. Liebs
K-H Hage	B90/Grüne	
Carmen Simukat	SPD	
Kieser Lika	CDU/CSU	
Tabbara, Tarik	Grüne	
Wollseifer, Johannes	SPD	
Glas, Vera	CDU/CSU	

Stand: 23. Februar 2015
Referat ZT 4 – Zentrale Assistenzdienste, Luisenstr. 32-34, Telefon: +49 30 227-32659, Fax: +49 30 227-36339

Tagungsbüro

Sitzung des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss)
Mittwoch, 31. Mai 2017, 16:00 Uhr

Bundesrat

Land	Name (bitte in Druckschrift)	Unterschrift	Amts-bezeichnung
Baden-Württemberg	VON TROTHA		StM
Bayern	Bauer M.		RD
Berlin			
Brandenburg			
Bremen			
Hamburg			
Hessen			
Mecklenburg-Vorpommern			
Niedersachsen	Komin, Hannes Hoffeld-Klein, Anne		
Nordrhein-Westfalen			
Rheinland-Pfalz			
Saarland			
Sachsen	Salz, Andrea		MdL
Sachsen-Anhalt			
Schleswig-Holstein			
Thüringen	Bieder, Hendrik		RiLG

Stand: 23. Februar 2015
Referat ZT 4 – Zentrale Assistenzdienste, Luisenstr. 32-34, Telefon: +49 30 227-32659, Fax: +49 30 227-36339

Tagungsbüro

Sitzung des Ausschusses für Recht und Verbraucherschutz
(6. Ausschuss)
Mittwoch, 31. Mai 2017, 16:00 Uhr

Ministerium bzw. Dienststelle (bitte in Druckschrift)	**Name** (bitte in Druckschrift)	Unterschrift	**Amts-bezeichnung**
BMJV	Claus, Susanne	Claus	RiLG
BMJV	Voss, Nikola		StA
BMJV	LANGE		RDir
BMJV	Dr. Krüger		MDg.
BMJV	Dr. Feldmann, Helga		RiLG
BMJV	Rut Ley		RD
~~AA~~	~~PLANK, IRENE~~		~~AR, REF~~

Stand: 23. Februar 2015
Referat ZT 4 – Zentrale Assistenzdienste, Luisenstr. 32-34, Telefon: +49 30 227-32659, Fax: +49 30 227-36339

Anwesenheitsliste der Sachverständigen

zur Anhörung des Ausschusses für Recht und Verbraucherschutz
am Mittwoch, 31. Mai 2017, 16.00 Uhr

Name	Unterschrift
Dr. Ulf Buermeyer, LL.M. (Columbia) Richter am Landgericht Berlin	
Peter Henzler Vizepräsident beim Bundeskriminalamt Wiesbaden	
Alfred Huber Staatsanwaltschaft Nürnberg-Fürth Oberstaatsanwalt, Stellvertretender Behördenleiter und Abteilungsleiter der BtM- und OK-Abteilung	
Dr. Matthias Krauß Bundesanwalt beim Bundesgerichtshof Karlsruhe	
Linus Neumann Berlin	
Prof. Dr. Arndt Sinn Universität Osnabrück Lehrstuhl für Deutsches und Europäisches Straf- und Strafprozessrecht, Internationales Strafrecht sowie Strafrechtsvergleichung Direktor des Zentrums für Europäische und Internationale Strafrechtsstudien (ZEIS)	

Sprechregister Abgeordnete

Sprechregister Sachverständige

* für Sachverständigen Michael Greven, Oberstaatsanwalt beim Bundesgerichtshof Karlsruhe

Die Vorsitzende **Renate Künast**: Herzlich Willkommen zur öffentlichen Anhörung zum Gesetzentwurf der Bundesregierung zur Änderung des Strafgesetzbuches (StGB), des Jugendgerichtsgesetzes (JGG), der Strafprozessordnung (StPO) und weiterer Gesetze. Ich begrüße auch die Abgeordneten aus den mitberatenden Ausschüssen – das sind Innenausschuss, Finanzausschuss, Familienausschuss und Umweltausschuss. Ich begrüße die sechs Sachverständigen. Dazu weise ich darauf hin, dass Herr Greven, der von der CDU/CSU benannt war für den Deutschen Richterbund, nicht hier sein kann, weil sein Flug gestrichen wurde. Ich schlage vor – so ist das wohl auch abgesprochen –, dass Herr Dr. Krauß, sein Kollege als Staatsanwalt beim BGH, sein schriftliches Statement verliest – sehr schön, dass Sie das machen, Herr Krauß. Ich begrüße Herrn Parlamentarischer Staatssekretär Lange, die übrigen Vertreter der Bundesregierung und die Gäste auf der Tribüne.

Meine Damen und Herren, wir haben heute die zweite Anhörung zum Gesetzentwurf der Bundesregierung zur Änderung des StGB, des JGG und der StPO. Die erste hatten wir am 22. März diesen Jahres. Das Protokoll liegt vor, ist auch im Netz veröffentlicht. Gegenstand der heutigen Anhörung ist die Ausschussdrucksache 18(6)334 vom 15. Mai diesen Jahres. Auf dieser Ausschussdrucksache finden Sie eine Formulierungshilfe der Bundesregierung für einen Änderungsantrag der Fraktionen der CDU/CSU und SPD zum genannten Gesetz. Damit sollen Rechtsgrundlagen in der StPO geschaffen werden für die Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) und die Online-Durchsuchung, also den verdeckten staatlichen Zugriff auf fremde informationstechnische Systeme über Kommunikationsnetze mittels Überwachungssoftware und die Telekommunikationsüberwachung ebenfalls durch Infiltration eines fremden IT-Systems. Mit beiden Maßnahmen sind spezifische Eingriffe in Grundrechte verbunden, deshalb sind spezifische Anforderungen zu stellen. Es gibt das Urteil zum BKA-Gesetz des Bundesverfassungsgerichts von April 2016, das Ausführungen macht zu den Anforderungen, die an heimliche Überwachungsmaßnahmen gestellt werden müssen. Darum wird es hier unter anderem gehen, dass die eingeladenen Sachverständigen uns darlegen, mit Blick auf die Formulierungshilfe, wie die verfassungsrechtlichen Anforderungen sind. Das soll erstmal genügen als kurzer Hinweis, um was es heute geht.

Noch ein paar formale Hinweise zum Ablauf. Wir machen es so: Die Sachverständigen erhalten zu Anfang die Gelegenheit zu einem kurzen Statement von ungefähr fünf Minuten. Die digitale Uhr zählt rückwärts. Wenn es rot wird, freuen wir uns, wenn Sie langsam zum Ende kommen, aber ich möchte Sie nicht in Ihren Gedankengängen unterbrechen. Wir werden alphabetisch mit Herrn Dr. Buermeyer beginnen. Die Abgeordneten können dann höchstens zwei Fragen stellen – so machen wir es hier. Sie antworten dann in umgekehrter alphabetischer Reihenfolge. Es gibt notfalls mehrere Fragerunden. Es gibt dann kein Zeitlimit, weil es ja von der Zahl der Fragen abhängt, aber Sie können durchaus zwischendurch auf die Uhr gucken.

Eine öffentliche Anhörung heißt: Tonaufzeichnung, Wortprotokoll durch das Ausschusssekretariat, aber keine Ton- und Bildaufnahmen auf der Tribüne.

Herr Dr. Buermeyer, Sie haben das Wort.

SV **Dr. Ulf Buermeyer**: Frau Vorsitzende, ganz herzlichen Dank. Meine Damen und Herren, ich möchte mich zunächst einmal bedanken für die Einladung und die Gelegenheit, heute ein paar Gedanken beisteuern zu können zu dieser Anhörung. Wir sprechen über den Einsatz von sogenannten Staatstrojanern, staatlich kontrollierte Software, mit der Rechnersysteme infiziert werden sollen. Und um das gleich in den einleitenden Sätzen zu sagen: Hier sprechen wir nicht von Petitessen, ganz im Gegenteil. Angedacht sind Rechtsgrundlagen für außerordentlich schwerwiegende Eingriffe. Es ist nämlich so, dass, wenn ein System mit einer solchen Software infiziert wird, alle Inhalte ausgelesen werden können, jedenfalls technisch. Die gesamte Kommunikation kann mitgeschnitten werden, und es können technisch auch Kameras und Mikrofone dieser Systeme infiziert werden. Es handelt sich also um eine Maßnahme mit einer Reichweite, wie sie die Strafprozessordnung bislang nicht kennt. Sie geht insbesondere auch deutlich hinaus über das, was wir als sogenannten großen Lauschangriff kennen, also die akustische Wohnraumüberwachung. Und das,

denke ich, sollte man sich klar machen, das ist wirklich das ganz große Besteck des Strafprozessrechts, das hier angedacht wird und das sollte auch die Debatte am heutigen Tage bestimmen. Die betroffen Personen werden in einer Weise zu gläsernen Menschen gemacht, wie es die Strafprozessordnung bisher nicht kennt. Damit ist natürlich der Stab nicht gebrochen über diese Maßnahmen. Auch schlimmste, auch schwerste Eingriffe können verhältnismäßig sein von Verfassung wegen, aber man muss eben die Schwere des Eingriffs einstellen in die Abwägung. Mit diesen besonders schweren Eingriffen korrespondieren auch die schärfsten Vorgaben, die das Bundesverfassungsgericht bisher dem Gesetzgeber überhaupt jemals gemacht hat – in seiner Entscheidung von Februar 2008, als es bereits einmal über den präventiven Einsatz von Staatstrojanern zu entscheiden hatte. Damals ging es um das Verfassungsschutzgesetz des Landes Nordrhein-Westfalen. Und ich möchte die zwei Kernsätze kurz zitieren, weil sie von so zentraler Bedeutung sind für die Debatte: „Ein derartiger Eingriff“ – so schreibt der Erste Senat – „darf nur vorgesehen werden, wenn die Eingriffsermächtigung ihn davon abhängig macht, dass tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut vorliegen. Überragend wichtig sind zunächst Leib, Leben und Freiheit der Person. Ferner sind überragend wichtig solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.“ Mit anderen Worten: Hier geht es ums Ganze. Hier geht es nicht um vermeintlich lässliche Sünden, sondern hier geht es ums Ganze, rechtsstaatlich betrachtet. Und das muss man sich als Gesetzgeber sehr genau überlegen, wenn man dieses ganz große Besteck tatsächlich zum Einsatz bringen will.

Jenseits des hohen Preises für die Freiheitsrechte sind aber auch Fragen der Sicherheitspolitik zu betrachten. Es wird ja sehr häufig vom Gegensatz von Freiheit und Sicherheit gesprochen. Hier allerdings würde eine Maßnahme, die der Sicherheit dienen soll, zugleich massiv zu einer Kultur der IT-Unsicherheit beitragen, und zwar aus einem recht einfachen Grund – ich bin überzeugt, dass Herr Neumann vom Chaos Computer Club dazu noch eine ganze Menge mehr sagen wird: Wenn man ein System mit einem Staatstrojaner infizieren will, braucht man eine Sicherheitslücke. Sie brauchen eine technische Hintertür in das betroffene System. Und bei solchen Sicherheitslücken ist es so – das ist die Natur einer Sicherheitslücke –, dass es da gerade keine Zugriffskontrolle gibt. Mit anderen Worten: Es gibt keine spezielle BKA-Sicherheitslücke. Jede Sicherheitslücke kann auch von irgendeinem russischen oder chinesischen Hacker ausgenutzt werden, der Ihnen dann einen Festplattenverschlüsselungstrojaner einbaut. Mit anderen Worten: Sicherheitslücken zu sammeln, um Staatstrojaner einsetzen zu können, führt zu einer massiven Beeinträchtigung der IT-Sicherheit insgesamt, weil es falsche Anreize setzt, solche Sicherheitslücken nicht den Herstellern zu melden, damit sie geschlossen werden können, sondern sie vielmehr zu sammeln.

Ich möchte kurz noch auf zwei Punkte eingehen, die mir aus rechtlicher Hinsicht besonders bedeutsam erscheinen. Die Online-Durchsuchung, also der vollumfängliche Zugriff auf ein System, wie ich es eben schon kurz geschildert habe, ist nach dem Vorschlag der Formulierungshilfe geplant bei einem außerordentlich weiten Straftatenkatalog, und viele der genannten Straftatbestände haben mit überragend wichtigen Rechtsgütern nichts zu tun. Ich denke insbesondere an die Straftatbestände zum Schutz des Vermögens. Damit will ich nicht sagen, dass der Vermögensschutz nicht bedeutend wäre, aber er ist in der Aufzählung der überragend wichtigen Rechtsgüter des Bundesverfassungsgerichts in seiner Entscheidung 2008 schlicht nicht enthalten. Und diese Vorgaben, denke ich, sind die Mindestvorgaben, die ein Gesetzgeber auch im repressiven Bereich beachten müsste.

Noch missratender, aus meiner Sicht, auch verfassungsrechtlich betrachtet, sind die Vorschläge zur Quellen-TKÜ, also zum Mitschneiden von laufender Kommunikation. Hier sind zwar nur die Vorgaben von Artikel 10 Absatz 1 des Grundgesetzes (GG), das Telekommunikationsgeheimnis, zu beachten. Aber diese Ausnahme gilt nur, wenn der Trojaner tatsächlich nur laufende Kommunikation mitschneiden kann. Hier soll es aber unter dem Deckmantel der Quellen-TKÜ möglich sein, auch frühere Kommunikationen mitzuschneiden, was im offenen Widerspruch steht zur Entscheidung

des Bundesverfassungsgerichts. Die großzügigen Regelungen für die Quellen-TKÜ sind schon eine Ausnahme von den grundsätzlich geltenden hohen Anforderungen für die Online-Durchsuchung, und eine analoge Anwendung einer Ausnahme verbietet sich. Das ist eigentlich das kleine Einmaleins der Juristerei. Insofern verwundert es mich, dass das Bundesministerium der Justiz und für Verbraucherschutz hier tatsächlich eine solche Ausnahme analog auf die frühere Kommunikation anwenden möchte.

Schließlich, das ist mein letzter Punkt, möchte ich kurz auf das Stichwort „Going Dark“ eingehen. Unter diesem Stichwort wird ja diskutiert, dass die Ermittlungsbehörden nicht mehr in der Lage seien, in angemessenem Maße Kommunikation mitzuschneiden. Sie werden sicherlich auch von meinen Kollegen noch schlimme Dinge hören, dass die Strafverfolger blind seien. Das muss man in dieser Eindeutigkeit allerdings in das Reich der Legenden verweisen. Natürlich sind Telekommunikationsüberwachungen wichtig, man sollte sie aber auch nicht überschätzen. Der Haupteinsatzzweck nach allen Statistiken ist die Bekämpfung der Betäubungsmittelkriminalität, und gerade in diesem Bereich erleben wir heute schon extrem konspiratives Handeln der Beschuldigten. Das heißt, da bestellt niemand mal eben am Telefon ein Kilo Koks, sondern da werden geheime Schlüsselbegriffe verwendet, da wird sich zu konspirativen Treffen verabredet. Mit anderen Worten: Auch in der heutigen klassischen Mobilfunkkommunikation erweisen sich TKÜ häufig als wenig hilfreich, und man bekommt ein bisschen den Eindruck, dass die Verschlüsselungsverfahren, die es natürlich gibt und die dazu führen, dass manche Kommunikation nicht mehr erfasst werden kann – ein wenig zum Sündenbock gemacht wird. Außerdem noch ein wichtiger Punkt in dem Zusammenhang: Durchsuchung und Beschlagnahme von Mobilfunkgeräten oder Computern führen dazu, dass die meisten der Daten durchaus noch gewonnen werden können, nur eben später. Mit anderen Worten: Es geht gerade nicht darum, dass ein kompletter Beweisverlust eintritt für die Ermittlungsbehörden. Das gibt es in Ausnahmefällen, im Regelfall aber handelt es sich hier nur um ein taktisches Problem, das heißt, man bekommt die Beweise nur etwas später, wenn man offen zugreift, und man bekommt sie nicht mehr, wie bei einer klassischen Telekommunikationsüberwachung, heimlich und etwas früher. Das sollte man sich bei der Verhältnismäßigkeitsabwägung immer vor Augen führen.

Schließlich: Verkehrsdaten und Standortdaten kann man überhaupt nicht verschlüsseln. Das heißt also, das „Going Dark“-Problem betrifft gerade nicht die Standorte. „Going Dark“ ist ein Problem, aber es ist durchaus nicht ein so großes Problem, wie es mitunter dargestellt wird, und der rechtsstaatliche Preis, denke ich, für den Einsatz von Trojanern erweist sich deswegen als doch sehr, sehr hoch. Vielen Dank für die Aufmerksamkeit.

Die **Vorsitzende**: Jetzt wäre Herr Greven dran, so dass ich Herrn Dr. Krauß um die Verlesung des Statements bitte. Danke.

SV **Dr. Matthias Krauß** *(für SV Michael Greven)*: Vielen Dank, Frau Vorsitzende. Herr Greven hat mich gebeten, nochmal seine Entschuldigung zu überbringen, weil Air Berlin es nicht geschafft hat, ihn von Karlsruhe nach Berlin zu bringen. Ich verlese jetzt sozusagen als Bote die Erklärung von Herrn Greven:

Mein Anliegen ist es, Ihnen die Sicht eines Praktikers zu vermitteln. Ich bearbeite seit 2002 Ermittlungsverfahren in der Abteilung für Straftaten gegen die äußere Sicherheit der Bundesrepublik Deutschland. Dabei handelt es sich zumeist um Straftaten im Bereich der Spionage und der Proliferation. Die Telekommunikationsüberwachung ist in den von mir geführten Verfahren eine regelmäßige Ermittlungsmaßnahme. Dies unterscheidet meine Tätigkeit vom Berufsalltag der Mehrzahl der deutschen Staatsanwältinnen und Staatsanwälte. Diese haben im Jahr 2015 rund 5 Millionen Ermittlungsverfahren eingeleitet. Lediglich in 5.945 Ermittlungsverfahren, dies sind etwa 0,12 Prozent, kam es zu Telekommunikationsüberwachungsmaßnahmen und nur in sieben Verfahren zu Maßnahmen der akustischen Wohnraumüberwachung. Ich wage jetzt eine Prognose: Durch die neu geschaffenen Rechtsgrundlagen für die Quellentelekommunikationsüberwachung und die Online-Durchsuchung wird sich an diesem Zahlenverhältnis wenig ändern. Fälle der Online-Durchsuchung werden genauso

selten vorkommen wie die akustische Wohnraumüberwachung. Der Grund liegt auf der Hand. Einsatzgebiet der Telekommunikationsüberwachung war und ist nicht, wie bisweilen suggeriert wird, das massenhafte und unkontrollierbare Abhören von zehntausenden Mobiltelefonen von Beschuldigten aus dem Bereich der mittleren oder sogar leichten Kriminalität. Nein, eingesetzt werden die Maßnahmen tatsächlich, wie sich aus der jährlichen Statistik des Bundesamtes für Justiz ergibt, im Bereich der schweren und organisierten Kriminalität sowie bei der Bekämpfung von Staatsschutzstraftaten wie Terrorismus und Spionage. In diesen Bereichen ist festzustellen, dass die herkömmliche Telekommunikationsüberwachung, die noch vor einigen Jahren zumeist verlässliche Erkenntnisse zu strafbaren Handlungen von Beschuldigten erbracht hat, im Laufe der letzten zwei bis drei Jahre in immer weniger Fällen einen erfolgversprechenden Ermittlungsansatz darstellt. Die technische Entwicklung hat dazu geführt, dass der für die Polizeibehörden auswertbare Anteil an der Telekommunikation nur noch marginal ist und weiter rasant abnimmt. In der weit überwiegenden Anzahl der von mir in den vergangenen Jahren geführten Ermittlungsverfahren erbrachte die Überwachung nur noch geringe oder überhaupt keine Erkenntnisse mehr. Erst vor wenigen Tagen habe ich in einem Protokoll einer herkömmlichen Telekommunikationsüberwachungsmaßnahme wieder lesen müssen, dass die Beschuldigten vereinbaren, im Anschluss an das gerade geführte Telefongespräch sensible Inhalte über einen Instant-Messenger auszutauschen, da dieser von der Polizei ja nicht abgehört werden könne. Dies ist nur einer von vielen Belegen dafür, dass die klassische Telekommunikationsüberwachung als Ermittlungsinstrument weitgehend ausfällt. Eine grundlegende Anpassung der wichtigen Eingriffsrechte der Strafverfolgungsbehörden gemäß § 100a ff. StPO an den rasanten Fortschritt moderner Kommunikationstechnologien ist bislang unterblieben. Aus Sicht der staatsanwaltlichen Praxis, die dringend klare gesetzliche Vorgaben benötigt, ist daher der vorliegende Gesetzentwurf zur Schaffung einer Rechtsgrundlage für die Quellen-Telekommunikationsüberwachung und die Online-Durchsuchung in der Strafprozessordnung ausdrücklich zu begrüßen. Vielen Dank.

Die **Vorsitzende**: Danke sehr. Herr Henzler hat das Wort jetzt, bitte.

SV **Peter Henzler**: Vielen Dank, Frau Vorsitzende, meine Damen und Herren. Im Gegensatz zu der in der Öffentlichkeit weit verbreiteten Meinung, fast schon Überzeugung, die Sicherheitsbehörden seien heutzutage technisch in der Lage, die Kommunikation der Bürgerinnen und Bürger, mithin auch die Kommunikation terroristischer und krimineller Akteure, umfassend zu überwachen, aufzuzeichnen und digitale Datenträger auszuwerten, sind die Strafverfolgungsbehörden auf diesem Gebiet weitreichend blind und taub. Gängige Kommunikationsdienste, sogenannte Messenger, wie Facebook-Messenger, WhatsApp, Telegram, Viber und Skype, um nur einige zu nennen, ohne solche russischer und chinesischer Vergleichbarkeit zu vergessen, verschlüsseln automatisch, das heißt ohne Zutun der Nutzer, den Datenverkehr. Datenträger, Festplatten, Sticks sind mit einigen wenigen Klicks, mit einem Passwort wirkungsvoll gegen jeden Zugriff von außen und für alle Zeit nicht überwindbar zu sperren. Diese Erfahrungen begegnen uns täglich in der polizeilichen Praxis. Besonders schmerzhaft sind sie dort, wo es um terroristische Aktivitäten und schwere, oft flächendeckende Straftaten auf dem Gebiet der allgemeinen, schweren und organisierten Kriminalität geht. Nach unseren Auswertungen wird die Kommunikation im Zusammenhang mit terroristischen Aktivitäten über Messenger zu nahezu 100 Prozent und auf den anderen Feldern im Regelfall, das heißt zu 70 Prozent, verschlüsselt. In zwei Wochen beginnt vor dem OLG Hamburg die Hauptverhandlung gegen drei Männer, von denen wir wissen, dass sie – lassen Sie mich das so sagen – eine Kopie der Selbstmordattentäter des Stade de France sind. Wie wir ermitteln konnten, bestanden folgende Parallelen: Sie haben das gleiche Schleusungsnetzwerk genutzt, sie hatten vom IS bereitgestellte Pässe, die bereits in Syrien in Auftrag gegeben wurden, sie haben eine Expressschleusung Rakka – Griechenland erhalten, sie hatten Reisegeld in Höhe von 2.000 bis 3.000 Dollar in der gleichen Stückelung, und sie haben gleiche Mobiltelefone, Smartphones, mit voreingestellten Kommunikationsprogrammen,

dabei unter anderem die Nutzung von bestimmten Telefonnummern-Blöcken, bei sich gehabt. Aufgrund der Parallelen leitete der Generalbundesanwalt (GBA) am 1. April 2016 ein Ermittlungsverfahren ein nach § 129a, b StGB – in unserer Sprache namens Codename „Galaxy“ – wegen der Smartphones.

Bei 67 Maßnahmen, unter anderem Telefonnummern, Geräteüberwachung, DSL- und Hotspot-Überwachung von April bis September, gab es nur 520 klassische Telefonate, in der Mehrzahl mit älteren Kontaktpersonen und Behörden. Die übrige Kommunikation blieb uns, weil über Messenger-Dienste geführt, verschlossen. Bei vielen der überwachten Maßnahmen ließ sich mangels Kommunikationsinhalten noch nicht einmal mehr feststellen und zuordnen, ob das Gerät oder die SIM-Karte noch von den Beschuldigten selbst oder von anderen, an die es weiter gegeben wurde, genutzt wurde. Wie im vorliegenden Fall hatte der IS im Mai zu Anschlägen in der Zeit der Europameisterschaft 2016 aufgerufen. Wir haben dann mit einem großen Aufwand durch Observationsmaßnahmen zumindest festgestellt, dass diese Personen nicht Zugriff auf Tatmittel nehmen oder gar eine Aktion starten. Wir haben keine weiteren Erkenntnisse zu dem Sachverhalt finden können, es muss also die Hauptverhandlung auf der Basis dessen stattfinden, was ich Ihnen im Wesentlichen gesagt habe. Mit einer besorgniserregenden Dynamik haben sich diverse Formen von Kriminalität durch Nutzung von elektronischen Handelsplattformen im Internet, dem sogenannten Darknet, entwickelt. Alle Beteiligten des Handels illegaler Güter, wie Rauschgift, entwendete Daten, illegale Arzneimittel, Waffen usw., wickeln die Geschäfte inklusive Bezahlung mittels verschlüsselter Informationstechnologie ab. Die Strafverfolgungsbehörden bleiben außen vor, es entwickeln sich insoweit strafverfolgungsfreie Räume. Die bei all diesen Aktivitäten anfallenden Daten dieser illegalen Geschäfte und auf dem Gebiet des Handels mit oder des Tausches von Kinderpornografie, die unerträglichen Bild- und Videodaten, werden auf Datenträgern, heutzutage oftmals im Terabyte-Bereich, gespeichert und mit einem Passwort geschützt. Wie schon gesagt, bei einem klugen Passwort ist es unmöglich, dieses herauszuarbeiten und die Dateien zu öffnen. Gelingt es uns, den Strafverfolgungsbehörden, nicht, die Passwörter vor ihrer Aktivierung zu ermitteln, ist der Zugang zu den Daten unmöglich. Im Übrigen führt das in nicht wenigen Fällen dazu, dass wir es schaffen müssen, Täter bei geöffnetem Computer zu erreichen, was den Einsatz von Spezialeinheiten bis hin zur GSG 9 für das Bundeskriminalamt erfordert, um auf einen Schlag in eine Wohnung eindringen zu können, um Täter daran zu hindern, mit sehr kreativen Mitteln – ein RFID-Chip im Armband, eingenäht in die Kleidung, durch eine Türsonde gehen, einfach den Rechner zuklappen und er verschlüsselt sich dann – den Strafverfolgungsbehörden den Zugang zu den Daten zu verwehren.

Wir, das BKA, sehen in der Formulierungshilfe der Bundesregierung und den vorgeschlagenen Regelungen zur sogenannten Quellen-TKÜ und zur Online-Durchsuchung die Absicht, die Ermittlungsfähigkeit der Strafverfolgungsbehörden gegenüber den genannten Gegebenheiten herzustellen – nicht wieder herzustellen, erstmals herzustellen – und begrüßen diese ausdrücklich. Für uns ist ersichtlich, dass nur so die Erkenntnisgewinnung und Beweisführung im strafrechtlichen Ermittlungsverfahren zu den Tatverdächtigen bzw. Beschuldigten, deren Tatanteilen zur Steuerung von kriminellen und terroristischen Netzwerken, den Planungen und Abläufen sowie im kommerziellen kriminellen Bereich zum Verbleib und zur Verwertung der Beute wirkungsvoll verbessert werden kann. Vielen Dank.

Die **Vorsitzende**: Ich danke Ihnen, Herr Henzler. Dann hat jetzt Herr Huber das Wort.

SV **Alfred Huber**: Frau Vorsitzende, meine Damen und Herren, besten Dank. Ich kann mich vergleichsweise kurz fassen, was das sogenannte Going Dark betrifft. Meine beiden Vorredner haben das bereits ausführlich dargestellt. Es ist tatsächlich so, dass wir immer weniger Erkenntnisse über die klassische TKÜ bekommen. Das erscheint mir auch absolut nachvollziehbar, logisch und eigentlich für jedermann leicht erkennbar. Wenn ich eine Möglichkeit habe, zu kommunizieren ohne überwacht zu werden, dann werde ich selbstverständlich diese Möglichkeit nutzen, wenn ich dabei beabsichtige, eine Straftat zu begehen. Das geht heutzutage immer leichter, ich brauche kein Technik-Freak zu sein, das kann

sich jeder Straftäter in kürzester Zeit beibringen. Die Frage ist jetzt: Spielt es vielleicht gar keine Rolle, haben wir andere Möglichkeiten, unsere Informationen über die Straftäter zu bekommen? Wenn wir Glück haben, sicherlich. Sie müssen sich das aus meiner Sicht so vorstellen: Die TKÜ ist ein ganz, ganz wichtiges Werkzeug im Rahmen der Strafverfolgung. Dieses Werkzeug müssen wir benutzen. Das können wir zurzeit aber nicht benutzen, weil es nicht mehr passt. Der Schlüssel passt nicht mehr. Wir kommen nicht rein, weil wir eine unverschlüsselte Telekommunikation in dem Maß, wie wir es zur Strafverfolgung bräuchten, nicht mehr haben. Sie müssen uns als Gesetzgeber jetzt diesen Schlüssel zur Verfügung stellen, dieses neue Werkzeug geben, damit wir wieder auf Augenhöhe mit den Straftätern agieren können – dass die keinen Vorsprung bekommen. Es ist auch nicht so, dass es mir als Strafverfolger in irgendeiner Weise etwas bringt, wenn ich vielleicht ein Vierteljahr, ein halbes Jahr später bei einem Zugriff Zugang habe zu diesen WhatsApp-Nachrichten und erkenne, dass hier eine Bande von drei Personen, die Wohnungseinbruchdiebstahltaten begeht, in dem letzten Vierteljahr oder in den letzten zwei Wochen – je nachdem, wie das Ganze von denen gehandhabt wird – bereits fünf Taten begangen hätte. Hätte ich diesen Zugriff gehabt auf die verschlüsselte Telekommunikation, dann hätte ich als Staatsanwalt, in Zusammenarbeit mit der Polizei, möglicherweise bei der zweiten oder dritten geplanten Tat bereits zugreifen und die Täter stellen können. Das bedeutet, es geht hier nicht nur um Strafverfolgung, es geht hier ganz klar auch um die Frage der inneren Sicherheit. Es geht hier ganz klar auch darum, dass wir sagen: Wir müssen die Täter möglichst bald fassen. Das ist ja unser Problem. Aus dem Grund führt an der Quellen-TKÜ kein Weg vorbei. Man kann – das möchte ich ganz kurz fassen – jetzt die Auffassung vertreten – das wird in der Rechtsprechung und Literatur ja unterschiedlich behandelt –, wir hätten schon eine gesetzliche Grundlage. Wenn Sie sich die Entscheidung des Bundesverfassungsgerichts zum Bundeskriminalamtsgesetz anschauen, dann ist es so, dass das Bundesverfassungsgericht hier ganz wesentlich darauf abgestellt hat, dass die technische Umsetzung der Quellen-TKÜ im Gesetz geregelt ist. Das BKA-Gesetz ist insoweit verfassungsgemäß, und der jetzige Vorschlag will das eins zu eins übernehmen. Ich denke aus dem Grund, dass Sie verpflichtet sind, wenn Sie uns diese Maßnahme zur Verfügung stellen wollen – wofür ich werben möchte –, auch eine entsprechende gesetzliche Regelung zu erlassen.

Bei der Online-Durchsuchung sieht die Sache aus meiner Sicht insoweit etwas anders aus, als wir die TKÜ sicherlich wesentlich häufiger einsetzen werden als die Online-Durchsuchung. Ich kann der Ausführung des Kollegen Buermeyer hier nicht zustimmen, dass eine Online-Durchsuchung ein wesentlich größerer Eingriff wäre als ein großer Lauschangriff. Das Verfassungsgericht hat ganz klar gesagt: Diese beiden Eingriffe sind vergleichbar – Entscheidung zum BKA-Gesetz –, und die jetzige Umsetzung dieser Entscheidung durch den vorliegenden Gesetzentwurf – der setzt genau das um. Wir haben einen Eingriff nur, wenn auch eine Wohnraumüberwachung zulässig wäre. Aus meiner Sicht ist die Wohnraumüberwachung hier ein weitergehender Eingriff, aber das möchte ich jetzt nicht detailliert darlegen – möglicherweise dann bei Nachfragen.

Die Frage ist: Was haben wir? Wir haben einen engen Straftatenkatalog, wir haben eine zusätzliche Einzelfallprüfung, dass eine besonders schwere Straftat vorliegt, und das muss auch einzelfallbezogen vom Gericht begründet werden. Es gibt zwei Punkte, über die man aus meiner Sicht diskutieren kann – wobei ich gleich dazu sagen muss: Mein Herz als Staatsanwalt hängt nur ganz bedingt daran. Man kann sich die Frage stellen, warum man zu einer Kammer des Landgerichts muss, wenn man die Online-Durchsuchung im Bereich der Gefahrenabwehr bei einem Richter vom Amtsgericht bekommen kann, abgesegnet vom Bundesverfassungsgericht; und man kann sich die Frage stellen, weshalb man die Online-Durchsuchung im StPO-Bereich zunächst nur für einen Monat bekommen soll, mit Verlängerung, während man im BKA-Gesetz eine dreimonatige Frist eingeführt hat. Da hat aber sicherlich Vorrang, dass das Gesetz überhaupt kommt. An der Frage, ob hier irgendwelche Feinheiten zugunsten der Strafverfolgungsbehörden noch berücksichtigt werden können hängt mein Herz erst in zweiter Linie. Wir werden mit Sicherheit keine Überwachung haben im Bereich der allgemeinen Kriminalität, wir

werden auch keine flächendeckende Überwachung haben. Es wurde zum Teil ein bisschen so dargestellt, als würde der Polizeibeamte, der einen Fahrraddiebstahl ermittelt, erstmal die Computer sämtlicher Tatverdächtiger hacken – das ist alles in das Reich der Fantasie zu verweisen. Wir haben ganz enge Vorgaben, die das Bundesverfassungsgericht hinsichtlich des BKA-Gesetzes gemacht hat, und ich möchte Sie bitten, dass Sie uns diese beiden Ermittlungsmöglichkeiten auch im StPO-Bereich geben. Besten Dank.

Die **Vorsitzende**: Danke, Herr Huber. Jetzt hat Herr Dr. Krauß das Wort.

SV **Dr. Matthias Krauß**: Vielen Dank. Sehr geehrte Frau Vorsitzende, sehr geehrte Damen und Herren Abgeordnete, ich halte die vorgeschlagenen Regelungen für die Quellen-TKÜ und die Online-Durchsuchung für sachgerecht und praktikabel, und ich habe auch keine grundlegenden verfassungsrechtlichen Bedenken. Sie sind die notwendige Antwort auf die rasante Entwicklung der Kommunikationstechnologien in den letzten Jahren, die dadurch gekennzeichnet ist, dass elektronische und digitale Kommunikationsmittel vermehrt genutzt werden und in alle Lebensbereiche vordringen und die damit einhergehende Verschlüsselungstechnik die Strafverfolgungsbehörden vor enorme Probleme stellt.

Zur Quellen-TKÜ: § 100a StPO läuft weitgehend ins Leere. Ich kann mich nur meinen Vorrednern anschließen. Ich kann auch bestätigen, dass ganz bewusst Verschlüsselungstechnologie von den Beschuldigten zur Verschleierung eingesetzt wird. Dies lässt sich in den überwachten Gesprächen immer wieder hören. Die TKÜ ist aber zumindest in den Fällen, wo es um Organisationsstrukturen geht, wo es um das arbeitsteiliges Zusammenwirken geht, ein ganz maßgebliches Ermittlungsinstrument. Wenn man sich vielleicht die letzten fünfzig Urteile im Staatsschutzbereich, aus dem ich komme, ansieht, sieht man, dass die Telekommunikationsüberwachung ein ganz wesentliches, oft sogar das einzige Beweismittel ist, auf das die Verurteilungen gestützt werden. Dieses Ermittlungsinstrument droht über kurz oder lang vollständig auszufallen. Es geht, um mit Herrn Buermeyer zu sprechen, tatsächlich ums Ganze. Wie kann man gegensteuern? Wie kann man das, was bisher möglich war, wieder möglich machen? Wie kann man den früheren Ermittlungszustand, die früheren Ermittlungsmöglichkeiten wieder herstellen? Darum geht es. Das geht nur, indem man die Kommunikation an der Quelle anzapft. Mildere Mittel vermag ich nicht zu erkennen. Als milderes Mittel kommt allenfalls eine Zusammenarbeit bzw. eine Verpflichtung der Instant-Messenger-Betreiber oder Provider in Betracht. Das scheint mir kein praktikabler Weg zu sein. Zum einen werben diese doch gerade damit, dass keinerlei Entschlüsselung möglich ist und dass sie vor den Strafverfolgungsbehörden sicher sind. Zum anderen sitzen die meisten dieser Provider im Ausland, so dass eine deutsche Regelung ins Leere laufen würde. Ich kann mich gut an einen Fall vor wenigen Wochen erinnern, wo wir versucht haben, Telegram einen Beschluss des Ermittlungsrichters des Bundesgerichtshofes zuzustellen. Trotz größter Bemühungen lief das ins Leere, weil einfach keine Adresse ausfindig zu machen war, weder im Netz noch in sonstigen Unterlagen. Also, eine Zusammenarbeit mit den Providern halte ich für keinen geeigneten Weg.

Zwei weitere Überlegungen. Es ist zutreffend angeführt worden, dass §100a StPO als Rechtsgrundlage für die Quellen-TKÜ umstritten ist und bislang nicht herangezogen wird. Ich habe aber die große Befürchtung, wenn nicht bald eine gesetzliche Regelung kommt, dass der Handlungsdruck in bestimmten Phänomenbereichen derart steigt, dass die Quellen-TKÜ auf der Grundlage des § 100a StPO vorgenommen wird. Das führt aber dann zu weniger Rechtssicherheit, zu weniger Rechtsklarheit und weniger Rechtsschutz. Eine zweite Überlegung: In vielen Fällen ist es so, dass Ermittlungen schon im Gefahrenabwehrbereich vorgenommen werden, auf polizeirechtlicher Grundlage. Das Polizeirecht kennt aber die Online-Durchsuchung und die Quellen-TKÜ. Werden dort Ermittlungsergebnisse erzielt – zum Beispiel, dass drei Beschuldigte planen, einen Terroranschlag in Berlin zu begehen –, dürfen diese Erkenntnisse gemäß § 160a Absatz 2 StPO – hypothetischer rechtmäßiger Ersatzeingriff – nicht im Ermittlungsverfahren verwendet werden. Ich kann also keinen Haftbefehl deswegen erwirken. Dieses im Grunde genommen unsinnige Ergebnis kann nur dadurch beseitigt werden, dass man wieder einen

gewissen Gleichlauf zwischen präventiv-polizeilichen Maßnahmen und strafprozessualen Ermittlungsmaßnahmen herstellt und die Quellen-TKÜ und die Online-Durchsuchung einführt.

Zu zwei Punkten vielleicht noch eine kurze Anmerkung. Zur Quellen-TKÜ: Da erscheint mir ein Punkt diskussionswürdig, der § 100a Absatz 2 Satz 3 StPO, weil dort geregelt wird, dass auch schon gespeicherte Telekommunikation mittels der Quellen-TKÜ ausgeleitet werden darf. Das ist im Grunde genommen ein Systembruch, weil das Bundesverfassungsgericht ja sagt: Soweit es um gespeicherte Kommunikation geht, ist nicht mehr Artikel 10 maßgeblich, sondern das Computergrundrecht in Artikel 1 in Verbindung mit Artikel 2 des Grundgesetzes. Hier sieht das Gesetz eine Ausnahme vor, die natürlich dann entsprechend begründet werden muss – es muss ein triftiger sachlicher Grund vorliegen. Der ist meines Erachtens hier gegeben, weil das auf ein sehr enges Zeitfenster beschränkt ist, nämlich auf die Kommunikation, die nach Anordnung des Beschlusses gespeichert werden. Und es geht ausschließlich um Kommunikation und nicht um einen Zugriff auf das gesamte Computersystem, wie es die Online-Durchsuchung zulässt. Deswegen ist meines Erachtens ein sachlicher Grund gegeben, der diese Regelung verfassungsrechtlich tragfähig erscheinen lässt.

Einen zweiten Punkt möchte ich noch ansprechen, weil er schon thematisiert worden ist. Das ist der Straftatenkatalog, also die Anlasstaten, der Online-Durchsuchung. Da teile ich die Auffassung meines Vorredners, dass es dem Gesetzgeber frei steht und verfassungsrechtlich unbedenklich ist, hier auf den Straftatenkatalog der Wohnraumüberwachung zuzugreifen. Das Bundesverfassungsgericht hat in der Tat in mehreren Entscheidungen betont, dass die Eingriffsmaßnahmen Online-Durchsuchung und Wohnraumüberwachung vergleichbar sind. Die Wohnraumüberwachung ist zulässig bei besonders schweren Straftaten, und deswegen erscheint es mir sehr wohl zulässig, auf diesen Straftatenkatalog auch bei der Online-Durchsuchung zurückzugreifen.

Insgesamt begrüße ich deswegen die vorgeschlagenen Maßnahmen. Vielen Dank.

Die **Vorsitzende**: Danke, Herr Dr. Krauß. Dann hat Herr Neumann das Wort.

SV **Linus Neumann**: Vielen herzlichen Dank für die Einladung und die Gelegenheit, hier neben ein paar Strafverfolgern die Seite der Praxis zu zeigen. Ich bin beruflich in der IT-Sicherheit tätig, das heißt, ich mache als Praktiker jeden Tag Online-Durchsuchungen und Quellen-TKÜ, unterliege damit dem Hacker-Paragraphen, mache das also im Auftrag für Unternehmen. Und wenn ich da Sicherheitslücken finde, dann habe ich eigentlich in vielen Jahren beruflicher Praxis immer nur eine Sache damit anzufangen gewusst, und das war, die zu melden und dafür zu sorgen, dass die beseitigt werden, weil eine Sicherheitslücke immer für alle betroffenen Systeme eine Gefahr ist. Und diese Sicherheitslücke nicht nur den Strafverfolgungsbehörden, sondern auch jedem anderen zum Ausnutzen zur Verfügung steht – also auch Leuten wie mir, oder meinen Konkurrenten, die es mit dem Gesetz vielleicht nicht ganz so ernst meinen. Warum ist das so wichtig? Herr Buermeyer hat das gerade schon angesprochen: Das, worum es in diesem Gesetz oder in dieser freundlichen Formulierungshilfe der Bundesregierung geht, ist ja immer eine Infektion. Es ist aber niemals davon die Rede, wie diese Infektion angebracht wird. Sie können diese Geräte nicht infizieren, ohne dass es eine Schwachstelle gibt. Die ist eine zwingende Voraussetzung für das, was hier geplant wird. Sie müssen also Ihren Staatstrojaner, sei es nun eine Online-Durchsuchung oder eine Quellen-TKÜ, so an dem System anbringen, dass es die betroffene Person nicht merkt. Dafür brauchen Sie eine Schwachstelle, und diese Schwachstelle brauchen Sie auf allen Geräten. Sie können ja nicht sagen: Wir patchen jetzt alle Geräte, außer die von den Kriminellen. Insofern nehmen Sie immer in Kauf, mit jeder einzelnen Schwachstelle, die Sie geheim halten, dass alle Geräte dieses Typs oder alle Software-Pakete dieses Typs diese Schwachstelle aufweisen, mit den entsprechenden Konsequenzen für die Allgemeinheit. Das ist nicht nur die deutsche Allgemeinheit, das ist die internationale Allgemeinheit. Und beim Datum dieser Formulierungshilfe, 15.5., musste ich doch ein bisschen schmunzeln, denn am 12.5. hatten wir die WannaCry-Attacken, die in Großbritannien Krankenhäuser lahmgelegt und die Deutsche Bahn über mehrere Tage in ein Notfallprogramm gebracht haben. Die konnten ihre Züge noch fahren, aber mussten die wieder

auf Kreidetafeln anzeigen. Und was da passiert ist, ist, dass der Geheimdienst NSA auf eine Sicherheitslücke, die geheim gehalten wurde, nicht aufgepasst hat. Und zwar haben sie die seit mindestens fünf Jahren. Das, was wir hier mit WannaCry gesehen haben, ist zwei Monate, nachdem diese Sicherheitslücke gepatcht wurde, passiert. Die wurde gepatcht, dann wurde sie veröffentlicht und nochmal einen Monat später wurde sie …

Die **Vorsitzende**: Könnten Sie für das Protokoll „gepatcht“ erklären?

SV **Linus Neumann**: Ja, „Beseitigung“. Sie haben eine Schwachstelle auf einem System, dann wird die bekannt und dann beseitigt der Hersteller die. Das ist der natürliche, hoffentlich natürliche Lauf der Dinge, wenn Sie das auch in Zukunft so zulassen wollen.

Was wir also mit WannaCry sehen – was ja immerhin noch der übelste Hacking-Angriff ist, den wir in den letzten Jahren oder überhaupt jemals begutachtet haben –, war nur ein Bruchteil des Risikos, das der Geheimdienst NSA wissentlich und willentlich eingegangen ist, und zwar jeden einzelnen Tag dieser fünf Jahre. Warum ist der Geheimdienst dieses Risiko eingegangen? An jedem einzelnen Tag hätte ja jemand anderes diese Sicherheitslücke finden können, und genau dann bricht die Hölle los. Und wir stehen alle daneben und können uns freuen, dass wir im Namen der inneren Sicherheit eine Sicherheitslücke in allen verfügbaren IT-Systemen weltweit zurückgelassen haben. Da würde ich, ohne dass ich – ich bin der einzige Nichtjurist, der hier geladen ist – da würde ich dann doch schon von Teilschuld sprechen oder zumindest von Verantwortung. Gleichzeitig erhöht jeder Einsatz von so einer Schadsoftware das Entdeckungsrisiko. Je öfter Sie das machen, desto wahrscheinlicher ist es, dass irgendein Viren-Scanner – oder dass Sie einmal an jemanden geraten, der klüger als Sie ist und erkennt, welche Schwachstelle Sie ausnutzen. Insofern ist es nochmal eine Erschwerung des Risikos für die innere Sicherheit, wenn man sagt: Wir machen das jetzt einfach mal für die komplette Breite der StPO, und das ist unabhängig davon – alles was ich hier über Sicherheitslücken sage, ist völlig unabhängig davon, ob ich eine Quellen-TKÜ oder eine Online-Durchsuchung mache.

Quellen-TKÜ ist sowieso ein interessanter Begriff. Wir reden ja hier davon – bzw. ich ja nicht, aber die Kollegen –, es gibt ja die TKÜ, die Ermächtigung, ein Telefonkabel abzuhören und zu sehen, was darüber gesprochen wird. Die soll jetzt ausgeweitet werden, und wir gehen alle – die Kollegen gehen alle wie selbstverständlich davon aus, dass es quasi das Gleiche ist – wir wollen ja nur den Messenger auf diesem Telefon abhören oder nur das Skype oder nur das Telegram. Herr Krauß hatte da ja schon mehrere Empfehlungen gegeben, welche Apps Sie da in Zukunft nutzen könnten. Das ist technisch einfach nicht möglich. Wir reden bei Computern von universell programmierbaren Geräten. Die sind nicht wie ein Telefon, an dem ein Mikrofon dran ist und ein Kabel, und dann ist da ein kleiner Verstärker, und dann ist fertig. Das haben wir heute nicht mehr. Wir haben Computer, die universell nicht nur alles in Ihrer Hosentasche tun, sondern auch all das tun könnten, was Sie nicht sehen. Diese Geräte sind nicht so etwas wie Single-Purpose, dass man sagen könnte: Ok, wir hören jetzt Telegram ab und bauen dafür einen spezifischen Trojaner. Aus diesem Grund war ja auch der Staatstrojaner, den Vertreter des Chaos Computer Clubs 2011 in der freien Wildbahn entdeckt und analysiert haben, direkt auf mehreren Wegen verfassungswidrig, weil er genau nicht die Grenzen der Quellen-TKÜ eingehalten hat und auch nicht einhalten konnte. Und als einziger technisch Bewanderter hier – auch wenn ich da gleich natürlich Widerspruch bekommen werde – werde ich Ihnen garantieren, dass das nicht anders geht. Sie können nicht ein System in seiner Integrität schwächen und garantieren, dass Sie nur und ausschließlich bestimmte Applikationen angreifen. Das leuchtet schon ein, wenn wir uns anschauen, von welcher Fülle von Applikationen hier immer wieder die Rede ist. Also, die Argumente kommen von den Kollegen hier.

Als letztes würde ich noch gerne kurz anmerken, welches Spiel hier gespielt wird. Und weil hier so ein paar kleine rhetorische Tricks zur Anwendung gekommen sind, will ich Sie gerne kurz darauf hinweisen. Und zwar geht es dabei um das Phänomen des „Going Dark“. Herr Krauß hat ja gesagt: Wir hören in der TKÜ immer wieder, das zieht ja so ein Verschlüsseln – da nickt er nochmal! Dann frage ich mich, was das für ein „Going Dark“ sein soll, wenn ich die Leute doch

eh schon abhöre? „Going Dark“ würde doch bedeuten, dass Sie keine Anhaltspunkte haben, um diese Kriminellen zu fassen. Ich frage mich, wie Sie dann darauf gekommen sind, bei denen eine TKÜ durchzuführen. Dieses Phänomen – das widerlegen Sie selber. Herr Greven, dessen Statement Sie gerade verlesen haben, der sagt, dass er in der äußeren Sicherheit tätig ist, spricht von 0,12 Prozent der Verfahren. Dann frage ich mich ja, wieso dann 100 Prozent der Rechner weltweit mit Sicherheitslücken versehen werden sollen, damit Sie in so wenigen Fällen diese Eingriffe machen können. Und wenn es doch nur um organisierte Kriminalität und äußere Sicherheit geht, warum bleiben wir dann nicht bei den Regelungen, die wir seit 2008 in diesem Lande haben, die genau diese Verfahren für genau die Beispiele, die hier die ganze Zeit genannt werden, längst legalisiert haben, nämlich für die innere Sicherheit. Insofern finde ich wirklich, dass das ziemlich unlautere Beispiele sind, mit denen hier darüber gesprochen wird, nicht mehr und nicht weniger zu tun, als erstens Sicherheitslücken geheim zu halten und zweitens es zu legalisieren für den gesamten Katalog der StPO, informationstechnische Systeme zu hacken.

Vielen Dank, dass Sie so viel Geduld hatten mit mir.

Die **Vorsitzende**: Heute scheinen zwei Minuten Überziehung angesichts des Themas notwendig zu sein. Jetzt hat Herr Professor Dr. Sinn als letzter in der Runde das Wort, und wir nehmen auch Wortmeldungen entgegen. Bitte.

SV **Prof. Dr. Arndt Sinn**: Frau Vorsitzende, meine sehr verehrten Damen und Herren Abgeordnete, meine sehr geehrten Damen und Herren. Herzlichen Dank, dass ich heute hier zu diesem sehr brisanten Thema, das in den letzten zehn Jahren auch in der Wissenschaft stark diskutiert wurde, Stellung nehmen darf. Es ist ein Privileg.

Ich darf kurz die Struktur des Änderungsvorschlags noch einmal rekapitulieren. Drei Maßnahmen werden geregelt: erstens die Quellen-Telekommunikationsüberwachung in § 100a StPO – Grundrechtsschutz nach Artikel 10 GG –, zweitens die kleine Online-Durchsuchung in Satz 3, auch zu messen an Artikel 10 GG, drittens die große Online-Durchsuchung in einer neu zu schaffenden Ermächtigungsgrundlage § 100b StPO. Das ist richtig, das ist folgerichtig, das ist Ausfluss des Volkzählungsurteils. Spezielle Grundrechtseingriffe müssen spezielle Ermächtigungsgrundlagen haben. Deshalb war es falsch, bleibt es falsch, eine Quellen-TKÜ an dem alten § 100a StPO zu messen, deshalb musste es so kommen.

Deshalb ist auch eine Generalermächtigung nicht möglich, weil man die Zweckbestimmung, die mit einer Erhebung mittels einer Software, mit dem aufzuspielenden Spähprogramm – Sie können das Smart-Auto zum Anhalten bringen, Sie können es auch in die Luft sprengen, Sie können ganz viele Dinge machen – wenn Sie das nicht in einer Ermächtigungsgrundlage beschreiben, kann es keine Generalermächtigung geben, weil das auch dem verfassungsrechtlichen Grundsatz der Normenklarheit und Normenbestimmtheit widersprechen würde.

Die technischen Probleme, von denen wir gehört haben, sind aus rechtlicher Sicht natürlich ernst zu nehmen. Das Recht ist auch von Missbrauch freizuhalten. Auch Ermächtigungsgrundlagen und der tatsächliche Umgang mit diesen sind von Missbrauch, insbesondere mit Schadsoftware, freizuhalten. Aber das Bundesverfassungsgericht hat auch klar gemacht, dass das den Gesetzesvollzug betrifft. Es kann also durchaus Normen geben, die einen Grundrechtseingriff mit technischen Mitteln beschreiben. Die Technik gibt es noch nicht, das macht die Norm nicht verfassungswidrig. Es gibt das schöne Zitat: „Das Internet ist nur ein Hype“, deshalb mag es auch irgendwann mal möglich sein, dass es eine Software gibt, die das kann, was heute alle bezweifeln, und ich nehme das ernst, dass die Software …

Die **Vorsitzende**: Das Internet ist nur ein …?

SV **Prof. Dr. Arndt Sinn**: … Hype - das ist ein Zitat. Eine Erscheinung.

Erstens, Quellen-TKÜ, zu messen an § 100a StPO, also am Grundrecht des Artikel 10 GG. Das entspricht einer Forderung aus der Wissenschaft – Deutscher Juristentag 2012, Sieber, ein Gutachten – das ist nicht etwas, was in der Wissenschaft nicht schon diskutiert wurde, und wo es auch durchaus namhafte Vertreter gibt, die diesen Eingriffen nähertreten können. Hier spielt die Software eine Rolle, natürlich, das sieht so

aus, als sei das dann der Eingriff in die Integrität und Vertraulichkeit informationstechnischer Systeme. Aber sie stellt sich dann doch wieder als Begleiteingriff dar, weil sie ja sicherstellen soll – wenn die Software funktioniert –, dass nur die unverschlüsselte Kommunikation, also an der Quelle, ausgeleitet werden soll. Rechtstechnisch also durchaus an Artikel 10 GG zu messen, obwohl es den Eingriff in das informationstechnische System tatsächlich auch gibt. Aber ich sage heute schon: Die Integrität dieser Programme, wenn sie denn benutzt werden, wird die Rechtsprechung beschäftigen. Man wird selbstverständlich jedes Programm, das benutzt wird, anfechten, und das wird dann auch den Bundesgerichtshof beschäftigen. Das ist klar.

Ich rege eine Diskussion über den Datenaustausch mit Endgeräten an, also die Kommunikation mit sich selbst. Meine Daten sind in der Cloud, sie unterfallen dem Begriff der Telekommunikation. Das ist wohl damit nicht gemeint. Dass das nicht gemeint ist, sollte man auch klarstellen und dem Bereich der Online-Durchsuchung, § 100b StPO, zuschlagen.

Zweitens: kleine Online-Durchsuchung, Satz 3. Das ist die interessanteste Maßnahme, denn welche Fälle damit gemeint sind, lässt die Formulierungshilfe etwas im Unklaren. Meiner Meinung nach geht es um die Fälle, die zwischen der Anordnung der Quellen-TKÜ und der tatsächlichen Ausleitung der Inhalte der Quellen-TKÜ liegen. Weil da ein zeitliches Loch entsteht, denn Sie müssen die Software ja erst mal draufbringen. Inzwischen kommunizieren die Verdächtigen miteinander, und das will man quasi „einfrieren“ – ich habe das in meiner Stellungnahme so genannt. Diese Nachrichten werden eingefroren im Grundrechtsbereich von Artikel 10 GG. Das ist, sozusagen, Quasi-Kommunikation, die in den Schutzbereich von Artikel 10 GG eingefroren wird, was dazu führt, dass es eben nicht am IT-Grundrecht zu messen ist. Das könnte so sein, die Formulierungshilfe lässt es etwas offen. Ich lasse mich gerne belehren, dass es um andere Fälle gehen soll. Ich habe sie noch nicht gefunden.

Wie soll die Software nun drauf kommen? In der Tat, das ist schwierig. Wer drückt denn heute noch auf so einen Link? Der ist ja irgendwie selbst schuld. Mitwirkungspflichten der Telekommunikationsanbieter sind hier angesprochen. Die sind ja schon § 100c des Telekommunikationsgesetzes (TKG) geregelt. Die Regelung ist relativ weit. Für ausgeschlossen halte ich, dass die Telekommunikationsanbieter selbst diese Software aufspielen. Grundrechtseingriffe hat der Staat durchzuführen, nicht ein Privater. Aber selbstverständlich müssten die Telekommunikationsanbieter ihre Infrastruktur zur Verfügung stellen, damit autorisierte Personen, die als einzige mit dieser Software zu tun haben, diese Systeme dann auch aufspielen können. Das soll dann über § 100c StPO-E geregelt werden.

Dritter und letzter Punkt: die Online-Durchsuchung. Verfassungsrechtlich ist die möglich. Das Bundesverfassungsgericht hat an keiner Stelle gesagt, dass das im repressiven Bereich nicht möglich sein soll. Die Orientierung an Artikel 13 GG halte ich für folgerichtig, das sagt das Bundesverfassungsgericht auch: es ist ein in der Schwere vergleichbarer Eingriff. Es sagt nicht: schwererer Eingriff, sondern: schwerer Eingriff. Allerdings rate ich an, den Gesetzeswortlaut dahingehend zu konkretisieren, um den Missbrauch mit dieser Art von Software zu minimieren, also den Personenkreis, der Zugang hat, diese Software zu benutzen, zu limitieren und andere Sicherheitslimitierungen einzubauen. Vielen Dank.

Die **Vorsitzende**: Danke, Herr Professor Sinn. Ich habe jetzt einige Wortmeldungen: Herr Dr.Fechner, Herr Dr. Sensburg, Frau Keul, Herr Korte, Frau Winkelmeier-Becker. Herr Dr. Fechner hat zuerst das Wort.

Abg. **Dr. Johannes Fechner** (SPD): Vielen Dank zunächst Ihnen allen, herzlichen Dank für Ihre Ausführungen. Ich hätte zwei Fragen an Herrn Dr. Krauß. Und zwar würde mich interessieren, wie Sie den Gesetzesentwurf unter dem Gesichtspunkt des Schutzes von Berufsgeheimnisträgern bewerten. Und zum anderen, wir haben ja Vorgaben vom Bundesverfassungsgericht, bestimmte Maßnahmen nur bei bestimmten Straftaten, schweren Straftaten, zuzulassen – wie Sie im Hinblick auf diese Vorgaben des Bundesverfassungsgerichts hin diesen Straftatenkatalog bewerten in § 100b StPO-E.

Die **Vorsitzende**: Danke. Herr Dr. Sensburg.

Abg. **Dr. Patrick Sensburg** (CDU/CSU): Herzlichen Dank, Frau Vorsitzende. Wenn ich jetzt richtig gezählt habe, haben fünf Sach.-verständige hier die Notwendigkeit betont. Ich weiß ja nicht, ob das jetzt so polemisch werden muss, aber zumindest beim Zählen habe ich hoffentlich keinen Fehler gemacht. Bei fünf Sachverständigen war die Expertise, dass wir dieses Instrument brauchen, zwei Sachverständige haben das anders gesehen, deswegen würde ich gerne Herrn Neumann zu der technischen Seite fragen. Denn Jurist, haben Sie gesagt, sind Sie nicht, das können Sie nicht beurteilen, aber die Frage, wie das technisch funktioniert. Das würde mich interessieren, ob Sie das beurteilen können? Haben Sie mal so eine Quellen-TKÜ gesehen, kennen Sie Software oder Hardware, wie das funktioniert, oder haben Sie sich vielleicht mit dem Bundestrojaner beschäftigt? Der Chaos Computer Club hat sich ja sehr intensiv damit beschäftigt. Vielleicht wissen Sie, wie damals die Vorgehensweisen waren, wie das drauf gekommen ist. Sie haben unheimlich viel von Sicherheitslücken, Back Doors und anderen Dingen erzählt. Können Sie mal genau beschreiben, wie das technisch so Schritt für Schritt funktioniert auf dem Gerät, wie das drauf gespielt wird? Das müssten Sie ja wissen. Ich weiß, wie das funktioniert, ich habe das selbst gesehen, von daher kann ich das beurteilen, habe auch damals dazu geredet. Der Chaos Computer Club hat damals auch eine Äußerung dazu abgegeben. Das könnten Sie mir nochmal detailliert darlegen als Fachmann.

Die **Vorsitzende**: Frau Keul und dann Herr Korte.

Abg. **Katja Keul** (BÜNDNIS 90/DIE GRÜNEN): Zunächst einmal vielen Dank für Ihre Statements. Es ist für mich durchaus so, dass Ihre Antworten, auch Fragen, noch etwas Neues sind und ich jetzt nicht nur Fragen stelle, zu denen ich die Antworten schon kenne – das will ich gleich von vornherein sagen. In der Tat haben wir ja jetzt von vier Ermittlern gehört, dass sie dieses neue Werkzeug gerne haben würden. Ich glaube, es steht außer Frage, dass man immer gerne, wenn man auf der einen Seite arbeitet, ein Werkzeug hat, das die Arbeit intensiver macht. Aber unsere Aufgabe ist es ja, hier insgesamt die Verhältnismäßigkeit abzuwägen, den Nutzen mit den Risiken, und deswegen habe ich da durchaus auch noch einige Fragen.

Ich fange mal an mit Herrn Dr. Buermeyer. Ich kann zwei Fragen stellen. Die erste wäre nochmal zum besseren Verständnis: Wir haben hier ja zwei Rechtsgrundlagen für zwei verschiedene Instrumente, die auch nach unterschiedlichen Maßstäben gemessen werden müssen. Ich habe noch nicht ganz verstanden, ob und wie man das in der Praxis überhaupt voneinander unterscheiden kann. Vielleicht können Sie dazu nochmal was sagen? Woran erkenne ich denn bei dem Trojaner, ob der nur Quellen-TKÜ kann, ob der Kommunikation kann, oder ob der auch Mikrofone manipuliert – ist das überhaupt abgrenzbar? Vielleicht können Sie das noch etwas aufhellen.

Dann haben wir einiges gehört zu der Frage: Wie kommt diese Software auf das Gerät drauf, in die Software rein. Aber ich habe noch nicht gehört, wie kommt es eigentlich wieder runter? Vielleicht können Sie etwas dazu sagen. Ist es dann einfach so, dass ich irgendwo auf einen Knopf drücke und dann ist diese Software abgeschaltet, oder kann das auch passieren, dass die vielleicht nicht ganz sauber beseitigt wird und dann vielleicht noch länger rumwabert als geplant? Wie muss ich mir das vorstellen, wie kommt der Trojaner da wieder weg, wie schalte ich den ab?

Die **Vorsitzende**: Danke. Dann hat jetzt Herr Korte Fragen.

Abg. **Jan Korte** (DIE LINKE.): Kurz zur Aufklärung: Was der Kollege Dr. Sensburg gesagt hat – warum jetzt eine Mehrheit der Sachverständigen überraschenderweise für die Vorschläge ist, hat damit zu tun, dass die CDU/CSU und SPD natürlich die Sachverständigen ausgesucht haben, die sagen, dass das total richtig ist, was sie machen. Also mal hier für die interessierte Öffentlichkeit. Ich will zum zweiten sagen …

Die **Vorsitzende**: Also, jeder sucht sich seine Sachverständigen aus, und ich habe schon viel erlebt, aber noch nicht, dass man gezielt das Gegenteil aussucht.

Abg. **Jan Korte** (DIE LINKE.): Zur zweiten Anmerkung, die ich machen möchte, um das einzuordnen. Meine Frage: Wir haben ja bei

alldem, was hier so vorgelegt wird – Herr Henzler, wir kennen uns ja auch aus dem Innenausschuss – man hört ja immer, ob Vorratsdatenspeicherung damals, Online-Durchsuchung jetzt – das ist ja immer dasselbe, man bekommt den Eindruck, wenn ich Sie höre, dass wir hier in einem Kriminellen-Paradies leben, und dass Sie dort völlig wehrlos sitzen und überhaupt nicht wissen, wie man dem Herr werden soll. Und wenn ich den Fall „Amri“ so sehe – da fragt man sich ja auch, ob man nicht vielleicht einfach zu viele Daten hatte und vielleicht die Behörden das gar nicht richtig alles einordnen konnten. Wie dem auch sei.

Und die zweite Sache, und damit komme ich auch zu der Frage – das, was wir heute verhandeln, das ist ja nicht Pillepalle, sondern das sind ja wirklich extreme Eingriffe, die gemacht werden. Das Verfahren, das mal nebenbei über Änderungsanträge zu machen, das habe ich in zwölf Jahren auch noch nicht erlebt. Das finde ich übrigens auch der Sache nicht angemessen. Und daher meine Frage, zuerst an Herrn Neumann: Sie haben das eben ja schon eingangs gesagt – ich bin da nicht der IT-Experte, ob Sie das nochmal beschreiben können – vielleicht kann es ja auch Herr Dr. Sensburg, der weiß das bestimmt schon –, warum es für die deutschen Behörden nicht möglich ist, wenn sie diese Befugnisse bekommen, die hier gewünscht sind, dass sie die aufgezeigten Sicherheitslücken für sich behalten. Das würde mich zum einen interessieren.

Und zum zweiten: In Ihrer Stellungnahme haben Sie geschrieben, dass die Quellen-TKÜ, so wie sie hier vorgesehen und angeblich eingegrenzt ist, ein rein theoretisches Konstrukt ist und real so nicht handhabbar ist. Vielleicht können Sie das auch nochmal ausführen?

Die **Vorsitzende**: Danke sehr. Jetzt hat Frau Winkelmeier-Becker in dieser Runde noch das Wort. Dann beginnen wir mit Professor Sinn in der Antwortrunde, soweit jemand Fragen hatte. Bitte.

Abg. **Elisabeth Winkelmeier-Becker** (CDU/CSU): Ich möchte gerne Herrn Henzler nochmal die Möglichkeit geben, auf die ungewollten Nebenwirkungen, die Herr Neumann geschildet hat, einzugehen – also die Gefährdungen, die damit verbunden sind, dass ein Trojaner eingesetzt wird oder eine Sicherheitslücke eingesetzt wird, die ja dann auch von anderen genutzt werden kann, wenn ich das richtig verstanden habe. Wie Sie das einschätzen, diese Gefahr? Und ob der begegnet werden kann oder ob dieses Risiko es wert ist, wenn man auf der anderen Seite steht?

Und ich hätte eine Frage an Herrn Huber: Sie sprachen gerade von Fällen, sogar im einstelligen Bereich, bei anderen vergleichbar gravierenden Maßnahmen, und dass es eben auch etwa in der Größenordnung bleiben würde. Könnten Sie das vielleicht nochmal unterstreichen dadurch, dass Sie nochmal schildern, um welche Fälle es in der Vergangenheit gegangen ist, wo man diesen Aufwand betrieben hat, wie hoch dieser Aufwand überhaupt ist, was alles getan werden muss. Also, um welche Fälle es da geht, ganz konkret. Aber auch Wohnraumüberwachung in der Vergangenheit – in welcher Kategorie sich das abspielt, dass man diesen Aufwand betreibt. Wir würden Ihnen ja, wenn wir das verabschieden, schon einen Vertrauensvorschuss mitgeben, den Ermittlungsbehörden, den staatlichen Behörden, und da möchte ich einfach nochmal hören, wie ist mit vergleichbaren Befugnissen in der Vergangenheit umgegangen worden, damit ich das einschätzen und daran die Hoffnung anknüpfen kann, dass das dann in Zukunft genauso verantwortungsvoll geht. Danke.

Die **Vorsitzende**: Danke. Wir kommen zu der ersten Antwortrunde. Ich habe gesagt, jetzt fangen wir rückwärts mit Herrn Professor Sinn an, der aber prompt in der Runde gar keine Frage hatte. Wir müssen also verzichten. Kommen wir jetzt zu Herrn Neumann und der spannenden Fortbildung auf die Frage von Herrn Dr. Sensburg, der die Antwort aber schon kennt. Er will wahrscheinlich, dass wir sie kennen. Und Herr Korte hatte zwei Fragen.

SV **Linus Neumann**: Ich werde die erste Frage von Herrn Korte zusammen mit der von Herrn Sensburg beantworten. Und zwar war das ja einmal die Frage: Wie funktioniert denn so eine Quellen-TKÜ – einmal von vorne bis hinten durchsprechen, und dann die Frage: Warum gelingt es dann nicht, einen Zugriff in irgendeiner Form exklusiv zu haben – also das Geheimhalten von Sicherheitslücken.

Sie können sich eine Quellen-TKÜ primär erstmal vorstellen wie ein Programm, das auf Ihrem Zielsystem in irgendeiner Form installiert wird. Es ist auf jeden Fall eine Software, die auf Ihrem Gerät ausgeführt wird. Üblicherweise, wenn Sie jetzt einen Computer oder Telefon vor sich haben, ist die Installation von Software ja ein Vorgang, den Sie erstens willentlich anstoßen müssen und zweitens, wo Sie in der Regel nach Ihrem Passwort gefragt werden. Nun gibt es unterschiedliche Möglichkeiten, eine solche Infektion anzubringen. Es gibt einmal die Idee, das lokal zu machen – das heißt, man hat vielleicht einen Zugriff auf das Gerät. Man sagt, wir müssen das mal kurz dem Sprengstofftest am Flughafen unterziehen oder so, und schafft es, das Gerät eine kurze Zeit außerhalb des Einblicks der Zielperson zu haben. Das ist natürlich eine etwas unschöne Methode, weil ein Verbrecher, der einmal seinen Rechner in den Händen der Zollpolizei oder so hatte, sich danach wahrscheinlich ein bisschen unwohl fühlt. Insofern wird man eher eine Möglichkeit suchen, das ganze „remote“ durchzuführen, also aus der Ferne, und dann natürlich möglichst so, dass keine weitere Nutzerinteraktion notwendig ist. Was häufig zum Einsatz kommt – das wurde ja nach meinen Informationen in diesem Hause auch schon festgestellt –, ist, dass man einen E-Mail-Anhang schickt, der dann geöffnet wird und eine Software installiert, und diese Software ist dann eben auf dem Zielsystem vorhanden. Was da in Wirklichkeit passiert, ist natürlich, dass eine Schwachstelle – in diesem Fall wäre das so ein Dokumentenleser, was weiß ich, Microsoft Word oder Adobe Acrobat Reader, der eine Schwachstelle hat, die es den Angreifern ermöglicht, aus dem Kontext des Programmes herauszukommen, auf der Ebene des Systems Code auszuführen und dann eine Installation durchzuführen. Das mit der Installation ist aber ein Problem, weil die Betriebssysteme dagegen – mehr schlecht als recht, aber immerhin – geschützt sind, dass eine persistente Veränderung stattfindet. Persistent heißt, dass das Programm, das ich installiere, nach dem Neustart des Systems wieder aufgerufen wird. Und weil diese Akkus, das kennen Sie selber – die gehen ja andauernd alle und ich möchte ja, dass mein Staatstrojaner möglichst dauerhaft da bleibt. Das heißt, ich suche nach einem Weg, Persistenz zu erlangen. Und um diesen Weg zu beschreiten, brauche ich in der Regel einen zweiten Schwachstellentyp, nämlich eine lokale Privilege Escalation. Sie müssen sich das so vorstellen, dass so ein Betriebssystem unterschiedliche Rechteebenen hat, mit denen Programme ausgeführt werden. Dazu komme ich später nochmal, ist auch noch ganz wichtig. Ein Microsoft Word oder sowas kann nicht einfach Programme auf Ihrem Computer installieren, sondern läuft im Kontext eines Nutzers und hat eingeschränkte Befugnisse auf dem System.

Durch eine Privilege Escalation gelingt es mir als Angreifer, diese Administratorenrechte zu bekommen, die ich benötige – einmal, um mich fest in diesem System einzunisten, bei einem Neustart wieder aufgerufen zu werden. Die brauche ich aber – da kommen wir jetzt eher auf das Sicherheitssystem von Smartphones, weil wir da jüngere Betriebssysteme haben, die schon mit größerer Separation gebaut wurden – die brauche ich auch, um dann in andere Applikationen einbrechen zu können. Man könnte das einfach so sagen: Wenn ich auf meinem Smartphone zwei Applikationen installiert habe, dann separiert das Betriebssystem die so, dass Applikation A nicht auf die Daten von Applikation B zugreifen kann – in weiser Voraussicht, weil ich ja vielleicht einen wichtigen Messenger für geheime Botschaften installiere und irgendwelche Malware aus russischen Stores. Und damit diese Malware aus dem russischen Store nicht auf die Daten der anderen Applikationen zugreifen kann, gibt es also diese Rechte-Separierung. Auch dafür brauche ich die Privilege Escalation, also das Erhöhen meiner Privilegien über das, was mir eigentlich zusteht, hinaus, um dann auf die anderen Daten der Applikationen zuzugreifen.

Zu diesem Zeitpunkt bin ich dann also Administrator des Gerätes, und das ist das, was Sie vielleicht schon mal gehört haben, was man gemeinhin als Jailbreak bezeichnet. Ich bin aus dem Gefängnis, in dem ich eigentlich als Applikation laufe, ausgebrochen und kann auf die Daten anderer Applikationen zugreifen. Bei bestimmten Herstellern kommt bei einem Jailbreak noch hinzu, dass die Geräte sich eigentlich weigern, Software auszuführen, die nicht von dem Zulieferer spezifisch genehmigt wurde für dieses Gerät. Das sind eigentlich

Maßnahmen, die dafür da sind, Raubkopien zu unterbinden. In dem Moment, wo Sie so eine Software in einem bekannten App-Store kaufen, signiert der Hersteller quasi: Ich erlaube das Ausführen dieser Software auf diesem Gerät – damit Sie nicht die Software einfach von dem einen Gerät auf das andere kopieren können. Der für Sie unschöne Nebeneffekt ist, dass das gleiche für Ihre Schadsoftware gilt, die Sie ja installieren wollen. Das heißt, Sie brauchen, um das zu umgehen, einen relativ tiefen Systemzugriff, der es Ihnen ermöglicht, diesen Sicherheitsmechanismus des Zielsystems außer Kraft zu setzen. Mit anderen Worten: Sie schwächen das System dahingehend, dass es sich nicht mehr weigert, nicht zugelassene Software auszuführen, und schwächen die Sicherheit des Systems dahingehend, dass eine Software auf den geschützten Bereich einer anderen zugreifen kann. Das sind also nochmal zwei Schwachstellen, die Sie lokal brauchen auf so einem Telefon, plus die Remoteschwachstelle. Remote könnte in diesem Fall so was bedeuten wie: Sie besuchen eine schadhafte Webseite, oder Sie öffnen einen E-Mail-Anhang. Und dann könnten Sie mit Ihrer Quellen-TKÜ langsam zu Werke schreiten und sich für jede einzelne Applikation, die es da nochmal gibt, Wege verschaffen, die dort gespeicherten Daten in irgendeiner Form abzugreifen. Entweder greifen Sie dabei auf den lokalen Speicher der Applikation zu, der bei solchen verschlüsselten Messengern verschlüsselt ist – das heißt, da müssen Sie nochmal das Passwort klauen – oder Sie versuchen, sich in die Applikation selber reinzupatchen oder mit einem Hack die Applikation dazu zu bringen, in ihrem normalen Arbeitsfluss nochmal die nicht verschlüsselten Nachrichten abzulegen.

Dann werden Sie aber relativ schnell sehen, dass Sie das für jede einzelne Applikation spezifisch machen müssen, und dass ja viele Leute auch Web-Dienste nutzen zur Kommunikation. Das Beispiel Facebook wurde ja hier genannt; die haben immer noch einen sehr großen Anteil des Zugriffes über den Web-Browser selber. Spätestens dann kommen Sie an die Grenzen der Theorien, denn dann müssen Sie ja den Web-Browser kompromittieren. Und dieser Web-Browser ist ja eine universelle Applikation, die für alles Mögliche genutzt werden kann. Die Fülle der Kommunikationsmöglichkeiten, die das Internet uns bietet, wird über kurz oder lang die Programmierfähigkeiten und die Kapazitäten beim Bau einer solchen Software überschreiten, und dann macht man das, was wir 2011 gesehen haben – dass man gesagt hat: Naja, alles was der Nutzer macht, findet ja auf dem Bildschirm statt, also fotografieren wir einfach am laufenden Band den Bildschirm. Und dieser kleine Schritt, der eigentlich sehr sinnvoll klingt – dass man sagt: Na gut, dann mache ich ein Foto von der E-Mail, während er die schreibt – mache ich ja bei der TKÜ auch nicht anderes. Ich höre zu, während er spricht, oder ich schalte einfach, statt zwanzig Voice-Applikationen zu umgehen, das Mikrofon mit ein und schreibe mir das, was das Mikrofon hört, in eine Datei und schicke die weg. Das sind die winzig kleinen Schritte, die aus dem Konzept der Quellen-TKÜ sofort eine Wohnraumüberwachung oder eine Online-Durchsuchung machen.

Deswegen halte ich es für in der Realität nicht abbildbar, dass wir eine spezifische Quellen-TKÜ schreiben, die nur das macht und zu keinem Zeitpunkt über ihre Berechtigung hinausgeht. Gleichzeitig haben Sie mindestens die Remote-Schwachstelle und eine zweifache Schwächung des Systems, indem Sie einmal Administrationsrechte bekommen haben und das Code-Signing außer Kraft gesetzt haben, was es einem weiteren Angreifer ermöglicht, dieses System einfacher zu übernehmen als andere. Insofern also eine klare Schwächung des Nutzers – genau das, was von Personen des Chaos Computer Clubs 2011 schon festgestellt wurde.

Dann noch die kurze Frage zu dem Geheimhalten: relativ einfach, wenn ich geheimes Wissen habe, was aber eigentlich öffentlich ist. Jeder Analyst, der so eine Software in seinen Händen hat, kann ja eine Schwachstelle da drin suchen und finden. Das ist ja genau der Wettlauf, an dem ich beruflich jeden Tag teilnehme – ich natürlich mit der Motivation, vielleicht irgendwann mal so was richtig Geiles zu finden und damit angeben zu können, dass ich das beseitigt habe, und dann dafür zu sorgen, dass niemand anders diesen Berg mehr erklimmen kann. Andere, die sich denken, wunderbarer Angriffsvektor, den verkaufe ich für teures Geld an Geheimdienste oder Strafverfolgungsbehörden und tue dann das – in meinen Augen – moralisch Falsche und auch das, was

überhaupt nicht im Sinne des nationalen Interesses ist und im Sinne der inneren Sicherheit, nämlich die Allgemeinheit diesen Schwachstellen und dem Risiko auszusetzen, dass irgendjemand anders sie findet.

Der Vollständigkeit halber, nur weil ich das hier gerade sehe: Ich denke, Herr Dr. Sensburg wird darauf eingehen wollen, dass es ja eine Mitwirkungspflicht der Betreiber geben könnte, also sowas wie: der Smartphone-Hersteller hilft bei der Installation der Schadsoftware. Da darf ich dann – das mache ich auch in meiner Stellungnahme – an die Eckpunkte der deutschen Kryptopolitik erinnern, wo Sie jahrelang sehr gut damit gefahren sind, diese „Büchse der Pandora“ nicht zu öffnen, die nämlich im Umkehrschluss bedeutet würde, dass niemand mehr diesen Herstellern vertraut. Sie erinnern sich unter Umständen: Der größte Knall der Snowdon-Enthüllungen war genau, dass die Menschen gesehen haben: Okay, wir können offenbar Facebook und unseren Telefonanbietern und wem alles nicht mehr trauen, und Microsoft und was nicht alles – das war dann die Situation, wo diese Firmen wirklich ausgerastet sind. Also, da gehen Sie wirklich in einen sehr gefährlichen Bereich, den ich echt nicht nahelegen würde.

Ich hoffe, dass ich das grob erklärt habe für Sie.

Die **Vorsitzende**: Zumindest war das ein guter Spaziergang durch das Gerät und seine Anwendungen. So, jetzt hat als nächster Herr Krauß zwei Fragen von Herrn Fechner.

SV **Dr. Matthias Krauß**: Die erste Frage betraf die Frage des Schutzes der Berufsgeheimnisträger. Das ist in § 100d Absatz 5 StPO-E geregelt. Da wird die bisherige Regelung bei der Wohnraumüberwachung übertragen auf die Online-Durchsuchung. Es ist letztlich auch konsequent, weil das Verfassungsgericht ja gesagt hatte, beide Maßnahmen sind in ihrer Eingriffstiefe vergleichbar. Es wird also ein Überwachungsverbot für sämtliche Berufsgeheimnisträger statuiert – in den Fällen des großen Lauschangriffes und der Online-Durchsuchung. Bei den übrigen Ermittlungsmaßnahmen, die es sonst noch gibt, sieht die Rechtslage etwas anders aus. Das ist in § 160a StPO geregelt, da wird eine Abstufung vorgenommen, um welche Berufsgeheimnisträger es geht. Und für die sonstigen Zeugnisverweigerungsberechtigten nach § 52 und § 53a StPO gibt es wiederum andere Regelungen. Das heißt, wir haben für die eine Eingriffsmaßnahme die Regelung A, für andere Eingriffsmaßnahmen die Regelung B. Deswegen wird natürlich, meines Erachtens auch zu Recht, kritisiert, dass hier ein Gesamtkonzept fehlt. Es wäre natürlich wünschenswert gewesen, im Zuge dieser Regelungen über ein solches konsequentes Gesamtkonzept nachzudenken, aber ich befürchte, aufgrund der zeitlichen Eile ist das hier einfach nicht machbar, sondern muss auf eine spätere Zeit verschoben werden.

Die zweite Frage betraf den Straftatenkatalog, also die Anlasstat, bei der Online-Durchsuchung. Da sieht der Gesetzvorschlag ja vor, dass der Katalog des § 100c StPO, also der Wohnraumdurchsuchung, angewandt wird, was ich grundsätzlich für zulässig erachte. Es geht dort nämlich um besonders schwere Straftaten. Das Bundesverfassungsgericht hat dazu in seiner Entscheidung zum großen Lauschangriff 2004 auch schon mal eine Stellungnahme abgegeben und war der Auffassung, das sind eben Straftaten, die besonders bestraft sind – in der Regel mehr als fünf Jahre –, aber auch solche Straftaten, die arbeitsteilig begangen werden, die wegen des vernetzten Zusammenwirkens mehrerer Täter im Zuge der Verwirklichung eines komplexen, mehrere Rechtsgüter verletzenden kriminellen Geschehens besonders strafwürdig sind. Es geht also nicht nur um die Strafhöhe, sondern auch um die Art der Straftatbegehung. Den dem § 100c StPO zugrunde liegenden Strafkatalog hat das Bundesverfassungsgericht für verfassungsrechtlich in Ordnung erachtet. Deswegen kann ich jetzt keine größeren verfassungsrechtlichen Bedenken erkennen, diesen Straftatkatalog des § 100c StPO auf die Online-Durchsuchung zu übertragen. Zumal hinzukommt, dass nach § 100b Absatz 1 Nummer 2 StPO ja erforderlich ist, dass die Straftat auch im Einzelfall schwer wiegen muss. Das heißt, selbst wenn eine Straftat aus diesem Katalog vorliegt, heißt das nicht automatisch, dass sie als Anlasstat für eine solche Maßnahme in Betracht kommt, sondern es muss noch im konkreten Einzelfall die besondere Schwere dargelegt werden.

Die **Vorsitzende**: Danke. Jetzt hat Herr Huber eine Frage von Frau Winkelmeier-Becker.

SV **Alfred Huber**: Es ging um die Frage, inwieweit Quellen-TKÜ und Online-Durchsuchung in der Praxis voraussichtlich – da muss es sich natürlich immer um eine Prognose handeln – umgesetzt werden. Ich denke, da kann man sagen, wenn man sich die Online-Durchsuchung anschaut, dass ein Vergleich zulässig ist zur Wohnraumüberwachung, die wir bereits seit geraumer Zeit haben und die das Verfassungsgericht für unbedenklich erachtet. Wir haben bei der Wohnraumüberwachung – und vergleichbar auch bei dieser neuen Vorschrift der Online-Durchsuchung – eine ganze Reihe von Verpflichtungen. Es beginnt bei Dokumentation, Benachrichtigung, nachträglichem Rechtsschutz usw., so dass sich jeder Staatsanwalt ganz genau überlegen wird, ob er einen entsprechenden Antrag stellt und auch entsprechende Arbeitskraft binden wird. Das wird er sicherlich dann nicht tun – und da liege ich mit Herrn Buermeyer, jedenfalls mit seiner Stellungnahme, durchaus nah bei einander –, wenn er eine einfachere Möglichkeit hat, um die von ihm gewünschten Ermittlungserfolge zu erzielen. Dann darf er das auch gar nicht tun. Das heißt, wenn ich einen Täter habe, der eine Straftat begangen hat – sagen wir mal, er hat kinderpornografische Bilder gespeichert auf seinem Computer –, dann ist das ganz einfach, dann wird eine Durchsuchung beantragt. Das Gericht wird den entsprechenden Beschluss erlassen, und ich bekomme all das, was auf dem Computer drauf ist, durch eine ganz einfache strafprozessuale Maßnahme – also all diese schützenswerten Daten. Auch hier gibt es selbstverständlich einen Kernbereichsschutz, der für uns in der Praxis eigentlich kein großes Problem darstellt, denn all die Dinge aus dem Kernbereich, die interessieren die Strafverfolgungsbehörden sowieso nicht. Uns interessieren hier die Straftaten.

Jetzt gibt es aber einen Bereich, wo wir nicht weiterkommen mit dieser Art und Weise der Ermittlungen, und da bewegen wir uns jetzt hauptsächlich – da kann ich jetzt sprechen als Leiter einer Abteilung für organisierte Kriminalität und Betäubungsmittelkriminalität, aus meinem Bereich – im Bereich der organisierten Kriminalität. Warum? Aus einem ganz einfachen Grund: Wir haben bei der organisierten Kriminalität unterschiedliche Organisationsstufen. Wir haben die Handlanger; wir haben oft eine zweite Stufe, die sind schon ein bisschen höher, und das geht immer weiter. Und jetzt habe ich das Problem, dass ich sicherlich eine ganze Reihe von Handlangern erwischen kann, weil ich irgendwie mitbekomme, dass er gerade ein Kilogramm Heroin von A nach B bringt. Ich bekomme aber schon nicht mehr mit, wer ihm diesen Auftrag gegeben hat und für wen er eigentlich tätig ist. Und ich bekomme nicht mit, in welcher Organisation er sich befindet. Ich brauche nicht zu versuchen, den Handlanger zu befragen – das mache ich natürlich, das Ergebnis ist aber ganz klar, er wird mir keine Angaben machen, da kommt nichts raus. Das bedeutet, ich muss, wenn ich die organisierte Kriminalität effektiv bekämpfen will, als Staatsanwalt und als Polizeibeamter einen langen Atem haben. Und das bedeutet, ich muss in der Lage sein, für einen gewissen Zeitraum verdeckt zu ermitteln. Und hier kommt die Online-Durchsuchung ins Spiel, in geeigneten Einzelfällen.

Aus der Praxis kann ich Ihnen einen Fall berichten, den wir im Bereich der organisierten Kriminalität, Betäubungsmittelhandel, hatten, wo wir im letzten Jahr über einen langen Zeitraum eine Wohnraumüberwachung bekommen haben. Es war eine Wohnraumüberwachung von Geschäftsräumen, die ja auch der Vorschrift unterfallen, und das war die einzige Möglichkeit, hier weiter zu kommen, weil diese Geschäftsräume genau dafür angemietet wurden, Gespräche über solche Delikte zu führen, auf einer etwas höheren Organisationsebene. Und genau so läuft das auch, wenn ich eine Online-Durchsuchung mache: Dann habe ich die Chance, eine Zeit lang zu beobachten, was alles passiert. Wer ist denn jetzt eigentlich der Chef, wer ist denn derjenige, der die entscheidenden Befehle gibt, und wer führt diese Taten nur aus? Für die Bekämpfung der organisierten Kriminalität ist aus diesem Grund die Online-Durchsuchung absolut unabdingbar. Wir können immer sagen – das ist eine politische Entscheidung und dafür muss ich ganz ehrlich sagen, gebe ich Ihnen die Verantwortung gerne zurück – wenn Sie sagen: Ich will die organisierte Kriminalität gar nicht so bekämpfen, ich lasse auch die Wohnungseinbrecher laufen, die sind mir nicht so wichtig, vielleicht sollen wir mal ein paar erwischen, dann haben wir einen schönen Ermittlungserfolg. Derzeit haben wir 20 Prozent. Mir persönlich ist das viel zu wenig –

sage ich ganz ehrlich – aber das ist eine politische Frage. Wenn Sie sagen: Ich möchte das nicht, wir schützen lieber die Daten, dann müssen Sie sich aus meiner Sicht aber auch die Frage stellen: Schützen Sie damit nicht eigentlich auch die Täter?

Die **Vorsitzende**: Sind Sie noch bei der Beantwortung dieser einen Frage?

SV **Alfred Huber**: Ja, ich war bei der Online-Durchsuchung, weshalb die für uns wichtig ist.

Die **Vorsitzende**: Weil jetzt schon sechs Minuten um sind.

SV **Alfred Huber**: Ich würde vielleicht noch zwei Minuten auf die Frage – wenn es Ihnen Recht ist, wenn nicht, haben Sie das Recht, mir das Wort zu entziehen, das ist natürlich völlig klar – zur Quellen-TKÜ, die auch gestellt war, eingehen.

Die **Vorsitzende**: An Sie?

SV **Alfred Huber:** Ich habe es so verstanden, aber wir können gerne nochmal nachfragen.

Die **Vorsitzende**: Machen Sie es, ich versuche nur immer – wenn jemand eine Frage hat, sollte er allemal mit fünf Minuten auskommen. Deshalb bitte ich um Konzentration.

SV **Alfred Huber**: Gut, also ganz kurz – es ist ja zum Teil schon angesprochen worden – wie schaut es mit der Quellen-TKÜ aus, wie oft werden wir die voraussichtlich einsetzen? Wir haben ja heute schon gehört, die normale TKÜ, da haben wir ca. 6.000 Verfahren im Jahr, wo sie eingesetzt wird. Ein minimaler Teil. Ich denke nicht, dass wir 6.000 Quellen-TKÜs haben werden, weil wir in dem einen oder anderen Fall – das muss man ganz klar sagen – mit der normalen TKÜ auch noch ein Stück weiter kommen und die Quellen-TKÜ da zusätzlich natürlich weitere Anforderungen an uns stellt. Wie viele Verfahren es tatsächlich werden, darüber werden wir selbstverständlich, wie bisher auch immer, entsprechend berichten. Das ist heute ein bisschen schwer zu prognostizieren. Ich kann Ihnen aber garantieren, da wird keiner sein, der es nicht wert ist. Besten Dank.

Die **Vorsitzende**: Danke. Herr Henzler hat auch eine Frage von Frau Winkelmeier-Becker. Bitte.

SV **Peter Henzler**: Frau Winkelmeier-Becker, ich hatte verstanden: Welche Gefährdungen bestehen für das Zielsystem, auf das wir drauf gehen, und welche Gefahren, Sicherheitslücken ergeben sich für andere? Im Gegensatz zu der Meinung von Herrn Neumann wird es sich bei den Maßnahmen um technische Unikate handeln, die speziell auf ein spezielles Zielsystem, nämlich des Täters, gebracht werden. Wir haben derzeit ungefähr – das sind die Zahlen, die mir bekannt sind – 346 unterschiedliche Smartphone-Modelle und ungefähr 67 unterschiedliche Betriebssysteme, unterschiedlichste Applikationen darauf, und die müssen analysiert werden, und dann wird eine zielgerichtete Maßnahme gemacht. Das heißt in der Ableitung, dass das, was für ein Zielsystem gemacht wird, noch lange nicht auf jedes andere oder schon das nächste Smartphone passt. Im Übrigen sind die Maßnahmen exakt zugeschnitten auf das, was das Bundesverfassungsgericht in seinem Urteil zur Online-Durchsuchung 2008 aufgestellt hat. Es ist ebenfalls unzutreffend, sowohl technisch unzutreffend wie bei dem Tool, das wir entwickelt haben, in der Sache unzutreffend, dass diese Remote-Software – eine solche ist das – mehr kann als das Verfassungsgericht zulässt. Die ist coupiert, die ist nur auf die Funktionen zugeschnitten und programmiert, die wir dürfen – schwer genug, weil das nämlich dann eine Software ist, die von uns selber entwickelt worden ist. Und diese Software entspricht einer sogenannten standardisierten Leistungsbeschreibung, abgeleitet aus dem Urteil des Bundesverfassungsgerichts. Im Wege des Qualitätsmanagements ist durch eine externe Firma geprüft worden, ob sie diesen Begrenzungen entspricht. Und sie entspricht diesen Begrenzungen.

Zu der Thematik, was passiert, wenn eine solche Software bekannt wird: Auch da ist interessant zu hören, dass Herr Neumann sich täglich damit befasst, Exploits zu finden, aber fünf Jahre lang nicht die Exploits gefunden hat, die die NSA hatte. Was ich damit sagen will, ist, die ist im Zuständigkeitsbereich der Sicherheitsbehörden gewesen, sie ist geleakt worden, sie ist dann, als das bekannt wurde, Microsoft gesagt worden, und sie bezog sich auf alte Systeme – das, denke ich, ist zwischenzeitlich hier in der Runde bekannt –,

die nicht, wie Herr Neumann gesagt hat, gepatcht worden sind, also mit neuesten Sicherheitsänderungen sicher gemacht worden sind, und deshalb angreifbar waren. Das BKA führt das Ermittlungsverfahren, und, wenn es jemanden beruhigt: Es war kein gezielter Angriff gegen Krankenhäuser, es war kein gezielter Angriff gegen kritische Infrastrukturen – wenn man bei der Bahn etwa von einer kritischen Infrastruktur sprechen kann, abgesehen davon, dass da nur die Fahrplananzeigen verändert wurden –, sondern das war ein Zufallstreffer, weil oft in Unternehmen oder im öffentlichen Bereich – in England ist das weit verbreitet – alte Software eingesetzt wird, die nicht den neuesten Sicherheitsvorkehrungen entspricht. Ich hoffe, ich habe damit Ihre Frage beantwortet.

Die **Vorsitzende**: Danke. Dann hat jetzt als letzter in der Runde Herr Dr. Buermeyer zwei Fragen von Frau Keul. Wir können noch eine zweite Runde machen, aber wir müssen das so gezielt machen, dass wir um 18.00 Uhr fertig sind. Außer jemand anderes möchte hier weiter leiten, aber ich müsste dann gehen. Herr Dr. Buermeyer.

SV **Dr. Ulf Buermeyer**: Vielen Dank. An mich wurde zunächst die Frage gerichtet zur Abgrenzung zwischen den beiden Maßnahmen, die hier in Rede stehen: Online-Durchsuchung und Quellen-TKÜ. Da möchte ich einen Punkt nochmal betonen, den Herr Neumann gerade schon angesprochen hat. Technisch ist es zunächst einmal – das hat auch mein Vorredner gerade im Grunde implizit gesagt – technisch ist es zunächst einmal dieselbe Maßnahme. Sie müssen irgendwie das System, dass Sie überwachen wollen, infizieren, und dann ist die Frage, welche Daten Sie aus diesem System ausleiten. Mit anderen Worten, um einen Begriff von meinem Vorgänger zu verwenden, die Maßnahme wird im Fall der Quellen-TKÜ coupiert, quasi im Nachhinein begrenzt. Sie müssen das System infizieren, Sie haben damit technisch zunächst mal den kompletten Zugriff. Sie können das System komplett auslesen, Kameras anschalten, was auch immer Sie damit tun wollen, in beiden Fällen – aber bei der Quellen-TKÜ dürfen Sie es nicht. Das heißt, es handelt sich zunächst mal um eine rechtliche Begrenzung. Wenn Sie diese Begrenzung nicht einhalten, dann führen Sie eine Online-Durchsuchung unter dem Deckmantel einer Quellen-TKÜ durch. Und das Bundesverfassungsgericht hat 2008 verlangt, dass diese Maßnahme rechtlich begrenzt wird, aber auch technisch. Rechtliche und technische Vorkehrungen müssen getroffen werden bei einer Quellen-TKÜ, um sicherzustellen, dass dieser Bereich der laufenden Kommunikation eingehalten wird.

Das bringt mich gleich zu einem nächsten Punkt. Im Fall des vom BKA entwickelten Trojaners glauben wir jetzt einfach mal das, was mein Vorredner gesagt hat, dass es da so eine externe Prüfung gab. Was da genau geprüft wurde, wissen wir nicht, weil die standardisierte Leistungsbeschreibung top secret ist – oder keine Ahnung, welche Klassifikation, aber jedenfalls nicht öffentlich. Niemand kann das neutral prüfen. Dass es innerhalb des BKA geprüft ist – es mag Menschen in diesem Haus geben, die da Einsicht hatten – aber von unabhängiger Seite geprüft ist das jedenfalls nicht, sondern nur von einer Firma, die BKA ausgesucht hat. Mit anderen Worten: Eine zentrale Forderung, die schon seit mindestens zehn Jahren im Raum steht, dass nämlich ein Staatstrojaner, wenn es denn einen gibt, wenigstens unabhängig geprüft wird, zum Beispiel, wenn man das denn will, von der Bundesbeauftragten für den Datenschutz – das ist bislang eben gerade nicht umgesetzt. Das BKA hat einen Teil dieser Forderung, wenn man so will, überobligationsmäßig erfüllt, aber eben auch nicht vollständig, und es gibt dazu vor allem keine Verpflichtung. Das, finde ich, ist eine zentrale Schwäche dieser Regelung, die zurzeit auf dem Tisch liegt. Wir können im Grunde einfach nur hoffen und beten, dass die Maßnahmen in grundgesetzkonformer Weise durchgeführt werden. Es gibt überhaupt keine Vorkehrungen im Gesetz, keine verfahrensrechtlichen Sicherungen. Diesen Ball muss man natürlich auch nach Karlsruhe spielen, das muss man aus Fairness sagen: Das Bundesverfassungsgericht hat sich an diesem Punkt auch vergleichsweise wenig problembewusst gezeigt. Es finden sich auch in der Entscheidung zum BKA-Gesetz keine genaueren Angaben hierzu, was ich persönlich sehr bedauerlich finde. Das bedeutet aber ja nicht, dass der Gesetzgeber nicht solche Vorgaben machen kann und aus meiner Sicht auch machen sollte. Das, denke ich, ist einer der Gründe, weswegen diese Formulierungshilfe, so

wie sie jetzt auf dem Tisch liegt, auf keinen Fall Gesetz werden darf in dieser Wahlperiode, ohne zentrale Nachbesserung. Ich habe in meiner Stellungnahme eine ganze Reihe von Formulierungsvorschlägen gemacht. Dieser Punkt „Prüfung der Software“ allerdings ist vergleichsweise komplex, deswegen findet sich da wegen der Kürze der Zeit kein Formulierungsvorschlag von mir, aber ich kann nur dringend davor warnen, es so eine Art Trojaner-Blindflug-Gesetz werden zu lassen, wo man, wie gesagt, nur hoffen kann, dass es letztlich alles so funktioniert wie es im Gesetz steht. Bei einer so eingriffsintensiven Maßnahme – wie gesagt, jede Quellen-TKÜ ist ständig in der Gefahr, zu einer Online-Durchsuchung quasi abzugleiten – muss es auch verfahrensrechtliche Sicherungen geben, die die Vorgaben, in diesem Fall der Strafprozessordnung, tatsächlich einhalten.

Zur zweiten Frage: Bekommt man die Software eigentlich wieder herunter vom System, wie schaltet man sie ab? Um da den schon zitierten Fall des Bayern-Trojaners nochmal ins Spiel zu bringen: Dort hatten die Ermittlungsbehörden – es war ein Windows-System, dass da infiziert worden war – den Trojaner einfach in den Papierkorb gelegt, – das ist kein Witz! – dann aber vergessen, den Papierkorb zu leeren. Deswegen hat der Chaos Computer Club bei der Analyse der Festplatte den Trojaner im Papierkorb gefunden. Das ist so das Niveau des Bayerischen Landeskriminalamts – aber ich will darüber jetzt gar nicht spotten. Das Problem ist, es handelt sich um extrem komplexe Maßnahmen. Ich will nicht für mich in Anspruch nehmen, dass ich das besser hinbekäme. Und auch Herr Neumann wäre da sicherlich, wenn er denn überhaupt Trojaner bauen würde, herausgefordert, das in einer Weise zu tun, dass der dann tatsächlich nur, wie das ja im Gesetz steht, die Eingriffe vornimmt, die tatsächlich technisch nötig sind, und die dann auch wieder rückgängig zu machen. Schlicht und ergreifend: Man kann es nicht wissen. Stellen Sie sich folgenden Fall vor: Das System wird überwacht. Es handelt sich vielleicht mal um ein Mac-System, bei Mac gibt es die sogenannte Time Machine – werden Sie vielleicht kennen? Das ist total praktisch, da speichert das System ständig quasi ein Abbild seiner selbst auf einer externen Festplatte. Jetzt stellen Sie sich vor, ein solches System wird mit einem Trojaner infiziert, dann landet der Trojaner natürlich auch in der sogenannten Time Machine. Dann entscheiden sich die Sicherheitsbehörden, den Trojaner abzuschalten. Ein paar Tage später macht die Festplatte schlapp. Der Betroffene stellt sein System mit Hilfe seiner Time Machine wieder her – und was passiert? Er spielt sich selber den Trojaner wieder ein. Ein ganz banales Beispiel, das zeigt, um was für einen komplexen Vorgang es sich handelt. Sie können letztlich nicht vorhersagen, ob Sie einen Trojaner rückstandsfrei wieder entfernen können. Natürlich würden sich dann die Sicherheitsbehörden an die Vorgaben halten und den Trojaner nicht mehr nutzen, aber er wäre jedenfalls wieder auf der Festplatte drauf, potentiell aktiv, und damit hätten Sie die Hintertüren, von denen Herr Neumann gesprochen hat. Wie gesagt, das ist nur ein plakatives Beispiel, was so alles schiefgehen kann. Letztlich, denke ich, ist das nicht deterministisch. Sie können nicht mit Sicherheit sagen, was auf einem System funktioniert und was wirklich einen Trojaner effektiv wieder entfernt. Das eine ist die verfahrensmäßige Sicherung, die bisher fehlt, das andere sind die großen technischen Probleme. Herzlich Dank.

Die **Vorsitzende**: Danke sehr. Ich habe für die zweite Runde drei Fragen. Bitte Frau Esken, Frau Keul, Frau Winkelmeier-Becker.

Abg. **Saskia Esken** (SPD): Vielen Dank, Frau Vorsitzende. Herr Dr. Buermeyer, ich habe zwei Fragen an Sie. Ich habe heute früh gelesen, der Innenminister denkt über Konsequenzen aus dem Angriff nach, der unter dem Hashtag WannaCry bekannt geworden ist. Er hält es für notwendig, das IT-Sicherheitsgesetz weiterzuentwickeln, insbesondere die Frage, welche Unternehmen, welche Institutionen, welche Branchen davon betroffen sein sollen. Ich finde ja durchaus, mit WannaCry ist es nochmal deutlich geworden: IT-Sicherheit ist teuer und mühsam, aber keine IT-Sicherheit ist noch teurer. Es wurde ein vergleichsweise geringer Betrag erbeutet, aber ein Schaden in vielfacher Milliardenhöhe verursacht. Insofern wollen wir begrüßen, dass der Innenminister darüber nachdenkt, die IT-Sicherheit unserer Infrastruktur zu verbessern. Und es geht ja um Meldepflichten für Angriffe mit dem Ziel, weitere Angriffe auf der Grundlage dieses Angriffsvektors zu verhindern, indem man dafür

sorgt, dass die Sicherheitslücken geschlossen werden – die Patches vorher. Insofern würde ich gerne verstehen, wie es nach Ihrer Meinung einzuschätzen ist, dass eine staatliche Behörde – denn das ist ja Sinn und Grundlage des Vorgehens – Sicherheitslücken erforscht und einkauft, diese aber dann nicht meldet für einen Patch, also für eine Reparatur sorgt, sondern diese den Sicherheitsbehörden zur Verfügung stellt für solche Eingriffe. Ist das nicht das Gegenteil von dem, was der Minister mit dem IT-Sicherheitsgesetz erzielen will, was wir mit dem IT-Sicherheitsgesetz erzielen wollen?

Und die zweite Frage bezieht sich auf das, was Sie gerade ausgeführt haben. In wie weit kann denn dieses externe Unternehmen, Herr Henzler, das Sie genannt hatten, oder kann ein Gericht, können wir als Parlament überprüfen, auch immer wieder überprüfen, ob technisch und rechtlich der Eingriff und die Wirkung eines solchen Trojaner überhaupt dem entsprechen, was vorgegeben ist? Woher wissen wir überhaupt, was vorgegeben ist? Wer kann so was überprüfen? Und wie oft müssten wir das überprüfen, damit auch gewährleistet ist, dass die Regeln eingehalten werden?

Die **Vorsitzende**: Danke. Frau Keul.

Abg. **Katja Keul** (BÜNDNIS90/DIE GRÜNEN): Eine Frage an Professor Sinn, nochmal zur richterlichen Überprüfung. Beide Maßnahmen müssen ja richterlich angeordnet oder vielleicht auch im Nachhinein überprüft werden, ob sie rechtmäßig waren. Und wir haben ja jetzt schon gehört, dass das mit der Überprüfung ganz schön schwierig ist. Wenn ich da jetzt als Richter sitze, egal ob Landgericht oder Amtsgericht, und muss entscheiden, ob der angewandte Trojaner tatsächlich nur Kommunikation ausgelesen hat oder ob er auch weitere Daten ausgelesen hat – das ist ja sowohl rechtlich als auch technisch schwer zu erkennen. Wie kann das funktionieren, kann es überhaupt funktionieren, dass ich als Richter die Reichweite der angewendeten Software erkennen und überprüfen kann? Und wenn nicht, was mache ich dann damit, benenne ich dann einen Sachverständigen dafür, wer ist das dann? Sind Sie das oder Herr Neumann, oder wie komme ich als Richter daran?

Die zweite Frage geht nochmal an Herrn Dr. Buermeyer, und zwar ganz konkret zum § 100d StPO-E. Da finde ich ein paar Sachen sehr erstaunlich; vielleicht können Sie das mal erhellen. Im § 100d StPO-E geht es ja um den Kernbereich, und ich frage Sie nach Absatz 3 und Absatz 5. Im Absatz 3 steht drin, dass man gehalten ist, den Kernbereich privater Lebensgestaltung nicht zu erheben, soweit technisch möglich. Das ist schon interessant: Wenn es technisch nicht möglich ist, dann kann ich den Kernbereich erheben. Oder? Das sagt mir als Anwender im Prinzip dann doch das Gesetz. Und auch bei Absatz 5 finde ich etwas sehr Erstaunliches: Da steht ja erfreulicherweise drin, dass in Fällen des § 53 StPO Maßnahmen nach §§ 100b und 100c StPO nicht angewendet werden dürfen – das betrifft die Anwälte, zum Beispiel. Freut mich als Anwältin, bin ich also geschützt. Dann steht im nächsten Satz aber: In den Fällen §§ 52 und 53a – § 53a sind meine Berufshelfer – dürfen die Maßnahmen nur dann nicht verwendet werden, wenn sie nicht außer Verhältnis zum Interesse an der Erforschung des Sachverhaltes stehen. Das ist doch irgendwie schizophren, denn § 53a sagt doch: Meine Berufshelfer sind mir als Anwalt gleichgestellt oder die Arzthelfer dem Arzt, und hier steht genau das Gegenteil. Hier wird der Schutz plötzlich differenziert, und plötzlich haben meine Berufshelfer nicht mehr den gleichen, sozusagen, Zeugenverweigerungsschutz wie ich selbst. Ist das nicht ein gravierender Eingriff in die Schweigepflicht?

Die **Vorsitzende**: Danke. Frau Winkelmeier-Becker? Gut, dann hat Herr Professor Sinn als Erster das Wort.

SV **Prof. Dr. Arndt Sinn**: Vielen Dank. Frau Keul, das ist natürlich ein Problem. Der Richter kennt das Recht, wie ich auch ein bisschen das Recht kenne, und wendet das Recht an, überprüft das Recht. Sobald es in die Technik geht – danach sind wir an der Schnittstelle. Was wird er tun, wenn tatsächlich Anhaltspunkte dafür bestehen, und die Verteidigung rügt: Es wurde hier eine Software benutzt, die eben nicht das gemacht hat, was sie eigentlich darf? Dann wird er sich das anschauen, nach der Aktenlage, und wird zu einer Entscheidung kommen können. Denn das kann er ja prüfen, wenn da Kernbereichsdinge

drinstehen – das kann er ja prüfen nach Aktenlage. – Ich komme gleich zur Akte, was da eigentlich reingehört. Und wenn er das nicht prüfen kann, dann kann der Sachverständige das machen. Es geht ja um die Verwertbarkeit der Beweise und nicht darum, ob die Software in Ordnung war. Die Verteidigung rügt nicht die Software, dass die nicht in Ordnung war, sondern die Verteidigung rügt: Der Beweis, der mit dieser Software erhoben wurde, darf nicht verwertet werden.

Jetzt komme ich zur Akte: Zur Akte müssen natürlich alle Bestandteile gelangen, die mit dieser Software ausgeleitet wurden. Es gilt der Grundsatz der Aktenklarheit und der Aktentransparenz. Wenn diese Akte nicht alles enthält, ist das natürlich rechtswidrig. Das kennen wir in anderen Zusammenhängen ja auch. Aber wir nehmen den Idealfall an: Die Akte enthält alles, was mit der Software ausgeleitet wurde. Dann hat der Richter eine Grundlage, um zu entscheiden, ob diese Dinge verwertbar sind, ob es nämlich die laufende Telekommunikation betraf. Das betrifft dann die Frage der Verwertbarkeit bis hin zur Revision.

Habe ich das zufriedenstellend beantwortet?

Die **Vorsitzende**: Wenn es eine kurze spontane Frage gibt, bitte. Das kriegen wir ja noch hin in der Zeit.

Abg. **Katja Keul** (BÜNDNIS 90/DIE GRÜNEN): Also ist die Akte dann das gesamte Handy? Wenn ich jetzt eine Kamera anschalte, obwohl ich es nicht darf, und das Schlafzimmer monatelang überwache, wie kann ich das in der Akte feststellen?

SV **Prof. Dr. Arndt Sinn**: So, wie Sie es gesagt haben. Da gehört alles rein, was mit dieser Software ausgeleitet wurde. Und wenn das zwanzig Aktenschränke sind, dann sind das zwanzig Aktenschränke. So was kennt man im Offline-Bereich bei Wirtschaftsstraftaten auch, oder im NSU-Prozess, dass man ganze Aktenschränke voll hat. Das ist nichts Neues. Und da muss man sich durchwühlen. Das Recht tut manchmal auch weh für den Richter.

Die **Vorsitzender**: Herr Henzler ist der Nächste, der eine Frage von Frau Esken hat, und dann Herr Dr. Buermeyer.

SV **Peter Henzler**: Ich werde im zweiten Teil etwas dazu sagen, wer das überprüfen kann mit der standardisierten Leistungsbeschreibung. Aber der erste Teil war ja: Da befassen sich welche mit der Suche und dem Kauf von Exploits – die war aber an Herrn Dr. Buermeyer. Wenn Software geschrieben wird, sind das Millionen von Zeilen, von Programmier-Code, wenn da nur 0,1 Prozent oder 0,01 Prozent Fehler drin sind, dann wird man sogenannte Exploits haben, die tatsächlich genutzt werden, weil es anders technisch nicht möglich ist, in ein System zu kommen. Das ist die technische Voraussetzung, um das, was das Recht geben soll, umsetzen zu können.

Wer kann die standardisierte Leistungsbeschreibung überprüfen? Das ist eine hoch spezialisierte, zertifizierte, nach allgemeinen Regeln ausgeschriebene Firma, die diese Aufgabe übernommen hat und die, geleitet von den Vorgaben des Bundesverfassungsgerichts von 2008, den Leistungsumfang, die Fähigkeiten dieser Remote-Software prüft, indem der sogenannten Quell-Code geprüft wird und die Software, das Engineering der Software, insgesamt nochmal nachvollzogen wird. Ich darf nochmal sagen, auch wenn das hier schon mehrfach gesagt worden ist: Diese Software hat keine technische Fähigkeit für die unzulässigen, vom Verfassungsgericht als unzulässig erkannten Features oder Funktionalitäten – wie Sie das bezeichnen wollen. Es gibt diese Software nur in dem verfassungskonformen technischen Aufbau – was immer Sie dazu sagen wollen. – Sie können auch keine Herzoperation überprüfen oder Sie können auch keine, was weiß ich …

Die **Vorsitzende**: Bei der Herzoperation ist es ein bisschen übersichtlicher als am Computer, zumindest kann man es sich optisch besser vorstellen. Wir wollen gar keine Diskussion. Ich weiß, Herr Neumann ist auch nervös, aber wir können bei einer Anhörung immer nur bestimmten Leuten das Wort geben.

SV **Linus Neumann**: Ich würde gerne die sachlichen Fehler korrigieren, die wir …

Die **Vorsitzende**: Nein, da muss Ihnen jemand eine Frage stellen wollen, sonst habe ich das Problem, dass Sie alles diskutieren, was Sie möchten – was auch spannend ist, aber nicht unser Plan heute. Die Anhörung basiert auf

Fragen, und dass da zwei unterschiedliche Auffassungen bestehen, haben wir, glaube ich, schon gehört. Jetzt hatte aber Herr Dr. Buermeyer noch eine Frage von Frau Esken und Frau Keul.

SV **Dr. Ulf Buermeyer**: Vielen Dank. Stichwort „Sicherheitslücken einkaufen, Sicherheitslücken verwenden, Sicherheitslücken geheim halten". Wir haben schon vielfach gehört, dass man Sicherheitslücken braucht, wenn man einen Trojaner auf ein System einspielen will. Und wenn man das rechtlich gestaltet, dann entsteht für Hoheitsträger ein Zielkonflikt: Es entsteht dann ein offensichtliches Interesse, Sicherheitslücken, die bekannt werden, geheim zu halten bzw. Sicherheitslücken sogar auf dem Markt einzukaufen. Es gibt einen Schwarzmarkt, einen Graumarkt für Sicherheitslücken, da werden hohe sechsstellige, manchmal auch siebenstellige Beträge aufgerufen, zum Beispiel für einen iPhone-Exploit. Da werden enorme Kosten auf uns zukommen, und wie gesagt, es entsteht ein großer Anreiz, solche Sicherheitslücken aufzukaufen, geheim zu halten, um sie dann ausnutzen zu können. Und das hat Herr Neumann ja schon gesagt: Für einige wenige Ermittlungsverfahren wird die IT-Sicherheit weltweit aufs Spiel gesetzt. Das muss man so deutlich sagen. Und das muss man auch wollen, auch als Gesetzgeber muss man das wollen, eine solche Anreizstruktur zu schaffen, wenn man das denn für verhältnismäßig hält. Es gibt aber einen Ausweg aus dem Dilemma – das habe ich in meiner Stellungnahme auch schon dargestellt. Man könnte nämlich einfach die Sicherheitsbehörden verpflichten, ausschließlich solche Schwächen des Systems auszunutzen, die dem Hersteller schon bekannt sind. Und das sagt uns ja WannaCry auch, da ist ja eine Sicherheitslücke ausgenutzt worden, die dem Hersteller bekannt war, für die es schon einen Patch gab, nur die Leute haben das eben nicht eingespielt. Und wenn man das beschränkt auf solche bekannten Sicherheitslücken, dann setzt man gerade nicht die IT-Sicherheit weltweit aufs Spiel, sondern dann nutzt man gezielt die Nachlässigkeit von Beschuldigten, und da muss man sagen, das ist ja genau das, was Ermittlungsbehörden im Grund landauf, landab jeden Tag tun. Wir warten ja im Grunde immer darauf, dass der Betreffende einen Fehler macht. Den perfekten Verbrecher kriegen wir nicht, aber die allermeisten sind eben keine perfekten Verbrecher. Nur so kommen wir ja auch zu Aufklärungsquoten von über 90 Prozent, zum Beispiel im Bereich von Tötungsdelikten. Bei Einbrüchen sieht es natürlich nicht so gut aus. Kurz und gut, das wäre mein ganz dringender Appell: Wenn Sie tatsächlich der Meinung sind, wir brauchen eine Rechtsgrundlage für den Trojaner-Einsatz, dann ist es zumindest zu beschränken auf die Ausnutzung von Sicherheitslücken, die dem Hersteller schon bekannt sind. So kann man, glaube ich, verhindern, dass ein Anreiz entsteht, dass ausgerechnet deutsche Sicherheitsbehörden sich an der IT-Sicherheit weltweit versündigen. Ein Formulierungsvorschlag dazu findet sich übrigens in meiner Stellungnahme. Das kann man im Grunde per Copy-and-paste umsetzen, wenn man das für richtig hält.

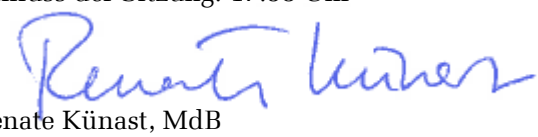
Zur Frage von Frau Keul, zum § 100d StPO-E, Kernbereichsschutz nur nach Maßgabe des Möglichen. Ja, das ist in der Tat der Trade-off, die Abwägung, die diesem Vorschlag zugrunde liegt. Ich teile da Ihre Verwunderung, um das so deutlich zu sagen. Ich finde das auch einigermaßen zynisch, wie das geregelt ist. Das heißt mit anderen Worten: Je schlechter der Trojaner, desto weniger Kernbereichsschutz. Darauf läuft es hinaus. Und das, zusammengenommen mit den schwachen verfahrensrechtlichen Sicherungen ist dann letztlich wieder Trojaner oder Grundrechtsschutz oder Kernbereichsschutz nach Kassenlage. Je weniger Mittel zur Verfügung gestellt werden für die Entwicklung eines kernbereichsschützenden Trojaners, desto schlechter ist der dann. Wie gesagt, ich kann im Grunde nur nach oben verweisen auf die fehlende technische, verfahrensrechtliche Prüfung des Trojaners. Und das Ganze möchte ich auch nochmal kurz in den Kontext dieser „Going Dark"-Debatte stellen, wir haben es ja eben schon angesprochen, da gibt es unterschiedliche Sichtweisen – die Kollegen haben da auch gute Punkte gemacht – wo es tatsächlich Probleme gibt bei der TKÜ, das kann man gar nicht in Abrede stellen. Aber, wie gesagt, man muss es auch immer im Kontext sehen der sehr weiten digitalen Ermittlungsmöglichkeiten, die wir als Ermittlungsbehörden heute haben mit der Vorratsdatenspeicherung, mit der Verkehrsdatenspeicherung, der man ja nicht entkommt durch Verschlüsselung. Mit welchen Handymasten sich mein Handy verbunden hat, das wird

gespeichert, mein Aufenthaltsort wird gespeichert von den Telekommunikationsanbietern – da komme ich nicht mehr drum herum. Insofern denke ich, ist „Going Dark“ ein Ausschnitt aus dem großen Problem, aber es gibt eine Studie der Harvard University in den Vereinigten Staaten, die zu dem Ergebnis kommt, dass die Ermittlungsbehörden noch nie so viele Daten zur Verfügung hatten über Beschuldigte wie heute. Wie gesagt, die Probleme, die Verschlüsselung aufwirft, bestehen, aber per Saldo ist die Situation durchaus nicht so katastrophal, wie es hier mitunter dargestellt wurde.

Absatz 5, die Berufsgeheimnisträger. Dazu vielleicht nur der Gedanke, dass ja schon die Formulierung dieses Absatzes 5 vergleichsweise nachlässig ist. Da heißt es nämlich „in den Fällen des § 53“, was ja auch die Abwägungsvorschrift einbezieht, die in § 53 StPO enthalten ist. Das heißt, selbst für Journalistinnen und Journalisten gilt das Erhebungsverbot nur nach Maßgabe einer Abwägung. Jedenfalls kann man den Absatz 5 so verstehen. „In den Fällen des § 53“ ist eben nicht dasselbe wie „gegenüber dem in § 53 Absatz 1 Satz 1 genannten Personenkreis“. Auch da findet sich in meiner Stellungnahme ein Formulierungsvorschlag, wie man das präzisieren kann. Denn so, wie der Absatz 5 jetzt gefasst ist, bezieht er seinerseits selbst bei dem § 53er Personenkreis schon eine Abwägung ein. Ob das tatsächlich gewollt ist – es kann sich auch um ein Redaktionsversehen oder ein Fassungsversehen des Gesetzgebers handeln. Aber jedenfalls wäre da aus meiner Sicht unbedingt nachzusteuern. In der Tat ist die Regelung zu dem Personenkreis des § 53a StPO eine offensichtliche Hintertür, und da würde ich letztlich im Interesse aller Beteiligten, auch der Ermittlungsbehörden, für eine klare Regelung plädieren. Es ist im Ermittlungsverfahren ohnehin schon unklar genug, gegenüber wem man eigentlich tätig wird. Oft genug weiß man das nicht, wenn die Personen nur unter irgendwelchen Decknamen agieren, in Bandenstrukturen zum Beispiel. Da gibt es schon auf tatsächlicher Ebene genügend Unsicherheiten, und jedenfalls die Rechtsgrundlagen sollten dann klar gefasst sein. Vielen Dank.

Die **Vorsitzende**: Danke. Ich habe jetzt keine Fragen mehr. Jetzt muss ich, auch wenn viele noch gerne reden würden, diese Sitzung beenden und mich bei Ihnen bedanken. Dass es unterschiedliche technische Vorstellungen und rechtliche Auffassungen gab, haben wir ja gesehen. Dann danke ich den Herren Sachverständigen und allen anderen, die hier waren, und schließe die Sitzung.

Schluss der Sitzung: 17:58 Uhr



Renate Künast, MdB
Vorsitzende

Anlagen: Stellungnahmen der Sachverständigen

Gutachterliche Stellungnahme

zur Öffentlichen Anhörung zur „Formulierungshilfe“ des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKÜ im Strafprozess

Ausschuss-Drucksache 18(6)334

im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages
am 31. Mai 2017

von

Dr. iur. Ulf Buermeyer, LL.M. (Columbia)

Richter am Landgericht Berlin
Vorsitzender der Gesellschaft für Freiheitsrechte e.V. (GFF)

ulf@buermeyer.de

Berlin, den 29. Mai 2017

We live in dangerous times, but we are not the first generation
of Americans to face threats to our security. Like those before us,
we will be judged by future generations on how we react to this crisis.
And by that I mean not just whether we win … but also
whether, as we fight that war, we safeguard for our citizens the
very liberties for which we are fighting.[1]

Robert Swan Mueller III am 13. Juni 2003
Director, Federal Bureau of Investigation

Wesentliche Ergebnisse

1. „Staatstrojaner" sind ein außerordentlich eingriffsintensives Instrument. Ihr Einsatz in Form der **Online-Durchsuchung geht** hinsichtlich der Eingriffstiefe **noch über die akustische Wohnraumüberwachung hinaus**: Wer Rechner und Smartphones überwacht, der kann deren Mikrofone aktivieren und alle Datenspeicher auslesen, weiß also nahezu alles über die Zielperson. Daher stellt die Online-Durchsuchung gegenüber dem „Großen Lauschangriff" ein Mehr dar, kein Aliud oder gar ein Minus.

2. Die vorgesehene Rechtsgrundlage zur **Online-Durchsuchung** ist insbesondere wegen ihres allzu weiten Straftatenkatalogs **verfassungsrechtlich nicht zu rechtfertigen**, denn sie steht mit den Vorgaben des BVerfG (BVerfGE 120, 274) nicht im Einklang.

3. Die vorgesehene Rechtsgrundlage zur **Quellen-TKÜ** geht ebenfalls über den Rahmen dessen hinaus, was das BVerfG als Eingriff allein in Art. 10 Abs. 1 GG für zulässig gehalten hat. Die geplanten Maßnahmen nach § 100a Abs. 1 Satz 2 und 3 StPO-E beziehen sich nicht nur auf die laufende Kommunikation und stellen daher gerade keine Quellen-TKÜ, sondern eine **verfassungswidrige** Online-Durchsuchung dar.

---

1 Wir leben in gefährlichen Zeiten, aber wir sind nicht die erste Generation von Amerikanern, die sich mit Gefahren für ihre Sicherheit konfrontiert sieht. Wie die Menschen früher, werden auch wir von späteren Generationen danach beurteilt werden, wie wir auf diese Krise reagieren. Und damit meine ich nicht die Frage, ob wir gewinnen, sondern ob wir – während wir diesen Krieg führen – unseren Bürgern ebenjene Freiheiten bewahren, für die wir Krieg führen. – Zitiert nach https://archives.fbi.gov/archives/news/speeches/protecting-americans-against-terrorism (letzter Abruf: 28. Mai 2017), Übersetzung des Verfassers.

4. Gravierende Bedenken bestehen auch gegen die verfahrensrechtliche Ausgestaltung des Einsatzes von Staatstrojanern: Die §§ 100a ff. StPO stellen in keiner Weise sicher, dass die von den Ermittlungsbehörden einzusetzende Überwachungs-Software Mindestanforderungen an die Datensicherheit und Resistenz gegen Manipulationsversuche erfüllen. Hier **fehlen Regelungen** sowohl **über die** an Staatstrojaner zu stellenden **technischen Anforderungen**, die wenigstens im Verordnungswege erlassen werden müssen, als auch über eine **obligatorische unabhängige Prüfung**, dass ein Staatstrojaner diese Anforderungen tatsächlich erfüllt.

5. Zudem schaffen die §§ 100a, 100b StPO-E ein massives Interesse für Sicherheitsbehörden, die Cyber-Sicherheit weltweit zu schwächen (!), um Systeme von Zielpersonen gegebenenfalls gem. §§ 100a ff. StPO-E „hacken" zu können. Die gesellschaftlichen Folgen einer solchen **Kultur der kalkulierten IT-Unsicherheit** können erheblich sein, wie jüngst der Ausbruch des „wannacry"-Trojaners deutlich gemacht hat. Diese Fehlanreize sollten durch ein bisher **fehlendes Verbot der Ausnutzung von Sicherheitslücken** verhindert werden, die auch den Herstellern noch unbekannt sind. Hierzu wird unten ein Formulierungsvorschlag gemacht.

6. Schließlich enthält die Formulierungshilfe **unzureichende Regelungen zum Schutz von Berufsgeheimnisträgern**, insbesondere Journalistinnen und Journalisten. Denn sie schließt Eingriffe ihnen gegenüber nicht zuverlässig aus, sondern überlässt solche Maßnahmen einer nicht zu prognostizierenden Abwägungsentscheidung.

7. Die vorgesehenen Maßnahmen sind schließlich auch **in keiner Weise eilbedürftig**, da für den Bereich der Terrorismusabwehr bereits Rechtsgrundlagen im BKAG für den Einsatz von Staatstrojanern in Kraft sind, diese aber bisher kaum genutzt werden, weil ohnehin keine hinreichend praxistauglichen Trojaner zur Verfügung stehen. Zudem verfügen die Ermittlungsbehörden über vielfältige Möglichkeiten, anderweitig an die gewünschten Daten zu gelangen. Der Entwurf sollte daher insgesamt überarbeitet, in zahlreichen Punkten geändert und in der 19. Wahlperiode erneut beraten werden. In der vorliegenden Form ist die „Formulierungshilfe" mit allem Nachdruck abzulehnen.

Einzelaspekte

Eine erschöpfende Stellungnahme zu einem 30 Seiten umfassenden, inhaltlich sehr komplexen de-facto-Gesetzentwurf würde deutlich mehr Zeit erfordern als die rund zehn Tage, die den Sachverständigen zur Verfügung standen. Hingewiesen werden kann daher nur auf ausgewählte rechtlich besonders bedenkliche Vorschläge oder sonst änderungsbedürftige Aspekte des Entwurfs. Ist eine Regelung in dieser Stellungnahme nicht ausdrücklich erwähnt, so ist dies keineswegs dahingehend zu verstehen, dass sie als unbedenklich anzusehen wäre.

1.) Einführung

Der Entwurf des BMJV sieht mit Ermächtigungen für den Einsatz von staatlich kontrollierter Überwachungs-Software („Staatstrojaner“) die mit Abstand weitgehendsten Eingriffe in Grundrechte vor, die die Strafprozessordnung zur Informationsgewinnung kennt. Insbesondere die vorgesehene Online-Durchsuchung umfasst all jene Eingriffe, die bisher bereits nach § 100c StPO als akustische Wohnraumüberwachung („Großer Lauschangriff“) zulässig waren, und fügt ihnen noch weitere erhebliche Eingriffe hinzu: Durch Infektion der informationstechnischen Systeme von Beschuldigten soll nämlich ermöglicht werden

- die heimliche Auswertung der gesamten laufenden und früheren Kommunikation,

- die Auswertung aller digital gespeicherten Inhalte auf den infizierten Systemen sowie

- ein „Großer Spähangriff“ auf die Umgebung des überwachten Systems, sofern es über eine Kamera-Funktion verfügt wie heute jedes Smartphone, jedes Tablet und nahezu jeder Laptop[2].

[2] Eine solche Maßnahme wäre in einer Wohnung an Art. 13 GG zu messen und nur für präventive Zwecke zulässig (Art. 13 Abs. 4 GG). § 100b StPO-E enthält aber keine entsprechende Begrenzung, vielmehr wäre eine

Die Bedeutung der geplanten Regelung wird deutlich, wenn man sich vor Augen führt, dass Computer und Smartphones heute oft eine unermessliche Fülle an Informationen[3] enthalten: alltägliche bis intimste Emails und Nachrichten wie SMS oder WhatsApp, Terminkalender, Kontakte, Kontoumsätze, Tagebücher und Social-Media-Daten. Mit Speicherkapazitäten im Giga- bis Terabyte-Bereich enthalten sie ein weitgehendes digitales Abbild unseres Lebens. Moderne informationstechnische Systeme gleichen so einem ausgelagerten Teil des Gehirns. Erhalten Ermittlungsbehörden Zugriff auf diese Datenmengen, können sie die Besitzer der Systeme so vollständig ausspähen, dass sie sie nicht selten besser kennen als die Besitzer sich selbst. Hinzu kommt bei der Online-Durchsuchung die Möglichkeit des Live-Zugriffs – Ermittler können den Betroffenen also virtuell heimlich über die Schulter blicken und ihnen so beim Denken zuschauen. Ein staatlicher Zugriff auf einen derart umfassenden Datenbestand ist mit dem naheliegenden Risiko verbunden, dass die erhobenen Daten in einer Gesamtschau weitreichende Rückschlüsse auf die Persönlichkeit des Betroffenen bis hin zu einer Bildung von Verhaltens- und Kommunikationsprofilen ermöglichen[4].

Dieser unvergleichlich tiefe Einblick in das Wissen und Fühlen eines Menschen macht den Einsatz von Trojanern in einem Rechtsstaat unvergleichlich heikel. Wie keine andere Ermittlungsmethode erlaubt es die Online-Durchsuchung, Menschen zum Objekt der Ausspähung zu machen. Gegen keine andere Methode sind Beschuldigte – für die immerhin die Unschuldsvermutung gilt – so wehrlos, denn der direkte Zugriff auf das System dient gerade dem Zweck, Verschlüsselungsverfahren zu umgehen, also den informationellen Selbstschutz ins Leere laufen zu lassen. Keine andere Ermittlungsmethode bietet insgesamt ein vergleichbares totalitäres Potential: Selbst der „Große Lauschangriff“ beschränkt sich auf die akustische Wahrnehmung dessen, was aktuell in einer Wohnung geschieht. Wird ein Rechner oder Smartphone mit einem Trojaner infiziert, so erlaubt dies ebenfalls einen Lauschangriff auf dessen Umgebung.

---

solche Maßnahme vom Wortlaut der Norm gedeckt. Der Formulierungsvorschlag des BMJV überlässt es mithin dem einzelnen Kriminalbeamten, der eine Online-Durchsuchung durchführt, ob er die Grenzen des GG einhält und eine Funktion zur Video-Überwachung nicht aktiviert. Verfahrensrechtlich sichergestellt ist dies nirgends.

[3] Vgl. bereits BVerfGE 120, 274, 303 ff. (2008).

[4] BVerfGE 120, 274, 323.

Hinzu kommt bei der Online-Durchsuchung aber ein heimlicher Zugriff auf mitunter über Jahrzehnte angesammelte digitale Daten sowie ein großer Spähangriff, indem auf die Kameras der infizierten Systeme zugegriffen wird. Die Eingriffstiefe einer Online-Durchsuchung geht daher über die einer akustischen Wohnraumüberwachung nochmals deutlich hinaus.

Neben einer ganz gravierenden Eingriffstiefe, auf die noch einzugehen sein wird, weisen die vorgesehene Regelungen zum Einsatz von Staatstrojanern auch verfahrensrechtliche Defizite auf, die miteinander verzahnt sind: Die vorgesehenen Regelungen in der Fassung des Entwurfs überlassen es den Ermittlungsbehörden und dem Gericht, die technischen Anforderungen an Software zu definieren, die in informationstechnische Systeme eingreift, obwohl von ihnen – ebenso wie von den verfahrensrechtlichen Vorkehrungen, um ihre Einhaltung sicherzustellen – das Gewicht des Grundrechtseingriffs maßgeblich bestimmt wird. Dies ist mit dem Gebot des Grundrechtsschutzes durch Verfahrensgestaltung ebenso wie mit dem Wesentlichkeitsgrundsatz unvereinbar.

Außerdem lassen die Normen den Ermittlungsbehörden und dem Gericht Raum für den Missbrauch von Sicherheitslücken in informationstechnischen Systemen (sog. *Zero Day Exploits* oder kurz *0days*[5]) zum Zwecke der Infiltration. Dies schafft fatale Fehlanreize, weil deutsche Behörden damit ein erhebliches Interesse hätten, Sicherheitslücken in informationstechnischen Systemen nicht an die Hersteller zu melden, sodass sie geschlossen werden können, sondern sie vielmehr zu horten. Dies ist der Mechanismus, der dem jüngst unter dem Stichwort „wannacry“ bekannt gewordenen Trojaner-Ausbruch zugrunde lag: Der US-amerikanische Geheimdienst NSA hatte seit Jahren Kenntnis von der Lücke, meldete sie aber dem Hersteller Microsoft nicht, sodass dieser seine Systeme nicht nachbessern konnte. Erst nachdem Unbekannte die Informationen über die Lücke der NSA gestohlen und sie im Internet veröffentlicht hatten, gab Microsoft für einige (nicht alle) betroffenen Systeme Korrekturen heraus. Diese konnten in der kurzen Zeit bis zum Ausbruch von „wannacry“ aber nicht mehr flächendeckend

[5] Gesprochen: Oh-Days.

eingespielt werden. Dies ist nur ein Beispiel für die real bestehende Missbrauchsgefahr aus jüngster Vergangenheit.

Die vorgeschlagenen Regelungen sind vor diesem Hintergrund insgesamt verfassungsrechtlich wie rechtspolitisch deutlich misslungen.

2.) Vorgaben des Bundesverfassungsgerichts

Der unvergleichlichen Gefahren staatlicher Überwachungssoftware war sich auch das Bundesverfassungsgericht bewusst, als es im Jahre 2008 über eine Rechtsgrundlage für Staatstrojaner im Verfassungsschutzgesetz des Landes Nordrhein-Westfalen zu entscheiden hatte. Der Erste Senat leitete aus der Menschenwürdegarantie des Art. 1 Abs. 1 GG sowie dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 GG) das „Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme“ ab (BVerfGE 120, 274). Wie alle Grundrechte mit Ausnahme der Menschenwürdegarantie gilt es zwar nicht schrankenlos. Doch geht das BVerfG von einem außerordentlichen Gewicht aller Eingriffe in dieses „Computer-Grundrecht“ aus. Denn eine heimliche technische Infiltration ermöglicht die längerfristige Überwachung der Nutzung des Systems und die laufende Erfassung der entsprechenden Daten[6]. Weiter vertieft wird der Eingriff durch seine unvermeidliche Streubreite[7]. Angesichts dieser Intensität entspricht ein Grundrechtseingriff, der in dem heimlichen Zugriff auf ein informationstechnisches System liegt, selbst im Rahmen einer präventiven Zielsetzung

> *„nur dann dem Gebot der Angemessenheit, wenn bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen, selbst wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr schon in näherer Zukunft eintritt. Zudem muss das Gesetz, das zu einem derartigen*

[6] BVerfGE 120, 274, 323.
[7] BVerfG a.a.O.

Eingriff ermächtigt, den Grundrechtsschutz für den Betroffenen auch durch geeignete Verfahrensvorkehrungen sichern."[8]

Zudem muss die Gefahr ganz bestimmten besonders wichtigen Rechtsgütern drohen:

„Ein derartiger Eingriff darf nur vorgesehen werden, wenn die Eingriffsermächtigung ihn davon abhängig macht, dass tatsächliche Anhaltspunkte einer konkreten Gefahr für ein ***überragend wichtiges Rechtsgut*** *vorliegen. Überragend wichtig sind zunächst Leib, Leben und Freiheit der Person. Ferner sind überragend wichtig solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Hierzu zählt etwa auch die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen."*[9]

Das bedeutet im Umkehrschluss:

„Zum Schutz sonstiger Rechtsgüter Einzelner oder der Allgemeinheit in Situationen, in denen eine ***existentielle Bedrohungslage*** *nicht besteht, ist eine staatliche Maßnahme grundsätzlich nicht angemessen, durch die ... die Persönlichkeit des Betroffenen einer weitgehenden Ausspähung durch die Ermittlungsbehörde preisgegeben wird. Zum Schutz solcher Rechtsgüter hat sich der Staat auf andere Ermittlungsbefugnisse zu beschränken, die ihm das jeweils anwendbare Fachrecht im präventiven Bereich einräumt."*[10]

Selbst präventiv ist der Einsatz von Staatstrojanern mithin nur dann zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr vorliegen, die für Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der

[8] BVerfGE 120, 274, 326.
[9] BVerfGE 120, 274, 328 – Hervorhebung nicht im Original.
[10] BVerfGE 120, 274, 328 – Hervorhebung nicht im Original.

Menschen berührt, besteht. Andere Rechtsgüter wie etwa Eigentum oder Vermögen können einen Eingriff in das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme hingegen per se nicht rechtfertigen.

Eingriffe mittels Staatstrojanern sind hingegen nicht am „Computer-Grundrecht", sondern lediglich am Telekommunikationsgeheimnis des Art. 10 Abs. 1 GG zu messen, wenn ausschließlich „laufende Kommunikation" mitgeschnitten wird. Im Falle einer solchen Online-Durchsuchung „light" – genannt Quellen-Telekommunikationsüberwachung oder auch Quellen-TKÜ – muss jedoch durch „technische Vorkehrungen und rechtliche Vorgaben"[11] sichergestellt werden, dass sich die Datenerhebung wirklich auf die laufende Kommunikation beschränkt.

Dies ist insbesondere deswegen bedeutsam, weil eine Quellen-TKÜ technisch von einer vollumfänglichen Online-Durchsuchung nicht zu unterscheiden ist: In beiden Fällen muss das Zielsystem mittels eines Staatstrojaners infiziert werden, was die Integrität und Vertraulichkeit des Systems aufhebt. Dieser Eingriff muss sodann jedoch durch „technische Vorkehrungen und rechtliche Vorgaben" gleichsam kastriert werden, damit ausschließlich laufende Kommunikation erhoben werden kann.

Daraus ergibt sich sogleich die besondere Gefährlichkeit von Quellen-TKÜ-Maßnahmen: Sie laufen stets Gefahr, bei einer Fehlfunktion des eingesetzten Trojaners oder bewusst pflichtwidrigem oder gar nur fahrlässigem Handeln des bedienenden Personals in eine vollumfängliche Online-Durchsuchung abzugleiten, die wesentlich höheren verfassungsrechtlichen Anforderungen unterliegt[12]. Neutrale IT-Sicherheits-Experten außerhalb der Ermittlungsbehörden vertreten daher praktisch einhellig die Ansicht, dass die Anforderungen an eine Quellen-TKÜ technisch nicht zu erfüllen sind[13]. Das BVerfG hat eindeutig verlangt, dass eine solche Maßnahme zu unterbleiben hat, solange dies technisch nicht möglich ist[14].

---

[11] BVerfGE 120, 274, 309.
[12] BVerfGE 120, 274, 309.
[13] Vgl. die Wiedergabe in BVerfGE 120, 274, 309, die sich der Senat zu eigen macht.
[14] BVerfG a.a.O.

3.) Schranken-Transfer von präventiven zu repressiven Eingriffen

Bei einer Regelung für den Strafprozess ist neben der Umsetzung der oben genannten Vorgaben des BVerfG auch eine Transferleistung zu erbringen. Die Anforderungen des BVerfG an Eingriffe in das Computer-Grundrecht, also an die Online-Durchsuchung, beziehen sich unmittelbar nur auf den *präventiven* Einsatz von Staatstrojanern, weil nur dieser Gegenstand des Verfassungsbeschwerdeverfahrens war. Zu fragen ist also, welche Eingriffsschwellen für *repressive* Eingriffe in das Computer-Grundrecht gelten, denn nur solche können in der Strafprozessordnung geregelt werden (Art. 74 Abs. 1 Nr. 1 GG).

Aus verfassungsrechtlicher Perspektive ist dies vergleichsweise leicht zu beantworten: Während bei präventiven Maßnahmen unmittelbar die bedrohten Rechtsgüter und der Grad der Gefahr in die Abwägung eingestellt werden können, dient eine repressive Regelung zunächst „nur“ der Durchsetzung des staatlichen Strafanspruchs und nur mittelbar dem Rechtsgüterschutz. Da die Funktionsfähigkeit der Strafrechtspflege jedoch nicht etwa Selbstzweck ist, sondern ihrerseits allein dem Schutz von Rechtsgütern dient, ist bei Eingriffsermächtigungen zu repressiven Zwecken stets zunächst der Nebel des „Meta-Rechtsguts“ Funktionsfähigkeit der Strafrechtspflege zu lichten und zu fragen, welche Rechtsgüter durch die Strafrechtspflege letztlich konkret geschützt werden sollen.

Darüber hinaus ist insbesondere auf der Ebene der Verhältnismäßigkeit zu berücksichtigen, dass – bildhaft gesprochen – bei einem Eingriff in das Computer-Grundrecht zu präventiven Zwecken (hoffentlich) noch verhindert werden, dass „das Kind in den Brunnen fällt“, also eine Rechtsgutsverletzung tatsächlich eintritt. Ist das Kind indes bereits gestürzt, so dienen die dann nur noch möglichen repressiven Eingriffe primär der Sanktionierung der Verantwortlichen, können das Kind aber nicht wieder zum Leben erwecken, da die Rechtsgutsverletzung bereits eingetreten ist. Da wie gezeigt die Strafrechtspflege als solche keinen verfassungsrechtlichen Rang hat, sondern dieser sich alleine aus den durch sie zu schützenden Rechtsgütern ableitet, sind an Eingriffe in das Computer-Grundrecht zu repressiven Zwecken jedenfalls keine geringeren Anforderungen zu stellen als an präventive Eingriffe. Mit Blick auf die

Gewichtung von Prävention und Repression im Hinblick auf den verfolgten Rechtsgüterschutz sind bei der Verfolgung allein repressiver Ziele eher höhere Anforderungen zu stellen. Denn es wird am Ende „nur“ die Sanktionierung eines bereits irreversibel eingetretenen Rechtsgutsverstoßes verfolgt. Dass von Verfassungs wegen deutlich größere Spielräume für präventive als für repressive Eingriffe bestehen zeigt sich schließlich auch an der Wertung des Art. 13 GG (Unverletzlichkeit der Wohnung), der zu präventiven Zwecken (Art. 13 Abs. 3 GG) weitaus mehr Eingriffe zulässt als zu repressiven Zwecken (Art. 13 Abs. 4 GG).

Im Lichte dessen ist daher zunächst maßgeblich, ob die Strafnorm ihrerseits *unmittelbar* dem Rechtsgüterschutz dient, letztlich also im repressiven Gewande der Abwehr einer konkreten Gefahr dient. So mag es sich etwa in Einzelfällen des § 129a StGB (Bildung einer terroristischen Vereinigung) oder des § 89a StGB (Vorbereitung einer schweren staatsgefährdenden Gewalttat) verhalten, sofern die Planungen sich zu einer konkreten Rechtsgutsgefährdung verdichtet haben, oder auch bei Erfolgsdelikten, die das Versuchsstadium erreichen.

In der Regel aber wird bei strafrechtlichen Ermittlungen *keine konkrete Gefahr* für ein überragend wichtiges Rechtsgut mehr gegeben sein; insbesondere ist dies bei den meisten Ermittlungsverfahren wegen Organisationsdelikten gerade nicht der Fall, und liegt doch ausnahmsweise eine konkrete Gefahr vor, so ist neben der Strafverfolgung parallel auch der Bereich der Gefahrenabwehr eröffnet, dessen Zulässigkeit und Umfang sich wiederum nach den existierenden Vorgaben hierzu richtet. In den meisten hier in Rede stehenden Fällen indes, bei denen es lediglich noch um Grundrechtseingriffe zu repressiven Zwecken ohne jede konkrete Gefahr geht, müsste also die Durchsetzung des staatlichen Strafanspruchs verfassungsrechtlich zumindest von gleicher Wertigkeit sein wie die Abwehr einer konkreten Gefahr für die vom BVerfG aufgezählten Rechtsgüter. Dies wird man allenfalls bei Straftatbeständen annehmen können, die die vom BVerfG genannten „überragend wichtigen“ Rechtsgüter schützen sollen, und dies auch nur dann, wenn die Verletzungen einen erheblichen Schweregrad erreichen. Dies gebietet auch die Verfassungsrang genießende und in Art. 6 Abs. 2 EMRK verankerte

Unschuldsvermutung, die im Rahmen der Verhältnismäßigkeitsprüfung bei Ermittlungseingriffen zu beachten ist.

4.) Die Regelung zur Online-Durchsuchung (§§ 100b, 100c StPO-E)

Gemessen insbesondere an diesen Vorgaben ist die vorgesehene Ermächtigungsgrundlage für Online-Durchsuchungen verfassungsrechtlich nicht zu rechtfertigen.

a) Straftaten-Katalog

So überschreitet insbesondere der im Entwurf vorgesehene Katalog von Straftaten (§ 100b Abs. 2 StPO-E), zu deren Aufklärung eine Online-Durchsuchung nach § 100b Abs. 1 StPO-E zulässig sein soll, den Rahmen des verfassungsrechtlich Möglichen. Denn der Straftatenkatalog, der weitgehend dem der klassischen Telekommunikationsüberwachung (§ 100a Abs. 2 StPO) entspricht, enthält viele Straftatbestände, die Rechtsgüter schützen, für die das BVerfG selbst eine präventive Online-Durchsuchung **nicht** für zulässig hält. Mit anderen Worten dürfte eine Online-Durchsuchung in diesen Fällen nicht einmal zur Abwehr einer konkret drohenden Gefahr für dieses Rechtsgut eingesetzt werden. Um es noch deutlicher zu formulieren: Wenn allein eine Online-Durchsuchung die Gefahr abwenden könnte, so müsste der Staat von Verfassungs wegen die drohende Rechtsgutsverletzung – etwa eine Verletzung des Vermögens – gleichwohl geschehen lassen. Wenn jedoch selbst eine potentiell noch abzuwendende Verletzung eines bestimmten Rechtsguts eine Online-Durchsuchung nicht rechtfertigen könnte, dann vermag die bloße Verfolgung einer (vermuteten) Verletzung desselben Rechtsguts dies umso weniger – schließlich ist „das Kind bereits in den Brunnen gefallen“, das Rechtsgut nicht mehr zu retten. Folglich ist eine repressive Online-Durchsuchung zur Verfolgung von Straftaten schlechthin unzulässig, wenn durch die mutmaßliche Straftat lediglich Rechtsgüter verletzt wurden, zu deren Schutz vor konkreter Gefahr eine Online-Durchsuchung nicht angeordnet werden dürfte. Dies betrifft alle Rechtsgüter mit Ausnahme der vom BVerfG als überragend wichtige Rechtsgüter bezeichneten:

> *„Überragend wichtig sind zunächst Leib, Leben und Freiheit der Person. Ferner sind überragend wichtig solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Hierzu zählt etwa auch die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen.“*[15]

Bei den Katalogtaten aus dem StGB, die gemäß § 100b Abs. 2 Nr. 1 StPO-E eine Online-Durchsuchung sollen rechtfertigen können, betrifft dies insbesondere solche, die primär Vermögen oder Eigentum schützen, also

- § 100b Abs. 2 Nr. 1 lit. c StPO-E (Geld- und Wertzeichenfälschung),
- § 100b Abs. 2 Nr. 1 lit. h StPO-E (Bandendiebstahl),
- § 100b Abs. 2 Nr. 1 lit. i und j StPO-E (bestimmte Formen von Raub oder räuberischer Erpressung, sofern es nicht tateinheitlich zu Körperverletzungen gekommen ist),
- § 100b Abs. 2 Nr. 1 lit. k StPO-E (Qualifikationen der Hehlerei)
- § 100b Abs. 2 Nr. 1 lit. l StPO-E (Geldwäsche u. ä.)

Ebenso zweifelhaft ist der Bezug zum Katalog der vom BVerfG genannten „überragend wichtigen“ Rechtsgüter bei den Straftaten gegen das Asyl- und Aufenthaltsgesetz. Jedenfalls die oben genannten Katalogtaten sowie die Taten der § 100b Abs. 2 Nr. 2 und 3 StPO-E sollten daher ersatzlos entfallen.

b) Verhältnismäßigkeit im engeren Sinne

Zudem ist die Regelung auch insoweit unzulänglich, als sie nicht hinreichend sicherstellt, dass es sich bei den mutmaßlichen Straftaten, zu deren Verfolgung eine Online-Durchsuchung möglich sein soll, auch tatsächlich um äußerst schwere Straftaten gegen die betreffenden Rechtsgüter handelt. Zwar soll nach § 100b Abs. 1 Nr. 2 StPO-E zu prüfen sein, ob „die Tat auch im Einzelfall besonders schwer wiegt“. Diese Prüfung durch

[15] BVerfGE 120, 274, 328.

die Kammer bzw. den Senat (vgl. § 100e Abs. 2 StPO) ist indes in keiner Weise angeleitet, weil jeder Hinweis darauf fehlt, wann dieses Kriterium erfüllt sein soll. So bleibt die Subsumtion unter dieses Tatbestandsmerkmal letztlich eine Frage des richterlichen Bauchgefühls, ob eine Tat nach bestehender Akten- und damit Verdachtslage „wirklich schlimm“ war oder nicht.

Im Bereich der Strafverfolgung gibt es indes ein vergleichsweise einfach zu handhabendes Kriterium für die Schwere einer Tat: die im Einzelfall zu erwartende Strafe. Die Einschätzung der Straferwartung ist im Bereich ermittlungsrichterlicher Entscheidungen auch gängige Praxis, nämlich bei der Entscheidung über Anträge auf Erlass eines Haftbefehls, wo die Straferwartung zentralen Einfluss auf die Frage hat, ob Fluchtgefahr (§ 112 Abs. 2 Nr. 2 StPO) anzunehmen ist oder nicht. Auch Spruchrichter haben aus ihrer täglichen Praxis in aller Regel in gutes Judiz, welche Strafe in etwa angemessen sein könnte. Freilich sind im Ermittlungsverfahren noch nicht alle Umstände bekannt, die in einer Hauptverhandlung für die Strafhöhe Bedeutung erlangen können. Dem kann jedoch durch plausible Annahmen über nach dem Stand der Ermittlungen wahrscheinliche Umstände mühelos begegnet werden – auch dies ist ständige Praxis im Ermittlungsverfahren. Daher sollte der bisher konturenlose Begriff der „besonderen Schwere der Tat“ durch ein Tatbestandsmerkmal der im Einzelfall zu erwartenden Strafe präzisiert werden. Angesichts der beispiellosen Eingriffstiefe der Online-Durchsuchung erscheint diese Maßnahme jedenfalls nicht unterhalb einer konkret zu erwartenden Freiheitsstrafe von 5 Jahren angemessen. Milderungen wegen erheblich verminderter Schuldfähigkeit sollten zur Vereinfachung außer Betracht bleiben, weil sie im Ermittlungsverfahren typischerweise noch nicht ohne Weiteres bestimmbar sind.

Formulierungsvorschlag:

An § 100b Abs. 1 werden folgende Sätze 2 und 3 angefügt:

„Eine Tat wiegt besonders schwer (Satz 1 Nr. 2), wenn im konkreten Fall nach dem jeweiligen Stand der Ermittlungen eine Freiheitsstrafe nicht unter fünf Jahren zu erwarten ist. Milderungen gemäß §§ 21, 49 Absatz 1 StGB bleiben außer Betracht.“

c) Wertungswidersprüche beim Kernbereichsschutz

Wie oben bereits gezeigt geht die Eingriffstiefe der Online-Durchsuchung über die der akustischen Wohnraumüberwachung deutlich hinaus – nicht zuletzt, weil praktisch alle im Wege einer akustischen Wohnraumüberwachung zu erwartenden Kenntnisse auch mittels einer Online-Durchsuchung zu erlangen sind, indem heimlich das Mikrofon eines Laptops oder Smartphones aktiviert wird. Die Online-Durchsuchung stellt gegenüber dem „Großen Lauschangriff" also ein – erhebliches – Plus dar, kein Aliud oder gar Minus.

Diesem Stufenverhältnis trägt indes die Regelung des Schutzes des Kernbereichs privaten Lebensgestaltung in § 100d Abs. 3 und 4 StPO-E nicht ausreichend Rechnung. Für die akustische Wohnraumüberwachung ist – zu Recht – ein vergleichsweise strenger Schutz des Kernbereichs vorgesehen. Maßnahmen dürfen nur angeordnet werden, soweit auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass durch die Überwachung Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, nicht erfasst werden. Insbesondere ist die Maßnahme „unverzüglich zu unterbrechen, wenn sich während der Überwachung Anhaltspunkte dafür ergeben, dass Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden" (§ 100d Abs. 4 Satz 2 StPO-E) – mit anderen Worten muss „live" überwacht werden. Nach § 100d Abs. 3 StPO-E soll ein vergleichbarer Schutz für die Online-Durchsuchung hingegen nicht gelten. Hier ist lediglich „soweit möglich, technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden". Mit anderen Worten soll für die schwerer wiegende Maßnahme der Online-Durchsuchung ein weniger zuverlässiger und weniger weitgehender Schutz des Kernbereichs privater Lebensgestaltung gelten – das leuchtet nicht ein. Die Differenzierung in § 100d Abs. 3 und 4 StPO-E sollte daher entfallen.

5.) Die Regelung zur Quellen-TKÜ (§ 100a StPO-E)

Noch weiter als die Regelung zur Online-Durchsuchung verfehlt die vorgeschlagene Norm zur Quellen-TKÜ die Vorgaben insbesondere aus der Entscheidung des BVerfG zur Online-Durchsuchung (BVerfGE 120, 274). Wie dargestellt ist *conditio sine qua non* einer

nur an Art. 10 Abs. 1 GG zu messenden Quellen-TKÜ – sonst liegt eine am „Computer-Grundrecht“ zu messende Online-Durchsuchung vor –, dass ausschließlich „laufende Kommunikation“ erhoben wird[16]. Hierüber setzt sich der Entwurf jedoch hinweg: Gemäß § 100a Abs. 1 Satz 3 StPO-E soll über die laufende Kommunikation hinaus auch die Erhebung „gespeicherter Inhalte und Umstände der Kommunikation“ – also das Auslesen quasi „kondensierter“ Kommunikation – unter den erleichterten Voraussetzungen der Quellen-TKÜ ausgelesen werden dürfen. Dies steht in einem offenen Widerspruch zu den Vorgaben des BVerfG, welches wie gezeigt nur die Erhebung *laufender* und nicht früherer Kommunikation aus dem Schutzbereich des Grundrechts auf Integrität und Vertraulichkeit informationstechnischer Systeme herausdefiniert hat.

Dessen war sich die Bundesregierung durchaus bewusst. Zur Begründung verweist die „Formulierungshilfe“ indes auf eine klassische Analogie: Ebenso wie bei laufender Kommunikation erscheint es ihnen auch bei früherer Kommunikation „verfassungsrechtlich nicht geboten, die wegen der besonderen Sensibilität informationstechnischer Systeme ... aufgestellten höheren Anforderungen des Bundesverfassungsgerichts [für Eingriffe in das Computer-Grundrecht] anzuwenden“[17]. Indes ist bereits die Figur der Quellen-TKÜ für laufende Kommunikation wie dargestellt eine Ausnahme von der Regel, dass Trojaner-Einsätze einen Eingriff in dieses Grundrecht darstellen; hinzu kommt, dass diese Ausnahme aus technischer Sicht ihrerseits eine fragwürdige, da kontrafaktische ist. Und Ausnahmen können gerade nicht analog angewendet werden, sondern sind restriktiv auszulegen. Dies lässt es unvertretbar erscheinen, aufgrund letztlich willkürlicher Überlegungen zur „Gebotenheit“ eines Grundrechtsschutzes die klaren Vorgaben des BVerfG zur Abgrenzung zwischen Online-Durchsuchung und Quellen-TKÜ zu übergehen.

Neben das rechtstechnische tritt indes ein weiteres, informationstechnisches Argument. Selbst die Entwurfsverfasser räumen ein, dass nicht sämtliche gespeicherte Kommunikation als Quellen-TKÜ auslesbar sein soll, sondern nur solche

---

[16] Vgl. zu Begriff und Inhalt eingehend *Buermeyer* StV 2013, 470.
[17] „Formulierungshilfe“, Seite 20.

Kommunikationsinhalte, die nach Erlass eines Beschlusses gem. § 100a StPO gespeichert wurden. Um diese Prüfung ausführen zu können, müsste der Trojaner – wie die Entwurfsbegründung wiederum zugesteht – zunächst *alle* gespeicherten Kommunikations-Inhalte auslesen und auswerten, um entscheiden zu können, welche davon nach dem Beginn der Maßnahme gespeichert wurden, sodass sie als Quellen-TKÜ erhoben werden können. In dieser *vollumfänglichen*, zeitlich naturgemäß nicht begrenzten Auswertung der gespeicherten Kommunikationsinhalte läge jedoch bereits eine dem Staat zuzurechnende Kenntnisnahme und damit eine Online-Durchsuchung, auch wenn die Daten nicht ausgeleitet, sondern noch „vor Ort" auf dem infizierten System der Zielperson analysiert werden. Mit anderen Worten schlägt der Entwurf eine stillschweigende Online-Durchsuchung vor, um festzustellen, welche ehemaligen Kommunikationsinhalte der Staatstrojaner unter den leichteren Voraussetzungen einer Quellen-TKÜ ausleiten darf. Ein solcher Taschenspielertrick des Gesetzgebers dürfte vor dem BVerfG kaum Bestand haben, zumal es sich der Sache nach um eine Ausweitung der vom Ersten Senat erkennbar als eng umrissene Ausnahme von der Online-Durchsuchung konzipierten Quellen-TKÜ handelt.

Schließlich ist zu berücksichtigen, dass eine solche Ausweitung der Quellen-TKÜ auf frühere Kommunikation auch im Tatsächlichen auf allzu schwankendem Grund stünde. Denn schon ein aus welchen Gründen auch immer falscher Zeitstempel einer gespeicherten Nachricht würde dazu führen, dass Inhalte ausgelesen würden, die vor Beginn einer Maßnahme gespeichert wurden. Dies jedoch würde bewirken, dass statt der angeordneten Quellen-TKÜ eine „irrtümliche" Online-Durchsuchung durchgeführt würde. Der Irrtum ändert jedoch nichts an der damit verbundenen Eingriffstiefe und die anzusetzenden verfassungsrechtlichen Anforderungen an eine Rechtfertigung dieses Eingriffs.

Angesichts all dessen muss § 100a Abs. 1 Satz 3 StPO entfallen; gleiches gilt für dessen verfahrensrechtliche Umsetzung in § 100a Abs. 5 Nr. 1 lit. b StPO-E. Dies ließe sich gesetzestechnisch wie folgt erreichen:

Formulierungsvorschlag

1. § 100a Abs. 1 Satz 3 wird gestrichen.

2. § 100a Abs. 5 Nr. 1 wird wie folgt gefasst:

„1. ausschließlich die laufende Telekommunikation (Absatz 1 Satz 2) überwacht und aufgezeichnet werden kann,“

6.) Mangelhafte verfahrensrechtliche Sicherungen des Trojaner-Einsatzes

Die Eingriffsbefugnisse der § 100a Abs. 5, § 100b Abs. 1 StPO-E enthalten zwar bestimmte an der Rechtsprechung des BVerfG orientierte Begrenzungen des „Eingreifens“, etwa eine Beschränkung von Veränderungen auf das Notwendige oder einen Schutz vor unberechtigten Zugriffen durch Dritte. Diese als solche begrüßenswerten Regelungen finden indes im Gesetz keinerlei verfahrensrechtliche Absicherung. Gemessen an den Anforderungen an die Anordnung und ihre Begründung (§ 100e Abs. 3 und 4 StPO-E) muss das „technische Mittel“, dessen Einsatz beabsichtigt ist – also immerhin der einzusetzende Staatstrojaner (!) – nicht einmal benannt, geschweige denn in seinen technischen Spezifikationen näher bezeichnet werden. Dies ermöglicht nach dem Wortlaut des Entwurfs den Einsatz beliebiger Staatstrojaner nach Gutdünken der Ermittlungsbehörden, sofern ein Beschluss über eine Maßnahme einmal erlangt werden kann. Das ist angesichts der erheblichen Eingriffstiefe der Online-Durchsuchung, aber auch der massiven Gefahren einer schleichenden Ausweitung eines Quellen-TKÜ hin zu einer Online-Durchsuchung, denen nur durch die Gestaltung des Trojaners entgegengewirkt werden kann, in jeder Hinsicht unangemessen. Jedenfalls nach den Vorstellungen des Entwurfs soll offenbar jede Steckdose[18] strengeren Anforderungen an die technisch sichere Gestaltung unterliegen als eine Software, die zur Ausspähung von Bürgerinnen und Bürgern eingesetzt werden soll. Das erscheint in einem Rechtsstaat unvorstellbar.

[18] Vgl. nur https://de.wikipedia.org/wiki/IEC_60309.

Die Verantwortung für die Prüfung der technischen Beschaffenheit des einzusetzenden Staatstrojaners kann auch nicht auf die Richter abgewälzt werden, die die Maßnahme anordnen sollen. Zum einen müssten sie gezielt Rückfragen stellen, um überhaupt zu erfahren, welches technische Mittel eingesetzt werden soll und wie dieses im Einzelnen beschaffen ist. Zum anderen kann von dem zuständigen Ermittlungsrichter (bei der Quellen, TKÜ, vgl. § 100e Abs. 1 StPO-E) und der zuständigen Kammer bzw. dem Senat (bei der Online-Durchsuchung, vgl. § 100e Abs. 2 StPO-E) nicht ernsthaft verlangt werden, eine EDV-technische Überprüfung des beabsichtigten Staatstrojaners selbst vorzunehmen. Eine externe Prüfung wiederum dürfte angesichts der hierfür notwenigen Zeit – wenigstens Tage, wohl eher Wochen – in vielen Fällen den Zweck der Maßnahme gefährden. Die Verantwortung hierfür wird kaum eine ein Gericht auf sich nehmen wollen, sodass man sich im Zweifel auf Beteuerungen der antragstellenden Staatsanwaltschaft verlassen wird, mit dem Staatstrojaner habe schon alles seine rechte Ordnung. Im Ergebnis ist daher zu besorgen, dass die Einhaltung der in §§ 100a, 100b StPO-E genannten, aber auch weiterer aus der Perspektive der Informationssicherheit gebotener technischer Anforderungen an Staatstrojaner allenfalls von den Ermittlungsbehörden (wohlwollend) geprüft werden wird.

Aus der Perspektive des Schutzes der Integrität und Vertraulichkeit informationstechnischer Systeme (Art. 1 Abs. 1, Art. 2 Abs. 1 GG) ist ein derart blindes Vertrauen in die von den Ermittlungsbehörden einzusetzenden Staatstrojaner ohne einen rechtsstaatlich ausreichenden Überprüfungsmechanismus nicht hinnehmbar. Dies gilt insbesondere angesichts des Umstands, dass die Software nach dem Wortlaut des Gesetzes durchaus von einem externen Anbieter stammen kann, sodass die Ermittlungsbehörden mitunter selbst nicht mit Sicherheit einzuschätzen vermöchten, welche Funktionen die einzusetzende Software ausführt. Ausdrücklich zu begrüßen ist in diesem Kontext, dass sich das Bundeskriminalamt nach Presseberichten um die Eigenprogrammierung einer Überwachungssoftware bemüht; für den Bereich der sogenannten Quellen-TKÜ soll diese einsatzbereit sein[19]. Der vorliegende Gesetzentwurf schließt aber gerade nicht aus, dass auch – oder gar ausschließlich – Staatstrojaner zum

[19] https://www.heise.de/newsticker/meldung/Quellen-Telekommunikationsueberwachung-Neuer-Bundestrojaner-steht-kurz-vor-Einsatzgenehmigung-3113444.html

Einsatz kommen, die weder vom BKA selbst programmiert noch extern und unabhängig geprüft sind.

Zwar mögen die technischen Details eines Staatstrojaners nicht unbedingt durch formelles Gesetz zu regeln sein. Zumindest aber muss das Gesetz im Lichte des Wesentlichkeitsgrundsatzes eine unabhängige technische Überprüfung der einzusetzenden Staatstrojaner vorschreiben. Die durch einen Staatstrojaner zu erfüllenden Spezifikationen könnten etwa im Verordnungswege durch das Bundesamt für Sicherheit in der Informationstechnik vorgegeben werden. Der Gesetzentwurf sollte hierzu um eine entsprechende Verordnungsermächtigung ergänzt werden. Zudem sollte ausschließlich der Einsatz erfolgreich geprüfter Staatstrojaner zulässig sein. Eine entsprechende Darlegung dessen sollte in den Katalog der obligatorischen Inhalte einer Anordnung (§ 100e Abs. 3 und 4 StPO-E) aufgenommen werden.

7.) Fehlanreize, die die Datensicherheit insgesamt schwächen

Zumindest ebenso schwer wie die geschilderten rechtlichen Bedenken gegen die fehlende Prüfung der Staatstrojaner wiegen indes die fatalen Fehlanreize, die die Norm für die Arbeit der Bundesbehörden – namentlich die im Aufbau befindliche „ZITIS“ (Zentrale Stelle für Informationstechnik im Sicherheitsbereich) – mit sich bringt. Nach §§ 100a, 100b StPO-E sollen Ermittlungsbehörden in informationstechnische Systeme „eingreifen“ dürfen, um aus ihnen Daten zu erheben. Hierzu ist denklogisch ein „Fuß in der Tür“ erforderlich, also das Aufbringen einer hoheitlichen Software, die Daten ausliest und an das BKA übermittelt. Solche Software-Lösungen werden allgemein als Staatstrojaner bezeichnet.

Der Entwurf definiert indes nicht weiter, wie der Staatstrojaner auf das Zielsystem aufgebracht werden darf. Denkbar sind insbesondere folgende Wege[20]:

[20] Vertiefend zu den technischen Grundlagen *Buermeyer* HRRS 2007, S. 154 ff.

- Aufspielen durch Hoheitsträger, etwa bei einer Grenzkontrolle

- Aufspielen durch Hoheitsträger durch heimliches Betreten der Räumlichkeiten, in denen sich das System befindet

- Ausnutzen der Unaufmerksamkeit des berechtigten Nutzers, etwa indem man ihm einen EMail-Anhang mit einem (getarnten) Infektions-Programm in der Hoffnung zuspielt, dass er ihn ausführen werde

- Aufspielen durch Ausnutzen von Sicherheitslücken des genutzten Systems, etwa indem der berechtigte Nutzer zum Aufruf einer speziell präparierten WWW-Seite animiert wird, deren bloße Ansicht aufgrund von Sicherheitslücken zur Infektion des Zielsystems führt (sogenannte *drive by downloads*)

Es erschließt sich unmittelbar, dass die rechtliche Bewertung der Zugriffe völlig unterschiedlich ausfällt: Das Betreten von Räumlichkeiten zur Infektion von Systemen ist im Lichte von Art. 13 Abs. 1 GG ohne eine (bisher fehlende) spezifische Ermächtigungsgrundlage hierzu schlechthin rechtswidrig. Das Aufspielen etwa bei einer Grenzkontrolle ist hingegen als solches unbedenklich, ebenso das Zusenden eine E-Mail mit einem getarnten Staatstrojaner (kriminalistische List), soweit dieser E-Mail-Anhang keine Sicherheitslücken ausnutzt.

Die Infektion des Zielsystems durch Ausnutzen von Sicherheitslücken – wiewohl vom Wortlaut der §§ 100a, 100b StPO-E gedeckt – führt hingegen zu gravierenden Fehlanreizen: Wenn Bundesbehörden solche Lücken ausnutzen dürfen, so haben sie ein durchaus nachvollziehbares Interesse daran, ein „Arsenal“ von Sicherheitslücken aufzubauen, um im Falle des Falles eine Zielperson angreifen zu können. Dieses Interesse wird sie jedoch davon abhalten, gefundene oder gar auf dem Schwarzmarkt angekaufte Sicherheitslücke den jeweiligen Herstellern der IT-Systeme mitzuteilen, damit die Lücken geschlossen werden können. So entstehen Anreize für Bundesbehörden, ihnen bekannte Sicherheitslücken gerade nicht schließen zu lassen, sondern sie lieber zu horten.

Solange aber die Lücken nicht von den Herstellern der Systeme geschlossen werden können, weil sie von ihnen keine Kenntnis erlangen, können natürlich nicht nur Bundesbehörden diese Lücken für den Einsatz von Staatstrojanern ausnutzen. Vielmehr kann jeder, der sie findet oder seinerseits auf dem Schwarzmarkt für *0days* kauft, die Lücken zur Infiltration informationstechnischer Systeme missbrauchen – insbesondere auch Cyber-Kriminelle, die es beispielsweise darauf anlegen könnten, die betroffenen Systeme zum Teil eines Botnetzes zu machen oder Zahlungsdaten für Online-Überweisungen abzugreifen. Im Ergebnis würden Bundesbehörden mitunter viele Millionen Nutzerinnen und Nutzer von IT-Systeme weltweit, die von der jeweiligen Lücke betroffen sind, einem fortbestehenden Risiko von Cyber-Angriffen aussetzen, um Sicherheitslücken im Einzelfall selbst für Maßnahmen nach §§ 100a, 100b StPO ausnutzen zu können. – Und all dies nur, um mit Blick auf die verfolgte Sanktionierung einer Einzelperson wegen einer vermuteten Straftat den Sachverhalt aufzuklären oder den Aufenthaltsort des Beschuldigten zu ermitteln. Das weltweite Missbrauchsrisiko, das hier durch ein Horten von Sicherheitslücken eingegangen wird, steht in keinem ausgewogenen Verhältnis zu dem verfolgten Zweck (bessere Strafverfolgung im Einzelfall).

Eine solche aus der Sicht einer Ermittlungsbehörde noch nachvollziehbare Güterabwägung verbietet sich aus der Perspektive des Gesetzgebers, der das Wohl der Allgemeinheit in den Blick zu nehmen hat. Nicht zuletzt hat sich die Bundesregierung politisch zur Förderung der IT-Sicherheit bekannt[21]. Damit sind Anreize für Bundesbehörden, die Cyber-Sicherheit in Deutschland und weltweit im Interesse einer möglicherweise einmal erforderlichen Gefahrenabwehr zu schwächen, schlechthin unvereinbar.

Die §§ 100a, 100b StPO-E sollten daher um ein explizites Verbot des Einsatzes von dem Hersteller eines informationstechnischen Systems bisher unbekannten Sicherheitslücken (sog. *0days*) ergänzt werden, um sicherzustellen, dass sich alle

[21] Vgl. die sog. Cyber-Sicherheitsstrategie für Deutschland 2016, abzurufen auf http://www.bmi.bund.de/DE/Themen/Sicherheit/IT-Cybersicherheit/Cyber-Sicherheitsstrategie/cyber-sicherheitsstrategie_node.html

Bundesbehörden darum bemühen, ihnen bekannte Sicherheitslücken durch die Hersteller der Systeme so schnell wie möglich schließen zu lassen. Eine Sicherheitslücke, die dem Hersteller bereits bekannt ist, aber beispielsweise wegen Nachlässigkeit des Systembetreibers noch nicht geschlossen wurde, kann hingegen auch aus der Perspektive der IT-Sicherheit ausgenutzt werden. Gleiches gilt für Sicherheitslücken, die nicht auf Fehlern der Hersteller beruhen, sondern auf einer individuellen fehlerhaften Einrichtung des informationstechnischen Systems.

Formulierungsvorschlag

An § 100a Abs. 5 wird der folgende Satz 2 angefügt:

Für den Einsatz des technischen Mittels dürfen Sicherheitslücken des informationstechnischen Systems, die auf die fehlerhafte Gestaltung von Systemkomponenten durch ihre Hersteller zurückgehen, nur ausgenutzt werden, wenn die Sicherheitslücken den jeweiligen Herstellern bereits bekannt sind.

8.) Unzureichender Schutz von Berufsgeheimnisträgern, namentlich der Presse

Nach § 100d Abs. 5 StPO des Entwurfs sollen Online-Durchsuchung und akustische Wohnraumüberwachung in „den Fällen des § 53“ StPO nicht zulässig sein. Was auf den ersten Blick wie eine begrüßenswerte Regelung zum Schutz von Berufsgeheimnisträgern erscheint, erweist sich bei genauerer Betrachtung als jedenfalls rechtstechnisch wenig gelungen. Denn die Formulierung in „den Fällen“ des § 53 StPO könnte jedenfalls so verstanden werden, dass die in § 53 Abs. 1 Satz 1 genannten Personen nicht etwa umfassend geschützt sind, sondern nur, soweit tatsächlich ein Fall der berechtigten Zeugnisverweigerung nach § 53 StPO vorläge. Dies wiederum würde auch auf die Verhältnismäßigkeitsprüfung des § 53 Abs. 2 Satz 2 StPO verweisen und dazu führen, dass jedenfalls in vielen Fällen der Ausschluss von Online-Durchsuchung und „Großem Lauschangriff“ ausgerechnet gegenüber Journalistinnen und Journalisten nur wenig Wirkung entfalten würde.

Aus der Perspektive der Pressefreiheit – insbesondere des vom Schutzbereich des Art. 5 Abs. 1 GG umfassten Schutzes des Vertrauensverhältnisses zwischen Journalist und

Quelle – wäre ein solches Ergebnis fatal. Der Gesetzentwurf berücksichtigt hier nicht hinreichend, dass für die nach der ständigen Rechtsprechung des BVerfG von Art. 5 Abs. 1 GG geschützte [22] journalistische Recherche ein *absolutes* Vertrauen in den Informantenschutz erforderlich ist. Ein Schutz von Informantinnen und Informanten allein nach Maßgabe einer im Einzelfall nicht zu prognostizierenden Abwägung kommt aus der Sicht eines potentiellen Informanten einem insgesamt fehlenden Schutz gleich, weil er sich nicht darauf verlassen kann, dass seine Kommunikation mit einer Journalistin oder einem Journalisten nicht ausgespäht werden darf. Dies wiegt im Bereich der journalistischen Recherche umso schwerer, als potentielle Informanten – anders als etwa Menschen, die medizinische Behandlung benötigen – auf den Kontakt zur Presse im Zweifel verzichten werden.

Dabei ist auch in Rechnung zu stellen, dass Informanten brisante Informationen auch vergleichsweise risikolos ins Netz stellen können, wobei die Kollateralschäden für die von Leaks betroffenen Personen typischerweise erheblich höher sind als bei verantwortlichem „Durchstechen" von Informationen an die Presse, die Persönlichkeitsrechte berücksichtigen kann. Daraus folgt ein erhebliches öffentliches Interesse daran, dass Leaks an verantwortungsbewusste Journalistinnen und Journalisten und nicht etwa an Plattformen wie Wikileaks erfolgen. Gerade angesichts dessen erscheint der nur relative – und damit im Ergebnis nicht hinreichend belastbare – Ausschluss von Journalistinnen und Journalisten anachronistisch.

Formulierungsvorschlag

§ 100d Abs. 5 Satz 1 wird wie folgt gefasst:

Gegenüber den in § 53 Abs. 1 Satz 1 genannten Personen sind Maßnahmen nach den §§ 100b und 100c unzulässig; ergibt sich während oder nach Durchführung der Maßnahme, dass eine solche Person von der Maßnahme betroffen ist, gilt Absatz 2 entsprechend.

---

[22] Geschützt sind namentlich die Geheimhaltung der Informationsquellen und das Vertrauensverhältnis zwischen Presse und Informanten (vgl. BVerfGE 100, 313 <365> m.w.N.). „Dieser Schutz ist unentbehrlich, weil die Presse auf private Mitteilungen nicht verzichten kann, diese Informationsquelle aber nur dann ergiebig fließt, wenn sich der Informant grundsätzlich auf die Wahrung des Redaktionsgeheimnisses verlassen kann." (BVerfGE 117, 244 <259>, vgl. bereits BVerfGE 20, 162 <176, 187>; 36, 193 <204>).

9.) Zeitplan

Eine so gewichtige Einschränkung von Grundrechten, wie sie die StPO in der Fassung der „Formulierungshilfe“ erlauben würde, bedarf der eingehenden Diskussion in der Öffentlichkeit wie auch im Parlament. Eine solche Diskussion schein dem Verfasser angesichts der wenigen Tage, die für die Vorbereitung der Anhörung zur Verfügung stehen, und den wenigen Wochen bis zum Ende der Legislaturperiode nicht mehr realistisch. Daher ist zu fragen, ob tatsächlich ein so besonderer Zeitdruck besteht, der es rechtfertigt, die vorgeschlagenen Normen mit all ihren verfassungsrechtlichen Sollbruchstellen ohne eingehende Beratung und Diskussion zu verabschieden.

Ein Sachgrund, der zur Eile drängen könnte, ist indes nicht zu erkennen. Für den Bereich der Terrorismusabwehr verfügt das BKA bereits über analoge Rechtsgrundlagen, sodass insoweit kein zwingendes Bedürfnis für strafprozessuale Rechtsgrundlagen besteht. Im Übrigen führt der Einsatz von Verschlüsselungstechnologien zwar dazu, dass bestimmte Beweismittel nicht mehr zur Kenntnis genommen werden können. Indes verfügen die Ermittlungsbehörden insbesondere in Form von Verkehrsdatenabfragen vor allem zu Verbindungen und Standorte von Mobilfunkgeräten über weitreichende Erkenntnisquellen, die sich auch durch Einsatz von Verschlüsselung nicht verbergen lassen. Außerdem lässt sich die Mehrzahl der Erkenntnisse, die sich mittels Online-Durchsuchung und Quellen-TKÜ gewinnen ließen, auch durch einen Zugriff und die Auswertung beschlagnahmter Systeme erlangen. Bei Licht betrachtet geht es also weniger darum, Erkenntnisse *überhaupt* zu gewinnen, sondern darum, sie früher und heimlich zu bekommen. So nützlich derlei taktische Möglichkeiten sein mögen, so wenig können sie indes eine mit allzu heißer Nadel gestrickte Rechtsgrundlage für Staatstrojaner im Strafverfahren rechtfertigen.

Schließlich ist auch zu berücksichtigen, dass massive technische Probleme bei der Entwicklung bisher den Einsatz von Trojanern auf der Grundlage des BKAG auf eine einstellige Anzahl beschränkt haben. Mit anderen Worten dürfte sich eine Verzögerung der Schaffung einer Rechtsgrundlage bis in die 19. Wahlperiode in der Praxis kaum auswirken.

Schlussbemerkung

Schon angesichts des erheblichen Änderungsbedarfs in den in dieser Stellungnahme erörterten Teilen des Entwurfs sollte der Entwurf insgesamt überarbeitet werden. In der vorgesehenen Form sind die geplanten Neuregelungen mit Nachdruck abzulehnen. Dies gilt umso mehr, führt man sich vor Augen, dass die Stellungnahmen der Sachverständigen schon aus Zeitgründen nur einen Abriss der verfassungsrechtlichen, aber auch rechtspolitischen Probleme des vorliegenden Entwurfs wiedergeben können.

Berlin, den 29. Mai 2017

Dr. Ulf Buermeyer, LL.M. (Columbia)

Michael Greven
Oberstaatsanwalt
beim Bundesgerichtshof

Karlsruhe, den 29. Mai 2017

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

Hier:

Gesetzentwurf der Bundesregierung vom 22. Februar 2017, Drucksache 18/11272

Formulierungshilfe der Bundesregierung für einen Änderungsantrag der Fraktionen CDU/CSU und SPD vom 15. Mai 2017, Ausschussdrucksache 18(6)334

A. Tenor der Stellungnahme

Der Gesetzentwurf zur Schaffung einer Rechtsgrundlage für die Quellen-Telekommunikationsüberwachung und die Online-Durchsuchung in der Strafprozessordnung wird ausdrücklich begrüßt, da die staatsanwaltschaftliche Praxis dringend klare gesetzliche Vorgaben benötigt.

Seit Beginn des 21. Jahrhunderts hat die Technik der Internettelefonie und sogenannte Voice-over-IP-Dienste - wie etwa das Programm „Skype" oder der Instant Messenger „WhatsApp" - eine immer größere Bedeutung gewonnen. Eine grundlegende Anpassung der wichtigen Eingriffsrechte der Strafverfolgungsbehörden gemäß §§ 100a ff. StPO an den rasanten Fortschrift moderner Kommunikationstechnologien ist jedoch bislang unterblieben.

B. Forderungen der Praxis

1. Bereits im September 2012 hat die Abteilung Strafrecht des 69. Deutschen Juristentags in München mehrheitlich die Schaffung einer Rechtsgrundlage für die Quellen-Telekommunikationsüberwachung und die Online-Durchsuchung in der Strafprozess-

ordnung gefordert (vgl. 69. Deutscher Juristentag München 2012 - Beschlüsse, Seite 10 f.; http://www.djt-net.de/beschluesse/beschluesse.pdf).

2. Im Oktober 2015 ist die „Expertenkommission zur effektiveren und praxistauglicheren Ausgestaltung des allgemeinen Strafverfahrens und des jugendgerichtlichen Verfahrens" zur Empfehlung gelangt, zum Zwecke des Grundrechtsschutzes der Betroffenen die Voraussetzungen der Quellen-Telekommunikationsüberwachung gesetzlich zu regeln und insoweit eine eigene Ermächtigungsgrundlage zu schaffen, die sowohl dem Eingriff in das Telekommunikationsgeheimnis als auch dem für diese Maßnahme typischen zusätzlichen Eingriff in das Grundrecht auf Vertraulichkeit und die Integrität informationstechnischer Systeme Rechnung trägt. Technisch müsse sichergestellt werden, dass mit der für die Quellen-TKÜ eingesetzten Software nur Zugriff auf Inhalt und Umstände der laufenden Telekommunikation genommen werden kann, nicht aber auf die auf dem überwachten Endgerät gespeicherten Daten (vgl. Bericht der „Expertenkommission zur effektiveren und praxistauglicheren Ausgestaltung des allgemeinen Strafverfahrens und des jugendgerichtlichen Verfahrens", Oktober 2015, Seite 73 ff.; https://www.bmjv.de/SharedDocs/Downloads/DE/PDF/Abschlussbericht_Reform_StPO Kommission.pdf?blob=publicationFile&v=2; insbesondere auch Anlagenband II - Protokolle Siebte Sitzung der Expertenkommission am 13./14. Juli 2015, Seite 247 ff.; https://www.bmjv.de/SharedDocs/Downloads/DE/PDF/Anlage_2_StPO_Kommission .pdf? blob=publicationFile&v=2).

3. Mit Beschluss vom 9. November 2016 wurde auf der Arbeitstagung des Generalbundesanwalts mit den Generalstaatsanwältinnen und Generalstaatsanwälten gefordert:

„Die Generalstaatsanwältinnen und Generalstaatsanwälte der Länder sowie der Generalbundesanwalt halten es für dringend erforderlich, die Strafverfolgungsbehörden durch eine Anpassung der bestehenden gesetzlichen Regelungen wieder in die Lage zu versetzen, bei schweren Straftaten aufgrund richterlicher Anordnung die Telekommunikation von Beschuldigten (und deren Nachrichtenmittlern) effektiv zu überwachen. Notwendig ist hierfür die technikoffene Fortschreibung der strafprozessualen Rechtsgrundlagen, die den verdeckten Zugriff auf laufende Telekommunikation möglich macht und den technisch bedingten, zwingend mit der Überwachung einhergehenden Eingriff in die informationstechnischen Systeme im Wege einer Installationsbefugnis gestattet."

Zur Begründung wurde ausgeführt:

„Die Telekommunikationsüberwachung stellte lange Zeit im Bereich der Verfolgung schwerer und organisierter Kriminalität einen Eckpfeiler erfolgreicher Ermittlungen dar. Dies galt in besonderer Weise für die Bekämpfung des Terrorismus und anderer schwerster Straftaten. Die technische Entwicklung hat jedoch dazu geführt, dass der für die Sicherheitsbehörden auswertbare Anteil an der Kommunikation rapide abgesunken ist und weiter rasant abnimmt. Die Telekommunikationsüberwachung nach geltendem Recht fällt deshalb als Ermittlungsinstrument weitgehend aus.

Die fortschreitende Umstellung der Festnetztelefonie auf VoIP, die Ende-zu-Ende-Verschlüsselung weit verbreiteter Kommunikationsapplikationen und der technische Fortschritt im Hardware-Bereich haben einen Zustand entstehen lassen, der die Erfüllung des grundgesetzlichen Auftrages des Schutzes der Bevölkerung vor Straftaten durch deren nachdrückliche Verfolgung in Frage stellt.

Aktuell ist festzustellen, dass nur noch in weniger als 15 % aller Fälle vollständig unverschlüsselte Kommunikation auf Seiten der Beschuldigten durchgeführt wird und damit von den Strafverfolgungsbehörden überwacht werden kann. Gleichzeitig ist ausweislich von Stichproben des BKA erkennbar geworden, dass in zwei Drittel der Fälle seitens der Täter bewusst verschlüsselte Kommunikation zur Verschleierung eingesetzt wird, während in den restlichen Fällen der Anstieg des verschlüsselten Anteils dem mittlerweile üblichen Verbraucherverhalten und den Entwicklungen der Anbieter geschuldet sein dürfte, standardmäßig verschlüsselte Applikationen anzubieten oder zu nutzen.

Im Ergebnis führt dies zu einem massiven Defizit bei der Gewinnung von Beweismitteln durch Telekommunikationsüberwachung, die gerade durch die wachsende Relevanz elektronischer Kommunikation von zentraler Bedeutung bei der Aufklärung schwerer und organisierter Kriminalität ist. Zugleich belegen die verschlüsselungsbedingten Ausfälle, dass es nicht um eine Ausweitung staatlicher Grundrechtseingriffe, sondern ausschließlich um die Wiederherstellung des Zustandes geht, der bei der klassischen Telefonie bestand, bevor die Strafverfolgungsbehörden durch die technische Weiterentwicklung von dieser Beweiserhebungsmöglichkeit weitgehend abgeschnitten wurden. Die rechtliche Möglichkeit einer Ausleitung von zum Zeitpunkt der Überwachung

erzeugten (laufenden) Kommunikationsinhalten noch vor ihrer Verschlüsselung ist daher dringend erforderlich.

Bereits im Koalitionsvertrag des Bundes ist deshalb eine Neufassung der gesetzlichen Regelung zur sog. Quellen-TKÜ festgeschrieben worden. Auch die Justizministerkonferenz hat am 1./2. Juni 2016 einstimmig eine Entschließung zum Erfordernis einer gesetzlichen Regelung der „Quellen-TKÜ" gefasst (TOP 11.21). Die Entscheidungen des Bundesverfassungsgerichts, insbesondere diejenigen zum Verfassungsschutzgesetz Nordrhein-Westfalen und zum BKAG (1 BvR 370/07 vom 27.02.2008; 1 BvR 966/09 vom 20.04.2016), haben einen gangbaren Weg für eine gesetzliche Regelung aufgezeigt.

Aus Sicht der Generalstaatsanwältinnen und Generalstaatsanwälte sowie des Generalbundesanwalts wird die erforderliche Neuregelung zu bedenken haben, dass es - jedenfalls solange eine Verpflichtung (auch ausländischer) Kommunikationsanbieter im Inland zur Entschlüsselung nicht existiert - eines verdeckten Zugriffs der Strafverfolgungsbehörden auf die Endgeräte der Betroffenen bedarf und dass zur Sicherstellung der Überwachung laufender Kommunikation zunächst ein technisch bedingter Eingriff in das informationstechnische System notwendig ist. Soweit davon unvermeidlich sonstige Daten des Systems betroffen sind, kann dem mit den bewährten Instrumentarien von Richtervorbehalt, gerichtlicher Überprüfung, Verwertungsverboten und Löschungspflichten begegnet werden.

Da eine Lösung unter Berufung auf lediglich ungeschriebene Annexkompetenzen auf rechtliche Bedenken stößt, wird in der Gesamtschau angeregt, dass der Gesetzgeber die gebotenen engen rechtlichen Grenzen für eine Installationsbefugnis technikoffen beschreibt, indem er sicherstellt, dass der Eingriff in das informationstechnische System im Ergebnis lediglich die Überwachung der laufenden Kommunikation bezwecken darf, mithin der Ermöglichung hergebrachter Telekommunikationsüberwachung dient."

C. Eigene Erfahrungen

Als Praktiker, der - mit kürzeren Unterbrechungen - seit rund fünfzehn Jahren als Staatsanwalt bei der Bundesanwaltschaft, weit überwiegend in der Abteilung für Straftaten gegen die äußere Sicherheit der Bundesrepublik Deutschland, tätig ist, teile ich diese Sicht.

Bei meiner arbeitstäglichen Befassung mit Ermittlungsverfahren, zumeist im Bereich der Spionage (§§ 94 ff. Strafgesetzbuch) und der Proliferation (§§ 17, 18 Außenwirtschaftsgesetz und §§ 19 ff. Kriegswaffenkontrollgesetz), ist festzustellen, dass die herkömmliche Telekommunikationsüberwachung, die noch vor zehn Jahren zumeist verlässliche Erkenntnisse zu strafbaren Handlungen von Beschuldigten erbracht hat, im Laufe der vergangenen Jahre in immer weniger Fällen einen erfolgversprechenden Ermittlungsansatz darstellt. Die technische Entwicklung hat dazu geführt, dass der für die Polizeibehörden auswertbare Anteil an der Kommunikation nur noch marginal ist und weiter rasant abnimmt. Die herkömmliche, sich nach geltendem Recht richtende Telekommunikationsüberwachung erbrachte in der weit überwiegenden Anzahl der von mir in den vergangenen Jahren geführten Ermittlungsverfahren nur noch geringe oder überhaupt keine Erkenntnisse mehr. Es hat sich ein Dunkelfeld gebildet, das immer größer wird, weil sich in der kriminellen Szene mittlerweile herumgesprochen hat, dass die Polizei „WhatsApp nicht (überwachen) kann", und an diesem Zustand wird sich auch nichts mehr ändern. Die klassische Telekommunikationsüberwachung fällt deshalb als Ermittlungsinstrument weitgehend aus.

Diese Feststellungen decken sich durchweg mit den Erfahrungen von Kolleginnen und Kollegen der Bundesanwaltschaft und der Staatsanwaltschaften der Länder, mit denen ich mich im Laufe der vergangenen Jahre über ihre Erfahrungen im Bereich der Telekommunikationsüberwachung nach geltendem Recht ausgetauscht habe.

„Klassisches" Einsatzgebiet der Telekommunikationsüberwachung war und ist die schwere und organisierte Kriminalität sowie die Bekämpfung von Staatsschutzstraftaten wie Terrorismus, Spionage, Straftaten gegen das Völkerstrafgesetzbuch und das Außenwirtschaftsgesetz. Dies ergibt sich auch aus der jährlichen Statistik des Bundesamtes für Justiz über Telekommunikationsüberwachungsmaßnahmen. Noch vor einigen Jahren haben die Beschuldigten versucht, durch den häufigen Wechsel von Prepaid-Mobiltelefonen der Überwachung ihrer Anschlüsse zu entgehen. Heute ist dies nicht mehr notwendig, da die Ende-zu-Ende-Verschlüsselung weit verbreiteter Kommunikationsapplikationen nahezu allen Beschuldigten bekannt ist und genutzt

wird. So ist bereits verschiedentlich in Protokollen herkömmlicher Telekommunikationsüberwachungsmaßnahmen zu lesen, dass die Beschuldigten vereinbaren, im Anschluss an das gerade geführte Telefongespräch „sensible Inhalte" über einen Instant Messenger auszutauschen, da dieser „von der Polizei ja nicht abgehört werden könne." Sollten dann noch Personen beteiligt sein, die, wie beispielsweise die Quellen und Führungsoffiziere fremder Nachrichtendienste oder die Mitglieder terroristischer Vereinigungen im Hinblick auf ihr Kommunikationsverhalten in besonderer Weise in konspirativem Verhalten geschult wurden, fallen auf diesem Wege keinerlei nutzbringende Erkenntnisse mehr an. Auch im Bereich der organisierten Kriminalität gehen die Täter immer professioneller vor, was eine abgetarnte, auf Verschleierung ausgerichtete Kommunikation einschließt. Nicht zuletzt durch die technische Weiterentwicklung von Kryptierungsmöglichkeiten werden die Strafverfolgungsbehörden von der Möglichkeit, über den Austausch von Information mittels technischer Kommunikation Beweise zu erheben, abgeschnitten.

Die aktuell geäußerte Befürchtung, dass die neu geschaffenen Rechtsgrundlagen für die Quellen-Telekommunikationsüberwachung und die Online-Durchsuchung zum massenhaften und unkontrollierbaren Abhören von zehntausenden Mobiltelefonen von Beschuldigten aus dem Bereich der mittleren oder sogar leichten Kriminalität führen, teile ich nicht. Im Jahr 2015 wurden von den deutschen Staatsanwaltschaften rund fünf Millionen Ermittlungsverfahren eingeleitet. In 5.945 Ermittlungsverfahren kam es zu Telekommunikationsüberwachungsmaßnahmen und in sieben Verfahren zu Maßnahmen der akustischen Wohnraumüberwachung. Durch die neuen Vorschriften wird sich an diesem Zahlenverhältnis wenig ändern. Fälle der Online-Durchsuchung werden genauso selten vorkommen wie die akustische Wohnraumüberwachung. Angesichts des bei jedem staatsanwaltschaftlichem Antrag zu beachtenden Grundsatzes der Verhältnismäßigkeit, des zu betreibenden erheblichen technischen Aufwandes bei den Polizeibehörden, der hohen Regelungs- und Dokumentationsdichte der neuen Vorschriften, der fein ziselierten Benachrichtigungspflichten und nicht zuletzt der - in den letzten Jahren immer stärkeren - Arbeitsbelastung der Kolleginnen und Kollegen der Bundesanwaltschaft und der Staatsanwaltschaften der Länder, wird sich jede Staatsanwältin und jeder Staatsanwalt genau überlegen, ob er einen entsprechenden Antrag beim zuständigen Ermittlungsrichter (§ 100a StPO-E) oder der zuständigen Kammer des Landgerichts (§ 100b StPO-E) stellen wird. Auch versteht es sich von selbst, dass jede Richterin und jeder Richter ihren Prüfpflichten zum Vorliegen der gesetzlichen Voraussetzungen für den Erlass einer entsprechenden Anordnung mit der gebotenen Sorgfalt und Verantwortung nachkommen wird.

D. Bewertung im Einzelnen mit besonderem Blick auf das Staatsschutzstrafrecht

1. Zu § 100b StPO-E:

a) Etliche der in dem Katalog des § 100b StPO-E genannten Tatbestände erfordern die Feststellung, dass es sich um einen besonders schweren Fall handelt. Das setzt voraus, dass das benannte oder unbenannte Regelbeispiel bereits in einem sehr frühen Stadium, in dem - neben anderen verdeckten Maßnahmen - die Überwachung der Telekommunikation ein zentrales Instrument der Beweisführung ist, mit einem den gesetzlichen Anforderungen entsprechenden verdichteten Tatverdacht bejaht werden kann. Dies wird in den seltensten Fällen möglich sein. Die Frage, ob ein besonders schwerer Fall vorliegt, kann in aller Regel erst nach erfolgter Durchsuchung, nach Auswertung aller Beweismittel, bejaht oder verneint werden.

Ich will dieses Problem am Beispiel der geheimdienstlichen Agententätigkeit verdeutlichen. Nach § 100b Abs. 1 Nr. 1, Abs. 2 Nr. 1 a) StPO-E soll die Online-Durchsuchung in Fällen der geheimdienstlichen Agententätigkeit gemäß § 99 Abs. 1 StGB auf solche Taten beschränkt sein, in denen ein besonders schwerer Fall im Sinne von § 99 Abs. 2 StGB vorliegt. Diese Regelung überzeugt bereits auf Grund ihrer Unbestimmtheit nicht. Bei § 99 Abs. 2 StGB handelt es sich um eine bloße Strafzumessungsregel mit Regelbeispielen. Das Verwirklichen eines Regelbeispiels führt nicht dazu, dass zwingend ein „besonders schwerer Fall" der geheimdienstlichen Agententätigkeit vorliegt. Zudem ist ein „besonders schwerer Fall" selbst dann nicht ausgeschlossen, wenn keines der zugehörigen Regelbeispiele verwirklicht ist. Hieraus können sich im Einzelfall erhebliche Unsicherheiten ergeben, ob ein Fall des § 99 Abs. 2 StGB vorliegt und damit die Voraussetzungen einer Online-Durchsuchung gemäß § 100b Abs. 1 Nr. 1, Abs. 2 Nr. 1 a) StPO-E erfüllt sind.

Zudem kann die Frage, ob ein besonders schwerer Fall i. S. von § 99 Abs. 2 StGB vorliegt, selbst bei Außerachtlassung der vorgenannten Unsicherheiten in aller Regel erst nach Auswertung der im Rahmen von Durchsuchungsmaßnahmen etc. gewonnenen Beweismittel - mithin zu einem Zeitpunkt, zu dem der Beschuldigte über den Tatverdacht bereits unterrichtet ist - zuverlässig beantwortet

werden. Dann wird kein Beschuldigter mehr einschlägige Daten speichern oder anderweitig auf seinem Computer verarbeiten. Durch die Beschränkung auf Fälle des § 99 Abs. 2 StGB läuft die Maßnahme in Bezug auf Straftaten nach § 99 StGB mithin praktisch ins Leere. Dies gilt im Übrigen in gleicher Weise für weitere Staatsschutztatbestände wie der landesverräterischen Ausspähung, aber auch beispielsweise für den schweren sexuellen Missbrauch von Kindern nach § 176a Abs. 1 StGB oder der sexuellen Nötigung und Vergewaltigung, wenn die Tat nicht von mehreren gemeinschaftlich begangen wird.

So konnte bei den von mir in den vergangenen rund fünfzehn Jahren bearbeitenden Ermittlungsverfahren wegen geheimdienstlicher Agententätigkeit in keinem einzigen Verfahren (!) die Frage, ob ein besonders schwerer Fall i. S. von § 99 Abs. 2 StGB vorliegt, bereits zum Zeitpunkt der Beantragung von Telekommunikationsüberwachungsmaßnahmen beantwortet werden. Ein aktuelles Beispiel für einen solchen Fall ist die - von der Presse ausführlich berichtete - Ausspähung des ehemaligen Bundestagsabgeordneten, Wehrbeauftragten und seinerzeitigen Präsidenten der Deutsch-Israelischen Gesellschaft, Reinhold Robbe, in Berlin durch eine der Islamischen Republik Iran zuzuordnende geheimdienstliche Einheit, die Qods-Kräfte des Korps der Revolutionsgarden. Mit (noch nicht rechtskräftigem) Urteil des Kammergerichts vom 27. März 2017 wurde der Angeklagte wegen geheimdienstlicher Agententätigkeit gemäß § 99 Abs. 1 StGB zu einer Freiheitsstrafe von vier Jahren und drei Monaten verurteilt.

Die Online-Durchsuchung würde demzufolge auch im Bereich der Cyber-Spionage, die von zunehmender Bedeutung und beachtlichem Gewicht (vgl. nur den von den Medien ebenfalls ausführlich berichteten Angriff auf den Deutschen Bundestag) ist, als Ermittlungsmaßnahme ausscheiden. Auch und gerade vor diesem Hintergrund erscheint es deshalb notwendig, im Katalog des § 100b Abs. 2 StPO-E den „Grundtatbestand" des § 99 Abs. 1 StGB aufzunehmen und die Beschränkung auf besonders schwere Fälle im Sinne von § 99 Abs. 2 StGB zu streichen. Angesichts der Tatsache, dass diese Straftaten unter Nutzung kompletter Serverstrukturen und einer Vielzahl „informationstechnischer Systeme" begangen werden und diese Ermittlungsmaßnahme hier deshalb in besonderer Weise erforderlich und geeignet ist, erscheint auch die geringfügige

Abweichung vom Katalog des § 100c Abs. 2 StPO (akustische Wohnraumüberwachung) sachgerecht.

Im Übrigen ist für den Bereich der Cyber-Spionage anzumerken, dass - bei der vorgesehenen Gesetzesfassung - damit ein Bereich von der Online-Durchsuchung ausgenommen wäre, bei dem diese Ermittlungsmaßnahme in besonderer Weise in Betracht kommt. Insofern ist darauf hinzuweisen, dass das Gesetz an anderer Stelle - § 100g Abs. 1 StPO - durchaus berücksichtigt, dass geringere Voraussetzungen für die Anwendung der Vorschrift genügen, wenn eine Straftat mittels Telekommunikation begangen worden ist. In diesen Fällen dürfen Verkehrsdaten auch erhoben werden, wenn keine Katalogtat nach § 100g Abs. 1 Nr. 1 i.V.m. § 100a Abs. 2 StPO vorliegt (§ 100g Abs. 1 Nr. 2 StPO). Sollte also § 99 StGB - was vorzugswürdig ist - nicht unabhängig vom Vorliegen eines „besonders schweren Falles" in den Katalog des § 100b Abs. 2 StPO-E aufgenommen werden, halte ich es für sachgerecht, dem § 100b Abs. 1 Nr. 1 StPO-E eine Alternative anzufügen, die den Anwendungsbereich für Fälle eröffnet, in den die Straftat „mittels Telekommunikation oder unter Nutzung eines informationstechnischen Systems begangen worden ist" (vgl. § 100g Abs. 1 Nr. 2 StPO). Die weitere Voraussetzung (Tat muss auch im Einzelfall besonders schwer wiegen) stellt dennoch sicher, dass die Online-Durchsuchung nicht in Fällen nur mittlerer oder leichter Kriminalität zum Einsatz kommt.

Die vorgenannte Problematik beschränkt sich schließlich nicht allein auf Strafgesetzverletzungen nach § 99 StGB. In gleicher Weise sind auch Taten nach §§ 95, 98, und 100a StGB betroffen, die ebenfalls nur bei Vorliegen eines „besonders schweren Falles" als Grundlage für eine Online-Durchsuchung in Betracht kommen sollen.

b) Im Entwurf [§ 100b Abs. 2 Nr. 1 lit. b) StPO-E] sind die Strafvorschriften des § 129a Abs. 3 und des § 129a Abs. 5 Satz 1 Alt. 2 und 3 und Satz 2 StGB bislang nicht enthalten. Eine Online-Durchsuchung wäre demnach bei der Unterstützung einer Vereinigung nicht möglich, deren Zwecke auf die Androhung der Straftaten nach § 129a Abs. 1 und Abs. 2 StGB gerichtet ist. Gleiches gilt für den Tatvorwurf der Unterstützung einer Vereinigung nach § 129a Abs. 2 und Abs. 3

StGB. Ebenso wenig in den Fällen des Werbens um Mitglieder oder Unterstützer für eine terroristische Vereinigung.

Ich rege an, den Straftatbestand der Unterstützung einer Vereinigung nach § 129a Abs. 2 StGB [§ 129a Abs. 5 Satz 1 Alt. 2 StGB] in den Gesetzesentwurf als mögliche Anlasstat für eine Online-Durchsuchung mit aufzunehmen. § 129a Abs. 2 StGB umfasst insbesondere Vereinigungen, deren Zwecke und Tätigkeit auf die Begehung von Brandstiftungs- und Sprengstoffdelikten gerichtet sind und denen ebenfalls ein hohes Gefährdungspotential innenwohnen kann. Gerade im Bereich der politisch motivierten Kriminalität rechts könnten Zusammenschlüsse zum Zwecke der Begehung solcher Straftaten relevant werden (zum Beispiel eine Vereinigung, die Anschläge auf noch unbewohnte Asylbewohnerwohnheime plant und durchführt).

Weiter empfehle ich die Aufnahme des § 129a Abs. 5 Satz 2 StGB („Werben um Mitglieder oder Unterstützer") in den Straftatenkatalog des § 100b Abs. 2 Nr. 1 lit. b) StPO-E, da diese Vorschrift im Bereich der Propagandadelikte für die Bundesanwaltschaft eine erhebliche tatsächliche Bedeutung hat: Jihadistisch motivierte Propaganda ist der wesentliche Grund für Radikalisierungen, für Ausreisen in jihadistische Kampfgebiete und für Anschlagsplanungen radikalisierter Einzelpersonen oder Gruppierungen. Aktuell existieren im Internet unzählige jihadistische Foren, Webseiten oder Plattformen auf sozialen Medien mit Deutschlandbezug, auf denen Propaganda des IS veröffentlicht und so zum „Globalen Jihad" gegen „Ungläubige" und „Abtrünnige" aufgerufen wird. Identifizierung und Verfolgung von Personen, die für diese Veröffentlichungen verantwortlich sind, quasi die „geistigen Brandstifter", sind aber wegen der regelmäßig getroffenen Schutzmaßnahmen mit erheblichen Schwierigkeiten verbunden oder gar erfolglos. Bei Propagandadelikten liegen zudem oftmals gerade keine zureichenden tatsächlichen Anhaltspunkte für eine vollendete Unterstützungshandlung im Sinne des § 129a Abs. 5 Satz 1 Alt. 1 StGB oder gar für eine mitgliedschaftliche Betätigungshandlung vor, was eine Online-Durchsuchung unmöglich machen würde und Strafbarkeitslücken befürchten ließe. Die praktische Relevanz der Propagandadelikte zeigt sich exemplarisch bei den von der Bundesanwaltschaft geführten und von den Medien ausführlich berichteten Ermittlungsverfahren gegen die „Globale Islamische Medienfront" (GIMF), deren Zielsetzung es war, jihadisti-

sche Texte, Bilder, Tondokumente und Filme durch die Veröffentlichung in ihren Foren weltweit im Internet zugänglich zu machen, gegen den Betreiber des GIMF-Nachfolgeforums „Al-Ansar-Medienbataillon“ sowie jüngst im Ermittlungsverfahren gegen den „Prediger“ „Abu Walaa“ und andere.

2. Zu § 100e StPO-E:

Hinsichtlich des Verfahrens ist darauf hinzuweisen, dass die in § 100e Abs. 2 Satz 4 StPO-E enthaltene Monatsfrist bei der Umsetzung einer Online-Durchsuchung schon im Hinblick auf die zu schaffenden technischen Voraussetzungen für die tatsächliche Durchführung der Maßnahme unzureichend sein dürfte. Hier sollte eine Frist von zumindest zwei Monaten bei der Erstanordnung möglich sein. Dabei wird nicht verkannt, dass dann der „Gleichlauf“ der Fristen mit einer Anordnung einer akustischen Wohnraumüberwachung nicht mehr gewährleistet wäre. Die tatsächliche Umsetzung einer akustischen Wohnraumüberwachung ist aber typischerweise nicht mit den technischen Hürden verbunden, die bei einer geplanten Online-Durchsuchung zu überwinden sind.

3. Hinweis zur Begründung in der Formulierungshilfe zum Gesetzentwurf (B., zu Buchstabe c, Absatz 5):

Die Aussage, eine nicht zur Verfügung stehende Software mache eine Maßnahme zur Quellen-TKÜ „unzulässig“, dürfte jedenfalls für den Fall einer bereits laufenden Maßnahme zu weit gehen, wenn die Software lediglich aufgrund von äußeren Umständen (zum Beispiel Updates einer Software eines Messengerprogramms) funktionsunfähig wird. Sollte die Maßnahme nach einer Veränderung des Zielsystems durch den Betroffenen nicht mehr vollzogen werden können, müsste bei dieser strikten Auslegung nach Anpassung der Überwachungssoftware ein erneuter Beschluss zur Überwachung beantragt werden, weil die Maßnahme selbst (vorübergehend) nicht mehr durchgeführt werden konnte und demnach beendet wäre. Dies scheint zur Wahrung der Verhältnismäßigkeit des Eingriffs aber nicht erforderlich, weil sich an der Überwachungssituation sonst nicht geändert hat. Eine solch strenge Auslegung findet im geplanten Wortlaut des Entwurfs aus meiner Sicht auch keine ausreichende Stütze.

4. Weiterer Hinweis zur Begründung in der Formulierungshilfe zum Gesetzentwurf (B., zu Buchstabe c, Absatz 6):

Grundsätzlich ist die Dokumentation und Protokollierung der Funktionsweise, der Änderungen im Zielsystem und der übermittelten Daten verfassungsrechtlich erforderlich, um den Eingriff so nachvollziehbar wie möglich zu dokumentieren und ihn richterlich überprüfbar zu machen. Soweit hierfür allerdings die Dokumentation des Quellcodes einer Überwachungssoftware für erforderlich gehalten wird, gebe ich zu bedenken, dass dieser Quellcode mit der Dokumentation der konkreten Funktionsweisen des Programms auch in den Akten nachvollziehbar dargelegt werden müsste. Dies würde - angesichts der Erfahrungen mit der tatsächlichen Geheimhaltung von sicherheitsrelevanten Sachverhalten - mit an Sicherheit grenzender Wahrscheinlichkeit regelmäßig dazu führen, dass die Überwachungssoftware lediglich einmalig einsetzbar wäre, weil Quellcode und konkrete Arbeitsweise des Überwachungsprogramms über die Akteneinsicht an die Beschuldigten heraus an die Öffentlichkeit gelangen und gegebenenfalls in öffentlicher Hauptverhandlung umfassend erörtert würden. Angesichts der tatsächlichen Umstände würden entsprechende Gegenmaßnahmen innerhalb kürzester Zeit zu erwarten sein, die die Überwachungssoftware funktionsunfähig machen und eine komplette Neukonstruktion derselben erfordern würde. Diese Neukonstruktion müsste wiederum umfassend in den Akten dokumentiert werden („Hase-und-Igel-Spiel"). Ausreichend muss daher aus meiner Sicht die nachvollziehbare Dokumentation der Funktionsweise und der durchgeführten Eingriffe sein, ferner, dass es über die dokumentierten Zugriffe und Änderungen hinaus keine weiteren gegeben hat. Hierzu bedarf es einer Darlegung des Quellcodes in den Akten nicht.

Anhörung des Vizepräsidenten des Bundeskriminalamtes

Peter Henzler

im Ausschuss für Recht und Verbraucherschutz
des Deutschen Bundestages am 31. Mai 2017

zum Entwurf eines Gesetzes zur Änderung
des Strafgesetzbuchs, des Jugendgerichtsgesetzes,
der Strafprozessordnung und weiterer Gesetze

hier: zum Thema Quellen-TKÜ und Online-Durchsuchung in der StPO gem. Formulierungshilfe der BReg

(Drs. 18/11272, *18(6)/334 Formulierungshilfe*)

Telekommunikation ist der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen (§ 3 Nr. 22 TKG). Durch die Entwicklungen im Bereich der Informations- und Kommunikationstechnologien, insbesondere in den Bereichen Anonymisierung und Kryptierung, läuft die „klassische“ Telekommunikationsüberwachung durch Ermittlungsbehörden im Rahmen ihrer gesetzlichen Befugnisse mittels Ausleitung der Daten durch den Telekommunikationsanbieter zunehmend ins Leere. Das liegt daran, dass der Ursprung der Telekommunikation in Form des genutzten physikalischen Anschlusses bzw. des Urhebers häufig nicht mehr ermittelt werden kann (Folge der Anonymisierung) und ein zunehmend hoher Anteil der Telekommunikation nicht mehr überwach- bzw. auswertbar ist (Folge der Verschlüsselung).

Dabei ist darauf hinzuweisen, dass verschlüsselte Kommunikation mittlerweile in vielen Fällen keine willentliche Nutzung einer Kryptierungssoftware voraussetzt, sondern zunehmend von den gängigen elektronischen Kommunikationsanbietern wie z. B. deutschen E-Mail-Anbietern als technischer Standard verwendet wird. Darüber hinaus integrieren die Anbieter der gängigsten (mobilen) IuK-Plattformen (z.B. Apple, Google) inzwischen Ende-zu-Ende-Verschlüsselungsverfahren in ihre Systeme, die die Kommunikation automatisch verschlüsseln. Insofern ist inzwischen ein signifikanter Teil der Kommunikation über allgemein gebräuchliche Anbieter aufgrund ihrer Verschlüsselung als nicht mehr auswertbar durch die Ermittlungsbehörden anzusehen.

Selbst wenn nicht bereits die Verschlüsselung die Überwachbarkeit der Kommunikation verhindert, ist dies häufig bei mobiler Nutzung von IT-Systemen der Fall, wenn sich der Nutzer nicht über den ihm zugeordneten Mobilfunk- oder Festnetzanschluss, sondern über freie WLAN anonym ins Internet einwählt (sog. nomadische Nutzung). Auch in diesen Fällen kann nur eine Quellen-TKÜ die Überwachung der Kommunikation gewährleisten.

Jenseits der Konstellation der Überwachung laufender kryptierter Telekommunikation stellt die Kryptierung bzw. Verschlüsselung von Daten seitens der Täter (z. B. bei Verschlüsselung eines Bereichs der Festplatte eines Computers oder einer externen Festplatte) die Sicherheitsbehörden zunehmend vor technische Probleme. Um im Einzelfall verschlüsselte Daten als Spurenansätze bzw. Beweismittel auswerten zu können, wäre mangels anderer Möglichkeiten das Ermittlungsinstrument der Online-Durchsuchung erfolgversprechend. Insbesondere bei schweren Delikten, Serientaten, Strukturermittlungen bei Organisierter Kriminalität und Terrorismus sind diese Daten aber aus polizeilicher Sicht unerlässlich.

Leider fehlen entsprechende Befugnisnormen für die Quellen-TKÜ und die Onlinedurchsuchung in der StPO bisher.

Dabei ist darauf hinzuweisen, dass das BVerfG in seiner Entscheidung zur Online-Durchsuchung (im LfV-Gesetz NRW) schon 2008 deutlich gemacht hat, dass eine Online-Durchsuchung in der StPO zur Verfolgung von schweren Straftaten durchaus denkbar wäre. In seiner Entscheidung 2016 zum BKAG hat das BVerfG zudem die

Wertigkeit von Wohnraumüberwachung und Online-Durchsuchung (im Gefahrenabwehrrecht) bezüglich der Eingriffstiefe (in unterschiedliche Grundrechte) auf eine Stufe gestellt. Zudem hat es in dieser Entscheidung grundsätzlich die im BKAG zur Prüfung angestandenen Befugnisnormen im Aufgabenfeld des BKA nach § 4a BKAG im Kern als verfassungskonform anerkannt.

Die nun vorgesehenen Änderungen in der StPO stellen zweifellos einen deutlichen Mehrwert für eine effiziente wie effektive Strafverfolgung aus Sicht des Bundeskriminalamtes dar. Bei der sogenannten Quellen-TKÜ wird die gebotene Rechts- und Handlungssicherheit geschaffen, bei der Online-Durchsuchung wird der seit Jahren vom Bundeskriminalamt begründeten Forderung zur Schaffung einer solchen konstitutiven Regelung – über das BKAG hinaus – auch zur Strafverfolgung nachgekommen.

Im Folgenden möchte ich noch einmal die Hauptargumente für den Bedarf an den geforderten Regelungen sowohl in rechtlicher als auch in polizeifachlicher Hinsicht darstellen:

1. Quellen-TKÜ

a. Polizeifachlicher Bedarf

Telekommunikationsüberwachung ist ein unverzichtbarer Bestandteil der Ermittlungsarbeit. Der Erfolgswert dieser Maßnahme wird bedroht durch die Nutzung kryptierter Telekommunikationswege und -dienste, die mit einer konventionellen TKÜ-Maßnahme nicht überwachbar sind. Damit durch die Nutzung von Kommunikationsverschlüsselung kein strafverfolgungsfreier Raum entsteht, benötigen die Ermittlungsbehörden Ausgleichsmaßnahmen, um die wachsenden Lücken bei der klassischen Telekommunikationsüberwachung zu schließen. Hier muss das derzeit erfolgversprechendste Ermittlungsinstrument, die Quellen-TKÜ, genutzt werden. Dieses verfolgt den Lösungsansatz, die Kommunikationsdaten vor der Verschlüsselung bzw. nach Entschlüsselung aufzuzeichnen und an die Ermittlungsbehörden zu übertragen (sog. Quellen-Telekommunikationsüberwachung). Die Verschlüsselung kann so umgangen werden. Hierzu ist erforderlich, eine spezielle Software auf das zur Kommunikation genutzte Endgerät aufzubringen. Die verdeckte Aufbringung der Software auf das Endgerät stellt für die Sicherheitsbehörden eine besondere technische Herausforderung dar und ist regelmäßig mit hohem Aufwand verbunden.

Hinsichtlich des polizeifachlichen Bedarfs an der Überwachung und Auswertung verschlüsselter Telekommunikationsinhalte wird auf die Ergebnisse einer vom BKA durchgeführten Bund-/Ländererhebung hingewiesen. Im Erhebungszeitraum 01.01.2012 bis 31.12.2013 wurden knapp 300 Sachverhalte mit dem Ergebnis ausgewertet, dass die nicht auswertbaren Telekommunikationsinhalte zu teils erheblichen Überwachungslücken führten und damit zu unvollständigen Ermittlungsergebnissen, einer mangelhaften Beweislage oder gar zum Scheitern der Ermittlungen. Insbesondere die Aufklärung der Kommunikations- und Organisationsstrukturen der Tatverdächtigen, sowie Planung und Durchführung von (Begleit-) Ermittlungsmaßnahmen werden in erheblichem Maße erschwert. Gleichzeitig gehen Versuche, die Ermittlungsdefizite auch nur im Ansatz auszugleichen, in der Regel mit deutlich intensiveren Grundrechtseingriffen bei den Betroffenen einher.

Keineswegs verwundert daher, dass sich dieser Trend fortsetzt. Im Rahmen einer Datenanalyse bezogen auf die im BKA durchgeführten TKÜ-Maßnahmen mit IP-Datenverkehr aus dem Jahr 2016 zeichnet sich aktuell folgendes Bild – allein bezogen auf die Kommunikation per Messengerdiensten ab:
In 67% der im BKA durchgeführten TKÜ-Maßnahmen mit IP-Datenverkehr war Messengerkommunikation enthalten. Die am häufigsten genutzten Messenger waren Facebook-Messenger (65%), WhatsApp (56%) und Viber (28%).

b. Rechtsrahmen und Bedarf an der Schaffung einer Befugnisnorm für die Quellen-TKÜ in der StPO

Das BKA begrüßt ausdrücklich, dass die Quellen-TKÜ nun (klarstellend) in der StPO geregelt werden soll, die tatbestandlichen Voraussetzungen (insbesondere Straftaten-Katalog) der „normalen" TKÜ entsprechen und die Schutzregelungen sich an die Regelung in §§ 4a, 20l BKAG anlehnen.
Bisher ist eine explizite Befugnisnorm zur Durchführung von Quellen-TKÜ in der StPO nicht enthalten. Im Rahmen der präventivpolizeilichen Aufgaben des BKA zur Abwehr von Gefahren des internationalen Terrorismus ist die Quellen-TKÜ, neben der TKÜ, für das BKA jedoch bereits explizit in § 20l Abs. 2 BKAG als zulässige Eingriffsmaßnahme vorgesehen.
Dabei ist es aus Sicht des BKA nicht ausreichend, diese Software ausschließlich im Bereich der Gefahrenabwehr zum Einsatz zu bringen. Vielmehr soll die mit hohem personellem und finanziellem Aufwand entwickelte Software auch bei der Strafverfolgung als Einsatzmittel zur Verfügung stehen. Um aber auch für Ermittlungsverfahren das Instrument der Quellen-TKÜ als Option zu erhalten und aus Gründen der einheitlichen Handlungs- und Rechtssicherheit in Bund und Ländern sieht es das BKA als geboten an, eine klarstellende Regelung in die StPO aufzunehmen.

Diese Forderung hatte auch Eingang in den Koalitionsvertrag für die 18. Wahlperiode gefunden. Zudem wurde mit Beschluss des 69. Deutschen Juristentages vom 20.09.2012 der fachliche Bedarf bestätigt und der Gesetzgeber aufgefordert, eine (klarstellende) Regelung zum Einsatz von Quellen-TKÜ im Rahmen der Strafverfolgung zu schaffen.

2. Online-Durchsuchung

a. Polizeifachlicher Bedarf

Neben kryptierter Telekommunikation (siehe Quellen-TKÜ) stellt die Kryptierung bzw. Verschlüsselung von Daten durch die Täter (z. B. bei Verschlüsselung eines Bereichs der Festplatte eines Computers oder einer externen Festplatte) sowie die von den Herstellern von Hardware zunehmend ab Werk voreingestellte Verschlüsselung (insbesondere von Handys) als „Standard-Sicherheitsfeature“ die Sicherheitsbehörden zunehmend vor technische Probleme. Um im Einzelfall verschlüsselte Daten als Spurenansätze bzw. Beweismittel auswerten zu können, wäre mangels anderer Möglichkeiten auch hier das Ermittlungsinstrument der Online-Durchsuchung erfolgversprechend. Jedoch fehlt eine Befugnisnorm in der StPO. In bestimmten Fallkonstellationen können im Ermittlungsverfahren mit einer Online-Durchsuchung Dateien erlangt werden, die auf dem Zielsystem nur für kurze Zeit klartextlich vorliegen, oder es können mittels Keylogging oder Screen-/Applicationshots Passwörter und Zugangscodes erlangt werden, die bei einer Beschlagnahme von verschlüsselten Datenträgern eine spätere Datenauswertung überhaupt erst ermöglichen.

Neben den klassischen Konstellationen der Online-Durchsuchung, die auf dem Rechner eines Endkunden stattfindet, ist auch der Zugriff auf Serversysteme oder auf mobile Devices (Smartphones/Tablets) notwendig. Zudem sollte es neben der reinen Erhebung von Daten auf dem Rechner möglich sein, den RAM des durchsuchten Gerätes auszulesen/zu sichern.

Fallbeispiele:

Folgende Fälle aus Ermittlungsverfahren und sonstige typische Konstellationen werden zur Veranschaulichung der Problematik beispielhaft aufgeführt:

- Terrorismus

Erkenntnisse über die Ausreise deutscher Staatsangehöriger im Frühjahr 2012 mit dem Ziel, sich im nordafrikanischen Raum für die Teilnahme am gewaltsamen Jihad terroristisch ausbilden zu lassen, führten im September 2012 zur Einleitung eines Ermittlungsverfahrens des GBA wegen des Verdachts der Unterstützung einer terroristischen Vereinigung im Ausland gemäß §§ 129a, 129b StGB gegen zunächst fünf Beschuldigte. Derzeit werden beim BKA dreizehn Ermittlungsverfahren und zwei Strafverfahren

wegen des Verdachts der Unterstützung einer terroristischen Vereinigung im Ausland sowie wegen des Verdachts der Mitgliedschaft in einer terroristischen Vereinigung im Ausland (AQM, ISIG, JaN, Junud Al Sham) mit insgesamt sechszehn Beschuldigten und fünf Angeklagten im Auftrag des GBA bearbeitet. Die Beschuldigten/Angeklagten stehen im Verdacht, sich an Kampfhandlungen radikaler Islamisten gegen das Assad-Regime in Syrien zu beteiligen, beteiligt zu haben oder die jihadistischen Kämpfer im Ausland oder aus Deutschland heraus zu unterstützen. Es wurden über 200 TKÜ-Maßnahmen geschaltet. Neben Mobiltelefonen, DSL- und Festnetzanschlüssen sowie E-Mail Adressen wurden auch zahlreiche Auslandskopf-und IMEI-Überwachungen durchgeführt. Etwa 10% der Maßnahmen sind derzeit noch aktiv. Trotz des Maßnahmenpakets kann weiterhin ein Großteil der geführten Kommunikation nicht festgestellt werden, da die Betroffenen regelmäßig bewusst kryptierte Kommunikationswege nutzen (z.B. Telegram, WhatsApp, Ask.fm, Skype, Tango), die technisch und/oder rechtlich nicht überwacht werden können. Regelmäßige verfahrensrelevante Kommunikation wird verbal oder schriftlich bewusst über die genannten verschlüsselten Dienste geführt. Konkrete Verabredungen, um auf verschlüsselte Kommunikationswege auszuweichen,
können regelmäßig auf den vorhandenen TKÜ-Maßnahmen festgestellt werden. Da in hiesigen Ermittlungsverfahren vor allem schriftliche Kommunikation über kryptierte Kommunikationswege geführt wird, würde die Möglichkeit der Online-Durchsuchung ein profundes Ermittlungsinstrument darstellen (Stichwort: Screenshots von geführter schriftlicher verschlüsselter Kommunikation), um an verschlüsselte und verfahrensrelevante Kommunikationsinhalte zu gelangen, die eine hohe Verfahrensrelevanz aufweisen dürften.

- PMK links

In einem Ermittlungsverfahren wurden 125 elektronische Datenträger (PC, USB-Sticks etc.) sichergestellt. Auf 29 Datenträgern (entspricht 23%) befinden sich verschlüsselte Daten, die nicht entschlüsselt werden konnten. Lediglich auf einem Datenträger konnten kryptierte Daten entschlüsselt werden (Entschlüsselung erfolgte durch Eingabe des sich aus der Asservatenauswertung ergebenden Passwortes); d.h., lediglich 3% der verschlüsselten Datenträger konnten entschlüsselt werden. Zur Verschlüsselung wurden u.a. folgende Programme verwendet: TrueCrypt, LUKS/dm-crypt, ecryptfs.

Das Verschlüsseln von E-Mailverkehr, Dateien oder ganzen Festplatten ist mittlerweile gängige Praxis im Phänomenbereich PMK -links-. Dabei werden täterseitig verschiedene Verschlüsselungsprogramme verwendet. Selbstverständlich wäre das Instrument der Onlinedurchsuchung in diesem Zusammenhang hilfreich, da z.B. die Erstellung von Selbstbezichtigungsschreiben, Dokumenten zur Ausspähung von Anschlagszielen und Vorbereitung von Straftaten auf Rechnern der Beschuldigten vor einer möglichen Verschlüsselung gesichtet und gesichert werden könnten. Ebenso ist denkbar, dass Verschlüsselungscodes, die innerhalb der Tätergruppe versandt werden, festgestellt werden.
Die Online-Durchsuchung wäre neben der Quellen-TKÜ wahrscheinlich das einzige zweckmäßige Überwachungsinstrument, wenn die Täter bspw. über offene WLAN-Netze kommunizieren. Die Online-Durchsuchung wäre neben der Quellen-TKÜ auch dann das einzige erfolgversprechende Mittel zur Erlangung aktueller IT-Erkenntnisse (Täterkontakte, Informationswege, Beweisdateien etc.), wenn der Beschuldigte über VPN kommuniziert.

- Kinderpornographie

In einem Ermittlungsverfahren wegen des Verdachts der Verbreitung kinderpornografischer Schriften verschlüsselt der Beschuldigte seine Festplatte. Eine offene Durchsuchung (inkl. Sicherstellung der Datenträger) ist nicht erfolgsversprechend, da der Beschuldigte das Passwort nicht preisgibt und eine Entschlüsselung der Festplatte aus technischen Gründen nicht möglich ist.
Eine Online-Durchsuchung auf dem Zielsystem des Beschuldigten ermöglicht die Sicherstellung von beweiserheblichem Material, während der Beschuldigte seinen Computer nutzt und mit dem Internet verbunden ist.

- Online-Betrug

In einem Ermittlungsverfahren wegen des Verdachts des gewerbsmäßigen Betrugs verschlüsselt der Beschuldigte seine Festplatte. Eine offene Durchsuchung ist aus den oben genannten Gründen nicht möglich.
Eine Online-Durchsuchung auf dem Zielsystem ermöglicht das Auslesen (die Sicherstellung) möglicher Zugangskennungen, die der Beschuldigte bei der Begehung der Straftaten benutzt hat. Mithilfe der Zugangskennungen ist ein detaillierter Tatnachweis in der offenen Ermittlungsphase möglich.

- Auslesen von Zugangskennungen

In einem Ermittlungsverfahren verschlüsselt der Beschuldigte seine Festplatte. Eine Entschlüsselung der Festplatte ist aus technischen Gründen nicht möglich.
Eine Online-Durchsuchung auf dem Zielsystem des Beschuldigten ermöglicht das Auslesen von im Arbeitsspeicher temporär hinterlegten Passwörtern/Verschlüsselungscodes. Mithilfe dieser Passwörter kann ein bei einer offenen Durchsuchung sichergestelltes Zielsystem entschlüsselt werden.

b. Rechtsrahmen und Bedarf an der Schaffung einer Rechtsgrundlage für Online-Durchsuchung in der StPO

Das BKA begrüßt ferner grundsätzlich, dass auch eine Online-Durchsuchungs-Regelung vorgesehen ist.
Die vorgenannten Beschlüsse des 69. Deutschen Juristentages zur Anerkennung des fachlichen Bedarfs und zur Aufforderung des Gesetzgebers zur Schaffung einer Rechtsgrundlage beziehen sich im Übrigen neben der Quellen-TKÜ auch auf die Online-Durchsuchung.

Der für die Online-Durchsuchung vorgeschlagene Straftatenkatalog lehnt sich nun nach hiesigem Verständnis an den der Wohnraumüberwachung und der Regelung der „Vorratsdatenspeicherung“ an, was vor dem Hintergrund der Eingriffsintensität der Maßnahme durchaus nachvollziehbar erscheint.

Das Verbot der Anordnung der Maßnahmen nach § 100b und § 100c StPO-E (ODS und WRÜ) erstreckt sich im Entwurf auf ALLE Berufsgeheimnisträger. Systematisch sollte aber ein solches pauschales Verbot nur auf die absolut geschützten und damit privilegierten Berufsgeheimnisträger (Parlamentarier, Geistliche, Verteidiger, Rechtsanwälte) beschränkt sein, gegen die relativ geschützten Berufsgruppen könnten die Maßnahmen bei Vorliegen der überwiegenden hoheitlichen Interessen im Einzelfall an der Durchführung der Maßnahme vorbehalten werden.

Die Regelung in § 100e Abs. 2 StPO-E, dass die Anordnung bei den Maßnahmen ODS und WRÜ einem Kollegialgericht vorbehalten ist, erscheint aus hiesiger Sicht schlüs-

sig, da bereits jetzt die WRÜ unter Kammervorbehalt des Landgerichts nach GVG steht.

In § 100e Abs. 6 Nr.1 StPO-E wird der vom BVerfG in seiner Entscheidung vom 20.04.2016 entworfene Grundsatz der Verwendung von Daten aus eingriffsintensiven Maßnahmen und ihre Möglichkeit der Umwidmung für andere Zwecke (Hypothetische Datenneuerhebung) aufgegriffen und in modifizierter Form in der StPO verankert.

In § 100e Abs. 6 Nr.2 StPO-E wird die Möglichkeit der Umwidmung der Informationen zum Zweck der Gefahrenabwehr an bestimmte Rechtsgüter geknüpft. Es fehlt hier das Rechtsgut „*Bestand des Staates*“, wohingegen die im Entwurf vorzufindenden Formulierungen „*im Einzelfall bestehende Lebensgefahr*“ und „*dringende Gefahr für Leib …*“ letztlich redundant sind.

Die Statistik- und Berichtspflichten nach § 101b StPO-E fordern grundsätzlich die Justiz, nicht die Polizei. Allerdings betrachtet das BKA mit Sorge, dass einige der auffällig extensiven Statistikpflichten faktisch auf die Polizei abgewälzt werden und einen hohen Mehraufwand fordern. Die Erfassungspflichten gehen über die ohnehin schon vorgesehenen (siehe etwa § 88 BKAG-E) Erfassungen durch das BKA hinaus.

Alfred Huber

Oberstaatsanwalt als ständiger Vertreter des Leitenden Oberstaatsanwalts
Leiter der Abteilung für Betäubungsmittelsachen und Organisierte Kriminalität

Staatsanwaltschaft Nürnberg – Fürth

Stellungnahme zur Sachverständigenanhörung am 31.05.2017 im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages zum Gesetzentwurf der Bundesregierung zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze (Ausschussdrucksache 18 (6) 334)

1. Erforderlichkeit der Quellen-TKÜ aus Sicht der staatsanwaltschaftlichen Praxis

Die Telekommunikationsüberwachung ist seit vielen Jahren ein unverzichtbares Ermittlungsinstrument bei der Bekämpfung schwerer Straftaten. Sie ermöglicht den Strafverfolgungsbehörden durch das Abhören und Aufzeichnen der Gespräche insbesondere

- Beweismittel für bereits begangene Straftaten zu erlangen (z.B. Gespräche über die Tat)

- Hinweise auf weitere bevorstehende Straftaten zu erhalten (z.B. Gespräche über Planung weiterer Verbrechen).

Die Telekommunikationsüberwachung kann darüber hinaus aber auch zahlreiche wertvolle Indizien (z.B. auf die Organisationsstruktur innerhalb einer Bande, zu Beschaffungs- und Absatzwegen, etc.) liefern, die Ansätze für weitere Ermittlungen geben.

Gerade im Bereich der Bekämpfung der Organisierten Kriminalität sowie der schweren Betäubungsmittelkriminalität ist eine nachhaltige und effektive Verbrechensbekämpfung ohne die Telekommunikationsüberwachung nicht vorstellbar.

In den letzten Jahren fällt immer wieder auf, dass über die derzeit technisch mögliche Telekommunikationsüberwachung in manchen Fällen keine für die Strafverfolgung brauchbaren Erkenntnisse gewonnen werden können. Über die überwachbaren Anschlüsse werden in zunehmenden Maß nur Gespräche geführt, die nicht deliktsbezogen sind. Gleichzeitig ist erkennbar, dass ein verschlüsselter Datenverkehr stattfindet. Bei einer späteren Beschlagnahme der informationstechnischen Systeme kann nicht selten festgestellt werden, dass die deliktsbezogene Kommunikation verschlüsselt geführt wurde.

Da immer mehr Dienste, die verschlüsselten Datenverkehr anbieten, auf den Markt drängen und die Benutzung immer bedienerfreundlicher wird, ist mittelfristig damit zu rechnen, dass die Telekommunikationsüberwachung im herkömmlichen Sinn nur noch unzureichende Ergebnisse bringen wird („Going Dark“).

Dem kann wirksam nur dadurch begegnet werden, dass die Inhalte der verschlüsselten Kommunikation für die Ermittlungsbehörden zugänglich werden.

Hinsichtlich der in Rechtsprechung und Literatur umstrittenen Frage, ob die Quellen – TKÜ bereits nach derzeitiger Rechtslage zulässig ist, wird auf die Ausführungen in der Ausschussdrucksache 18(6)334 unter „B. Besonderer Teil; Zu Nummer 2“ verwiesen.

In der Entscheidung vom 20.04.2016 zum Bundeskriminalamtgesetz (BKAG) hat sich das Bundesverfassungsgericht mit der Zulässigkeit der Quellen-TKÜ befasst.[1] Das Gericht hält diese – für den Fall, dass eine eindeutige Befugnisnorm (dort: § 20l Abs.2 BKAG) gegeben ist - für zulässig. Dabei spielt für das Gericht der Umstand, dass der Gesetzgeber die technische Umsetzung der Quellen-TKÜ in § 20l Abs.2 Nr.1 und 2 BKAG ausdrücklich geregelt hat, offenbar eine wichtige Rolle. Es darf daher bezweifelt werden, ob sich die Auffassung, dass eine gesetzliche Regelung der Quellen-TKÜ nicht erforderlich ist, noch aufrechterhalten lässt.

Aus Sicht der staatsanwaltschaftlichen Praxis ist daher eine eindeutige Reglung durch den Gesetzgeber, die dem derzeitigen Meinungsstreit die Grundlage entzieht, dringend erforderlich.

Die Arbeit der Strafverfolgungsbehörden wird erheblich erschwert, wenn in jedem Fall mit dem zuständigen Gericht erst eine juristische Auseinandersetzung über die streitige Frage geführt werden muss, ob die Quellen-TKÜ nach derzeitiger Rechtslage zulässig ist. Muss z.B. gegen eine ablehnende Entscheidung des Ermittlungsrichters erst Beschwerde eingelegt werden, so entsteht ein Zeitverlust, der das Ergebnis der Ermittlungen unter Umständen gefährden kann. Auch können in einer Hauptverhandlung zeitintensive Auseinandersetzungen über die Frage der Verwertbarkeit von Erkenntnissen aus einer Quellen-TKÜ vermieden werden, wenn eine klare gesetzliche Regelung vorliegt.

---

[1] **BVerfG, Urteil vom 20.04.2016, 1 BvR 966/06, 1 BvR 1140/09:**

Rn 228: „a) § 20 l BKAG regelt die Telekommunikationsüberwachung und begründet damit Eingriffe in Art. 10 I GG. An Art. 10 I GG ist dabei nicht nur § 20 l I BKAG zu messen, der die herkömmliche Telekommunikationsüberwachung regelt, sondern auch § 20 l II BKAG, der die Quellen-Telekommunikationsüberwachung erlaubt, sofern durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation erfasst wird. Zwar setzt diese technisch einen Zugriff auf das entsprechende informationstechnische System voraus. Jedoch erlaubt § 20 l II BKAG ausschließlich Überwachungen, die sich auf den laufenden Telekommunikationsvorgang beschränken. Die Vorschrift hat damit 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 alten Überwachungstechnik nicht mehr möglich ist. Von daher ist sie nicht am Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, sondern an Art. 10 I GG zu messen (vgl. *BVerfGE* 120, 274 [309] = NJW 2008, 822).“

Selbstverständlich muss die erforderliche Software so konzipiert werden, dass nur Kommunikationsinhalte erfasst werden, die auch auf herkömmlichem Wege ausgeleitet werden können. Dies ist im Gesetzesentwurf festgeschrieben (§ 100a Abs.5 StPO-E)

2. Die Online-Durchsuchung aus Sicht der staatsanwaltschaftlichen Praxis

Die Online-Durchsuchung ist eine Ermittlungsmaßnahme, die nach hiesiger Einschätzung in der Praxis nur selten und ausschließlich im Bereich der Schwerkriminalität zum Tragen kommen wird. In diesen Fällen kann sie aber ein äußerst effektives Mittel der Strafverfolgung darstellen. Nach der derzeitigen Rechtslage (§ 161 Abs.2 StPO) dürfen in einem Strafverfahren nicht einmal die Erkenntnisse verwertet werden, die die Behörden im Rahmen der Gefahrenabwehr in zulässiger Weise erlangt haben (vgl. § 20k BKAG, Art.34d BayPAG, Art.10 BayVSG). Dass dieser Umstand im Sinne einer nachhaltigen Strafverfolgung völlig unbefriedigend ist, bedarf keiner näheren Darlegung.[2]

Die Darstellung in den Medien, dass die Online-Durchsuchung auch „für die Verfolgung leichterer Delikte wie Hehlerei oder Drogenbesitz“ (SZ vom 18.05.2017) möglich sei bzw. „flächendeckend bei ganz normaler Alltagskriminalität“ (Netzpolitik.org) eingesetzt werden soll, ist irreführend und geht sowohl in rechtlicher als auch in tatsächlicher Hinsicht an der Realität vorbei.

a) Rechtliche Voraussetzungen

aa) Straftatenkatalog

Eine Online-Durchsuchung ist nach dem Gesetzesentwurf nur bei besonders schweren Straftaten zulässig, der Katalog des § 100b StPO-E ist dem des § 100c StPO nachgebildet. Bei den in diesem Katalog genannten Straftaten hat das Bundesverfassungsgericht die akustische Wohnraumüberwachung für zulässig erklärt.[3] Da das Bundesverfassungsgericht den Grundrechtseingriff bei einer Online-Durchsuchung mit dem Eingriff in die Unverletzlichkeit der Wohnung vergleicht[4], ist

[2] Die in § 161 Abs.2 StPO vorgesehene Ausnahme - die Einwilligung der von der Maßnahme betroffenen Person - spielt in der Praxis keine Rolle.

[3] **BVerfGE 109,279**; auch in seiner Entscheidung vom 27.02.2008 (**BVerfGE 120,274 ff.**) stellt das BVerfG klar, dass das Grundrecht auf Gewährung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht schrankenlos gewährleistet wird. Den dort aufgezeigten verfassungsrechtlichen Anforderungen wird durch den Straftatenkatalog des §100b StPO-E und der erforderlichen Einzelfallprüfung hinreichend Rechnung getragen.

[4] **BVerfG, Urteil vom 20.04.2016, 1 BvR 966/06, 1 BvR 1140/09,** Rn.210: „Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme schützt dementsprechend vor einem geheimen Zugriff auf diese Daten und damit insbesondere vor Online-Durchsuchungen, mit denen private Computer wie sonstige informationstechnische Systeme manipuliert und ausgelesen, sowie persönliche Daten, die auf externen Servern in einem berechtigten Vertrauen auf Vertraulichkeit ausgelagert sind, erfasst und Bewegungen der Betroffenen im Netz verfolgt werden. Wegen der oft höchstpersönlichen Natur dieser Daten, die sich insbesondere auch aus deren Verknüpfung ergibt, ist ein Eingriff in dieses Grundrecht von besonderer Intensität. Er ist seinem Gewicht nach mit dem Eingriff in die Unverletzlichkeit der Wohnung vergleichbar.“

es nur folgerichtig, wenn der Gesetzesentwurf davon ausgeht, dass der Eingriff bei denselben Delikten zulässig ist.

Die Argumentation der Gegner des Entwurfs, das Bundesverfassungsgericht erlaube die Online-Durchsuchung nur bei „Gefährdung von Menschenleben, ihrer Gesundheit und elementarsten Lebensgrundlagen“ (vgl. netzpolitik.org.) ignoriert vollständig, dass das Bundesverfassungsgericht in seiner Entscheidung vom 20.04.2016 zum BKAG eine Entscheidung zur Frage der Zulässigkeit einer Online-Durchsuchung zur Gefahrenabwehr getroffen hat. In Randnummer 107 der genannten Entscheidung stellt das Gericht dabei sogar ausdrücklich klar, dass sich für den Bereich der Strafverfolgung andere Maßstäbe gelten.[5]

bb) Einzelfallprüfung

Von den Kritikern des Gesetzesentwurfes wird verschwiegen, dass der Gesetzesentwurf die Online-Durchsuchung nur gestattet, wenn die Tat auch im Einzelfall besonders schwer wiegt (§ 100b Abs.1 Nr.2 StPO-E). Damit wird klargestellt, dass der Gesetzgeber bei Katalogtaten, die sich – anders als z.B. Mord oder schwerer Raub mit Todesfolge - nicht in jedem Einzelfall den besonders schweren Straftaten zuordnen lassen (z.B. § 100b Abs.2 Nr.1 StPO-E „gewerbsmäßige Hehlerei“ oder § 100b Abs.2 Nr.2a StPO-E „Verleiten zur missbräuchlichen Asylantragstellung nach § 84 Abs.3 Asylgesetz“), eine weitere Einschränkung fordert, um einen ausufernden Einsatz der Online-Durchsuchung zu verhindern.

In der Praxis prüfen die Gericht gerade diesen Punkt sehr genau, so dass die Befürchtung, auch bei Delikten aus dem Bereich der mittleren Kriminalität müsse mit Online-Durchsuchungen gerechnet werden, unbegründet sind. Da das zuständige Gericht verpflichtet ist, die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme einzelfallbezogen in der Begründung der

---

[5] **BVerfG Urteil vom 20.04.2016, 1 BvR 966/06, 1 BvR 1140/09:**

Rn. 107: „Für Maßnahmen, die der Strafverfolgung dienen und damit repressiven Charakter haben, kommt es auf das Gewicht der verfolgten Straftaten an, die der Gesetzgeber insoweit in – jeweils näher bestimmte – erhebliche, schwere und besonders schwere Straftaten eingeteilt hat. So bedarf die Durchführung einer Wohnraumüberwachung des Verdachts einer besonders schweren Straftat (vgl. *BVerfGE* 109, Seite 279, 343 ff. = NJW 2004,Seite 999), die Durchführung einer Telekommunikationsüberwachung oder die Nutzung von vorsorglich erhobenen Telekommunikationsverkehrsdaten des Verdachts einer schweren Straftat (vgl. *BVerfGE* 125,Seite 260, 328 f. = NJW 2010,Seite 833, *BVerfGE* 129, Seite 208, 243 = NJW 2012, 833) und die Durchführung einer anlassbezogenen Telekommunikationsverkehrsdatenerhebung oder einer Observation etwa durch einen GPS-Sender einer – im ersten Fall durch Regelbeispiele konkretisierten – Straftat von erheblicher Bedeutung (vgl. *BVerfGE* 107,Seite 299, 321f. = NJW 2003, 1787; *BVerfGE* 112,Seite 304, 315 f. = NJW 2005, 1338; zu letzterer Entscheidung vgl. auch *EGMR*, NJW 2011, 1333, 1337 § 70 – Uzun/Deutschland zu Art.8 EMRK). “

Anordnung darzulegen (§ 100e Abs.4 Ziffer 2 StPO-E), ist eine weitere verfahrenstechnische Sicherung gegen eine ausufernde Anordnung der Online-Durchsuchung getroffen.

Da § 100b StPO-E dem § 100c StPO (Wohnraumüberwachung) nachgebildet ist, ist für eine Prognose, wie häufig künftig eine Online–Durchsuchung angeordnet werden wird, ein Vergleich mit § 100c StPO zulässig. Die hierzu erhobenen Statistiken belegen eindrucksvoll, dass die Strafverfolgungsbehörden die Vorgaben des Bundesverfassungsgerichts verantwortungsvoll umsetzen und nur in absoluten Ausnahmefällen auf die Wohnraumüberwachung zurückgreifen.

cc) Verfahrensrechtliche Absicherung

Aus hiesiger Sicht darf bezweifelt werden, ob die Verfassungsmäßigkeit der Online–Durchsuchung davon abhängt, dass anstelle des Ermittlungsrichters beim Amtsgericht gemäß § 100e Abs.2 StPO-E eine Kammer des Landgericht über die Anordnung entscheidet. Vergleichbares gilt für die in § 100e Abs.2 S.4 StPO-E angeordnete Monatsfrist.

Das Bundesverfassungsgericht hält in der zitierten Entscheidung vom 20.04.2016 zum BKAG eine Entscheidung durch das Amtsgericht (vgl. § 20v BKAG) sowie eine Befristung der Online-Durchsuchung auf drei Monate für verfassungsrechtlich unbedenklich.[6] Es ist nicht ersichtlich, weshalb die Online-Durchsuchung in der StPO nur unter strengeren Voraussetzungen zulässig sein soll.

Aus Sicht der staatsanwaltschaftlichen Praxis ist aber festzustellen, dass die Antragstellung bei einer Kammer des Landgerichts für die Staatsanwaltschaft ebenso problemlos möglich ist wie eine Antragstellung beim Ermittlungsrichter.

Die Möglichkeit, die Dauer der Online–Durchsuchung von vorherein auf drei Monate zu befristen, wenn bereits zum Zeitpunkt der Anordnung sicher zu erwarten ist, dass länger andauernde Ermittlungen, z.B. zur Struktur einer kriminellen Organisation erforderlich sind, wäre demgegenüber für die Strafverfolgungsbehörden eine deutliche Entlastung. Da § 100e Abs.5 StPO-E vorsieht, dass die Maßnahme unverzüglich zu beenden ist, wenn die Voraussetzungen der Anordnung nicht mehr vorliegen, werden die Rechte des Betroffenen gewahrt.

---

[6] **BVerfG, aaO.** Rn.216 „c) Keine Bedenken bestehen weiter gegen die verfahrensrechtliche Ausgestaltung der Vorschrift (vgl. § 20k V, VI BKAG). Die Anordnung einer Maßnahme ist nur durch den Richter möglich und dabei sachhaltig zu begründen (vgl. *BVerfGE* 120, 274 [331ff.] = NJW 2008, 822; s. oben C IV 2). Die mögliche lange Dauer von drei Monaten, für die die Maßnahme angeordnet werden kann, ist verfassungsrechtlich allerdings nur mit der Maßgabe tragfähig, dass es sich hierbei für die jeweilige Anordnung um eine Obergrenze handelt und sich die tatsächliche Dauer der Anordnung nach einer Verhältnismäßigkeitsprüfung im Einzelfall richtet."

b) Prognose über die Umsetzung in der Praxis

Zunächst muss klargestellt werden, dass die Strafverfolgungsbehörden in der großen Masse der Fälle eine wesentlich einfachere Möglichkeit haben, um auf Daten eines informationstechnischen Systems zuzugreifen. Durch eine richterliche Durchsuchungs- und Beschlagnahmeanordnung können sie unter den Voraussetzungen der §§ 94 ff. StPO auf die Daten eines Mobilfunkgerätes bzw. Computers zugreifen. Diese Art der Ermittlung wird in der staatsanwaltschaftlichen Praxis auch künftig der Regelfall bleiben. Sie ist erforderlich und – im Sinne des Übermaßverbotes – auch ausreichend, wenn es sich um die Ermittlung eines abgeschlossenen Sachverhalts handelt und Anhaltspunkte dafür bestehen, dass auf den informationstechnischen Systemen des Beschuldigten (ggfls. eines Dritten) Beweise gespeichert sind, die für einen Tatnachweis benötigt werden (z.B. Speicherung von kinderpornographischen Bildern, volksverhetzenden Äußerungen etc.).

Der Nachteil dieser Art des Zugriffs ist der Umstand, dass der Beschuldigte ab dem Moment der Beschlagnahme Kenntnis von den gegen ihn geführten Ermittlungen hat. Gerade bei der Bekämpfung der Organisierten Kriminalität ist eine nachhaltige Strafverfolgung jedoch nur möglich, wenn die Ermittlungen – gegebenenfalls auch über einen längeren Zeitraum – verdeckt geführt werden, z.B. um Erkenntnisse über die Strukturen innerhalb einer Organisation zu gewinnen. Werden die Ermittlungen zu früh offen gelegt, so ist es regelmäßig nicht möglich, gegen die Beschuldigten auf der Führungsebene einer Organisation einen Tatnachweis zu führen. Die Handlanger, die häufig bei der Ausführung der Taten verhaftet werden können, sind nur in den seltensten Fällen bereit, gegen ihre Auftraggeber auszusagen. Häufig besteht dann zwar der Verdacht, dass eine bestimmte Person innerhalb einer Organisation die Aufträge für die Straftaten gibt und den Großteil der dadurch erzielten Gewinne einstreicht. Ebenso häufig fehlen allerdings gerichtsverwertbare Beweise. In derartigen Fällen gibt die Online-Durchsuchung die Möglichkeit, die Mitglieder einer Organisationen über einen gewissen Zeitraum zu überwachen, um festzustellen, wer die Entscheidungen trifft und wer die Befehle lediglich ausführt.

3. Zusammenfassung

Sowohl die Quellen–TKÜ als auch die Online-Durchsuchung sind strafprozessuale Ermittlungsmaßnahmen, die für eine zeitgemäße Strafverfolgung unabdingbar sind. Durch den Gesetzesentwurf ist sichergestellt, dass sie nur bei schweren (Quellen-TKÜ) bzw. besonders schweren (Online-Durchsuchung) Straftaten zum Einsatz kommen dürfen.

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.

Chaos Computer Club

Risiken für die innere Sicherheit beim Einsatz von Schadsoftware in der Strafverfolgung

Sachverständigenauskunft zum Änderungsantrag der Fraktionen CDU/CSU und SPD zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze (Ausschussdrucksache 18/11272)

Linus Neumann,
Constanze Kurz, Frank Rieger
Mittwoch, 31. Mai 2017

Abstract

Gefahr für die innere Sicherheit: Mit der Geheimhaltung von Sicherheitslücken, die zum Anbringen von Schadsoftware benötigt werden, geht eine Gefahr für die innere Sicherheit einher.

Unverhältnismäßiger Grundrechtseingriff bei niedriger rechtlicher Schwelle: Die rechtlichen Grenzen der sogenannten Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) lassen sich technisch kaum umsetzen, wodurch de facto eine Online-Durchsuchung geschaffen wird.

Fehlender Beleg der Notwendigkeit: Strafverfolgungsbehörden haben dank der fortschreitenden Digitalisierung aller Lebensbereiche bereits heute Zugriff auf eine nie dagewesene Fülle an Daten.

Fehlende technische Überprüfbarkeit und Nachvollziehbarkeit: Die technischen Rahmenbedingungen für den Einsatz von Schadsoftware sind nicht ausreichend spezifiziert, um Rechtssicherheit oder adäquate Kontrolle sicherzustellen.

Drohende Verletzung der Eckpunkte deutscher Kryptopolitik: Die unklare Definition der Mitwirkungspflichten sowie anstehende Änderungen der Regulierung im Telekommunikationsmarkt erschweren die Folgenabschätzung für Vertrauen, Sicherheit und Marktposition deutscher Anbieter von Verschlüsselungslösungen.

Einleitung

Im vorliegenden Änderungsantrag sollen die Ermittlungsmethoden der sogenannten „Quellen-Telekommunikationsüberwachung“ (Quellen-TKÜ) und der „Online-Durchsuchung“ im Rahmen der Strafprozessordnung geregelt werden.

Beide Maßnahmen bezeichnen das Anbringen einer Schadsoftware auf ein informationstechnisches System zum Zwecke der Ausleitung von Daten. Der Umfang der auszuleitenden Daten wird bei der Quellen-TKÜ rechtlich auf Kommunikationsinhalte begrenzt, während im Rahmen der Online-Durchsuchung das gesamte informationstechnische System übernommen werden darf. Für beide Methoden müssen vorab technische Systemparameter auf dem Zielsystem ermittelt und verifiziert werden.

Beide Maßnahmen sind aufgrund des hohen Grundrechtseingriffs bereits seit längerer Zeit Gegenstand öffentlicher und juristischer Debatten. Wichtige Ergebnisse dieser Diskussionen und der Beschwerdeverfahren vor dem Bundesverfassungsgericht müssen für den Änderungsantrag berücksichtigt werden und seien daher einleitend in Erinnerung gerufen:

Februar 2008: Der Erste Senat des Bundesverfassungsgerichts urteilt, dass das allgemeine Persönlichkeitsrecht gemäß Art. 2 Abs. 1 und Art. 1 Abs. 1 des Grundgesetzes auch ein Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst.[1]

Dezember 2008: Mit der Novellierung des BKA-Gesetzes erhält das Bundeskriminalamt (BKA) die Ermächtigungsgrundlage sowohl zur Quellen-TKÜ als auch zur Online-Durchsuchung.[2] Mehrere Verfassungsbeschwerden werden dagegen vorgebracht. Bereits am 27. Januar 2009 legt eine Journalistin Beschwerde ein, gefolgt von dem damaligen Herausgeber der Zeit, Michael Naumann, und dem Vorsitzenden der Humanistischen Union, Dr. Fredrik Roggan. Der ehemalige Innenminister Gerhart R. Baum und der Vorsitzende des Landesverbands Berlin des Deutschen Anwaltsvereins, Ulrich Schellenberg, sowie einige weitere Beschwerdeführer wenden sich ebenfalls mit umfangreichen Verfassungsbeschwerden gegen das Gesetz. Jede der Beschwerden befasst sich auch mit den Varianten des Staatstrojaners.

---

[1] BVerfG, Urteil des Ersten Senats vom 27. Februar 2008, 1 BvR 370/07, Rn. (1-333), http://www.bverfg.de/e/rs20080227_1bvr037007.html

[2] Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt vom 25. Dezember 2008, http://www.bundesgerichtshof.de/SharedDocs/Downloads/DE/Bibliothek/Gesetzesmaterialien/16_wp/terrorismusabwehr_int_bka/bgbl108s3083.pdf;jsessionid=51B97D121F672E704ED6C241A4BB6BC6.1_cid368?__blob=publicationFile

Oktober 2011: Der Chaos Computer Club analysiert vom Landeskriminalamt Bayern eingesetzte Schadsoftware und deckt schwere technische Mängel und ein rechtswidriges Vorgehen auf.[3]

Februar 2016: Noch vor Abschluss der Prüfung durch das Bundesverfassungsgericht gibt das BKA bekannt, dass es über eine neue Schadsoftware zur Durchführung der Quellen-TKÜ verfüge. Das Bundesministerium des Innern (BMI) gibt die Software zur Nutzung frei, eine Billigung durch die Bundesdatenschutzbeauftragte wird nicht angestrebt.[4]

April 2016: Das Bundesverfassungsgericht kommt zu einem Urteil über das 2008 verabschiedete BKA-Gesetz und setzt darin erneut Grenzen für den Einsatz von staatlicher Schadsoftware.[5]

Zur Terrorismusabwehr sind seitens des BKA somit sowohl Quellen-TKÜ als auch Online-Durchsuchung bereits seit Dezember 2008 rechtlich zulässig, nach dem Urteil sind jedoch einige Regelungen für verfassungswidrig erklärt worden. Mit dem vorliegenden Änderungsantrag soll nun die Quellen-TKÜ ohne weitere Einschränkungen der einfachen Telekommunikationsüberwachung (TKÜ) gleichgestellt werden. Nur die Online-Durchsuchung soll auf schwerere Straftaten eingeschränkt bleiben.

Eine konventionelle Telekommunikationsüberwachung wird bekanntlich mit Hilfe des Telekommunikationsanbieters durchgeführt, der die Aufforderung erhält, die im Rahmen der Telekommunikationsvorgänge eines Verdächtigen anfallenden Daten an die Strafverfolgungsbehörden auszuleiten. Das Kommunikationsgerät der Zielperson bleibt dabei unberührt: Nur der Leitungsweg wird angezapft. Die gesetzlichen Schranken für diese Form der Überwachung nun auf eine weit komplexere, technisch anspruchsvolle und direkt in das betroffene Systeme eingreifende Methode anwenden zu wollen, zeugt von erheblicher Ignoranz für die damit einhergehenden Risiken.

Die im Jahr 2008 mit der Begründung der Terrorismusabwehr eingeführten Grundrechtseinschränkungen würden damit von der *ultima ratio* der inneren Sicherheit zum maximalinvasiven Alltagsinstrument der Strafverfolgung. Dabei konnten trotz des erheblichen Eingriffs in die Persönlichkeitsrechte und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme bisher die Notwendigkeit, Wirksamkeit und Effektivität dieser Maßnahmen nicht belegt werden. Die Infektion von Rechnern mit Schadsoftware ist keineswegs alternativlos, jedoch unbestritten mit zahlreichen Risiken verbunden. Keines dieser Risiken ist

---

[3] Chaos Computer Club (2011): *Analyse einer Regierungs-Malware,*
https://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf
Chaos Computer Club (2011): *0ZAPFTIS – Analyse einer Regierungs-Malware – Teil 2,*
https://www.ccc.de/system/uploads/83/original/staatstrojaner-report42.pdf

[4] Spiegel Online vom Mittwoch, 24.02.2016: *Innenministerium gibt umstrittenen Bundestrojaner frei,*
http://www.spiegel.de/netzwelt/netzpolitik/bundestrojaner-innenministerium-gibt-spaehsoftware-frei-a-1078656.html

[5] BVerfG, Urteil des Ersten Senats vom 20. April 2016, 1 BvR 966/09, Rn. (1-29),
http://www.bverfg.de/e/rs20160420_1bvr096609.html

jedoch mit einer konventionellen Telekommunikationsüberwachung verbunden, die rechtliche Gleichsetzung beider Maßnahmen verbietet sich daher auf technischer und rechtlicher Ebene.

Eine Ausweitung der Nutzung von Schadsoftware wird unweigerlich Folgen nach sich ziehen, die bereits in Staaten zu beobachten sind, deren Regierungen staatlichen Behörden eine Erlaubnis zum Hacken gegeben haben. Generell betreffen diese nachfolgend skizzierten Folgen sowohl konkrete technische Risiken als auch ökonomische Fragen, da die Ausnutzung von Sicherheitslücken und Schwachstellen mit einem Anbietermarkt in Zusammenhang steht. Angesichts der Tatsache, dass wir bereits heute vor erheblichen Problemen bei der technischen Beherrschbarkeit der Sicherheit von IT-Systemen stehen, ist eine weitere Destabilisierung der IT-Sicherheit durch staatliche Alimentierung dieses Marktes nicht anzuraten.

1. Gefahr für die innere Sicherheit

Für jeden Einsatz von Schadsoftware im Rahmen der Quellen-TKÜ oder Online-Durchsuchung wird (a) eine auf das Zielsystem spezifisch angepasste Softwarelösung sowie (b) ein Angriffspunkt auf diesem System benötigt, der zur Infektion genutzt werden kann. Im vorliegenden Änderungsantrag findet die technische Realität dieser Infektion eines informationstechnischen Systems keine Berücksichtigung. Zwar wird der gewünschte Funktionsumfang der anzubringenden Schadsoftware allgemein erläutert, jedoch bleibt die zentrale Frage außer Acht, wie die Schadsoftware auf dem Gerät der Zielperson angebracht werden soll. Auch die Vielzahl der verschiedenen Zielsysteme und -anforderungen bleibt unbeachtet.

Eine Infektion durch Dritte ist grundsätzlich nur bei fehlenden oder fehlerhaften Zugangsbeschränkungen oder durch Ausnutzung einer Software-Schwachstelle möglich. Da vollständig fehlende Zugangsbeschränkungen in den seltensten Fällen vorkommen und diese darüber hinaus direkten physischen Zugriff auf das Gerät voraussetzen würden, wären vorhandene Software-Schwachstellen für den größeren Teil der Einsätze Grundvoraussetzung.

➡ *Software-Schwachstellen werden zur Infektion eines informationstechnischen Systems benötigt. Sie sind separat von der Infektion selbst, in diesem Falle einer Schadsoftware zur Quellen-TKÜ oder zur Online-Durchsuchung, zu betrachten. Über eine vorhandene Software-Schwachstelle lassen sich andere Infektionen anbringen, und eine Infektion kann unter Inanspruchnahme unterschiedlicher Schwachstellen angebracht werden. Das Vorhandensein einer Schwachstelle ist jedoch Voraussetzung für die Infektion.*

Das Common Vulnerability Scoring System[6] (CVSS) bietet als de-facto-Branchenstandard eine Möglichkeit zur einheitlichen Betrachtung des technischen Risikos von Software-Schwachstellen. Der Wertebereich des Basiswerts reicht dabei von 0 (kein Risiko) bis 10 (kritisch).

Eine Schwachstelle, die bei physischem Zugriff die Infektion mit einer Schadsoftware (beispielsweise zur Quellen-TKÜ) ermöglicht, wird gemäß CVSS als mittleres Risiko (CVSS = 6.8) ausgewiesen.[7] Eine solche Schwachstelle würde jedoch immer noch voraussetzen, dass Ermittler des Zielgerätes temporär habhaft werden. Entsprechend aufwendig und auffällig wäre ihr Einsatz im Rahmen von Ermittlungsverfahren.

Um eine vom Nutzer des Gerätes unbemerkte Infektion vorzunehmen, wird eine Schwachstelle benötigt, die sich über das Netzwerk ausnutzen lässt. Sofern diese eine Nutzerinteraktion

---

[6] The CVSS Special Interest Group: *Common Vulnerability Scoring System v3.0: Specification Document,* https://www.first.org/cvss/specification-document

[7] Vgl. https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Die Einschränkung der Verfügbarkeit ist zwar nicht Ziel des Angriffs, jedoch im Rahmen der hypothetischen Schwachstelle ebenfalls im Rahmen der Möglichkeiten des Angreifers. Aus diesem Grund wird die Schwachstelle mit dem Wert 6.6 statt 5.9 bewertet.

voraussetzt, beispielsweise das Bestätigen einer Warnmeldung, wird die Schwachstelle mit einem Wert von 8.8 als „hoch“ eingestuft.[8] Ist eine Infektion ohne weitere Nutzerinteraktion möglich, so gilt die Schwachstelle mit einem CVSS-Wert von 9.8 als „kritisch“.[9]

➡ *Zur Infektion werden mindestens mittlere, im Regelfall sogar schwere bis kritische Schwachstellen benötigt.*

Um eine fortwährende Ausnutzung der Schwachstelle sicherzustellen, muss diese geheim gehalten werden, da sonst mit ihrer Beseitigung zu rechnen wäre. Dies bedeutet im Umkehrschluss, dass die Schwachstelle ausnahmslos auf allen betroffenen Geräten weltweit vorhanden sein muss. Damit geht zwingend das Risiko einher, dass die Schwachstelle von anderen interessierten Gruppen, insbesondere von Kriminellen oder anderen staatlichen Akteuren ebenfalls entdeckt und ausgenutzt wird.

Diese Abwägung gilt für jede einzelne Schwachstelle unabhängig von der Intention im Einzelfall. Dem möglicherweise berechtigten und legitimen Interesse zur Nutzung einer Schwachstelle zum Zwecke der Strafverfolgung steht somit unweigerlich das Risiko für die Allgemeinheit gegenüber, das sich aus dem Vorhandensein der Schwachstelle ergibt. Je öfter die Schwachstelle ausgenutzt wird, desto mehr erhöht sich auch das Risiko ihrer Entdeckung durch Dritte, die durch forensische Analyse und Reverse Engineering das Einfallstor entdecken und für eigene Zwecke missbrauchen können. Nicht zuletzt deshalb ist es geboten, die Anzahl der Schadsoftware-Einsätze gering zu halten. Eine Ausweitung wie im Änderungsantrag vorgesehen steht diesem Gebot jedoch entgegen.

Aus den offensichtlichen Erwägungen zur inneren Sicherheit ist es daher grundsätzlich falsch, das Wissen über Schwachstellen geheim zu halten und somit ihre Beseitigung zu verhindern oder aktiv zu verzögern. Entsprechend risikoarme und grundrechtsschonende Alternativen sind zu entwickeln.

➡ *Mit der Geheimhaltung von Wissen über Schwachstellen geht grundsätzlich ein Risiko für die innere Sicherheit einher, dessen Ausmaß proportional zur Anzahl und Kritikalität der betroffenen Geräte ist.*

Selbstverständlich wird regelmäßig argumentiert, dass staatliche Stellen mit dem Wissen über Schwachstellen verantwortungsbewusst und im strengen Rahmen rechtlicher Regulierung umgehen. Dabei wird außer Acht gelassen, dass Schwachstellen grundsätzlich agnostisch gegenüber Angreifer und Angriffsmotivation sind: Sie stehen allen, die Kenntnis darüber erlangen, gleichermaßen zur Verfügung.

So wurde der massenhafte Ausbruch der Schadsoftware „WannaCry“ durch eine kritische Schwachstelle (CVSS-Basiswert 8.1-9.3) ermöglicht,[10] über die der US-amerikanische Geheimdienst

[8] Vgl. https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

[9] Vgl. ebd.

[10] National Vulnerability Database: CVE-2017-0144 Detail, https://nvd.nist.gov/vuln/detail/CVE-2017-0144

NSA seit mindestens fünf Jahren Kenntnis hatte.[11] Zu den von WannaCry betroffenen Institutionen und Unternehmen gehörten zahlreiche Unternehmen, die den „Kritischen Infrastrukturen" zuzuordnen sind, unter anderem der spanische Telekommunikationskonzern Telefónica, das brasilianische Telekommunikationsunternehmen Vivo, der britische National Health Service (NHS) mit mehreren Krankenhäusern, das US-Logistikunternehmen FedEx, die Deutsche Bahn mit der Logistiktochter Schenker sowie das Russische Innenministerium (MWD), das Katastrophenschutzministerium sowie das Telekommunikationsunternehmen MegaFon.

Dieses Ausmaß an Schaden wurde erreicht, obwohl Microsoft zwei Monate zuvor einen Patch für die Schwachstelle bereitgestellt hatte, nachdem ein entsprechendes Angriffswerkzeug der NSA von Unbekannten gestohlen wurde. Zum Zeitpunkt der WannaCry-Angriffe war der größere Teil der betroffenen Systeme daher bereits „immun". Das Risiko, das die NSA durch das Geheimhalten der Schwachstelle für mehrere Jahre einging, war weitaus größer: Gemessen am möglichen Desaster-Ausmaß können die WannaCry-Angriffe als glimpflicher Ausgang bezeichnet werden. Allerdings ist die Veröffentlichung der Hacking-Werkzeuge der US-Behörden durch eine unbekannte Gruppe mit dem Namen „TheShadowsBrokers" zu diesem Zeitpunkt noch nicht abgeschlossen,[12] so dass weitere derartige Vorfälle nicht auszuschließen sind.

➡ *IT-Sicherheit ist ein kritischer Bestandteil der inneren Sicherheit. Kritische Infrastrukturen werden zu großen Teilen mit Standard-Software betrieben und verfügen über die gleichen Schwachstellen, die zur Infektion mit staatlicher Schadsoftware benötigt werden. Das Geheimhalten dieser Schwachstellen setzt somit die Kritischen Infrastrukturen einem direkten und unnötigen Angriffsrisiko aus.*

Zu der allgemeinen Frage, wie staatliche Stellen überhaupt Kenntnis von öffentlich nicht bekannten, zur Infektion informationstechnischer Systeme geeigneter Schwachstellen erlangen können, hat der Chaos Computer Club bereits 2016 Stellung genommen:[13]

> *„In den letzten Jahren ist international eine verstärkte Verbreitung kommerziell angebotener staatlicher Überwachungstrojaner zu verzeichnen. Diese Entwicklung ist problematisch, da das staatliche Ausnutzen von Schwachstellen einen Interessenkonflikt darstellt. Er besteht vor allem darin, dass aus wirtschaftlichen und Gemeinwohlerwägungen heraus ein hohes staatliches Interesse darin liegt, Computer-Schwachstellen schnell zu schließen, um Wirtschaftsspionage*

---

[11] The Washington Post, 16. Mai 2017: *NSA officials worried about the day its potent hacking tool would get loose. Then it did,* https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html

[12] Vgl. „TheShadowBrokers Monthly Dump Service – June 2017",
https://steemit.com/shadowbrokers/@theshadowbrokers/theshadowbrokers-monthly-dump-service-june-2017

[13] Constanze Kurz, Linus Neumann, Frank Rieger, Dirk Engling (2016): *Stellungnahme zur „Quellen-TKÜ" nach dem Urteil des Bundesverfassungsgerichts vom 20. April 2016, 1 BvR 966/09,*
https://ccc.de/system/uploads/216/original/quellen-tkue-CCC.pdf

> *zurückzudrängen und die grauen Märkte, in denen diese Sicherheitslücken gehandelt werden, nicht zusätzlich zu befeuern.*
>
> *Tritt der Staat als Käufer von Exploits auf, liegt es jedoch in seinem Interesse, die Sicherheitslücke möglichst lange selbst ausnutzen zu können und entsprechend nicht zu schließen. Generell wird der europäische Markt durch das Auftreten staatlicher Behörden als Käufer sowohl für die Verkäufer von ausnutzbaren Sicherheitslücken als auch für die spezialisierten Anbieter von Spionagesoftware attraktiver. Wenn die „Quellen-TKÜ" und damit der Einbruch in informationstechnische Systeme als Ermittlungsinstrument angestrebt wird, sollte zuvor eine Folgenabschätzung vorgenommen werden, um die Effekte auf diesen Markt abzuschätzen."*

Diese Situation besteht unverändert fort, weswegen diese Folgenabschätzung noch immer zu fordern ist.

2. Unverhältnismäßiger Grundrechtseingriff bei niedriger rechtlicher Schwelle

Gerade weil der Einsatz von Schadsoftware ein besonders schwerwiegender Grundrechtseingriff ist, hat das Bundesverfassungsgericht das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme überhaupt erst definiert. Diese wegweisende und weitsichtige Entscheidung wurde in einer Zeit getroffen, als die Digitalisierung aller Lebensbereiche noch weit weniger vorangeschritten war, als es heute der Fall ist.

Die Geschwindigkeit und die Dynamik, mit der diese Digitalisierung voranschreitet, erfordern eine behutsame und bedachte Politik, die der vorliegende Änderungsantrag vermissen lässt. Im Jahr 2008 war das Smartphone gerade erfunden worden, und die Entwicklung der digitalen Sphäre stand am Anfang der in ihrer Folge massiven gesellschaftlichen Veränderungen. Heute sind informationstechnische Systeme zum wesentlichen Ablagemedium für berufliche Informationen und private, sogar intimste Gedanken geworden.

Gleichermaßen stehen wir heute am Beginn der Digitalisierung aller Produkt- und Lebensbereiche. Die informationstechnischen Systeme einer Zielperson mögen heute noch weitestgehend auf Personal Computer und Smartphones beschränkt sein. In absehbarer Zeit wird eine Vielzahl an verschiedenen Produkten keinen Aspekt des Lebens mehr unerfasst lassen. Digitale Systeme werden zu weit mehr als Telekommunikationsmedien: zu unserem ausgelagerten Gehirn, das mehr über uns weiß, als wir selbst.

Technischer Kern sowohl der Quellen-TKÜ als auch der Online-Durchsuchung ist die erfolgreiche Manipulation des Rechners oder Smartphones und künftig weiterer, heute noch nicht typischer informationstechnischer Systeme, um die gewünschten Daten zu erlangen. Vor diesem Hintergrund ist zu betonen, dass – im Gegensatz zur Telekommunikationsüberwachung auf der Leitung oder einer Hausdurchsuchung – die Differenzierung in Quellen-TKÜ und Online-Durchsuchung eine rein virtuelle und willkürliche Unterscheidung ist, für die es keine reale technische Entsprechung geben kann: Informationstechnische Systeme sind universell programmierbar und einsetzbar. Entsprechend groß ist die Vielfalt an Kommunikationsmethoden und -applikationen, die eine Zielperson zum Einsatz bringen kann. Sie alle zielgerichtet erfassen zu können, ohne das informationstechnische System in der Vielzahl seiner weiteren Funktionen und Anwendungen zu erfassen, ist nicht möglich.

Dass die 2011 vom CCC analysierte staatliche Schadsoftware das Erfassen von E-Mail-Nachrichten und Chats durch das „Abfotografieren“ des gesamten Bildschirms realisierte, lässt sich nicht nur durch einen zufälligen oder nachlässigen Verstoß gegen die gesetzlichen Bestimmungen erklären: Es war auch Ausdruck der schieren Hilflosigkeit der Programmierer bei dem Versuch, in ihrer Software die schon damals kaum zu überblickenden verschiedenen Kommunikationsmöglichkeiten im Rahmen der Überwachungsmaßnahme zu erfassen. Eine der vielen Lehren aus diesem Skandal lautet daher auch, dass eine „reine“ Quellen-TKÜ praktisch nicht realisierbar ist.

Spionagesoftware leitet stets über die Überwachung der laufenden Telekommunikation hinausgehende Daten aus. Entsprechend stellte der Chaos Computer Club in seiner Stellungnahme 2015 fest:[14]

> *„De facto handelt es sich bei der Quellen-TKÜ um eine optische und akustische Wohnraumüberwachung, sowohl beim Benutzer des Systems als auch bei Kommunikationspartnern, die mit dem Tatvorwurf nichts zu tun haben könnten. Diese optische und akustische Überwachung wird nach der Plazierung der Computerwanze auf dem Zielsystem automatisch selektiv aktiviert, wenn eine der zu überwachenden Applikationen auf dem informationstechnischen System eine Kommunikation einleitet oder angeschaltet wird. Daß die betreffende Anwendung wirklich aktiv ist und sich die Überwachung primär auf den Kommunikationsvorgang erstreckt, ist nicht mit abschließender Sicherheit zu garantieren.“*

Daran hat sich auch 2017 nichts geändert.

➡ *Für die juristische Unterscheidung in Quellen-TKÜ und Online-Durchsuchung gibt es keine adäquate technische Entsprechung. Die Eingriffstiefe einer „Quellen-TKÜ“ ist nicht mit der einer Telekommunikationsüberwachung zu vergleichen.*

Das Bundesamt für Justiz berichtet für das Jahr 2015 eine Gesamtanzahl von

- **3.332** Anordnungen zur Überwachung von Festnetz-Telekommunikation,
- **21.905** Anordnungen zur Überwachung von Mobilfunk-Kommunikation,
- **7.432** Anordnungen zur Überwachung von Internet-Kommunikation.

Der Großteil dieser Anordnungen erfolgte im Rahmen der Überwachung von Ermittlungsverfahren wegen Verstoßes gegen das Betäubungsmittelgesetz.[15]

Durch die Gleichsetzung der rechtlichen Voraussetzungen von Quellen-TKÜ mit konventioneller Telekommunikationsüberwachung auf der Leitung erhält das bisher der Terrorismusabwehr und der Verfolgung schwerer Straftaten vorbehaltene Mittel Einzug in den Ermittlungsalltag.

➡ *Die Quellen-TKÜ würde von der „ultima ratio“ zum Standardinstrument der Strafverfolgung werden. Die Eingriffsschwere gebietet jedoch höhere rechtliche Hürden, um einen inflationären Einsatz zu verhindern.*

---

[14] Constanze Kurz, Dirk Engling, Frank Rieger, Thorsten Schröder (2015): *Stellungnahme an das Bundesverfassungsgericht zum BKA-Gesetz und zum Einsatz von Staatstrojanern, 1 BvR 966/09, 1 BvR 1140/09*, http://www.ccc.de/system/uploads/189/original/BKAG_Stellungnahme.pdf

[15] Bundesamt für Justiz, Referat III: Übersicht Telekommunikationsüberwachung (Maßnahmen nach § 100a StPO) für 2015, Stand 14.07.2016, https://www.bundesjustizamt.de/DE/SharedDocs/Publikationen/Justizstatistik/Uebersicht_TKUE_2015.pdf?__blob=publicationFile&v=2

3. Fehlender Beleg der Notwendigkeit

Zur Begründung der Ausweitung des schweren Grundrechtseingriffs der Quellen-TKÜ wird im vorliegenden Änderungsantrag angeführt:[16]

> *„Die Nutzung dieser mobilen Geräte ersetzt zunehmend die herkömmlichen Formen der Telekommunikation. Das Internet als komplexer Verbund von Rechnernetzen öffnet dem Nutzer eines angeschlossenen Systems nicht nur den Zugriff auf eine praktisch unübersehbare Fülle von Informationen, die von anderen Netzrechnern zum Abruf bereitgehalten werden. Es stellt ihm daneben zahlreiche neuartige Kommunikationsdienste zur Verfügung, mit deren Hilfe er über das Internet aktiv soziale Verbindungen aufbauen und pflegen kann, ohne herkömmliche Formen der Telekommunikation in Anspruch nehmen zu müssen.“*

Es wird der Eindruck erweckt, die vielfältigen Möglichkeiten der Telekommunikationsüberwachung gemäß § 110 Telekommunikationsgesetz und Telekommunikations-Überwachungsverordnung, die bereits seit 2005 bestehen, sowie die vollumfängliche Internet-Metadaten-Überwachung gemäß dem 2015 erlassenen Gesetz zur Wiedereinführung der vorher bereits für verfassungswidrig erklärten Vorratsdatenspeicherung[17] stünden Strafverfolgungsbehörden gar nicht zur Verfügung. Mit der wieder eingeführten Vorratsdatenspeicherung wird ab 1. Juli 2017 (§ 150 Abs. 13 TKG) der Vollzugriff auf sämtliche Metadaten der Internetkommunikation der Bundesrepublik ermittlungstechnischer Alltag.

Ferner wird angeführt, dass das Ziel der Quellen-TKÜ primär die Erfassung verschlüsselter Kommunikationsinhalte ist:

> *„Im Bereich der Strafverfolgung ist umstritten, inwieweit die Überwachung insbesondere verschlüsselter Kommunikation über das Internet zulässig ist. Die Möglichkeit eines verdeckten Eingriffs in informationstechnische Systeme zum Zweck ihrer Durchsuchung besteht bislang für die Strafverfolgungsbehörden nicht.“*

Es wird der Anschein erweckt, dass verschlüsselte Kommunikation Strafverfolgungsbehörden sämtlicher Ermittlungsansätze berauben und auf diese Weise eine Strafverfolgung oder Gefahrenabwehr verhindern würde. Diese unter dem Stichwort „Going Dark“ bekannt gewordene

---

[16] Deutscher Bundestag, Ausschuss für Recht und Verbraucherschutz: Ausschussdrucksache 18(6)334: Formulierungshilfe der Bundesregierung für einen 15.05.2017 Änderungsantrag der Fraktionen CDU/CSU und SPD zu dem Gesetzentwurf der Bundesregierung – Drucksache 18/11272 – Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze, https://www.bundestag.de/blob/507632/c2362af32d325de93cc8342400d998bd/formulierungshilfe-data.pdf, dauerhaft verfügbar unter https://netzpolitik.org/2017/wir-veroeffentlichen-den-gesetzentwurf-der-grossen-koalition-zum-massenhaften-einsatz-von-staatstrojanern/#Formulierungshilfe

[17] Bundesrat Drucksache 492/15: Gesetzesbeschluss des Deutschen Bundestages – Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, http://dip21.bundestag.de/dip21/brd/2015/0492-15.pdf

Behauptung geht auf den ehemaligen FBI-Direktor James Comey zurück[18] und ist eine direkte öffentliche Reaktion zur Rechtfertigung der Enthüllungen Edward Snowdens, der eine bis heute fortdauernde Massenüberwachung durch US-Geheimdienste und Strafverfolgungsbehörden belegte.

Snowdens Enthüllungen zeigten das Gegenteil dessen, was als „Going Dark" bezeichnet wird: Ermittlungsbehörden verfügen trotz der zunehmenden Verschlüsselung von Gesprächsinhalten über mehr Daten und Ermittlungsansätze als je zuvor. Primär liegt dies an der Digitalisierung der gesamten Kommunikation an sich sowie an den heute typischen Online-Geschäftsmodellen und Zentralisierungstendenzen: Zugriff auf Nutzerdaten zum Zwecke der Auswertung ist treibender Wirtschaftsfaktor fast aller Online-Dienste. Für diese Geschäftsmodelle ist es unerlässlich, dass die Anbieter Einsicht in unverschlüsselte Daten ihrer Nutzer haben. Die Zentralisierungstendenzen lassen sich primär im Wandel von produktbasierten zu Dienstleistungsmodellen beobachten, die eine zentralisierte Erfassung begünstigen.

Auch bei verschlüsselten Kommunikationsinhalten fallen in der Regel Metadaten an, deren Analyse sehr genaue Einblicke in Bewegungsprofile, Gruppenzugehörigkeiten und Kommunikationsmuster ermöglicht und damit mannigfaltige Ermittlungsansätze liefert. Deutsche Strafverfolger sammeln diese Metadaten beispielsweise im Rahmen der sogenannten Funkzellenabfrage gemäß § 100g Abs. 3 StPO, der Telekommunikationsüberwachung gemäß § 110 TKG und zukünftig der sämtliche Internetkommunikation umfassenden Vorratsdatenspeicherung gemäß § 150 Abs. 13 TKG. Durch die Anwendung sogenannter „Stiller SMS" werden sogar eigens Metadaten erzeugt, Mobiltelefone regelmäßig als Ortungswanzen missbraucht und auf diese Weise eine Ausweitung der durch Telekommunikationsüberwachung erlangten Erkenntnisse erreicht. Die heute bereits existierende Fülle der Erfassungsmöglichkeiten lässt einzig einige Inhalte verschlüsselter Kommunikation außen vor: Für die Erfassung und Auswertung sämtlicher sonstigen Kommunikationsinhalte und Metadaten gibt es bereits eine Ermächtigungsgrundlage. Zusätzlich ist zu konstatieren, dass die Fülle an informationstechnischen Systemen, die Menschen heute in allen Lebenslagen umgeben, eine Menge an Datenspuren erzeugt, die noch vor wenigen Jahren kaum vorstellbar war. In dieser Konstellation entbehrt die Behauptung, man säße ermittlungstechnisch im Dunkeln, jeder Grundlage.

Doch auch unter der unzutreffenden Annahme, dass „Going dark" ein tatsächliches Phänomen wäre, existiert im Bereich der nationalen Sicherheit keine Schutzlücke, da die Mittel der Online-Durchsuchung und Quellen-TKÜ dem BKA bereits seit 2008 zur Verfügung stehen. Der vorliegende Änderungsantrag zielt jedoch darauf ab, diese als *ultima ratio* zum Schutz der nationalen Sicherheit begründeten Grundrechtseingriffe zu einem ermittlungstechnischen Alltag zu machen, ohne dass in diesem Bereich eine nennenswerte Schutzlücke belegt werden kann.

---

[18] James B. Comey, Director Federal Bureau of Investigation (2014): *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?,*
https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

4. Fehlende technische Überprüfbarkeit und Nachvollziehbarkeit

Informationstechnische Systeme sind universell programmierbar. Dies bedeutet, dass sie prinzipbedingt jede Funktion haben oder auch nicht haben können. Der genaue Funktionsumfang einer im Rahmen der Strafverfolgung zum Einsatz gebrachten Schadsoftware ist jedoch von fundamentaler Bedeutung für die Bewertung und Einordnung der auf diesem Wege erbrachten Indizien und Beweise sowie zur Beurteilung der Rechtmäßigkeit des Einsatzmittels.

Die im Jahre 2011 veröffentlichte Analyse des „Bundestrojaners" offenbarte beispielsweise Programmierfehler, die neben einer weiteren Schwächung der Integrität des Zielsystems auch noch eine beliebige Erweiterbarkeit der Funktionalität der Schadsoftware zufolge hatten – und das auch durch Dritte.[19]

Während die technischen Rahmenbedingungen einer Telekommunikationsüberwachung sich auch Laien vollständig erschließen können, handelt es sich bei einer Quellen-TKÜ um einen komplexen, intransparenten und nur durch Experten nachvollziehbaren und zu bewertenden Vorgang. Da auch digital erfasste Daten per se keinen Integritätsschutz haben, also zu jedem Zeitpunkt beliebig veränderbar sind, sind mehrere technische Anforderungen unabdingbar, um die Beweiskraft und Rechtmäßigkeit einer Online-Durchsuchung oder einer Quellen-TKÜ sicherzustellen.

Der vorliegende Änderungsantrag macht hierzu nur vage, daher nicht überprüfbare und rechtlich verbindliche technische Vorgaben:[20]

> *„Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen."*

Diese Vorgaben sind nicht ausreichend, um Rechtssicherheit und Überprüfbarkeit zu erreichen. Die parlamentarische Gruppe „Civici e Innovatori" der 17. Legislatur des italienischen Parlaments hat im

---

[19] Chaos Computer Club (2011): *Analyse einer Regierungs-Malware,* https://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf

[20] Deutscher Bundestag, Ausschuss für Recht und Verbraucherschutz: Ausschussdrucksache 18(6)334: Formulierungshilfe der Bundesregierung für einen 15.05.2017 Änderungsantrag der Fraktionen CDU/CSU und SPD zu dem Gesetzentwurf der Bundesregierung – Drucksache 18/11272 – Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze, https://www.bundestag.de/blob/507632/c2362af32d325de93cc8342400d998bd/formulierungshilfe-data.pdf, dauerhaft verfügbar unter https://netzpolitik.org/2017/wir-veroeffentlichen-den-gesetzentwurf-der-grossen-koalition-zum-massenhaften-einsatz-von-staatstrojanern/#Formulierungshilfe

Februar 2017 mehrere technische Anforderungen vorgeschlagen, die ein Mindestmaß an Rechtssicherheit und Überprüfbarkeit definieren.[21] Dazu gehören:

A. Der Quellcode muss hinterlegt und verifizierbar sein. Den Vorgang des Umwandelns des menschenlesbaren Quellcodes in ein ausführbares Programm wird als „Kompilieren" bezeichnet. Das resultierende Programm ist in seiner Funktionsweise sehr viel komplizierter und kaum abschließend zu erfassen. Erschwerend kommt hinzu, dass eine solche als „reverse engineering" bezeichnete Analyse bei Schadsoftware regelmäßig durch verschiedene Verschleierungsmaßnahmen erschwert wird, beispielsweise um den Schutz des Zielsystems durch Virenscanner auszuhebeln.

Für alle Betroffenen und auch für die zuständigen Datenschutzbehörden muss eine Einsichtnahme in den Quellcode zur Prüfung der rechtmäßigen Ausgestaltung der Spionagesoftware gesetzlich festgeschrieben werden. Zu diesem Schluss kam bereits der Bericht des bayerischen Landesbeauftragten für den Datenschutz, dessen Behörde als eine der wenigen staatlichen Kontrollbehörden überhaupt je Einblick in tatsächlich zum Einsatz gekommene staatliche Spionagesoftware nehmen konnte. Der Landesbeauftragte empfahl, sowohl bei konkretem Anlass als auch generell eine Quellcode-Sichtung zu ermöglichen:[22]

> *„Es wäre jedoch geboten, den jeweiligen Quellcode einzusehen, wenn hierzu ein konkreter Anlass besteht. Um verdeckte Funktionalitäten zuverlässig auszuschließen, ist auch die stichprobenartige Einsichtnahme in den Quellcode zu empfehlen."*

Ohne das Ergreifen besonderer Maßnahmen beim Kompilieren des Quellcodes zu einer ausführbaren Datei kommt es regelmäßig zu unterschiedlichen Ergebnissen. Dies erschwert eine Beweisführung, dass eine zum Einsatz gebrachte Schadsoftware tatsächlich dem zertifizierten Quellcode entspricht. Durch das Vorschreiben eines Vorgehens zur Sicherstellung reproduzierbarer Kompilierungsergebnisse[23] kann diese Schutzlücke geschlossen werden.

B. Jede Aktion muss vollständig, manipulationssicher und verifizierbar dokumentiert werden. Von der Infektion über die Datenextraktion bis zur Desinfektion muss der gesamte Vorgang der Quellen-TKÜ oder Online-Durchsuchung nachvollziehbar protokolliert sein, um es sowohl

---

[21] Civici e Innovatori: *Disciplina dell'uso dei captatori legali nel rispetto delle garanzie individuali,*

- Gesetzesvorschlag: http://www.civicieinnovatori.it/wp-content/uploads/2017/02/PDL-Captatori-Legali_DEFV3.pdf
- Technische Regeln: http://www.civicieinnovatori.it/wp-content/uploads/2017/02/DisciplinareTecnicoPropostadiLeggeCaptatore.pdf
- Begründung und Inhalt der technischen Regeln: http://www.civicieinnovatori.it/wp-content/uploads/2017/02/PDL-Captatori-Legali_DEFV3.pdf
- Zusammenfassung in englischer Sprache: *Rules governing the use of government trojan with respect for individual rights,* http://www.civicieinnovatori.it/wp-content/uploads/2017/02/Sintesi-PDL-captatori-EN.pdf

[22] Der Bayerische Landesbeauftragte für den Datenschutz (2012): *Prüfbericht Quellen-TKÜ*, S. 20f., https://www.datenschutz-bayern.de/0/bericht-qtkue.pdf

[23] Vgl. bspw. https://reproducible-builds.org

Richtern als auch Betroffenen zur Beweisführung zu ermöglichen, das Vorgehen der Ermittler nachzuvollziehen. Das Protokoll muss auf eine Weise angefertigt und gespeichert werden, die sowohl seine Umgehung als auch seine nachträgliche Veränderung verhindert. Kryptographische Hash-Funktionen eignen sich dabei zur beweissicheren Aufnahme von extrahierten Dateien, ohne deren Inhalte zum Teil des Protokolls werden zu lassen.

Weiterhin kann durch sogenannte Hash-Chains die Vorwärts-Integrität des Logs erhöht werden. Das Log sollte zwingend off-site und außerhalb des vom Angreifer kontrollierten Bereichs geführt werden, um die Manipulationswahrscheinlichkeit zu minimieren. Insbesondere sollten auf diese Weise auch die Löschvorgänge gemäß des geplanten § 100d (2) StPO inklusive der Prüfsummen-Hashes der gelöschten Dateien dokumentiert werden. Dies ermöglicht es, Eingriffe in den Kernbereich privater Lebensgestaltung auch im Nachhinein zu erkennen, und mindert damit unerkannten Missbrauch.

C. Die Schadsoftware darf nicht das allgemeine Sicherheitsniveau des Gerätes schwächen. Unter 1. wurde bereits dargestellt, dass vorhandene Schwachstellen Grundvoraussetzung für die Infektion eines Zielgerätes sind. Darüber hinaus verfügt eine steigende Anzahl informationstechnischer Systeme über Sicherheitsmaßnahmen, die eine Infektion verhindern oder erschweren sollen. Hierzu gehören insbesondere Maßnahmen der Integritätssicherung wie Code-Signing und Secure Boot. Das Umgehen derartiger Schutzmechanismen wird häufig als *„jailbreak“* bezeichnet und ist bei vielen Geräten Voraussetzung für eine erfolgreiche persistente Infektion mit Schadsoftware.

Das *Jailbreaking* setzt jedoch dauerhaft die Sicherheitsmaßnahmen außer Kraft und erlaubt das Ausführen arbiträren Programmcodes. Das Ergebnis ist ein gemindertes Grundsicherheitsniveau des Zielgerätes, welches infolgedessen einfacher durch weitere Angreifer infiziert werden kann. Eine derartige Kompromittierung und Risikoerhöhung ist im Rahmen staatlich angeordneter Maßnahmen nicht hinnehmbar.

D. Die Entwicklung und der Einsatz der Schadsoftware muss mittels einer zentralen Erfassung nachvollziehbar sein. Analog zur oben dargestellten manipulationssicheren Aufbewahrung von extrahierten Daten müssen auch die unterschiedlichen Versionen und Varianten der zum Einsatz gebrachten Schadsoftware-Typen festgehalten werden, um zu jedem Zeitpunkt eine vollständige Untersuchung zu ermöglichen.

E. Eine unabhängige Zertifizierung der technischen und datenschutzrechtlichen Vorgaben muss regelmäßig erneuert werden. Den Vorgaben gemäß A. entsprechend, sollte jede zum Einsatz gebrachte Version der Schadsoftware durch eine unabhängige Stelle geprüft und zertifiziert werden, bevor diese zum Einsatz kommt: Die Feststellung jahrelanger rechtswidriger Praxis kann nicht zur Beweislast der im Strafverfahren Beschuldigten gemacht werden. Jede Änderung der Schadsoftware muss gemäß D. protokolliert und wesentliche Zusatzfunktionen neu zertifiziert werden.

Zudem kann bei der vorliegenden Eingriffsintensität auf eine Evaluation auch der richterlichen Beschlüsse, die eine Quellen-TKÜ oder Online-Durchsuchung anordnen, nicht verzichtet werden. Sie soll neben den technischen Vorgaben auch die Sinnhaftigkeit der Einsätze sowie langfristige Folgen unabhängig untersuchen.

F. Verschlüsselung und Integritätsschutz der erfassten Daten. Die mit Hilfe der Schadsoftware extrahierten Daten müssen nach dem Stand der Technik verschlüsselt und gegen Manipulation geschützt ausschließlich auf informationstechnischen System unter der Hoheit der Strafverfolgungsbehörden gespeichert werden.

G. Beschränkung hoheitlicher Aufgaben auf staatliche Stellen. Der Eingriff in die Vertraulichkeit und Integrität eines informationstechnischen Systems ist ein schwerer Grundrechtseingriff im Rahmen der hoheitlichen Aufgabe der Strafverfolgung. Ein Auslagern dieser Aufgabe auf privatwirtschaftliche Dienstleister ist daher grundsätzlich abzulehnen. Sämtliche Schadsoftware muss direkt von Strafverfolgungsbehörden angebracht und bedient werden.

Verstöße gegen dieses Gebot sind dabei kein theoretisches Konstrukt, sondern gängige Praxis in Ländern wie Bahrain, Äthiopien, Bangladesch, den Niederlanden, Estland, Australien, der Mongolei oder Nigeria, die Schadsoftware vom Zulieferer und Betreiber Gamma International einsetzen.[24] Das Bundeskriminalamt beschaffte die Software bereits im Oktober 2012.[25] Weder der in den seltensten Fällen in demokratischer Tradition stehende Kundenstamm des Unternehmens noch ein erfolgreicher Hacking-Angriff auf Gamma International/FinFisher wird vom Bundeskriminalamt als Hindernis für eine Zusammenarbeit gesehen, wie aus einem Bericht des Bundesrechnungshofs hervorgeht:[26]

> *„Die Analyse des Hacking-Angriffs auf einen Internet-Server der Firma FinFisher im Zeitraum vom 1. bis 3. August 2014, in dessen Folge ca. 40 Gigabyte interne Daten der Firma erlangt und im Internet veröffentlicht wurden, hat das BKA im November 2014 mit dem Ergebnis abgeschlossen, die Zusammenarbeit mit der Firma fortzusetzen.“*

---

[24] Ben Wagner, Claudio Guarnieri (2014): *Finfisher – Deutsche Firmen verdienen Millionen mit Überwachungstechnik,* in Zeit Online vom 5. September 2014,
http://www.zeit.de/digital/datenschutz/2014-09/export-finfisher-gamma-gastbeitrag

[25] Andre Meister (2013): *Bundeskriminalamt bestätigt Anschaffung von Staatstrojaner Gamma FinFisher: „Wir haben die Software“,* https://netzpolitik.org/2013/bundeskriminalamt-bestatigt-anschaffung-von-staatstrojaner-gamma-finfisher-wir-haben-die-software/

[26] Der Bundesrechnungshof: Bericht zur Nr. 10 des Beschlusses des Haushaltsausschusses des Deutschen Bundestages zu TOP 20 der 74. Sitzung am 10. November 2011, öffentlich einsehbar unter: Andre Meister (2016): *Kritik vom Bundesrechnungshof: Das Bundeskriminalamt will gleich zwei Staatstrojaner einsetzen,*
https://netzpolitik.org/2016/kritik-vom-bundesrechnungshof-das-bundeskriminalamt-will-gleich-zwei-staatstrojaner-einsetzen/

5. Drohende Verletzung der Eckpunkte der deutschen Kryptopolitik

Durch Änderung des § 100a soll eine konventionelle TKÜ zur Quellen-TKÜ erweitert werden dürfen:

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

Hier stellt sich die Frage, ob damit auch Server-Systeme erfasst sein können. Ist dies der Fall, ließe sich aus dieser Ermächtigung eine Handhabe konstruieren, um beispielsweise für derartige Angriffe anfällige Systembetreiber zu zwingen, den Schlüsselaustausch einer sich aufbauenden Verschlüsselung zu beeinträchtigen, vergleichbar dem Vorgehen beim Abhören von Skype-Gesprächen. Praktisch würde dies bedeuten, dass der Dienstanbieter die Verschlüsselung umgeht.

Eine solche Ermächtigung zum Eingriff in informationstechnische Systeme wäre sehr weitreichend, jedoch unspezifisch formuliert, da der Betroffene nach dem Wortlaut der Regelung auch serverseitige Systeme seines Anbieters „nutzt". Damit würden Strafverfolgungsbehörden die Ermächtigung erhalten, auch auf Systemen der Dienstanbieter Manipulationen zur Absenkung des Sicherheitsniveaus vorzunehmen: etwa an den Servern, über die Nachrichten weitergeleitet werden oder über die der Schlüsselaustausch erfolgt, mit dem dann in der Folge Nachrichten verschlüsselt werden.

De facto ergäbe sich mit dieser Ermächtigung eine Verpflichtung von Dienstanbietern zur Duldung von staatlichen Hintertüren, die den auch vom BMI unterstützten Eckpunkten deutscher Kryptopolitik[27] klar widersprechen.

➡ *Mindestens muss eine deutliche Beschränkung auf die Manipulation von direkt vom Betroffenen genutzten Endgeräten und ein expliziter Ausschluss der Manipulation und Infiltration von Systemen der Dienstanbieter erfolgen, um eine uferlose Ausweitung der Eingriffsbefugnisse zu vermeiden.*

---

[27] Bundesministerium des Innern und Bundesministerium für Wirtschaft und Technologie vom 2. Juni 1999: *Eckpunkte der deutschen Kryptopolitik,* Quelle beim BMWI nicht mehr vorhanden, dauerhaft verfügbar unter, https://hp.kairaven.de/law/eckwertkrypto.html
Vgl. Deutscher Bundestag, Drucksache 14/1149, http://dipbt.bundestag.de/doc/btd/14/011/1401149.pdf und Deutscher Bundestag Drucksache 18/5144, http://dipbt.bundestag.de/dip21/btd/18/051/1805144.pdf

Die in der StPO definierte Mitwirkungspflicht der Anbieter von Telekommunikationsdiensten an Überwachungsmaßnahmen (neu: Absatz 4 § 100 StPO) wird durch die parallel zu diesem Gesetzgebungsverfahren angestrebte Ausweitung des Geltungsbereichs des TKG zum beweglichen Ziel in einem hochgradig kritischen Rechtsgebiet: Die vom Bundesrat geforderte Ausdehnung des TKG und damit des Kreises der gemäß dem vorliegenden Änderungsantrag zur Mitwirkung Verpflichteten auf alle Anbieter von „Messengerdiensten und standortbezogenen Diensten mit Telekommunikationsdiensten“[28] könnte in Kombination mit den hier angestrebten Änderungen der StPO ebenfalls zu einer Situation führen, in der Dienstanbieter zu einer Schaffung bzw. Duldung von Hintertüren für Behörden gezwungen werden können. Dies wäre erneut in direktem Widerspruch zu den Eckpunkten deutscher Kryptopolitik und würde zu einer erheblichen Verschlechterung von Vertrauen, Sicherheit und Marktposition deutscher Anbieter von Verschlüsselungslösungen führen.

➡ *Sämtliche derartige Gesetzesvorhaben müssen zwingend gemeinsam betrachtet werden.*

[28] Bundesrat Drucksache 88/16 vom 17.02.16: Entschließung des Bundesrates zur Anpassung des Rechtsrahmens an das Zeit- alter der Digitalisierung im Telekommunikationsbereich – Rechtssicherheit bei Messengerdiensten, standortbezogenen Diensten und anderen neuen Geschäftsmodellen,
http://www.bundesrat.de/SharedDocs/drucksachen/2016/0001-0100/88-16.pdf?__blob=publicationFile&v=1

Fazit

Mit dem Geheimhalten von Sicherheitslücken, die zum Anbringen von Schadsoftware genutzt werden können, geht ein hohes Risiko für die innere Sicherheit einher. Das Risiko für das Entdecken dieser Sicherheitslücken durch Dritte steigt mit der Häufigkeit ihrer Ausnutzung durch staatliche Stellen. Im Sinne der inneren Sicherheit ist eine Beseitigung sämtlicher Schwachstellen anzustreben und von deren Hortung und Geheimhaltung abzusehen.

Die Anwendung von Schadsoftware im Strafverfahren stellt einen schweren Grundrechtseingriff dar. Die rechtlichen Grenzen der sogenannten Quellen-Telekommunikationsüberwachung lassen sich technisch kaum umsetzen. Bei alltäglichen Strafverfahren gibt es keine Rechtfertigung derart schwerwiegender Grundrechtseingriffe.

Die Prämisse, dass Strafverfolgungsbehörden aufgrund von Verschlüsselung der Kommunikation keine Ermittlungsansätze oder Daten zur Verfügung stünden, hält der Empirie nicht stand. Das Gegenteil ist der Fall: Strafverfolgungsbehörden steht dank der fortschreitenden Digitalisierung aller Lebensbereiche eine nie dagewesene Fülle an Daten zur Verfügung.

Die technischen Rahmenbedingungen für den Einsatz von Schadsoftware sind sowohl für die generell abzulehnende gedankliche Konstruktion der Quellen-TKÜ als auch für die vollumfängliche Online-Durchsuchung nicht ausreichend spezifiziert: weder eine Rechtssicherheit noch adäquate Kontrollmöglichkeiten werden sichergestellt.

Eine Verletzung der Eckpunkte deutscher Kryptopolitik würde zu einer erheblichen Verschlechterung von Vertrauen, Sicherheit und Marktposition deutscher Anbieter von Verschlüsselungslösungen führen.

Der Änderungsantrag ist folglich in seiner Gänze abzulehnen.

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

Universität Osnabrück · FB 10 · 49069 Osnabrück

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

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 Quellentelekommunikations-überwachung (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.