DR. IUR. H. C. GERHARD STRATE
KLAUS-ULRICH VENTZKE
RECHTSANWÄLTE

DR. IUR. H.C. GERHARD STRATE
KLAUS-ULRICH VENTZKE
JOHANNES RAUWALD
RECHTSANWÄLTE

An das
Bundesverfassungsgericht
Schlossbezirk
76131 Karlsruhe

Hamburg, den 22. August 2018

In dem Verfahren

1. des Rechtsanwalts Stefan Conen, …,
2. der Rechtsanwaltsfachangestellen Sina Mika, …,
3. des Journalisten Hajo Seppelt, …,
4. des Journalisten Can Dündar, …,
5. des Rechtsanwalts und Mitglieds des Deutschen Bundestags

   Konstantin von Notz, …,

HOLSTENWALL 7 – 20355 HAMBURG
TELEFON: 040/4502160 - TELEFAX: 040/4502166 - GERICHTSKASTEN: 112
USt.-IdNr.: DE118301981

erhebe ich namens und in Vollmacht der Beschwerdeführerin und Beschwerdeführer

Verfassungsbeschwerde

gegen

§ 100a Abs. 1 Satz 2 und 3, Abs. 3 und 5

§ 100b

§ 100d Abs. 5 Satz 2 und 3

der Strafprozessordnung (StPO) in der Fassung des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017 (BGBl. I S. 3202)

und rüge eine Verletzung von Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, Art. 10 Abs. 1, Art. 12 Abs. 1 GG und Art. 19 Abs. 4 GG.

Wir bitten das Gericht, die Adresse des Beschwerdeführers zu 3 unbedingt geheim zu halten, weil er andernfalls physischen Gefahren ausgesetzt ist. Aus diesem Grunde ist bei den Beschwerdeführern zu 4 und zu 5 auch eine c/o-Adresse bzw. eine Büro-Adresse angegeben.

Alle drei erhalten regelmäßig Morddrohungen und stehen teilweise unter Personenschutz durch das Landeskriminalamt Berlin.

Gliederung des Schriftsatzes

A. Einleitung

Diese Verfassungsbeschwerde betrifft die rechtsstaatlichen Anforderungen an den Einsatz sogenannter „Staatstrojaner“ als Standardmaßnahme im strafrechtlichen Ermittlungsverfahren. Während es aufgrund der seit 2009 geltenden Rechtsgrundlagen für solche Eingriffe im Gesetz über das Bundeskriminalamt nur zu einer kleinen zweistelligen Zahl von Maßnahmen gekommen ist, die zudem entsprechend der Aufgabenzuweisung an das BKA nur den Bereich der Abwehr terroristischer Gefahren betrafen, erlauben die angegriffenen Normen der StPO nunmehr den Einsatz von Staatstrojanern in mehreren 10.000 Fällen im Jahr, nämlich in allen Fällen, in denen bisher eine klassische Telekommunikationsüberwachung gem. § 100a Abs. 1 StPO unter Einbindung der jeweiligen Provider (vgl. § 100b StPO a.F.) vorgenommen wurde.

Diese Verfassungsbeschwerde wendet sich zunächst gegen einige Details der angegriffenen Normen, die mit den – extrapolierten – Maßstäben von BVerfGE 120, 274 („Online-Durchsuchung“) für den Einsatz von Staatstrojanern nicht im Einklang stehen. Insofern erstreben die Beschwerdeführer eine Fortentwicklung der genannten Entscheidung durch das angerufene Gericht, namentlich eine Schrankenübertragung vom präventiven auf den repressiven Bereich, sowie eine Klärung des Begriffs der „laufenden“ Kommunikation, den die vorgenannte Senatsentscheidung als zentral für die Abgrenzung zwischen Quellen-TKÜ und Online-Durchsuchung definiert hat.

Vor allem aber rügen die Beschwerdeführer eine Leerstelle: Der Bund ist bisher seiner Verpflichtung nicht nachgekommen, entsprechend dem Grundrecht auf **Gewährleistung** der Integrität und Vertraulichkeit informationstechnischer Systeme einen Rechtsrahmen für den Einsatz von Staatstrojanern zu schaffen, der geeignet ist, fatale Fehlanreize für Behörden des Bundes und der Länder zu vermeiden, die die IT-Sicherheit im Geltungsbereich des Grundgesetzes und darüber hinaus insgesamt unterminieren. Derzeit wirkt sich aus dem Bereich

des Bundes namentlich die Arbeit der im Aufbau befindlichen Behörde „ZITiS“ (Zentrale Stelle für Informationstechnik im Sicherheitsbereich) negativ auf die IT-Sicherheit aus; nach Presseberichten soll eine weitere Bundes-Hacking-Behörde in Kürze vom Bundeskabinett beschlossen werden, die „Agency for Strategic Projects in Innovation and Research“ (ASPIRE), die offenbar vor allem im militärischen Bereich aktiv werden soll.

Nach §§ 100a Abs. 1 Satz 2, 100b StPO 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 in dem informationstechnischen System des von einer Überwachung Betroffenen, die Daten ausliest und an die Strafverfolgungsbehörden übermittelt. Solche Software-Lösungen werden allgemein als „Staatstrojaner“ bezeichnet.

Weder die StPO in der angegriffenen Fassung noch die Begründung des Gesetzesentwurfs zur Einführung der angegriffenen Normen definieren indes, wie ein Staatstrojaner auf das Zielsystem aufgebracht werden darf. Denkbar sind insbesondere folgende Wege:

- Aufspielen durch Hoheitsträger, etwa bei einer Grenzkontrolle,

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

- Ausnutzen der Unaufmerksamkeit des berechtigten Nutzers, etwa indem man ihm einen E-Mail-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, rechtspolitisch aber mitunter bereits geforderte) spezifische Ermächtigungsgrundlage schlechthin rechtswidrig. Das Aufspielen etwa bei einer Grenzkontrolle ist hingegen als solches unbedenklich, ebenso das Zusenden einer 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 Abs. 1 Satz 2, 100b StPO gedeckt – führt hingegen zu gravierenden Fehlanreizen: Wenn Bundesbehörden solche Lücken ausnutzen dürfen, so haben sie ein, isoliert betrachtet, 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, eine entdeckte 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“.

Schon heute kaufen staatliche Stellen Sicherheitslücken auf dem Schwarzmarkt auf bzw. haben entsprechende Mittel im Zuge der Haushaltsberatungen bewilligt bekommen. Dies führt dazu, dass Sicherheitslücken nicht nur nicht geschlossen werden. Vielmehr wird der bestehende Schwarzmarkt, auch wenn ihn wohl nie ganz wird austrocknen können, so noch zusätzlich angeheizt. Steigende Preise für Sicherheitslücken wiederum schaffen vermeidbare Anreize für Sicherheitsforscher, ihre Erkenntnisse nicht den Herstellern zur Verfügung zu stellen, sondern sie auf dem Schwarzmarkt zu verkaufen.

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 Sicherheitslücken kauft, diese Lücken zur Infiltration informationstechnischer Systeme missbrauchen. Das gilt insbesondere auch für Cyber-Kriminelle, die es beispielsweise regelmäßig darauf anlegen, möglichst viele Systeme zum Teil eines sogenannten Botnetzes zu machen oder Zahlungsdaten für Online-Überweisungen von ihnen abzugreifen. Im Ergebnis setzen Bundesbehörden bereits heute Millionen Nutzerinnen und Nutzer von IT-Systeme weltweit, die von einer dem Bund bekannten Lücke betroffen sind, einem fortbestehenden Risiko von Cyber-Angriffen aus, um diese Sicherheitslücken im Einzelfall selbst für Maßnahmen nach §§ 100a Abs. 1 Satz 2 und 3, 100b StPO ausnutzen zu können. Und all diese Kollateralschäden werden in Kauf genommen, nur um mit Blick auf die erstrebte 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 bewusst eingegangen wird, steht in keinem ausgewogenen Verhältnis zu dem verfolgten Zweck, nämlich der (möglicherweise) erleichterten Strafverfolgung im Einzelfall.

Die Ausnutzung von staatlicherseits geheim gehaltenen Sicherheitslücken ist durchaus keine düstere Phantasie, sondern bittere Realität. Erinnert sei an den Vorfall um „WannaCry“: In den Abendstunden des 12. Mai 2017 machte sich dieses Schadprogramm, ein sog. Kryptotrojaner, auf den Weg. Innerhalb weniger Stunden waren weltweit etwa 220.000 Systeme betroffen. Der Trojaner verschlüsselte die Daten auf den betroffenen Computern und bot den Nutzern zeitgleich einen Code für die Entschlüsselung an, ansonsten werde die Löschung der Daten veranlasst. In Deutschland war vor allem die Deutsche Bahn betrof-

fen. Besonders schwer traf es das Gesundheitssystem in Großbritannien. Zahlreiche Rechner des National Health Service waren befallen. Patienten berichteten von chaotischen Zuständen. Die Daten von Krebs- und Herzpatienten standen nicht mehr zur Verfügung. Viele Kranke mussten in andere Kliniken umgeleitet werden.

Der WannaCry-Trojaner nutzte eine Lücke im Betriebssystem Microsoft Windows. Diese Lücke war schon Jahre zuvor von der National Security Agency, des auf Hacking spezialisierten US-Geheimdienstes, entdeckt, aber nicht an den Hersteller Microsoft gemeldet worden, damit er die Sicherheitslücke schließe. Brad Smith, Präsident von Microsoft, erhob in einer Erklärung den Vorwurf, die Geheimdienste würden diese Lücken absichtsvoll horten, statt sie sofort an die Hersteller zu melden.

Angesichts der eindringlichen Erfahrungen mit diesem Kryptotrojaner, dessen schnelle Verbreitung weltweit zu einem zeitweiligen Stillstand von Gesundheits- und Verkehrseinrichtungen geführt hat, bekommen die eindringlichen Worte des angerufenen Gerichts in seinem Urteil vom 27. Februar 2008 ein zusätzliches Gewicht:

> *„Je nach der eingesetzten Infiltrationstechnik kann die Infiltration auch weitere Schäden verursachen, die im Zuge der Prüfung der Angemessenheit einer staatlichen Maßnahme mit zu berücksichtigen sind. Wird dem Betroffenen etwa eine Infiltrationssoftware in Form eines vermeintlich nützlichen Programms zugespielt, lässt sich nicht ausschließen, dass er dieses Programm an Dritte weiterleitet, deren Systeme in der Folge ebenfalls geschädigt werden. Werden zur Infiltration bislang unbekannte Sicherheitslücken des Betriebssystems genutzt, kann dies einen Zielkonflikt zwischen den öffentlichen Interessen an einem erfolg-*

> *reichen Zugriff und an einer möglichst großen Sicherheit informationstechnischer Systeme auslösen. In der Folge besteht die Gefahr, dass die Ermittlungsbehörde es etwa unterlässt, gegenüber anderen Stellen Maßnahmen zur Schließung solcher Sicherheitslücken anzuregen, oder sie sogar aktiv darauf hinwirkt, dass die Lücken unerkannt bleiben. Der Zielkonflikt könnte daher das Vertrauen der Bevölkerung beeinträchtigen, dass der Staat um eine möglichst hohe Sicherheit der Informationstechnologie bemüht ist."*
>
> BVerfGE 120, 274 <325 f.>.

Eine solche Güterabwägung, die aus der isoliert auf den Ermittlungserfolg fokussierenden Sicht einer Ermittlungsbehörde vielleicht noch nachvollziehbar sein mag, 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.

> 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 (zuletzt abgerufen am 20. August 2018).

Damit sind Anreize für Bundesbehörden, die Cyber-Sicherheit in Deutschland und weltweit zu schwächen, schlechthin unvereinbar. Die Beförderung dieser immensen Sicherheitsgefahren darf nicht der Preis sein, wenn der ohnehin schon weit reichende Katalog an repressiven Eingriffsmaßnahmen noch um eine weitere ergänzt wird.

Die in §§ 100a Abs. 1 Satz 2, 100b StPO geschaffenen Regelungen sind deshalb mit dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) erst dann vereinbar, wenn sie um ein explizites Verbot der Ausnutzung bisher un-

bekannter Sicherheitslücken (sog. *0-days*) ergänzt werden, solange der Hersteller des Systems nicht über die Lücke informiert ist. Es ist sicherzustellen, dass sich alle 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.

Die Beschwerdeführer erbitten im Sinne der vorstehenden Überlegungen eine Weiterentwicklung des Grundrechts auf Integrität und Vertraulichkeit informationstechnischer Systeme durch explizite Anerkennung seiner objektiv-rechtlichen Dimension sowie eine Aufforderung an den Gesetzgeber, ein Regime zur angemessenen Behandlung von IT-Sicherheitslücken einzuführen.

B. Sachverhalt

I. Verfahrensgegenstand

Die Verfassungsbeschwerde betrifft auf einer ersten Ebene die Rechtsgrundlagen zum Einsatz sogenannten „Staatstrojaner“ – also staatlich kontrollierter Überwachungssoftware – in der Strafprozessordnung, die den Vorgaben des angerufenen Gerichts in vielen Details nicht genügen. Darüber hinaus rügen die Beschwerdeführer, dass die Bundesrepublik Deutschland durch die Einführung dieser Rechtsgrundlagen ohne zwingend gebotene Begleitregelungen zum verantwortungsvollen staatlichen Umgang mit IT-Sicherheitslücken ihre aus der objektiv-rechtlichen Dimension des Grundrechts auf Integrität und Vertraulichkeit informationstechnischer Systeme erwachsende Schutzpflicht verletzt hat.

II. Die Beschwerdeführer

1. Der Beschwerdeführer zu 1

Der Beschwerdeführer zu 1 ist Strafverteidiger in Berlin. Die Kanzlei des Beschwerdeführers zu 1. verteidigt eine Vielzahl von Mandanten – allein 2017 wurden dort ca. 450 neue Verfahren angelegt. Bei diesen Mandanten handelt es sich in mindestens der Hälfte der Fälle um Beschuldigte, denen auch Taten im Bereich der Betäubungsmittel- und Kapitaldelikte sowie der sog. organisierten Kriminalität vorgeworfen werden, mithin eine die Telekommunikationsüberwachung ermöglichende Katalogtat des § 100a Abs. 2 Nr. 1 lit. j, k, l und Nr. 7 StPO.

Mit Mandanten kommuniziert der Beschwerdeführer zu 1 teilweise auch auf elektronischem Weg, insbesondere durch E-Mails und Nachrichten über den Messenger-Dienst WhatsApp, den Mandanten mit Blick auf die Vertraulichkeit auch von sich aus zur Kommunikation mit dem Beschwerdeführer nutzen, da er seine Mobilfunknummer auf der Homepage der Kanzlei u. a. als Notfallnummer angegeben hat.

2. Die Beschwerdeführerin zu 2

Die Beschwerdeführerin zu 2 ist Rechtsanwaltsfachangestellte des Beschwerdeführers zu 1. Der überwiegende Teil (ca. 80 Prozent) der E-Mail-Korrespondenz zwischen Kanzlei und Mandanten verläuft aus organisatorischen Gründen über die E-Mail-Adresse der Beschwerdeführerin zu 2.

3. Der Beschwerdeführer zu 3

Der Beschwerdeführer zu 3 ist freier investigativer Journalist und einer der weltweit renommiertesten Doping-Experten. Für seine investigativen Erfolge wurde er mit zahlreichen Auszeichnungen geehrt. 2016 bekam er den Deutschen Fernsehpreis in der Kategorie „Beste Sportsendung“ für seine beiden Produktionen „Geheimsache Doping: Wie Russland seine Sieger macht“ sowie „Geheimsache Doping: Im Schattenreich der Leichtathletik“. Mit diesen beiden Sendungen hat der Beschwerdeführer zu 3 die Aufdeckung des russischen Staats-Dopings angestoßen und dafür gesorgt, dass der Chefermittler der Welt-Anti-Doping-Agentur Russland vorwerfen konnte, eine staatliche Dopingpolitik betrieben zu haben, an der mehr als 1.000 Sportler beteiligt waren. Außerdem wurde dem Beschwerdeführer zu 3 der Hanns–Joachim-Friedrichs-Preis für Fernsehjournalismus verliehen, daneben erhielt er den Journalistenpreis „Der lange Atem“ des Journalistenverbands Berlin-Brandenburg.

Als investigativ arbeitender Journalist lebt die Arbeit des Beschwerdeführers zu 3. von seinen Quellen. Nur durch Menschen, die bereit sind, brisante Informationen weiterzugeben, kann er aufklären. Er ist immer bestrebt, Menschen aus dem Umfeld von Sportlern für sich zu gewinnen, damit sie mit ihm ihr Wissen um Doping-Geheimnisse teilen. Die Quellen sind dabei meistens darauf bedacht, ihr Gewissen zu erleichtern und Dinge aufzuklären. Neben Interviews mit Sportlern und Ex-Sportlern, Trainern und Ex-Trainern, Funktionären und Ex-Funktionären, Dopingtestern und Ex-Dopingtestern, Dealern und Ex-Dealern usw. führt der Beschwerdeführer zu 3 auch Recherchen mit versteckter Kamera durch oder studiert Akten und elektronisch vorliegende Daten, um Informationen zu gewinnen, zu bündeln und auszuwerten. Seine Recherchen mündeten neben den beiden oben bereits genannten in einer Vielzahl von Berichten vor allem in Rundfunk- und Fernsehsendungen der ARD, die wiederum letztlich mit zum Ausschluss russischer Leichtathleten von den Olympischen Spielen in Rio de Janeiro 2016 beitrugen.

Da nie genau vorherzusehen ist, wie überführte Doping-Sünder und ihr Umfeld reagieren, hält der Beschwerdeführer zu 3 seine Adresse möglichst geheim. Auch das angerufene Gericht wird wegen der bestehenden Gefährdung des Beschwerdeführers zu 3 gebeten, seine Adresse – wie auch diejenigen der anderen Beschwerdeführer – in geeigneter Weise zu schützen.

Journalistische Recherchen im Bereich Doping sind stets konkret: Es geht um Namen von bestimmten Personen, zum Beispiel einen prominenten Sprinter oder einen Langstreckenläufer. Dann erfährt der Beschwerdeführer zu 3 etwa von seiner Quelle X, dass Sportler Y gedopt hat. Vor einer Veröffentlichung muss er die Sache indes „hart bekommen", also möglichst über Dealer oder vertuschte positive Dopingtests Klarheit schaffen, im besten Fall Beweise für Annahmen „herrecherchieren".

Informationen erreichen den Beschwerdeführer zu 3 auf den unterschiedlichsten Wegen: Er bekommt Anrufe, Briefe, SMS-Nachrichten und Faxe – aber vor allem E-Mails mit Dateianhängen, die häufig aus „Leaks" stammen. Zudem nutzt er für Kommunikation mit einem besonderen Geheimhaltungsbedürfnis verschiedene Dienste, die eine Verschlüsselung anbieten, darunter Signal, WhatsApp, Protonmail, Telegram, Secureline, Skype und Threema. Er schützt seine IT-Systeme mit Anti-Viren-Programmen.

Dieser Schutz ist auch erforderlich. Der Beschwerdeführer zu 3. erhält zwei bis drei Mal pro Woche Drohungen, mutmaßlich von russischer Seite. Er steht deshalb auch unter Personenschutz.

4. Der Beschwerdeführer zu 4

Der Beschwerdeführer zu 4 ist Journalist, Dokumentarfilmer und Buchautor mit türkischer Staatsbürgerschaft und lebt und arbeitet in Berlin. Er besitzt eine Aufenthaltserlaubnis.

Bis Juli 2016 lebte der Beschwerdeführer zu 4 in der Türkei, wo er für verschiedene türkische Zeitungen schrieb und Dokumentation für diverse TV-Sender produzierte. Er hat über 20 Bücher geschrieben und erhielt für seine Arbeit zahlreiche Preise.

Bis August 2016 war der Beschwerdeführer zu 4 Chefredakteur der *Cumhuriyet*, einer linksliberalen türkischen Zeitung, die 2015 für ihr Engagement gegen den zunehmend autoritären Kurs der türkischen Regierung den *Freedom-of-the-Press*-Preis von der Nichtregierungsorganisation „Reporter ohne Grenzen" erhielt. Im selben Jahr initiierte die türkische Staatsanwaltschaft ein Strafverfahren gegen ihn und den Chef des Ankara-Büros der *Cumhuriyet*, Erdem Gül, wegen angeblicher Unterstützung einer terroristischen Vereinigung, Spionage, Veröffentlichung vertraulicher Dokumente und Unterstützung eines Umsturzversuchs. Auslöser des Strafverfahrens war die Veröffentlichung von Videos und Fotos, die Waffentransporte nach Syrien in Lastwagen des türkischen Nachrichtendienstes zeigen. Kurz nach Veröffentlichung dieser Videos und Fotos erklärte der türkische Präsident Recep Tayyip Erdoğan, dass *Cumhuriyet* sich der Spionage schuldig gemacht habe, und dass die verantwortlichen Journalisten einen hohen Preis bezahlen würden.

> ZEIT Online vom 3. Juni 2015, online abrufbar unter: https://www.zeit.de/politik/ausland/2015-06/erdogan-can-duendar-anzeige-cumhuriyet (zuletzt abgerufen am 4. August 2018).

In der darauf folgenden Anklage forderte die Staatsanwaltschaft für den Beschwerdeführer zu 4 zweifach lebenslange Freiheitsstrafe. Ende November 2015 wurde er in Untersuchungshaft genommen, aus der er erst Ende Februar 2016 nach einer Entscheidung des damals noch unabhängigen Verfassungsgerichts mangels hinreichenden Tatverdachts wieder entlassen wurde – eine Entscheidung, die wiederum die öffentliche Missbilligung des Staatsoberhaupts Erdoğan auf sich zog.

SPIEGEL Online vom 25. März 2016, online abrufbar unter: http://www.spiegel.de/politik/ausland/can-duendar-und-erdem-guel-prozess-gegen-tuerkische-journalisten-beginnt-a-1084149.html (zuletzt abgerufen am 4. August 2018).

Nach hoher medialer Aufmerksamkeit auch aus dem Ausland wurde das Hauptverfahren unter Ausschluss der Öffentlichkeit fortgeführt. Vor der Urteilsverkündung am 6. Mai 2016 schoss außerhalb des Gerichtsgebäudes ein Attentäter auf den Beschwerdeführer zu 4, verfehlte ihn aber. Der Beschwerdeführer zu 4 wurde der Veröffentlichung von Staatsgeheimnissen für schuldig befunden, die Anklage bezüglich der Unterstützung einer terroristischen Vereinigung wurde zu einem gesonderten Verfahren abgetrennt. Der Beschwerdeführer zu 4 wurde zu fünf Jahren und zehn Monaten Freiheitsstrafe verurteilt. Das Urteil ist noch nicht rechtskräftig. Als angeblicher Hinweisgeber wurde der seinerzeitige Abgeordnete der Mitte-links-Partei CHP, Enis Berberoğlu, zu 25 Jahren Haft verurteilt.

ZEIT Online vom 14. Juni 2017, online abrufbar unter: https://www.zeit.de/politik/ausland/2017-06/tuerkei-chp-abgeordneter-haftstrafe-geheimnisverrat (zuletzt abgerufen am 4. August 2018).

Bereits zuvor war der Beschwerdeführer zu 4 wegen Beleidigung des Staatspräsidenten zu einer Geldstrafe verurteilt worden; auch diese Verurteilung ist noch nicht rechtskräftig.

Nachdem der Beschwerdeführer zu 4 im Juli 2016 das Land verließ, wurde am 31. Oktober 2016 ein Haftbefehl gegen ihn erlassen. Seither versuchen verschiedene türkische Stellen, ihn mittels einer sog. „Red Notice“ bei Interpol international inhaftieren zu lassen.

RP Online vom 2. April 2018, online abrufbar unter: https://rp-online.de/politik/ausland/tuerkei-will-interpol-auf-can-duendar-ansetzen_aid-17093615 (zuletzt abgerufen am 4. August 2018).

Nach seiner Flucht aus der Türkei trat der Beschwerdeführer zu 4 als Chefredakteur der *Cumhuriyet* zurück. Zurzeit ist er Chefredakteur der deutsch-türkischsprachigen Journalismusplattform *Özgürüz*. In dieser Eigenschaft und auch privat nutzt er folgende IT-Systeme:

- einen Computer der Marke Apple zum Verfassen von Büchern und Artikeln, für E-Mails und Skype.
- ein iPhone für die Dienste Scope (eine virtuelle TV-Station, mit der er etwa 4 Millionen Personen erreicht), Twitter (ein Mikrobloggingdienst, über den er etwa 4,7 Millionen Personen erreicht), Signal, WhatsApp (beides Messengerdienste), SMS und E-Mail (die vier Letztgenannten nutzt er sowohl für private als auch für berufliche Zwecke).

Der Beschwerdeführer zu 4 ist regelmäßig Opfer von Angriffen auf seine IT-Systeme. Er erhält E-Mails und Nachrichten mit Viren oder Links zu Websites, auf denen sich Viren befinden können, und erhält Anrufe von unbekannten Telefonnummern. Dazukommen unzählige Drohungen gegen sein Leben und das seiner Familie, die häufig gespickt sind mit Angaben zu seinem Aufenthaltsort, den er eigentlich geheim hält. Seit er in Deutschland lebt, haben die virtuellen (und auch physischen) Angriffe zugenommen. Aufgrund der besonders hohen Gefährdungslage steht der Beschwerdeführer zu 4 in Deutschland unter Personenschutz.

Bislang war seines Wissens noch kein Hackerangriff gegen ihn erfolgreich, was allerdings auf seine Sicherheitsvorkehrungen zurückzuführen ist: Von „Reporter ohne Grenzen“ (RoG) hat er sich in Fragen der IT-Sicherheit fortbilden lassen und nutzt nun Instrumente wie die Ende-zu-Ende-Verschlüsselung und die

Zwei-Faktor-Authentifizierung; außerdem berät ihn ein RoG-Sicherheitsteam, wenn er verdächtige E-Mails, Nachrichten oder Anrufe erhält.

Es ist nicht anzunehmen, dass die Angriffe gegen seine IT-Systeme nachlassen werden, solange er als Journalist aktiv ist. Alles spricht dafür, dass ihn die türkische Regierung sowie ihr nahestehende Gruppierungen wegen seiner politisch geprägten Berichterstattung attackieren. Nur die türkische Regierung hat ein Interesse daran, den Beschwerdeführer zu 4 anhaltend zu attackieren, und zwar in dreifacher Hinsicht: Erstens will sie die Quellen seiner früheren und aktuellen Berichterstattung identifizieren. Zweitens sucht sie nach Material, um ihn zu diskreditieren. Letzteres hat sie etwa bereits dadurch versucht, dass Bewegungen auf seinem türkischen Bankkonto öffentlich wurden, die belegen sollten, dass er für einen bestimmten Bericht finanzielle Vorteile erhalten habe. Und drittens versucht die türkische Regierung bzw. ihr nahestehende Gruppierungen den Beschwerdeführer zu 4 einschüchtern. Nur die türkische Regierung wäre auch bereit, die für die Hackerangriffe erforderlichen Ressourcen zu investieren. Der Beschwerdeführer zu 4 wurde bereits Opfer von Hackerangriffen, deren Kosten auf Seiten der Angreifer sich angesichts der Schwarzmarktpreise für Trojaner auf mittlere sechsstellige Dollarbeträge belaufen dürften.

Anschaulich macht einen solchen aufwändigen Hacking-Versuch ein Fall aus dem Jahr 2017. Der Beschwerdeführer zu 4 erhielt sog. Direkt-Nachrichten, die scheinbar von den Twitter-Accounts zweier Freunde an ihn gesendet wurden und einen Link zu einer Internetseite enthielten. Eine der Nachrichten übersah er zunächst, eine andere hielt er für verdächtig, weil der angebliche Freund eine falsche Anrede verwendete. Das RoG-Sicherheitsteam untersuchte den Fall. Der Link führte auf eine Internetseite, die bereits inaktiv war. Allerdings hätte der Beschwerdeführer zu 4 mit einem Klick auf den Link zum Zeitpunkt des Angriffs nach Einschätzung des RoG-Sicherheitsteams wahrscheinlich unwillkürlich einen Trojaner eines **deutschen** Herstellers von Überwachungssoftware, der Firma FinFisher GmbH, heruntergeladen. Der Trojaner hätte unter

Ausnutzung einer Sicherheitslücke den Rechner des Beschwerdeführers zu 4. manipuliert. Dafür, dass es sich um einen Angriff mit dem FinFisher-Trojaner handelte, sprechen Mittel und Zeitpunkt des Angriffs sowie der verwendete Link, die allesamt den Angriffen mit diesem Trojaner auf andere türkische Oppositionelle entsprachen, die die US-amerikanische Nichtregierungsorganisation Access Now aufgedeckt hat.

> Access Now, Bericht vom 14. Mai 2018, online abrufbar unter: https://www.accessnow.org/new-report-finfisher-changes-tactics-to-hook-critics/ (zuletzt abgerufen am 4. August 2018); vgl. dazu auch Süddeutsche Zeitung Online vom 14. Mai 2018, online abrufbar unter: https://www.sueddeutsche.de/digital/spionage-in-der-tuerkei-falle-mit-deutscher-spitzeltechnik-1.3979756 (zuletzt abgerufen am 4. August 2018).

5. Der Beschwerdeführer zu 5

Der Beschwerdeführer zu 5 ist seit 2009 Mitglied des Deutschen Bundestags. Er beschäftigt sich im Rahmen seiner Mandatstätigkeit vor allem mit Fragen der Innen-, Rechts- und Digitalpolitik. Als stellvertretender Fraktionsvorsitzender ist er Mitglied des Vorstands der Fraktion Bündnis90/Die Grünen. In der aktuellen Wahlperiode vertritt er die Fraktion unter anderem als ordentliches Mitglied im Innenausschuss und als stellvertretendes Mitglied im 1. Parlamentarischen Untersuchungsausschuss der 19. Wahlperiode zum Anschlag auf dem Berliner Breitscheidplatz. Zudem ist der Beschwerdeführer zu 5 stellvertretender Vorsitzender des Parlamentarischen Kontrollgremiums. Darüber hinaus ist er stellvertretendes Mitglied der IuK-Kommission, einer Unterkommission des Ältestenrats des Deutschen Bundestages, die sich mit Fragen rund um die IT-Ausstattung von Abgeordneten und Bundestag beschäftigt. Neben diesen parlamentarischen Aufgaben nimmt der Beschwerdeführer zu 5 verschiedene Aufgaben in unterschiedlichen Parteigremien auf Bundes- und Landesebene wahr.

In seiner Eigenschaft als Abgeordneter hat der Beschwerdeführer zu 5 immer wieder auch mit als geheimhaltungsbedürftig eingestuften Informationen zu tun, die qua Gesetz besonders geschützt werden müssen. Der Beschwerdeführer zu 5 nutzt verschiedene Programme zur Verschlüsselung seiner Kommunikation, um sich, seine private wie berufliche Kommunikation als Abgeordneter, die Kommunikation von und mit seinen Mitarbeiterinnen und Mitarbeitern, aber auch die von und mit Hinweisgeberinnen und Hinweisgebern, unter ihnen auch immer wieder (andere) Berufsgeheimnisträgerinnen und -träger, bestmöglich zu schützen. Dazu gehören der Verschlüsselungsstandard GnuPG für seine und die Mails seiner Mitarbeiter sowie verschiedene Ende-zu-Ende-verschlüsselte Messenger-Dienste. In seiner Eigenschaft als Obmann des 1. Untersuchungsausschusses der 18. Wahlperiode (NSA-Untersuchungsausschuss) wurde dem Beschwerdeführer zu 5 zwischenzeitlich ein „Krypto-Handy“ (ein abhörsicheres Mobiltelefon) zur Verfügung gestellt.

Die Arbeit des Beschwerdeführers zu 5 insgesamt, insbesondere seine eigenen politischen Ansichten und Bewertungen, aber auch die seiner Fraktion und seiner Partei sind aus Sicht von Geheimdiensten anderer Staaten und Hackergruppen lohnende Aufklärungsziele. Hiervon zeugen nicht nur dokumentierte Aufklärungsbemühungen verschiedener Nachrichtendienste von (befreundeten) Staaten im Regierungsviertel selbst, sondern auch wiederholte Angriffe auf digitale Infrastrukturen des Deutschen Bundestags sowie beobachtete Versuche der Infiltration der Geräte und Kommunikation von Abgeordneten und ihre Mitarbeiter, vor allem über soziale Netzwerke, aber beispielsweise auch durch die passgenaue und persönlich zugeschnittene Versendung von sog. „Phishing Mails“ von (vermeintlichen) Adressen des Beschwerdeführers zu 5 an Kolleginnen und Kollegen sowie die Zusendung entsprechender Mails, die wiederum vermeintlich von Kolleginnen und Kollegen stammten, an ihn. Die präzise, zielgenaue Adressierung spricht insbesondere dafür, dass der Beschwerdeführer zu 5 nicht nur wie jedermann mit allfälligen Versuchen des „Phishing“ konfrontiert wird, sondern gerade im Hinblick auf seine berufliche und politische Situation gezielten, maßgeschneiderten Attacken ausgesetzt ist.

Für seine berufliche Kommunikation greift der Beschwerdeführer zu 5 auf verschiedene, vom Bundestag gestellte Arbeitsplatzcomputer (sowohl Desktop-PCs wie auch Laptops), auf eigene Computer (sowohl Desktop-PCs wie auch Laptops) und Tablets sowie Smartphones zurück. Er nutzt diese Geräte täglich.

C. Zulässigkeit

Die Verfassungsbeschwerde ist zulässig.

I. Frist

Die Jahresfrist des § 93 Abs. 3 BVerfGG ist gewahrt. Die Verfassungsbeschwerde richtet sich gegen Regelungen, die das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017 (BGBl. I, S. 3202) eingefügt hat und die die Strafprozessordnung vorher nicht kannte. Die angegriffenen Eingriffsermächtigungen sind gemäß Art. 18 Abs. 1 dieses Gesetzes am Tag nach der Verkündung und damit am 24. August 2017 in Kraft getreten.

II. Beschwerdebefugnis der Beschwerdeführerin und Beschwerdeführer zu 1 bis 3 unter dem Aspekt der Betroffenheit von Maßnahmen nach §§ 100a Abs. 1 Satz 2, 100b StPO

Die Beschwerdeführerin und Beschwerdeführer zu 1 bis 3 sind im Sinne von § 90 Abs. 1 BVerfGG beschwerdebefugt, weil eine Verletzung ihrer Grundrechte durch die angegriffenen Regelungen zumindest möglich ist und die Regelungen sie auch selbst, gegenwärtig und unmittelbar betreffen.

1. Möglichkeit der Grundrechtsverletzung

Es ist zumindest möglich, dass Überwachungsmaßnahmen auf der Grundlage der angegriffenen Regelungen Grundrechte der Beschwerdeführerin und Beschwerdeführer zu 1 bis 3 verletzen.

Sowohl § 100a Abs. 1 Satz 2 und 3 StPO als auch § 100b StPO ermächtigen zu Eingriffen in die informationstechnischen Systeme der Betroffenen, einerseits

(im Falle des § 100a StPO) zur Durchführung einer Telekommunikationsüberwachung, andererseits (bei § 100b StPO) zur Durchsuchung der Systeme selbst. Dies beschränkt das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) derjenigen Zielpersonen, deren IT-Systeme infiltriert werden.

Es ist zumindest möglich, dass die neuen Befugnisse auch die Grundrechte der Beschwerdeführerin und Beschwerdeführer zu 1 bis 3 verletzen, weil diese aus beruflichen Gründen mithilfe informationstechnischer Systeme mit potenziellen Zielpersonen von Überwachungsmaßnahmen nach §§ 100a, 100b StPO kommunizieren.

Dies ergibt sich zum einen aus der – nach Auskunft der vom angerufenen Gericht in den Verfahren 1 BvR 370/07 und 1 BvR 595/07 angehörten Sachverständigen technisch nie ganz auszuschließenden – Gefahr einer Infektion von „Kontaktpersonen“ bei Gelegenheit des Versuch, den eigentlichen Zielpersonen aus der Mandantschaft bzw. dem Informantenkreis der drei Beschwerdeführer eine staatliche Überwachungssoftware unterzuschieben: Wegen der besonderen Schwierigkeit der zielgenauen Infektion informationstechnischer Systeme liegt eine Infektion eigener Systeme der drei Beschwerdeführer als „Kollateralschäden“ der eigentlich vorgesehenen Infektion nicht fern. Beispielsweise ist ein gängiger Infektionsweg das Versenden von Emails mit infektiösen Anhängen bzw. von Nachrichten mit Links auf infektiöse Websites. Sollte eine der Kontaktpersonen der genannten Bf. diese Nachrichten an die Bf. weiterleiten, etwa um deren Meinung dazu einzuholen, so werden auch die Systeme der Bf. infiziert und jedenfalls solange Informationen daraus erhoben, bis der Irrtum auffällt. Selbst eine nachträgliche Löschung der irrtümlich erhobenen Informationen vermag den Eingriff in das „IT-Grundrecht“, die informationelle Selbstbestimmung sowie das Telekommunikationsgeheimnis dann nicht mehr ungeschehen zu machen.

Zum anderen tauschen die Beschwerdeführerin und der Beschwerdeführer zu 1 und zu 2 Nachrichten mit ihrer Mandantschaft aus, die wiederum gem. §§ 100a Abs. 1 Satz 2, 100b StPO überwacht werden können, womit eine Verletzung sowohl ihres Rechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) als auch des Rechts auf unüberwachte Telekommunikation (Telekommunikationsgeheimnis; Art. 10 Abs. 1 GG) zumindest möglich ist. Weil dadurch die Vertraulichkeit ihrer beruflichen Kommunikation nicht mehr im selben Maße gewährleistet ist, ist auch eine Verletzung der Berufsfreiheit (Art. 12 Abs. 1 GG) zumindest möglich; für den Beschwerdeführer zu 3 gilt das zumindest im Anwendungsbereich des § 100a Abs. 1 Satz 2 und 3 StPO.

Schließlich kann die Zurückstellung der Benachrichtigung über die Überwachungsmaßnahmen (§ 101 Abs. 5, 6 StPO) die Beschwerdeführerin und Beschwerdeführer zu 1 bis 3 auch in ihrem Recht auf effektiven Rechtsschutz (Art. 19 Abs. 4 GG) verletzen. Denn die zeitweilige oder gar dauerhafte Zurückstellung verzögert bzw. verhindert Rechtsschutzmöglichkeiten und reduziert mit zunehmendem zeitlichen Abstand zur angeordneten Maßnahme auch die Effektivität des Rechtsschutzes.

Die Beschwerdeführerin und Beschwerdeführer zu 1 bis 3 machen sich für die Darlegung der Möglichkeit einer Grundrechtsverletzung zudem die untenstehenden Ausführungen zur Begründetheit zu eigen.

2. Betroffenheit

a) Unmittelbare Betroffenheit

Die angegriffenen Regelungen betreffen die Beschwerdeführerin und Beschwerdeführer zu 1 bis 3 unmittelbar.

Zwar ist ein Beschwerdeführer nur dann von einer gesetzlichen Regelung unmittelbar betroffen, wenn diese in seinen Rechtskreis eingreift, ohne dass es eines weiteren Vollzugsaktes bedürfte. Erfordert das Gesetz zu seiner Durchführung rechtsnotwendig oder auch nur nach der tatsächlichen staatlichen Praxis einen besonderen, vom Willen der vollziehenden Stelle beeinflussten Vollzugsakt, muss der Beschwerdeführer grundsätzlich zunächst diesen Akt angreifen und den gegen ihn eröffneten Rechtsweg erschöpfen, bevor er die Verfassungsbeschwerde erhebt.

BVerfGE 1, 97 <101 ff.>; 109, 279 <306>; 133, 277 <311>.

Unmittelbar betroffen ist der Beschwerdeführer jedoch, wenn er den Rechtsweg nicht beschreiten kann, weil er keine Kenntnis von der betreffenden Vollziehungsmaßnahme erhält. In solchen Fällen steht ihm die Verfassungsbeschwerde unmittelbar gegen das Gesetz ebenso zu wie in den Fällen, in denen die grundrechtliche Beschwer ohne vermittelnden Vollzugsakt durch das Gesetz eintritt.

BVerfGE 30, 1 <16 f.>; 113, 348 <362 f.>; 120, 378 <394>; 133, 277 <311>.

So liegen die Dinge hier. Die Beschwerdeführerin und Beschwerdeführer zu 1 bis 3 erhalten keine Kenntnis von laufenden Überwachungsmaßnahmen nach § 100a Abs. 1 Satz 2 und § 100b Abs. 1 StPO.

Dass sie nach Abschluss der Ermittlungen gemäß § 101 Abs. 4 Satz 1 Nr. 3 und 4 StPO möglicherweise über die Maßnahme informiert werden, ändert an der unmittelbaren Betroffenheit nichts. Die Möglichkeit, eine Verfassungsbeschwerde unmittelbar gegen ein Gesetz zu erheben, das zu heimlichen Maßnahmen berechtigt, entfällt unter dem Gesichtspunkt der Unmittelbarkeit nur, wenn

die spätere Kenntniserlangung des Betroffenen durch eine aktive Informationspflicht des Staates rechtlich gesichert ist.

> BVerfGE 133, 277 <312> unter Verweis auf BVerfG, Beschl. v. 25. April 2001 – 1 BvR 1104/92 (= NVwZ 2001, 1261).

Das ist durch § 101 StPO nicht gewährleistet. Nach § 101 Abs. 5 Satz 1 erfolgt die Benachrichtigung über Maßnahmen nach §§ 100a und 100b StPO nämlich erst, wenn dies ohne Gefährdung des Untersuchungszwecks, des Lebens, der körperlichen Unversehrtheit und der persönlichen Freiheit einer Person und von bedeutenden Vermögenswerten möglich ist. Die Norm bietet damit einen weiten Beurteilungsspielraum, wonach eine Mitteilung an die Betroffenen auf unabsehbare Zeit ausgeschlossen bleiben kann. Dementsprechend hat das Bundesverfassungsgericht bereits zu einer früheren Fassung des § 101 StPO erklärt, dass infolge der seinerzeitigen Ausnahmetatbestände effektiver Rechtsschutz nicht erlangt werden könne und deshalb die Regelungen zum damals im Streit stehenden „großen Lauschangriff“ die dortigen Beschwerdeführer unmittelbar beträfen.

> BVerfGE 109, 279 <307>.

Diese Einschätzung gilt entsprechend für die heute geltenden Ausnahmetatbestände des § 101 Abs. 5 Satz 1 StPO – die sich mit den Tatbeständen des § 101 StPO a.F. teilweise decken –, insbesondere für den unbestimmten Rechtsbegriff der „bedeutenden Vermögenswerte[ ]“.

Zudem hat das Bundesverfassungsgericht in seiner Entscheidung zum BKA-Gesetz die Verfassungsbeschwerde gegen eine mit § 101 StPO vergleichbare Vorschrift unter anderem mit dem Argument zugelassen, dass Benachrichtigungspflichten möglicherweise erst spät greifen.

> BVerfGE 141, 220 <261> zu § 20w BKA-Gesetz a.F., wie er durch das Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch

das Bundeskriminalamt vom 25. Dezember 2008 (BGBl. I, S. 3083) eingeführt wurde.

Auch das ist hier im Hinblick auf die Möglichkeit der potentiell sogar dauerhaften Zurückstellung nach § 101 Abs. 5, 6 Satz 3 StPO der Fall.

b) Eigene und gegenwärtige Betroffenheit

Die Beschwerdeführerin und Beschwerdeführer zu 1 bis 3 sind zudem durch die angegriffenen Regelungen selbst und gegenwärtig betroffen. Erforderlich, aber auch ausreichend ist hierfür bei gesetzlichen Ermächtigungen zu verdeckten Überwachungsmaßnahmen die Darlegung, zukünftig mit einiger Wahrscheinlichkeit von einer solchen Maßnahme betroffen zu sein.

BVerfGE 100, 313 <354>; 109, 279 <307 f.>; 113, 348 <363>; 133, 277 <312 f.>; 141, 220 <262>; 143, 1 <21>.

Das gilt für beide sowohl für Maßnahmen nach § 100a Abs. 1 Satz 2 StPO als auch für Maßnahmen nach § 100b Abs. 1 StPO.

(1) Beschwerdeführer zu 1

(i) Betroffenheit durch Maßnahmen nach § 100a Abs. 1 Satz 2 StPO

Der Beschwerdeführer zu 1 steht als Strafverteidiger berufsbedingt regelmäßig in Kontakt zu Personen, die unter einem Tatverdacht im Sinne von § 100a Abs. 1, Abs. 2 StPO stehen. Viele Mandanten des Beschwerdeführers zu 1 sind demnach Personen, bei denen gem. § 100a Abs. 1 StPO bestimmte Tatsachen den Verdacht begründen, dass sie „als Täter oder Teilnehmer eine in Absatz 2 bezeichnete schwere Straftat begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht, oder durch eine Straftat vorbereitet“ haben (Nr. 1) und

bei denen die angebliche Tat oftmals „auch im Einzelfall schwer wiegt“ (Nr. 2) und „die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre“ (Nr. 3).

Der Beschwerdeführer zu 1 nutzt zur Kommunikation mit seinen Mandanten häufig den Messenger-Dienst WhatsApp. Unter anderem zur Überwachung der Kommunikation über Messenger-Dienste wie WhatsApp dient die Quellen-TKÜ nach § 100a Abs. 1 Satz 2 StPO.

Gesetzesbegründung, BT-Drs. 18/12785, S. 48 ff.

Der Beschwerdeführer zu 1 ist mit einiger Wahrscheinlichkeit von der Überwachung seiner WhatsApp-Kommunikation betroffen. Selbst wenn für jeden einzelnen Telekommunikationsvorgang des Beschwerdeführers zu 1 mit einem Mandanten jeweils nur eine geringe Wahrscheinlichkeit besteht, dass ihn eine Überwachungs- oder Durchsuchungsmaßnahme erfasst, ist wegen der Vielzahl der in der Kanzlei des Beschwerdeführers zu 1 anfallenden Telekommunikationsvorgänge und des weit gefassten Straftatenkataloges des § 100a Abs. 2 StPO anzunehmen, dass Maßnahmen nach § 100a Abs. 1 Satz 2 StPO jedenfalls einzelne Mandanten des Beschwerdeführers zu 1 betreffen werden.

Dabei ist zu erwarten, dass nicht nur die klassische Telekommunikation der Mandanten des Beschwerdeführers zu 1 gem. § 100a Abs. 1 Satz 1 StPO überwacht und aufgezeichnet wird, sondern die Aufzeichnung und Überwachung sich gem. § 100a Abs. 1 Satz 2 StPO durch Eingriff in informationstechnische Systeme der Mandanten mit technischen Mitteln auch auf ihre WhatsApp-Kommunikation erstrecken. Dies ist insbesondere dann denkbar, wenn eine „klassische“ Telekommunikationsüberwachung während des Übertragungsvorgangs wegen eingesetzter Verschlüsselungstechnik nicht möglich ist. WhatsApp-

Nachrichten sind inzwischen standardmäßig Ende-zu-Ende-verschlüsselt, sodass sie nur noch durch einen Zugriff direkt auf das sendende oder empfangende System mitgelesen werden können (Eingriff in Art. 10 Abs. 1 GG). Neben einer Überwachung und Aufzeichnung laufender Kommunikation ermöglicht § 100a Abs. 1 Satz 3 StPO zusätzlich eine Überwachung und Aufzeichnung aller seit dem Anordnungszeitpunkt auf dem betroffenen informationstechnischen Gerät gespeicherten Kommunikationsinhalte (Eingriff in das sog. IT-Grundrecht).

Die Gefahr einer Überwachung der Kommunikation mit seinen Mandanten schränkt die Kommunikationsmöglichkeiten des Beschwerdeführers zu 1 ein, weil sie zu einer nachvollziehbaren Hemmung führen kann, Fernkommunikationsmittel in Anspruch zu nehmen, die bis zu einem Abstandnehmen reichen kann. Damit wird zugleich die Effektivität seiner Arbeit als Rechtsanwalt beeinträchtigt (Eingriff in Art. 12 Abs. 1 GG).

Somit ist der Beschwerdeführer zu 1 durch die Wahrscheinlichkeit von Maßnahmen nach § 100a Abs. 1 Satz 2 StPO, die sich gegen seine Mandanten richten, in seinen Grundrechten aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG (Recht auf informationelle Selbstbestimmung sowie „IT-Grundrecht“), Art. 10 Abs. 1 GG (Telekommunikationsfreiheit) sowie Art. 12 Abs. 1 GG (Berufsfreiheit) betroffen. Die Wahrscheinlichkeit seiner Betroffenheit ist auch gegenüber der Durchschnittsbevölkerung erheblich erhöht.

(ii) Betroffenheit durch Maßnahmen nach § 100b Abs. 1 StPO

Die Ausführungen zu § 100a Abs. 1 Satz 2 StPO gelten für Maßnahmen nach § 100b Abs. 1 StPO entsprechend, da diese Maßnahme alles umfasst, was bei jener zulässig ist, und darüber hinaus noch den Zugriff auf alle auf dem System gespeicherten Daten. Insbesondere hat der Beschwerdeführer zu 1 eine Vielzahl von Mandanten, die Straftaten aus dem Katalog des § 100b Abs. 2 StPO verdächtigt werden, insbesondere nach § 100b Abs. 2 Nr. 1 lit. g, h, i, k, Nr. 3 und

Nr. 4 StPO. § 100b Abs. 1 StPO ermächtigt zu einem Zugriff auf alle gespeicherten Daten ohne zeitliche Begrenzung (Online-Durchsuchung). Danach können neben den bereits nach § 100a Abs. 1 Satz 3 StPO zu erhebenden Daten auch alle weiteren mit der Kanzlei des Beschwerdeführers zu 1 ausgetauschten Kommunikationsinhalte potentiell erfasst werden, was gerade bei längerfristigen Mandatsverhältnissen von Bedeutung ist. Hierunter fallen neben E-Mails und ihren Anhängen auch sonstige Daten, die die Mandanten des Beschwerdeführers zu 1 zu seiner Person auf ihren Systemen gespeichert haben. Eine Kommunikation per E-Mail ist heutzutage unerlässlich, ihre Kompromittierung würde das Vertrauensverhältnis zwischen Strafverteidiger und Mandant erschüttern und bedeutete für den Beschwerdeführer zu 1 eine erhebliche Erschwernis im Arbeitsalltag.

Entsprechend ist der Beschwerdeführer zu 1 durch eine Online-Durchsuchung bei einem Mandanten in eigenen Grundrechten aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG (Recht auf informationelle Selbstbestimmung, IT-Grundrecht), Art. 10 Abs. 1 sowie Art. 12 Abs. 1 GG betroffen.

(iii) Kein anderes Ergebnis auf Grund von § 100d StPO

Das in § 100d Abs. 1 StPO vorgesehene Beweiserhebungsverbot sowie das in § 100d Abs. 2 Satz 1 StPO vorgesehene Beweisverwertungsverbot ändern an dieser Betroffenheit des Beschwerdeführers zu 1 ebenso wenig etwas wie die in § 100d Abs. 2 Satz 2 StPO ferner normierte Löschpflicht:

Zwar sind Verteidigergespräche grundsätzlich dem Kernbereich zuzuordnen,

> vgl. etwa *Schmitt* in: Meyer-Goßner/Schmitt, StPO, 61. Aufl. 2018, § 100a Rn. 24a oder auch die Gesetzesbegründung, BT-Drucksache. 18/12785, S. 47,

womit Erkenntnisse hieraus gem. § 100d Abs. 2 Satz 1 StPO nicht verwertet werden dürfen und Aufzeichnungen hierüber gem. § 100d Abs. 2 Satz 1 StPO unverzüglich zu löschen sind. Auf diese Weise erlangte Erkenntnisse können

für die Ermittlungsbehörden gleichwohl mittelbar von großer Bedeutung sein. Insbesondere gilt dies etwa, wenn sich hierdurch der Tatverdacht gegen den Mandanten erhärtet oder ein neuer Tatverdacht gegen weitere Mandanten des Beschwerdeführers zu 1 begründet wird. Die Überwachung und Aufzeichnung der Telekommunikation seiner Mandanten beeinträchtigt den Beschwerdeführer zu 1 damit umfassend in seinen auf Vertrauen ausgerichteten beruflichen Beziehungen zu seinen Mandanten. Dies erschwert die Arbeit des Beschwerdeführers zu 1 erheblich und gefährdet letztlich eine erfolgreiche Verteidigung seiner Mandanten.

Im Übrigen bringt die Löschpflicht in § 100d Abs. 2 Satz 2 StPO zum Ausdruck, dass es gerade zu einer Erhebung und Speicherung von Daten kommen kann, die den Austausch mit einem Verteidiger betreffen. Der mit Erhebung und Speicherung verbundene Eingriff ist jedoch endgültig. Damit geht auch das Gesetz davon aus, dass Strafverteidiger wie der Beschwerdeführer zu 1 von Maßnahmen gegen ihre Mandanten betroffen sein können.

Eine noch konkretere Darlegung der voraussichtlichen Betroffenheit ist den Beschwerdeführern aufgrund der verdeckten Durchführung der Ermittlungsmaßnahmen nicht möglich; dies hat dementsprechend auch das angerufene Gericht zur Frage der Betroffenheit durch die insoweit vergleichbaren Regelungen in § 20k und § 20l Abs. 2 des Bundeskriminalamtsgesetzes in der Fassung des Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt vom 25. Dezember 2008 (BGBl. I, S. 3083) nicht für erforderlich gehalten.

Vgl. BVerfGE 141, 220 <262>.

(2) Beschwerdeführerin zu 2

Auch die Beschwerdeführerin zu 2 steht berufsbedingt regelmäßig in Kontakt zu Mandanten des Beschwerdeführers zu 1, die von Maßnahmen nach § 100a Abs. 1 Satz 2 und § 100b Abs. 1 StPO betroffen sein können. Damit gelten die Ausführungen zum Beschwerdeführer zu 1 entsprechend auch für die Beschwerdeführerin zu 2.

Darüber hinaus besteht die Gefahr, dass Informationen, die die Beschwerdeführerin zu 2 mit Mandanten des Beschwerdeführers zu 1 austauscht, infolge der Überwachungsmaßnahmen nach §§ 100a Abs. 1 Satz 2, 100b Abs. 1 StPO sogar direkt in das Strafverfahren einfließen. Der Kernbereichsschutz des § 100d Abs. 2 StPO gilt nämlich ausschließlich im speziellen Vertrauensverhältnis zwischen Verteidiger und Mandant. Zwar steht der Beschwerdeführerin zu 2 als Rechtsanwaltsfachangestellte des Beschwerdeführers zu 1 gem. §§ 53 Abs. 1 Satz 1 Nr. 2, 53a Abs. 1 StPO grundsätzlich auch ein Zeugnisverweigerungsrecht zu. Hieraus ergibt sich jedoch kein eigenständiges, dem Kernbereich zuzuordnendes und damit absolut schützenswertes Vertrauensverhältnis zum Mandanten.

Auch schützt § 100d Abs. 5 Satz 1 StPO nur die nach § 53 StPO Zeugnisverweigerungsberechtigten vor gegen sie selbst gerichtete Maßnahmen nach § 100b Abs. 1 StPO. In Bezug auf die nach §§ 52 und 53a StPO Zeugnisverweigerungsberechtigten gilt kein absolutes Beweis**erhebungs**verbot, sondern lediglich ein von einer Abwägungsentscheidung abhängendes, eingeschränktes **Verwertungs**verbot, vgl. § 100d Abs. 5 Satz 2 StPO.

Infolge dieser möglichen Verwertbarkeit von erhobenen Informationen besteht für die Beschwerdeführerin zu 2 eine gegenüber dem Beschwerdeführer zu 1 noch erhöhte Gefahr, von Maßnahmen nach §§ 100a Abs. 1 Satz 2, 100b Abs. 1 StPO und damit analog zum Beschwerdeführer. zu 1 in ihren Grundrechten betroffen zu sein.

(3) Beschwerdeführer zu 3

Der Beschwerdeführer zu 3 recherchiert seit Jahren im Deliktsbereich des § 265e StGB. Dazu nutzt er u.a. Mittel der elektronischen Kommunikation, insbesondere E-Mails. Er hat Kontakt nicht nur zu reinen Hinweisgebern, sondern auch zu Personen, die möglicherweise selbst Straftaten begangen haben. Seine Recherchen beziehen sich regelmäßig auf große Sportwettbetrugs- und Manipulationsfälle, die die Voraussetzungen eines besonders schweren Falls gem. § 265e Satz 2 StGB erfüllen. Indem sich der Beschwerdeführer zu 3 auf den Bereich Doping spezialisiert hat, steht er mit potentiellen Straftätern auch nicht nur gelegentlich in Kontakt.

Es ist deshalb wahrscheinlich, dass er im Rahmen seiner Recherchen mit Personen kommuniziert, die Maßnahmen nach § 100a Abs. 1 Satz 2 StPO unterworfen sind, wodurch er in seinen Grundrechten aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG (Recht auf informationelle Selbstbestimmung) und Art. 12 Abs. 1 GG betroffen ist.

III. Beschwerdebefugnis der Beschwerdeführer zu 3 bis 5 unter dem Aspekt der Schutzpflichtverletzung

Auch die Beschwerdeführer zu 3 bis 5 sind möglicherweise in Grundrechten verletzt (dazu unter 1) und unmittelbar, selbst und gegenwärtig von den angegriffenen Vorschriften betroffen (dazu unter 2).

1. Möglichkeit der Grundrechtsverletzung

§§ 100a Abs. 1 Satz 2 und 3, 100b StPO verletzen die Beschwerdeführer zu 3 bis 5 zumindest möglicherweise in ihrem Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1

i.V.m. Art. 1 Abs. 1 GG), da die Bundesrepublik Deutschland sie durch die Einführung der angegriffenen Rechtsgrundlagen ohne flankierende Regelungen zur Sicherung der IT-Sicherheit bewusst dem Risiko von Angriffen auf ihre IT-Systeme aussetzt.

Der Beschwerdeführer zu 4 ist als Investigativ-Journalist im Exil besonders angewiesen auf ein hohes Sicherheitsniveau seiner IT-gestützten Kommunikation und seiner IT-Systeme. Nur dank sicherer Kommunikationskanäle können Investigativ-Journalisten Hinweisgebern und Informanten die Vertraulichkeit ihrer Kommunikation zusichern und dadurch das für ihre Arbeit erforderliche Vertrauen aufbauen. Und nur ein integres IT-System verhindert, dass darauf gespeicherte Informationen und Arbeitsprodukte durch Dritte heimlich verändert oder gelöscht werden. Im Falle des Beschwerdeführers zu 4 kommt hinzu, dass er wegen massiver Anfeindungen sowohl durch die türkische Regierung wie durch der Regierung nahestehende Gruppen auch ein ganz persönliches Interesse an einem integren IT-System hat, um sich selbst und seine Familie zu schützen, etwa indem sein Aufenthaltsort nicht bekannt wird.

Analog gilt das für den Beschwerdeführer zu 3, der sich durch seine Aufdeckung des staatlich gelenkten russischen Doping-Programms die Regierung der Russischen Föderation zum Gegner gemacht hat. Es darf zugleich als allgemeinkundig gelten, dass staatliche russische Stellen eine zentrale Rolle spielen, wenn es um Hacking-Angriffe gegen private und staatliche Stellen westlicher Staaten geht, beispielsweise werden der „Hack“ des Deutschen Bundestages 2015 sowie des Wahlkampfteams von Hillary Clinton 2016 seitens der jeweils zuständigen Ermittlungsbehörden solchen Täterkreisen zugeordnet. Dies zusammengenommen liegt es nahe, dass der Beschwerdeführer zu 3 einer großen Bedrohung durch IT-Angriffe mit staatlich-russischem Hintergrund ausgesetzt ist.

Auch der Beschwerdeführer zu 5 hat ein hohes Interesse an IT-Sicherheit. Die von ihm bearbeiteten Themenfelder und die von ihm bekleideten Ämter machen ihn zu einem außerordentlich attraktiven Ziel für fremde Geheimdienste. Er muss außerdem mit Informationen umgehen, die eine besondere Sicherheit seiner IT-Systeme verlangen.

Die Beschwerdeführer zu 3 bis 5 sind folglich darauf angewiesen, dass – infolge der Fehlbarkeit menschlichen Handelns als solche unvermeidbare – Sicherheitslücken ihrer IT-Systeme schnellstmöglich geschlossen werden. Denn je länger eine Sicherheitslücke besteht, desto höher die Wahrscheinlichkeit, dass sie durch interessierte Kreise gefunden und für Angriffe auf die IT-Systeme der Bf. missbraucht wird. Dabei hängen die Beschwerdeführer zu 3 bis 5 in erster Linie ab von Maßnahmen der Hersteller der von ihnen verwendeten Programme und IT-Systeme. Diese haben ein eigenes Interesse daran – und sind je nach Vertragsverhältnis ggf. dazu verpflichtet –, ihnen bekanntwerdende Sicherheitslücken zu schließen, bevor böswillige Personen sie ausnutzen. In diesem Wettlauf suchen die Hersteller zwar auch selbständig nach Sicherheitslücken und loben mitunter gar Preisgelder für gefundene Lücken aus (sog. Bug-Bounty-Programme). Gleichwohl sind sie davon abhängig, dass Dritte sie auf bestehende Sicherheitslücken hinweisen.

Staatliche Stellen können Kenntnis von Sicherheitslücken noch vor den Herstellern der betroffenen Programme und IT-Systeme erhalten, beispielsweise über Meldungen von Firmen oder Behörden, die von Angriffen auf ihre IT-Systeme betroffen waren. Die §§ 100a Abs. 1 Satz 2 und 3, 100b StPO begünstigen indes einen Umgang mit solchen Sicherheitslücken, der sich besonders auf die Beschwerdeführer zu 3 bis 5, abgeschwächt aber auch auf die restliche Bevölkerung fatal auswirkt. Denn durch die Erlaubnis, IT-Sicherheitslücken für Angriffe auf Zielpersonen im Ermittlungsverfahren zu nutzen, schaffen §§ 100a Abs. 1 Satz 2 und 3, 100b StPO einen starken Anreiz für Ermittlungsbehörden, Sicherheitslücken gerade nicht den Herstellern zu melden und dadurch zu ihrer

Schließung beizutragen. Vielmehr legen es die angegriffenen Normen – jedenfalls im Zusammenspiel mit dem staatlichen Unterlassen, klare Regeln für das Melden von Sicherheitslücken aufzustellen – allen Behörden geradezu nahe, zukünftig ein „Arsenal“ staatlicher Infiltrationsmöglichkeiten anzulegen und geheimzuhalten, die sich für Maßnahmen gem. §§ 100a Abs. 1 Satz 2 und 3, 100b StPO nutzen lassen. Die Geheimhaltung der Sicherheitslücken vor den Herstellern ist nach der derzeitigen Ausgestaltung der §§ 100a Abs. 1 Satz 2 und 3, 100b StPO offenbar sogar erwünscht, jedenfalls enthalten diese Ermächtigungsgrundlagen entgegen beispielsweise dem Vorschlag der vom Rechtsausschuss des Deutschen Bundestages angehörten Sachverständigen RiLG Dr. Ulf Buermeyer und Linus Neumann gerade keine Begrenzung auf bestimmte Formen staatlichen Hackings. Dieses bewusste und beredte Schweigen des Gesetzgebers lässt sich nur so verstehen, dass er jede Form staatlichen Hackings zur Durchführung von Maßnahmen nach §§ 100a Abs. 1 Satz 2 und 3, 100b StPO in seinen Willen aufgenommen hat.

Durch diese für die IT-Sicherheit in Deutschland und der Welt verheerende Anreizstruktur verletzen §§ 100a Abs. 1 Satz 2 und 3, 100b StPO die Beschwerdeführer zu 3 bis 5 zumindest möglicherweise in ihrem Grundrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG („IT-Grundrecht“). Denn nach der Rechtsprechung des Bundesverfassungsgerichts hat der Einzelne ein aus dem Allgemeinen Persönlichkeitsrecht abgeleitetes Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Dazu grundlegend BVerfGE 120, 274 <302 ff.>.

Geschützt von diesem Grundrecht ist zunächst das Interesse des Nutzers, dass die von einem vom Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben. Ein Eingriff in dieses Grundrecht ist zudem dann anzunehmen, wenn die Integrität des geschützten informationstechnischen Systems angetastet wird, indem auf das

System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können; dann ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen.

> BVerfGE 120, 274 <314>.

Neben dieser Abwehrdimension leiten sich aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG auch grundrechtliche Schutzpflichten ab.

> Vgl. allgemein zu Schutzpflichten bzgl. des Allgemeinen Persönlichkeitsrechts *Di Fabio*, in: Maunz/Dürig, GG, Stand: 81. EL Sep. 2017, Art. 2 Rn. 135 f.

Die Vernachlässigung von grundrechtlichen Schutzpflichten kann von den Betroffenen mit der Verfassungsbeschwerde geltend gemacht werden.

> BVerfGE 77, 170 <214>; 77, 381 <402 f.>; 79, 174 <201 f.>; 125, 39 <78>.

Die hier zumindest mögliche Schutzpflicht folgt bereits aus dem Auftrag zur **Gewährleistung** der Vertraulichkeit und Integrität informationstechnischer Systeme. Diesen Auftrag erfüllt der Staat, indem er den Einzelnen auch vor Angriffen Dritter auf seine IT-Systeme schützt, in welcher konkreten Form auch immer: Die Beschwerdeführer verkennen nicht, dass dem Gesetzgeber im Bereich der grundrechtlichen Schutzpflichten traditionell ein weiter Gestaltungsspielraum zugebilligt wird. Dieser wird jedoch dann verlassen, wenn der Bund seiner Schutzpflicht überhaupt nicht nachkommt: Sachgerecht und naheliegend wäre etwa eine umfassende Verpflichtung aller Stellen des Bundes, insbesondere aber der mit der Durchführung von Maßnahmen nach §§ 100a Abs. 1 Satz 2, 100b Abs. 1 StPO betrauten Stellen, ihnen bekannte, dem Hersteller aber noch unbekannte Sicherheitslücken diesem zu melden, damit für Abhilfe gesorgt werden kann. Diese besteht indes nicht. Als absolute Mindestanforderung

hat der Bund aber im Lichte seines Schutzauftrags davon abzusehen, eine ohnehin prekäre IT-Sicherheitslage noch zu verschärfen, indem er durch die gesetzliche Neuregelung der §§ 100a, 100b StPO massive Anreize zum Horten und Geheimhalten von Sicherheitslücken schafft.

> Eine staatliche Pflicht zum Schutz der IT-Systeme von Privaten bejahen auch *Gersdorf*, in: BeckOK Informations- und Medienrecht, Stand: 1.05.2017, Art. 2 Rn. 29; *Roßnagel/Schnabel*, NJW 2008, 3534 (3535); *Becker*, NVwZ 2015, 1335 (1339 f.) *Sachs/Krings*, JuS 2008, 481 (486). Für eine ausführliche Herleitung der Schutz- und Förderpflicht zur Gewährleistung der IT-Sicherheit *Heckmann*, in: FS Käfer, 2009, S. 129 (133 ff.).

Weil die §§ 100a Abs. 1 Satz 2 und 3, 100b StPO jedoch Anreize für Sicherheitsbehörden schaffen bzw. es sogar erfordern, bekannt gewordene Sicherheitslücken von Programmen und IT-Systemen nicht an die Hersteller zu melden, stehen sie der staatlichen Pflicht entgegen, die Vertraulichkeit und Integrität der informationstechnischen Systeme der Beschwerdeführer zu 3 bis 5 zu schützen. Eine Grundrechtsverletzung erscheint zumindest möglich. Auch insoweit machen sich die Beschwerdeführer zu 3 bis 5 die untenstehenden Ausführungen zur Begründetheit der Verfassungsbeschwerde zu eigen.

2. Betroffenheit

§§ 100a Abs. 1 Satz 2 und 3, 100b StPO betreffen die Beschwerdeführer zu 3 bis 5 unmittelbar in ihrem Grundrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, weil es zu ihrer Beschwer keines weiteren gegen sie gerichteten Akts bedarf. Vielmehr folgt ihre Betroffenheit gerade aus der signifikant erhöhten Dauergefahr, die daraus resultiert, dass Stellen des Bundes wegen §§ 100a Abs. 1 Satz 2 und 3, 100b StPO ihnen bekanntwerdende Sicherheitslücken unter Verletzung der Schutzpflicht des Bundes gegenüber den Beschwerdeführern zu 3

bis 5 nicht an die Hersteller der betroffenen Programme und IT-Systeme melden.

Die Beschwerdeführer zu 3 bis 5 sind auch selbst und gegenwärtig von dem Gesetz betroffen, weil sie IT-Systeme nutzen und auf ihre Integrität und Vertraulichkeit in besonderem Maße angewiesen sind.

Die Betroffenheit der Beschwerdeführer zu 3. und zu 4. ergibt sich daraus, dass sie – der Beschwerdeführer zu 3 als ein seitens russischer Stellen als feindlich eingestufter westlicher Journalist, der Beschwerdeführer zu 4 als türkischer Investigativjournalist im Exil – sehr attraktive Ziele für die russische bzw. türkische Regierung und ihr nahestehende Gruppen sind (vgl. dazu bereits oben B.II.3 sowie B.II.4). Die IT-Systeme beider Beschwerdeführer werden regelmäßig mit elektronischen Mitteln attackiert. Es bestehen keine Anhaltspunkte dafür, dass sich das in Zukunft ändert.

Auch der Beschwerdeführer zu 5 ist als Mitglied des Bundestags und auf Grund der besonderen Ausrichtung seiner Tätigkeit täglich mit der Gefahr von Angriffen auf seine IT-Systeme konfrontiert (vgl. dazu oben B.II.5). Im Jahr 2015 war der Bundestag bereits Opfer eines großangelegten Angriffs.

> Bericht der taz vom 29. August 2017, online abrufbar unter: http://www.taz.de/!5436704/ (zuletzt abgerufen am 4. August 2018).

Es ist – jedenfalls für die Dauer seiner Mandatstätigkeit – jederzeit damit zu rechnen, dass Hacker versuchen werden, unter Ausnutzung einer Sicherheitslücke die IT-Systeme des Beschwerdeführers zu 5 auszuforschen oder zu manipulieren.

IV. Rechtsschutzbedürfnis

Gegen formelle Gesetze des Bundes ist ein Rechtsweg nicht gegeben, weshalb die Verfassungsbeschwerde trotz § 90 Abs. 2 Satz 1 BVerfGG erhoben werden konnte.

D. Begründetheit der Verfassungsbeschwerde

Im Zentrum dieser Verfassungsbeschwerde stehen zwei eigenständige verfassungsrechtliche Angriffe: zum einen die (partielle) materielle Verfassungswidrigkeit der Regelungen über die Quellen-Telekommunikationsüberwachung (§ 100a Abs. 1 Satz 2 und 3, Abs. 5 und 6 StPO) und der Online-Durchsuchung (§ 100b StPO) sowie daraus abgeleiteter gesetzlicher Bestimmungen (hierzu unter II), zum anderen die Verletzung der staatlichen Schutzpflicht für die IT-Sicherheit, die aus der objektiv-rechtlichen Dimension des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme erwächst und die die Beschwerdeführer zu 3 bis 5 aufgrund ihrer besonderen Verletzlichkeit auch als Verletzung subjektiver Rechte rügen können (hierzu unter III).

Da der Inhalt und der verfassungsrechtliche Bestand eines Gesetzes indes auch durch das bei seiner Entstehung gewählte Verfahren bestimmt wird, wird vorab auf einige Ungewöhnlichkeiten in der Gesetzgebungsgeschichte hingewiesen, aufgrund derer die angegriffenen Normen bereits formell verfassungswidrig sind (hierzu unter I).

I. Zur Gesetzgebungsgeschichte

Die mit dieser Verfassungsbeschwerde angegriffenen Regelungen der Quellen-Telekommunikationsüberwachung (§ 100a Abs. 1 Satz 2 und 3, Abs. 5 und 6 StPO) sowie der Online-Durchsuchung (§ 100b StPO) sowie daraus abgeleiteter gesetzlicher Regelungen sind nicht in einem den Anforderungen des Grundgesetzes genügenden Gesetzgebungsverfahren zustande gekommen.

Ausgangspunkt waren die Entwürfe der Bundesregierung eines „Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens“,

BT-Drucksache 18/11277,

sowie eines „Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze“,

BT-Drucksache 18/11272,

beide datierend auf den 22. Februar 2017. Diese enthielten die hier verfahrensgegenständlichen Ermächtigungsgrundlagen für Online-Durchsuchung und Quellen-TKÜ noch nicht. Vor ihrer Zuleitung an den Bundestag hatte der Bundesrat zu beiden Gesetzesinitiativen Gelegenheit zur Stellungnahme (gemäß Art. 76 Abs. 2 Satz 2 GG), wovon er auch Gebrauch gemacht hat.

BT-Drucksache 18/11277, S. 44 ff.; BT-Drucksache 18/11272, S. 44 ff. mit einer Gegenäußerung der Bundesregierung, BT- Drs. 18/11272, S. 48 ff.

Die Gesetzesentwürfe wurden in der 221. Sitzung des Deutschen Bundestages am 9. März 2017 beraten und an den Ausschuss für Recht und Verbraucherschutz zur federführenden Beratung und an den Innenausschuss zur Mitberatung überwiesen. Der Ausschuss für Recht und Verbraucherschutz hat beide Gesetzesentwürfe auf seiner Sitzung am 8. März 2017 anberaten und beschlossen, eine öffentliche Anhörung durchzuführen. Diese fand hinsichtlich der BT-Drucksache 18/11272 am 22. März 2017 unter Anhörung von sieben Sachverständigen und hinsichtlich der BT-Drucksache 18/11277 unter Anhörung weiterer sieben Sachverständiger statt. Bis zu diesem Zeitpunkt handelte es sich damit um ein unauffälliges Gesetzgebungsvorhaben.

Unter dem 15. Mai 2017 kursierte plötzlich eine Drucksache des Ausschusses für Recht und Verbraucherschutz, die die Überschrift trägt „Formulierungshilfe der Bundesregierung für einen Änderungsantrag der Fraktionen CDU/CSU und SPD zum dem Gesetzentwurf der Bundesregierung – Drucksache 18/11272 – Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze“.

Ausschussdrucksache 18(6)334.

Auf wen die Initiative zur Ausarbeitung einer derartigen „Formulierungshilfe“ zurückgeht, lässt sich den veröffentlichten Dokumenten des Ausschusses und des Bundestages nicht entnehmen. Sie enthält auf 14 eng gedruckten Seiten Vorschläge vor allem zur Ergänzung und Änderung der Strafprozessordnung und partieller Änderungen bei zehn anderen Gesetzen; auf weiteren 16 Seiten werden die Änderungen näher begründet.

Die in der „Formulierungshilfe“ vorgeschlagenen gesetzlichen Änderungen dürften (nebst Begründung) beim Bundesministerium der Justiz und für Verbraucherschutz schon seit längerer Zeit „auf Halde“ gelegen haben. Die Begründung zitiert als letzte Entscheidung des Bundesverfassungsgerichts die vom 20. April 2016 zum BKAG (BVerfGE 141, 220 ff.).

Schon die zur Auslegung des Merkmals „Telekommunikation“ am 6. Juli 2016 getroffene Entscheidung der 3. Kammer des Zweiten Senats des Bundesverfassungsgerichts,

> Beschluss vom 6. Juli 2016 – 2 BvR 1454/13 (= NJW 2016, 3508 ff.) –,

kommt nicht mehr vor. Die zitierte Kommentarliteratur stammt aus dem Jahr 2015.

> So wird der Kommentar von *Meyer-Goßner/Schmitt* zur StPO noch mit der 58. Auflage aus 2015 zitiert. Zum Zeitpunkt der Einbringung der „Formulierungshilfe“ am 15. Mai 2017 war schon die 60. Auflage erschienen.

Auch der Umstand, dass die im Art. 1 der „Formulierungshilfe“ geregelten Änderungen der Strafprozessordnung mit dem Hinweis beginnen, die Strafprozessordnung sei *„zuletzt durch Artikel 3 Absatz 5 des Gesetzes vom 23. Dezember 2016 (BGBl. I S. 3346) geändert worden“,* während tatsächlich zum Zeitpunkt der Einbringung dieser „Formulierungshilfe“ die Strafprozessordnung zuletzt durch Artikel 3 des Gesetzes vom 13. April 2017 (BGBl. I S. 1074,

1319) geändert worden war, ist ein untrügliches Indiz, dass die „Formulierungshilfe“ schon längere Zeit bereit gelegen hat, bis sie schließlich am 15. Mai 2017 zum Einsatz kam.

Schon dieser Sachverhalt – einer wahrscheinlich schon wenigstens seit einigen Monaten im Bundesministerium der Justiz und für Verbraucherschutz abgeschlossenen Vorbefassung und Ausformulierung des im Mai 2017 aus heiterem Himmel als „Formulierungshilfe“ präsentierten de-facto-Gesetzesentwurfs – lässt es als anstößig erscheinen, dass er ohne vorherige Anhörung des Bundesrates und ohne eine erste Beratung im Deutschen Bundestag als schlichter Änderungsantrag, angeblich aus der Mitte der Abgeordneten der Regierungsfraktionen, in größter Eile in das Gesetzgebungsverfahren zu den Gesetzesentwürfen vom 22. Februar 2017 integriert wurde:

Bereits zwei Tage nach dem „Auftauchen“ der „Formulierungshilfe“ wurde sie – gemeinsam mit der BT-Drucksache 18/11272 – im Ausschuss für Recht und Verbraucherschutz beraten und die Durchführung einer weiteren Anhörung von Sachverständigen beschlossen. Diese Anhörung fand am 31. Mai 2017 statt. Die Sachverständigen, die zur Vorbereitung knapp zehn Tage Zeit hatten, verwiesen überwiegend darauf, dass ein so gewichtiges Gesetzesvorhaben mehr Zeit des Überdenkens und Beratens bedürfe. Nur beispielhaft hierfür der Sachverständige Richter am Landgericht Dr. Ulf Buermeyer:

> *„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 scheint 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."

Das kümmerte die Mehrheit des Ausschusses offenbar nicht. In der Beschlussempfehlung und dem Bericht des Ausschusses für Recht und Verbraucherschutz vom 20. Juni 2017 wurde ein Gesetzentwurf vorgelegt, der die Vorschläge aus der BT-Drucksache 18/11272 und aus der „Formulierungshilfe" in den Gesetzesentwurf aus der BT-Drucksache 18/11277 integrierte,

BT-Drucksache 18/272,

so dass das Gesamtpaket nunmehr als „Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens" firmierte. Zum Beratungsverlauf im Ausschuss berichtet die Beschlussempfehlung vom 20. Juni 2017 lediglich folgendes:

„Die Fraktion BÜNDNIS 90/DIE GRÜNEN kritisierte das Gesetzgebungsverfahren. Mit einem Überraschungscoup werde ein schwerer Grundrechtseingriff eingeführt. Dieser betreffe insbesondere das Grundrecht auf die Integrität informationstechnischer Systeme und das Recht auf informationelle Selbstbestimmung der gesamten Bevölkerung. Die Qualität dieses Eingriffs verändere das ursprüngliche Vorhaben zur Änderung der Strafprozessordnung völlig; er sei noch gravierender und umfassender als der Große Lauschangriff. Angesichts der bestehenden Gefahren bestreite die Fraktion eine gewisse Notwendigkeit zur Schaffung solcher Regelungen nicht. Diese müssten jedoch sehr sorgfältig überlegt und im Einzelnen abgewogen werden. Dies sei vorliegend nicht der Fall, insbesondere seien zu viele Öffnungsklauseln vorgesehen. Außerdem müsse sichergestellt werden, dass neben der

richterlichen Überprüfung auch Fachleute an der Technik und Kontrolle der Maßnahmen beteiligt seien. Die Fraktion kritisierte zudem eine Ungleichbehandlung von zeugnisverweigerungsberechtigten Berufsgeheimnisträgern und deren Helfern in § 100d Absatz 5 StPO-E.

Die Fraktion DIE LINKE. schloss sich der Kritik daran an, dass die Quellen-Telekommunikationsüberwachung über einen Änderungsantrag in das Gesetz gebracht werde."

Das Gesetz wurde im Deutschen Bundestag nach kurzer und heftiger Debatte am 22. Juni 2017 in zweiter und dritter Lesung verabschiedet.

BT-Protokolle, 18. Wahlperiode, S. 24549.

Die Kritik der Fraktionen der GRÜNEN und der LINKEN ist angesichts der Eingriffstiefe der zur Quellen-TKÜ und zur Online-Durchsuchung getroffenen Regelung angebracht. Zugleich markiert sie auch die formelle Verfassungswidrigkeit der angegriffenen Normen:

Die „Formulierungshilfe" wurde zwar formell seitens der damaligen Regierungsfraktionen als Änderungsantrag zu einem laufenden Gesetzgebungsverfahren eingeführt. Dabei handelt es sich indes um eine Scheinkonstruktion: Der Sache nach beinhaltet die „Formulierungshilfe" einen Gesetzentwurf der Bundesregierung, der unter Umgehung der Verfahrensvorschriften des Grundgesetzes für solche Vorlagen in das parlamentarische Verfahren eingebracht wurde. Insoweit ist es bedeutsam, dass die Formulierungshilfe in der o.g. Ausschussdrucksache als eine solche „der Bundesregierung" bezeichnet wurde: Sie muss also auf eine Beschlussfassung der Bundesregierung zurückgehen. Sie ist nicht etwa nur eine „verkappte Regierungsvorlage",

So das Stichwort in der staatsrechtlichen Literatur: *Masing*, in von Mangoldt/Klein/Starck (Hrsg.), GG, 6. Aufl., Art. 76 Rn. 97; *Masing/Risse* in

von Mangoldt/Klein/Starck (Hrsg.), GG, 7. Aufl., Art. 76 Rn. 105; *Brosius-Gersdorf* in Dreier (Hrsg.), GG, 3. Aufl., Art. 76 Rn. 58,

unter der Maskerade einer Vorlage „aus der Mitte des Bundestages“, sondern, wenn auch als „Formulierungshilfe“ bezeichnet, die **Entschließung der Bundesregierung über einen Gesetzgebungsvorschlag**, der nach der Kompetenzordnung des Grundgesetzes zunächst dem Bundesrat zuzuleiten gewesen wäre (Art. 76 Abs. 2 Satz 1 GG).

Masing a.a.O.; *Brosius-Gersdorf* in Dreier (Hrsg.), GG, 3. Aufl., Art. 76 Rn. 60.

Die Umgehung des grundgesetzlichen Verfahrens lässt sich schließlich auch nicht damit rechtfertigen, dass besondere Eile geboten gewesen wäre: Zum einen war das vermeintliche Bedürfnis nach Rechtsgrundlagen für „Staatstrojaner“ in der StPO bereits Gegenstand des Koalitionsvertrages aus dem Jahr 2013, sodass während der gesamten Legislaturperiode reichlich Gelegenheit gewesen wäre, einen Gesetzentwurf im Einklang mit den Verfahrensvorschriften des Grundgesetzes zum Gegenstand der parlamentarischen Beratungen zu machen. Zum anderen ließ das Bundesministerium der Justiz und für Verbraucherschutz den fertigen Gesetzentwurf wie oben gezeigt wenigstens einige Monate „in der Schublade“ liegen, ehe es ihn in Form der „Formulierungshilfe“ in die laufenden Beratungen eines Gesetzgebungsverfahrens zu völlig anderen Gegenständen einspeisen ließ.

Zwar wären die Beschwerdeführer nicht berechtigt, diese Kompetenzverstöße isoliert zum Gegenstand ihrer Beschwerde zu machen. Das ändert aber nichts daran, dass die angegriffenen Normen schon formell verfassungswidrig sind, sodass die in dieser Beschwerdeschrift ansonsten dargestellten Eingriffe in Grundrechte nicht auf einer verfassungsmäßigen Ermächtigungsgrundlage beruhen.

II. Verletzung der Beschwerdeführerin und Beschwerdeführer zu 1 bis 3 in ihren Grundrechten

1. Zum Eingriff in ein informationstechnisches System „mit technischen Mitteln“, insbesondere zur unzureichenden verfahrensmäßigen Absicherung

Sowohl die neuen Vorschriften zur Telekommunikationsüberwachung in § 100a Abs. 1 Satz 2 und 3 StPO als auch zur Online-Untersuchung in § 100b Abs. 1 StPO haben die Gemeinsamkeit, dass in ein von dem Betroffenen genutztes informationstechnisches System „mit technischen Mitteln“ eingegriffen werden darf. Technisch sollen die Quellen-Telekommunikationsüberwachung und die Online-Durchsuchung „über eine spezielle Software erfolgen, die auf dem Endgerät des Betroffenen verdeckt installiert wird“.

BT-Drucksache 18/12785, S. 49.

Jeder Zugriff auf ein informationstechnisches System dürfe „grundsätzlich nur auf technischem Wege oder mittels kriminalistischer List“ erfolgen (nicht durch ein heimliches Betreten der Wohnung).

BT-Drucksache 18/12785, S. 52.

Eine nähere Beschreibung der eingesetzten „speziellen Software“ sowie des von „kriminalistischer List“ geprägten Vorgehens findet sich in der Begründung des maßgeblichen Gesetzesentwurfs nicht.

Dies ist verfassungsrechtlich nicht hinnehmbar:

Die § 100a Abs. 5, § 100b Abs. 1 StPO 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) 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 einer 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[1] 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.

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) und der zuständigen Kammer bzw. dem Senat (bei der Online-Durchsuchung, vgl. § 100e Abs. 2 StPO) nicht ernsthaft verlangt werden, eine EDV-technische Überprüfung des beabsichtigten Staatstrojaners selbst vorzunehmen. Eine externe Prüfung wiederum dürfte angesichts der hierfür notwendigen Zeit – wenigstens Tage, wohl eher Wochen – in vielen Fällen den Zweck der Maßnahme gefährden. Die Verantwortung hierfür wird kaum 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 genannten, aber auch weiterer aus der Perspektive

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

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. 2 Abs. 1 i.V.m. Art. 1 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. Zwar ist zu begrüßen, dass sich das Bundeskriminalamt nach Presseberichten um die Eigenprogrammierung einer Überwachungssoftware bemüht; für den Bereich der sogenannten Quellen-TKÜ soll diese einsatzbereit sein.

> Vgl. Heise online, online abrufbar unter https://www.heise.de/newsticker/meldung/Quellen-Telekommunikationsueberwachung-Neuer-Bundestrojaner-steht-kurz-vor-Einsatzgenehmigung-3113444.html (zuletzt abgerufen am 20. August 2018).

Zugleich ist es aber auch nach jahrelangen Bemühungen dem BKA bis heute offenbar nicht gelungen, eine Lösung zu programmieren, die tatsächlich nachvollziehbar die rechtlichen Grenzen für Staatstrojaner einhält. Daher ist der Bund hier weiterhin auf die Hilfe dubioser Dienstleister wie etwa der Firma FinFisher angewiesen, die ihre nicht zuletzt mit Mitteln des Bundes erstellten Schadprogramme auch in autoritäre Staaten exportieren – so etwa in die Türkei, die damit den Beschwerdeführer zu 4 auszuspähen versucht, aber u.a. auch nach Ägypten und Bahrain. Zudem enthalten diese Trojaner oftmals zusätzliche, durch die Rechtsprechung des angerufenen Gerichts in Deutschland schlechthin nicht zugelassene Funktionen, etwa zur bewussten Manipulation des Zielsystems durch Unterschieben von Beweismitteln, die dann bei einer offenen

Durchsuchung aufgefunden werden können. Konsequenterweise schließt das am 22. Juni 2017 verabschiedete Gesetz gerade nicht aus, dass auch – oder gar ausschließlich – Staatstrojaner zum Einsatz kommen, die weder vom BKA selbst programmiert noch extern und unabhängig geprüft sind und deren Verwendung zugleich Menschenrechtsverletzungen in Drittstaaten fördert. So „pragmatisch" dies auch sein mag – der Gesetzgeber nimmt damit billigend in Kauf, dass auch in Deutschland Staatstrojaner zum Einsatz kommen, die gerade nicht den (ohnehin nur fragmentarischen) gesetzlichen Anforderungen an deren technische Gestaltung genügen. Zudem bedarf es einer obligatorischen Prüfung beispielsweise durch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit auf Ebene des Quelltextes, weil nur diese oder eine ähnlich unabhängige Stelle die Gewähr für eine wirklich neutrale Begutachtung der Software bietet.

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 unter verpflichtender Mitwirkung der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vorgegeben werden. Die geltende gesetzliche Regelung 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) aufgenommen werden. Solange dies nicht geschehen ist, trifft die geltende Regelung das Verdikt der Verfassungswidrigkeit.

2. Zur „kleinen“ Online-Durchsuchung gemäß § 100a Abs. 1 Satz 2 und 3 StPO

Es ist Voraussetzung einer nur an Art. 10 Abs. 1 GG zu messenden Quellen-TKÜ, dass ausschließlich „laufende Kommunikation“ erhoben wird.

> BVerfGE 120, 274 <309>; vgl. zu Begriff und Inhalt eingehend *Buermeyer,* StV 2013, 470.

Der Grundrechtsschutz „lediglich“ nach Art. 10 Abs. 1 GG erstreckt sich nicht auf die nach Abschluss eines Kommunikationsvorgangs im Herrschaftsbereich eines Kommunikationsteilnehmers gespeicherten Inhalte und Umstände der Telekommunikation,

> BVerfGE 220, 274 <307 f.>,

(„kondensierte“ Kommunikation). Gilt ein heimlicher staatlicher Zugriff der Ausforschung dieser Inhalte, so misst sich dessen Zulässigkeit vielmehr an den weitaus strengeren Anforderungen des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

> BVerfGE 120, 274 <308>.

Der neu geschaffene § 100a Abs. 1 Satz 2 und 3 StPO soll jedoch 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 gestatten.

Dass dies im Widerspruch zu den Vorgaben des Bundesverfassungsgerichts steht, war der Bundesregierung durchaus präsent. Zur Begründung verweist die „Formulierungshilfe“ indes auf eine klassische Analogie: Ebenso wie bei laufender Kommunikation erscheine es auch bei früherer Kommunikation „verfas-

sungsrechtlich nicht geboten, die wegen der besonderen Sensibilität informationstechnischer Systeme ... aufgestellten höheren Anforderungen des Bundesverfassungsgerichts [für Eingriffe in das IT-Grundrecht] anzuwenden“.

BT-Drucksache 18/12785, S. 50.

Indes ist bereits die Figur der Quellen-TKÜ für laufende Kommunikation eine Ausnahme von der Regel, dass Trojaner-Einsätze einen Eingriff in dieses Grundrecht darstellen; hinzukommt, 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 Bundesverfassungsgerichts zur Abgrenzung zwischen Online-Durchsuchung und Quellen-TKÜ zu übergehen.

Neben das rechtstechnische tritt indes ein weiteres, informationstechnisches Argument. Der Gesetzesentwurf räumt ein, dass nicht sämtliche gespeicherte Kommunikation als Quellen-TKÜ auslesbar sein soll, sondern nur solche 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 liegt 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. Das Gesetz erlaubt somit eine stillschweigende Online-Durchsuchung, um festzustellen, welche ehemaligen Kommunikationsinhalte der Staatstrojaner unter den leichteren Voraussetzungen einer Quellen-TKÜ ausleiten darf.

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 ist § 100a Abs. 1 Satz 2 und 3 StPO verfassungswidrig; gleiches gilt für dessen verfahrensrechtliche Umsetzung in § 100a Abs. 5 Nr. 1 lit. b StPO-E.

3. Zur Online-Durchsuchung gemäß § 100b StPO

Die am 24. August 2017 in Kraft getretene Regelung der Online-Durchsuchung in § 100b StPO ist der mit Abstand weitest gehende Eingriff in Grundrechte, die die Strafprozessordnung zur Informationsgewinnung kennt. Sie 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 Infiltration der informationstechnischen Systeme von Beschuldigten wird ermöglicht

- 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.

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 enthält aber keine entsprechende Begrenzung, vielmehr wäre eine solche Maßnahme vom Wortlaut der Norm gedeckt. Die gesetzliche Regelung 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.

Die Bedeutung der Regelung wird deutlich, wenn man sich vor Augen führt, dass Computer und Smartphones heute oft eine unermessliche Fülle an Informationen

vgl. bereits BVerfGE 120, 274 <303 ff.> aus dem Jahr 2008.

enthalten: alltägliche bis intimste E-Mails 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.

BVerfGE 120, 274 <323>.

Dieser unvergleichlich tiefe Einblick in das Wissen und Fühlen eines Menschen macht die Online-Durchsuchung in einem Rechtsstaat unvergleichlich heikel. Wie keine andere Ermittlungsmethode erlaubt sie es, Menschen zum Objekt der Ausspähung zu machen. Gegen keine andere Methode sind Beschuldigte – für die immerhin die Unschuldsvermutung gilt – so wehrlos, denn der direkte heimliche 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. Hinzukommt 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.

Der unvergleichlichen Gefahren staatlicher Überwachungssoftware war sich auch das angerufene Gericht 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 der allgemeinen Handlungsfreiheit (Art. 2 Abs. 1 GG) das „Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme“ als neue Ausprägung es Allgemeinen Persönlichkeitsrechts 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.

BVerfGE 120, 274 <323>.

Weiter vertieft wird der Eingriff durch seine unvermeidliche Streubreite[2].

BVerfG, a.a.O.

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 Eingriff ermächtigt, den Grundrechtsschutz für den Betroffenen auch durch geeignete Verfahrensvorkehrungen sichern.“
>
> BVerfGE 120, 274 <326>.

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

[2] BVerfG a.a.O.

> 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."
>
> BVerfGE 120, 274 <328> (Herv. d. Verf.).

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."
>
> BVerfGE 120, 274 <328> (Herv. d. Verf.).

Selbst präventiv ist der Einsatz von Staatstrojanern mithin nur dann zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr 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 Menschen berührt. Andere Rechtsgüter wie etwa Eigentum oder Vermögen können einen Eingriff in das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme hingegen per se nicht rechtfertigen.

Bei einer **Regelung für den Strafprozess** ist neben der Umsetzung der oben genannten Vorgaben des Bundesverfassungsgerichts auch eine Transferleistung zu erbringen. Die Anforderungen des Bundesverfassungsgerichts an Eingriffe

in das IT-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 dem Schutz von Rechtsgütern dient, ist bei Eingriffsermächtigungen zu repressiven Zwecken stets zunächst der Nebel des „Meta-Rechtsguts" Funktionsfähigkeit der Strafrechtspflege zu lichten, das sich jeder inhaltlich aussagekräftigen, über apodiktische Aussagen hinausgehenden Abwägung mit anderen grundrechtlichen Positionen entzieht. Vielmehr ist zu fragen, welche Rechtsgüter durch die Strafrechtspflege letztlich konkret geschützt werden sollen. Diese können und müssen sodann in Beziehung gesetzt werden zu denjenigen Rechtsgütern, in die Ermittlungsmaßnahmen eingreifen, die zur Verfolgung einer Straftat durchgeführt 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 gefallen, so dienen die dann nur noch möglichen repressiven Eingriffe primär der Sanktionierung der Verantwortlichen, können – um im Bilde zu bleiben – das Kind aber nicht wieder zum Leben erwecken, da die Rechtsgutsverletzung bereits eingetreten ist. Da, wie gezeigt, die Strafrechtspflege kein Wert an sich ist, sondern dieser sich 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 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 angerufenen Gericht in der Entscheidung von 2008 abschließend 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.

Gemessen insbesondere an diesen Vorgaben ist der **Straftatenkatalog des § 100b Abs. 2 StPO** zu großen Teilen **verfassungsrechtlich nicht tragfähig**:

So überschreitet insbesondere der Katalog von Straftaten (§ 100b Abs. 2 StPO), zu deren Aufklärung eine Online-Durchsuchung nach § 100b Abs. 1 StPO 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 angerufene Gericht selbst eine präventive Online-Durchsuchung **nicht** für zulässig hält. Mit anderen Worten: eine Online-Durchsuchung dürfte in diesen Fällen nicht einmal zur Abwehr einer konkret drohenden Gefahr für dieses Rechtsgut eingesetzt werden. Um es zuzuspitzen: Wenn allein eine präventiv angelegte Online-Durchsuchung die Gefahr abwenden könnte, so müsste der Staat von Verfassungs wegen die drohende Rechtsgutsverletzung – etwa eine Verletzung des Vermögens – gleichwohl geschehen lassen! Nach der Konzeption des Straftatenkataloges aus § 100b StPO indes soll eine Strafverfolgung später, nach Verletzung des bedrohten Rechtsguts, unter Einsatz einer Online-Durchsuchung möglich sein.

Das ist offenkundig nicht folgerichtig: Wenn selbst eine potentiell noch abzuwendende Verletzung eines bestimmten Rechtsguts eine Online-Durchsuchung

nicht rechtfertigen könnte, dann vermag die bloße Verfolgung einer (bereits geschehen oder als geschehen vermuteten) Verletzung desselben Rechtsguts dies umso weniger – schließlich ist „das Kind bereits in den Brunnen gefallen“, die Beeinträchtigung des Rechtsguts also nicht mehr zu verhindern. 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.“
>
> BVerfGE 120, 274 <328>.

Bei den Katalogtaten aus dem StGB, die gemäß § 100b Abs. 2 StPO eine Online-Durchsuchung sollen rechtfertigen können, betrifft dies insbesondere solche, die primär Vermögen oder Eigentum schützen, ebenso Verstöße gegen das Asyl und Aufenthaltsgesetz:

- § 100b Abs. 2 Nr. 1 lit. c StPO (Geld- und Wertzeichenfälschung),
- § 100b Abs. 2 Nr. 1 lit. h StPO- (Bandendiebstahl),
- § 100b Abs. 2 Nr. 1 lit. i und j StPO (bestimmte Formen von Raub oder räuberischer Erpressung, sofern es nicht tateinheitlich zu Körperverletzungen gekommen ist),
- § 100b Abs. 2 Nr. 1 lit. k StPO (Qualifikationen der Hehlerei)
- § 100b Abs. 2 Nr. 1 lit. l StPO(Geldwäsche u. ä.)
- § 100b Abs. 2 Nr. 2 und Nr. 3 (Verstöße gegen Asyl- und Aufenthaltsgesetz)

Eine zum Zwecke der Strafverfolgung der vorgenannten Katalogtaten angeordnete Online-Durchsuchung ist verfassungsrechtlich nicht hinnehmbar. § 100b Abs. 2 StPO ist daher – soweit er sich auf die vorgenannten Straftaten erstreckt – verfassungswidrig.

III. Verletzung der Beschwerdeführer zu 3 bis 5 in ihrem Grundrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG (Schutzpflichtverletzung)

Die Ausgestaltung der Quellen-TKÜ und der Online-Durchsuchung in der StPO verletzt zudem die Beschwerdeführer zu 3 bis 5 in ihrem Grundrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, weil der Bund die genannten Befugnisse nicht mit einem effektiven Schwachstellen-Management verbunden hat, das insbesondere die Verwendung von Sicherheitslücken verhindert, die dem Hersteller des betreffenden Systems noch nicht bekannt sind (sog. Zero-Day-Exploits oder kurz: 0days).

1. Maßstab

a) Das sog. IT-Grundrecht

Die Informationstechnik hatte für die Lebensgestaltung des Einzelnen schon zur Zeit der ersten Entscheidung des Bundesverfassungsgerichts zur Online-Durchsuchung,

> BVerfGE 120, 274 ff.,

eine hohe Relevanz. Mit dieser Bedeutung gehen nach der Rechtsprechung des angerufenen Gerichts „besondere Persönlichkeitsgefährdungen“ und „ein grundrechtlich erhebliches Schutzbedürfnis“ einher.

> BVerfGE 120, 274 <306>.

Für dieses besondere Schutzbedürfnis entwickelte das angerufene Gericht ein besonderes Grundrecht, nämlich das **Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme** (im Folgenden auch: IT-Grundrecht). Der Schutzbereich dieses Grundrechts ist eröffnet,

wenn eine Eingriffsermächtigung Systeme erfasst, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten. Eine solche Möglichkeit besteht etwa beim Zugriff auf Personalcomputer, einerlei ob sie fest installiert oder mobil betrieben werden.

BVerfGE 120, 274 <314>.

Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme schützt zunächst das Interesse des Nutzers, dass die von einem (vom Schutzbereich erfassten) informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich blieben. Ein Eingriff in dieses Grundrecht ist zudem dann anzunehmen, wenn die Integrität des geschützten informationstechnischen Systems angetastet wird, indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden könnten; dann ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen. Das Grundrecht schützt dabei insbesondere vor einem heimlichen Zugriff, durch den die auf dem System vorhandenen Daten ganz oder zu wesentlichen Teilen ausgespäht werden können.

BVerfGE 120, 274 <314>.

b) Staatliche Schutzpflichten

Nach ständiger Rechtsprechung des Bundesverfassungsgerichts enthalten die grundrechtlichen Verbürgungen indes nicht lediglich subjektive Abwehrrechte des Einzelnen gegen die öffentliche Gewalt, sondern sind zugleich objektivrechtliche Wertentscheidungen der Verfassung, die für alle Bereiche der

Rechtsordnung gelten und Richtlinien für Gesetzgebung, Verwaltung und Rechtsprechung geben.

BVerfGE 7, 198 <205>; 35, 79 <114>; 39, 1 <41 f.>; 49, 89 <141 f.>.

Dies wird am deutlichsten in Art. 1 Abs. 1 Satz 2 GG ausgesprochen, wonach es Verpflichtung aller staatlichen Gewalt ist, die Würde des Menschen zu achten und zu schützen. Daraus können sich verfassungsrechtliche Schutzpflichten ergeben, die es gebieten, rechtliche Regelungen so auszugestalten, dass auch die Gefahr von Grundrechtsverletzungen eingedämmt bleibt.

BVerfGE 49, 89 <142>; 92, 26 <46>; 125, 39 <78>.

Ob, wann und mit welchem Inhalt eine solche Ausgestaltung von Verfassungs wegen geboten ist, hängt von der Art, der Nähe und dem Ausmaß möglicher Gefahren, der Art und dem Rang des verfassungsrechtlich geschützten Rechtsguts sowie von den schon vorhandenen Regelungen ab.

BVerfGE 49, 89 <142>.

Im Zusammenhang mit den Gefahren der friedlichen Nutzung der Kernenergie hat das Bundesverfassungsgericht ausgeführt, dass der Gesetzgeber zur Abschätzung künftiger Schäden durch die Errichtung oder den Betrieb einer Anlage oder durch ein technisches Verfahren weitgehend auf Schlüsse aus der Beobachtung vergangener tatsächlicher Geschehnisse auf die relative Häufigkeit des Eintritts und den gleichartigen Verlauf gleichartiger Geschehnisse in der Zukunft angewiesen ist. Fehlt eine hinreichende Erfahrungsgrundlage hierfür, muss er sich auf Schlüsse aus simulierten Verläufen beschränken. Der Gesetzgeber muss allerdings keine Regelungen schaffen, die mit absoluter Sicherheit Grundrechtsgefährdungen ausschließen.

BVerfGE 49, 89 <142>.

Das Bundesverfassungsgericht kann deswegen die Verletzung einer Schutzpflicht nur feststellen, wenn die öffentliche Gewalt Schutzvorkehrungen entweder überhaupt nicht getroffen hat oder die getroffenen Regelungen und Maßnahmen gänzlich ungeeignet oder völlig unzulänglich sind, das gebotene Schutzziel zu erreichen, oder erheblich dahinter zurückbleiben.

> BVerfGE 77, 17 <214 f.>; 88, 203 <251 ff.>; 92, 26 <46>; 125, 39 <78 f.>; 143, 313 <337 f.>.

Das angerufene Gericht hat bereits zu Art. 10 Abs. 1 GG erklärt, dass er nicht nur vor der Kenntnisnahme des Inhalts und der näheren Umstände der Telekommunikation durch den Staat schütze, sondern auch einen Auftrag an den Staat enthalte, Schutz auch insoweit vorzusehen, als private Dritte sich Zugriff auf die Kommunikation verschaffen.

> BVerfGE 106, 28, <37>.

Auch zum Allgemeinen Persönlichkeitsrecht hat das Bundesverfassungsgericht eine Schutzpflicht des Staates anerkannt.

> BVerfGE 63, 131 <142>; 73, 118 <201>; 96, 56 <64>; 100, 271 <284>; vgl. zu Schutzpflichten bzgl. des Allgemeinen Persönlichkeitsrechts auch *Di Fabio*, in: Maunz/Dürig, GG, Stand: 81. EL Sep. 2017, Art. 2 Rn. 135 f. (zur Pflicht zum Schutz der informationellen Selbstbestimmung: Rn. 189).

2. Staatliche Pflicht zum Schutz informationstechnischer Systeme vor Integritäts- und Vertraulichkeitsverletzungen

Dass das Bundesverfassungsgericht auch dem IT-Grundrecht eine objektivrechtliche Dimension zuerkennt, hat das Gericht bereits sprachlich durch den Auftrag zur *Gewährleistung* der Vertraulichkeit und Integrität informationstechnischer Systeme zum Ausdruck gebracht.

Hoffmann-Riem hat dies mit Bezug auf das IT-Grundrecht unmittelbar im Anschluss an die Entscheidung des angerufenen Gerichts wie folgt formuliert:

> „Vom grundrechtlichen Schutz umfasst ist die Abwehr (nicht gerechtfertigter) staatlicher Eingriffe. Es geht aber auch um die Gewährung von Schutz, sei es durch Erfüllung der in Grundrechten enthaltenen subjektiven Schutzansprüche und gegebenenfalls entsprechender Schutzpflichten, sei es in Ausgestaltung der objektiv-rechtlichen Vorgaben der Grundrechte. Schutzdimensionen außerhalb des rein abwehrrechtlichen Schutzes der Grundrechte treten umso eher in das Zentrum grundrechtlicher Garantien, je mehr die realen Voraussetzungen der Freiheitausübung der Bürger einerseits durch den Staat, andererseits aber auch durch Private oder im Zuge von Kooperationsakten zwischen Staat und Privaten geschaffen und erhalten werden müssen, aber gegebenenfalls auch von ihnen in Frage gestellt werden. Deshalb wird immer bedeutsamer, dass das BVerfG schon seit längerem vermehrt auf die objektiv-rechtliche Dimension des Grundrechtsschutzes zurückgegriffen hat. ... Soweit es um die Aktivierung anderer, also auch der objektiv-rechtlichen Grundrechtsfunktionen geht, bedarf es ... regelhaft entsprechender Ausgestaltungen."
>
> JZ 2008, 1009, 1013 f.

Diesen Auftrag erfüllt der Staat, indem er den Einzelnen im Rahmen seiner Möglichkeiten vor Angriffen Dritter auf seine IT-Systeme schützt, nämlich durch eine entsprechende Ausgestaltung der Rechtsordnung.

> Eine objektiv-rechtliche Dimension bzw. staatliche Schutzpflicht bejahen *Sachs/Krings*, JuS 2008, 481 (486); *Kutscha*, NJW 2008, 1042 (1044); *Roßnagel/Schnabel*, NJW 2008, 3534 (3535); *Hoffmann-Riem*, JZ 2008, 1009 (1014 und bei Fn. 44); *Hoffmann-Riem*, JZ 2014, 53); *Becker*, NVwZ 2015, 1335 (1339 f.); *Gersdorf*, in: BeckOK Informations- und Medienrecht, Stand: 1.05.2017, Art. 2 Rn. 29. Für eine ausführliche Herleitung der Schutz- und Förderpflicht zur Gewährleistung der IT-Sicherheit *Heckmann*, in: FS Käfer, 2009, S. 129 (133 ff.).

Diese objektiv-rechtliche Dimension folgt auch aus der enormen Bedeutung, die informationstechnische Systeme in der heutigen Gesellschaft haben. Die Relevanz informationstechnischer Systeme, die das Bundesverfassungsgericht im Jahr 2008 zur Anerkennung einer neuen Ausprägung des Allgemeinen Persönlichkeitsrechts führte, ist in den vergangenen zehn Jahren noch gewachsen – insbesondere durch die nahezu lückenlose Verwendung sog. Smartphones, aber auch durch den noch einmal gestiegenen Verbreitungs- und Vernetzungsgrad der bereits 2008 existierenden IT-Systeme. Informationstechnische Systeme sind dadurch auch zentral geworden für die Wahrnehmung und Ausübung anderer Grundrechte wie der Wissenschafts-, Meinungs-, Presse-, Versammlungs-, Vereinigungs- und Berufsfreiheit.

> Vgl. *Heckmann*, in: FS Käfer, 2009, S. 129 (135), der deshalb von der Sicherheit von IT-Systemen als einer „Querschnittsbedingung für die Grundrechtsausübung“ spricht.

Die Bedeutung der IT-Systeme für den Einzelnen, für die Wirtschaft und die Gesellschaft im Ganzen führt dazu, dass sich der Gehalt des Grundrechts auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme nicht in einem Gebot an den Staat erschöpfen kann, nicht in die IT-Systeme der Bürger einzudringen oder sie auszuspähen oder zu manipulieren (von eng zu regelnden Ausnahmen abgesehen). So wie der Staat die physische Infrastruktur zu sichern hat und den Umgang mit Waffen durch Polizei und Militär oder mit Kernbrennstoffen durch die Betreiber von Atomkraftwerken strengen Regeln unterwirft, so muss er auch für die virtuelle Infrastruktur Schutzvorkehrungen treffen und für den (eigenen) Umgang mit virtuellen Waffen – denn nichts anderes sind (Staats-)Trojaner zur Ausnutzung von Sicherheitslücken in IT-Systemen – überzeugende Regelungen treffen, die tatsächlich geeignet sind, die Lückenhaftigkeit und damit Verletzlichkeit von IT-Systemen zu verringern.

Dabei ist auch zu berücksichtigen, dass die Erweiterung der staatlichen Befugnisse in den virtuellen Raum gerade damit begründet wird, dass ehedem physisch beobachtbare Ereignisse nunmehr gleichsam im Cyberspace stattfinden. Diese Erkenntnis kann aber nicht lediglich eine Befugniserweiterung begründen, um virtuelle Räume besser überwachen zu können, sondern geht Hand in Hand mit zugehörigen staatlichen Pflichten. Es zeichnet den Rechtsstaat aus, dass er neuen, ihm ungestüm oder gar als „rechtsfreie Räume" erscheinenden Strukturen nicht mit ebenso ungezügelten (trojanischen) Pferden, sondern gemessen und umsichtig begegnet. Zu dieser Umsicht gehört auch die Vermeidung von Kollateralschäden durch einen verantwortungsvollen Umgang mit Schwachstellen in IT-Systemen, die den Herstellern noch nicht bekannt sind.

3. Verletzung staatlicher Schutzpflicht durch fehlendes Schwachstellen-Management beim Einsatz von Staatstrojanern

Die Ausnutzung von Sicherheitslücken bzw. von Schwachstellen in IT-Systemen kann gravierende Folgen haben (dazu unter a)). Aus der staatlichen Pflicht zum Schutz der Integrität und Vertraulichkeit informationstechnischer Systeme folgt, dass der Staat zumindest **irgendwelche** mutmaßlich wirksamen Schutzmaßnahmen ergreifen muss (dazu unter b)). Daraus wiederum ergibt sich, dass jedenfalls ein Schwachstellenmanagement einzurichten ist, das die Ausnutzung von Sicherheitslücken verhindert, die dem Hersteller der betroffenen Soft- oder Hardware oder eines Online-Dienstes noch unbekannt sind (dazu unter c)).

a) Arten und Auswirkungen von Sicherheitslücken/Schwachstellen in IT-Systemen

Sicherheitslücken oder Schwachstellen (die Begriffe werden im Folgenden synonym verwendet) sind nach einer Definition der US-amerikanischen nationalen Telekommunikations- und Informationsbehörde „Schwächen einer Software, Hardware oder eines Online-Dienstes, die ausgenutzt werden können, um

die Vertraulichkeit, Integrität oder Verfügbarkeit eines Systems oder die auf ihm gespeicherten Daten zu verletzen."

> Im Original: „Vulnerabilities are weaknesses of software, hardware, or online services that can be used to damage the confidentiality, integrity, or availability of those systems or the data they store."
>
> United States National Telecommunications and Information Administration (NTIA), Vulnerability Disclosure Attitudes and Actions, online abrufbar unter: https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf (zuletzt abgerufen am 30. Juli 2018).

§ 2 Abs. 6 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik („BSIG") definiert Sicherheitslücken als „Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Dritte gegen den Willen des Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen oder die Funktion der informationstechnischen System beeinflussen können."

Innerhalb dieser Definition werden Schwachstellen danach unterschieden, ob sie dem Hersteller bereits bekannt (dann „n-days", im Sinne von: dem Hersteller bereits seit n Tagen bekannt) oder noch unbekannt sind (dann „0-days", sprich: Zero-days oder Oh-days, dem Hersteller Null Tage bekannt).

Aus der Perspektive der IT-Sicherheit von Systemen, die mit der fehlerhaften Software arbeiten, unterscheiden sich n-days und 0-days fundamental:

Für 0-days stehen in aller Regel noch keine technischen Lösungen – sogenannte „fixes" oder „patches" – bereit, abgesehen von dem seltenen Fall, dass der Hersteller die Software auch in Unkenntnis der Sicherheitslücke zufällig so ändert, dass die Lücke gleichsam „nebenbei" geschlossen wird.

Für n-days hingegen können seitens des Herstellers des betroffenen Systems grundsätzlich bereits Gegenmittel entwickelt worden sein. Gleichwohl zeigt sich auch hier ein sehr diverses Bild: Die Software mancher IT-Systeme lässt sich gar nicht updaten, dies ist etwa im Bereich internetfähiger Kleingeräte wie Webcams oder WLAN-Router verbreitet. Hier konvergieren also 0-days und n-days in ihren praktischen Auswirkungen; allein eine Information aller Nutzer und eine Abkoppelung der Geräte vom Internet können hier Angriffe vereiteln. Für andere Systeme – etwa Smartphones, Laptops und Desktop-Computer – gibt es zwar prinzipiell die Möglichkeit, sowohl das Betriebssystem als auch die installierte Anwendungssoftware zu aktualisieren. Diese Möglichkeit nutzen aber sowohl die Hersteller als auch die Nutzerinnen und Nutzer der Systeme in sehr unterschiedlicher Weise: Seitens der Hersteller werden insbesondere ältere Systeme oft nicht mehr mit Updates versorgt. „Ältere" ist hier allerdings ein sehr relativer Begriff – während beispielsweise iPhones noch einige Jahre nach dem Verkaufsschluss mit Updates des Betriebssystems iOS versorgt werden, endet die Update-Versorgung bei Android-Smartphones teilweise bereits mit dem Ende des Vertriebs eines Modells oder jedenfalls wenige Monate danach. Selbst wenn für ein bestimmtes Gerät oder eine Anwendungssoftware ein Update verfügbar ist, ist aber keineswegs gewährleistet, dass es auch jedes betroffene System (rechtzeitig) erreicht: Teilweise arbeiten Nutzerinnen und Nutzer jahrelang mit veralteten Versionen von Betriebssystem und Anwendungen, weil sie sich über Updates und Sicherheitslücken keine Gedanken machen oder sich von der Komplexität eines Update-Vorgangs überfordert fühlen.

Sicherheitslücken stellen dabei in alltäglichen IT-Systemen keine Ausnahme, sondern den Normalfall dar. Das Bundesamt für Sicherheit in der Informationstechnik („BSI") geht davon aus, dass

> „bei jedem hinreichend komplexen Softwareprodukt von der Existenz kritischer Schwachstellen auszugehen ist. (…) Da nur ein Teil der gefundenen Fehler beseitigt oder veröffentlicht wird, ist eine Gefährdung durch nicht öffentlich bekannte Schwachstellen, für die es noch keine Sicherheits-Updates gibt, immer latent vorhanden. Daher sollte davon

ausgegangen werden, dass die eingesetzte Software immer Schwachstellen enthält, die auch ausgenutzt werden (…)."

BSI, Die Lage der IT-Sicherheit in Deutschland 2017, online abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?__blob=publicationFile&v=4 (zuletzt abgerufen am 31. Juli 2018), S. 18.

Geraten n-days, für die noch keine technischen Lösungen bestehen oder verbreitet wurden, oder 0-days in die falschen Hände, kann das gravierende Folgen haben. Die Entwicklung von Schadsoftware dauert im Median 22 Tage.

RAND Corporation, Zero Days, Thousands of Nights , online abrufbar unter https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1751/RAND_RR1751.pdf (zuletzt abgerufen am 31. Juli 2018), S. 57.

Werden die IT-Systeme von Infrastruktureinrichtungen oder Krankenhäusern geschädigt, sind auch Tote nicht ausgeschlossen. Das ist kein weitgehend hypothetisches Szenario, das als Restrisiko der sicherheitsbehördlichen Aufklärung außer Acht gelassen werden könnte. Solche Folgen von Angriffen auf IT-Systeme liegen vielmehr ausgesprochen nahe und sind teilweise bereits eingetreten. So hat erst im Mai 2017 das Schadprogramm „WannaCry" weltweit Schäden verursacht, indem es die IT-Systeme von Behörden und Unternehmen, insbesondere auch von britischen Krankenhäusern lahmlegte und nur gegen Lösegeldzahlung wieder freigab.

Vgl. etwa https://www.zeit.de/digital/internet/2017-05/wannacry-microsoft-nsa-hackerangriff-usa-regierung (zuletzt abgerufen am 31. Juli 2018) sowie bereits oben A.

„WannaCry" ist kein Einzelfall. Das BSI hat in seinem Lagebericht eine ganze Reihe an Fällen dargestellt, darunter einen, bei dem durch Ausnutzung einer

Sicherheitslücke in der E-Commerce-Software *Magento* die Zahlungsinformationen der Kunden von mindestens 1.000 deutschen Online-Shops an die Täter weitergleitet wurden.

> BSI, Die Lage der IT-Sicherheit in Deutschland 2017, online abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?__blob=publicationFile&v=4 (zuletzt abgerufen am 31. Juli 2018), S. 20.

Andere Unternehmen werden Opfer von Wirtschaftsspionage oder fremden Regierungen, häufig ohne ihr Wissen. Viele Angriffe unter Ausnutzung von Sicherheitslücken werden nicht öffentlich bekannt, weil Unternehmen nicht mit mangelnder IT-Sicherheit in Verbindung gebracht werden möchten. Aus diesem Grunde kommt zu den ohnehin hohen Fallzahlen eine hohe Dunkelziffer hinzu. Das Versicherungsunternehmen Lloyd‘s schätzt, dass künftige massenweise Angriffe auf IT-Systeme Schäden von bis zu 53 Mrd. US-Dollar verursachen könnten.

> Lloyd’s-Bericht vom 17. Juli 2017, online abrufbar unter: https://www.lloyds.com/news-and-risk-insight/press-releases/2017/07/cyber-attack-report (zuletzt abgerufen am 5. August 2018).

b) Staatliche Schutzpflicht aus dem IT-Grundrecht in Bezug auf Sicherheitslücken

Vor diesem Hintergrund ist der Staat nicht gehalten, die Beschwerdeführer zu 3 bis 5 und andere Personen im Geltungsbereich des Grundgesetzes vor jeder Beeinträchtigung ihrer IT-Systeme zu schützen: Vom Staat ist nichts objektiv Unmögliches zu verlangen. Er muss auch nicht schlechterdings alles in seiner Macht Stehende zu ihrem Schutz unternehmen, etwa indem er Gegenmaßnahmen für alle ihm bekannten Gefahren selbst entwickelt und bereitstellt oder gar ihm noch unbekannte Gefahren selbst ermittelt und so Sicherheitslücken anstelle der Anbieter der betroffenen IT-Systeme schließt. Denn das brächte ihn

schnell an technische, regulatorische und fiskalische – und scheiterte letztlich auch am Fehlen virtueller – Grenzen.

Das bedeutet aber nicht, dass der Staat im Angesicht von Gefahren für die IT-Systeme der Beschwerdeführer zu 3 bis 5 sowie anderer Personen im Geltungsbereich des Grundgesetzes untätig bleiben oder gar seinerseits die IT-Sicherheitslage weiter verschärfen darf. Denn die aus dem IT-Grundrecht abgeleitete staatliche Schutzpflicht für die Integrität informationstechnischer Systeme (vgl. dazu oben) erfordert jedenfalls, dass der Staat sich dieser Herausforderung erkennbar annimmt und in einer Weise tätig wird, die aus der Perspektive der IT-Sicherheit noch als sachdienlich und hinreichend wirksam angesehen werden kann. In der Terminologie des allgemeinen Verwaltungsrechts formuliert: Das Ermessen des Staates hinsichtlich der Frage des Ob eines Tätigwerdens zugunsten der IT-Sicherheit ist angesichts der dramatischen Bedrohung durch IT-Sicherheitslücken auf Null reduziert. Ein Tätigwerden des Staates, das der IT-Sicherheit zuwiderläuft, ist demnach schlechthin nicht mit der aus dem IT-Grundrecht resultierenden staatlichen Schutzpflicht vereinbar; ein positives Tätigwerden ist daran zu messen, ob die (traditionell weit verstandenen) legislatorischen Spielräume eingehalten worden sind.

Fraglich kann demnach nur sein, welchen Mindestumfang staatliche Maßnahmen zur Gewährleistung der IT-Sicherheit haben müssen. Um diesen **Mindest**umfang zu bestimmen, sind zunächst alle **möglichen** Maßnahmen zum Schutz von IT-Systemen vor Gefahren durch Sicherheitslücken zu betrachten. Sie lassen sich in folgender Matrix darstellen:

Staatliche …	… Gegenmaßnahmen	… Befähigung Dritter zu Gegenmaßnahmen
… Ermittlung von Sicherheitslücken	*hoher staatlicher Einsatz*	*mittlerer staatlicher Einsatz*
… Kenntniserlangung von Sicherheitslücken	*mittlerer staatlicher Einsatz*	*geringer staatlicher Einsatz*

Matrix des staatlichen Umgangs mit Sicherheitslücken in IT-Systemen

Der Staat kann also einerseits entscheiden, ob er Sicherheitslücken selbst aktiv ermittelt oder ob er nur Kenntnis von ihnen erlangt. Er kann andererseits entscheiden, ob er nach Ermittlung oder Kenntniserlangung selbst Gegenmaßnahmen einleitet oder ob er lediglich Dritte zu Gegenmaßnahmen befähigt.

Zu diesen beiden Dimensionen kommt eine dritte hinzu, nämlich das **Wann** der Maßnahmen zur Schließung einer Sicherheitslücke. Dass der Staat **nie** Maßnahmen ergreift, ist – wie bereits dargestellt – bei grundsätzlicher Anerkennung einer staatlichen Schutzpflicht keine Option.

Auf der Grundlage dieser Matrix der staatlichen Reaktionsmöglichkeiten wird deutlich, dass die geringste Anforderung an staatliches Tätigwerden angesichts von IT-Sicherheitsbedrohungen darin besteht, sie Dritten – typischerweise dem Hersteller – zu melden und so auf Abhilfe zu drängen. Ein Weniger an staatlichem Schutz vor den Gefahren von Sicherheitslücken ist kaum denkbar: nämlich die aktive Befähigung Dritter zu Gegenmaßnahmen, nachdem der Staat Kenntnis von Sicherheitslücken erlangt hat, sowie eine nachvollziehbare Entscheidung über den Zeitpunkt staatlichen Tätigwerdens. Zur Befähigung Dritter zu Gegenmaßnahmen gehört auch, dass der Staat bis zum Wirksamwerden der Gegenmaßnahmen nicht selbst die Gefahr eines Schadens erhöht, indem er etwa die Informationen über Sicherheitslücken nicht so gut wie möglich schützt.

c) Mindestanforderungen an ein staatliches Schwachstellen-Management beim Einsatz von Staatstrojanern

Um Staatstrojaner einzusetzen, müssen Ermittlungsbehörden Sicherheitslücken kaufen; derzeit verfügen sie noch nicht über die Fähigkeiten, selbst Sicherheitslücken aufzudecken. Das bestätigte der Präsident der Zentralen Stelle für Informationstechnik im Sicherheitsbereich („ZITiS“), eine Einrichtung, die die Ermittlungs- und andere Behörden bei der Identifikation und Ausnutzung von Schwachstellen unterstützt.

> Heise im Februar 2018, online abrufbar unter: https://www.heise.de/newsticker/meldung/Schlagabtausch-zu-ZITiS-IT-Sicherheitsluecken-schliessen-oder-ausnutzen-3976587.html (zuletzt abgerufen am 3. August 2018).

Die Bundesregierung schließt auch explizit nicht aus, 0-days – also Schwachstellen, die dem Hersteller noch unbekannt sind –, für Quellen-TKÜ und Online-Durchsuchung einzusetzen:

> „Ob und inwieweit im Spannungsfeld technischer Erfordernisse, rechtlicher Vorgaben, sicherheits- und rechtspolitischer Erwägungen sowie taktischer Einsatzrahmenbedingungen zukünftig eine Nutzung sog. ‚Zero-Day-Exploits' für die Durchführung von Maßnahmen der Quellen-TKÜ und Online-Durchsuchung durch Sicherheitsbehörden in Betracht kommt, ist durch die zuständigen Stellen der Bundesregierung in Abstimmung mit den zu beteiligenden nationalen und ggf. internationalen Stellen und Gremien zu prüfen."
>
> Antwort der Bundesregierung auf Fragen 26 bis 31 einer Kleinen Anfrage, BT-Drs. 18/13413; Antworten auf diese Fragen sind eingestuft, aber online zugänglich unter https://netzpolitik.org/2018/geheime-dokumente-das-bundeskriminalamt-kann-jetzt-drei-staatstrojaner-einsetzen/#Antwort-Drucksache-18-13566-NfD (zuletzt abgerufen am 3. August 2018).

Wenn der Gesetzgeber den Einsatz sog. Staatstrojaner zur Quellen-TKÜ und Online-Durchsuchung für erforderlich hält, also regelmäßig Kenntnis von Sicherheitslücken in IT-Systemen erlangt bzw. sich diese Kenntnis sogar aktiv verschafft, so hat er zwingend zu gewährleisten, dass die betroffenen Systemhersteller den Behörden bekanntwerdende Sicherheitslücken schnellstmöglich beseitigen können. Denn das Zurückhalten von Sicherheitslücken, die den Herstellern der betreffenden Systeme noch nicht bekannt sind, ist bei Gegenüberstellung der betroffenen Rechtsgüter schlechthin unzulässig:

Für das Zurückhalten von Sicherheitslücken könnte das Strafverfolgungsinteresse der Allgemeinheit sprechen, also das Interesse, durch Ausnutzung der unbekannten Sicherheitslücke Maßnahmen gem. §§ 100a Abs. 1 Satz 2 und 3, 100b StPO durchführen zu können, die sodann möglicherweise zur Aufklärung eines Tatverdachts etwas beitragen können. Indes spricht nichts dafür, dass es für die Infiltration des intendierten Zielsystems gerade einen 0-day, also eine auch dem Hersteller noch unbekannte Sicherheitslücke braucht. Wie oben im Einzelnen ausgeführt wurde, lassen sich in den meisten Fällen auch den Herstellern bekannte Lücken ausnutzen – etwa weil der Hersteller für das konkrete Zielsystem noch kein Update bereitgestellt oder die Zielperson dieses nicht eingespielt hat. Aus der Perspektive der Strafverfolgung bedeutet also die Nutzung von 0-days allenfalls einen gewissen Komfort-Gewinn, weil dies die Suche nach einem Infiltrationsvektor gelegentlich verkürzen mag.

Aus der Perspektive der IT-Sicherheit der Allgemeinheit indes ist der Unterschied zwischen der Erlaubnis zur Nutzung von 0-days und n-days fundamental: Während ersteres die oben im Detail hergeleiteten fatalen Anreize schafft, 0-days geheimzuhalten, ist die Nutzung von n-days aus der Perspektive der IT-Sicherheit der Allgemeinheit unproblematisch: Die Lücke ist dem Hersteller ja bereits bekannt, also besteht kein Anlass mehr zu einer Mitteilung ihm gegenüber, und ob andere IT-Systeme mit einem Update versorgt werden liegt nunmehr allein in der Sphäre des Herstellers sowie der Nutzerinnen und Nutzer.

Vor diesem Hintergrund – geringe Vorteile des 0-day-Einsatzes, aber erhebliche Beeinträchtigung der IT-Sicherheit bis hin zur Gefährdung von Leib und Leben (etwa von Krankenhauspatienten, wenn lebenswichtige IT-Systeme gehackt werden), weil eine Stelle des Bundes eine Sicherheitslücke geheim gehalten hat – ist eine Rechtslage, die den Einsatz von 0-days erlaubt, schlechthin unvereinbar mit der aus dem IT-Grundrecht resultierenden staatlichen Schutzpflicht.

Selbst wenn man diesen zwingenden Schluss nicht ziehen wollte, so müsste der Gesetzgeber mindestens ein – angesichts der Grundrechtsrelevanz jedenfalls in seinen Grundzügen und in seiner Ausrichtung auf die Förderung der IT-Sicherheit der Allgemeinheit zwingend durch formelles Gesetz einzuführendes – Verwaltungsverfahren vorsehen, mit dem eine hiermit zu betrauende Behörde ihr bekannt werdende Sicherheitslücken auf ihre Bedeutung hin untersuchen und einzustufen hat, um auf dieser Grundlage über den Umgang mit der Sicherheitslücke zu entscheiden. Verfassungswidrig erscheint jedenfalls der derzeitige Rechtszustand, in dem nicht näher bestimmte Stellen des Bundes und der Länder ohne irgendeine gesetzliche Grundlage nach Gutdünken entscheiden, wie sie mit Sicherheitslücken verfahren und welche sie ggf. für hoheitliche Eingriffe verwenden wollen.

Damit die Entscheidung über den Mitteilungszeitpunkt nachvollziehbar ist, muss sie zunächst zwingend in einem gesetzlich geregelten Verwaltungsverfahren getroffen werden, in dem auch die Interessen der Allgemeinheit an größtmöglicher IT-Sicherheit mit entscheidender Stimme vertreten sind.

Materiell könnten der Bedeutung der Lücke für einen potentiellen späteren Einsatz als „Staatstrojaner“ beispielsweise folgende Punkte gegenübergestellt werden:

- Verbreitung der Sicherheitslücke,
    - quantitativ: Zahl der betroffenen Nutzer
    - qualitativ: Art der betroffenen Nutzer
- Gewicht der Sicherheitslücke,
    - zur Ausnutzung erforderlicher Aufwand
    - aus Ausnutzung resultierender Schaden
- Wahrscheinlichkeit, dass der Betroffene die Ausnutzung der Lücke bemerkt und im Einzelfall Gegenmaßnahmen einleitet,
- Wahrscheinlichkeit einer technischen Lösung für die Lücke,

- Wahrscheinlichkeit einer Verbreitung der technischen Lösung,
- Möglichkeiten zur Linderung der Folgen bei (zeitweiser) Geheimhaltung der Lücke,
- Wahrscheinlichkeit, dass Dritte die Lücke finden.

Außerdem muss der Staat Vorkehrungen dagegen treffen, dass seine Kenntnis von Sicherheitslücken bzw. seine Mittel zu ihrer Ausnutzung von Dritten erbeutet werden. Es ist derzeit nicht erkennbar, dass deutsche Ermittlungsbehörden die bei ihnen vorhandenen Informationen oder Einsatzmittel bedeutend besser schützen können als die US-amerikanische National Security Agency im Falle „WannaCry“. Ein Schwachstellen-Management muss aber erst recht gewährleisten, dass aus dem staatlichen Horten von Sicherheitslücken und den Mitteln zu ihrer Ausnutzung keine **zusätzliche** Gefahr für die öffentliche IT-Sicherheit entsteht.

d) Bisherige Gesetze des Bundes erfüllen nicht Mindestanforderungen an Schwachstellen-Management

Bislang gibt es keinen Prozess zur Bewertung von Schwachstellen, die die Ermittlungsbehörden zu Quellen-TKÜ und Online-Durchsuchung nutzen wollen, sowie keine Verfahren und Kriterien, nach denen über eine Meldung der Schwachstelle an die Hersteller entschieden werden kann.

> Vgl. Bericht von einer Veranstaltung im Februar 2018 mit dem ZITiS-Präsidenten, online unter: https://www.heise.de/newsticker/meldung/Schlagabtausch-zu-ZITiS-IT-Sicherheitsluecken-schliessen-oder-ausnutzen-3976587.html (zuletzt abgerufen am 3. August 2018).

Insbesondere stützt sich die Einrichtung „ZITiS“ – die als „Bundes-Hacking-Behörde“ möglicherweise naheliegende Stelle für die Bewertung von Sicher-

heitslücken wäre – nicht auf ein formelles Bundesgesetz, sodass bereits aus diesem Grunde die ZITiS die Anforderungen an den Bund zur Kompensation der durch §§ 100a Abs. 1 Satz 2, 100b StPO geschaffenen Fehlanreize und zum Schutz der IT-Sicherheit nicht erfüllt.

Aber auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) erfüllt die Vorgaben des Grundgesetzes für den Bund insoweit nicht, denn das BSIG enthält keine Regelungen, die wenigstens die Mindestanforderungen an ein effektives Schwachstellen-Management erfüllen würden.

Zu den Aufgaben des BSI zählt laut § 13 Nr. 14 BSIG u.a. die Warnung der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik. Dazu ermöglicht § 7 Abs. 1 Satz 1 Nr. 2 lit. a BSIG Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten gegenüber der Öffentlichkeit oder an die betroffenen Kreise sowie eine Vorabwarnung an die Hersteller betroffener Produkte (§ 7 Abs. 1 Satz 3 BSIG). Kenntnis von Sicherheitslücken soll das BSI bspw. dadurch erlangen, dass nach § 4 Abs. 3 i.V.m. Abs. 2 Nr. 1 BSIG u.a. Informationen zu Sicherheitslücken, die einer Bundesbehörde bekannt werden, an das BSI weiterzugeben sind, wenn diese Informationen für die Erfüllung der Aufgaben oder die Sicherheit der Informationstechnik anderer Behörden von Bedeutung sind, soweit andere Vorschriften dem nicht entgegenstehen.

Dies gewährleistet nicht hinreichend, dass Sicherheitslücken, die die Ermittlungs- oder ihnen zuarbeitende Behörden im Vorfeld der Ausübung der Befugnisse nach §§ 100a Abs. 1 Satz 2, 100b StPO erkennen, tatsächlich an das BSI gemeldet werden; auch ist nicht gewährleistet, dass das BSI im Falle einer Meldung von Sicherheitslücken die staatliche Schutzpflicht gegenüber den Nutzern von IT-Systemen hinreichend erfüllt.

Einem effektiven Schwachstellen-Management steht zunächst entgegen, dass die Meldepflicht nach § 4 Abs. 3 i.V.m. Abs. 2 Nr. 1 BSIG nur für Bundesbehörden gilt. Von den Befugnissen nach §§ 100a Abs. 1 Satz 2, 100b StPO können aber insbesondere auch Landesbehörden Gebrauch machen.

Weiter sind gemäß § 4 Abs. 4 BSIG von der Unterrichtungspflicht nach § 4 Abs. 3 BSIG u.a. Informationen ausgenommen, die aufgrund von Regelungen zum Geheimschutz,

> nach dem BVerfSchG, dem MADG und dem BNDG, vgl. *Buchberger*, in: Sicherheitsrecht des Bundes, 2014, § 4 BSIG Rn. 3, sowie die Gesetzesbegründung, BT-Drs. 16/11967, S. 13,

oder Vereinbarungen mit Dritten nicht weitergegeben werden dürfen. Damit ist nicht gewährleistet, dass das BSI jede Schwachstelle überprüft, weil davon auszugehen ist, dass die Behörden beim Kauf von Sicherheitslücken Vertraulichkeitsvereinbarungen mit den Verkäufern schließen müssen, wodurch es zu einem Ausschluss nach § 4 Abs. 4 BSIG käme.

Selbst wenn aber weder Regelungen zum Geheimschutz noch eine Vertraulichkeitsvereinbarung eine Sicherheitslücke erfassen, muss diese Lücke auch für die Erfüllung von Aufgaben oder die Sicherheit der Informationstechnik anderer Behörden von Bedeutung sein (§ 4 Abs. 3 BSIG). Diese Einschätzung nimmt die potentiell berichtspflichtige Behörde selbst vor; das BSIG kennt kein Verfahren, das gewährleistet, dass diese Einschätzung korrekt ist.

Weiter ist auch nach Mitteilung einer Sicherheitslücke an das BSI nicht sichergestellt, dass sie ordnungsgemäß bewertet und an den Hersteller gemeldet wird. Insbesondere stellt § 5 der Allgemeinen Verwaltungsvorschrift über das Meldeverfahren gemäß § 4 Abs. 6 BSIG keine Kriterien auf, nach denen eine Sicherheitslücke zu bewerten ist. Auch hat das BSI nach § 7 Abs. 1 Satz 1, Nr. 1 lit. a, Satz 3 BSIG einen Ermessensspielraum, ob es eine Warnung ausspricht.

Schließlich ist zu bedenken, dass der Gesetzgeber ausweislich der Gesetzesbegründung zu den hier angegriffenen Vorschriften offensichtlich nicht berücksichtigte, dass die §§ 100a Abs. 1 Satz 2, 100b StPO wegen der dazu erforderlichen Ausnutzung von Sicherheitslücken mit der Meldepflicht der (Bundes-) Behörden nach § 4 Abs. 3 BSIG in Konflikt steht. Es ist deshalb zumindest unklar, ob nicht wegen des Grundsatzes *lex posterior derogat legi priori* die §§ 100a Abs. 1 Satz 2, 100b StPO die Meldepflicht nach § 4 Abs. 3 BSIG ohnehin ausschließen. Denn es ist wahrscheinlich, dass der Gesetzgeber – indem er nicht zugleich ein differenziertes Schwachstellen-Management geschaffen hat – annahm, die Ermittlungsbehörden müssten Sicherheitslücken nicht unmittelbar an das BSI melden, auch wenn gerade dies verfassungsrechtlich erforderlich gewesen wäre.

4. Verletzung subjektiver Rechte der Beschwerdeführer zu 3 bis 5

Die Beschwerdeführer zu 3 bis 5 sind – wie vorgetragen – nahezu täglich Versuchen ausgesetzt, ihre Systeme zu „hacken“. Es liegt nahe, dass dabei seitens ausländischer Stellen – etwa türkischer oder russischer Geheimdienste – auch solche Sicherheitslücken zum Einsatz kommen, die Stellen des Bundes unter Verletzung ihrer Schutzpflicht geheimhalten. Näherer Vortrag hierzu ist den Beschwerdeführern naturgemäß nicht möglich, weil sie keine Kenntnis der konkreten geheim gehaltenen Sicherheitslücken haben.

E. Anträge

Die Beschwerdeführer beantragen zu entscheiden:

1. § 100a Abs. 1 Satz 2 der Strafprozessordnung in der Fassung des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017 (BGBl. I S. 3202) ist mit Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG unvereinbar und nichtig.

2. Aus § 100b Abs. 2 Strafprozessordnung in der Fassung des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017 (BGBl. I S. 3202) sind mit Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG unvereinbar und nichtig

- Nr. 1 lit. c,
- Nr. 1 lit. h,
- Nr. 1 lit. k,
- Nr. 1 lit. l,
- Nr. 1 lit. m,
- Nr. 2,
- Nr. 3 lit. a,
- Nr. 5,
- Nr. 7.

3. § 100a Abs. 1 Satz 2 sowie § 100b Abs. 1 StPO sind mit Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG unvereinbar, soweit sie es erlauben, zur

Durchführung von Eingriffen in informationstechnische Systeme mit technischen Mitteln auch Schwachstellen dieser Systeme auszunutzen, die den jeweiligen Herstellern noch nicht bekannt sind (sog. *0-days*).

4. Dem Bundesgesetzgeber wird aufgegeben, bis zum [...] durch Bundesgesetz zu regeln, welche technischen Mittel zur Durchführung von Eingriffen in informationstechnische Systeme gemäß § 100a Abs. 1 Satz 2 sowie § 100b Abs. 1 der Strafprozessordnung sowie ähnlicher Maßnahmen auf der Grundlage anderer Bundesgesetze genutzt werden dürfen.

Dr. iur. h.c. Gerhard Strate
Rechtsanwalt