Meinhard Starostik · Rechtsanwalt

RECHTSANWALTSKANZLEI
Wittestr. 30E · D- 13509 Berlin
+49 30 8800030 · Fax: +49 30 88000310
kanzlei@starostik.de
USt-ID-Nr.: DE165877648

KANZLEI VEREIDIGTER BUCHPRÜFER
Schwarzenberger Str. 7 · D-08280 Aue
+49 3771 564700 · Fax: +49 3771 5647025

Commerzbank AG
Konto: 3 855 855 00 · BLZ: 430 400 36
IBAN: DE57 4304 0036 0385 5855 00
BIC: COBADEFFXXX

Kanzlei Starostik Berlin

RA Starostik · Wittestr. 30 E · D-13509 Berlin

Bundesverfassungsgericht
Postfach 1771
76006 Karlsruhe

Mein Zeichen: 400/2017

Berlin, den 19. Apr. 2018

Verfassungsbeschwerde

des TeleTrusT - Bundesverband IT-Sicherheit e.V.
ges. vertreten durch den Geschäftsführer Dr. Holger Mühlbauer
Chausseestraße 17, 10115 Berlin

Beschwerdeführer zu 1

Prof. Dr.Norbert Pohlmann, bonhoefferstr. 40a, 52078 Aachen

Beschwerdeführer zu 2

Dr. Holger Mühlbauer, Chausseestraße 17, 10115 Berlin

Beschwerdeführer zu 3

Rechtsanwaltes Karsten U. Bartels LL.M.
HK2 Rechtsanwälte, Hausvogteiplatz 11 A,10117 Berlin

Beschwerdeführer zu 4

Prozessbevollmächtigte:

Rechtsanwalt Meinhard Starostik, Wittestr. 30E, 13509 Berlin

Rechtsanwalt Benjamin Derin, Braunschweiger Str. 31, 12055 Berlin

Zustellungen und Nachrichten nur an RA Starostik erbeten!

Wegen: „Staatstrojaner“

§§ 100a Abs. 1 S. 2 und 3, 100b Abs. 1 StPO in der Fassung nach dem Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017, das am 23. August 2017 verkündet wurde (Bundesgesetzblatt I, Seite 3202 ff.).

Verletzte Grundrechte:

Art. 1 Abs. 1, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1, Art. 10 Abs. 1 und Art. 19 Abs. 4 GG

sowie Art. 7 und 8 der Charta der Grundrechte der Europäischen Union.

Anträge:

Namens und in Vollmacht der Beschwerdeführer und unter Beifügung entsprechender Voll-machten der Beschwerdeführer zu 1 bis 3, die Vollmacht des Beschwerdeführers zu 4 nachzureichen versprechend, erheben wir die Verfassungsbeschwerde und beantragen,

1. die §§ 100a Abs. 1 S. 2 und 3, Abs. 5 und 6, 100b Abs. 1 und 100d Abs. 5 Strafprozessordnung in der Fassung nach dem Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017, das am 23. August 2017 verkündet wurde (Bundesgesetzblatt I, Seite 3202 ff.), für mit dem Grundgesetz unvereinbar und nichtig zu erklären,

2. dem Europäischen Gerichtshof die Frage vorzulegen, ob die zu 1. benannten angefochtenen Vorschriften mit Art. 7 und 8 der Charta der Grundrechte der Europäischen Union vereinbar sind,

Gliederung

A. Sachverhalt und Situation der Beschwerdeführer

I. Sachverhalt

1. Technischer Hintergrund

Die Online-Durchsuchung und die sog. Quellen-TKÜ bezeichnen Maßnahmen, die einen externen und vom Betroffenen grundsätzlich unbemerkten Zugriff auf informationstechnische Systeme ermöglichen, um diese zu durchsuchen, zu überwachen bzw. über sie abgewickelte Kommunikation unter Umgehung etwaiger eingesetzter Verschlüsselungsmechanismen zu verfolgen. Dies erfolgt mittels bestimmter Anwendungen, die nach ihrer Installation auf einem System dessen unbemerkte Steuerung und Auslesung erlauben. Solche Anwendungen sind unabhängig von ihrer rechtlichen Reichweite grundsätzlich dazu in der Lage, das gesamte informationstechnische System zu kontrollieren und etwa die Eingaben über die Tastatur aufzuzeichnen, Dateien zu verändern, die Bildschirmansicht mitzuverfolgen oder Mikrofone und Kameras des Geräts zu bedienen.

Da informationstechnische Systeme mit vielfältigen Schutzvorkehrungen gegen einen solchen vom Nutzer nicht gestatteten Zugriff ausgestattet sind, muss zunächst ein Weg gefunden werden, diese Schutzvorkehrungen zu neutralisieren und dem Zugriffsprogramm gewissermaßen die Tür zu öffnen. Essentiell hierfür sind bestehende Schwachstellen auf dem Zielsystem. Aufgrund der vielfältigen, oft hochkomplexen Anwendungen, die von informationstechnischen Systemen genutzt werden, entstehen regelmäßig Sicherheitslücken. Diese Lücken ermöglichen teilweise und bei entsprechender Ausnutzung einen unbefugten externen Zugriff auf das System. Sie können nicht nur von Ermittlungsbehörden, sondern von jedermann zu beliebigen, auch bösartigen Zwecken genutzt werden, denn sie existieren unabhängig von ihrer spezifischen Nutzung. Sie bilden damit ein erhebliches Risiko für alle Nutzer der Software (im Falle von Betriebssystemen oder weit verbreiteter Programme regelmäßig viele Millionen Menschen), weshalb Hersteller darum bemüht sind, jegliche Sicherheitslücken möglichst rasch zu schließen. Behörden, die eine Online-Durchsuchung oder Quellen-TKÜ durchführen wollen, müssen sich auf die Suche nach entsprechenden Lücken begeben oder hierüber von anderen Behörden in Kenntnis gesetzt werden.

Die Gefahr der Ausnutzung durch Dritte wächst dabei sowohl mit dem Zeitraum des Bestehens der Schwachstelle als auch mit der Häufigkeit ihrer behördlichen Nutzung. Je länger eine Sicherheitslücke nicht geschlossen wird, umso höher ist die Wahrscheinlichkeit ihrer Entdeckung durch Ausnutzungswillige, die letztlich auf demselben Wege nach ihr suchen wie damit betraute Behörden. Zudem lässt sich eine Schwachstelle, sobald sie genutzt wird, durch Dritte – etwa mittels forensischer Analyse – ermitteln und selbst ausnutzen.[1] Staatliche Behörden riskieren also bei jeder Anwendung, zum Hinweisgeber für kriminelle oder fremdstaatliche Akteure zu werden. Wird eine erkannte

[1] Neumann / Kurz / Rieger: Sachverständigenauskunft zum Änderungsantrag der Fraktionen CDU/CSU und SPD zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze (2017), S. 7.

Sicherheitslücke nicht geschlossen, vergrößert sich das von ihr ausgehende Missbrauchspotential folglich stetig. Da die Ermittler zur Anwendung der hier gegenständlichen Maßnahmen aber auf Schwachstellen angewiesen sind, entsteht ein Interesse staatlicher Stellen am Offenhalten von Sicherheitslücken.

Bei Betrachtung der praktischen Voraussetzungen eines staatlichen Trojanereinsatzes stellt sich die Lage sogar weitaus gravierender dar. Zur Gewährleistung effektiven Zugriffs auf verschiedene Systeme reicht es nicht aus, lediglich eine einzelne Schwachstelle zu nutzen. Prominente Angriffsprogramme vereinten im Jahr 2015 durchschnittlich zwölf verschiedene Schwachstellen, um auch nur im Bereich der Desktop-Systeme einigermaßen übergreifend anwendbar zu bleiben.[2] Dies liegt begründet in der Vielfalt der Kombinationsmöglichkeiten verschiedener Betriebssysteme und Anwendungen auf einem jeden Zielsystem, das nur durch die richtige Kombination anzuzapfender Schwachstellen angreifbar wird: Der Zugriff auf ein mit einer bestimmten Version des Android-Betriebssystems ausgestattetes Smartphone erfordert eine völlig andere Zusammenstellung von Schwachstellen als ein mit Linux betriebener Desktop-PC oder ein Windows-Tablet, womit sich die Anzahl benötigter Schwachstellen vervielfacht. Angesichts der rasanten Entwicklung und zunehmenden Fragmentierung des Marktes durch immer neue Systeme (etwa mobile Endgeräte) und Anwendungen ist davon auszugehen, dass die Anzahl der von Sicherheitsbehörden jährlich benötigten Schwachstellen deren Kapazität des autarken Auffindens solcher Schwachstellen bei weitem übersteigen wird.[3] Es ist deshalb mit einem staatlichen Erwerb entsprechender Informationen auf dem freien Markt zu rechnen. Dies gilt erst recht, wenn man bedenkt, dass sich potentielle Zielpersonen von Ermittlungsmaßnahmen durch die simple Nichtnutzung von Anwendungen mit bekannten Sicherheitslücken effektiv schützen können, weshalb es für die Behörden darauf ankommt, Lücken in einem besonders frühen Stadium zu finden und zu nutzen, bevor sie an die Öffentlichkeit gelangen (sog. Zero Day Exploits).

Die Kenntnis der teils schwer zu entdeckenden Schwachstellen hat einen hohen Marktwert, weil sie einerseits von Ausnutzungswilligen benötigt wird, andererseits von den Softwareherstellern, die ihre Produkte frei von Schwachstellen halten wollen. Für jeden, der sich im Besitz solcher Informationen oder Technologien befindet, bieten sich deshalb stets die Alternativen des Verkaufs an betroffene Unternehmen oder aber an Käufer, die unter Geheimhaltung dieses Wissens eine Ausnutzung beabsichtigen. In der Folge hat sich eine Strategie zur Verbesserung der IT-Sicherheit etabliert, die darauf beruht, die Anreize für die Offenlegung von Schwachstellen zu erhöhen: Im Rahmen sog. Bug-Bounty-Programme bieten Unternehmen ein Kopfgeld für die Aufdeckung von Schwachstellen an und fördern so die Entstehung einer Bewegung und einer Industrie, die sich der Bekanntmachung und Behebung von Sicherheitslücken widmet. Das weltweite Bestreben, informationstechnische Systeme

---

[2] Pohlmann / Riedel: Strafverfolgung darf die IT-Sicherheit im Internet nicht schwächen, in: Datenschutz und Datensicherheit, 42. Jg. (2018), H. 1, 37 (41).

[3] Pohlmann / Riedel: Strafverfolgung darf die IT-Sicherheit im Internet nicht schwächen, in: Datenschutz und Datensicherheit, 42. Jg. (2018), H. 1, 37 (42 f.).

sicher zu gestalten und vor unbefugtem Zugriff oder Manipulation zu schützen, beruht maßgeblich auf der Fähigkeit zur Entdeckung und Behebung dieser Sicherheitslücken.

2. Gesetzgebungsverfahren, Gesetzesbegründung und bisherige fachliche Stellungnahmen

Der Gesetzgeber hat die Einführung der Eingriffsbefugnisse nach §§ 100a Abs. 1 S. 2 und 3, 100b Abs. 1 StPO im Wesentlichen mit der fortschreitenden Entwicklung und Verbreitung informationstechnischer Systeme und der damit einhergehenden Entstehung neuer und Verlagerung herkömmlicher Kommunikationsformen auf mobile Geräte und Datennetze begründet.[4] Informationstechnische Systeme spielten eine große Rolle bei der Verhinderung und Aufklärung von Straftaten. Eine Entschlüsselung internetbasierter Kommunikation sei bislang entweder unmöglich oder langwierig und kostenintensiv. Der eine Stärkung von Verschlüsselungstechnologien befürwortenden Kryptopolitik der Bundesregierung stehe das Gebot effektiver Strafverfolgung gegenüber, welches ohne eine Überwachung bei den hier vorgesehenen Katalogtaten nicht verwirklicht werden könne.

Die deshalb für erforderlich gehaltenen Maßnahmen sind mittels einer Formulierungshilfe der Bundesregierung als Änderungsantrag zu einem bereits eingebrachten Gesetzentwurf am 15. Mai 2017 in das Gesetzgebungsverfahren eingeführt worden. Sodann wurden durch den Ausschuss für Recht und Verbraucherschutz verschiedene gutachterliche Stellungnahmen von Sachverständigen eingeholt und am 31. Mai 2017 angehört und die Vorlage am 20. Juni 2017 abschließend beraten. Die zweite und dritte Beratung des Gesetzes durch den Bundestag erfolgte bereits am 22. Juni 2017, nachdem der Tagesordnungspunkt gegen die Stimmen der Opposition kurzfristig und mit einer Debattenzeit von 38 Minuten aufgesetzt worden war.

Die am 31. Mai 2017 angehörten Gutachter haben in ihren Stellungnahmen unterschiedlich Stellung bezogen.

Oberstaatsanwalt beim BGH Michael Greven hält die Maßnahmen als Anpassung der Eingriffsrechte von Strafverfolgungsbehörden an den rasanten Fortschritt moderner Kommunikationstechnologien für erforderlich und bezieht sich dabei maßgeblich auf die Einsatzgebiete der schweren und organisierten Kriminalität sowie Staatsschutzdelikte.[5] Verschlüsselungstechnologien würden die Behörden von der Möglichkeit abschneiden, über den Austausch von Informationen mittels technischer Kommunikation Beweis zu erheben. Er weist darauf hin, dass die Bewertung des Gewichts einer zu untersuchenden Tat und insbesondere die Frage, ob ein besonders schwerer Fall vorliegt, aufgrund des meist frühen Zeitpunkts des Einsatzes solcher Maßnahmen mit erheblichen Schwierigkeiten verbunden sein wird.

---

[4] BT-Drs. 18/12785, S. 51 ff.

[5] Greven: Stellungnahme zum Gesetzentwurf zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze (2017).

Bundesanwalt beim BGH Dr. Matthias Krauß hält das Vorhaben für notwendig, da die Verschlüsselung moderner Kommunikationswege die bisherige TK-Überwachung weitgehend ins Leere laufen lasse und bei der offenen Beschlagnahme von Datenbeständen keine Auswertbarkeit gewährleistet werden könne.[6] Bei der sog. Quellen-TKÜ handele es sich um ein neuartiges Ermittlungsinstrument, das zwangsläufig mit einem Eingriff in die Integrität des Zielsystems verbunden sei. Insbesondere der Zugriff auf gespeicherte Daten betreffe grundsätzlich nicht mehr den Schutzbereich des Art. 10 GG, sondern stelle einen Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme dar. Dennoch sei auch die Variante des § 100a Abs. 1 S. 3 StPO als Ausnahmeregelung vertretbar. Die Online-Durchsuchung ermögliche zwar die Bildung von Verhaltensprofilen und weise eine große Streubreite auf, begegne aber aufgrund der wirksamen Beschränkung auf besonders schwere Straftaten keinen Bedenken.

Oberstaatsanwalt Alfred Huber rechnet damit, dass die herkömmliche Telekommunikationsüberwachung aufgrund der Möglichkeiten verschlüsselten Datenverkehrs mittelfristig nur noch unzureichende Ergebnisse bringen werde, weshalb die sog. Quellen-TKÜ und Online-Durchsuchung unabdingbar seien.[7] Letztere werde nur selten zum Einsatz kommen. Da die Anlasstat auch im Einzelfall besonders schwer wiegen müsse, sei die Aufnahme von Tatbeständen in den Straftatenkatalog, die sich nicht in jedem Einzelfall den besonders schweren Taten zuordnen lassen, unbedenklich.

Der Vizepräsident des Bundeskriminalamts Peter Henzler sieht in den vorgesehenen Änderungen einen deutlichen Mehrwert für eine effektive Strafverfolgung.[8] Kryptierte Kommunikationswege bedrohten den Erfolgswert der TK-Überwachung und die Auswertung verschlüsselter Datenspeicher als Spurenansatz bzw. Beweismittel machten das Ermittlungsinstrument der Online-Durchsuchung erfolgsversprechend. Mittels Keylogging oder der Fertigung von Screenshots könnten Passwörter erlangt werden, die eine Auswertung nach einer Beschlagnahme überhaupt ermöglichten. Typische Anwendungsbereiche seien Terrorismus, PMK links, Kinderpornographie und Online-Betrug.

Richter am Landgericht Dr. Ulf Buermeyer lehnt die Einführung der Maßnahmen ab.[9] Die Online-Durchsuchung gehe hinsichtlich der Eingriffstiefe noch über die akustische Wohnraumüberwachung hinaus und sei insbesondere aufgrund des zu weiten Straftatenkatalogs nicht zu rechtfertigen. Die sog. Quellen-TKÜ stelle mangels Beschränkung auf laufende Kommunikation eine verfassungswidrige Online-

---

[6] Krauß: Stellungnahme zum Gesetzentwurf zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze (2017).

[7] Huber: Stellungnahme zur Sachverständigenanhörung am 31.05.2017 im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages zum Gesetzentwurf der Bundesregierung zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze (2017).

[8] Henzler: Anhörung des Vizepräsidenten des Bundeskriminalamtes Peter Henzler im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages am 31. Mai 2017 zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze (2017).

[9] Buermeyer: Gutachterliche Stellungnahme zur Öffentlichen Anhörung zur „Formulierungshilfe" des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKÜ im Strafprozess (2017).

Durchsuchung dar. Es sei in beiden Fällen weder durch Regelungen zu den technischen Anforderungen noch durch eine unabhängige Prüfung sichergestellt, dass die einzusetzende Software die Mindestanforderungen an Datensicherheit und Manipulationsresistenz erfülle. Der Schutz von Berufsgeheimnisträgern sei unzureichend. Das mit den Maßnahmen geschaffene Interesse der Sicherheitsbehörden, die Cyber-Sicherheit weltweit zu schwächen, setze Fehlanreize hin zu einer Kultur der kalkulierten IT-Unsicherheit.

Prof. Dr. Arndt Sinn stellt fest, die Variante des § 100a Abs. 1 S. 3 StPO stelle eine „kleine Online-Durchsuchung dar" und der dort vorgesehene Zugriff auf gespeicherte Daten unterliege grundsätzlich dem Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme.[10] Ob die Beschränkung des Zugriffs auf Kommunikationsvorgänge es erlaube, den Eingriff an Art. 10 GG zu messen, bedürfe weiterer parlamentarischer Diskussion. Die Maßnahme des § 100b Abs. 1 StPO dürfe nicht zur Ausleitung von Informationen etwa durch Kameras genutzt werden. Wie diesem Missbrauchspotential begegnet werden solle, bleibe bislang offen, müsse sich aber im Gesetzeswortlaut niederschlagen.

Die Vertreter des Chaos-Computer-Clubs Linus Neumann, Constanze Kurz und Frank Rieger betonen, dass die zum Anbringen der erforderlichen Software erforderliche Geheimhaltung von Sicherheitslücken mit einer Gefahr für die innere Sicherheit einhergehe.[11] Die rechtlichen Grenzen der sog. Quellen-TKÜ ließen sich technisch kaum umsetzen, wodurch de facto eine Online-Durchsuchung geschaffen werde. Strafverfolgungsbehörden hätten aufgrund der fortschreitenden Digitalisierung aller Lebensbereiche heute Zugriff auf eine nie dagewesene Fülle an Daten, weshalb die vorgeschlagenen Maßnahmen nicht erforderlich seien. Mangels hinreichend spezifischer technischer Rahmenvorgaben und Überprüfbarkeit seien Rechtssicherheit und adäquate Kontrolle nicht sicherzustellen. Es sei mit gravierenden Folgen für Vertrauen, Sicherheit und Marktposition deutscher Anbieter von Verschlüsselungslösungen zu rechnen und eine Verletzung der Eckpunkte deutscher Kryptopolitik zu befürchten.

3. Die gerügten Vorschriften

Die angegriffenen Vorschriften haben den folgenden Wortlaut und werden hier in ihrem systematischen Zusammenhang wiedergegeben:

§ 100a StPO (Telekommunikationsüberwachung)

[10] Sinn: Stellungnahme zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze sowie zur Formulierungshilfe der Bundesregierung für einen Änderungsantrag zum o.g. Gesetzentwurf (2017).

[11] Neumann / Kurz / Rieger: Sachverständigenauskunft zum Änderungsantrag der Fraktionen CDU/CSU und SPD zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze (2017).

(1) Auch ohne Wissen der Betroffenen darf die Telekommunikation überwacht und aufgezeichnet werden, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete schwere Straftat begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht, oder durch eine Straftat vorbereitet hat,
2. die Tat auch im Einzelfall schwer wiegt und
3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

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

(2) Schwere Straftaten im Sinne des Absatzes 1 Nr. 1 sind:

1. aus dem Strafgesetzbuch:
   a) Straftaten des Friedensverrats, des Hochverrats und der Gefährdung des demokratischen Rechtsstaates sowie des Landesverrats und der Gefährdung der äußeren Sicherheit nach den §§ 80a bis 82, 84 bis 86, 87 bis 89a, 89c Absatz 1 bis 4, 94 bis 100a,
   b) Bestechlichkeit und Bestechung von Mandatsträgern nach § 108e,
   c) Straftaten gegen die Landesverteidigung nach den §§ 109d bis 109h,
   d) Straftaten gegen die öffentliche Ordnung nach den §§ 129 bis 130,
   e) Geld- und Wertzeichenfälschung nach den §§ 146 und 151, jeweils auch in Verbindung mit § 152, sowie nach § 152a Abs. 3 und § 152b Abs. 1 bis 4,
   f) Straftaten gegen die sexuelle Selbstbestimmung in den Fällen der §§ 176a, 176b und, unter den in § 177 Absatz 6 Satz 2 Nummer 2 genannten Voraussetzungen, des § 177,
   g) Verbreitung, Erwerb und Besitz kinder- und jugendpornographischer Schriften nach § 184b Absatz 1 und 2, § 184c Absatz 2,
   h) Mord und Totschlag nach den §§ 211 und 212,

i) Straftaten gegen die persönliche Freiheit nach den §§ 232, 232a Absatz 1 bis 5, den §§ 232b, 233 Absatz 2, den §§ 233a, 234, 234a, 239a und 239b,

j) Bandendiebstahl nach § 244 Abs. 1 Nr. 2 und schwerer Bandendiebstahl nach § 244a,

k) Straftaten des Raubes und der Erpressung nach den §§ 249 bis 255,

l) gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei nach den §§ 260 und 260a,

m) Geldwäsche und Verschleierung unrechtmäßig erlangter Vermögenswerte nach § 261 Abs. 1, 2 und 4; beruht die Strafbarkeit darauf, dass die Straflosigkeit nach § 261 Absatz 9 Satz 2 gemäß § 261 Absatz 9 Satz 3 ausgeschlossen ist, jedoch nur dann, wenn der Gegenstand aus einer der in den Nummern 1 bis 11 genannten schweren Straftaten herrührt,

n) Betrug und Computerbetrug unter den in § 263 Abs. 3 Satz 2 genannten Voraussetzungen und im Falle des § 263 Abs. 5, jeweils auch in Verbindung mit § 263a Abs. 2,

o) Subventionsbetrug unter den in § 264 Abs. 2 Satz 2 genannten Voraussetzungen und im Falle des § 264 Abs. 3 in Verbindung mit § 263 Abs. 5,

p) Sportwettbetrug und Manipulation von berufssportlichen Wettbewerben unter den in § 265e Satz 2 genannten Voraussetzungen,

q) Straftaten der Urkundenfälschung unter den in § 267 Abs. 3 Satz 2 genannten Voraussetzungen und im Fall des § 267 Abs. 4, jeweils auch in Verbindung mit § 268 Abs. 5 oder § 269 Abs. 3, sowie nach § 275 Abs. 2 und § 276 Abs. 2,

r) Bankrott unter den in § 283a Satz 2 genannten Voraussetzungen,

s) Straftaten gegen den Wettbewerb nach § 298 und, unter den in § 300 Satz 2 genannten Voraussetzungen, nach § 299,

t) gemeingefährliche Straftaten in den Fällen der §§ 306 bis 306c, 307 Abs. 1 bis 3, des § 308 Abs. 1 bis 3, des § 309 Abs. 1 bis 4, des § 310 Abs. 1, der §§ 313, 314, 315 Abs. 3, des § 315b Abs. 3 sowie der §§ 316a und 316c,

u) Bestechlichkeit und Bestechung nach den §§ 332 und 334,

2. aus der Abgabenordnung:

a) Steuerhinterziehung unter den in § 370 Abs. 3 Satz 2 Nr. 5 genannten Voraussetzungen,

b) gewerbsmäßiger, gewaltsamer und bandenmäßiger Schmuggel nach § 373,

c) Steuerhehlerei im Falle des § 374 Abs. 2,

3. aus dem Anti-Doping-Gesetz:
Straftaten nach § 4 Absatz 4 Nummer 2 Buchstabe b,

4. aus dem Asylgesetz:
a) Verleitung zur missbräuchlichen Asylantragstellung nach § 84 Abs. 3,
b) gewerbs- und bandenmäßige Verleitung zur missbräuchlichen Asylantragstellung nach § 84a,

5. aus dem Aufenthaltsgesetz:
a) Einschleusen von Ausländern nach § 96 Abs. 2,
b) Einschleusen mit Todesfolge und gewerbs- und bandenmäßiges Einschleusen nach § 97,

6. aus dem Außenwirtschaftsgesetz:
vorsätzliche Straftaten nach den §§ 17 und 18 des Außenwirtschaftsgesetzes,

7. aus dem Betäubungsmittelgesetz:
a) Straftaten nach einer in § 29 Abs. 3 Satz 2 Nr. 1 in Bezug genommenen Vorschrift unter den dort genannten Voraussetzungen,
b) Straftaten nach den §§ 29a, 30 Abs. 1 Nr. 1, 2 und 4 sowie den §§ 30a und 30b,

8. aus dem Grundstoffüberwachungsgesetz:
Straftaten nach § 19 Abs. 1 unter den in § 19 Abs. 3 Satz 2 genannten Voraussetzungen,

9. aus dem Gesetz über die Kontrolle von Kriegswaffen:
a) Straftaten nach § 19 Abs. 1 bis 3 und § 20 Abs. 1 und 2 sowie § 20a Abs. 1 bis 3, jeweils auch in Verbindung mit § 21,
b) Straftaten nach § 22a Abs. 1 bis 3,

9a. aus dem Neue-psychoaktive-Stoffe-Gesetz:
Straftaten nach § 4 Absatz 3 Nummer 1 Buchstabe a,

10. aus dem Völkerstrafgesetzbuch:
a) Völkermord nach § 6,
b) Verbrechen gegen die Menschlichkeit nach § 7,
c) Kriegsverbrechen nach den §§ 8 bis 12,
d) Verbrechen der Aggression nach § 13,

11. aus dem Waffengesetz:
a) Straftaten nach § 51 Abs. 1 bis 3,
b) Straftaten nach § 52 Abs. 1 Nr. 1 und 2 Buchstabe c und d sowie Abs. 5 und 6.

(3) Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss oder ihr informationstechnisches System benutzt.
(4) [...]
(5) Bei Maßnahmen nach Absatz 1 Satz 2 und 3 ist technisch sicherzustellen, dass

1. ausschließlich überwacht und aufgezeichnet werden können:
   a) die laufende Telekommunikation (Absatz 1 Satz 2), oder
   b) Inhalte und Umstände der Kommunikation, die ab dem Zeitpunkt der Anordnung nach § 100e Absatz 1 auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz hätten überwacht und aufgezeichnet werden können (Absatz 1 Satz 3),
2. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und
3. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.
(6) Bei jedem Einsatz des technischen Mittels sind zu protokollieren

1. die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,
2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,
3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und
4. die Organisationseinheit, die die Maßnahme durchführt.

§ 100b StPO (Online-Durchsuchung)

(1) Auch ohne Wissen des Betroffenen darf mit technischen Mitteln in ein von dem Betroffenen genutztes informationstechnisches System eingegriffen und dürfen Daten daraus erhoben werden (Online-Durchsuchung), wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete besonders schwere Straftat begangen oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat,
2. die Tat auch im Einzelfall besonders schwer wiegt und
3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

(2) Besonders schwere Straftaten im Sinne des Absatzes 1 Nummer 1 sind:

1. aus dem Strafgesetzbuch:

a) Straftaten des Hochverrats und der Gefährdung des demokratischen Rechtsstaates sowie des Landesverrats und der Gefährdung der äußeren Sicherheit nach den §§ 81, 82, 89a, 89c Absatz 1 bis 4, nach den §§ 94, 95 Absatz 3 und § 96 Absatz 1, jeweils auch in Verbindung mit § 97b, sowie nach den §§ 97a, 98 Absatz 1 Satz 2, § 99 Absatz 2 und den §§ 100, 100a Absatz 4,

b) Bildung krimineller Vereinigungen nach § 129 Absatz 1 in Verbindung mit Absatz 5 Satz 3 und Bildung terroristischer Vereinigungen nach § 129a Absatz 1, 2, 4, 5 Satz 1 erste Alternative, jeweils auch in Verbindung mit § 129b Absatz 1,

c) Geld- und Wertzeichenfälschung nach den §§ 146 und 151, jeweils auch in Verbindung mit § 152, sowie nach § 152a Absatz 3 und § 152b Absatz 1 bis 4,

d) Straftaten gegen die sexuelle Selbstbestimmung in den Fällen des § 176a Absatz 2 Nummer 2 oder Absatz 3 und, unter den in § 177 Absatz 6 Satz 2 Nummer 2 genannten Voraussetzungen, des § 177,

e) Verbreitung, Erwerb und Besitz kinderpornografischer Schriften in den Fällen des § 184b Absatz 2,

f) Mord und Totschlag nach den §§ 211, 212,

g) Straftaten gegen die persönliche Freiheit in den Fällen der §§ 234, 234a Absatz 1, 2, der §§ 239a, 239b und Menschenhandel nach § 232 Absatz 3, Zwangsprostitution und Zwangsarbeit nach § 232a Absatz 3, 4 oder 5 zweiter Halbsatz, § 232b Absatz 3 oder 4 in Verbindung mit § 232a Absatz 4 oder 5 zweiter Halbsatz und Ausbeutung unter Ausnutzung einer Freiheitsberaubung nach § 233a Absatz 3 oder 4 zweiter Halbsatz,

h) Bandendiebstahl nach § 244 Absatz 1 Nummer 2 und schwerer Bandendiebstahl nach § 244a,

i) schwerer Raub und Raub mit Todesfolge nach § 250 Absatz 1 oder Absatz 2, § 251,

j) räuberische Erpressung nach § 255 und besonders schwerer Fall einer Erpressung nach § 253 unter den in § 253 Absatz 4 Satz 2 genannten Voraussetzungen,

k) gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei nach den §§ 260, 260a,

l) besonders schwerer Fall der Geldwäsche, Verschleierung unrechtmäßig erlangter Vermögenswerte nach § 261 unter den in § 261 Absatz

4 Satz 2 genannten Voraussetzungen; beruht die Strafbarkeit darauf, dass die Straflosigkeit nach § 261 Absatz 9 Satz 2 gemäß § 261 Absatz 9 Satz 3 ausgeschlossen ist, jedoch nur dann, wenn der Gegenstand aus einer der in den Nummern 1 bis 7 genannten besonders schweren Straftaten herrührt,

m) besonders schwerer Fall der Bestechlichkeit und Bestechung nach § 335 Absatz 1 unter den in § 335 Absatz 2 Nummer 1 bis 3 genannten Voraussetzungen,

2. aus dem Asylgesetz:

a) Verleitung zur missbräuchlichen Asylantragstellung nach § 84 Absatz 3,

b) gewerbs- und bandenmäßige Verleitung zur missbräuchlichen Asylantragstellung nach § 84a Absatz 1,

3. aus dem Aufenthaltsgesetz:

a) Einschleusen von Ausländern nach § 96 Absatz 2,

b) Einschleusen mit Todesfolge oder gewerbs- und bandenmäßiges Einschleusen nach § 97,

4. aus dem Betäubungsmittelgesetz:

a) besonders schwerer Fall einer Straftat nach § 29 Absatz 1 Satz 1 Nummer 1, 5, 6, 10, 11 oder 13, Absatz 3 unter der in § 29 Absatz 3 Satz 2 Nummer 1 genannten Voraussetzung,

b) eine Straftat nach den §§ 29a, 30 Absatz 1 Nummer 1, 2, 4, § 30a,

5. aus dem Gesetz über die Kontrolle von Kriegswaffen:

a) eine Straftat nach § 19 Absatz 2 oder § 20 Absatz 1, jeweils auch in Verbindung mit § 21,

b) besonders schwerer Fall einer Straftat nach § 22a Absatz 1 in Verbindung mit Absatz 2,

6. aus dem Völkerstrafgesetzbuch:

a) Völkermord nach § 6,

b) Verbrechen gegen die Menschlichkeit nach § 7,

c) Kriegsverbrechen nach den §§ 8 bis 12,

d) Verbrechen der Aggression nach § 13,

7. aus dem Waffengesetz:

a) besonders schwerer Fall einer Straftat nach § 51 Absatz 1 in Verbindung mit Absatz 2,

b) besonders schwerer Fall einer Straftat nach § 52 Absatz 1 Nummer 1 in Verbindung mit Absatz 5.

(3) Die Maßnahme darf sich nur gegen den Beschuldigten richten. Ein Eingriff in informationstechnische Systeme anderer Personen ist nur zulässig, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass

1. der in der Anordnung nach § 100e Absatz 3 bezeichnete Beschuldigte informationstechnische Systeme der anderen Person benutzt, und
2. die Durchführung des Eingriffs in informationstechnische Systeme des Beschuldigten allein nicht zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes eines Mitbeschuldigten führen wird.

Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

(4) § 100a Absatz 5 und 6 gilt mit Ausnahme von Absatz 5 Satz 1 Nummer 1 entsprechend.

§ 100d (Kernbereich privater Lebensgestaltung; Zeugnisverweigerungsberechtigte)

(1) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach den §§ 100a bis 100c allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden, ist die Maßnahme unzulässig.

(2) Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach den §§ 100a bis 100c erlangt wurden, dürfen nicht verwertet werden. Aufzeichnungen über solche Erkenntnisse sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren.

(3) Bei Maßnahmen nach § 100b ist, soweit möglich, technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Erkenntnisse, die durch Maßnahmen nach § 100b erlangt wurden und den Kernbereich privater Lebensgestaltung betreffen, sind unverzüglich zu löschen oder von der Staatsanwaltschaft dem anordnenden Gericht zur Entscheidung über die Verwertbarkeit und Löschung der Daten vorzulegen. Die Entscheidung des Gerichts über die Verwertbarkeit ist für das weitere Verfahren bindend.

(4) [...]

(5) In den Fällen des § 53 sind Maßnahmen nach den §§ 100b und 100c unzulässig; ergibt sich während oder nach Durchführung der Maßnahme, dass ein Fall des § 53 vorliegt, gilt Absatz 2 entsprechend. In den Fällen der §§ 52 und 53a dürfen aus Maßnahmen nach den §§ 100b und 100c gewonnene Erkenntnisse nur verwertet werden, wenn dies unter Berücksichtigung der Bedeutung des zugrunde liegenden Vertrauensverhältnisses nicht außer Verhältnis zum Interesse an der Erforschung des Sachverhalts oder der Ermittlung des Aufenthaltsortes eines Beschuldigten steht. § 160a Absatz 4 gilt entsprechend.

II. Beschwerdeführer

1. Beschwerdeführer zu 1

Der Beschwerdeführer zu 1 ist ein bundesweiter Verband für IT-Sicherheit. Es handelt sich um ein interdisziplinäres Kompetenznetzwerk in- und ausländischer Mitglieder aus Industrie, Verwaltung, Beratung, Wissenschaft und inhaltlich verwandter Organisationen. Der Verband beschäftigt sich mit aktuellen Fragen der IT-Sicherheit und ist unter anderem Träger des Vertrauenszeichens „IT Security Made In Germany". Themen sind unter anderem die Beschränkung des Datenzugriffs US-amerikanischer Behörden, insbesondere der Geheimdienste, der Schutz von Whistleblowern, die Abwehr von Cyberspionage und -sabotage und die Förderung von IT-Sicherheit in der Wirtschaft.

2. Beschwerdeführer zu 2

Der Beschwerdeführer zu 2 ist Informatiker und Professor für Informationssicherheit, Direktor des Instituts für Internet-Sicherheit, Vorstandsvorsitzender des Bundesverbands IT-Sicherheit „TeleTrusT" und Vorstandsmitglied des Verbandes der Internetwirtschaft „eco". Er unterstützt und berät Unternehmen in den Bereichen IT und IT-Sicherheit. Er reist zu nationalen und internationalen Kongressen und forscht im Hochsicherheitsbereich. Ein Schwerpunt seiner Forschung liegt im Bereich der Bekämpfung von Malware, was im Ergebnis auch staatlich eingesetzte Software wie den sog. Bundestrojaner betrifft. Im Rahmen seiner Forschung im Bereich von Frühwarnsystemen, Botnet-Detektion und allgemeiner Robustheit von IT-Systemen entwickelt er Technologien, die verhindern sollen, dass kriminelle Schadprogramme oder staatliche Zugriffsprogramme wie der sog. Bundestrojaner auf einem System zur Ausführung kommen.

3. Beschwerdeführer zu 3

Der Beschwerdeführer zu 3 ist Geschäftsführer des Beschwerdeführers zu 1. Er reist auch in seiner beruflichen Kapazität häufig in Drittländer, zuletzt in einen arabischen Staat, nach Vietnam und in die USA.

4. Beschwerdeführer zu 4

Der Beschwerdeführer zu 4 ist Rechtsanwalt. Er ist spezialisiert auf das IT-Recht und betreut Mandanten unter anderem in Fragestellungen der IT-Compliance, der Informationssicherheit und des Datenschutzrechts.

B. Rechtsschutzbegehren

I. Die Beschwerdeführer wenden sich mit der Verfassungsbeschwerde gegen §§ 100a Abs. 1 S. 2 und 3, Abs. 5 und 6, 100b Abs. 1 und 100d Abs. 5 StPO in der Fassung nach dem Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017, das am 23. August 2017 verkündet wurde (Bundesgesetzblatt I, Seite 3202 ff.).

II. Die Beschwerdeführer rügen die Verletzung ihrer Grundrechte aus Art. 1 Abs. 1, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1, Art. 10 Abs. 1, Art. 12 Abs. 1 und Art. 19 Abs. 4 GG sowie Art. 7 und 8 der Charta der Grundrechte der Europäischen Union.

C. Zulässigkeit

I. Grundrechtsträgereigenschaft der Beschwerdeführer

Der Beschwerdeführer zu 1 ist eine inländische juristische Person. Die Grundrechte aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1, Art. 10 Abs. 1, Art. 12 Abs. 1 und Art. 19 Abs. 4 GG sind gem. Art. 19 Abs. 3 GG ihrem Wesen nach auch auf juristische Personen anwendbar. Art. 7 und 8 der Charta der Grundrechte der Europäischen Union gebieten nicht zuletzt hinsichtlich eines effektiven Schutzes des personalen Substrats ebenfalls eine Einbeziehung juristischer Personen in den Schutzbereich.
Die Beschwerdeführer zu 2-4 sind natürliche Personen. Bei den Grundrechten aus Art. 1 Abs. 1, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1, Art. 10 Abs. 1, Art. 12 Abs. 1 und Art. 19 Abs. 4 GG sowie Art. 7 und 8 EuGrCh handelt es sich um Jedermann-Grundrechte, deren Verletzung insofern von den Beschwerdeführern geltend gemacht werden kann.

II. Beschwerdebefugnis

Die Beschwerdeführer sind hinsichtlich der angegriffenen Regelungen beschwerdebefugt. Sie sind durch diese Regelungen mit einiger Wahrscheinlichkeit selbst, unmittelbar und gegenwärtig in ihren Grundrechten betroffen. Dabei gilt, dass die Anforderungen an die Darlegung der Wahrscheinlichkeit eigener Betroffenheit an den tatsächlichen Möglichkeiten einer solchen Darlegung auszurichten sind.[12]

1. Selbstbetroffenheit

Die in den §§ 100a Abs. 1 S. 2 und 3, Abs. 5 und 6, 100b Abs. 1, 100d Abs. 5 StPO geregelten Befugnisse zur Online-Durchsuchung und sog. Quellen-TKÜ verletzen die Beschwerdeführer in eigenen Grundrechten. Die Beschwerdeführer sind nicht Adressaten der Normen, es handelt sich bei

[12] BVerfGE 109, 279 (308); 100, 313 (356 f.).

den angegriffenen Vorschriften aber um Befugnisse, die Eingriffe grundsätzlich gegen jedermann erlauben. Es ist mit einiger Wahrscheinlichkeit anzunehmen, dass die Beschwerdeführer von den hiermit ermöglichten Ermittlungsmaßnahmen betroffen sind. Somit besteht eine hinreichend enge Beziehung zwischen der Grundrechtsposition der Beschwerdeführer und den angegriffenen Vorschriften.[13] Dies gilt schon aufgrund der hohen Streubreite, die einer Datenerhebung innewohnt, die so weitreichenden Aufschluss über die Kommunikation mit Dritten geben kann,[14] und die hier darüber hinaus für eine Vielzahl von Katalogtaten – darunter Tatbestände leichter bis mittlerer Kriminalität – zugelassen wird. Zudem sind die Maßnahmen gegen Personen zulässig, deren Systeme durch einen Beschuldigten genutzt worden sein könnten, womit in weitem Umfang gutgläubige Dritte miterfasst werden können.

Die Beschwerdeführer nutzen allesamt informationstechnische Systeme und verschlüsselte Kommunikation. Insbesondere der Beschwerdeführer zu 1 nutzt neben Festnetz, Mobilfunk und SMS auch diverse Internetplattformen und Internetforen zum vereinsinternen Austausch sowie zum Kontakt mit der Öffentlichkeit und zahlreichen Ansprechpartnern in Politik und Gesellschaft, auch und insbesondere in Drittländern, wo der Verein Werbung für „IT-Sicherheit made in Germany“ macht.

Dabei besteht eine hohe Wahrscheinlichkeit, dass die Beschwerdeführer aufgrund ihrer professionellen Beschäftigung mit Verschlüsselungstechnologien, IT-Sicherheit und Datenschutz im Hochrisikobereich beruflich mit Personen in Kontakt kommen, gegen welche die hier gegenständlichen Maßnahmen eingesetzt werden. Hierzu gehören etwa die Themenkomplexe des Schutzes von Whistleblowern, der Entwicklung von Sicherheitslösungen im Angesicht des Zugriffs internationaler Nachrichtendienste, der Beschäftigung mit Cyber-War und -Spionage sowie des Umgangs mit Wirtschaftskriminalität. Dies kann sowohl dazu führen, dass ihre eigenen Systeme zum Ziel der hier gegenständlichen Maßnahmen werden, als auch dazu, dass sie als Dritte etwa im Rahmen von durch die Maßnahmen sehr weitläufig erfassten Kommunikationsvorgängen mitbetroffen sind. Insbesondere der Beschwerdeführer zu 3 reist regelmäßig in Drittländer wie zuletzt einen arabischen Staat und Vietnam, sodass neben der Exponierung als Geschäftsführer eines Verbandes, der sich mit hochsensiblen Daten und Sicherheitstechnologie befasst, auch die den Hochsicherheitsbereich betreffende Tätigkeit in solchen Ländern zur Einbeziehung in Strafverfahren führen kann, auch als unbeteiligter Dritter. Angesichts der Heimlichkeit der Maßnahme[15] und der Unzumutbarkeit von Darlegungen, durch die sich ein Beschwerdeführer selbst einer Straftat bezichtigen würde,[16] dürfen an die Darlegungslast keine überspannten Anforderungen gestellt werden.

Darüber hinaus betrifft die mit diesen Vorschriften einhergehende systematische staatliche Proliferation von Sicherheitslücken, die eine allgemeine Schwächung der Sicherheit informationstechnischer Systeme zur Folge hat, die Beschwerdeführer zu 1-3 auch in ihrer beruflichen

---

[13] Vgl. BVerfGE 108, 370 (384).
[14] Vgl. BVerfGE 120, 274 (323).
[15] Vgl. BVerfGE 113, 348 (362 f.); 100, 313 (355 f.); 109, 279 (306 f.).
[16] Vgl. BVerfGE 113, 348 (363).

Tätigkeit. In dieser befassen sie sich mit der Bekämpfung von Schadsoftware und unberechtigten Zugriffen auf informationstechnische Systeme und entwickeln entsprechende Technologien und Abwehrsysteme. Mit den angegriffenen Vorschriften werden Anreize für eine behördliche Aushöhlung der durch die Beschwerdeführer betreuten, entwickelten oder eingesetzten Sicherheitsmechanismen gesetzt. Des Weiteren sind die Vorschriften geeignet, das Vertrauen in Sicherheitslösungen wie die von den Beschwerdeführern entwickelten und angebotenen nachhaltig zu erschüttern.

Der Beschwerdeführer zu 4 kommt als Rechtsanwalt und damit Angehöriger der freien Advokatur regelmäßig mit Personen und Sachverhalten in Kontakt, bei denen eine strafrechtliche Relevanz nicht ausgeschlossen werden kann. Es ist mit hoher Wahrscheinlichkeit davon auszugehen, dass er von der Streuwirkung der hier angegriffenen Ermittlungsbefugnisse als Dritter betroffen ist. Er ist zudem dadurch in seiner Berufsausübung betroffen, dass die Vorschriften spezifische Regelungen zu Berufsgeheimnisträgern und ihren Berufshelfern enthalten.

2. Unmittelbarkeit der Betroffenheit

Die Verfassungsbeschwerde richtet sich gegen gesetzliche Befugnisse und nicht gegen sie umsetzende weitere Vollzugsakte. Eine unmittelbare Betroffenheit durch ein Gesetz ist jedoch gegeben, wenn der Rechtsweg gegen die darauf beruhenden Vollzugsakte mangels Kenntnis der Vollzugsmaßnahmen nicht oder nicht effektiv beschritten werden kann.[17] Die hier gegenständlichen Maßnahmen der Online-Durchsuchung und sog. Quellen-TKÜ erfolgen grundsätzlich heimlich. Der gesamte Zweck der Vorschriften ist darauf gerichtet, die Eingriffe ohne Wissen der Betroffenen durchzuführen und einige Zeit aufrecht zu erhalten. Soweit hierzu Benachrichtigungspflichten vorgesehen sind, vermögen sie dies nicht aufzufangen, da sie gegebenenfalls erst spät greifen und erhebliche Ausnahmen vorsehen.[18] Für Maßnahmen nach den §§ 100a, 100b StPO gilt die sich aus § 101 Abs. 4 Nr. 3 und 4 StPO ergebende Pflicht, die Beteiligten der überwachten Kommunikation (Nr. 3) bzw. die Zielperson und erheblich Mitbetroffene (Nr. 4) zu benachrichtigen. Dabei wird der effektive Rechtsschutz für § 100b StPO bereits durch die Beschränkung des Anwendungsbereichs der Benachrichtigungspflicht auf „erheblich" Mitbetroffene und den dadurch entstehenden, für den Mitbetroffenen nicht nachprüfbaren Spielraum eingeschränkt. Darüber hinaus bestehen erhebliche Ausnahmen von der Benachrichtigungspflicht. So sieht § 101 Abs. 4 S. 3 StPO das Ausbleiben der Benachrichtigung bei überwiegenden schutzwürdigen Belangen einer betroffenen Person vor, während § 101 Abs. 4 S. 4 StPO weitere Ausnahmen von der Benachrichtigung Dritter bei Eingriffen nach § 100a StPO normiert. Gem. § 101 Abs. 5 StPO ist eine Zurückstellung der Benachrichtigung aus Gesichtspunkten der Gefährdung des Untersuchungszwecks oder bestimmter individueller Rechtsgüter zulässig, wobei eine erste gerichtliche Überprüfung der Zurückstellung bei Maßnahmen nach § 100b StPO erst sechs

[17] Vgl. BVerfGE 113, 348 (362 f.); 100, 313 (354); 109, 279 (306 f.).
[18] Vgl. BVerfGE 141, 220 (261).

Monate nach Beendigung der Maßnahme und bei Maßnahmen nach § 100a Abs. 1 S. 2 und 3 StPO sogar erst nach zwölf Monaten zu erfolgen hat. Von der Gewährleistung einer zeitnahen Benachrichtigung kann somit nicht ausgegangen werden.

Empirische rechtstatsächliche Feststellungen zeigen zudem, dass die Rechtsschutzmöglichkeiten bei dieser Art heimlicher Maßnahmen faktisch noch eingeschränkter sind. So unterbleibt eine Benachrichtigung im Rahmen von TKÜ-Maßnahmen häufig und wird teilweise ohne Vorliegen oder ersichtliche Prüfung der Voraussetzungen unterlassen.[19]

Aus der Intensität der mit der sog. Quellen-TKÜ und vor allem mit der Online-Durchsuchung verbundenen Grundrechtseingriffe, die zu den ganz besonders eingriffsintensiven Maßnahmen gehören,[20] ergibt sich verbunden mit ihrem weiten Anwendungsbereich eine neue Qualität staatlicher digitaler Eingriffsbefugnisse, angesichts derer es unzumutbar ist, Betroffene ausschließlich auf die Möglichkeit zu verweisen, einzelne Vollzugsakte (und die Benachrichtigung hierüber ggf. mehrere Monate oder Jahre danach) abzuwarten, um nachträglichen Rechtsschutz in Anspruch zu nehmen.

3. Gegenwärtige Betroffenheit

Die angegriffenen Vorschriften sind zum 24. August 2017 in Kraft getreten. Aufgrund der hohen Streubreite der Ermittlungsmaßnahmen,[21] die bei Verdacht auf einen weitreichenden Katalog an Straftaten zugelassen sind und in großem Umfang auch gutgläubige Dritte erfassen, sowie des heimlichen Charakters der Eingriffe, welcher die Möglichkeiten der Darlegung weiter einschränkt, ist auch unter dem Gesichtspunkt des effektiven Rechtsschutzes von der Gegenwärtigkeit der Betroffenheit mit einiger Wahrscheinlichkeit auszugehen. Auch hier gilt zudem, dass im Hinblick auf die Selbstbelastungsfreiheit an die Darlegungslast keine zu hohen Anforderungen gestellt werden dürfen.

III. Subsidiarität

Die Verfassungsbeschwerde wahrt auch den Grundsatz der Subsidiarität. Den Beschwerdeführern ist nicht zuzumuten, einzelne Vollzugsakte und die Benachrichtigung hierüber abzuwarten, um dann gegen diese gerichtlich vorzugehen. § 101 Abs. 7 S. 2 StPO gewährt diesbezüglich lediglich nachträglichen Rechtsschutz gegen bereits beendete Maßnahmen. Die Eingriffe gehen jedoch in der

---

[19] Vgl. Albrecht / Dorsch / Krüpe: Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen (2003), S. 276 ff, 450 f.; Berliner Beauftragte für Datenschutz und Informationsfreiheit: Abschlussbericht zur datenschutzrechtlichen Überprüfung des Einsatzes von Stillen SMS in strafrechtlichen Ermittlungsverfahren (2016), S. 14; Bürgerschaft der Freien und Hansestadt Hamburg: Drs. 21/4900 (2016), S. 9 f.

[20] Vgl. BVerfGE 120, 274 (322); 141, 220 (304).

[21] Vgl. BVerfGE 109, 279 (308); 120, 274 (323).

gegenwärtigen Fassung der Vorschriften mit schwerwiegenden und irreversiblen Grundrechtsverletzungen einher, die Rechtsschutz auf diesem Wege erforderlich machen.

D. Begründetheit

I. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG (Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme)

1. Schutzpflichtverletzung

Die nach den §§ 100a Abs. 1 S. 2 und 3, 100b Abs. 1 StPO vorgesehenen Maßnahmen verletzen die sich aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ergebende aktive Schutzpflicht des Staates zur Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Wie unter D. I. 2. zu zeigen sein wird, verletzen die angegriffenen Vorschriften auch das diesem Grundrecht innewohnende Abwehrrecht. Das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme erschöpft sich jedoch nicht in der Abwehr ungerechtfertigter staatlicher Eingriffe in den Schutzbereich, sondern umfasst auch das Schaffen der Voraussetzungen für einen wirksamen Schutz des Einzelnen vor Eingriffen Dritter.[22] Dem werden die hier gegenständlichen Vorschriften nicht gerecht.

Aus dem objektiv-rechtlichen Gehalt der Grundrechte kann sich die Pflicht der staatlichen Organe ergeben, sich schützend und fördernd vor bedrohte Rechtsgüter zu stellen.[23] Die konkrete Ausgestaltung solcher Pflichten ist abhängig von Art und Ausmaß möglicher Gefahren sowie von Art und Gewicht des verfassungsrechtlich geschützten Rechtsguts.[24] Die Verdichtung des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu einem solch subjektiven Schutzanspruch lässt sich zunächst aus seinem Bezug auf Art. 1 Abs. 1 GG und den darin unstreitig enthaltenen Schutzauftrag herleiten. Des Weiteren ist das Grundrecht ausdrücklich als Recht auf Gewährleistung betitelt worden, was auf seinen objektiv-rechtlichen Gehalt hinweist.[25] Das Gericht hat die herausragende Intensität von Eingriffen in dieses Grundrechts bereits mehrfach zutreffend betont.[26] Hinzu kommt die besondere Relevanz des Aspekts der Vertraulichkeit: Voraussetzung für die Funktionsfähigkeit moderner informationstechnischer Systeme und die

---

[22] Vgl. BVerfGE 120, 274 (326); Deiseroth, Alles legal?, in: DVBl. 2015, 197 (199); Hahn / Johannes / Lange, Schutzschilde gegen die NSA, in: Datenschutz und Datensicherheit, 39. Jg. (2015), H. 2, 71 (73); Hauser, Das IT-Grundrecht (2015), S. 292 f.; Hoffman-Riem, Freiheitsschutz in den globalen Kommunikationsinfrastrukturen, in: JZ 2014, 53 (56 f.); Ullrich, Die Verpflichtung der Exekutive und Legislative zum Schutz deutscher Bürger vor der Ausspähung durch ausländische Geheimdienste, in: DVBl. 2015, 204 (207 f.).

[23] S. nur BVerfGE 39, 1 (42); 46, 160 (164); 53, 30 (57); 103, 89 (100 ff.); 106, 28 (37); 114, 1 (33 ff.).

[24] BVerfGE 49, 89 (142).

[25] Hoffman-Riem, Freiheitsschutz in den globalen Kommunikationsinfrastrukturen, in: JZ 2014, 53 (57).

[26] BVerfGE 120, 274 (313, 323 ff.) 141, 220 (304).

Möglichkeit einer unbefangenen Nutzung ist das Vertrauen der Nutzer in sie.[27] Ohne gewichtige Garantien droht dieses Vertrauen zu erodieren. Als Schutzobjekt befinden sich informationstechnische Systeme zudem an einem intersektionalen Schnittpunkt von rasantem technologischen Fortschritt, dessen Auswirkungen und Kontrollierbarkeit zum gegenwärtigen Zeitpunkt nicht überschaubar sind, einer Vernetzung nie dagewesenen Ausmaßes, der ein gewaltiges Risiko des unbefugten Zugriffs durch private Dritte innewohnt, und den Interessen ausländischer staatlicher Akteure, die von systematischer Wirtschaftsspionage bis zu einer totalen Datenauswertung durch Sicherheitsbehörden reichen. Gefahren für die Rechte der Bürger gehen folglich gleichzeitig von privaten Dritten, neuen Technologien und anderen Staaten aus, weshalb die Bürger besonders auf einen aktiven Schutz durch den Staat angewiesen sind.[28] Wie im Folgenden gezeigt wird, stehen Ermittlungsmethoden, die eine Infiltration informationstechnischer Systeme durch Ausnutzung von Sicherheitslücken voraussetzen, dem diametral entgegen.

Wie einleitend dargelegt wurde, setzt die Anwendung der Online-Durchsuchung und der sog. Quellen-TKÜ die Infiltration des Zielsystems über eine bestehende Schwachstelle des Systems voraus. Damit entsteht ein Interesse staatlicher Stellen an der Offenhaltung von Sicherheitslücken, obwohl sie gleichzeitig verpflichtet sind, ermittelte Lücken zur Vorbeugung von Gefahren für die Bürger schnellstmöglich zu schließen.[29] Dabei erhöht sich die Gefahr einer Ausnutzung durch Dritte sowohl mit der Zeit, die bis zur Schließung einer Lücke vergeht, als auch wegen der Möglichkeiten einer forensischen Analyse des verwendeten Angriffspunktes mit jeder behördlichen Anwendung. Aufgrund der Vielfalt informationstechnischer Systeme und Anwendungen wird wie unter A. I. 1. ausgeführt ein großer Pool an hochaktuellen Schwachstellen (sog. Zero Day Exploits) benötigt, um die Ermittlungsmaßnahmen der Online-Durchsuchung und der sog. Quellen-TKÜ praktisch anwendbar zu machen und zu halten. Es ist erläutert worden, dass der staatliche Bedarf an stets wechselnden, aktuellen Schwachstellen die staatlichen Kapazitäten zu ihrer autarken Entdeckung zwangsläufig um ein Vielfaches übersteigt und den Erwerb der entsprechenden Informationen auf dem freien Markt erforderlich macht. Der staatliche Bedarf wird Auswirkungen auf diesen Markt haben, auf dem Ausnutzungswillige und an der Gewährleistung von Sicherheit Interessierte um Schwachstellenwissen konkurrieren. Insbesondere die erwähnten sog. Bug-Bounty-Programme, die ein wesentliches Instrument zur Bekämpfung von IT-Kriminalität darstellen, basieren darauf, dass Unternehmen höhere Anreize für die Aufdeckung einer Schwachstelle bieten als die an der Geheimhaltung interessierten Käufer. Zu letzteren gehören nunmehr staatliche Einrichtungen, die damit in direkte Konkurrenz zu den auf die Gewährleistung von Sicherheit bedachten Institutionen treten, den Preis in die Höhe treiben und eine drastische Schwächung der allgemeinen IT-Sicherheit bewirken. Dieser Zielkonflikt

[27] Hoffman-Riem, Freiheitsschutz in den globalen Kommunikationsinfrastrukturen, in: JZ 2014, 53 (57).
[28] Vgl. Ullrich, Die Verpflichtung der Exekutive und Legislative zum Schutz deutscher Bürger vor der Ausspähung durch ausländische Geheimdienste, in: DVBl. 2015, 204 (208).
[29] Vgl. BVerfGE 120, 274 (326).

lässt sich unter den mit dieser Beschwerde angegriffenen Vorschriften nicht verfassungskonform auflösen.

Ein staatliches Interesse an struktureller Unsicherheit innerhalb informationstechnischer Systeme wird auf Dauer zu einem erheblichen Schaden für die einzelnen Nutzer, für die gesamte maßgeblich auf die Integrität solcher Systeme angewiesene IT-Wirtschaft und für die innere Sicherheit der Bundesrepublik Deutschland führen. Welchen Ausmaßes die durch die staatliche Sammlung von Software-Schwachstellen verursachten Schäden sind, hat sich zuletzt eindrücklich durch die Verbreitung des unter dem Namen „WannaCry" bekannt gewordenen Schadprogramms im Mai 2017 eindrücklich gezeigt. „WannaCry" machte sich eine Sicherheitslücke in einem von Windows-Betriebssystemen genutzten Netzwerkprotokoll zunutze. Innerhalb kurzer Zeit wurden Hunderttausende von Systemen in über 150 Ländern infiziert und unbrauchbar gemacht, darunter Systeme von großen Kommunikationsunternehmen, Krankenhäusern, Logistikdienstleistern, Transportunternehmen, Banken, Ministerien und anderer wesentlicher Infrastruktur. Es wird davon ausgegangen, dass die National Security Agency der Vereinigten Staaten von der zugrunde liegenden Sicherheitslücke mindestens fünf Jahre zuvor Kenntnis erlangt hatte.[30] Um die schwerwiegende Lücke selbst nutzen zu können, informierte die Behörde aber niemanden von ihrer Entdeckung und verhinderte so die Behebung. Stattdessen ließ sie eine Anwendung zur systematischen Ausnutzung (sog. Exploit) entwickeln, die im März 2017 von Unbekannten entwendet wurde. Nach dem Abhandenkommen der entwickelten Angriffstechnologie informierte die Behörde schließlich den Hersteller Microsoft, der nun die zur Schließung der Lücke erforderlichen Softwareupdates ausgab. Da diese nicht auf alle Systeme anwendbar waren und nicht von allen Nutzern sofort installiert wurden, kam es im Mai 2017 dennoch zu einem der größten Cyberangriffe der Geschichte, als das Schadprogramm „WannaCry" ausbrach und sich rasant verbreitete.

An diesen potentiell katastrophalen Auswirkungen wird ersichtlich, welche Gefahr der staatlichen Geheimhaltung von Schwachstellen und der Entwicklung von Angriffstechnologie innewohnt. Denn der Cyberangriff erfolgte in diesem Fall, nachdem bereits die zur Behebung der Schwachstelle erforderliche Software in Umlauf gebracht worden war, und konnte so nur einen Bruchteil seines Schadpotentials verwirklichen. Dass die hier ursächliche Angriffstechnologie vermutlich sogar in staatlichem Auftrag entwickelt wurde, ist dabei nicht so gravierend wie das Risiko, dass mit der jahrelangen Offenhaltung der entdeckten Schwachstelle eingegangen wurde. Hätten andere Akteure zu einem früheren Zeitpunkt selbstständige Kenntnis hiervon erlangt – worüber staatliche Stellen keinerlei Kontrolle haben, da sich eine bestehende Sicherheitslücke nicht „verstecken" lässt – wäre die Verbreitung des Schadprogrammes nicht durch die schon relativ weit verbreiteten Schutzupdates gehemmt worden. Die Folgen wären dann noch weitaus dramatischer gewesen und hätten zu einem

[30] Nakashima / Timberg: NSA officials worried about the day its potent hacking tool would get loose. Then it did, The Washington Post v. 16.05.2017, https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-toolwould-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html

Zusammenbruch kritischer Infrastruktur führen können. Die vorgesehene Anwendung von Online-Durchsuchung und sog. Quellen-TKÜ lässt sich nur unter Inkaufnahme dieses Risikos umsetzen.
Das systematische Unterlassen der gebotenen Aufklärung über Schwachstellen und das Aushöhlen der Bemühungen anderer staatlicher Stellen und der privaten Wirtschaft um die Gewährleistung sicherer IT-Systeme stehen in unmittelbarem Widerspruch zu der dargelegten Pflicht des Staates, seinen Bürgern ausreichend Schutz zu bieten. Damit werden die zivilrechtlichen, öffentlich-rechtlichen und strafrechtlichen Vorkehrungen (etwa die §§ 201 ff. StGB), die diese Schutzpflicht ausfüllen sollen, umgangen und ignoriert. Um das gebotene Mindestmaß an Schutz zu gewährleisten, muss der Staat garantieren, dass die mit Maßnahmen wie der Online-Durchsuchung und sog. Quellen-TKÜ verbundene Schwächung der allgemeinen IT-Sicherheit kontrollierbar bleibt. Gerade dies ist angesichts der beschriebenen technischen Problematiken nicht möglich. Jedenfalls würde dies aber die Offenlegung und Überprüfbarmachung der verwendeten Software sowie von Art und Umfang der Schwachstellenbeschaffung voraussetzen, sowie wirksame Maßnahmen zur Aufrechterhaltung des allgemeinen Sicherheitsniveaus und vor allem rechtlich verbindliche und überprüfbare Kriterien für die Entscheidung über Offenhaltung oder Schließung einer entdeckten bzw. erworbenen Schwachstelle. Gegenwärtig verbleibt wie ausgeführt kein angemessener Schutz im Sinne des Untermaßverbotes. Die angegriffenen Vorschriften verletzen die staatliche Schutzpflicht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.

2. Abwehrrecht

Die Maßnahmen nach §§ 100a Abs. 1 S. 2 und 3, 100b Abs. 1 StPO verletzen auch den aus dem Grundrecht auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG herzuleitenden Abwehranspruch.

a) Online-Durchsuchung

aa) Die Infiltration und Durchsuchung eines Zielsystems im Wege der Online-Durchsuchung nach § 100b Abs. 1 StPO stellt einen Eingriff in dieses Grundrecht dar. Eingriffe in dieses Recht stehen aufgrund des gewaltigen Umfangs und der Tiefe der auf solchen Systemen gespeicherten Daten aus allen Lebensbereichen unter besonders strengen verfassungsrechtlichen Anforderungen.[31] Die besondere Eingriffsintensität ergibt sich weiter aus der Heimlichkeit der Maßnahme, die dem Betroffenen ein rechtliches Vorgehen erst nachträglich ermöglicht,[32] sowie aus der manipulativen Natur der Beweiserhebung, bei der verändernd auf jenes informationstechnische System eingewirkt wird, das selbst Objekt der Erhebung sein soll. Besonders zu berücksichtigen sind die mit der

[31] BVerfGE 120, 274 (322 ff.).
[32] Vgl. BVerfGE 120, 274 (347 f.); 115, 320 (353); 113, 348 (383 f.).

technischen Methode des heimlichen Zugriffs zwingend verbundenen Gefahren, die oben näher ausgeführt worden sind (vgl. D. I. 1.).[33]

bb) Zu berücksichtigen ist die sich aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ergebende Schutzpflicht des Staates zur aktiven Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme auch in ihrer Funktion als Schranken-Schranke. Eine Einschränkung des Grundrechts kann nur soweit in Betracht kommen, wie dies den Staat nicht zu einer systematischen Verletzung seiner verfassungsrechtlichen Pflichten gegenüber seinen Bürgern zwingt. Diese Grenze ist vorliegend überschritten.

cc) Der schwerwiegende Eingriff ist in der jetzigen Ausgestaltung der Vorschrift unverhältnismäßig und deshalb nicht gerechtfertigt. Die Unverhältnismäßigkeit ergibt sich insbesondere aus der fehlenden Angemessenheit.

Für die Online-Durchsuchung zur Gefahrenabwehr hat das Gericht festgestellt, dass zur Rechtfertigung eine im Einzelfall drohende konkrete Gefahr für ein überragend wichtiges Rechtsgut erforderlich ist.[34] Hierunter fallen Gefahren 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.[35]

Die angegriffene Vorschrift dient nicht der Gefahrenabwehr, sondern der Strafverfolgung. Durch die Verschiebung von der präventiven auf die repressive Ebene entfällt der Ansatzpunkt der für ein spezifisches Rechtsgut konkret drohenden Gefahr, die es durch den Eingriff zu verhindern gilt. Sie wird ersetzt durch den allgemeinen staatlichen Strafanspruch und die Funktionsfähigkeit der Strafrechtspflege. Das Gewicht dieser Rechtsgüter hängt von der jeweils verfolgten Straftat ab.[36] Einen Anhaltspunkt für die Gewichtung liefern abstrakt besehen die gesetzlich vorgesehenen Strafrahmen, die darin festgelegten Höchststrafen sowie der Rang des durch die Tat verletzten Rechtsguts.[37] Vorliegend müssen die verfolgten Anlasstaten der repressiven Online-Durchsuchung von einem Gewicht sein, das mit den Anforderungen an die zu schützenden Rechtsgüter bei der präventiven Online-Durchsuchung vergleichbar ist. Zu berücksichtigen ist zudem, dass repressive Maßnahmen nicht mehr der Verhinderung einer drohenden Rechtsgutsverletzung dienen, sondern der bloß nachträglichen Verfolgung bereits eingetretener Verletzungen. Die Anforderungen an repressive Eingriffe sind entsprechend noch strenger zu fassen als in der Gefahrenabwehr, was sich auch in der bisherigen Rechtsprechung und Gesetzgebung widerspiegelt. Die Vorschrift wird dem in der gegenwärtigen Fassung nicht gerecht.

§ 100b Abs. 1 StPO erklärt die Online-Durchsuchung für anwendbar bei dem Verdacht einer besonders schweren Straftat, die auch im Einzelfall besonders schwer wiegt und deren Aufklärung auf andere Weise wesentlich erschwert oder aussichtslos wäre. Der Katalog des § 100b Abs. 2 StPO legt

---

[33] Vgl. BVerfGE 120, 274 (325 f.).
[34] BVerfGE 141, 220 (304 f.); 120, 274 (326 ff.).
[35] Ebd.
[36] BVerfGE 141, 220 (270)
[37] BVerfGE 109, 279 (343 ff.)

fest, welche Taten als schwere Taten im Sinne des Abs. 1 zu verstehen sind. Dieser Katalog knüpft jedoch nicht an den genannten wichtigen Rechtsgütern an und enthält stattdessen eine Vielzahl von Tatbeständen, deren Verfolgung keinesfalls von solch überragender Bedeutung ist, wie es zur Rechtfertigung dieses äußerst schwerwiegenden Grundrechtseingriffs bedarf. Vielmehr sind unter anderem bloße Vergehen erfasst sowie Delikte, die keines der genannten Rechtsgüter schützen. Dass der Gesetzgeber bei jeder Katalogtat voraussetzt, sie müsse auch im Einzelfall besonders schwer wiegen, kann nicht darüber hinwegtäuschen, dass mit der Aufstellung des Straftatenkatalogs eine normative Wertung getroffen wurde und gerade die Bewertung im Einzelfall entscheidend von dieser Wertung geprägt sein wird. Dass hier zu einem großen Teil Straftaten aufgenommen werden, deren Verdacht auch in schweren Erscheinungsformen nicht den verfassungsrechtlichen Kriterien genügt, zeigt sich vor allem, aber nicht ausschließlich an der in § 100b Abs. 2 StPO genannten Geld- und Wertzeichenfälschung (Nr. 1 Buchst. c), den Bandendiebstahlsdelikten (Nr. 1 Buchst. h), der qualifizierter Hehlerei (Nr. 1 Buchst. k), den besonders schweren Fällen der Geldwäsche und Verschleierung unrechtmäßig erlangter Vermögenswerte (Nr. 1 Buchst. l), den besonders schweren Fällen der Bestechlichkeit und Bestechung (Nr. 1 Buchst. m), der Verleitung zur missbräuchlichen Asylantragstellung (Nr. 2), dem Einschleusen von Ausländern (Nr. 3 Buchst. a) sowie den Straftaten aus dem Betäubungsmittelgesetz (Nr. 4). Eine Gefährdung des Bestands des Staates bzw. der Grundlagen der Existenz der Menschen oder Rechtsgutsverletzungen von vergleichbarem Gewicht scheinen insofern weitgehend ausgeschlossen. Dass demgegenüber auch Tatbestände enthalten sind, die im Einzelfall die in der bisherigen Rechtsprechung dieses Gerichts entwickelten Kriterien erfüllen können, führt zu keiner anderen Bewertung.

Der Katalog lässt über die bloße Anknüpfung an die Höchststrafe auch kein überzeugendes Konzept erkennen, nach dem es gerechtfertigt sein könnte, sämtliche aufgeführte Taten zum Anlass einer Online-Durchsuchung zu nehmen.[38] Die Übernahme des Straftatenkatalogs für die Wohnraumüberwachung verdeutlicht vielmehr, dass die Besonderheiten der Online-Durchsuchung und des damit verbundenen Eingriffs in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht hinreichend einbezogen worden sind. So ist die Online-Durchsuchung wie ausgeführt mit schwerwiegenden Vorfeldmaßnahmen verbunden, die erhebliche Folgeschäden in betroffenen Systemen verursachen und deren allgemeine Sicherheit einschränken können. Die Eingriffsintensität kann in Hinblick auf die Vielfalt der auf informationstechnischen Systemen gespeicherten Daten und ihre technologiebedingt höhere Auswertbarkeit über die Intensität eines Eingriffs in Art. 13 Abs. 1 GG hinausgehen. Zuletzt geht die Online-Durchsuchung mit einer geringeren Zielgenauigkeit und erhöhten Streubreite einher. Sie wird typischerweise eine größere Anzahl nichtverdächtiger Dritter mitbetreffen, da informationstechnische Systeme zu weitreichenden Kommunikationszwecken genutzt werden und regelmäßig in lokale oder andere Netzwerke eingebunden sind, mit denen sie Informationen austauschen.

[38] Vgl. BVerfGE 120, 274 (334).

Es handelt sich hier nicht um eine Frage der praktischen Normanwendung. Dies betrifft etwa Fälle, in denen die verfassungswidrige Anwendung einer Maßnahme nicht ausgeschlossen werden kann, das Gesetz aber keinen Zweifel daran lässt, was es als verfassungskonforme Anwendung verstanden wissen möchte. Dann kann gegebenenfalls ein vorübergehender „Leerlauf" praktisch nicht verfassungsgemäß anwendbarer Normenteile in Kauf genommen werden.[39] In ihrer gegenwärtigen Ausgestaltung bildet die Online-Durchsuchung aber die durch das Gericht aufgestellten Voraussetzungen nicht hinreichend ab und schafft stattdessen die Voraussetzungen für eine systematisch verfassungswidrige alltägliche Anwendung.

Zu berücksichtigen ist auch, dass die Online-Durchsuchung den Zugriff auf Daten ermöglicht, die den Ermittlern größtenteils bereits durch weniger eingriffsintensive Mittel zur Verfügung stehen. Die Durchsuchung nach den §§ 102 ff. StPO und die Beschlagnahme nach den §§ 94 ff. StPO zielen weitgehend auf den selben Datenbestand ab, erfolgen aber offen und sind deshalb mit einem effektiven Rechtsschutz für die Betroffenen und einem weniger schwerwiegenden Grundrechtseingriff verbunden. Die Überwindung von Verschlüsselungstechnologien hängt nicht grundsätzlich von der Heimlichkeit des Eingriffs ab. Ein unbemerkter Zugriff auf einen derart vielfältigen und sensiblen Datenbestand mag unter Gesichtspunkten der Gefahrenabwehr im Einzelfall für zulässig gehalten werden. Im Strafverfahren werden die durch den heimlichen externen Zugriff gewährten Vorteile bei einem Großteil der vorgesehenen Anlassdelikte nicht in einem angemessenen Verhältnis zu der damit verbundenen gravierenden Eingriffsintensivierung stehen. Der Strafprozess gebietet keine Wahrheitserforschung um jeden Preis.[40]

Zudem gehen mit der Funktionsweise der Online-Durchsuchung nicht nur Vorteile, sondern auch erhebliche Nachteile für die Beweiserhebung einher. Denn um unbemerkt auf ein gesichertes informationstechnisches System zuzugreifen, müssen technische Schutzlücken dieses Systems ausgemacht und genutzt werden. Diese Lücken ermöglichen es, das System von außen so zu manipulieren, dass es entgegen der vorgesehenen Funktionsweise die eingespeisten schädlichen Komponenten aufnimmt und selbst umsetzt. Es handelt sich dabei um eine Manipulation eben jenes Datensystems, das Ziel der Beweiserhebung sein soll, und damit um eine Manipulation des zu erhebenden Beweismittels. Bei dieser neuen Form informationstechnischer Eingriffe kann nicht länger wie bei klassischeren Ermittlungsmaßnahmen ohne Weiteres zwischen der kompromittierten Schutzhülle (etwa Wohnung, Fahrzeug) und den darin enthaltenen Gegenständen oder sich abspielenden Vorgängen differenziert werden. Der Inhalt des angegriffenen Systems verändert sich mit dem Angriff. Diese Problematik beruht auf einer Kernerkenntnis der digitalen Forensik, dem sog. „Lying Endpoint Problem": Der Zustand eines Informationssystems kann nicht auf diesem System selbst ermittelt werden, da nie ausgeschlossen werden kann, dass auch die Zustandsinformation

---

[39] Vgl. BVerfGE 141, 220 (311 f.).

[40] Vgl. BVerfG, Beschluss v. 24.02.2011 – 2 BvR 1596/10 –, Rn. 10; BGHSt 51, 285 (289 f.); Schmitt, in: Meyer-Goßner / Schmitt, Strafprozessordnung (60. Aufl. 2017), Einl. Rn. 50.

manipuliert worden ist.[41] Der Beweiswert eines auf diese Art erhobenen Beweismittels muss folglich grundsätzlich als gering betrachtet werden, was den Nutzen der Erhebungsmaßnahme als solche schmälert und in die Abwägung ihrer Angemessenheit mit einfließt.

Zuletzt trägt zur Unverhältnismäßigkeit des Eingriffs die unzureichende Ausgestaltung des Schutzes von Berufsgeheimnisträgern und ihren Berufshelfern in § 100d Abs. 5 StPO bei. Die Norm sieht für Berufsgeheimnisträger im Sinne des § 53 Abs. 1 StPO ein absolutes Beweiserhebungsverbot vor, während bezüglich ihrer Berufshelfer im Sinne des § 53a Abs. 1 StPO lediglich ein relatives Beweisverwertungsverbot gilt. Diese Differenzierung verkennt, dass die auch nach Ansicht des Gesetzgebers absolut schützenswerte vertrauliche Kommunikation eines Beschuldigten mit einem Berufsgeheimnisträger unter Einsatz informationstechnischer Systeme in der Praxis regelmäßig über die Berufshelfer abgewickelt wird. Dies schließt auch den Austausch von Informationen ein, die den Kernbereich der besonders geschützten Beziehung zu einem Berufsgeheimnisträger betreffen. Konsequenterweise werden die Berufshelfer auch in § 160a Abs. 3 StPO den Geheimnisträgern gleichgestellt. Dass dem entgegenstehend für die Online-Durchsuchung auf die Regelungen zum Schutz von Berufsgeheimnisträgern bei der akustischen Wohnraumüberwachung zurückgegriffen wurde, kann schon deshalb nicht überzeugen, weil die Beziehung zum Beschuldigten selten durch Berufshelfer in der überwachten Wohnung ausgestaltet wird, bei der Nutzung informationstechnischer Systeme aber den Regelfall darstellen dürfte.[42] Der unkontrollierte Verkehr etwa des Strafverteidigers mit seinem Mandanten wird durch die Vorschrift in der gegenwärtigen Fassung nicht mehr effektiv gewährleistet.

b) Sog. Quellen-TKÜ

aa) Die sog. Quellen-TKÜ nach § 100a Abs. 1 S. 2 StPO dient im Gegensatz zur Online-Durchsuchung ihrer ursprünglichen Zwecksetzung nach nicht der Durchsuchung gespeicherter Daten, sondern stellt eine Vorbereitungsmaßnahme zur Ermöglichung der Überwachung verschlüsselter laufender Telekommunikation dar. Insofern soll ihre Rechtmäßigkeit nicht am Recht auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, sondern am Fernmeldegeheimnis aus Art. 10 Abs. 1 GG zu messen sein.[43] Diese Differenzierung ist aufgrund der technisch identischen, kaum wirksam einschränkbaren Zugriffsmethode beider Maßnahmen[44] problematisch und gilt auch nach der Rechtsprechung des Gerichts nur, wenn durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt ist, dass sich die Überwachung ausschließlich

[41] Vgl. Pohlmann / Riedel: Strafverfolgung darf die IT-Sicherheit im Internet nicht schwächen, in: Datenschutz und Datensicherheit, 42. Jg. (2018), H. 1, 37 (43 f.).
[42] Vgl. DAV: Stellungnahme Nr. 44/2017 des Deutschen Anwaltvereins durch den Ausschuss Strafrecht zur Formulierungshilfe der Bundesregierung für einen Änderungsantrag der Fraktionen CDU/CSU und SPD zu dem Gesetzentwurf der Bundesregierung (2017), S. 18 ff.
[43] BVerfGE 120, 274 (309).
[44] Neumann / Kurz / Rieger: Sachverständigenauskunft zum Änderungsantrag der Fraktionen CDU/CSU und SPD zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze (2017), S. 10.

auf Daten aus einem laufenden Kommunikationsvorgang beschränkt.[45] Sie greift deshalb nicht, soweit § 100a Abs. 1 S. 3 StPO die Durchsuchung aller auf dem System gespeicherten Daten nach abgeschlossenen Kommunikationsvorgängen zu deren nachträglichen Erhebung vorsieht. Denn hiermit wird die Begrenzung auf laufende Kommunikation aufgehoben, womit der Schutzbereich des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG betroffen ist.[46] Es handelt sich gleichsam um eine „kleine Online-Durchsuchung".[47] Gespeicherte Kommunikationsvorgänge können auch nicht mit laufender Kommunikation gleichgesetzt und dadurch aus dem Schutzbereich des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ausgenommen werden. Denn für die Eröffnung des Schutzbereichs ist es unerheblich, ob ein gespeicherter Datenbestand zur Sicherung aller beweiserheblichen Informationen oder nur eines bestimmten Informationstyps unter ihnen durchsucht wird. Von Bedeutung dürfte in diesem Zusammenhang auch die Tatsache sein, dass eine etwaige Differenzierung zwischen vor und nach dem Erlass einer Überwachungsanordnung gespeicherten Daten nur durch eine vorherige Gesamterfassung aller Daten und ihre vollständige Auswertung auf das Speicherdatum hin erreichbar ist,[48] was letztlich einer vollumfänglichen Durchsuchung gleichkommt.

bb) Soweit mit der Maßnahme nach § 100a Abs. 1 S. 3 StPO ein Eingriff in das Grundrecht auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme verbunden ist, kann weitgehend auf die obigen Ausführungen zur Online-Durchsuchung verwiesen werden (vgl. D. I. 2. Buchst. a). Auch bei der sog. Quellen-TKÜ ergeben sich aus der Durchsuchung des gesamten Datenbestandes sowie der Heimlichkeit der Maßnahme, der manipulativen Natur der Beweiserhebung und der mit den technischen Methoden einhergehenden Gefahren die für die Online-Durchsuchung dargelegten Anforderungen. Ausgehend von den bisher durch das Gericht entwickelten Kriterien zu gefahrenabwehrrechtlichen Eingriffen in das Grundrecht auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und den Rechtfertigungsgrundsätzen repressiver Eingriffe genügt auch die sog. Quellen-TKÜ, soweit sie den Zugriff auf gespeicherte Daten erlaubt, nicht den verfassungsrechtlichen Anforderungen. Der in § 100a Abs. 2 StPO enthaltene Katalog an Taten, die unter den sonstigen Voraussetzungen des Abs. 1 S. 1 eine Überwachung erlaubt, ist noch erheblich weiter als der bereits zu weite Katalog des § 100b Abs. 2 StPO und knüpft erkennbar nicht am Schutz von überragend wichtigen Rechtsgütern an. Er enthält eine Vielzahl an Taten, die bereits ihrem Strafrahmen nach nicht als besonders schwer einzustufen sind und Höchststrafen von nicht mehr als fünf Jahren androhen. Dass die sog. Quellen-TKÜ einen engeren Erhebungszweck verfolgt, kann dies nicht auffangen. Zum einen betrifft die Durchsuchung nach gespeicherten Daten dennoch

---

[45] BVerfGE 141, 220 (309); 120, 274 (309).
[46] Singelnstein / Derin: Das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens, in: NJW 2018, 2646 (2648).
[47] Sinn: Stellungnahme zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze sowie zur Formulierungshilfe der Bundesregierung für einen Änderungsantrag zum o.g. Gesetzentwurf (2017), S. 5.
[48] BT-Drs. 18/12785, S. 55.

das gesamte System, zum anderen wiegt die Auswertung der gesamten gespeicherten Kommunikation besonders schwer[49].

c) Anwendung auf nichtverdächtige Dritte

Nicht mit Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG vereinbar ist insbesondere die Anwendung der Maßnahmen nach §§ 100a Abs. 1 S. 2 und 3, 100b Abs. 1 StPO auf Dritte nach §§ 100a Abs. 3, 100b Abs. 3 S. 2 StPO. Der Zugriff auf informationstechnische Systeme greift derart intensiv in die Privatsphäre der Betroffenen ein, dass entsprechende Maßnahmen nicht auf nichtverdächtige Dritte ausgedehnt werden dürfen. Systeme Dritter dürfen nur insoweit Ziel der Durchsuchung bzw. der die Überwachung ermöglichenden Infiltration sein, wie dies unvermeidbar ist und tatsächliche Anhaltspunkte dafür bestehen, dass die Zielperson dort ermittlungsrelevante Daten speichert.[50] § 100b Abs. 3 S. 2 Nr. 1 StPO lässt hingegen ebenso wie § 100a Abs. 3 StPO die Annahme genügen, dass der Beschuldigte das System des Dritten benutze. Der bloße Verdacht der Mitnutzung sagt jedoch noch nichts darüber aus, ob der Beschuldigte auch Daten auf dem System speichert. Im Gegenteil dient der Zugriff dann gerade dazu, erst festzustellen, ob sich Daten des Beschuldigten auf dem System befinden. Eine solche mit dem Absenken der Voraussetzungen verbundene Vorverlagerung des Eingriffs ist verfassungswidrig. Soweit hierdurch der nichtverdächtige Dritte zum objektivierten Werkzeug der staatlichen Strafverfolgung gemacht wird, liegt darüber hinaus eine Verletzung von Art. 1 Abs. 1 GG vor.

II. Art. 1 Abs. 1 GG

Die Vorschriften sowohl zur Online-Durchsuchung als auch zur sog. Quellen-TKÜ sind in ihrer jetzigen Ausgestaltung nicht mit Art. 1 Abs. 1 GG vereinbar.

1. Kernbereichsschutz

a) §§ 100a Abs. 1 S. 3, 100b Abs. 1 StPO erlauben schwere Eingriffe in informationstechnische Systeme. Angesichts der Bedeutung solcher Systeme für die Persönlichkeitsentfaltung geht ein solcher Eingriff typischerweise mit der Gefahr der Erfassung höchstpersönlicher Daten aus dem Kernbereich privater Lebensgestaltung einher.[51] Unter dem Gesichtspunkt der Menschenwürde darf der Staat in diese Sphäre schlichtweg nicht eindringen, weshalb verletzungsgeneigte Maßnahmen unter dem Vorbehalt angemessener Vorkehrungen zum Kernbereichsschutz stehen.

---

[49] Vgl. BVerfGE 141, 220 (310).
[50] BVerfGE 141, 220 (273 f.).
[51] BVerfGE 141, 220 (306); 120, 274 (335 ff.).

b) Der Schutz des Kernbereichs wird für die Online-Durchsuchung in § 100d Abs. 1 bis 3, Abs. 5 StPO geregelt. § 100d Abs. 1 StPO sieht insofern die Unzulässigkeit der Maßnahme vor, wenn Anhaltspunkte dafür bestehen, dass allein Erkenntnisse aus dem Kernbereich erlangt werden würden, während § 100d Abs. 3 StPO verlangt, nach Möglichkeit technisch sicherzustellen, dass den Kernbereich betreffende Daten gar nicht erst erhoben werden, und sie andernfalls unverzüglich zu löschen. Diese Regelung wird den strikten Anforderungen an den Schutz des Kernbereichs privater Lebensgestaltung im Sinne des Art. 1 Abs. 1 GG nicht gerecht. Dabei ist zwischen der Erhebungs- und der Verwertungsebene zu unterscheiden.

Für die Erhebung gilt, dass höchstsensible Daten in der Realität der alltäglichen Datennutzung weder als solche deklariert noch grundsätzlich von sonstigen Daten getrennt aufbewahrt werden. Im Gegenteil ergibt sich der höchstpersönliche Charakter von Daten oftmals gerade aus der Summe einzelner Datenbestände, die es in ihrer Gesamtheit ermöglichen, ein umfassendes Persönlichkeitsbild des Betroffenen zu erstellen. Auf dieser Erkenntnis basiert etwa die gesamte moderne Datenindustrie, die kostenlose Angebote wie soziale Netzwerke, Suchmaschinen, Videoplattformen und Kurznachrichtendienste bereitstellt, um die von den Nutzern zur Verfügung gestellten Daten auszuwerten und auf deren Basis hochpräzise individuelle Kundenprofile zu entwerfen, welche die Wünsche, Träume und Bedürfnisse des einzelnen Nutzers oftmals besser verstehen und vorherzusagen vermögen als dieser selbst. Daraus ergibt sich nicht, dass eine Erfassung intimer Daten mangels Differenzierbarkeit in Kauf genommen werden darf. Es folgt vielmehr die Pflicht, einer Erhebung von Daten mit Kernbereichsbezug so weitgehend wie möglich vorzubeugen.[52] Erforderlich ist deshalb eine dem § 100d Abs. 4 StPO vergleichbare Regelung, die Anhaltspunkte dafür voraussetzt, dass durch die konkrete Anwendung der Maßnahme dem Kernbereich zuzurechnende Daten nicht erfasst werden.[53] Dies liegt nahe, da eine heimliche und ohne Einverständnis erfolgende Gesamterhebung aller auf den informationstechnischen Systemen eines Betroffenen gespeicherter Daten jedenfalls in ihrem Gewicht nicht nur mit dem Eindringen in eine Wohnung und dem Schutzbereich des Art. 13 Abs. 1 GG vergleichbar ist,[54] sondern in vielerlei Hinsicht noch darüber hinaus geht.

Kann auf der Erhebungsebene nicht vollständig vermieden werden, dass durch einen Zugriff auf informationstechnische Systeme auch höchstpersönliche Daten miterfasst werden, ist der unverändert hohe Schutzbedarf der Betroffenen durch umso zuverlässigere Sicherungen auf der Verwertungsebene in Anschlag zu bringen.[55] Dazu ist zu gewährleisten, dass erfasste kernbereichsrelevante Daten so frühzeitig ausgefiltert werden, dass sie den Sicherheitsbehörden nach Möglichkeit gar nicht erst zur Kenntnis gelangen.[56] Dies setzt die Kontrolle durch eine externe und unabhängige Stelle voraus. Eine solche externe Kontrolle ist in den angegriffenen Normen nicht vorgesehen. Die angegriffenen

---

[52] BVerfGE 120, 274 (337).
[53] Singelnstein / Derin: Das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens, in: NJW 2018, 2646 (2647).
[54] BVerfGE 141, 220 (304).
[55] BVerfGE 141, 220 (307).
[56] BVerfGE 141, 220 (307); 120, 274 (338 f.).

Vorschriften treffen somit nicht die verfassungsrechtlich erforderlichen Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung.

c) Für die Telekommunikationsüberwachung ist die Miterfassung kernbereichsrelevanter Informationen – trotz hoher Kernbereichsnähe – gemeinhin weniger typusprägend als für die Online-Durchsuchung. Die sog. Quellen-TKÜ nach § 100a Abs. 1 S. 2 und 3 StPO ist allerdings aufgrund der ihr zugrunde liegenden technischen Methode mit einem für herkömmliche Kommunikationsüberwachungsmaßnahmen ungewöhnlich tiefen Eingriff in die Privatsphäre der Betroffenen verbunden, da sie mit einer Infizierung eines informationstechnischen Systems und dem Eindringen in selbiges einhergeht. Die Funktionsweise der sog. Quellen-TKÜ macht es darüber hinaus erforderlich, nicht nur den aktiven Kommunikationsvorgang, sondern durchweg das gesamte System zu überwachen, um auf die Aktivierung einer Kommunikationsanwendung mit der Aufzeichnung reagieren zu können. Zudem erlaubt die Vorschrift in ihrer jetzigen Fassung auch die Durchsuchung des Systems nach gespeicherten Kommunikationsvorgängen. Die Anforderungen an den Kernbereichsschutz sind daher eher im Bereich der Online-Durchsuchung als bei der herkömmlichen TKÜ anzusiedeln. Die Vorkehrungen des § 100d Abs. 1 und 2 StPO sind hierfür nicht ausreichend. Insbesondere setzen sie keinerlei technische Sicherungen voraus, um die Erhebung von Daten aus dem Kernbereich privater Lebensgestaltung zu vermeiden. Auch eine Sichtung durch eine unabhängige Kontrollstelle ist nicht vorgesehen. Das Gericht hat bezüglich jeder Form der Kommunikationsüberwachung die Pflicht zur Sichtung durch eine unabhängige Stelle davon abhängig gemacht, in welchem Ausmaß mit einer Erfassung höchstprivater Informationen zu rechnen ist. Jedenfalls dann, wenn der Gesetzgeber die Erhebung von Informationen erlaubt, für die Zweifel bestehen können, ob sie dem Kernbereich privater Lebensgestaltung unterfallen, bedarf es demnach für solche Aufzeichnungen der Sichtung durch eine unabhängige Stelle.[57]

2. Umfassende Persönlichkeitsprofile

Mit der grundgesetzlich garantierten Würde des Menschen nicht vereinbar ist insbesondere die mit der Online-Durchsuchung nach § 100b Abs. 1 StPO geschaffene Möglichkeit der Erstellung von Persönlichkeitsprofilen. Das systematische Erheben einer Vielzahl von Informationen zu einer Person, die es erlauben, durch ihre Zusammenstellung ein umfassendes Bild der Persönlichkeit zu erstellen, ist unzulässig. Durch eine solche Registrierung in seiner ganzen Persönlichkeit würde der Mensch in den Händen des Staates zum Objekt.[58] Eine Datenerhebung lässt die Würde des Erfassten nur dann unangetastet, wenn sie sich auf die Abbildung einzelner Lebensbereiche beschränkt, ohne deren Verknüpfung zu einem Totalabbild zu ermöglichen.[59] Gerade ein derartiges Totalabbild geht aber mit einer Gesamterhebung der auf persönlichen informationstechnischen Systemen gespeicherten Daten

[57] BVerfGE 141, 220 (314).
[58] BVerfGE 27, 1 (6).
[59] BVerfGE 65, 1.

einher und lässt den Bürger gleichsam gläsern vor dem Blick des Staates werden. Dies liegt vor allem an der großen Vielfalt an Daten aus allen Lebensbereichen, welche sich heute – als Konsequenz der technologischen Fortschritte der letzten Jahrzehnte – auf informationstechnischen Systemen regelmäßig vereint findet.[60] So hat der Europäische Gerichtshof zuletzt zur Vorratsdatenspeicherung festgestellt, dass schon die dort erhobenen (hinter der Online-Durchsuchung zurückbleibenden) Daten die Erstellung umfassender Persönlichkeitsprofile ermöglichen.[61] Auch der bereits angesprochene enorme wirtschaftliche Wert persönlicher Daten für die sie verarbeitende Werbe- und Datenindustrie beruht auf nichts anderem als ihrer Eignung zur Erstellung umfassender Persönlichkeitsbilder.
Es folgt, dass der mit § 100b Abs. 1 StPO verbundene Zugriff durch den Gesetzgeber streng auf die Suche nach bestimmten Beweismitteln zu beschränken ist, um eine Erstellung von Persönlichkeitsprofilen zu unterbinden. Die Maßnahme darf nicht dazu genutzt werden, die Betroffenen in der Hoffnung auf weitere Ermittlungsansätze komplett zu durchleuchten. Eine solche Nutzung lässt sich mangels hinreichender Nachvollziehbarkeit gegenwärtig nicht ausschließen.

III. Art. 19 Abs. 4 GG

Die §§ 100a Abs. 1 S. 2 und 3, Abs. 5 und 6, 100b Abs. 1 StPO verstoßen gegen Art. 19 Abs. 4 GG und die Garantie effektiven Rechtsschutzes. Im Gegensatz zu bisherigen vergleichbaren Maßnahmen erfolgen die Online-Durchsuchung und sog. Quellen-TKÜ zu Zwecken der Strafverfolgung. Insofern dienen die Maßnahmen ganz überwiegend der Erhebung von Beweismitteln. Während Wohnungsdurchsuchungen oder die heimliche Installation von Überwachungstechnik in Wohnungen keinen Einfluss auf die dort aufzufindenden potentiellen Beweismittel nehmen und dazu von Vorkehrungen begleitet werden, die ihre Kontrolle und Nachvollziehbarkeit ermöglichen, stellt sich dies für die Online-Durchsuchung und die sog. Quellen-TKÜ anders dar. Wie bereits ausgeführt, müssen Schutzlücken dieses Systems ausgemacht und genutzt werden, die eine Manipulation des Systems und damit der zu erhebenden Beweismittel ermöglichen. Da der Inhalt des angegriffenen Systems sich mit dem Angriff verändert, kann die Garantie effektiven Rechtsschutzes nicht als erfüllt angesehen werden, solange nicht wirksame Vorkehrungen getroffen werden, anhand derer die Bewegungen der Ermittler innerhalb des Systems nachvollziehbar werden. Diesen Anforderungen genügen die Regelungen der §§ 100a Abs. 5 und Abs. 6, 100b Abs. 4 StPO nicht, da sie diese Nachvollziehbarkeit nicht im erforderlichen Umfang herzustellen vermögen. Die Sicherungsmaßnahmen nach § 100a Abs. 5 StPO lassen sich, soweit sie sich technisch überhaupt umsetzen lassen, mangels einer Veröffentlichung des eingesetzten Quellcodes nicht überprüfen. Die Protokollierungspflichten nach § 100a Abs. 6 StPO ermöglichen es nicht, nachträglich die

[60] Singelnstein / Derin: Das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens, in: NJW 2018, 2646 (2647).
[61] EuGH, Urteil v. 21.12.2016, C □203/15 und C □698/15, Rn. 99.

durchsuchten Daten nachzuvollziehen.[62] Schwer wiegt auch hier insbesondere das Fehlen einer unabhängigen Kontrollstelle. Es fehlen zudem weitgehend Vorgaben zur technischen Ausgestaltung der einzusetzenden Exploits und Trojaner, die einen grundrechtskonformen Einsatz zu gewährleisten versuchten.

IV. Art. 10 Abs. 1 GG

Soweit die Maßnahme der sog. Quellen-TKÜ nach § 100a Abs. 1 S. 2 StPO nicht an Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, sondern am Fernmeldegeheimnis des Art. 10 Abs. 1 GG zu messen ist, werden sie auch dessen Anforderungen nicht gerecht. Die sog. Quellen-TKÜ ist aufgrund ihrer ganz spezifischen Funktionsweise, die eine heimliche Infiltration eines informationstechnischen Systems mit Schadsoftware und seine ununterbrochene Überwachung auf die Aktivierung von Kommunikationsanwendungen hin voraussetzt, nicht ohne Weiteres mit den durch herkömmliche TK-Überwachung einhergehenden Eingriffen gleichzusetzen. Ihr kommt eine wesentlich erhöhte Eingriffsintensivität zu. Gleichzeitig reduziert die manipulative Einwirkung auf das Beweismittel seinen Beweiswert. Deshalb ist im Sinne der Verhältnismäßigkeit eine Beschränkung auf Verdachtsfälle erheblicher Straftaten zwingend vorzunehmen. Der Straftatenkatalog des § 100a Abs. 2 StPO konstituiert hingegen einen Anwendungsbereich von beträchtlicher Breite, der die Eingriffsschwelle unzulässig niedrig ansetzt.

Auch bei Annahme eines Eingriffs ausschließlich in Art. 10 Abs. 1 GG sind die Regelungen zum Kernbereichsschutz in § 100d Abs. 1 und 2 StPO nicht ausreichend. Das Einschleusen eines Trojaners auf das informationstechnische System geht – erst recht in Anbetracht der wiederholt festgestellten Unzuverlässigkeit technischer Zugriffsbeschränkungen – mit einem großen Risiko der versehentlichen oder missbräuchlichen Erfassung weiterer, auch dem Kernbereich privater Lebensgestaltung zuzuordnenden Daten einher. Dies gebietet weitergehende, insbesondere schon die Erhebung entsprechender Informationen verhindernde Vorkehrungen zum Kernbereichsschutz.

V. Art. 12 Abs. 1 GG

Die Vorschriften der §§ 100a Abs. 1 S. 2 und 3, 100b Abs. 1 StPO, bzgl. des als Rechtsanwalt tätigen Beschwerdeführers zu 4 zudem 100d Abs. 5 StPO, verletzen die Beschwerdeführer in ihrer Berufsfreiheit aus Art. 12 Abs. 1 GG.

---

[62] Vgl. insofern die Forderungen bei Neumann / Kurz / Rieger: Sachverständigenauskunft zum Änderungsantrag der Fraktionen CDU/CSU und SPD zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze (2017), S. 15 ff.

Die Tätigkeiten der Beschwerdeführer sind auf Dauer angelegt und dienen der Schaffung und Aufrechterhaltung einer Lebensgrundlage, sie unterfallen dem Schutzbereich der Berufsfreiheit.
Die angegriffenen Vorschriften greifen in die Berufsausübungsfreiheit der Beschwerdeführer ein. Neben unmittelbar auf eine Einschränkung der Berufsausübung zielenden Maßnahmen schützt die Berufsfreiheit auch vor solchen belastenden Maßnahmen, die einen spezifischen Berufsbezug in Form einer zumindest objektiv berufsregelnden Tendenz aufweisen oder die in ihren tatsächlichen Auswirkungen zu einer Beeinträchtigung der freien Berufsausübung führen.[63] Die Beschwerdeführer zu 1-3 sind beruflich mit dem Schutz von IT-Systemen vor Schadprogrammen und Infiltration befasst. Sie sind zur Entwicklung und Umsetzung solcher Schutzvorkehrungen sowie zur Kommunikation im Hochsicherheitsbereich selbst maßgeblich auf die Nutzung und Vertraulichkeit von IT-Systemen angewiesen. Die angegriffenen Ermittlungsbefugnisse greifen damit die spezifischen Arbeitsmittel der Beschwerdeführer an. Zudem besteht ein erheblicher Aspekt ihrer beruflichen Tätigkeit darin, die Aufklärung von Sicherheitslücken zu fördern und das Schließen von Schwachstellen zu gewährleisten. Hierin werden sie durch die angegriffenen Vorschriften beeinträchtigt, denn diese setzen ein staatliches Konterkarieren solcher Bemühungen und die Etablierung des Staates als Konkurrenten auf dem Schwachstellenmarkt voraus. Der Beschwerdeführer zu 4 ist als Angehöriger der freien Advokatur ganz besonders auf eine vertrauliche Beziehung zu Mandanten angewiesen, die durch heimliche Überwachungsmaßnahmen wie die Online-Durchsuchung und die sog. Quellen-TKÜ gefährdet wird. Die Möglichkeit solcher Maßnahmen kann potentielle Mandanten davon abhalten, sich an einen Rechtsanwalt zu wenden, und so schwerwiegende Folgen für die freie Berufsausübung verursachen. Hinsichtlich der Zeugnisverweigerungsrechte des § 100d Abs. 5 StPO wird die Rechtsstellung des Beschwerdeführers zu 4 speziell als Rechtsanwalt geregelt.
Der hier erfolgende Eingriff genügt dem Grundsatz der Verhältnismäßigkeit nicht. Er ist insbesondere nicht angemessen. Die Berufsfreiheit ist ein Grundrecht höchsten Ranges. Online-Durchsuchung und sog. Quellen-TKÜ konstituieren in ihrer Anwendung schwerwiegende Eingriffe in die Freiheit, den Beruf uneingeschränkt auszuüben. Dies betrifft sowohl die Gefahr, von solchen Maßnahmen miterfasst oder selbst zu ihrem Ziel zu werden, als auch die mit der Funktionsweise der Ermittlungsmaßnahmen verbundene allgemeine Schwächung des Sicherheitsniveaus informationstechnischer Systeme, der in der gegenwärtigen Ausgestaltung nicht hinreichend Rechnung getragen wird. Die Regelung zu den Zeugnisverweigerungsrechten des § 100d Abs. 5 StPO differenziert zudem unzulässig zwischen Berufsgeheimnisträgern und ihren Berufshelfern (vgl. D. I. 2. a) cc)) und beschädigt damit das für die Berufsausübung unentbehrliche Vertrauensverhältnis zwischen Rechtsanwalt und Mandant in einer Weise, die durch die verfolgten Zwecke nicht gerechtfertigt wird.

[63] Vgl. BVerfGE 110, 226 (254) m.w.N.

VI. Vereinbarkeit mit der Charta der Grundrechte der Europäischen Union

1. Anwendbarkeit

a) Die Charta der Grundrechte der Europäischen Union ist auf den vorliegenden Sachverhalt unmittelbar anwendbar. Die Anwendbarkeit der Charta bemisst sich nach Art. 51 EuGrCh. Eine Bindungswirkung für die Mitgliedsstaaten besteht gem. Art. 51 Abs. 1 S. 1 EuGrCh, soweit diese das Recht der Union durchführen. Nach der Rechtsprechung des Europäischen Gerichtshofs ist dies dann der Fall, wenn eine Handlung in den Geltungsbereich des Unionsrechts fällt.[64] Diese Voraussetzungen sind nach der Rechtsprechung des Bundesverfassungsgerichts dann nicht gegeben, wenn das gegenständliche nationale Handeln aus dem Anwendungsbereich einer in Betracht kommenden europäischen Richtlinie herausfällt und deshalb nicht explizit durch Unionsrecht determiniert ist.[65] Es handelt sich dann nicht mehr um eine unionsrechtlich geregelte Fallgestaltung, auf die eine Anwendung der europäischen Grundrechte zu beschränken ist.

b) Entscheidend ist hier insoweit, ob die Einführung der Online-Durchsuchung und sog. Quellen-TKÜ in die Strafprozessordnung dem Regelungsbereich einer europäischen Richtlinie angehören. Dies ist der Fall. Die heimliche Infiltration informationstechnischer Systeme und die Überwachung der Online-Telekommunikation sind Gegenstand der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation. Betroffen ist insbesondere die sich aus der Richtlinie ergebende staatliche Pflicht zur Garantie der Vertraulichkeit mittels öffentlicher Kommunikationsnetze und -dienste versandter Nachrichten aus Art. 5 Abs. 1 der Richtlinie.

Die Maßnahmen werden auch nicht als Ausnahme im Sinne des Art. 15 Abs. 1 und Art. 1 Abs. 3 der Richtlinie aus ihrem Anwendungsbereich ausgeschlossen. Art. 15 Abs. 1 der Richtlinie 2002/58/EG erlaubt die Beschränkung der Rechte aus Art. 5, 6, 8 Abs. 1-4 sowie Art. 9 dieser Richtlinie, sofern eine solche Beschränkung gemäß Artikel 13 Abs. 1 der Richtlinie 95/46/EG für die nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist, wobei gem. Art. 15 Abs. S. 3 der Richtlinie alle Maßnahmen stets den allgemeinen Grundsätzen des Gemeinschaftsrechts (und damit auch der Charta) genügen müssen. Der Europäische Gerichtshof hat insofern im Wege der systematischen Richtlinienauslegung festgestellt, dass Art. 15 Abs. 1 und Art. 1 Abs. 3 der Richtlinie 2002/58/EG die genannten Bereiche nicht vom Geltungsbereich ausschließen, sondern vielmehr erst die Kriterien festlegen, unter denen eine in Art. 1 Abs. 3 der Richtlinie genannte Tätigkeit vom Anwendungsbereich

---

[64] EuGH, Urteil v. 26.02.2013, C-617/10 (Åkerberg Fransson), Rn. 19 m.w.N.
[65] BVerfGE 133, 277 (313 ff.).

ausgenommen werden kann.[66] Art. 15 Abs. 1 setzt nämlich zwangsläufig voraus, dass die dort genannten nationalen Vorschriften, etwa für Zwecke der Kriminalitätsbekämpfung, in den Geltungsbereich der Richtlinie fallen. Die hier gegenständlichen Vorschriften der Online-Durchsuchung und sog. Quellen-TKÜ sind zwar solche der Strafverfolgung im Sinne des Art. 15 Abs. 1 der Richtlinie, müssen aber aufgrund ihrer Beschränkung von in der Richtlinie garantierten Rechten den Anforderungen der Charta genügen müssen und hierzu die Voraussetzungen der Notwendigkeit, Angemessenheit und Verhältnismäßigkeit zu erfüllen haben.

2. Konsequenzen für die verfassungsrechtliche Bewertung der angegriffenen Vorschriften

Die Grundrechte der Charta stellen übergeordnetes Unionsrecht dar. Als solches können sie zwar gem. Art. 53 EuGrCh den Schutzbereich nationaler Grundrechte nicht einschränken. Sofern sie aber in der Schutzgewährung über diesen hinausgehen, bleibt für diesen Schutzüberschuss der Anwendungsvorrang erhalten. Hieraus ergeben sich verschiedene Möglichkeiten der Gewährleistung dieses Schutzes. Die Frage der genauen Reichweite der Grundrechte der Charta löst, sofern sie umstritten ist, grundsätzlich die Vorlagepflicht gem. Art. 267 Abs. 3 AEUV aus. Gelangt das Gericht hingegen zu der Auffassung, die richtige Anwendung des Unionsrechts sei entsprechend der acte-claire-Doktrin derart offenkundig, dass keinerlei Raum für vernünftige Zweifel verbleibe,[67] lässt sich der Schutzüberschuss der Charta in Erweiterung der Grundrechte des Grundgesetzes unmittelbar zur Geltung bringen. Art. 23 Abs. 1 GG enthält ein Wirksamkeits- und Durchsetzungsversprechen für das unionale Recht,[68] das insoweit dazu dienen kann, den Grundrechten der Charta gerecht zu werden.

3. Vereinbarkeit mit den unionsrechtlichen Vorgaben

a) Die mit der Online-Durchsuchung nach § 100b Abs. 1 StPO und der sog. Quellen-TKÜ nach § 100a Abs. 1 S. 2 und 3 StPO verbundenen Zugriffe auf informationstechnische Systeme – sowohl in der Infiltration des Systems zur Zugriffsverschaffung als auch in der Durchsuchung der Datenbestände – stellen besonders schwerwiegende Eingriffe insbesondere in die Grundrechte auf Achtung des Privatlebens aus Art. 7 und den Schutz personenbezogener Daten nach Art. 8 Abs. 1 EuGrCh dar.

So hat der Europäische Gerichtshof zur Vorratsdatenspeicherung ausgeführt, ein Eingriff in diese Rechte sei als besonders schwerwiegend anzusehen, wenn aus der Gesamtheit der Daten sehr genaue Schlüsse auf das Privatleben gezogen werden können, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende

[66] EuGH, Urteil v. 21.12.2016, C-203/15 (Post- och telestyrelsen), Rn. 73.
[67] EuGH, Urteil v. 06.10.1982, C-283/81 (CILFIT), Rn. 10 ff.
[68] BVerfGE 140, 317 (335).

Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen und das soziale Umfeld.[69] Denn solche Daten ermöglichen insbesondere die Erstellung des Profils der betroffenen Personen.[70] Die Online-Durchsuchung und die mit der sog. Quellen-TKÜ verbundene „kleine Online-Durchsuchung" erlauben ohne Schwierigkeiten genau diese Schlüsse. Der Umstand, dass die Maßnahme heimlich durchgeführt wird und eine Benachrichtigung regelmäßig erst nach vielen Monaten oder sogar Jahren (wenn überhaupt) erfolgt, sodass die Betroffenen nicht wissen, ob sie zu einem gegebenen Zeitpunkt überwacht werden, birgt zudem das Potential, das Gefühl einer ständigen Überwachung des Privatlebens zu erzeugen.[71] Zu berücksichtigen ist, dass der Europäische Gerichtshof seine strengen Kriterien ausdrücklich für Datenerhebungen entwickelt hat, die nicht den Inhalt einer Kommunikation betreffen und folglich nicht den Wesensgehalt der vorgenannten Grundrechte antasten.[72] Die hier gegenständlichen Maßnahmen zielen hingegen auch auf Kommunikationsinhalte ab und berühren damit sogar den Wesensgehalt der Rechte aus Art. 7 und 8 EuGrCh.

b) Die Online-Durchsuchung und die mit der sog. Quellen-TKÜ verbundene Erlaubnis zur Durchsuchung eines Systems nach gespeicherten Kommunikationsdaten können mit dem Wesensgehalt der Rechte aus Art. 7 und 8 EuGrCh nicht in Einklang gebracht werden. Die Ermöglichung der Erstellung von Profilen geht bei den vorgesehenen Eingriffsbefugnissen mit der Aufzeichnung der gesamten Kommunikation einher und damit über etwa mit der Vorratsdatenspeicherung verbundene Eingriffsintensivität weit hinaus. Ein derart schwerwiegender Eingriff kann angesichts der dargelegten Kriterien nicht gerechtfertigt werden und ist mit den unionsrechtlich garantierten Freiheiten grundsätzlich nicht vereinbar.

In jedem Fall können diese Maßnahmen nur zur Bekämpfung schwerster Straftaten zulässig sein. Die Kataloge der §§ 100a Abs. 2, 100b Abs. 2 StPO enthalten aber wie bereits ausgeführt keine Beschränkung auf schwere Straftaten, sondern nehmen im Gegenteil eine Vielzahl von Straftatbeständen leichter bis mittlerer Kriminalität auf. Es fehlt damit an der Verhältnismäßigkeit des Eingriffs.

Zwei einfache Abschriften anbei.

Starostik
Rechtsanwalt

Derin
Rechtsanwalt

[69] EuGH, Urteil v. 21.12.2016, C-203/15 (Post- och telestyrelsen), Rn. 99; Urteil v. 08.04.2014, C-293/12 (Digital Rights), Rn. 27.
[70] EuGH, Urteil v. 21.12.2016, C-203/15 (Post- och telestyrelsen), Rn. 99.
[71] Vgl. EuGH, Urteil v. 21.12.2016, C-203/15 (Post- och telestyrelsen), Rn. 100; Urteil v. 08.04.2014, C-293/12 (Digital Rights), Rn. 37.
[72] EuGH, Urteil v. 21.12.2016, C-203/15 (Post- och telestyrelsen), Rn. 101.