DeutscherAnwaltVerein

Stellungnahme

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 – Drucksache 18/11272 –

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

Stellungnahme Nr.: 44/2017 Berlin, im Juni 2017

Mitglieder des Ausschusses

- RA Dr. Rainer Spatscheck, München (Vorsitzender)
- RA Stefan Conen, Berlin
- RA Dr. h.c. Rüdiger Deckers, Düsseldorf
- RAin Dr. Margarete Gräfin von Galen, Berlin
- RAin Dr. Gina Greeve, Frankfurt am Main
- RA Prof. Dr. Rainer Hamm, Frankfurt am Main
- RA Eberhard Kempf, Frankfurt am Main
- RA Dr. Stefan Kirsch, Frankfurt am Main
- RA Prof. Dr. Stefan König, Berlin
- RAin Dr. Jenny Lederer, Essen
- RA Dr. Ali B. Norouzi, Berlin
- RAin Gül Pinar, Hamburg
- RA Michael Rosenthal, Karlsruhe
- RA Martin Rubbert, Berlin (Berichterstatter)
- RAin Dr. Heide Sandkuhl, Potsdam
- RA Prof. Dr. Gerson Trüg, Freiburg im Breisgau

Zuständig in der DAV-Geschäftsführung

- RAin Tanja Brexl, Berlin

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Verteiler

- Bundesministerium des Innern
- Bundesministerium der Justiz und für Verbraucherschutz
- Rechts- und Verbraucherschutzausschuss, Innenausschuss des Deutschen Bundestages
- Vorsitzenden des Rechts- und Verbraucherschutzausschusses des Deutschen Bundestages
- Vorsitzenden des Innenausschusses des Deutschen Bundestages
- Landesjustizministerien
- Rechts- und Innenausschüsse der Landtage
- Bundesgerichtshof
- Bundesanwaltschaft

- Vorstand des Deutschen Anwaltvereins
- Landesverbände des Deutschen Anwaltvereins
- Vorsitzende der Gesetzgebungsausschüsse des Deutschen Anwaltvereins
- Strafrechtsausschuss des Deutschen Anwaltvereins
- Geschäftsführender Ausschuss der Arbeitsgemeinschaft Strafrecht des Deutschen Anwaltvereins
- Strafrechtsausschuss der Bundesrechtsanwaltskammer
- Vorsitzende des Strafrechtsausschusses des KAV, BAV
- Vorsitzende des FORUM Junge Anwaltschaft des DAV

- Deutscher Strafverteidiger e. V.
- Regionale Strafverteidigervereinigungen
- Organisationsbüro der Strafverteidigervereinigungen und -initiativen

- Arbeitskreise Recht der im Bundestag vertretenen Parteien
- Deutscher Richter
- Bund Deutscher Kriminalbeamter

- Strafverteidiger-Forum (StraFo)
- Neue Zeitschrift für Strafrecht, NStZ
- Strafverteidiger
- Juris
- KriPoZ Kriminalpolitische Zeitschrift

- Prof. Dr. Jürgen Wolter, Universität Mannheim
- ver.di, Bereich Recht und Rechtspolitik
- Deutscher Juristentag (Präsident und Generalsekretär)
- Prof. Dr. Schöch, LMU München

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV mit derzeit ca. 65.000 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

Der Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze (Bundestagsdrucksache 18/11272) vom 22.02.2017 wurde durch den Änderungsantrag der Fraktionen der CDU/CSU und SPD im laufenden Gesetzgebungsverfahren erheblich erweitert.

Ging es zuvor – und im Rahmen einer Anhörung im Rechtsausschuss – um die Frage des Fahrverbots als allgemeine Sanktion und den Richtervorbehalt bei der Blutentnahme, hat der Entwurf nunmehr einen völlig neuen Schwerpunkt mit der Einführung der „Quellen-TKÜ“ und der „Online-Durchsuchung“. Einzige Verbindung zum ursprünglichen Gesetzesentwurf ist die geplante Veränderung der StPO – aber an völlig anderer Stelle und ohne jeden inhaltlichen Bezug zum ursprünglichen Gesetzesentwurf. Es stellt sich bereits die Frage, ob dieser „Änderungsantrag“ ein Änderungsantrag im Sinne des § 82 Abs. 1 GO BT ist. Änderungsanträge zu Gesetzesanträgen knüpfen an „die vom federführenden Ausschuss empfohlenen Formulierungen“ an.[1] Ob dies bei der Einfügung völlig andere Rechtsfragen betreffende „Änderungsanträge“ noch der Fall ist, erscheint zumindest fraglich. Immerhin soll durch den Änderungsantrag der „Staatstrojaner“ in die StPO eingeführt werden.

Der Entwurf geht in seiner Bedeutung weit über die bisher im Entwurf enthaltenen Regelungen hinaus. Die neuen Regelungen dürften an Eingriffstiefe und Konsequenzen den bereits sehr umstrittenen „großen Lauschangriff“ noch deutlich überbieten. Angesichts dieser Eingriffstiefe ist das von der Bundesregierung und den Regierungsparteien gewählte Verfahren („Änderungsantrag der Fraktionen CDU/CSU und SPD“[2]) scharf zu kritisieren. Der begründete Eindruck, ein gravierender Grundrechtseingriff werde bewusst in einem Änderungsantrag versteckt, um ohne Diskussion

---

1 https://www.bundestag.de/service/glossar/glossar/A/aend_antraege/245336
2 vgl. Änderungsantrag, S. 1

und mit großer Eile durchgesetzt zu werden, ist nicht von der Hand zu weisen. Diese Eile ist weder geboten noch – angesichts einer Reihe von verfassungsrechtlichen Problemen und offenen Fragen in der Sache – tunlich. Es geht nicht um die Abwehr von Gefahren für überragend wichtige Rechtsgüter. Zudem dürften die den Anforderungen des Entwurfs (vgl. § 100a Abs. 5 StPO) entsprechenden technischen Mittel auch noch nicht existieren[3] und – so neutrale IT-Experten außerhalb der Ermittlungsbehörden – diese Anforderungen auch technisch nur sehr schwer erfüllbar sein.[4]

Mag es auch am 31.05.2017 zu einer Anhörung im Rechtsausschuss zu dem Änderungsantrag gekommen sein, ist es trotz der Tragweite der geplanten Änderungen der StPO nicht zu den sonst üblichen Verbandsanhörungen gekommen – und sollte es offenbar auch nicht.

Angesichts der Reichweite der Änderungen und der insbesondere auch technischen Fragen beim staatlichen Einsatz von Schadsoftware („Staatstrojaner“) ist darauf hinzuweisen, dass eine umfassende Stellungnahme zu allen der problematischen Aspekte des Entwurfs nicht möglich ist - ein Problem, welches auch schon die Vorbereitung der Teilnehmer in der kurzfristigen Anhörung im Rechtsausschuss am 31.05.2017 prägte.[5] Angesichts der Eingriffstiefe der Änderungen einerseits und einer gesetzlichen Regelung einer „Online-Durchsuchung“ im Bereich der Gefahrenabwehr andererseits ist ein eiliger Handlungsbedarf zum Rechtsgüterschutz nicht nachvollziehbar. Nicht nur im Hinblick auf die verfassungs- und datenschutzrechtlichen Implikationen bedarf es dieser gesellschaftlichen Auseinandersetzung über die „Quellen-TKÜ“ und die „Online-Durchsuchung“. Es passt indes in das Bild dieses Gesetzgebungsverfahrens, dass noch nicht einmal die Bundesdatenschutzbeauftragte ausweislich ihres Schreibens an den Rechtsausschuss vom 29.05.2017 vom BMJV im Gesetzgebungs-verfahren zum Änderungsantrag beteiligt wurde.[6]

Nachdem der Änderungsantrag vom 15.05.2017 nunmehr auch bis in die Presse „durchgesickert“ ist, gibt es nunmehr auch die ersten kritische Reaktionen. Es ginge offenbar darum, der Polizei mehr Macht zu geben und

---

[3] vgl. Änderungsantrag S. 22/23

[4] vgl. gutachterliche Stellungnahme von RiLG Buermeyer v. 29.05.2017 zur Ausschussdrucksache 18(6)334, S. 9, m.w.N. Vgl. gutachterliche Stellungnahme von RiLG Buermeyer v. 29.05.2017 zur Ausschussdrucksache 18(6)334, S. 4

[5] vgl. gutachterliche Stellungnahme von RiLG Buermeyer v. 29.05.2017 zur Ausschussdrucksache 18(6)334

[6] Schreiben der Bundesbeauftragten für Datenschutz und Informationsfreiheit Voßhoff v. 29.05.2017

Sicherheitslücken nicht zu schließen – was im Interesse aller wäre -, sondern zu nutzen.[7] „Die Kanone wird zur Standardwaffe“ titelte Zeit-Online.[8]

Der Deutsche Anwaltverein wird nur zum Inhalt des Änderungsantrages Stellung nehmen, zu dem ursprünglichen Entwurf in Form des Referentenentwurfs ist bereits eine Stellungnahme erfolgt.[9]

Die geplante Einführung der sogenannten „Quellen-TKÜ“ und der „Online-Durchsuchung“ begegnet massiven – verfassungsrechtlichen – Bedenken. Jenseits dieser verfassungsrechtlichen Bedenken besteht die Notwendigkeit einer gesellschaftlichen Auseinandersetzung, welche Grundrechtseingriffe zur Sicherung der Funktionsfähigkeit der Strafrechtspflege – das ist Ziel von Zwangsmaßnahmen im Strafverfahren – hinzunehmen sind. Hinzu kommt das praktische Problem der Ansammlung unbegrenzter Datenmengen in den Bereichen, die von der „Quellen-TKÜ“ und der „Online-Durchsuchung“ abgedeckt würden. Bereits jetzt geraten Strafprozesse an die Grenzen ihrer Möglichkeiten, wenn z.B. Smartphones beschlagnahmt und ausgewertet werden – mit Gigabytes von durchzusehenden Daten.

Jedenfalls abzulehnen ist der vorgesehene unterschiedliche Umgang mit der Kommunikation der Berufsgeheimnisträger einerseits und ihrer Berufshelfer andererseits.

I. Die Überwachungsmaßnahmen – Quellentelekommunikationsüberwachung und Online-Durchsuchung

Die in den Jahren 2014/2015 tagende „Expertenkommission zur effektiveren und praxistauglicheren Ausgestaltung des allgemeinen Strafverfahrens und des jugendgerichtlichen Verfahrens“ hatte in ihrem Bericht vom Oktober 2015[10] empfohlen, für die Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) zum Zwecke des Grundrechtsschutzes des Betroffenen eine Rechtsgrundlage zu schaffen. Hintergrund waren unterschiedliche Auffassungen zur Frage der unmittelbaren Anwendbarkeit von § 100a StPO.

---

7 http://www.spiegel.de/wissenschaft/mensch/ueberwachung-warum-polizisten-keine-smartphones-hacken-sollten-kolumne-a-1152499.html

8 http://www.zeit.de/digital/datenschutz/2017-06/staatstrojaner-whatsapp-ueberwachung-bundesregierung/seite-2

9 vgl. Stellungnahme des DAV Nr. 47/16 v. 23.08.16

10 https://www.bmjv.de/SharedDocs/Downloads/DE/PDF/Abschlussbericht_Reform_StPO_Kommission.pdf?__blob=publicationFile&v=2, dort Nr. 5.1

Es ist zweifelhaft, ob der nunmehr vorliegende Entwurf einer gesetzlichen Regelung den verfassungsrechtlichen Vorgaben standhält und die Fragen, auf die es dem Änderungsantrag ausweislich seiner Begründung ankommt, abschließend regelt.

1. Quellen-TKÜ

Die Einführung der Quellen-TKÜ soll über die Anfügung der Sätze 2 und 3 an § 100a Abs. 1 StPO erfolgen:

> „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."

Die Überwachung soll – subsidiär[11] zur „klassischen" Telefonüberwachung (vgl. § 100a Abs. 1 Satz 2 StPO-E: „wenn dies notwendig ist") – in diesen Fällen durch das Aufspielen einer hierzu geeigneten Software („Staatstrojaner") auf ein Telekommunikationsendgerät erfolgen, um dort anfallende Daten aus aktuell überwachter Kommunikation sowie verschlüsselte und während der Überwachung gespeicherte Daten zu erlangen. Die technischen Anforderungen an die einzusetzende Software sind in § 100a Abs. 5 StPO-E aufgeführt.

a. Straftatenkatalog

Trotz der geplanten Erweiterung einer möglichen Telefonüberwachung auf den Bereich der Quellen-TKÜ soll der Straftatenkatalog des § 100 a Abs. 2 StPO-E unverändert gelten.

---

[11] vgl. Änderungsantrag, S. 21

Das Bundesverfassungsgericht hat auf die besonderen Risiken hingewiesen, die mit einer Quellen-TKÜ verbunden sind.[12] Denn mit der Infiltration des Systems sei die entscheidende Hürde gefallen, dass System insgesamt auszuspähen.[13] Diese Gefahren entstehen nicht nur durch das gezielte Auslesen des Systems durch Ermittlungsbehörden, sondern auch durch abstrakte Gefährdungen wie etwa der Nutzung von Sicherheitslücken im System durch die Behörden oder die Nutzung der Infiltration durch Dritte. Angesichts der aus dieser Infiltration des informationstechnischen Systems folgenden größeren Eingriffstiefe der Ermittlungsmaßnahme ist die Eingriffsschwelle für eine entsprechende Maßnahme deutlich höher anzusetzen als bei herkömmlichen TKÜ-Maßnahmen.[14] Dies folgt ohne weiteres schon aus der für den Gefahrenabwehrbereich getroffenen Entscheidung des Bundesverfassungsgerichts aus dem Jahr 2008[15], nach der entsprechende Eingriffe nur zulässig sein sollen, wenn ein

> „überragend wichtiges Rechtsgut“

betroffen ist[16], wobei zugleich festgestellt wurde, dass entsprechende Maßnahmen verfassungsrechtlich bedenklich sind, wenn sie zum Schutz

> „sonstiger Rechtsgüter Einzelner oder der Allgemeinheit in Situationen, in denen eine existenzielle Bedrohungslage nicht besteht“

eingesetzt werden.[17] Diesen verfassungsrechtlichen Anforderungen wird die bloße Übernahme des Straftatenkatalogs der „herkömmlichen“ und weniger eingriffsintensiven Befugnis zur Telekommunikationsüberwachung ersichtlich nicht gerecht. Zu fordern wäre hier zumindest, die Einsatzmöglichkeit der Ermittlungsmaßnahme auf schwere und schwerste Straftaten zu begrenzen.

Es ist zu prüfen, ob überhaupt ein – umsetzbarer – Bedarf an einer Quellen-TKÜ für alle im Katalog des § 100a Abs. 2 StPO aufgeführten Straftaten besteht. Im Vergleich mit der herkömmlichen TKÜ sind sowohl der

---

12 vgl. BVerfG, Beschluss v. 30.08.2007, 1 BvR 370/07 und 595/07, Rn. 187/188
13 vgl. BVerfG, Beschluss v. 30.08.2007, 1 BvR 370/07 und 595/07, Rn. 188
14 vgl. Stellungnahme der Bundesdatenschutzbeauftragten Voßhoff v. 29.05.17, S. 3
15 vgl. BVerfG, Beschluss v. 30.08.2007, 1 BvR 370/07 und 595/07 Rn.
16 vgl. BVerfG, Beschluss v. 30.08.2007, 1 BvR 370/07 und 595/07, Rn. 242
17 BVerfG, Beschluss v. 30.08.2007, 1 BvR 370/07 und 595/07, Rn. 248

technische Aufwand sowie die rechtlichen und technischen Risiken deutlich höher.[18]

b. Eingesetzte Schadsoftware

Der Gesetzesentwurf enthält lediglich in § 100a Abs. 5 StPO eine abstrakte Regelung dazu, welche technischen Anforderungen an eine entsprechende, bei der Durchführung der Quellen-TKÜ eingesetzte Schadsoftware zu stellen sind. Diese begegnet angesichts dezidierter verfassungsrechtlicher Vorgaben erheblichen Bedenken: Nach der Entscheidung des Bundesverfassungsgerichts aus dem Jahr 2008 ist beim Einsatz einer solchen Schadsoftware zum Zwecke der Quellen-TKÜ durch

> „technische Vorkehrungen und rechtliche Vorgaben“

sicherzustellen, dass

> „sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt“.[19]

Nach § 100a Abs. 5 StPO-E soll bei der Online-TKÜ technisch sichergestellt werden, dass

- nur im Rahmen der Ermächtigung die Telekommunikation überwacht und aufgezeichnet wird,
- nur für die Datenerhebung unerlässliche Veränderungen am betroffenen informationstechnischen System vorgenommen und
- diese nach Beendigung der Maßnahme rückgängig gemacht werden können.
- Das eingesetzte technische Mittel soll ausweislich des Gesetzestextes nach dem Stand der Technik gegen unbefugte Nutzung geschützt werden.

Weitere Vorgaben und Regelungen enthält der Gesetzesentwurf nicht. Nach der vorgesehenen Regelung müsste eine entsprechende Schadsoftware weder zertifiziert werden noch wäre der Einsatz von Schadsoftware von

---

[18] vgl. Stellungnahme der BundesdatenschutzbeauftragtenVoßhoff v. 29.05.17, S. 3
[19] BVerfG, Beschluss v. 30.08.2007, 1 BvR 370/07 und 595/07, Rn. 190

Herstellern aus der Privatwirtschaft unzulässig. Bereits dies dürfte den verfassungsrechtlichen Vorgaben nicht entsprechen.

Hinzu kommt eine fehlende gesetzliche Regelung zu der Frage, wie mit den Daten überwachter und aufgezeichneter Kommunikation umgegangen werden soll, wenn sich im Nachhinein herausstellt, dass das eingesetzte technische Mittel die technischen Anforderungen gem. § 100a Abs. 5 StPO-E nicht erfüllt. Es existiert keine Regelung dazu, ob dies nur zum Ausscheiden der jenseits der Grenze der Ermächtigung aufgezeichneten Daten oder zu einer Unverwertbarkeit aller aufgezeichneten Daten führt.

c. Fehlende Bestimmtheit der Norm

§ 100a Abs. 1 Satz 2 StPO lässt nach seinem Wortlaut neben der Überwachung der Kommunikation zwischen zwei Personen im Wege der Quellen-TKÜ auch die Überwachung der Kommunikation zwischen zwei Endgeräten zu, wenn diese Kommunikation dem Cloud-Computing durch einen Datenaustausch zwischen dem Endgerät eines Nutzers und einer Cloud dient, oder der Nutzer sich Daten von einem seiner Endgeräte auf ein anderes Endgerät weiterleitet. Denn jeweils entsteht technisch gesehen ein Kommunikationsvorgang. Allerdings liegt beim Cloud-Computing oder dem Weiterleiten von Nachrichten an ein anderes eigenes Endgerät ein höchstpersönlicher Datenaustausch vor, welcher mit einer klassischen Kommunikation zwischen zwei Personen nicht gleichzusetzen ist.[20] Obwohl der Wortlaut eine Überwachung dieses höchstpersönlichen Datenaustausches zulassen könnte, dürfte es nach dem Ziel und der Rechtfertigung der Quellen-TKÜ genau wie bei der klassischen TKÜ nur um die Überwachung der Kommunikation zwischen zwei (oder mehr) Personen gehen.

Insofern dürfte aber § 100a Abs. 1 Satz 2 StPO aufgrund fehlender Bestimmtheit den Anforderungen des BVerfG nicht genügen:

> „Ermächtigungen zu Grundrechtseingriffen bedürfen einer gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenbestimmtheit und Normenklarheit entspricht. Bei Eingriffen in

[20] vgl. Stellungnahme Prof. Dr. Sinn v. 30.05.2017, S. 4 f.; vgl. auch Bundesdatenschutzbeauftragte Voßhoff, Stellungnahme v. 29.05.17, S. 4

> das Grundrecht auf informationelle Selbstbestimmung – wie auch in die Spezialgrundrechte der Art. 10 und 13 GG – hat der Gesetzgeber insbesondere den Verwendungszweck der Daten bereichsspezifisch und präzise zu bestimmen.“[21]

d. Unzureichende Abgrenzung von der Regelung des § 100a Abs. 1 Satz 3 StPO-E zur Online-Durchsuchung

§ 100a Abs.1 Satz 3 StPO-E ermöglicht die Aufzeichnung und Überwachung

> „auf dem informationstechnischen System des Betroffenen gespeicherter Inhalte und Umstände der Telekommunikation […], wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können“.

In der derzeitigen Entwurfsfassung ermächtigt dies die Strafverfolgungsbehörden zu einem Eingriff in das „Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme“. Es wird Zugriff genommen auf bereits gespeicherte Daten, die nicht im Rahmen der Überwachung der Kommunikation vor Speicherung und eventuell Verschlüsselung ausgeleitet werden können. Dieser Eingriff darf sich aber nur auf Daten beziehen, die nach Anordnung der Maßnahme durch das Gericht hätten ausgeleitet werden können. Auf dem Endgerät eines Kommunikationsinhabers sind jedoch unter Umständen auch Nachrichten gespeichert, die sich auf Zeiträume vor der Anordnung erstrecken. Die einzusetzende Software muss daher so programmiert sein, dass sie anhand der zu den einzelnen Nachrichten hinterlegten Meta-Daten, die etwa die Absende-, Empfangs- und Lesezeitpunkte enthalten, nur die erst ab dem Zeitpunkt der Anordnung ein- und ausgehenden Nachrichten ausleitet.[22]

Trotz dieser zumindest beabsichtigten Beschränkung kommt es jedenfalls zur Durchsuchung der auf dem Endgerät gespeicherten Daten, was die Quellen-TKÜ insoweit zur Online-Durchsuchung macht - ohne das es des Vorliegens der erheblich strengeren Voraussetzungen des § 100b Abs. 1 StPO bedürfen soll: Angesichts der heutigen technischen Möglichkeiten und

---

[21] vgl. BVerfG, Beschluss v. 04.04.2006, 1 BvR 518/02, Rn. 150
[22] vgl. Änderungsantrag, S. 20

der für Übertragung von Daten zur Verfügung stehenden großen Bandbreiten werden jegliche auf dem informationstechnischen System gespeicherten Inhalte hypothetisch im öffentlichen Telekommunikationsnetz zu übertragen sein. Zudem beziehen sich die Vorgaben des BVerfG zur Quellen-TKÜ nur auf die Erhebung laufender und nicht früherer – gespeicherter – Kommunikation.

Die Überlegung im Änderungsantrag, dass es auf die höheren Anforderungen des BVerfG bei der Online-Durchsuchung im Hinblick auf das betroffene „Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme“ nicht ankäme, da beide Maßnahmen Kommunikationen – laufend oder frühere – beträfen, so dass eine Unterscheidung verfassungsrechtlich nicht geboten sei.[23] Zur Begründung wird eine Analogie zur gesetzgeberisch bereits gewählten Ausnahme herangezogen, dass das für die laufende Quellen-TKÜ eingesetzte technische Mittel trotz Infizierung des informationstechnischen Systems nur an Art. 10 GG zu messen sein soll. Eine Ausnahme muss jeweils restriktiv ausgelegt werden und kann nicht weitere Ausnahmen über eine Analogie begründen. Es ist verfassungsrechtlich kaum zu vertreten, für die durch § 100a Abs. 1 Satz 3 StPO eröffnete Online-Durchsuchung die klaren Vorgaben des BVerfG zur Abgrenzung zwischen Online-Durchsuchung und Quellen-TKÜ zu übergehen.[24]

Das eingesetzte technische Mittel soll die Anforderungen des § 100a Abs. 5 Satz 1 Nr. 1b StPO-E bezüglich der Begrenzung auf die Ausleitung von nach der gerichtlichen Anordnung entstandenen Daten erfüllen. Bei im informationstechnischen System gespeicherten und nicht aktuell übertragenen Daten dürfte sich – auch für das eingesetzte technische Mittel – erst nach Ausleitung und Auswertung feststellen lassen, ob es sich um Daten handelt, welche während des laufenden Übertragungsvorganges hätten überwacht und aufgezeichnet werden können.[25]

---

[23] vgl. Änderungsantrag, S. 20
[24] vgl. vgl. Stellungnahme RiLG Buermeyer v. 31.05.2017, S. 16
[25] vgl. Stellungnahme RiLG Buermeyer v. 31.05.2017, S. 17

e. Einsatz der Maßnahme gegen Dritte

§ 100a Abs. 3 StPO-E sieht vor, dass sich die Anordnung auch gegen Personen richten kann, von denen aufgrund bestimmter Tatsachen anzunehmen ist,

> „dass der Beschuldigte [...] ihr informationstechnisches System benutzt“.

Nach dem Wortlaut der Regelung – insbesondere in Zusammenschau mit der Ausweitung auf Daten, die hypothetisch hätten überwacht und aufgezeichnet werden können (§ 100a Abs. 1 Satz 3 StPO-E) – ermöglicht die Regelung den Zugriff auf informationstechnische Systeme Dritter, die durch den Beschuldigten gerade außerhalb von Kommunikationsvorgängen genutzt werden. Dies ist mit den verfassungsrechtlichen Vorgaben erst recht nicht vereinbar.

2. Online-Durchsuchung

Die vorgesehene Online-Durchsuchung umfasst all jene Eingriffe, die bisher bereits nach § 100c StPO als akustische Raumüberwachung („Großer Lauschangriff“) zulässig waren. Es kommen durch die Infektion der informationstechnischen Systeme des Beschuldigten noch weitere erhebliche Eingriffe hinzu:

- heimliche Auswertung der gesamten laufenden und früheren Kommunikation,
- die Auswertung aller digital gespeicherten Inhalte auf den infizierten Systemen,
- ein „Großer Spähangriff“ auf die Umgebung des überwachten Systems, sofern es über eine Kamera-Funktion verfügt wie heute nahezu jedes Smartphone, jedes Tablet und nahezu jeder Laptop.[26]

Über die auf den zu durchsuchenden Geräten im Giga- bis Terrabereich abgelegten Daten aus beruflichen sowie höchstpersönlichen Bereichen erhalten die Ermittlungsbehörden ein weitgehendes digitales Abbild des

[26] vgl. Stellungnahme RiLG Buermeyer v. 31.05.2017, S. 5

Lebens des Betroffenen. „Moderne informationstechnische Systeme gleichen so einem ausgelagerten Teil des Gehirns.“[27]

Die Online-Durchsuchung ist daher im Verhältnis zum „Großen Lauschangriff“ ein deutliches „Mehr“ an Grundrechtseingriff.

Im Unterschied zur offenen Durchsuchung und Beschlagnahme eines informationstechnischen Systems erfolgt der Zugriff heimlich und kann nicht nur einmalig und punktuell stattfinden, sondern sich auch über einen längeren Zeitraum erstrecken. In Abgrenzung zur ebenfalls „heimlichen“ Telekommunikationsüberwachung können nicht nur neu hinzukommende Kommunikationsinhalte, sondern alle auf einem informationstechnischen System gespeicherten Inhalte sowie das gesamte Nutzungsverhalten einer Person überwacht werden.[28]

a. Straftatenkatalog

Der Gesetzgeber sieht als Anlasstaten für die Anordnung einer Online-Durchsuchung denselben Straftatenkatalog wie beim „Großen Lauschangriff“ vor (vgl. § 100c Abs. 2 StPO) und hält trotz der deutlich schwerer wiegenden Eingriffstiefe die Übertragung dieses Straftatenkatalogs auf die Online-Durchsuchung für gerechtfertigt. Denn das BVerfG habe die Eingriffsintensität einer Online-Durchsuchung mit der Eingriffsintensität einer Wohnraumüberwachung verglichen.[29] Tatsächlich führt das BVerfG in der in Bezug genommenen Entscheidung zur „Online-Durchsuchung“ aus, dass es sich um einen Grundrechtseingriff besonderer Intensität handele, der seinem Gewicht nach mit dem Eingriff in die Unverletzlichkeit der Wohnung vergleichbar sei[30] – der sich aber nicht im „Großen Lauschangriff“ erschöpft.

Angesichts der oben bereits angeführten verfassungsrechtlichen Vorgaben, wonach eine mit der Infiltration eines informationstechnischen Systems verbundene Ermittlungsmaßnahme nur im Hinblick auf „überragend wichtige Rechtsgüter“ und nicht zum Schutz sonstiger Rechtsgüter Einzelner oder der Allgemeinheit angeordnet und angewendet werden darf, geht der für die Online-Durchsuchung vorgesehene Straftatenkatalog deutlich zu weit.

---

27 vgl. Stellungnahme RiLG Buermeyer v. 31.05.2017, S. 5
28 vgl. Änderungsantrag, S. 23
29 vgl. Änderungsantrag, S. 24
30 vgl. BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, Rn. 210

Überragend wichtig sind nach der Rechtsprechung des BVerfG Leib, Leben und Freiheit einer Person; Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt sowie die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen,[31] nicht aber „zum Schutz sonstiger Rechtsgüter Einzelner oder der Allgemeinheit in Situationen, in denen eine existenzielle Bedrohung nicht besteht".[32]

Bereits an diesem Maßstab gemessen, ist eine Anordnung von Online-Durchsuchungen für Straftaten aus dem Bereich der mittleren Kriminalität, wie der Geld- und Wertzeichenfälschung, des Bandendiebstahls, der gewerbsmäßigen Hehlerei und der Bandenhehlerei sowie Straftaten gegen das Asylverfahrens- oder Aufenthaltsgesetz verfassungswidrig.

Hinzu kommt, dass das BVerfG die dargestellten Vorgaben im Präventivbereich entwickelt hat, in dem es um konkreten Rechtsgüterschutz im Bereich der dargestellten Rechtsgüter geht. Im Ermittlungsverfahren geht es um repressive Ermittlungstätigkeiten und geschütztes Rechtsgut ist – von Ausnahmen abgesehen – die Funktionsfähigkeit der Strafrechtspflege. Dies muss gemessen an den Vorgaben des BVerfG zu einer noch restriktiveren Regelung bzgl. der Zulässigkeit einer Online-Durchsuchung führen – nicht zu einer Gleichschaltung mit dem „Großen Lauschangriff".

Mit dieser Frage findet im Änderungsantrag keine wirkliche inhaltliche Auseinandersetzung statt. So heißt es in der Begründung lapidar und ohne jede weitere Erläuterung:

> „Das Bundesverfassungsgericht hat die genannten Maßstäbe im Bereich des Rechts der Nachrichtendienste und der Gefahrenabwehr entwickelt. Nichtsdestoweniger müssen sie auch im Bereich der Strafverfolgung berücksichtigt werden, wobei einzelne Elemente wegen der unterschiedlichen Natur der jeweiligen Eingriffe modifiziert werden müssen."[33]

Offenbar soll dann aber trotz obiger Ausführungen zum geschützten Rechtsgut nach Auffassung des Änderungsantrages zwischen präventiven

---

[31] vgl. BVerfGE 120, 274, 326
[32] vgl. BVerfGE 120, 274, 328
[33] vgl. Änderungsantrag, S. 17

und repressiven Maßnahmen unterschieden werden bzw. die Eingriffsschwelle für die präventive Maßnahme höher liegen – und genau andersherum, wie bereits entwickelt. Denn nach § 100e Abs. 6 StPO soll bei der Verwertung von im Rahmen der Strafverfolgung erlangten Daten für die Gefahrenabwehr wieder der Maßstab des BVerfG (Schutz überragend wichtiger Rechtsgüter) gelten.

b. Die im Einzelfall besonders schwerwiegende Tat (§ 100b Abs. 1 Nr. 2 StPO-E)

Im Gesetz fehlt jeder Hinweis darauf, wann das Kriterium „die Tat auch im Einzelfall besonders schwer wiegt“ erfüllt ist. Im Hinblick auf die Eingriffstiefe und die notwendige Bestimmtheit einer Ermächtigungsgrundlage ist diese durch nichts als ein „richterliches Bauchgefühl“[34] konkretisierte Eingangsvoraussetzung für die Anordnung einer Online-Durchsuchung zu unbestimmt.

c. Unzureichender Kernbereichsschutz

§ 100d Abs. 1 StPO-E übernimmt für Quellen-TKÜ und Online-Durchsuchungen die in der Kommentarliteratur seit Einführung der entsprechenden Vorgängerregelung enthaltene „Schutzvorschrift“, nach der die entsprechenden Maßnahmen nur dann unzulässig sein sollen, wenn durch die Maßnahme

> „allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden“.

Fälle, in denen dies vor Anordnung der Maßnahme anzunehmen ist, kommen in der Praxis nicht vor; es handelt sich insoweit um eine völlig untaugliche Placebo-Regelung, die nun in der Neufassung der Vorschrift übernommen werden soll.

Vorstehendes wäre mit Blick auf die deutlich effektivere und weitergehende Regelung des § 100d Abs. 4 StPO-E nur insoweit nachvollziehbar, als dass erkannt worden ist, dass ein Großteil dessen, was „abgefischt“ wird, eben

[34] vgl. Stellungnahme RiLG Buermeyer v. 31.05.2017, S. 14

auch und gerade den Kernbereich des Privaten betrifft und dessen Verletzung als Regelfall nunmehr legitimiert werden soll.

§ 100d Abs. 4 StPO-E lautet:

> „soweit auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass durch die Überwachung Äußerungen, die dem Kernbereich privater Lebensgestaltung zu zurechnen sind, nicht erfasst werden“

und findet Anwendung auf den „großen Lauschangriff“, soll aber nicht für Maßnahmen der Online-Durchsuchung gelten. Die Online-Durchsuchung ermöglicht – über die akustische Wohnraumüberwachung hinaus – den Zugriff auf in dem informationstechnischen System abgespeicherte Informationen, die oft tagebuchähnlichen Charakter haben und dem absoluten Kernbereich privater Lebensgestaltung zuzurechnen sind. Diese Eingriffstiefe muss sich auch in der entsprechenden Vorschrift zum Kernbereichsschutz wiederspiegeln. Die (Schutz-)Regelung des § 100d Abs. 4 StPO-E sollte deshalb auch zumindest auf die Regelungen der Online-Durchsuchung erstreckt werden.

II. Allgemeine Erwägungen

1. Ungeeignetheit der neu eingeführten Ermittlungsmaßnahmen

Online-Durchsuchung und Quellen-TKÜ stellen in der durch den Gesetzentwurf vorgesehenen Ausgestaltung im Hinblick auf das Gesetzgebungsziel untaugliche Ermittlungsinstrumente dar:

Gesetzgeberisches Ziel ist – anders als in den Verfassungsschutzgesetzen der Länder und den entsprechenden Regelungen im BKA-Gesetz – nicht die Gefahrenabwehr, sondern die Gewinnung von gerichtsverwertbaren Beweisen zum Zwecke der Strafverfolgung. Da sowohl der Beweiserhebung durch eine Maßnahme der Quellen-TKÜ als auch der Online-Durchsuchung eine Manipulation des betroffenen informationstechnischen Systems durch das Einbringen einer Schadsoftware vorausgeht, führt die das Ermittlungsinstrument einsetzende Strafverfolgungsbehörde – im Falle „erfolgreichen“ Einsatzes – selbst den Nachweis, dass das angegriffene

informationstechnische System durch Dritte manipulierbar ist. Zudem ist nach allgemeinen forensischen Grundsätzen jede Manipulation des betroffenen Gerätes zu unterlassen. Es wäre nach bisherigen Standards ein polizeilicher Kunstfehler, ein beschlagnahmtes Gerät unmittelbar zu analysieren, statt nur ein Image der sichergestellten Datenträger auszuwerten.[35]

Diese Tatsache dürfte den Beweiswert der insoweit erlangten Daten derart schmälern, dass unter verfassungsrechtlichen Gesichtspunkten die Zulässigkeit der Maßnahme insgesamt in Frage zu stellen ist, da die enorme Eingriffstiefe in keinem Verhältnis zur Eignung der Maßnahme steht.

2. Staatlicher Zielkonflikt

Die Einführung der beiden Ermittlungsinstrumente schafft auf staatlicher Seite zudem einen kaum hinnehmbaren Zielkonflikt:

Ziel und Interesse des Gesetzgebers und entsprechenden staatlichen Handelns ist angesichts zunehmender Bedrohungen der Allgemeinheit durch die sog. Cyber-Kriminalität (z.B. Ransomware-Erpressungen, DDoS-Angriffe, Phishing) der Schutz informationstechnischer Systeme, in denen in zunehmendem Maße persönliche und dem Kernbereich privater Lebensgestaltung zuzurechnende Daten gespeichert werden. Die insoweit grundrechtliche Relevanz der Integrität informationstechnischer Systeme hat letztlich zur „Schaffung“ eines entsprechenden Grundrechts durch die Entscheidung des Bundesverfassungsgerichts aus dem Jahr 2008 geführt.[36] Die vorgesehenen Regelungen des Gesetzesentwurfs schaffen für staatliche Stellen nun nicht nur einen Anreiz gerade zur Schaffung und Offenhaltung technischer Schutzlücken in informationstechnischen Systemen, um einen entsprechenden Fremdzugriff zum Einbringen der erforderlichen Schadsoftware zu ermöglichen. In der Konsequenz beinhalten sie auch ein enormes Missbrauchspotential für Dritte, die sich den durch die Ermittlungsmaßnahme geschaffenen Zugriffskanal auf das informationstechnische System für weitere Angriffe oder Manipulationen zu Nutze machen können.[37]

---

[35] Bundesdatenschutzbeauftragte Voßhoff, Stellungnahme v. 29.05.2017, S. 8
[36] vgl. BVerfG, Beschluss v. 30.08.2007, 1 BvR 370/07 und 595/07
[37] vgl. auch http://www.spiegel.de/wissenschaft/mensch/ueberwachung-warum-polizisten-keine-smartphones-hacken-sollten-kolumne-a-1152499.html

III. Zur Differenzierung zwischen §§ 53 und 53a StPO im Rahmen der Verwertungsregeln des § 100d Abs. 5 StPO-E

Als sachlich unsystematisch und rechtlich verfehlt erweist sich weiterhin die Regelung des § 100d Abs. 5 StPO-E. Gemäß dieser soll für betroffene Kommunikation mit Berufsgeheimnisträgern ein Beweiserhebungsverbot gelten, für deren Berufshelfer im Range des § 53a StPO indes allenfalls ein ***relatives*** Verwertungsverbot.

Diese Differenzierung in § 100d Abs. 5 StPO-E zwischen Berufsträgern nach § 53 und deren Helfern gem. § 53a StPO ist als systemwidrig abzulehnen. Sie gefährdet darüber hinaus ua. für Strafverteidiger die Gewährleistung einer effektiven Verteidigung, weil sie das Vertrauen in den Schutz der Kommunikation rechtsstaatswidrig nur noch dann staatlicherseits weitgehend respektieren will, wenn diese unmittelbar mit dem Berufsgeheimnisträger geführt wird. Die diesem verpflichteten Helfer, Sekretariate etc., und damit der zur Berufsausübung regelmäßig erforderliche Kommunikationsapparat, sollen hingegen potenziell staatlich abschöpfbar sein.

1. Berufsgeheimnisträger und Berufshelfer

Der Zweck des § 53a Abs. 1 StPO ist es, der Gefahr zu begegnen, dass durch Rückgriff auf die Berufshelfer das Zeugnisverweigerungsrecht des jeweiligen Berufsträgers nach § 53 StPO umgangen wird. Es soll verhindert werden, dass anstelle des schweigeverpflichteten Berufsträgers auf dessen Berufshelfer als Zeugen zugegriffen werden kann und hierdurch das Verschwiegenheitsversprechen des Berufsstandes letztlich gebrochen bzw. das entsprechende Zeugnisverweigerungsrechst faktisch leerlaufen würde.[38] Soll also sinnvollerweise der Schutz der Berufsgeheimnisträger vor Umgehung dadurch geschützt werden, dass die notwendig mit den anvertrauten Berufsgeheimnissen in Berührung kommenden Hilfspersonen ebenfalls (gem. § 53a StPO) ein Zeugnisverweigerungsrecht gleichen Umfangs haben, verbietet sich systematisch eine Differenzierung, zumal dann, wenn sie eine Umgehung ermöglichen würde. Dies ist bei dem in Rede stehenden Gesetzesvorschlag eindeutig der Fall:

[38] Allgem. M. vgl. nur den RegE eines 3. StÄG, BT-Drucks. I/3713, S. 48; SK-StPO/Rogall, § 53a Rn. 1; HK-GS/Trüg § 53a Rn. 1; Radtke/Hohmann/Otte § 53a Rn. 1; Graf/Huber § 53a Rn. 1

§ 100d Abs. 5 StPO-E übernimmt den geltenden § 100c Abs. 6 StPO. Schon dieser galt zu Recht als verunglückt, was indes zu verschmerzen war, da er zumindest in der Praxis keine Rolle spielte.[39] Der Grund liegt auf der Hand: Es ist höchst selten, dass ein Verteidiger oder ein Arzt seine Klienten in der überwachten Wohnung aufsucht. In aller Regel, werden diese seine – unüberwachte – Kanzlei bzw. Praxis aufsuchen. Noch – und dies ist an dieser Stelle entscheidender – seltener werden sich die Hilfspersonen des Berufsgeheimnisträgers allein auf den Weg in überwachte Wohnungen machen. Indes würde nur für diesen Fall die Differenzierung in § 100c Abs. 6 StPO überhaupt zum Tragen kommen. Entscheidungen oder Fälle hierzu sind nicht bekannt, da es sich – wie gesagt – um eine praktisch nicht vorkommende, sondern nur theoretisch denkbare Konstellation handelt.

In ihrer Eingriffswahrscheinlichkeit und -tiefe ist die hier in Aussicht genommene Online-Durchsuchung nach § 100b StPO-E, auf die § 100d Abs. 5 E-StPO rekurriert, gänzlich anders zu beurteilen. Tatsächlich sind es gerade die „Berufshelfer“ in Form von Sekretariaten, Mitarbeitern etc., die oftmals erste Ansprechpartner der Beschuldigten sind, wenn diese versuchen, über informationstechnische Systeme (vermeintlich) vertraulichen Kontakt zum Berufsgeheimnisträger i.S.d. § 53 StPO aufzunehmen. Regelmäßig werden hierbei die Anliegen der Beschuldigten bereits skizziert, mithin auch inhaltlich den Kernbereich der besonders geschützten Beziehung zum Berufsträger betreffende Informationen preisgegeben. Der Schutz der Berufsgeheimnisträger und insbesondere Sinn und Zweck des § 53a StPO laufen künftig leer, wenn § 100d Abs. 5 StPO-E in der angedachten Form verabschiedet wird. Es ist für den Schutz der Berufsgeheimnisträger und der ihnen anvertrauten Geheimnisse unentbehrlich, dass nicht nur die Informationen des Beschuldigten, soweit sie den Berufsgeheimnisträger erreichen bei diesem, gleichsam als Endstation geschützt sind, sondern auch auf dem Weg zu ihm über seine Berufshelfer.

Der Gesetzgeber hat dies bislang auch selbst erkannt und vorausgesetzt. Dementsprechend hat er in § 160a Abs. 3 StPO normiert, dass Berufshelfer den Berufsgeheimnisträgern, was die Betroffenheit von heimlichen

---

[39] Lesenswert: SK-StPO/Wolter § 100c Rn. 79

Ermittlungsmaßnahmen angeht, gleichgestellt sind. Die nunmehr erwogene – begründungslose – Differenzierung in § 100d Abs. 5 StPO im Falle der schwersten Eingriffe (Online-Durchsuchung gem. § 100b sowie Wohnraumüberwachung n. § 100c StPO-E) zwischen Berufsgeheimnisträgern und deren -helfern kann daher auch binnensystematisch nicht überzeugen, mag diese Differenzierung bislang auch ihr praktisch bedeutungsloses (s. o.) Schattendasein im bisherigen § 100c Abs. 6 StPO gefristet haben.

Weiterhin gilt: Wurde bislang (und wird auch künftig) im Rahmen einer offenen Durchsuchung ein Endgerät bei einem Beschuldigten beschlagnahmt, durfte seine hierauf gespeicherte Kommunikation mit dem Strafverteidiger und seinen Berufshelfern nicht erhoben werden. Dies ist – über den engeren Wortlaut des § 97 Abs. 4 StPO – aufgrund der auch einfachgesetzlich in § 148 StPO verbrieften Garantie unüberwachten Kommunikationsverkehrs des Beschuldigten mit dem Verteidiger ebenso unbestritten wie die ungeteilte Geltung dieses Grundsatzes auch für die Berufshelfer des Verteidigers.[40]

Mit der nunmehr in den Blick genommenen Aufweichung dieses Schutzes für Berufshelfer des Verteidigers schafft der Gesetzgeber mithin gegebenenfalls einen (weiteren) untunlichen Anreiz für die Ermittlungsbehörden, dem Bürger nicht mehr offen im Rahmen einer Durchsuchung gegenüberzutreten, sondern ihn durch heimlichen Zugriff auf die Daten seiner informations-technischen Systeme wesentlich weitergehend auszuspähen, um auf diesem Wege u. a. auch – etwa über das Abfischen von Kommunikation mit dem Sekretariat des Verteidigers – bislang grund- und einfachgesetzlich dem staatlichen Zugriff verschlossene Daten zu erlangen. Dass dies auch verfassungsrechtlich nicht haltbar sein dürfte, erscheint anhand der zu diesen Fragen ergangenen Rechtsprechung des Bundesverfassungsgerichts jedenfalls hinsichtlich der Berufsgruppe der Strafverteidiger evident (dazu sogleich).

---

[40] vgl. SK-StPO/Wohlers/Greco § 97, Rn. 87 m. w. N.

2. Folgen für Anwälte, insbesondere Strafverteidiger

Effektive Verteidigung setzt ungestörte Kommunikation zwischen Verteidiger und Mandant voraus. Sobald der Beschuldigte mit staatlicher Kommunikationsüberwachung rechnen muss, steht dies einer unbefangenen und offenen Informationsweitergabe an den Verteidiger im Wege. Essenziell ist weiterhin, dass er jederzeit mit seinem Verteidiger Kontakt aufnehmen kann und insoweit keinen unsachgerechten zeitlichen Beschränkungen unterliegt. Die Vorschrift gibt dem Verteidiger ein eigenes Recht auf unkontrollierten Verkehr mit seinem inhaftierten Mandanten.[41] Dass eine solche Kommunikation auch notwendig diejenige eines Beschuldigten mit den Berufshelfern des Anwalts – etwa dessen Sekretariat – umfassen muss, ist evident und auch für den Gesetzgeber nicht disponibel:

Das Recht auf Verkehr mit dem Verteidiger ist Ausfluss des Rechts auf ein *faires Verfahren* und des Rechtsstaatsprinzips i.S.v. Art. 20 Abs. 3 GG[42] bzw. auch der Selbstbelastungsfreiheit des Beschuldigten. Sie sind daher geronnenes Verfassungsrecht, das dem einfachgesetzlichen Zugriff und entsprechender Einschränkung so nicht zugänglich ist. Zudem sind diese Rechte auch in der EMRK als solche auf *effektive* Verteidigung in Art. 6 Abs. 3 lit. c EMRK garantiert. Aus Sicht der anwaltlichen Tätigkeit unterfallen die Kommunikationsrechte des § 148 Abs. 1 StPO zudem dem Schutzbereich des Art. 12 GG, da sie für den Verteidiger elementare Grundlage seiner Tätigkeit sind.[43] Es sollte in Ansehung dieser Rechtspositionen selbstverständlich sein, dass die Kommunikation des Berufsgeheimnisträgers, welche er über seine Berufshelfer gleichsam als Boten vermittelt führt (was regelmäßig die Aufgabe etwa von Sekretariaten ist), keinen minderen Schutz erfährt als die unmittelbare.

3. Bezug zur Novelle des § 203 StGB

Wie wenig durchdacht und letztlich systemwidrig der Entwurf (auch) an dieser Stelle ist, verdeutlicht weiterhin die gerade im Gesetzgebungsprozess befindliche Novelle des § 203 StGB. Dort will der Gesetzgeber den

---

41 Beck-OK/Wessing § 148 StPO vor Rn. 1; s. a. MüKo/Thomas/Kämpfer § 148 StPO Rn. 1
42 vgl. etwa jüngst BVerfG 2 BvR 988/10 v. 7.3.2012 = NJW 2012, 2790
43 MüKo/Thomas/Kämpfer § 148 StPO Rn. 2

Berufsgeheimnisträgern die Möglichkeit verschaffen, sich verstärkt Dritter als Hilfspersonen zu bedienen, insbesondere auch soweit es um „digitales outsourcing“ oder die Wartung informationstechnischer Systeme geht.[44] Materiell-rechtlich soll mit diesem Entwurf zum einen die Erweiterung des Personenkreises, der mit Geheimnissen des Berufsgeheimnisträgers befasst wird, erleichtert und der heutigen Arbeitswelt angepasst, andererseits der Schutz dieser Geheimnisse bei Dritten unverändert durch Strafbarkeit der Offenbarung auch durch den erweiterten Personenkreis gewährleistet werden.[45]

Der Wertungswiderspruch dieser beiden parallel betriebenen Gesetzesvorhaben ist nicht hinnehmbar. Während das eine den Kreis von potenziellen Berufshelfern ausdehnt und dabei den Schutz der Geheimnisse materiell-rechtlich in vergleichbarer Weise wie beim Berufsgeheimnisträger vermeintlich gewährleisten soll, zielt das andere u. a. auch darauf, den Schutz dieser Geheimnisse bei Dritten zu relativieren, sofern sie staatlicherseits durch Quellen-TKÜ oder Online-Durchsuchungen von den Ermittlungsbehörden heimlich und ggf. auch zielgerichtet erlangt werden.

4. Praktische Auswirkungen

Für Anwälte, insbesondere auch Strafverteidiger, ist die geplante Regelung unakzeptabel. Sie müssten letztlich zum Schutze ihrer Mandanten in ihren Arbeitsabläufen verfügen, dass diese gerade auch per E-Mail nur noch mit ihnen direkt kommunizieren, um den Schutz der anvertrauten Geheimnisse gewährleisten zu können. Dies wird ähnlich mutmaßlich auch für die Arbeitsorganisation der anderen in § 53 StPO genannten Berufsgeheimnisträger und ihrer -helfer gelten.

---

[44] vgl. entsprechende Begründung des Gesetzesentwurfs der Bundesregierung zu § 203 StGB: http://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/ReGE_Neuregelung_Schutzes_von_Geheimnissen_bei_Mitwirkung_Dritter_an_der_Berufsausuebung_schweigepflichtiger_Personen.pdf?__blob=publicationFile&v=2 n. 1; Graf/Huber § 53a Rn. 1

[45] vgl. ausführlich zu diesem Gesetzesvorhaben Kargl, StV 2017, 482 ff.