Prof. Dr. Jan Dirk Roggenkamp
Prof. Dr. Frank Josef Braun

Korrespondenzadresse
c/o Digitalcourage e.V.
Marktstraße 18
33602 Bielefeld

Tel: 0521-1639 1639
Fax: 0521-6 11 72

An das
Bundesverfassungsgericht
Postfach 1771
76006 Karlsruhe

Karlsruhe/Bielefeld, den 7. August 2018

Verfassungsbeschwerde

des Herrn [redacted] - Beschwerdeführer zu 1 -

des Herrn - Beschwerdeführer zu 2 -

des Herrn - Beschwerdeführer zu 3 -

des Herrn - Beschwerdeführer zu 4 -

des Herrn - Beschwerdeführer zu 5 -

der Frau - Beschwerdeführerin zu 6 -

<u>Prozessbevollmächtigte:</u>

Prof. Dr. jur. Frank Josef Braun
Prof. Dr. jur. Jan Dirk Roggenkamp
c/o Digitalcourage e.V.
Marktstraße 18
33602 Bielefeld

Namens und im Auftrag der Beschwerdeführer erheben wir unter Beifügung entsprechender Vollmachten (**Anlage 1**) Verfassungsbeschwerde gegen § 100a Abs. 1 S. 2 und 3, Abs. 3 bis 6, § 100b sowie § 100d Abs. 1 bis 3 und Abs. 5 Strafprozessordnung (i.W. 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.),

und beantragen

1. § 100a Abs. 1 S. 2 und 3, Abs. 3 bis 6, § 100b sowie § 100d Abs. 1 bis 3 und 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.) für mit dem Grundgesetz unvereinbar und nichtig zu erklären;

2. den Beschwerdeführern die notwendigen Auslagen zu erstatten.

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. 13 Abs. 1 und Art. 19 Abs. 4 GG durch die oben genannten Vorschriften und begründen die Verfassungsbeschwerde wie folgt:

A. Sachverhalt

I. Inhalt der Regelungen

1. § 100a Abs. 1 S. 2, 3, Abs. 3, 5-6 StPO - Quellen-Telekommunikationsüberwachung

§ 100a Abs. 1 StPO (Telekommunikationsüberwachung) wurde um die hier angegriffenen Sätze 2 und 3 erweitert. Es wurde eine Befugnis zur Durchführung einer sog. Quellen-Telekommunikationsüberwachung geschaffen.

Die Vorschrift – die Ergänzung wurde durch die Unterzeichner hervorgehoben – lautet nunmehr:

> „(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.**“

§ 100a Abs. 3 StPO regelt unter anderem, dass sich eine Quellen-Telekommunikationsüberwachung nicht nur gegen Beschuldigte, sondern auch gegen (unverdächtige) Personen richten darf, deren informationstechnische Systeme durch den Beschuldigten benutzt werden. § 100a Abs. 3 StPO lautet nunmehr (Änderung hervorgehoben):

„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."

Die neu hinzugefügten Absätze 5 und 6 des § 100a StPO lauten:

„(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."

2. § 100b StPO - Online-Durchsuchung

Darüber hinaus wurde § 100b StPO vollständig neu gefasst. Es wurde eine Befugnis zur Durchführung einer sog. Online-Durchsuchung eines informationstechnischen Systems geschaffen.

Die Regelung lautet nunmehr:

> „§ 100b 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."

3. § 100d Abs. 1 bis 3 und Abs. 5 StPO - Kernbereichsschutz

Die Regelungen zum Kernbereichsschutz betreffend die Maßnahmen nach § 100a und § 100b StPO wurden in § 100d Abs. 1 bis 3 und Abs. 5 StPO wie folgt neu gefasst:

„§ 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.

[...]

(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. Gesetzgebungsverfahren

Die gegenständlichen Neuregelungen wurden (erst) im Rahmen der Beratungen des Gesetzentwurfs durch einen Änderungsantrag (BT-Drs. 18/12785) in das Gesetzgebungsverfahren eingebracht.[1]

Durch diesen Änderungsantrag wurden der Entwurf eines Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens (BT-Drs. 18/11277)[2] sowie der Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze (BT-Drs. 18/11272)[3], jeweils vom

[1] Darstellung auch bei *Roggan*, StV 2017, 821 (821).

[2] Hierdurch sollten z.B. eine Pflicht für Zeugen, bei der Polizei zu erscheinen, Änderungen im Befangenheitsrecht, die Möglichkeit einer Fristsetzung im Beweisantragsrecht und die teils verpflichtende audiovisuelle Aufzeichnung von Beschuldigtenvernehmungen im Ermittlungsverfahren eingeführt werden.

[3] Dieser regelte u.a. die Möglichkeit der Verhängung eines Fahrverbots bei allen Straftaten, die Ergänzung von § 266 a StGB und die Schaffung einer Ausnahme von der vorrangigen richterlichen Anordnungskompetenz für die Entnahme einer Blutprobe bei bestimmten Straßenverkehrsdelikten.

22.2.2017, zusammengefasst, und – wie *Beukelmann*[4] zutreffend feststellt – „*durch die Hintertür erheblich erweitert*".

Diese Erweiterung enthielt erstmals auch die hier angegriffenen Neuregelungen.

Der o.g. Änderungsantrag basierte seinerseits auf einer vom Ausschuss für Recht und Verbraucherschutz fast wörtlich übernommenen „Formulierungshilfe" der Bundesregierung vom 15.05.2017.[5]

Nach einer am 31.05.2017 durchgeführten Sachverständigenanhörung – mit äußerst konträren Einschätzungen – und einer abschließenden Beratung vom 20.06.2017 wurde das Gesetzespaket am 22.06.2017 vom Bundestag verabschiedet.

Der Empfehlung des Ausschusses für Agrarpolitik und Verbraucherschutz zur Anrufung des Vermittlungsausschusses mit dem Ziel, die hier angegriffenen Regelungen zu streichen, ist der Bundesrat nicht gefolgt[6].

III. Technische Hintergründe

1. Online-Durchsuchung (§ 100b StPO)

§ 100b StPO gestattet eine sog. Online-Durchsuchung. Hiermit wird der heimliche Zugriff auf informationstechnische Systeme bezeichnet, der auf eine längerfristige Überwachung[7] mit Hilfe einer sog. Trojanersoftware abzielt.[8]

Im Rahmen einer Online-Durchsuchung haben die Ermittlungsbehörden mit Installation der Trojanersoftware vollumfänglichen Zugriff auf das gesamte informationstechnische System.

---

[4] *Beukelmann*, NJW Spezial 2017, 440.
[5] Formulierungshilfe der Bundesregierung vom 15.5.2017, Ausschussdrucksache 18[6]334.
[6] Vgl. BR-Drs. 527/1/17; BR-Drs. 527/17 (Beschluss).
[7] Dementsprechend wird durch § 100e Abs. 2 StPO eine Anordnung der Online-Durchsuchung für einen Zeitraum von zunächst einem Monat gestattet. Eine Verlängerung ist ausweislich § 100e Abs. 2 StPO möglich. Zwar darf nur jeweils eine Verlängerung von einem Monat gestattet werden, eine zeitliche Obergrenze ist jedoch nicht vorgesehen.
[8] *Petri*, in Lisken/Denninger, Handbuch Polizeirecht, Teil G Rn. 355.

Sie können sämtliche auf dem System vorhandenen Dateien lesen, verändern und herunterladen. Alle auf dem Gerät installierten Programme bzw. sog. Apps können ausgeführt oder beendet werden. Software kann heimlich installiert und gelöscht werden.

Mit der Trojanersoftware können vorhandene Kameras (sog. Webcams, aber auch sonstige mit dem System verbundene Kameras wie z.B. optische Babyfone und Hausüberwachungssysteme) und Mikrofone ein- und ausgeschaltet und über diese der Nutzer des Systems und dessen Umgebung beobachtet werden. Es besteht damit die Möglichkeit eines „Großen Spähangriffs“[9].

Zudem kann jederzeit der aktuelle Bildschirminhalt überwacht und aufgezeichnet werden, so dass die Nutzung des informationstechnischen Systems de facto in Echtzeit mitverfolgt werden kann.

Über sog. Keylogging-Funktionen kann zudem jede Tastatureingabe überwacht und aufgezeichnet werden, auch wenn diese nicht (z.B. in einem Dokument) auf dem informationstechnischen System gespeichert wird. So können z.B. auch Passworteingaben aufgezeichnet werden, wenn diese auf dem Bildschirm nicht dargestellt werden (vgl. Abbildung).

[9] So *Beukelmann*, NJW-Spezial 2017, 440.

Abbildung 1: Verdeckte Passworteingabe

2. Quellen-Telekommunikationsüberwachung (§ 100a Abs. 1 S. 2 StPO)

Durch § 100a Abs. 1 S. 2 StPO wird eine sog. Quellen-Telekommunikationsüberwachung gestattet. Durch sie soll das Mitlesen und Mithören der Inhalte verschlüsselter laufender Kommunikation (z.B. über sog. Messenger wie WhatsApp oder Signal) ermöglicht werden.

Hierzu müssen sämtliche Kommunikationsinhalte vor der Verschlüsselung bzw. nach der Entschlüsselung ausgeleitet werden. Dies soll technisch durch einen Zugriff auf dem informationstechnischen System (der „Quelle" der Telekommunikation) erfolgen. Auch hier wird eine Trojanersoftware, die heimlich auf dem Zielsystem installiert werden muss, genutzt.

3. „Kleine Online-Durchsuchung" (§ 100a Abs. 1 S. 3 StPO)

Durch § 100a Abs. 1 S. 3 StPO wird ergänzend ein heimlicher Zugriff auf *„gespeicherte Inhalte und Umstände der Kommunikation"* zugelassen, *„wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können"*.

Es handelt sich hierbei nicht mehr um eine (Quellen-)Telekommunikationsüberwachung, da diese nur die laufende Kommunikation erfasst.

Da § 100a Abs. 1 S. 3 StPO einen Zugriff auf „ruhende“ Kommunikation (gespeicherte Inhalte und Umstände der Kommunikation) auf einem informationstechnischen System gestattet, stellt die Maßnahme eine Online-Durchsuchung dar. Sie wird auf Grund ihrer inhaltlichen Beschränkung auf Telekommunikationsinhalte und -umstände auch als „kleine Online-Durchsuchung“ bezeichnet.[10]

4. Vorgehensweise

Unabhängig davon, ob eine Online-Durchsuchung, eine „kleine Online-Durchsuchung“ oder eine Quellen-Telekommunikationsüberwachung durchgeführt werden soll, muss eine Softwarelösung[11] eingesetzt werden, mit Hilfe derer ein Zugriff auf das Zielsystem ermöglicht wird (sog.„Trojanersoftware“).

Hierzu ist es erforderlich, auf dem informationstechnischen System der Zielperson (in der Regel einem Smartphone) die Trojanersoftware heimlich zu installieren (sog. Infiltration), um dann aus der Ferne auf das informationstechnische System zugreifen zu können.

Die Installation erfolgt technisch durch Ausnutzen eines Programmierfehlers, einer sog. Sicherheitslücke in einer Software auf dem von der Zielperson genutzten System. Hierbei kann es sich um das Betriebssystem oder auch eine Anwendungssoftware handeln. Der Zielperson wird z.B. ein unverdächtig erscheinendes Textdokument zugesandt (oder auf einem Datenträger übergeben). Sobald dieses geöffnet wird, wird die Trojanersoftware bei bestehender Internetverbindung unbemerkt auf das Zielsystem geladen und installiert.[12]

---

[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), S. 5 - (i.W. *Sinn*, Stellungnahme); *Roggan*, StV 2017, 821 (824).

[11] Eine gewisse Marktführerstellung hat hierbei offenbar die Software FinSpy des Anbieters FinFisher, vgl. *Holland*, FinSpy: Deutsche Überwachungssoftware gegen türkische Opposition eingesetzt, heise.de v. 15.5.2018 - https://www.heise.de/newsticker/meldung/FinSpy-Deutsche-Ueberwachungssoftware-gegen-tuerkische-Opposition-eingesetzt-4049677.html - Ausdruck als **ANLAGE 2** anbei.

[12] Vgl. z.B. *Gierow*, FINSPY: Neuer Staatstrojaner-Exploit in RTF-Dokument gefunden, golem.de v. 13.9.2017 - https://www.golem.de/news/finspy-neuer-staatstrojaner-exploit-in-rtf-dokument-gefunden-1709-130025.html - Ausdruck als **ANLAGE 3** anbei.

Vor der Installation muss eine solche Sicherheitslücke entweder eigenständig ermittelt oder entsprechende Informationen über diese Schwachstellen von Dritten „beschafft" werden. Der Ankauf von Informationen über offene Sicherheitslücken erfolgt auf entsprechenden „Schwarzmärkten". Hauptnachfrager sind nach Erkenntnissen der Gesellschaft für Informatik e.V. (i.W. „GI") Cyberkriminelle, die diese für die Installation sog. Ransomware (also eine Software, die einen Computer infiziert, sperrt und dann Geld dafür verlangt, ihn zu entsperren) ausnutzen wollen.[13]

Die Nutzung der Sicherheitslücken ist regelmäßig nur zeitlich beschränkt möglich. Sobald die Hersteller die betreffenden Sicherheitsdefizite in ihren Softwareprodukten/Betriebssystemen beseitigen können [14] , ist ein Zugriff ausgeschlossen. Dementsprechend ist es, soll die Sicherheitslücke für Zwecke der Online-Durchsuchung oder Quellen-Telekommunikationsüberwachung tauglich sein, erforderlich, diese den Anbietern der lückenhaften Software *nicht* mitzuteilen. Damit ein effektiver Zugriff auf ein möglichst breites Portfolio von Betriebssystemen (z.B. Windows, Linux, iOS, Android, MacOS) und Anwendungssoftware (z.B. Microsoft Office, Adobe PDF) möglich ist, müssen möglichst viele Sicherheitslücken ermittelt, vorgehalten und genutzt werden. Der Bedarf kann de facto nur durch einen Ankauf von Informationen zu (unbekannten) Sicherheitslücken und Möglichkeiten zur Ausnutzung auf dem „freien Markt" gedeckt werden.

Wird eine Sicherheitslücke nicht geschlossen, kann sie nicht nur von den Strafverfolgungsbehörden, sondern auch von jedem anderen genutzt werden.

Dies war z.B. im Jahr 2017 der Fall, als eine von der amerikanischen NSA „vorgehaltene" Sicherheitslücke von Cyberkriminellen zur Verbreitung des Schadprogramms „WannaCry" genutzt wurde. Dieses Schadprogramm infizierte im Mai 2017 über eine Sicherheitslücke im Windows-Betriebssystem innerhalb weniger Tage weltweit eine

---

[13] *Federrath*, Stellungnahme der GI zum Gesetzentwurf der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen v. 6. und 8.2.2018 - abrufbar unter https://gi.de/fileadmin/GI/Hauptseite/Aktuelles/Meldungen/2018/GI-Stellungnahme_Neuausrichtung_HessVS_2018-02-08.pdf - Ausdruck als **ANLAGE 4** anbei.

[14] Das Schließen einer Sicherheitslücke erfolgt über einen sog. Patch,der über die (häufig automatisch ausgeführte) Aktualisierungsfunktion der Software auf dem System eingespielt wird.

große Zahl von informationstechnischen Systemen und legte sie lahm. Betroffen waren neben vielen privaten Nutzern z.B. die Deutsche Bahn AG, der japanische Autohersteller Nissan, der französische Autohersteller Renault sowie Banken, Geldautomaten und Schulen. [15] Auch lebenswichtige Einrichtungen wie z.B. Krankenhäuser waren betroffen.[16] Die Folgen des Angriffs, dessen Umfang auf Millionen von Infektionen geschätzt wird, dauern bis heute an.[17]

5. Insbesondere: Limitierung des Zugriffs auf „laufende Kommunikation“

Nach den Vorgaben des *BVerfG* ist bei Quellen-Telekommunikationsüberwachungsmaßnahmen durch „*technische Vorkehrungen*“ sicherzustellen, dass „*sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt*“[18]. Dies wurde in einer späteren Entscheidung dahingehend konkretisiert, dass die zur Quellen-Telekommunikationsüberwachung genutzte Software so ausgestaltet sein müsse, dass sie *„hinreichend abgesichert auch gegenüber Dritten – den mit der Überwachung betrauten Mitarbeiterinnen und Mitarbeitern [...] – inhaltlich eine ausschließlich auf die laufenden Kommunikationsinhalte begrenzte Kenntnisnahme ermöglicht.*“[19]

Eine Trojanersoftware zur Durchführung einer Quellen-Telekommunikationsüberwachung darf dementsprechend weder beabsichtigt noch unbeabsichtigt persönlichkeitsrelevante Informationen erheben, die nicht Inhalte und Umstände der laufenden Telekommunikation betrifft.

---

[15] *Biermann*, WannaCry: Großer Schaden für 31.000 Dollar, Zeit Online v. 14.05.2017, https://www.zeit.de/digital/datenschutz/2017-05/wannacry-ransomware-cyberattacke-bitcoin-windows-microsoft - Ausdruck als **ANLAGE 5** anbei.
[16] Vgl. z.B. *Wittmann*, Erpresser-Software lähmt 40 Kliniken in Großbritannien, Berliner Morgenpost v. 12.05.2017, https://www.morgenpost.de/politik/article210553117/Krankenhaeuser-in-England-durch-Hacker-Angriff-lahmgelegt.html - Ausdruck als **ANLAGE 6** anbei.
[17] *Gierow*, MS17-010: Noch immer Millionen Wanna-Cry-Infektionen aktiv, golem.de v. 14.05.2018, https://www.golem.de/news/ms17-010-noch-immer-millionen-wanna-cry-infektionen-aktiv-1805-134360.html - Ausdruck als **ANLAGE 7** anbei.
[18] BVerfGE 120, 274 (309 - Rn. 190).
[19] BVerfGE 141, 220 (311f. - Rn. 234).

Es ist jedoch technisch nicht möglich derartige Vorkehrungen zu treffen und somit die verfassungsrechtlichen Anforderungen zu erfüllen.[20]

Eine Quellen-Telekommunikationsüberwachung zielt darauf ab, auf Kommunikationsinhalte vor deren Verschlüsselung zuzugreifen. Es muss damit aus technischer Sicht – notwendigerweise – gerade nicht die „laufende Telekommunikation" überwacht werden. Die Telekommunikation kann erst dann als „laufend" betrachtet werden, wenn sie vom Absender unwiderruflich und ohne Möglichkeit der Rückholung dem Informationsmittler (z.B. dem Messengerdienstanbieter) technisch „übergeben" wurde, z.B. durch Anklicken des „Absendebutton". Die Trojanersoftware greift indes bereits vor diesem Zeitpunkt auf die Inhalte zu. Es werden bereits Entwürfe von Nachrichten, die mehr oder weniger kurz vor dem Absenden erstellt wurden (und ggf. dann gar nicht mehr abgesendet werden) abgegriffen.[21]

Zudem muss eine Software zur Durchführung einer Quellen-Telekommunikationsüberwachung denknotwendigerweise weitere Daten erheben und weiterleiten, die weder laufende noch ruhende Kommunikation darstellen. So muss die Trojanersoftware beispielsweise erfassen (und weiterleiten), wann das überwachte informationstechnische System ein- und ausgeschaltet wird, ob es – unabhängig von einem konkreten Kommunikationsvorgang – mit dem Internet verbunden ist, ob und welche Kommunikationsprogramme – ebenfalls unabhängig von einem konkreten Kommunikationsvorgang – geöffnet oder geschlossen wurden. Da stets die Möglichkeit besteht, dass ein informationstechnisches System und die darauf vorgehaltenen Kommunikationsprogramme von verschiedenen Personen genutzt werden, muss die Trojanersoftware den Zugriff verschiedener Nutzer protokollieren. Zudem wird, um nicht in rechtswidriger Weise eine Telekommunikationsüberwachung außerhalb Deutschlands durchzuführen, eine permanente Erhebung und Übermittlung des Standorts des Geräts erforderlich sein.

---

[20] *Kurz/Neumann/Rieger/Engling*, „Stellungnahme zur „Quellen-TKÜ" nach dem Urteil des Bundesverfassungsgerichts vom 20. April 2016 - 1 BvR 966/09", S. 6 ff., https://www.ccc.de/system/uploads/216/original/quellen-tkue-CCC.pdf - Ausdruck als **ANLAGE 8** anbei.

[21] *Hornung*, Stellungnahme zur öffentlichen Anhörung zu dem Gesetzentwurf der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen - Drucks. 19/5412 - sowie dem Änderungsantrag der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN - Drucks. 19/5782 - S. 6 (i.W. „*Hornung*, Stellungnahme").

Somit ist eine Überwachung der Telekommunikationsaktivitäten „an der Quelle“ faktisch nur im Wege einer Online-Durchsuchung möglich.

6. Ausgestaltung der genutzten Software und Überprüfung

Quellen-Telekommunikationsüberwachungsmaßnahmen sowie Online-Durchsuchungen sind im präventiv-polizeilichen Bereich bereits etabliert.

Darüber, welche Programme verwandt und welche Methoden zur Installation genutzt werden, kann nur spekuliert werden. Auch über den Umfang der Funktionalitäten der genutzten Software gibt es keine belastbaren Informationen.

Im Gegenteil: Eine von der Plattform *netzpolitik.org* veröffentlichte Stellungnahme des Parlamentarischen Staatssekretärs *Mayer* (BMI) aus der 18. Sitzung des Bundestagsausschusses für Inneres und Heimat vom 13. Juni 2018 suggeriert, dass zur Durchführung der in Rede stehenden Überwachungsmaßnahmen kommerzielle Software eingesetzt wird, deren Quellcode außer den (privaten) Herstellern niemandem (!) bekannt ist und bekanntgegeben wird.

In dem kolportierten Wortprotokoll[22] wird dem Parlamentarischen Staatssekretär folgende Äußerung zugeschrieben:

> *„...ich bitte einfach um Verständnis, dass wir keine konkreten Unternehmensnamen nennen können, die hier mit dem BKA oder mit dem BMI zusammenarbeiten. Ich sage es hier ganz offen, die sind verbrannt, wenn die Namen zirkulieren und öffentlich werden. Ich habe auch Verständnis dafür, dass die Unternehmen das Heiligste ihres Geschäftsinteresses, die Quellcodes, nicht offenbaren können.“*

Aus dem Protokoll geht zudem hervor, dass entsprechende Informationen nicht einmal bei der Geheimschutzstelle des Deutschen Bundestags hinterlegt wurden:

---

[22] Wiedergabe bei *Meister*, Geheime Sitzung im Bundestag: Regierung verweigert jede Auskunft über Staatstrojaner-Firmen, netzpolitik.org v. 12.7.2018, https://netzpolitik.org/2018/geheime-sitzung-im-bundestag-regierung-verweigert-jede-auskunft-ueber-staatstrojaner-firmen/ - Ausdruck als **ANLAGE 9** anbei.

> „*Es wäre in keiner Weise zu rechtfertigen, wenn wir, selbst unter Hinweis auf eine Hinterlegung bei der Geheimschutzstelle des Deutschen Bundestages, die Namen hinterlegen würden. Ich habe dies schon oft genug erfahren müssen, dass da leider doch Dokumente oder Inhalte von Dokumenten aus der Geheimschutzstelle den Weg in die Öffentlichkeit gefunden haben.*“[23]

Sollte dies zutreffen, liegt es nahe, dass entsprechende Informationen im Falle einer Überwachung erst recht nicht dem anordnenden Gericht vorgelegt würden, noch dass eine Überprüfung der Rechtskonformität der Software und des Softwareeinsatzes im Verfahren möglich wäre oder diese vor dem Einsatz erfolgt.

Der ehemalige Bundesbeauftragte für Datenschutz und Informationsfreiheit *Peter Schaar* hat treffend wie folgt ausgeführt[24]:

> „*Ob diese Grenzen [*Anm. die Vorgaben des *BVerfG* zu den Grenzen einer Quellen-Telekommunikationsüberwachung*] eingehalten werden, kann nur durch die Begutachtung und systematisches Testen der Software beurteilt werden. Erforderlich ist hierzu die Vorlage des sogenannten Quellcodes – einen lesbaren, in einer Programmiersprache geschriebenen Text der eingesetzten Software –, damit sich die verantwortliche Stelle nachhaltig über den Umfang der zur Verfügung stehenden programmierten Funktionen überzeugen kann. Auch eine verlässliche und umfassende interne oder externe Datenschutzkontrolle ist nur unter diesen Voraussetzungen möglich.*
>
> *Insbesondere ist ohne die Vorlage des Quellcodes eine sichere Beurteilung einer Software hinsichtlich des Vorhandenseins oder eben Nichtvorhandenseins von Funktionen nicht möglich. Die Übersendung oder Vorlage nur eines umfangreichen ausführbaren Programms (Codes, Binärcodes) reicht zur Beurteilung nicht, denn*

[23] Ebda.

[24] BfDI, Bericht gemäß § 26 Abs. 2 Bundesdatenschutzgesetz über Maßnahmen der Quellen-Telekommunikationsüberwachung bei den Sicherheitsbehörden des Bundes, S. 40 f. - abrufbar unter https://www.ccc.de/system/uploads/103/original/Schaar-Bericht.pdf (Ausdruck als **ANLAGE 10** anbei - i.W. „BfDI, Bericht“).

> *vor allem das Nichtvorhandensein von Funktionen kann allein anhand eines Binärcodes nicht abschließend bewertet werden.*
>
> *Auch (mögliche) Seiteneinstiege für Dritte und andere Sicherheitslücken sind allein mit Hilfe des Binärcodes nicht auszuschließen. Gerade bei Überwachungssoftware, mit der in einem rechtstaatlichen Verfahren auch gerichtsverwertbare Daten erhoben werden sollen, sind Fragen nach den Möglichkeiten der Manipulation der Daten von immenser Wichtigkeit. Die Vertraulichkeit und Unversehrtheit der erhobenen Daten sind hier von entscheidender Bedeutung. Dies betrifft nicht nur die Übertragungswege, sondern auch die Speicherung der Daten in jedem Stadium der Überwachungsmaßnahme.*"

Es ist also unmöglich zu überprüfen, wie die Software funktioniert. Eine Kontrolle, ob sich der kommerzielle Hersteller einer Trojanersoftware eine Hintertür für „eigene Zwecke" offengelassen hat oder ob die Software selbst eine Sicherheitslücke hat, steht nicht offen. Zudem ist nicht sichergestellt, dass elementare Anforderungen bezüglich des Datenschutzes erfüllt werden[25], wie sie insbesondere in der Richtlinie (EU) 2016/680 des Europäischen Parlamentes und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates niedergelegt wurden.

IV. Tatsächliche Nutzung von informationstechnischen Systemen

Im Jahr 2008 hat das *BVerfG* festgestellt, dass mit der Infiltration eines informationstechnischen Systems die entscheidende Hürde genommen ist, um dieses

[25] Das war z.B. bei der bis 2011 verwendeten Staatstrojanersoftware des Unternehmens DigiTask wohl nicht der Fall, vgl. Beckedahl, Geleakt: Datenschutzbericht zum Staatstrojaner, netzpolitik.org v. 17. 2. 2018, https://netzpolitik.org/2012/geleakt-datenschutzbericht-zum-staatstrojaner/ Ausdruck als **ANLAGE 11** anbei - der referenzierte Bericht ist unter https://www.ccc.de/system/uploads/103/original/Schaar-Bericht.pdf abrufbar und liegt als **ANLAGE 10** anbei.

insgesamt auszuspähen.[26] In der Folge sei es möglich, heimlich „*ein umfangreiches Verhaltens- und Kommunikationsprofil*“ der jeweiligen Nutzer des Zielsystems zu erstellen.[27]

Heute, zehn Jahre später, ist diese Feststellung in dieser Form nicht mehr zutreffend. Eine Überwachung eines informationstechnischen Systems wie sie durch die gegenständlichen Regelungen ermöglicht wird, ist nicht nur geeignet „*ein umfangreiches Verhaltens- und Kommunikationsprofil*“ zu erstellen. Sie ist vielmehr darauf angelegt, die betroffene Person in ihrer *gesamten* Persönlichkeit zu erfassen.

Dies gilt insbesondere für die durch die Maßnahmen intendierte Überwachung von Smartphones, also Mobiltelefonen mit umfangreichen Funktionalitäten (Foto, Navigation, Ausführen von diversen Anwendungsprogrammen etc.) und Internetzugang.

Durch die Überwachung dieser Geräte kann die überwachende Stelle mehr und umfangreichere Informationen über die betroffene Person und ihre Persönlichkeit erhalten, als diese ihren intimsten Gesprächspartnern oder z.B. einem Tagebuch preisgeben würde.

Die Überwachung des Smartphones macht dessen Nutzer zum schutzlosen, gläsernen Objekt staatlicher Beobachtung.

Inzwischen nutzen in Deutschland rund 57 Millionen Menschen ein Smartphone[28]. Solche Geräte werden nicht – wie dies vor zehn Jahren bei PCs der Fall war – vorwiegend als Arbeitsgeräte genutzt, sondern dienen ganz überwiegend persönlichen und persönlichsten Zwecken.

[26] BVerfGE 120, 274 (308f. - Rn. 188).
[27] BVerfGE 120, 274 (323f. - Rn. 234 - 238.)
[28] Bitkom, Anzahl der Smartphone-Nutzer in Deutschland in den Jahren 2009 bis 2018 (in Millionen), Statista, https://de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenutzer-in-deutschland-seit-2010/ - Ausdruck als **ANLAGE 12** anbei.

Sie sind für ihre Nutzer intimer und intensiv genutzter Begleiter vom Aufstehen bis zum Zubettgehen. Smartphonebesitzer im Alter zwischen 18 und 24 Jahren nutzen im Schnitt über fünfzig Mal am Tag ihr Gerät.[29]

Die inzwischen in jedem Smartphone eingebaute Foto- und Videotechnik wird von 90 Prozent der Smartphonebesitzer auch genutzt.[30] Die Einsatzmöglichkeiten der Geräte sind vielfältig, faktisch in aller Regel aber privater Natur, wie etwa zur Herstellung von Fotos im familiären Bereich. Weit verbreitet ist auch das sog. Sexting, also das Erstellen und Austauschen erotischer Selbstportraits mit dem Smartphone.[31] Sobald ein Foto oder Video erstellt wird, wird es in digitaler Form auf dem informationstechnischen System gespeichert. Regelmäßig wird zudem automatisch eine Kopie unter Nutzung der Internetverbindung an einen externen Speicherdienst (sog. Cloud-Diensteanbieter – z.B. Apple iCloud, GoogleDrive) gesendet und dort abgelegt. Gerätespeicher und Anbietercloud werden typischerweise als dauerhafte Foto- und Videoarchive genutzt.

Ebenfalls regelmäßig (ca. 74 % der Nutzer) werden Suchmaschinen über das Smartphone aufgerufen. Auch hier dominiert die private Nutzung. Bei der Suche nach Antworten (und Hilfe) in privaten und privatesten Angelegenheiten, wie zum Beispiel der Behandlung und Diagnose von Krankheiten ist für einen Großteil der Nutzer die Abfrage von Suchmaschinen und der Besuch der dort zu findenden Webseiten selbstverständlich. [32] Die eingegebenen Suchbegriffe, aber auch die aufgerufenen Internetseiten, werden im jeweiligen informationstechnischen System gespeichert.

---

[29] *Nier*, "Ziemlich bester Smartphone-Freund" (Statista GmbH) (2018), https://de.statista.com/infografik/13337/umfrage-smartphone-nutzungsverhalten/ - Ausdruck als **ANLAGE 13** anbei.

[30] Bitkom, Anteil der befragten Smartphone-Nutzer, die die folgenden Funktionen mit ihrem Smartphone nutzen, Statista, https://de.statista.com/statistik/daten/studie/166150/umfrage/nutzung-von-smartphone-funktionen-in-deutschland/ - Ausdruck als **ANLAGE 14** anbei.

[31] Über 50 % der erwachsenen Smartphonenutzer haben bereits einmal ein erotisches Selbstporträit erstellt und weitergeleitet, vgl. *Döring*, „Sexting. Aktueller Forschungsstand und Schlussfolgerungen für die Praxis“, in: Bundesarbeitsgemeinschaft Kinder- und Jugendschutz e.V., „Gewalt im Netz“, S. 15 (19) - mit weiteren Nachweisen und umfassender Darstellung des Phänomens. - Kopie der zitierten Seite als **ANLAGE 15** anbei.

[32] Bitkom, Habe Sie schon einmal Krankheitssymptome in eine Internet-Suchmaschine eingegeben?, Statista, https://de.statista.com/statistik/daten/studie/546285/umfrage/eingabe-von-krankheitssymptomen-in-suchmaschinen-nach-geschlecht-in-deutschland/ - Ausdruck als **ANLAGE 16** anbei; Civey, Informieren Sie sich online über Ihre Symptome, bevor Sie zum Arzt gehen?, Statista, https://de.statista.com/statistik/daten/studie/741962/umfrage/umfrage-in-deutschland-zur-internetrecherche-nach-symptomen-vor-dem-arztbesuch/ - Ausdruck als **ANLAGE 17** anbei.

Abhängig von der verwendeten Internetzugangssoftware wird der Verlauf der Internetaktivitäten dauerhaft im Speicher des Geräts abgelegt.

Über informationstechnische Systeme werden auch die unterschiedlichsten sozialen Netzwerke (z.B. Facebook) zur Interaktion und Kommunikation mit Bekannten, Freunden und dem oder den Geschlechtspartnern genutzt. Darüber hinaus dienen soziale Netzwerke dem Austausch mit „gleichgesinnten" Personen in unterschiedlichsten Kontexten. Die Möglichkeit der anonymen Nutzung dieser Netzwerke ermöglicht es den Teilnehmern sich frei und ohne Selbstzensur und Angst vor (vermeintlichen) Repressalien über die sie interessierenden Themen auszutauschen und ihre Meinung frei zu äußern. Auch diese Aktivitäten werden mitunter dauerhaft auf dem jeweils genutzten Gerät protokolliert und „archiviert".

Die in einem Smartphone enthaltene GPS-Funktion wird regelmäßig (64 %)[33] zu Navigationszwecken bzw. zur Orientierung mit Hilfe von Kartenapps (z.B. Google Maps) verwendet. Der Standort des Smartphones wird zudem unabhängig von der Nutzung im System erfasst. In der Regel wird durch das System automatisch ein Bewegungsprofil erstellt und dauerhaft gespeichert[34]. Aus diesem kann abgelesen werden, wann, wie lange und wie häufig der Nutzer des Smartphones bestimmte Orte besucht hat (vgl. Abbildung).

[33] Bitkom, Anteil der befragten Smartphone-Nutzer, die die folgenden Funktionen mit ihrem Smartphone nutzen, Statista, https://de.statista.com/statistik/daten/studie/166150/umfrage/nutzung-von-smartphone-funktionen-in-deutschland/ - Ausdruck als **ANLAGE 14** anbei.

[34] Siehe zum Umfang der Speicherung am Beispiel von Apple iPhones Erxleben, Versteckte iPhone-Karte speichert deine Standorte, in: BASICthinking Blog, https://www.basicthinking.blog/blog/2018/04/18/versteckte-iphone-karte/ - Ausdruck als **ANLAGE 18** anbei.

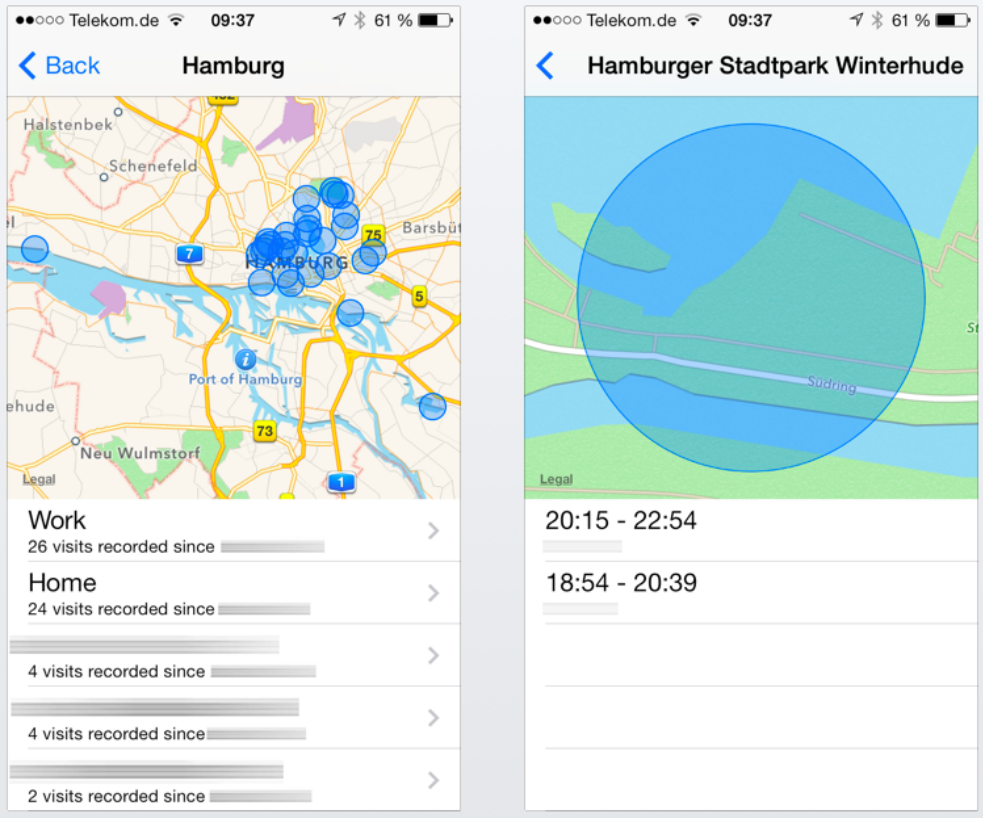

Abbildung 2: Darstellung häufig besuchter Orte iPhone

Dass ein solches Profil automatisiert angelegt wird, ist der weit überwiegenden Zahl der Nutzer eben so wenig bekannt wie das technische Wissen um dieses Profil zu löschen.[35]

Für über 20 Prozent[36] der Smartphonenutzer ist dieses der Begleiter bei der Suche nach (potentiellen) Lebens- oder Geschlechtspartnern (sog. Dating). Die Dating-Applikation Tinder ist im Juni 2018 die dritterfolgreichste Applikation für Smartphones der Marke iPhone gewesen, die Dating-Applikation LOVOO folgte auf dem siebten Platz.[37]

[35] *Fiene*, „Wenn Smartphones uns den Spiegel vorhalten“, in: RP Online v. 14.9.2014, https://rp-online.de/digitales/internet/apple-iphone-wie-eine-landkarte-ihre-lieblings-orte-verraet_aid-20117101 - Ausdruck als **ANLAGE 19** anbei.
[36] Bitkom, Anteil der befragten Smartphone-Nutzer, die die folgenden Funktionen mit ihrem Smartphone nutzen, Statista, https://de.statista.com/statistik/daten/studie/166150/umfrage/nutzung-von-smartphone-funktionen-in-deutschland/ - Ausdruck als **ANLAGE 14** anbei.
[37] Priori Data, Ranking der erfolgreichsten iPhone-Apps nach Umsatz in Deutschland im Juni 2018 (in 1.000 US-Dollar), Statista, https://de.statista.com/statistik/daten/studie/691356/umfrage/erfolgreichste-iphone-apps-nach-umsatz-in-deutschland/ - Ausdruck als **ANLAGE 20** anbei.

Durch den heimlichen Zugriff auf ein Smartphone wird der zugreifenden Stelle mit Blick auf die Art der Informationen, die abgerufen werden können, aber auch mit Blick auf den Umfang der abrufbaren Informationen, technisch unvermeidbar ein Einblick in die engste Persönlichkeitssphäre des Betroffenen gewährt, der mit keiner anderen Überwachungsmaßnahme vergleichbar ist. Selbst durch eine Kombination von „herkömmlichen" heimlichen Maßnahmen wie der akustischen Wohnraumüberwachung, der (einfachen) Telekommunikationsüberwachung und der (technikunterstützten) längerfristigen Observation können keine derart umfassenden Einblicke in die Privat- und Intimsphäre, insbesondere die Gedankenwelt der betroffenen Personen gewonnen werden.

V. Beschwerdeführerinnen und Beschwerdeführer

Die Beschwerdeführerinnen und Beschwerdeführer (i.W. „Beschwerdeführer") nutzen allesamt informationstechnische Systeme und kommunizieren über diese teils verschlüsselt. Die Nutzung findet auch und gerade im privaten Bereich statt. Die Beschwerdeführer recherchieren Informationen zu unterschiedlichsten privaten Themen im Internet und tauschen sich anonym in Internetforen aus. Alle Beschwerdeführer nutzen sog. Smartphones mit Kamera(s), GPS-Funktion und eingebautem Mikrofon. Alle Beschwerdeführer überlassen ihre informationstechnischen Systeme bei Bedarf (und Vertrauen) anderen Personen zur Mitnutzung. Ebenso nutzen sie informationstechnische Systeme von Dritten (z.B. Freunde/Verwandte aber auch von kommerzielle Anbietern wie z.B. Internetcafés).

Der *Beschwerdeführer zu 1*, [redacted], ist Rechtsanwalt, Journalist, Publizist und Kuratoriumsmitglied der Internationalen Liga für Menschenrechte. Seit 2007 ist er stellvertretender Richter am Staatsgerichtshof der Freien Hansestadt Bremen sowie Mitglied der staatlichen Deputation für Inneres der Bremischen Bürgerschaft. Er arbeitet zudem als Sachverständiger in Gesetzgebungsverfahren, u.a. zu Antiterror-Gesetzen im Bundestag, zu Verfassungsschutz- und Polizeigesetzen in diversen Landtagen; er ist außerdem Mitglied der Jury zur Verleihung des Negativpreises „BigBrotherAward" an Institutionen, die in besonderem Maße den Datenschutz missachten sowie Mitherausgeber des jährlich erscheinenden „Grundrechte-Reports – Zur Lage der Bürger- und Menschenrechte in Deutschland" (Fischer-Verlag, Ffm). Er

wurde von 1970 bis 2008 wegen Kontakten zu angeblich „linksextremistischen" beziehungsweise „linksextremistisch beeinflussten" Personen und Gruppierungen durch das Bundesamt für Verfassungsschutz heimlich beobachtet. Im Verfahren vor dem OVG NRW (Az. 16 A 906/11 n.rkr. – Vorinstanz VG Köln Az.: 20 K 2331/08) wurde behauptet, dass während des gesamten Beobachtungszeitraums tatsächliche Anhaltspunkte für verfassungsfeindliche Bestrebungen des Klägers und für die Unterstützung solcher Bestrebungen vorgelegen hätten (in beiden Instanzen ist die geheimdienstliche Langzeitbeobachtung für rechtswidrig erklärt worden). Der Beschwerdeführer hat die naheliegende Befürchtung, dass er beziehungsweise die von ihm privat und beruflich genutzten informationstechnischen Geräte Ziel repressiver Maßnahmen der hier angegriffenen Art werden könnten. Dies auch und nicht zuletzt auf Grund seiner Tätigkeit als Anwalt und Strafverteidiger, bei welcher er auch mit Personen in Kontakt kommt, die Zielperson von Quellen-Telekommunikationsüberwachungen und Online-Durchsuchungen werden können. Aber auch im Rahmen seiner Tätigkeit als Publizist und Buchautor (z.B. „Geheime Informanten. V-Leute des Verfassungsschutzes: Neonazis im Dienst des Staates", München 2003/2012) kommt der Beschwerdeführer – insbesondere im Rahmen investigativer Recherchen im staatlichen Sicherheitsbereich – mit Whistleblowern oder Straftatverdächtigen in Kontakt und es besteht stets die Wahrscheinlichkeit, dass ihm eine Mittäterschaft oder Teilnahme unterstellt wird. Gleiches gilt für seine Arbeit für die „Internationale Liga für Menschenrechte", bei welcher er es nicht selten mit Personen und Gruppen zu tun hat, die möglicherweise von Polizei und Geheimdiensten im In- und Ausland überwacht oder verfolgt werden (z.B. kurdische Gruppen wegen angeblicher Nähe zur PKK, die in der Bundesrepublik und der EU als „terroristisch" eingestuft sind, oder iranische Volksmodjaheddin, islamische Gemeinschaften etc., die ihrerseits nicht selten im Fokus der Sicherheitsbehörden stehen und ausgeforscht werden). Der Beschwerdeführer sieht im Übrigen die Gefahr, dass er als Berufsgeheimnisträger mit Maßnahmen und Methoden der hier angegriffenen Art Mandats- und Beratungsgeheimnis sowie Informantenschutz letzlich nicht mehr durchgängig gewährleisten kann.

Der *Beschwerdeführer zu 2*, [redacted], ist Künstler. Er ist Verfasser der Känguru-Trilogie. Diese handelt von seinem Zusammenleben mit einem kommunistischen Känguru in Wohngemeinschaft. Dieses hat nach eigener Aussage auf

Seiten des Vietcong gekämpft, will das System umstürzen und betreibt einen Boxclub („Nazis boxen“). Auf Grund einiger absurder (realer) Erlebnisse anderer Beschwerdeführer mit der Polizei liegt die Befürchtung nahe, dass Strafverfolgungsbehörden das Känguru nicht als Romanfigur erkennen, sondern als Täter einer der in den §§ 100a Abs. 2, 100b Abs. 2 StPO genannten Anlasstaten einstufen und er Betroffener einer Online-Durchsuchung oder Quellen-Telekommunikationsüberwachung wird.

Der *Beschwerdeführer zu 3*, [redacted], ist als Rechtsanwalt und Strafverteidiger tätig. Er kommuniziert über informationstechnische Systeme täglich einerseits mit Personen, denen schwere und schwerste Straftaten vorgeworfen werden, andererseits mit deren Familienangehörigen (beispielsweise im Zuge einer Inhaftierung, oder um Fragen des familiären Miteinanders zu regeln). Er übermittelt und speichert auf den von ihm (und seinen Berufshelferinnen und –helfern) genutzten informationstechnischen Geräten (be- oder entlastende) Dateien, Fotos etc. Über diese Geräte kommuniziert er auch über Belange, die nicht beruflicher, sondern privater Natur sind. Er befürchtet insbesondere als „andere Person“ im Sinne des § 100a Abs. 3 StPO sowie § 100b Abs. 3 StPO zum Betroffenen einer Quellen-Telekommunikationsüberwachung sowie einer Online-Durchsuchung zu werden.

Der *Beschwerdeführer zu 4*, [redacted], ist seit 1976 mit unterschiedlichsten Kommunikationsmedien politisch arbeitender Künstler. Seit den frühen 80er-Jahren ist es sein Anliegen, Menschen digital zu 'ermündigen'. Zu diesem Zweck beschäftigt er sich intensiv mit den Möglichkeiten moderner digitaler Technologien und deren Vernetzungsmöglichkeiten. Diese Beschäftigung beinhaltet Elemente des Erfindens, des Entdeckens, des Erforschens und des Umsetzens. Im Zusammenhang mit dieser Tätigkeit ist er bereits mehrfach wegen Täterschaft und Teilnahme unterschiedlichster Straftaten beschuldigt worden. Im Nachgang einer Veranstaltung namens "Bitnappingparty", die er im November 1987 zusammen mit dem Jugendamt der Stadt Bielefeld durchführte, fand bei ihm eine Hausdurchsuchung der Abteilung KK23 für Wirtschaftskriminalität der Bielefelder Kriminalpolizei statt. Das Verfahren wurde kurz danach von der Staatsanwaltschaft eingestellt. Im April 1994, als er mit der Beschwerdeführerin zu 6. sog. MailBox-Netzwerke aufbaute, führte der Staatsschutz Bielefeld, KK ST 2 (unter Mitwirkung des LKA Nordrhein-Westfalen) eine

Hausdurchsuchung durch, da über das Netzwerk eine angebliche Bombenbauanleitung abrufbar war. Seit vielen Jahren betreibt er mit der Beschwerdeführerin zu 6. sogenannte Tor-Server („TOR" steht für „The Onion Router"). Das sind Anonymisierungsserver, die innerhalb eines globalen Netzwerkes dafür sorgen, dass Menschen ihr Recht auf anonyme Nutzung des Internet in Anspruch nehmen können, da dieses Netzwerk verschleiert, wer auf welche Inhalte zugreift. So kann, wenn das Tor-Netzwerk genutzt wird, zum Beispiel eine Zeitung nicht feststellen, dass eine bestimmte Person X einen Artikel auf ihrer Website liest. Für die Zeitung würde es immer so aussehen, als sei der Beschwerdeführer selbst – also der Betreiber des Servers – derjenige, der auf den Zeitungsartikel zugreift. Genauso, wie Kriminelle eine öffentliche Straße anonym nutzen können, können auch Kriminelle, die Anonymisierungsstrukturen des Tor-Netzwerkes nutzen. Auch deren Kommunikationsverhalten kann über den Tor-Server des Beschwerdeführers geleitet werden – mithin sieht es so aus, als sei dieser der Nutzer, da die zugehörige IP-Adresse auf seinen Namen eingetragen ist. Aus diesem Grund ist der Beschwerdeführer bereits häufiger Beschuldigter wegen schwerster Straftaten gewesen. Im Jahr 2006 wurde beispielsweise – vermutlich im Zusammenhang mit umfangreichen Ermittlungen wegen Verbreitung von Kinderpornografie[38] – durch die Staatsanwaltschaft Konstanz eine Festplatte seines Tor-Servers beschlagnahmt. Bis heute hat er weder Benachrichtigung, Aktenzeichen oder auch nur eine Information der Staatsanwaltschaft bekommen. Wegen dieser Erfahrungen befürchtet der Beschwerdeführer, dass er nunmehr auch Zielperson von heimlichen Quellen-Telekommunikations- und Online-Durchsuchungsmaßnahmen wird bzw. eventuell sogar bereits ist.

Der *Beschwerdeführer zu 5*, Herr [redacted], ist Rechtsanwalt und Strafverteidiger in der Kanzlei Joester & Partner. Er ist zudem Honorarprofessor an der Universität Bremen, Vorsitzender des 1. Senats des Bremer Anwaltsgerichtshofs und Redakteur der Fachzeitschrift „Strafverteidiger" sowie Autor und Herausgeber zahlreicher Bücher und Aufsätze zu den Themenbereichen Strafverteidigung, Kriminologie, Vollstreckungs- und Vollzugsrecht, Menschenrechte und Psychiatrie. Er

[38] Darauf ließen seinerzeit entsprechende Zeitungsberichte schließen, vgl. z.B. *Bleich*, Anonymisierungsserver bei Razzia beschlagnahmt, heise.de v. 8.9.2006 - abrufbar unter https://www.heise.de/newsticker/meldung/Anonymisierungsserver-bei-Razzia-beschlagnahmt-160475.html (letzter Abruf 3.8.2018).

engagiert sich kriminalpolitisch und ist als Bürgerrechtler, etwa im Zusammenhang mit Demonstrationsbeobachtungen, aktiv. Er hat in der letztgenannten Eigenschaft mitunter und von Berufs wegen ständig mit Personen zu tun, gegen die sich Maßnahmen gem. §§ 100a, 100b StPO richten können. Er befürchtet, dass sich solche Maßnahmen nicht nur mittelbar, sondern auch unmittelbar zugleich gegen ihn selbst richten (§ 100a Abs. 3 StPO). Er befürchtet zudem, dass sich einschlägige Ermittlungsverfahren (etwa gem. § 100b Abs. 1 i.V.m. Abs. 2 Nr. 1 lit. l StPO iVm § 261 StGB bzw. § 100a Abs. 1 S. 2 und 3 i.V.m. Abs. 2 Nr. 1 lit. m StPO i.V.m. § 261 StGB) auch direkt gegen ihn wenden. Seinen Schutz als Berufsgeheimnisträger (§ 53 StPO; § 203 StGB) und der seiner sog. Berufshelfer – mit denen er ebenfalls über informationstechnische Systeme kommuniziert und die auch seine informationstechnischen Systeme nutzen – sieht er (insbesondere in Anbetracht der Heimlichkeit der Maßnahmen) in den §§ 160a, 100d Abs. 5 StPO nur unzureichend ausgestaltet.

Die *Beschwerdeführerin zu 6*, [redacted], ist Mitglied im Vorstand des Digitalcourage e.V. In dieser Tätigkeit recherchiert sie sehr viel, sowohl telefonisch als auch im Internet, unter anderem für den Datenschutz-Negativpreis „BigBrotherAwards“. Hierbei erhält sie vertrauliche Informationen aus Behörden, zivilgesellschaftlichen Organisationen und Unternehmen. Die Informantinnen und Informanten bewegen sich mitunter im Bereich der in §§ 100a Abs. 2 und 100b Abs. 2 StPO genannten Straftaten. Die Beschwerdeführerin, die Ehrenmitglied im Chaos Computer Club ist, betreibt darüber hinaus mit dem Beschwerdeführer zu 4. einen Tor-Server über den Dritte anonym über das Internet kommunizieren und anonym Internetdienste aufrufen können. Diese Möglichkeit wird – wie bereits dargelegt – mitunter zu illegalen Zwecken ausgenutzt. Die „digitale Spur“ (sog. IP-Adresse) führt technikbedingt auch zur Beschwerdeführerin als Zugangsvermittlerin. Es ist daher denkbar, dass sie als Verdächtige beziehungsweise (Mit-)Beschuldigte Ziel der hier angegriffenen Maßnahmen wird. So ist beispielsweise eine Verdächtigung wegen Verbreitung von kinderpornographischen Schriften oder gewerbsmäßiger Hehlerei nicht ausgeschlossen, da diese Straftaten häufig über anonyme Internetdienste begangen werden. Da auch bei der Beschwerdeführerin bereits wegen angeblichen Verbreitens einer vermeintlichen „Bombenbauanleitung“ über elektronische Netze eine Hausdurchsuchung durchgeführt wurde, hat sie die begründete Befürchtung, dass sie Zielperson der hier angegriffenen Maßnahmen wird bzw. gegebenenfalls bereits ist.

VI. Prozessbevollmächtigte

Die Prozessbevollmächtigten erfüllen die in § 22 Abs. 1 BVerfGG niedergelegten Anforderungen. Sie sind Rechtslehrer an einer staatlichen Hochschule und besitzen die Befähigung zum Richteramt.

Der Prozessbevollmächtigte Prof. Dr. Jan Dirk Roggenkamp ist Professor für Öffentliches Recht an der Hochschule für Wirtschaft und Recht Berlin (HWR Berlin).[39] Er hat im Jahr 2005 die Befähigung zum Richteramt im Sinne des § 5 Abs. 1 DRiG erworben und war mehrere Jahre als Rechtsanwalt zugelassen und tätig.

Der Prozessbevollmächtigte Prof. Dr. Frank Josef Braun ist Professor für Staatsrecht und Allgemeines Verwaltungsrecht an der Fachhochschule für Öffentliche Verwaltung Nordrhein-Westfalen (FHöV NRW).[40] Er hat die Befähigung zum Richteramt im Sinne des § 5 Abs. 1 DRiG im Jahr 2001 erworben.

B. Rechtsschutzbegehren

Die Beschwerdeführer wenden sich mit der Verfassungsbeschwerde gegen § 100a Abs. 1 S. 2 und 3, Abs. 3, Abs. 5 und 6 StPO, § 100b StPO sowie § 100d Abs. 1 bis 3 und 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.), die sie für mit dem Grundgesetz unvereinbar und nichtig erachten.

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. 13 Abs. 1 und Art. 19 Abs. 4 GG.

---

[39] https://www.hwr-berlin.de/fachbereich-polizei-und-sicherheitsmanagement/lehrende/kontakt-info/jan-dirk-roggenkamp/ (letzter Besuch 13. Juli 2018).
[40] https://www.fhoev.nrw.de/organisation/personalverzeichnis/eintrag/dr-frank-braun/ (letzter Besuch 13. Juli 2018).

C. Zulässigkeit

1. Grundrechtsträger

Die Beschwerdeführer sind natürliche Personen und damit Träger der hier als verletzt gerügten Grundrechte.

2. Beschwerdebefugnis

Die Beschwerdeführer sind beschwerdebefugt. Durch die Regelungen werden sie mit hinreichender Wahrscheinlichkeit selbst, unmittelbar und gegenwärtig in ihren Grundrechten betroffen.

a. Unmittelbar

Den Beschwerdeführern steht die Verfassungsbeschwerde unmittelbar gegen die angegriffenen gesetzlichen Regelungen zu. Diese sind zwar vollzugsbedürftig, nach der Rechtsprechung des *BVerfG* gilt indes:

> *„Die Verfassungsbeschwerde kann sich jedoch ausnahmsweise unmittelbar gegen ein vollziehungsbedürftiges Gesetz richten, wenn der Beschwerdeführer den Rechtsweg nicht beschreiten kann, weil es ihn nicht gibt (vgl. BVerfGE 67, 157 [170]) oder weil er keine Kenntnis von der Maßnahme erlangt (vgl. BVerfGE 100, 313 [354]). In solchen Fällen steht ihm die Verfassungsbeschwerde unmittelbar gegen das Gesetz ebenso zu wie in jenen Fällen, in denen die grundrechtliche Beschwer ohne vermittelnden Vollzugsakt durch das Gesetz selbst eintritt (vgl. BVerfGE 30, 1 [16 f.]; 67, 157 [169 f.]; 100, 313 [354]).“*[41]

Diese Voraussetzungen sind vorliegend erfüllt. Die angegriffenen Maßnahmen werden heimlich durchgeführt. Der Betroffene erfährt von diesen weder vor noch während der Überwachung. Die Inanspruchnahme fachgerichtlichen Rechtsschutzes ist dementsprechend nicht möglich. Eine nachträgliche Benachrichtigung ist zwar grundsätzlich vorgesehen, steht der Zulässigkeit der Verfassungsbeschwerde aber nicht entgegen:

[41] BVerfGE 109, 279 (306 f. - Rn. 96).

> *„Ihre Erhebung unmittelbar gegen das Gesetz ist nicht nur dann zulässig, wenn nach der gesetzlichen Regelung die Betroffenen zu keinem Zeitpunkt Kenntnis von einem heimlichen Vollzugsakt erhalten, sondern darüber hinaus auch dann, wenn eine nachträgliche Bekanntgabe zwar vorgesehen ist, von ihr aber auf Grund weit reichender Ausnahmetatbestände auch langfristig abgesehen werden kann. Unter diesen Umständen ist ebenfalls nicht gewährleistet, dass der Betroffene effektiven fachgerichtlichen Rechtsschutz erlangen kann (vgl. MVVerfG, LKV 2000, 345 [346]).“*[42]

Derart weitreichende Ausnahmetatbestände von der nachträglichen Unterrichtung liegen hier vor. Nach § 101 Abs. 4 S. 4 StPO kann eine Benachrichtigung vollständig unterbleiben, wenn ihr „*schutzwürdige Belange einer betroffenen Person entgegenstehen*“. Bereits aus diesem Grund kann die Mitteilung an die Betroffenen auf unabsehbare Zeit ausgeschlossen sein. Zudem erfolgt eine Benachrichtigung ausweislich § 101 Abs. 5 StPO erst „*..., sobald dies ohne Gefährdung des Untersuchungszwecks, des Lebens, der körperlichen Unversehrtheit und der persönlichen Freiheit einer Person und von bedeutenden Vermögenswerten, [...] möglich ist.*“ Nach § 101 Abs. 6 S. 2 StPO kann das nach § 101 Abs. 7 StPO zuständige Gericht „*[...] dem endgültigen Absehen von der Benachrichtigung zustimmen, wenn die Voraussetzungen für eine Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden.*“ Auch hiernach besteht die Möglichkeit, dass eine Benachrichtigung erst lange nach Beendigung der Maßnahme oder gar nicht erfolgt. Schließlich erstreckt sich die Benachrichtigungspflicht bei Maßnahmen nach § 100b StPO grundsätzlich nur auf „*die Zielperson sowie die erheblich mitbetroffene Person*“. Es ist unklar, wann eine derartige „erhebliche“ Betroffenheit vorliegt. Es besteht dadurch stets die Gefahr, dass eine Benachrichtigung unterbleibt, weil – für den Betroffenen nicht nachvollziehbar, da dies ihm ja unbekannt bleibt – eine „erhebliche“ Betroffenheit verneint wird.

[42] BVerfGE 109, 279 (307 - Rn. 97).

b. Selbst und gegenwärtig

Die Beschwerdeführer werden durch die angegriffenen Befugnisse zur Durchführung einer Quellen-Telekommunikationsüberwachung, einer „kleinen Online-Durchsuchung" sowie einer Online-Durchsuchung in eigenen Grundrechten und gegenwärtig verletzt.

Die Beschwerdeführer werden zwar nicht unmittelbar durch die Regelungen, die zum 24. August 2017 in Kraft getreten sind, adressiert. Da diese jedoch bereits jetzt einen Eingriff gegenüber jedermann erlauben, ist mit einiger Wahrscheinlichkeit anzunehmen, dass die Beschwerdeführer von den durch die angegriffenen Regelungen gestatteten (heimlichen) Maßnahmen betroffen werden.

Nach der Rechtsprechung des *BVerfG* gilt in diesen Fällen:

> *„Die Möglichkeit der eigenen und gegenwärtigen Betroffenheit ist grundsätzlich erfüllt, wenn der Bf. darlegt, dass er mit einiger Wahrscheinlichkeit durch die auf den angegriffenen Rechtsnormen beruhenden Maßnahmen in seinen Grundrechten berührt wird (vgl. BVerfGE 67, 157 [169f.] = NJW 1985, 121; BVerfGE 100, 313 [354] = NJW 2000, 55). Der geforderte Grad der Wahrscheinlichkeit wird davon beeinflusst, welche Möglichkeit der Bf. hat, seine Betroffenheit darzulegen (vgl. BVerfGE 100, 313 [355f.] = NJW 2000, 55). So ist bedeutsam, ob die Maßnahme auf einen tatbestandlich eng umgrenzten Personenkreis zielt (dazu vgl. BVerfG [1. Kammer des Ersten Senats], NVwZ 2001, 1261 = NJW 2002, 1037 L = DVBl 2001, 1057) oder ob sie eine große Streubreite hat und Dritte auch zufällig erfassen kann. Darlegungen, durch die sich der Bf. selbst einer Straftat bezichtigen müsste, dürfen zum Beleg der eigenen gegenwärtigen Betroffenheit nicht verlangt werden."*[43]

Die hier gegenständlichen Maßnahmen sind im Rahmen der Ermittlungstätigkeit bei Vorliegen des Verdachts einer großen Zahl unterschiedlichster Straftaten zulässig (vgl. § 100a Abs. 2 StPO sowie § 100b Abs. 2 StPO).

Sie betreffen nicht nur die informationstechnischen Systeme der jeweils Beschuldigten, sondern dürfen sich auch auf informationstechnische Systeme „*anderer Personen*", also

[43] BVerfGE 109, 279 (307f. - Rn. 99).

unverdächtiger Dritter erstrecken, vgl. § 100a Abs. 3 StPO bzw. § 100b Abs. 3 StPO. Insbesondere darf nach § 100b Abs. 3 S. 3 StPO eine Online-Durchsuchung auch durchgeführt werden, wenn „andere Personen unvermeidbar betroffen werden".

Alle Beschwerdeführer nutzen umfänglich und insbesondere zu privaten Zwecken eine Vielzahl informationstechnischer Systeme (z.B. Smartphones, PC, Laptop, sowie mit den jeweiligen Geräten verbundene Kameras und Mikrofone). Sie teilen diese Geräte auch mit Dritten bzw. nutzen informationstechnische Systeme Dritter. Sie gebrauchen diese Systeme sowohl zur (verschlüsselten) Kommunikation, z.B. über sog. Messengerdienste wie Signal oder Threema als auch für private und berufliche Zwecke zur Speicherung und zum Austausch von Daten aller Art. Darüber hinaus nutzen alle Beschwerdeführer das Internet und unterschiedliche Internetdienste, insbesondere sog. Cloud Computing Anwendungen (z.B. zur Sicherung des lokalen Datenspeichers – sog. Backup oder zur Synchronisation der genutzten Geräte). Es besteht stets die Möglichkeit, dass die Beschwerdeführer zufällig von einer der hier angegriffenen Maßnahmen erfasst werden. Zudem besteht die Möglichkeit, dass die informationstechnischen Systeme der Betroffenen durch die bewußte Offenhaltung von unbekannten Sicherheitslücken beeinträchtigt werden.

Bei der durch § 100a Abs. 1 S. 2 und 3 StPO gestatteten Quellen-Telekommunikationsüberwachung handelt es sich zudem um eine Telekommunikationsüberwachungsmaßnahme:

> „*Die Möglichkeit, Objekt einer Maßnahme der Telekommunikationsüberwachung aufgrund der angegriffenen Regelung zu werden, besteht praktisch für jedermann. Sie kann nicht nur den möglichen Straftäter selbst oder dessen Kontakt- und Begleitpersonen erfassen, sondern auch Personen, die mit den Adressaten der Maßnahme über Telekommunikationseinrichtungen in Verbindung stehen.*"[44]

Auch wenn weitere Darlegungen für die Frage der eigenen und gegenwärtigen Betroffenheit mit Blick auf mögliche Nachteile für die Beschwerdeführer nicht

[44] BVerfGE 113, 348 (363f. - Rn. 77).

erforderlich sind, sei auf die Erläuterungen der Beschwerdeführer zu ihrer persönlichen Situation hingewiesen (oben A.V). Daraus wird ersichtlich, dass diese unmittelbar eine Quellen-Telekommunikationsüberwachung oder Online-Durchsuchung wegen Verdachts der Begehung einer der in den o.g. Anlasskatalogen genannten Straftat zu befürchten haben. Es besteht jedenfalls enger Kontakt zu Personen, bei denen die hinreichende Wahrscheinlichkeit besteht, dass gegen diese entsprechende Ermittlungsverfahren durchgeführt werden. Da nicht auszuschließen ist, dass diese Personen zumindest auch die informationstechnischen Geräte der Beschwerdeführer nutzen, besteht eine hohe Wahrscheinlichkeit, dass diese – auch ohne selbst einer Katalogtat verdächtig zu sein – Objekt einer der hier angegriffenen Maßnahmen zu werden.

3. Subsidiarität

Auch der Grundsatz der Subsidiarität der Verfassungsbeschwerde ist gewahrt. Es kann den Beschwerdeführern nicht zugemutet werden, einzelne Vollzugsakte und die Benachrichtigung hierüber abzuwarten, die – wie bereits dargelegt -gegebenenfalls niemals erfolgt.

§ 101 Abs. 7 S. 2 StPO gewährleistet für den Fall einer nachträglichen Benachrichtigung, keinen hinreichenden Rechtsschutz, da er nur retrograden Charakter hat. Mit Blick auf die hier gerügten schwerwiegenden Grundrechtsverletzungen können die Beschwerdeführer auf diese (theoretische) Möglichkeit nicht verwiesen werden.

4. Beschwerdefrist

Die Beschwerdefrist von einem Jahr (§ 93 Abs. 3 BverfGG) ist gewahrt. Die hier gegenständlichen Regelungen sind zum 24. August 2017 in Kraft getreten.

D. Begründetheit

Die Verfassungsbeschwerde ist begründet.

Die Beschwerdeführer werden durch § 100a Abs. 1 S. 2, 3, Abs. 3, Abs. 5 und 6 StPO, § 100b StPO sowie § 100d Abs. 1 bis 3 und Abs. 5 StPO in ihren Grundrechten aus Art. 1

Abs. 1, Art. 2 Abs. 1 i.V.m. 1 Abs. 1, Art. 10 Abs. 1, Art. 13 Abs. 1 und Art. 19 Abs. 4 GG verletzt.

I. Unvereinbarkeit mit der Menschenwürdegarantie (Art. 1 Abs. 1 GG)

Sowohl die Online-Durchsuchung als auch die Quellen-Telekommunikationsüberwachung stellen eine nicht zu rechtfertigende Verletzung der durch Art. 1 Abs. 1 GG absolut geschützten Menschenwürde dar.

Diese heimlichen Überwachungsmaßnahmen implizieren einen Zugriff auf Informationen, die der unantastbaren Intimsphäre des Nutzers zuzurechnen sind. Sie stellen eine selbständige Verletzung [45] der in Art. 1 Abs. 1 GG geschützten Menschenwürde dar.

Im Jahr 2008 hat das *BVerfG* anhand der damaligen Nutzungsgepflogenheiten festgestellt, dass informationstechnische Systeme (seinerzeit ganz überwiegend Personal Computer) „*typischerweise bewusst zum Speichern auch persönlicher Daten von gesteigerter Sensibilität, etwa in Form privater Text-, Bild- oder Tondateien, genutzt*“ werden.[46]

Diese Nutzungsgepflogenheiten haben sich drastisch geändert.

Informationstechnische Systeme sind nicht mehr in erster Linie Arbeitsgeräte und werden „auch“, also nur nachrangig, zum Speichern persönlicher Daten genutzt. Sie sind inzwischen unabkömmliche persönliche Begleiter, die mitunter „auch“ für die berufliche Tätigkeit genutzt werden. Darauf vorgehaltene persönliche Daten sind regelmäßig nicht nur von „gesteigerter“, sondern von höchster Sensibilität werden nicht nur bewusst, sondern auch unbewusst automatisiert erfasst und gespeichert.

[45] Vgl. *Di Fabio*, in: Maunz/Dürig, Art. 2 Abs. 1, Rn. 158.
[46] BVerfGE 120, 274 (322f.- Rn. 231); ähnlich, ohne erkennbar neue Bewertung der zwischenzeitlich geänderten Nutzungsgepflogenheiten BVerfGE 141, 220 (306f. - Rn. 218).

Die oben unter A.IV dargestellten aktuellen Nutzungsgepflogenheiten informationstechnischer Systeme, lassen es als ausgeschlossen erscheinen, ein solches zu infiltrieren, ohne hierdurch gleichzeitig nicht nur in das gewissermaßen „ausgelagerte Gehirn", sondern in die Tiefen der Persönlichkeit eines Nutzers einzudringen. Das gilt insbesondere für die heute im Fokus der Ermittlungsbehörden stehenden Smartphones und anderen mobilen Endgeräte.

Es findet ein Zugriff auf Informationen statt, an denen die Zielperson der Maßnahme (und ebenfalls betroffene andere Personen, die das informationstechnische System mitnutzen) nicht einmal engste Vertraute teilhaben lassen würde. Die Erstellung eines allumfassenden Persönlichkeitsbildes – einschließlich der dem Betroffenen selbst nicht bewussten persönlichkeitsprägenden Merkmale – wird möglich.

Die ausnahmsweise Gestattung der (offenen!) Verwertung eines Tagebuchs zur Aufklärung einer schweren Straftat wird bislang als „*äußerste Grenze staatlicher Ausforschung der Intimsphäre*"[47] angesehen.

Die Quellen-Telekommunikationsüberwachung und die Online-Durchsuchung überschreiten diese Grenze bei weitem. Sie gestatten nicht nur die offene Verwertung höchstvertraulicher Informationen, sie erlauben gewissermaßen die dauerhafte heimliche Überwachung des Verfassens der Tagebucheinträge und dessen, was der Betroffene nicht einmal seinem Tagebuch anvertrauen würde.[48] Die hier angegriffenen Regelungen eröffnen, wie *Prantl* zutreffend formuliert, „*die Möglichkeit, Gedanken auszulesen*"[49].

Jede durch die hier angegriffenen Regelungen gestattete Maßnahme macht den Kernbereich privater Lebensgestaltung denknotwendigerweise zum Ziel staatlicher Ermittlungen und ist damit absolut auszuschließen.[50]

---

[47] *Herdegen*, in: Maunz/Dürig, Art. 1 Rn. 90.
[48] Im Ergebnis ebenso *Roggan*, StV 2017, 821 (826 f.) der die Maßnahme in ihrer Eingriffsintensität mit wiederholten heimlichen Hausdurchsuchungen vergleicht.
[49] *Prantl*, Der Staatstrojaner ist ein Einbruch ins Grundrecht, SZ v. 22.6.2017 - https://www.sueddeutsche.de/digital/ueberwachung-der-staatstrojaner-ist-ein-einbruch-ins-grundgesetz-1.3555917 - Ausdruck als **ANLAGE 21** anbei.
[50] BVerfGE 121, 220 (278 - Rn. 125).

Es handelt sich bei beiden Maßnahmen nicht lediglich um „verletzungsgeneigte Maßnahmen“, sondern um Maßnahmen denen eine Verletzung des Kernbereichs immanent ist. Es ist technisch nicht möglich, eventuelle nicht kernbereichsrelevante Informationen im Rahmen eines Zugriffs auszufiltern. Im Gegensatz zur Wohnraumüberwachung – bei welcher bestimmte Räumlichkeiten von der Überwachung ausgenommen werden können – besteht, bei einer Online-Durchsuchung nur die Alternative von „ganz oder gar nicht“[51].

Können kernbereichsrelevante Daten vor oder bei der Datenerhebung nicht ausgesondert werden, ist

> *„ein Zugriff auf das informationstechnische System jedoch auch dann zulässig,* ***wenn*** *hierbei* ***eine Wahrscheinlichkeit*** *besteht, dass* ***am Rande auch*** *höchstpersönliche Daten miterfasst werden.*“[52]

Hieraus folgt im Umkehrschluss, dass ein Zugriff auf informationstechnische Systeme dann *nicht* zulässig ist, wenn die Wahrscheinlichkeit besteht, dass *überwiegend* höchstpersönliche Daten erfasst werden. Wenn aber eine Maßnahme regelmäßig und nicht nur in Ausnahmefällen und ganz „*am Rande auch*“ den Kernbereich der privaten Lebensgestaltung erfasst, kann sie nicht gerechtfertigt werden und verstößt gegen die Menschenwürde.

[51] BVerfGE 121, 220 (306 - Rn. 218).
[52] BVerfGE 121, 220 (307 - Rn. 220) - Hervorhebung nur hier.

II. Unvereinbarkeit mit dem Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG)

Sowohl Online-Durchsuchung als auch Quellen-Telekommunikationsüberwachung verletzen das aus dem allgemeinen Persönlichkeitsrecht abgeleitete Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.

1. Online-Durchsuchung (§ 100b StPO)

Die heimliche Installation einer Trojanersoftware und die hierdurch ermöglichte heimliche Überwachung eines informationstechnischen Systems nach § 100b Abs. 1 StPO stellt, wenn man hierin nicht bereits eine Verletzung der Menschenwürdegarantie erkennen wollte, jedenfalls einen Eingriff in das Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme dar.[53]

Die Regelung verstößt gegen den verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit. Die mit einer Online-Durchsuchung einhergehenden Grundrechtsbeeinträchtigungen sind nur ganz ausnahmsweise zu rechtfertigen und unterliegen strengen verfassungsrechtlichen Rechtfertigungsanforderungen[54]. Diese hat der Gesetzgeber nicht in ausreichendem Maße beachtet.

a. Ungeeignetheit

Die durch § 100b StPO gestattete repressive Online-Durchsuchung ist bereits unverhältnismäßig, da sie zur Zielerreichung – der Aufklärung mehr oder weniger gewichtiger Straftaten – nicht geeignet ist.

Zur Durchführung einer Online-Durchsuchung muss das Zielsystem manipuliert und mit einer Trojanersoftware infiltriert werden. Die Ermittlungsbehörden haben im Anschluss daran – ggf. monatelang (vgl. § 100d Abs. 2 StPO) – Zugriff auf das gesamte

[53] BVerfGE 120, 274 (302 f.).
[54] BVerfGE 120, 274 (322 ff.).

informationstechnische System, das – bewusst oder unbewusst – manipuliert werden könnte.

Zur Gewinnung „gerichtsfester Beweise" ist eine Online-Durchsuchung als ungeeignet anzusehen. Das System bzw. dort aufgefundene Dateien haben keinen Beweiswert.[55] Durch die heimliche Datenerhebung wird gegen Grundlagen der Computerforensik verstoßen. Denn bei der Untersuchung und Analyse eines informationstechnischen Systems darf das maßgebliche Untersuchungsobjekt (die Originalfestplatte) nicht verändert werden, um dessen Beweiswert nicht zu mindern bzw. aufzuheben. Untersuchungen dürfen nicht am Untersuchungsobjekt selbst vorgenommen werden.[56] Im Gegensatz zur Untersuchung am Tatort, kann bei digitalen Informationen nicht mehr nachvollzogen werden, ob sie von „Tatortberechtigten" stammt oder vom Beschuldigten. Daher ist vor der Untersuchung eines beschlagnahmten informationstechnischen Systems eine „bit-identische" 1:1 Kopie des Originaldatenträgers zu erstellen, die alleiniger Gegenstand der IT-Forensik ist. Der Originaldatenträger wird indes versiegelt verwahrt.

Das alles ist bei einer Online-Durchsuchung nicht möglich. Daher ist der Beweiswert der durch eine Online-Durchsuchung gewonnenen Erkenntnisse gleich Null.

Der beschriebenen Gefährdungslage können die in § 100b Abs. 4 i.V.m. § 100a Abs. 5 StPO normierten *Dokumentationspflichten* nicht entgegenwirken. Zum einen ist es ohnehin kaum möglich, Softwareoperationen auf einem nicht exklusiv kontrollierten System nachzuweisen. Zum anderen trägt die Dokumentationspflicht nicht ansatzweise dazu bei, eine umfassende nachträgliche Überprüfung der Einhaltung der gesetzlichen Vorschriften zu gewährleisten. Denn hierzu hätte die Vorschrift explizit auch zur Dokumentation und Offenlegung der technischen Details des Zugriffs – vor allem des Quellcodes der eingesetzten Software – verpflichten müssen. Hinzuweisen ist auch auf

[55] Vgl. auch *Hansen/Pfitzmann*, in: Roggan (Hrsg.), Online-Durchsuchungen, 2008, S. 131 (133).
[56] *Gercke/Brunst*, Praxishandbuch Internetstrafrecht, Rz. 1000.

die diesbezügliche „Mauer des Schweigens“ der verantwortlichen Stellen, die jegliche Informationen zur eingesetzten Software verweigern[57].

b. Fehlende Erforderlichkeit

Eine Datenerhebung im Wege einer heimlichen Online-Durchsuchung ist auch nicht erforderlich. Mit der offenen Beschlagnahme der informationstechnischen Zielsysteme und deren anschließender Auswertung stehen mildere und zudem wirksamere Mittel zur Verfügung.[58]

Das *BVerfG* hat in Bezug auf präventiv intendierte Online-Durchsuchungen explizit festgestellt, dass ein offener Zugriff auf die Datenbestände einer Zielperson vor einer heimlichen Infiltration grundsätzlich Vorrang hat[59]. Eine heimliche Maßnahme ist zur Prävention nur ausnahmsweise zulässig, wenn die offene Informationserhebung die Zielerreichung (Abwehr von Gefahren für überragend wichtige Rechtsgüter) ernsthaft gefährdet wäre, weil z.B. Hintermänner gewarnt würden.

Die präventive Informationserhebung ist zukunftsbezogen. Das gilt für die repressive Informationserhebung – und damit auch für die repressive Online-Durchsuchung – nicht. Durchsuchungsmaßnahmen nach den §§ 102 ff. StPO und die anschließende Beschlagnahme und Auswertung des informationstechnischen Zielsystems gem. §§ 94 ff. StPO zielen auf denselben Datenbestand ab, wie er durch eine heimliche Online-Durchsuchung gewonnen werden soll, erfolgen aber offen und wirken deshalb, auch mit Blick auf die Gewährleistung effektiven Rechtsschutzes, deutlich weniger grundrechtsbelastend. Zudem werden durch einen offenen Datenzugriff die mit einer heimlichen Infiltration des informationstechnischen Systems verbundenen Risiken für die IT-Sicherheit minimiert.

Zu berücksichtigen ist in diesem Zusammenhang, dass sich sichernde offene polizeiliche Zugriffsstrategien in der Praxis bewährt haben, die einem theoretisch möglichen Einsatz

---

[57] Vgl. *Meister*, Geheime Sitzung im Bundestag: Regierung verweigert jede Auskunft über Staatstrojaner-Firmen, netzpolitik.org v. 12.7.2018, https://netzpolitik.org/2018/geheime-sitzung-im-bundestag-regierung-verweigert-jede-auskunft-ueber-staatstrojaner-firmen/ - Ausdruck als **ANLAGE 9** anbei.
[58] Vgl. *Roggan*, StV 2017, 821 (827).
[59] BVerfGE 141, 220 (305 f. - Rn. 215).

zugriffsvereitelnder Verschlüsselungstechniken wirksam entgegenwirken. So kann durch heimliche Vorfeldermittlungen regelmäßig ein Zugriff bei laufendem Rechner gesichert und unter Beiziehung von IT-Forensikern erfolgreich gestaltet werden. Auch die zwangsweise Entsperrung von Smartphones mittels Fingerprint ist bereits Gegenstand der polizeilichen Praxis[60].

Sollte man unter Berücksichtigung einer etwaigen Einschätzungsprärogative des Gesetzgebers für derartige Fallkonstellationen dennoch die Notwendigkeit eines heimlichen Datenzugriffs im Wege einer Online-Durchsuchung erkennen wollen, hat der Gesetzgeber die Eingriffsbefugnis im Hinblick auf dafür allenfalls marginale Bedarfe zu unbestimmt und deutlich zu weit gefasst.

Zwei ausdrückliche Einschränkungen wären in der gesetzlichen Regelung erforderlich gewesen: Nämlich zum einen, dass tatsächliche Anhaltspunkte dafür bestehen müssen, dass das informationstechnische Zielsystem verschlüsselt bzw. dass ein offener Zugriff aussichtslos oder unverhältnismäßig erschwert wäre[61]. Zum anderen – und dies ist das wesentliche rechtsfolgenbeschränkende Kriterium – dass nach Infiltration des Systems *lediglich Maßnahmen zur Extraktion und Exfiltrierung des für die Kryptierung des Datenträgers verwendeten Schlüssels* getroffen werden dürfen[62].

Gelingt dies, kann das Zielsystem nach offener Beschlagnahme problemlos ausgelesen werden. Nur bei einer solchen gesetzlich determinierten „grundrechtsschonenderen" Vorgehensweise, können unnötige Zugriffe vermieden und im (zweifelhaften) Bedarfsfall die heimliche Datenerhebung auf das Notwendigste beschränkt, insbesondere die Erfassung kernbereichsrelevanter Daten minimiert und die Dauer der Maßnahme drastisch verkürzt werden.

Das Verhältnis zu offenen Maßnahmen als Alternative zu einer Online-Durchsuchung ist gesetzgeberisch völlig unzureichend und im Ergebnis verfassungswidrig behandelt worden. Die Gesetzesbegründung schweigt sich zu Fragen der Erforderlichkeit bis auf

---

[60] Hierzu *Bäumerich*, NJW 2017, 2718; *Momsen*, DRiZ 2018, 14.
[61] Gleicher Gedanke bei *Freiling/Safferling/Rückert*, JR 2018, 9 (22) und *Winter*, ZStW 129 (2017), 205 (225).
[62] So treffend *Freiling/Safferling/Rückert*, JR 2018, 9 (19).

Allgemeinplätze aus. Auch mit Blick auf das „verkürzte" Gesetzgebungsverfahren ist davon auszugehen, dass der Gesetzgeber von der Möglichkeit einer substantiierten Einschätzung der Erforderlichkeit (die vom angerufenen Gericht überprüft werden könnte[63]) keinen Gebrauch gemacht hat, sondern pauschal und unreflektiert die Erforderlichkeit der Maßnahme angenommen hat.

Es besteht bei derzeitiger Gesetzeslage die dringende Gefahr, dass gleich wirksamen, grundrechtsschonenderen offenen Ermittlungsmaßnahmen gegenüber einer heimlichen Online-Durchsuchung aufgrund kriminaltaktischer Erwägungen Nachrang eingeräumt wird.

c. Unangemessenheit

Die Gestattung der Online-Durchsuchung wie sie § 100b StPO vorsieht ist aus den folgenden Gründen auch unangemessen:

- Der *Anlasstatenkatalog* in § 100b Abs. 2 StPO entspricht nicht den vom *BVerfG* niedergelegten Anforderungen**(aa)**.
- Das Erfordernis eines bloßen *„auf bestimmten Tatsachen" beruhenden Verdachts* einer Katalogtat in § 100b Abs. 1 Nr. 1 StPO ist eine unzureichende, da zu niedrige Eingriffsschwelle**(bb)**.
- § 100b StPO fordert keine auf bestimmte Tatsachen begründete positive *Erfolgsprognose* dahingehend, dass die hinreichende Wahrscheinlichkeit besteht, durch die Maßnahme verfahrensrelevante Informationen zu gewinnen. Eine solche wäre insbesondere mit Blick auf die Überwachung informationstechnischer Systeme „anderer Personen" zwingend erforderlich gewesen**(cc)**.
- Durch die vom Gesetzgeber gewählte, die Verhältnismäßigkeitsprüfung steuernde *Subsidiaritätsklausel* in § 100b Abs. 1 Nr. 3 StPO wird die Eingriffsintensität der Maßnahme verkannt. Erforderlich wäre eine „Ultima-Ratio-Konzeption" gewesen**(dd)**.
- Die notwendige Berücksichtigung *additiver Grundrechtseingriffe* bei der Anordnung der Maßnahme wurde gesetzgeberisch nicht abgebildet. Zudem ist in § 100e StPO keine Information des anordnenden Gerichts über gegenwärtige und künftige

[63] Vgl. BVerfGE 109, 279 (340).

repressive und präventive Überwachungsmaßnahmen gegen den Beschuldigten vorgesehen. Dem Gericht ist es somit nicht möglich, eine menschenunwürdige Totalüberwachung zu verhindern.**(ee)**

- Der zeitliche Rahmen der Anordnungsdauer nach § 100e Abs. 2 StPO ist unverhältnismäßig lang. **(ff)**
- Durch die *Einbeziehung von Vorfeldstraftaten* in § 100b Abs. 2 StPO werden die Grenzen zwischen Gefahrenabwehr und Strafverfolgung unzulässig verwischt. Zudem ist mit Blick auf entsprechende präventive Befugnisse ein freies Changieren zwischen repressiven und präventiven Maßnahmen zu befürchten.**(gg)**
- Der verfassungsrechtlich erforderliche *Schutz des Kernbereichs privater Lebensgestaltung* wurde in § 100d StPO sowohl für die Erhebungsphase als auch für die Verwertungsphase unzureichend ausgestaltet**(hh)**; gleiches gilt für den *Schutz von Berufsgeheimnisträgern***(ii)**.

Im Einzelnen:

aa) Unangemessenheit des Anlasstatenkatalogs (§ 100b Abs. 2 StPO)

§ 100b StPO ist bereits unangemessen, da der in § 100b Abs. 2 StPO enthaltene Katalog der Anlasstaten nicht den auf den repressiven Bereich übertragenen Anforderungen des *BVerfG* entspricht.

Bei der verfassungsrechtlichen Bewertung der präventiven Online-Durchsuchung hat das *BVerfG* festgestellt, dass eine Rechtfertigung nur bei Vorliegen einer im Einzelfall drohenden Gefahr für ein „*überragend wichtiges Rechtsgut*“ in Betracht gezogen werden kann.[64]

> „*Überragend wichtig sind zunächst Leib, Leben und Freiheit der Person. Ferner sind überragend wichtig solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.*“[65]

[64] BVerfGE 141, 220 (304 f.); 120, 274 (326 ff.).
[65] BVerfGE 120, 274 (326 ff. - Rn. 247).

Für alle anderen Rechtsgüter hat das Gericht festgehalten:

> *„Zum Schutz sonstiger Rechtsgüter Einzelner oder der Allgemeinheit in Situationen, in denen eine existentielle Bedrohungslage nicht besteht, ist eine staatliche Maßnahme grundsätzlich nicht angemessen, durch die – wie hier – die Persönlichkeit des Betroffenen einer weitgehenden Ausspähung durch die Ermittlungsbehörde preisgegeben wird. Zum Schutz solcher Rechtsgüter hat sich der Staat auf andere Ermittlungsbefugnisse zu beschränken …*“[66]

Die mit einer *repressiven* Online-Durchsuchung verfolgten Anlasstaten müssten von einem Gewicht sein, das mit den Anforderungen an die zu schützenden „überragend wichtigen Rechtsgüter“ bei der präventiven Online-Durchsuchung korreliert. Nur so ist ein Gleichlauf mit den Anforderungen an eine *präventive* Online-Durchsuchung gegeben. Voraussetzung für eine solche Vergleichbarkeit ist, unter Heranziehung der „Nagelprobe“ von *Buermeyer*, dass *„eine Online-Durchsuchung zur Verhinderung der entsprechenden Taten hätte vorgesehen werden dürfen*“[67].

Das ist bei § 100b Abs. 2 StPO nicht der Fall.

In diesem Katalog ist festgelegt, welche Taten als besonders schwere Anlasstaten im Sinne des Abs. 1 zu verstehen sind. Dieser Katalog knüpft erkennbar nicht an „überragend wichtige“ Rechtsgüter an. Es wurde vielmehr unreflektiert der Straftatenkatalog des § 100c Abs. 2 StPO a.F. übernommen.

Dieser enthält eine Vielzahl von Straftatbeständen, zu deren Verhinderung eine präventive Online-Durchsuchung unzulässig wäre.

Exemplarisch sei hier die in § 100b Abs. 2 Nr. 1c StPO genannte „Geld- und Wertzeichenfälschung“ genannt. Die §§ 146 ff. StGB dienen dem Schutz des Rechtsguts

---

[66] BVerfGE 120, 274 (326 ff. - Rn. 248).
[67] Vgl. die Stellungnahme im „Gesetzgebungsverfahren“ von *Buermeyer*, S. 12, www.bundestag.de/ausschuesse18/a06/anhoerungen/stellungnahmen/508846; ebenso *Roggan*, StV 2017, 821 (827).

„Allgemeininteresse an der Sicherheit und Zuverlässigkeit des Geldverkehrs“[68], einem zwar wichtigen, aber nicht „überragend“ wichtigem Rechtsgut.

Auch der in § 100b Abs. 2 Nr. 1h StPO genannte Bandendiebstahl (Schutzgut: Eigentum und Gewahrsam), die in § 100b Abs. 2 Nr. 1k StPO genannten Hehlereidelikte (Schutzgut: Eigentum), die in § 100b Abs. 2 Nr. 1l StPO genannte Geldwäsche (Schutzgut: „die inländische Rechtspflege in ihrer Aufgabe, die Wirkung von Straftaten zu beseitigen“[69]) oder die in § 100b Abs. 2 Nr. 1k genannten Straftatbestände der Bestechlichkeit bzw. Bestechung (Schutzgut: „Vertrauen in die Unkäuflichkeit von Trägern staatlicher Funktionen und damit zugleich in die Sachlichkeit staatlicher Entscheidungen“[70]) würden die vorgenannte Nagelprobe nicht bestehen. Gleiches gilt für die Verleitung zur missbräuchlichen Asylantragstellung (§ 100b Abs. 2 Nr. 2 StPO), dem Einschleusen von Ausländern (§ 100b Abs. 2 Nr. 3a StPO) sowie den Straftaten aus dem Betäubungsmittelgesetz (§ 100b Abs. 2 Nr. 4 StPO).

Ausweislich § 100b Abs. 1 StPO muss die Tat zwar zusätzlich „*auch im Einzelfall besonders schwer wiegen*“. Was hierunter aber zu verstehen sein soll, lassen sowohl Gesetz als auch Gesetzgebungsmaterialien offen[71]. Da hierdurch der Rechtsgüterschutz nicht verändert wird, kann diese Klausuel die Unangemessenheit des Anlasstatenkatalogs nicht beseitigen.

Im Straftatenkatalog des § 100b Abs. 2 StPO zeigt sich das unreflektierte und überhastete Vorgehen des Gesetzgebers, welches mit Blick auf die Eingriffsintensität der gestatteten Maßnahme als unangemessen zu bewerten ist.

bb) Unangemessenheit der Straftatenprognose

§ 100b Abs. 1 Nr. 1 StPO setzt voraus, dass „*bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete besonders*

[68] *Lackner/Kühl*, StGB, § 146 Rn. 1. Über § 151 StGB werden bestimmte Wertpapiere dem Geld gleichgestellt.
[69] *Lackner/Kühl*, StGB, § 261 Rn. 1 unter Verweis auf BT-Drs. 12/989, S. 27.
[70] *Lackner/Kühl*, StGB, § 331 Rn. 1 m.w.N.
[71] BT-Drs. 18/12785, S. 60.

schwere Straftat begangen oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat". Hierdurch werden die für eine Online-Durchsuchung erforderlichen eingriffseröffnenden Prognoseleistungen in nicht ausreichendem Maße abgebildet. Die Regelung ist auch insoweit unangemessen.

(1) „Auf bestimmten Tatsachen beruhender Verdacht" als Eingriffsschwelle

Die Anforderungen an das Vorliegen eines *Anfangsverdachts*, dem besondere Schutzfunktion zukommt[72], sind äußerst geringer Natur. Allgemein anerkannt ist inzwischen, dass ein durch konkrete Tatsachen belegter, in kriminalistischer Hinsicht begründeter Anhalt dafür gegeben sein muss, dass eine verfolgbare Straftat vorliegt[73]. Ein Anfangsverdacht muss sich auf mehr als bloße Hypothesen, vage Anhaltspunkte oder Vermutungen stützen lassen[74].

Bei der Annahme eines solchen Verdachts handelt es sich um ein *Wahrscheinlichkeitsurteil*. Welche Faktoren in die Wahrscheinlichkeitsprüfung eingestellt werden dürfen und müssen, ab welchem Grad von Wahrscheinlichkeit ein Verdacht besteht und wie diese Wahrscheinlichkeit festgestellt werden kann, ist unklar [75]. Letztlich beruht die Verdachtsbegründung auf einen „*subjektiven Induktionsschluss*"[76]. Die prägenden Akzentuierungen finden im Wesentlichen ihre Grundlage in nicht näher verifizierbaren Wertungen des Abwägenden[77].

Durch das Erfordernis eines durch „bestimmte Tatsachen" begründeten Verdachts in §100b Abs. 1 Nr. 1 StPO soll offenbar deutlich gemacht werden, dass an den erforderlichen Grad des Verdachts erhöhte Anforderungen gestellt werden. Das ist indes nicht der Fall. Ein Unterschied zwischen einem „Anfangsverdacht" und einem durch „bestimmte Tatsachen" begründeten Verdacht besteht nicht (mehr).

---

[72] *Fincke*, ZStW 95 (1983), 918 (924).
[73] *Pfeiffer*, StPO, 5. Aufl. 2005, § 152 Rn. 1a m.w.N.; *Fincke*, ZStW 95 (1983), 918 ff.
[74] BVerfG, Urt. v. 13.03.2014 – 2 BvR 974/12 - Rn. 17 m.w.N.
[75] *Lohner*, Der Tatverdacht im Ermittlungsverfahren, 1994, S. 39.
[76] *Fincke*, ZStW (95) 1983, 918 (923).
[77] So können nach der Rechtsprechung des BGH auch verschiedene Betrachter zu unterschiedlichen Ergebnissen gelangen, ohne jeweils pflichtwidrig zu handeln, BGH StV 1988, 441 (443). Auch sind bislang alle Versuche in der Literatur, die erforderliche Wahrscheinlichkeitsprognose zu „objektivieren" – sei es mittels statistisch-mathematischer Methoden , einer kasuistischen Betrachtungsweise oder am prima-facie-Beweis angelehnten Erfahrungssätzen – gescheitert; dazu *Lohner*, Der Tatverdacht im Ermittlungsverfahren, 1994, S. 38 f.

Im Jahr 2004 hat das *BVerfG* in der Entscheidung zum „Großen Lauschangriff“ den gegenständlichen „durch bestimmte Tatsachen begründeten Verdacht“ wie folgt umschrieben:

> *„Der durch bestimmte Tatsachen begründete Verdacht unterliegt zwar höheren Anforderungen als der bloße Anfangsverdacht, erreicht jedoch nicht bereits den Grad eines "hinreichenden" oder gar "dringenden" Tatverdachts, den andere Normen der Strafprozessordnung vorsehen. § 100 c Abs. 1 Nr. 3 StPO erfordert eine konkretisierte Verdachtslage. Hierfür reicht das bloße Vorliegen von Anhaltspunkten nicht aus. Es müssen vielmehr konkrete und in gewissem Umfang verdichtete Umstände als Tatsachenbasis für den Verdacht vorhanden sein (vgl. BVerfGE 100, 313 [395]). Nur bereits ermittelte und in Antrag und Anordnung genannte Tatsachen kommen für die jeweilige Bewertung in Betracht.“*[78]

Diese graduellen Unterschiede zwischen einem Anfangsverdacht und einem „auf bestimmten Tatsachen“ beruhenden Verdacht bestehen nach der aktuellen Rechtsprechung des *BVerfG* nicht mehr. Das Gericht definiert den *Anfangsverdacht* wie folgt:

> *„Dieser Verdacht muss auf konkreten Tatsachen beruhen; vage Anhaltspunkte und bloße Vermutungen reichen nicht aus [...]. Eine Durchsuchung darf nicht der Ermittlung von Tatsachen dienen, die zur Begründung eines Verdachts erforderlich sind; denn sie setzen einen Verdacht bereits voraus [...]. Notwendig ist, dass ein auf konkrete Tatsachen gestütztes, dem Bf. angelastetes Verhalten geschildert wird, das den Tatbestand eines Strafgesetzes erfüllt [...].“*

Die vor vierzehn Jahren noch erkannten „höheren Anforderungen“ des „auf bestimmten Tatsachen“ beruhenden Verdachts gegenüber dem „bloßen Anfangsverdacht“ sind nicht (mehr) vorhanden. Es handelt sich bei der Forderung nach einem auf „bestimmten Tatsachen“ beruhenden Verdacht vielmehr um eine Selbstverständlichkeit, aus der kein erhöhter Schutz resultiert.

[78] BVerfGE 109, 279 (350 f - Rn. 247).

(2) Prognoseanforderungen bei der Prävention

Für den präventiven Bereich führt das *BVerfG* aus, dass eine Rechtsgutsgefährdung im Einzelfall hinreichend konkret absehbar und der Adressat der Maßnahmen aus Sicht eines verständigen Dritten den objektiven Umständen nach in sie verfangen sein muss.[79] Dabei müssen die Eingriffsgrundlagen eine hinreichend konkretisierte Gefahr in dem Sinne verlangen, dass zumindest *tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr* für die Schutzgüter bestehen. Allgemeine Erfahrungssätze reichen nicht aus, um einen Zugriff zu rechtfertigen. *Es müssen bestimmte Tatsachen festgestellt sein, die im Einzelfall die Prognose eines Geschehens, das zu einer zurechenbaren Verletzung der relevanten Schutzgüter führt, tragen*[80].

Für weniger eingriffsintensive Maßnahmen zu Zwecken der Straftatenverhütung (etwa längerfristigen Observationen oder dem Einsatz technischer Mittel außerhalb von Wohnungen) billigte das *BVerfG* auch gesetzliche Tatbestandsformulierungen[81], die darauf abstellen, dass „*bestimmte Tatsachen die Annahme rechtfertigen, dass (katalogisierte) Straftaten begangen werden*". Voraussetzung ist dabei, dass gesetzgeberisch ausgeschlossen wird, dass sich die Prognose nicht allein auf allgemeine Erfahrungssätze stützt. Erforderlich ist, dass ein wenigstens seiner Art nach konkretisiertes und absehbares Geschehen erkennbar sein muss, oder die alternative Anforderung, dass das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft Straftaten begeht[82].

(3) Übertragung der Eingriffsschranken auf den repressiven Bereich

Die vorstehenden Anforderungen lassen sich auf den repressiven Bereich übertragen. Die dem Rechtsanwender abverlangten Prognoseleistungen unterscheiden sich in der Sache kaum. Lediglich der zeitliche Anknüpfungspunkt der Prognose (Zukunft/Vergangenheit) ist ein anderer. Während im präventiven Bereich bei der Straftatenverhütung zu prognostizieren ist, ob eine bestimmte Straftat begangen

[79] BVerfGE 141, 220 (270 Rn. 109); BVerfGE 120, 274 (328 f.); 125, 260 (330 f.).
[80] BVerfGE 141, 220 (270 Rn. 109); BVerfGE 110, 33 (56 f., 61); 113, 348 (377 f.).
[81] BVerfGE 141, 220 (290 ff.; Rn. 162 ff.).
[82] BVerfGE 141, 220 (291.; Rn. 165).

werden *wird* und wer möglicher Täter sein *wird*, gilt es im repressiven Kontext zu bestimmen, ob eine Straftat begangen *wurde* und wer der Täter *war*. Anknüpfungspunkt der Prognose sind jeweils in der Gegenwart festgestellte Tatsachen.

Dabei erfüllt die Eingriffsschwelle des § 100b StPO („*bestimmte Tatsachen, die den Verdacht einer Straftat begründen*") – allenfalls – in etwa die Anforderungen, die der erste Senat an die präventive Straftatenprognose in Bezug auf heimliche Maßnahmen i.S.d. § 20g BKAG a.F.[83] gesetzt hat („*bestimmte Tatsachen rechtfertigen die Annahme, dass eine Straftat begangen wird*" usw.).

Die für eine Online-Durchsuchung geforderten Prognoseleistungen werden dagegen nicht abgebildet. Hier sind die Prognoseanforderungen erhöht und die Eingriffsschwellen stark an eine konkrete Gefahr angenähert[84], die eine *hinreichende Wahrscheinlichkeit* einer Rechtsgutsverletzung erfordert. Für den repressiven Bereich bedeutet dies nichts anderes, als dass der erforderliche Verdacht einem „hinreichenden" Tatverdacht angenähert sein müsste.

Erforderlich gewesen wäre eine explizite gesetzliche Regelung, die im Hinblick auf die Eingriffsintensität der Maßnahme die Prognose des Normanwenders dergestalt lenkt, dass eine Anordnung einer Online-Durchsuchung nur bei *hinreichend schwerem* Tatverdacht erfolgt.

(4) Beurteilungsspielraum des anordnenden Gerichts bei der Tatverdachtsprognose

Weiter zur Unverhältnismäßigkeit der gesetzlich determinierten Verdachtsprognose trägt die Tatsache bei, dass der *BGH* den zur Anordnung strafprozessualer Eingriffsmaßnahmen zuständigen Stellen bei Annahme des erforderlichen Tatverdachts einen *Beurteilungsspielraum* einräumt, den auch die Rechtsmittelgerichte zu beachten haben[85].

---

[83] BVerfGE 141, 220 (271 f. Rn. 165 ff.).
[84] Nur „leichte Verlagerung ins Gefahrenvorfeld", so *Möstl*, DVBl. 2010, 808 (809) unter Bezugnahme auf *Roggan*, in: ders., Online-Durchsuchungen, 2008, 97 (103 f.); *Böckenförde*, JZ 2008, 925 (931), *Hornung*, CR 2008, 299 (304); *Baum/Schantz*, ZRP 2008, 137 (138 f.).
[85] BGHSt 41, 30 (33).

Dadurch wird die ohnehin eingeschränkte Nachprüfbarkeit heimlicher Ermittlungsmaßnahmen zusätzlich erschwert. Dass dagegen *nur* im präventiv-polizeilichen Bereich die anzustellende Prognose im Sinne eines umfassenden Grundrechtsschutzes verobjektiviert und einer rational-juristischen Kontrolle zugänglich gemacht wird[86], ist im Hinblick auf die identische Eingriffsintensität der Maßnahmen nicht begründbar.

(5) Verdachtsprognose und Stigmatisierungseffekte

Die niedrigschwellige gesetzliche Ausgestaltung der Verdachtsprognose ist zudem mit Blick auf mögliche Stigmatisierungseffekte als unverhältnismäßig zu beurteilen.

Gerade in den von § 100b Abs. 2 StPO erfassten Fällen von Schwerkriminalität, die regelmäßig enormen Ermittlungsdruck generieren[87], vermitteln heimliche Maßnahmen, bei denen sich nachträglich herausstellt, dass sich der ursprüngliche Tatverdacht nicht bestätigt hat, schwerste Persönlichkeitsrechtsbeeinträchtigungen.

Generell ist das Risiko einer Fehlprognose im repressiven Bereich für den Betroffen im Hinblick auf etwaige *Stigmatisierungseffekte* wesentlich grundrechtsbelastender als im Rahmen der Gefahrenabwehr. Denn schließlich wird der Betroffene als „beschuldigter Schwerkrimineller“ geführt, nicht als bloßes „Objekt der Gefahrenabwehr“.

---

[86] Dazu *Poscher*, Gefahrenabwehr – Eine dogmatische Rekonstruktion, 1999, S. 125 ff. u. passim.

[87] Dass in diesen Fällen bei lediglich „dünner“ Tatsachenbasis die erforderliche Verdachtsprognosen stark mit „kriminalistischem Erfahrungswissen“ und Vermutungen aufgeladen werden, die in der Praxis zur Rechtfertigung ganz erheblicher Grundrechtseingriffe herangezogen werden, ist Legende. Als Beispielsfall mögen die Ermittlungen im Mordfall „*Bögerl*“ dienen (hierzu *Albrecht/Braun*, HRRS 2013, 500; Braun, jurisPR-ITR 1/2017 Anm. 2). Hier wurde erfolglos in alle Richtungen ermittelt und – mit steigendem Ermittlungsdruck – auch ein „hinreichender Anfangsverdacht“ erkannt: Vom Ehemann der Ermordeten bis hin zu Personen aus dem Rockermilieu. Schließlich richtete sich der Verdacht – auf äußerst geringe Tatsachenbasis und im Wesentlichen auf kriminalistisches Erfahrungswissen gestützt - gegen Verwandte der Ermordeten. Die gegen sie gerichteten Ermittlungsmaßnahmen (insbesondere eine „IP-basierte Telekommunikationsüberwachung“), waren in Ausmaß und Schwere der damit verbundenen Persönlichkeitsbeeinträchtigungen mit einer Online-Durchsuchung vergleichbar (*Hieramente*, StraFo 2013, 96). Zudem wurde in diesem Verfahren rechtswidrig Verteidigerkommunikation abgehört. Der „Anfangsverdacht“ gegen die betroffenen Verwandten der Ermordeten stellte sich retrospektiv als haltlos heraus, wie bei allen anderen Ermittlungsmaßnahmen auch. Freilich hat das LG Ellwangen die „Schwere“ des Verdachts als ausreichend erachtet, intensivste Grundrechtseingriffe zu rechtfertigen (LG Ellwangen, Beschl. v. 28.05.2013 - 1 Qs 130/12; m. Anm. *Albrecht/Braun*, HRRS 2013, 500).

Insoweit reicht als eingriffsrechtfertigendes Tatbestandsmerkmal ein de facto „einfacher“ Tatverdacht nicht aus und bedarf einer Einhegung im Sinne eines hinreichend schweren Tatverdachts, der dem Risiko von Fehlprognosen entgegenwirkt.

cc) Fehlende Erfolgsprognose

Die Online-Durchsuchung ist unverhältnismäßig, da sie den Zugriff auf informationstechnische Systeme – insbesondere solcher „anderer Personen“ – nicht von einer auf Tatsachen basierenden Erfolgsprognose abhängig macht.

In der Entscheidung zum großen Lauschangriff hat das *BVerfG* explizit entsprechende gesetzliche Einschränkungen im Tatbestand gefordert:

> *„Allein mit der aktuellen Anwesenheit des Beschuldigten in der Wohnung eines unverdächtigen Dritten wird die Angemessenheit der Maßnahme in Wohnungen Dritter aber noch nicht erreicht. Neben der von § 100c II 5 StPO vorgeschriebenen Subsidiarität einer Überwachung von Wohnungen Nichtbeschuldigter muss eine* ***hinreichende Wahrscheinlichkeit bestehen, verfahrensrelevante Informationen zu gewinnen. Das verlangt nach tatsächlichen Anhaltspunkten dafür, dass der Beschuldigte in den zu überwachenden Räumlichkeiten im Überwachungszeitraum verfahrensrelevante und im weiteren Verfahren verwertbare Gespräche führen wird****. Bloße Vermutungen und eine Überwachung „ins Blaue hinein”, allein getragen von der Hoffnung auf Erkenntnisse, genügen nicht.*“[88].

Eine derartige Erfolgsprognose ist bei Maßnahmen nach § 100b Abs. 1 StPO nicht vorgesehen. Nach der neu geschaffenen Regelung können *alle* informationstechnischen Systeme, die der Betroffene „benutzt“, überwacht werden, ohne dass die Ermittlungsbehörden Anhaltspunkte dafür haben müssten, dass dort auch verfahrensrelevante Informationen gespeichert bzw. generiert würden. Entspricht dies bereits nicht den verfassungsrechtlichen Vorgaben an eine verhältnismäßige Ausgestaltung eingriffsintensiver Maßnahmen, wird zudem noch der Grundsatz

[88] BVerfGE 109, 279, (356 f.) - Hervorhebung nur hier.

missachtet, dass eine Ausdehnung der Online-Durchsuchung auf Geräte „anderer Personen“ nur subsidiär und nur unter strengen Voraussetzungen möglich sein darf.

Das *BVerfG* hat hierzu ausgeführt:

> „[E]*ine Online-Durchsuchung* [kann] *auf informationstechnische Systeme Dritter erstreckt werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Zielperson dort ermittlungsrelevante Informationen speichert und ein auf ihre eigenen informationstechnischen Systeme beschränkter Zugriff zur Erreichung des Ermittlungsziels nicht ausreicht.*“[89]

Der Gesetzgeber hätte also vorsehen müssen, dass eine Online-Durchsuchung auf informationstechnischen Geräten „anderer Personen“, die durch den Beschuldigten „benutzt“ werden, nur dann zulässig ist, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass nur so Daten erhoben werden können, die für die Erforschung des Sachverhalts von maßgeblicher Bedeutung sind[90].

Tatsächlich ist für den Zugriff auf informationstechnische Systeme „anderer Personen“ nach § 100b Abs. 3 Nr. 2 StPO lediglich erforderlich, dass die tatsachenbegründete Annahme besteht, dass die „*Durchführung des Eingriffs in informationstechnische Systeme des Beschuldigten allein nicht zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes eines Mitbeschuldigten führen wird*“. Das entspricht den vorgenannten Anforderungen nicht. Gestattet wird vielmehr eine Online-Durchsuchung informationstechnischer Systeme „anderer Personen“, die in ihren Anforderungen noch hinter der einfachen, offenen Durchsuchung bei „anderen Personen“ nach § 103 StPO, die nur bei einer tatsachenbegründeten Erfolgsprognose zulässig ist[91], zurückbleibt.

---

[89] BVerfGE 141, 220 (274 - Rn. 115).
[90] Vgl. *Roggan*, StV 2017, 821 (823 f.; 827).
[91] § 103 Abs. 1 S. 1 lautet: „Bei anderen Personen sind Durchsuchungen nur zur Ergreifung des Beschuldigten oder zur Verfolgung von Spuren einer Straftat oder zur Beschlagnahme bestimmter Gegenstände und nur dann zulässig, wenn Tatsachen vorliegen, aus denen zu schließen ist, daß die gesuchte Person, Spur oder Sache sich in den zu durchsuchenden Räumen befindet.“

dd) Unangemessene Subsidiaritätsklausel

Die in § 100b Abs. 1 Nr. 3 StPO enthaltene Subsidiaritätsklausel, wonach „*die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos*“ sein muss, vermag es nicht der Unverhältnismäßigkeit der Regelung entgegenzuwirken, noch diese herzustellen. Durch den Verzicht auf die gebotene Verwendung der Ultima-Ratio-Klausel, wie sie in § 100c Abs. 1 Nr. 4 StPO zur Anwendung kommt, verdeutlicht der Gesetzgeber zudem seine Fehleinschätzung der Eingriffsintensität der Online-Durchsuchung.

(1) Praktische Bedeutungslosigkeit

Wie alle heimlichen Maßnahmen im Ermittlungsverfahren beinhaltet § 100b Abs. 1 Nr. 3 StPO eine sog. Subsidiaritätsklausel.

Materielles Gewicht haben diese formelhaften Beschwörungen in der Praxis kaum. In Bezug auf die wortlautgleiche Regelung in § 100a Abs. 1 Nr. 3 StPO haben Befragungen im Rahmen einer Untersuchung des *Max-Planck-Instituts*[92] ergeben, dass in der Praxis *lediglich auf das Vorliegen einer Katalogtat* abgestellt wird. Eine Prüfung der weiteren Voraussetzungen auf Tatbestandsebene wird von den Ermittlungsbehörden regelmäßig als nicht notwendig erachtet. 47 % der überprüften richterlichen Beschlüsse enthielten entweder keine Ausführungen zur Subsidiarität oder begnügten sich mit der schlichten Wiedergabe des Gesetzeswortlautes. In 24 % der Anordnungen durch den Ermittlungsrichter fanden sich Ausfertigungen dessen, was die Staatsanwaltschaft vorgelegt hatte.

(2) Verkennung des Ultima-Ratio-Gebots

Unstreitig bezwecken die Subsidiaritätsklauseln eine *Steuerung der Verhältnismäßigkeitsprüfung*. Erkennbar ist ein gesetzgeberischer Wille der Abstufung

[92] *Albrecht/Dorsch/Krüpe*, Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen, Kriminologische Forschungsberichte aus dem Max-Planck-Institut für Ausländisches und internationales Strafrecht, 2003.

der Prüfungsdichte, wie die Ausgestaltung der unterschiedlichen Subsidiaritätsklauseln zeigt[93]:

- Stufe 1: „weniger erfolgversprechend oder erschwert“ (einfache Subsidiaritätsklausel, z.B. § 100h StPO[94]),
- Stufe 2: „erheblich weniger erfolgversprechend oder wesentlich erschwert“ (qualifizierte Subsidiaritätsklausel, z.B. § 163f StPO),
- Stufe 3: „aussichtslos oder wesentlich erschwert“ (strenge Subsidiaritätsklausel etwa § 100a und § 100b StPO) und
- Stufe 4: „unverhältnismäßig erschwert oder aussichtslos“ (Ultima-Ratio-Klausel, § 100c StPO).

Diese Kategorisierung verdeutlicht die gesetzgeberische Fehleinschätzung der Eingriffstiefe einer Online-Durchsuchung. Diese steht einer akustischen Wohnraumüberwachung nicht nach und ist *deutlich* grundrechtsbelastender als eine heimliche Erfassung der Telekommunikation.

Insoweit ist es unverhältnismäßig, wenn der Gesetzgeber die Steuerung der Verhältnismäßigkeitsprüfung durch eine Subsidiaritätsklausel auf das Niveau derjenigen bei einer Telekommunikationsüberwachung setzt und nicht den *gebotenen Ultima-Ratio-Ansatz* wie bei einer akustischen Wohnraumüberwachung manifestiert.

Das inhaltliche Prüfprogramm der Subsidiaritätsklausel ist zudem unpräzise. Aus dem Gesetzeswortlaut lässt sich kein exaktes Prüfprogramm ableiten. Für die streitgegenständliche Subsidiaritätsklausel wird in der Kommentarliteratur festgestellt, der Eingriff müsse gegenüber anderen Ermittlungsangriffen mit ähnlicher Erfolgseignung nachrangig sein.[95] Die Erfolgsaussichten der geplanten Überwachung müssten höher sein, als die Erfolgsaussichten anderer Ermittlungsmaßnahmen. Eine „wesentliche Erschwerung“ läge vor, wenn andere Ermittlungsmaßnahmen zeitlich

[93] „Abstufung der Güterabwägung“, *Bruns*, in: Hannich, Karlsruher Kommentar zur StPO, 7. Aufl. 2013, § 100c Rn. 8-15.
[94] BGH, Urt. v. 22.8.1996 – 5 StR 680/94.
[95] *Bär*, TK-Überwachung, 2009, § 100a, Rn. 24.

erheblich aufwendiger sind oder schlechtere bzw. nicht für eine schnelle Ermittlung erforderliche und ausreichende Erkenntnisse erwarten lassen[96].

Ein derart „laxes" Prüfprogramm wird indes der Eingriffsintensität einer Online-Durchsuchung nicht gerecht. Wenn ein materieller Zugewinn mit einer Subsidiaritätsklausel zu erreichen gewesen wäre, hätte der Ultima-Ratio-Grundsatz festgeschrieben werden müssen.

(3) Untaugliches Mittel zur Schärfung der Tatverdachtsprognose

Das *BVerfG* hat in der Entscheidung zur akustischen Wohnraumüberwachung einen „auf bestimmten Tatsachen beruhenden Verdacht" mitunter nur deshalb als verhältnismäßig beurteilt, weil die Überwachungsmaßnahme nur „als letztes Mittel" der Strafverfolgung eingesetzt werden dürfe, woraus sich regelmäßig auch eine erhöhte Wahrscheinlichkeit für die Begehung der besonders schweren Katalogstraftat ergeben würde[97].

Diese Argumentation kann auf den vorliegenden Gegenstand nicht übertragen werden. Mangels gesetzgeberischer Einordnung der Maßnahme als „ultima ratio" kann auch keine entsprechende „Kompensierung" des als Eingriffsschwelle unzureichenden Tatverdachts in Anlehnung an die Rechtsprechung des *BVerfG* zum großen Lauschangriff konstruiert werden.

(4) Unangemessener Beurteilungsspielraum

Im Übrigen ist es wiederum (wie bei Annahme des erforderlichen Tatverdachts) verfassungsrechtlich unhaltbar, dass den anordnenden Gerichten bei Prüfung der Subsidiaritätsklauseln ein Beurteilungsspielraum eingeräumt werden soll[98]. Damit werden im Ergebnis wesentliche Anordnungsvoraussetzungen von einer eingehenden nachträglichen gerichtlichen Nachprüfung suspendiert und in das Ermessen der anordnenden Stellen gelegt, was eine Verletzung des Rechts auf effektiven Rechtsschutzes indiziert.

---

[96] *Meyer-Goßner/Schmitt*, StPO, 61. Aufl. 2018, § 100a Rn. 13.; BeckOK StPO/*Graf*, § 100a Rn. 104.
[97] BVerfGE 109, 279 (350).
[98] Dazu *Eschelbach*, in: Satzger/Schluckebier/Widmaier, StPO, 3. Aufl. 2018, § 100b Rn. 15.

ee) Unverhältnismäßige Nicht-Berücksichtigung additiver Grundrechtseingriffe

(1) Fehlende gesetzliche Schutzvorkehrungen

Das *BVerfG* hat mehrfach auf das Bedürfnis einer besonders sorgfältigen Verhältnismäßigkeitsprüfung beim Zusammenwirken unterschiedlicher (heimlicher) Überwachungsmaßnahmen hingewiesen[99].

Ob und wie das Zusammenwirken mehrerer Überwachungsmaßnahmen aus dem Blickwinkel der Verhältnismäßigkeit zu beurteilen und in Abwägung zu bringen ist, bleibt nach dem gegenständlichen Regelungsregime offen, obwohl dies vorzuzeichnen notwendige Aufgabe gesetzlicher „Subsidiaritätsklauseln" gewesen wäre; vor allem unter dem Gesichtspunkt einer möglichen unzulässigen „*Totalüberwachung*":

> „*Mit der Menschenwürde unvereinbar ist es, wenn eine Überwachung sich über einen längeren Zeitraum erstreckt und derart umfassend ist, dass nahezu lückenlos alle Bewegungen und Lebensäußerungen des Betroffenen registriert werden und zur Grundlage für ein Persönlichkeitsprofil werden können (vgl. BVerfGE 109, 279 [323]; 112, 304 [319]; 130, 1 [24]; stRspr). Beim Einsatz moderner, insbesondere dem Betroffenen verborgener Ermittlungsmethoden müssen die Sicherheitsbehörden mit Rücksicht auf das dem "additiven" Grundrechtseingriff innewohnende Gefährdungspotenzial koordinierend darauf Bedacht nehmen, dass das Ausmaß der Überwachung insgesamt beschränkt bleibt (vgl. BVerfGE 112, 304 [319 f.]).*"[100]

Mögliche Kriterien zur Bestimmung der Schwelle, ab der kumulative Überwachungsmaßnahmen in eine unzulässige Totalüberwachung umschlagen sind nach *Hornung* beispielsweise[101]: die Anzahl der Maßnahmen, die Anzahl und Art der beteiligten staatlichen Stellen, die Dauer der einzelnen Maßnahmen, die Dauer der zeitlichen Überschneidung der Anwendung, die Anzahl und Bedeutung der überwachten Lebensbereiche, die Betroffenheit höchstpersönlicher Kommunikation, das Bestehen

[99] Dazu etwa BVerfG, NJW 2005, 1338 (1341).
[100] BVerfGE 141, 220 (280 - Rn. 130).
[101] *Hornung*, Die kumulative Wirkung von Überwachungsmaßnahmen, in: Albers/Weinzierl, MenschenrechtlicheStandards in der Sicherheitspolitik, 2010, S. 65 (74).

besonderer Vertrauensverhältnisse, die Kombination mehrerer Erfassungsmodi (Bild, Ton, Video, Bewegung), der Bezug zu Rückzugsräumen (wie durch Art. 13 GG und das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme vermittelt) sowie das Bestehen überwachungsfreier Bereiche in zeitlicher und örtlicher Hinsicht.

In dieser Hinsicht die Verhältnismäßigkeitsprüfung zu konturieren hat der Gesetzgeber keine Unternehmungen angestellt.

(2) Fehlende Prüfungsmöglichkeit der anordnenden Stelle

Selbst wenn man keine speziellen Regelungen zur Verhinderung einer Totalüberwachung gesetzgeberisch für geboten halten wollte und diesbezügliche Verpflichtungen aus dem allgemeinen zu beachtenden Verhältnismäßigkeitsgrundsatz ableiten möchte, müsste nach dem gesetzgeberischen Konzept zumindest sichergestellt sein, dass eine entsprechende Prüfung durch die anordnende Stelle praktisch ermöglicht wird.

Das ist vorliegend nicht der Fall.

Über die Zulässigkeit einer Online-Durchsuchung – eingeschlossen deren Unzulässigkeit aufgrund einer möglichen Totalüberwachung – entscheidet ausschließlich ein Gericht (§ 100e StPO). Damit die anordnende Stelle dieser Aufgabe nachkommen kann, müssen ihr obligatorisch Auskünfte über alle bisherigen bereits ergriffenen und geplanten repressiven *und* präventiven (!) (heimlichen) Maßnahmen gegeben und die daraus gewonnene Erkenntnisse detailliert mitgeteilt werden.

Eine Verpflichtung hierzu ist in verfassungswidriger Weise in § 100e StPO nicht niedergelegt worden.

Selbst wenn man, wie hier vertreten, eine Online-Durchsuchung unter Berücksichtigung des gegenwärtigen Stands der Technik und der heutigen Nutzungsgepflogenheiten nicht a priori als unzulässige Totalüberwachung klassifizieren möchte, so dürfte doch

unbestritten sein, dass bei einer Online-Durchsuchung im Falle zusätzlicher heimlicher Datenerhebungsmaßnahmen in aller Regel die merkliche Gefahr einer unzulässigen Rundumüberwachung besteht, die zwingend effektiver richterlicher Vorabeinschätzung bedarf. Dies ist hingegen durch das gesetzgeberische Konzept nicht gewährleistet[102].

ff) Unverhältnismäßige Dauer der Maßnahme

In § 100e Abs. 2 Sath 4 StPO beträgt die Anordnungsdauer einen Monat. Allerdings kennt das Gesetz keine Höchstdauer. Eine Verlängerung ist nach Maßgabe der Vorschrift bis zu einer Gesamtdauer von sechs Monaten (!) möglich; darüber hinaus im Falle oberlandesgerichtlicher Anordnung theoretisch unbegrenzt.

Die gesetzliche Ermöglichung einer solchen Dauerüberwachung eines informationstechnischen Systems ist nicht erforderlich (vgl. oben b), impliziert eine menschenunwürdige Totalüberwachung und ist generell unvereinbar mit dem Grundsatz der Verhältnismäßigkeit. Dementgegen enthält etwa die spanische Regelung zu einer Online-Durchsuchung eine feste Obergrenze von drei Monaten[103].

gg) Tatverdacht, Vorfeldstrafbarkeit und kompetentielle Friktionen

Die dem Erfordernis eines bloßen einfachen Tatverdachts immanenten Prognosedefizite werden verschärft, wenn man Straftaten in den Blick nimmt, die weit im Vorfeld von konkreten Rechtsgutverletzung ansetzen [104] und mit der klassischen Strafrechtsdogmatik brechen. Nicht nur wird damit im Ergebnis polizeiliche Gefahrenabwehr betrieben[105], auch Prognoseschwierigkeiten sind virulent, die ein Ausgreifen ins stark Spekulative befeuern.

---

[102] Auch müssen vor einer Online-Durchsuchung erfolglos durchgeführte heimliche Überwachungsmaßnahmen bekannt sein, um eine Güterabwägung vornehmen zu können. Ist nämlich die erforderliche Tatsachenbasis „dünn“ und haben etwaige vorab getroffene heimliche Überwachungsmaßnahmen, insbesondere Überwachungen der Telekommunikation, keine weiteren verdachtsbegründenden Erkenntnisse gebracht, liegt die Annahme nahe, dass sich der angenommene Verdacht womöglich nicht bestätigen könnte.
[103] *Winter*, ZStW 129 (2017), 205 (215 f.).
[104] Siehe etwa die in § 100b Abs. 2 Nr. 1 a) und b) genannten Straftaten.
[105] Dazu *Griesbaum/Wallenta*, NStZ 2013, 369 ff.

Zudem werden die Grenzen zwischen Gefahrenabwehr und Strafverfolgung unzulässig verwischt, indem es den Ermittlern ermöglicht wird, überschießende gefahrenabwehrende Motive in das Gewand des Strafrechts zu kleiden: In Bundesländern, in denen keine präventive Befugnis für eine Online-Durchsuchung besteht, könnte in typischen Vorfeldkonstellationen (etwa im Bereich der Terrorismusbekämpfung) kompetenzwidrig auf die strafprozessuale Befugnis zurückgegriffen werden[106].

So werden bei Gefahren, die durch den internationalen Terrorismus ausgehen, regelmäßig auch zureichende tatsächliche Anhaltspunkte etwa für die Mitgliedschaft in einer terroristischen Vereinigung nach §§ 129a Abs. 1 und 2, 129b Abs. 1 StGB vorliegen (vgl. § 100b Abs. 2 Nr. 1 b StPO). Mit den Vorschriften der §§ 129a, 129b StGB soll im Sinne einer Vorverlagerung des Rechtgüterschutzes erhöhten Gefahren begegnet werden, die im Falle der Planung, Vorbereitung oder Begehung von schweren Straftaten von festgefügten Organisationen aufgrund der ihnen innewohnenden Eigendynamik für die innere Sicherheit ausgehen können. Sobald die „Gefahrenermittlungen" also Bezüge zu einer in- oder ausländischen terroristischen Vereinigung ergeben, korrespondiert die Gefahrenprognose mit der Tatverdachtsprognose[107].

In diesen Fällen ist es unter Zugrundelegung der neueren Rechtsprechung des *BGH* („legendierte Kontrollen") [108] möglich, präventive, wie repressive Maßnahmen zu ergreifen. Die besagte Rechtsprechung intendiert eine Wahlmöglichkeit der Polizei, eine Situation als Gefahrenabwehr- oder Strafverfolgungsbehörde zu bewältigen und demzufolge auf polizeirechtlicher oder strafprozessualer Grundlage zu agieren. Die Folgen einer solchen Option sind gerade in verfahrensmäßiger Hinsicht, wie *Roggan* für Maßnahmen einer Online-Durchsuchung durch das Bundeskriminalamt herausarbeitet,

[106] Vergleichbare Konstellationen haben sich in der Praxis bei der Überwachung der Telekommunikation realisiert.
[107] *Griesbaum/Wallenta*, NStZ 2013, 369 ff. „Das gilt in besonderem Maße für die Straftatbestände der Vorbereitung einer schweren staatsgefährdenden Gewalttat (§ 89a StGB) und der Aufnahme von Beziehungen zur Begehung einer schweren staatsgefährdenden Gewalttat (§ 89b StGB), die bereits bei der Vorbereitung terroristischer Anschläge eingreifen können, auch wenn lediglich Einzeltäter identifizierbar sind und" die Voraussetzungen der §§ 129a, 129b StGB fehlen oder nicht nachgewiesen werden können.
[108] BGH, Urt. v. 26.04.2017 - 2 StR 247/16 „Legendierte Kontrollen"; BGH NStZ 2018, 296; NStZ-RR 2018, 146.

weitreichend[109] und mit verfassungsrechtlich gebotenen Kompetenzabschichtungen nicht vereinbar. Zudem sind eine Emanzipation der Polizei von der justiziellen Sachleitungsbefugnis und ein freies Changieren zwischen repressiven und präventiven Maßnahmen zu befürchten[110].

hh) Unzureichender Kernbereichsschutz

Die in § 100d Abs. 1 und § 100d Abs. 3 S. 1 StPO vorgesehenen Regelungen entsprechen nicht den Anforderungen an die gesetzgeberische Verpflichtung zum Schutz des Kernbereichs privater Lebensgestaltung.

Die Online-Durchsuchung geht in ihrer Eingriffsintensität weit über jede bisher durch die StPO gestattete Ermittlungsmaßnahme hinaus. Wie bereits dargelegt ist bei einer Online-Durchsuchung mit an Sicherheit grenzender Wahrscheinlichkeit eine Erhebung von Daten verbunden, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind. Wenn man entsprechende heimliche Datenerhebungen nicht bereits aus diesem Grund a priori für unzulässig halten möchte, so sind doch wirksame Maßnahmen zum Schutz des Kernbereichs privater Lebensgestaltung erforderlich.

(1) Unzureichender Kernbereichsschutz in der Erhebungsphase

Für die Erhebungsphase bestehen nach dem vorliegenden gesetzgeberischen Regelungskonzept faktisch keine Schutzvorkehrungen, die Eingriffen in den Kernbereich privater Lebensgestaltung wirksam vorbeugen könnten.

§ 100d Abs. 1 StPO läuft völlig leer[111]. Danach ist von der Maßnahme abzusehen, wenn Tatsachen die Annahme rechtfertigen, dass durch sie *allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung* erlangt werden. Es ist indes kaum denkbar, dass auf informationstechnische Systeme zugegriffen werden sollte, auf denen nach vorangegangener Prognose ausschließlich kernbereichsrelevante Inhalte gespeichert wären. Soweit man Anwendungsfälle für die Regelung finden wollte, wären diese jedenfalls ausnahmslos praxisfern und konstruiert.

---

[109] Hierzu *Roggan*, GSZ 2018, 52 ff.
[110] Vgl. *Roggan*, GSZ 2018, 52 ff.; *Schiemann*, NStZ 2017, 657 ff.
[111] Hierzu *Roggan* HRRS 2013, 153 (154 m.w.N.).

Zwar wurde in einem Beschluss des *BVerfG* eine entsprechende Regelung für heimliche Eingriffe in die Telekommunikation für verfassungskonform erachtet[112]. Allerdings sind die diesbezüglichen Feststellungen des Gerichts nicht auf den vorliegenden Gegenstand übertragbar. Anders als bei einer Überwachung der Telekommunikation ist bei einer Online-Durchsuchung nämlich eine Erfassung kernbereichsrelevanter Inhalte nicht nur am Rande (dazu sogleich), sondern *typischerweise*, wie bei einer heimlichen Wohnraumüberwachung, *zu erwarten*, sodass schon für die Erhebungsphase, ein wirksamer Kernbereichsschutz gesetzlich zu implementieren ist.

Als allein denkbar wirksame Schutzmaßnahmen in der Erhebungsphase verbleiben somit die in § 100d Abs. 3 S. 1 StPO normierten.

Dort heißt es:

> „*Bei Maßnahmen nach § 100b ist, soweit möglich, technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden.*“

Bislang ist es jedoch technisch unmöglich „sicherzustellen“, dass kernbereichsrelevante Daten nicht erhoben werden. Die Einordnung von Daten als zum Kernbereich privater Lebensführung zugehörend setzt einen äußerst komplexen und normativen Abwägungsvorgang voraus, den ein Computerprogramm nicht leisten kann. Zwar könnte versucht werden, bestimmte kernbereichsspezifische Arten von Daten auf Basis von syntaktischen Kriterien bei der Untersuchung auszuschließen, etwa auf Basis des Dateityps[113]. Eine solche Vorgehensweise ist jedoch nicht zielführend, da der Dateitypus allein nicht über die Zugehörigkeit der gespeicherten Information zum Kernbereich privater Lebensgestaltung entscheiden kann. Die Einschränkung läuft daher in der Praxis ebenso leer.

---

[112] BVerfGE 129, 208 (246 ff.); dagegen *Roggan* HRRS 2013, 153 (155 ff.).
[113] *Freiling/Safferling/Rückert*, JR 2018, 9 (14).

Die Wirksamkeit der gesetzlichen Regelung ist abhängig von *künftigen* technischen Entwicklungen. Mit Blick auf die Rechtsprechung des *BVerfG* ist dies insoweit nicht schädlich, da im Sinne eines Grundrechtsschutzes durch technische Verfahren zunächst nur ein Schutzauftrag besteht, der auf das technisch Mögliche begrenzt ist (so auch die Regelung: „soweit möglich"). Freilich hätte dann der Gesetzgeber sicherstellen müssen, dass diese Verpflichtungen durch erkennbare Bemühungen des Normanwenders auch *eingehalten* werden. So hätte zwingend eine explizite *Dokumentationspflicht* normiert werden müssen, nach der etwaige eingesetzte technische Schutzvorkehrungen in ihrer Funktionsweise und technischen Beschaffenheit zu protokollieren sind; flankiert von einer obligatorischen Kontrollpflicht durch eine unabhängige Stelle, wie den Bundesdatenschutzbeauftragten, die in die Lage versetzt wird, regelmäßig nachzuprüfen, ob die eingesetzten technischen Schutzvorkehrungen auch dem *gegenwärtigen Stand der Technik*[114] entsprechen. Nur so kann sichergestellt werden, dass der „technische Kernbereichsschutz" nicht lediglich symbolische, der verfassungsgerichtlichen Rechtsprechung formelhaft Tribut zollende Leerformel bleibt, sondern auch zur praktischen Anwendung kommt.

Der Gesetzgeber missachtet die Vorgabe des *BVerfG*, nach welcher ein Absehen von einer strengeren Regelung auf der „Erhebungsebene" (wie derjenigen in § 100d Abs. 4 StPO) *nur dann* zulässig ist, wenn lediglich „*eine Wahrscheinlichkeit besteht, dass* ***am Rande*** *auch höchstpersönliche Daten* ***miterfasst***"[115] werden.

Mit Blick auf die oben (A.IV) dargestellte Änderung der Nutzungsgepflogenheiten im Umgang mit informationstechnischen Systemen hätte es jedenfalls einer abgestuften Regelung bedurft. Auf der Erhebungsebene ist – ähnlich wie bei der akustischen Wohnraumüberwachung – eine Prognose zu erstellen, ob und in welchem Umfang kernbereichsrelevante Daten erfasst werden. Ergibt diese Prognose, dass eine Erhebung kernbereichsrelevanter Daten in nicht nur unerheblichem Umfang (also nicht nur am Rande) erhoben werden, ist von einer Anordnung und Durchführung der Maßnahme abzusehen.[116] Dies dürfte z.B. regelmäßig bei privat genutzten Smartphones der Fall

[114] BVerfGE 120, 274 (338).
[115] BVerfGE 141, 220 (307 Rn. 220) – Hervorhebung nur hier.
[116] Eine entsprechende Regelung könnte in Anlehnung an § 100d Abs. 4 S. 1 StPO lauten: „Maßnahmen nach § 100b dürfen nur angeordnet werden, soweit auf Grund tatsächlicher Anhaltspunkte anzunehmen

sein. Ergibt die Prognose hingegen, dass höchstpersönliche Daten voraussichtlich nur am Rande erhoben werden, wären zureichende Regelungen auf der „Aus- und Verwertungsebene“ zu treffen.

(2) Unzureichender Kernbereichsschutz in der Verwertungsphase

Die Regelungen auf der Verwertungsebene sind ebenfalls unzureichend ausgestaltet. Sie enthalten keine Vorgaben für den Fall, dass sich die o.g. Prognose als unzutreffend erwiesen hat und wider Erwarten in nicht nur ganz unerheblichem Umfang höchstpersönliche Informationen erfasst werden. Auch hier hat der Gesetzgeber offensichtlich übersehen, dass ein Abweichen von den für die akustische Wohnraumüberwachung geltenden Vorgaben nur dann angezeigt ist, wenn eine Erfassung von Daten aus dem Kernbereich privater Lebensgestaltung nur ganz am Rande zu besorgen ist.

Es hätte auch im Fall der Online-Durchsuchung einer Regelung bedurft, die – wie § 100d Abs. 4 StPO – eine (technisch mögliche!) Unterbrechung der Online-Durchsuchung und eine Entscheidung über die Fortführung durch ein Gericht fordert. § 100b StPO gestattet Zugriffe in Echtzeit[117]. Dann muss im Umkehrschluss auch ein Äquivalent zum Gebot einer Live-Überwachung zum Zwecke der Möglichkeit einer unverzüglichen Maßnahmeunterbrechung wie bei Lauschangriffen bestehen[118].

ii) Unzureichender Schutz von Berufsgeheimnisträgern

Nach der Ausgestaltung des § 100d Abs. 5 StPO besteht in verfassungswidriger Weise kein absoluter Schutz für sog. Berufshelfer der Berufsgeheimnisträger.

Die Regelung enthält zum Schutz der Kommunikation mit Berufsgeheimnisträgern ein absolutes Beweiserhebungsverbot.

---

ist, dass durch die Online-Durchsuchung Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, nur in unerheblichem Umfang erhoben werden.“.

[117] Hierzu *Freiling/Safferling/Rückert*, JR 2018, 9 (13).

[118] *Roggan*, StV 2017, 821 (828); ebenso *Freiling/Safferling/Rückert*, JR 2018, 9 (13).

Für die ebenso schutzbedürftige Kommunikation mit sog. Berufshelfern i.S.d. § 53a StPO ist hingegen lediglich ein relatives Beweisverwertungsverbot normiert. Die Verwertbarkeit staatlich erlangter Kommunikationsinhalte mit den Helfern des Berufsgeheimnisträgers soll nach § 100d Abs. 5 S. 2 StPO „*unter Berücksichtigung der Bedeutung des zugrundeliegenden Vertrauensverhältnisses nicht außer Verhältnis zum Interesse an der Erforschung des Sachverhalts oder der Ermittlung des Aufenthaltsortes eines Beschuldigten*“ in einem Abwägungsprozess entschieden werden.

Vor dem Hintergrund, dass in der Praxis vor allem in der elektronischen Kommunikation mit Berufsgeheimnisträgern deren Berufshelfer vor- (Sekretariate) bzw. notwendig zwischengeschaltet sind (man denke an Dolmetscher usw.), trägt die Regelung dem verfassungsrechtlich gebotenen Schutz des Kernbereichs privater Lebensgestaltung nicht Rechnung. Zu erinnern ist auch, dass in anderen Sachverhaltskonstellationen der Gesetzgeber die notwendige Schutzwürdigkeit der Berufshelfer mit Blick auf deren regelmäßigen Umgang mit besonders sensitiven, kernbereichsspezifischen Informationen erkannt und entsprechend forciert hat; man denke an die Novellierung des § 203 StGB (Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen vom 30.10.2017 [119]), die Berufsgeheimnisträgern die Einbindung von Berufshelfern mit Blick auf die Besorgnis eigener potentieller Strafbarkeit wegen Geheimnisverrats erleichtert[120]. Ebenso ist auf die Gleichstellung der Berufshelfer in § 160a Abs. 3 StPO hinzuweisen.

d. Schranken-Schranke: nationale (und internationale) IT-Sicherheit

Die Regelung des § 100b StPO ist auch insofern verfassungswidrig als sie pauschal einen Eingriff in informationstechnische Systeme gestattet, ohne die technischen Wege der Infiltration dergestalt zu begrenzen, dass eine Gefährdung der IT-Sicherheit Dritter zumindest nicht gefördert wird.

Nach dem vorliegenden Regelungskonzept ist zum Zweck der Infiltration des informationstechnischen Zielsystems eine Ausnutzung noch unbekannter

[119] BGBl. I S. 3618.
[120] Vgl. *Conen*, AnwBl. 2017, 640 (642 m.w.N.).

Sicherheitslücken in Betriebssystemen und Anwendungssoftware möglich. Die Informationen über diese Sicherheitslücken müssen ermittelt und vor den betroffenen Softwareherstellern verheimlicht werden, damit diese die Lücken nicht schließen. Die hieraus resultierenden und bewusst in Kauf genommenen Gefahren für die nationale (und internationale) IT-Sicherheit stehen zu dem Zweck der effektiven Strafverfolgung auch schwerer Straftaten in krassem Missverhältnis. Es besteht die hinreichende Wahrscheinlichkeit, dass die unbekannten Sicherheitslücken den „falschen" Personen bekannt werden bzw. unabhängig von den staatlichen Stellen entdeckt werden. Die Folge wäre, dass hierdurch mitunter lebenswichtige IT-Infrastrukturen Schaden nehmen (zum Vorfall „WannaCry" siehe bereits oben A.III.4).

Der Gesetzgeber hat, trotz eines entsprechenden Hinweises durch Sachverständige[121], ohne nähere Begründung von einer Ausnahmeregelung abgesehen, nach welcher eine Ausnutzung unbekannter Sicherheitslücken zum Zweck der Infiltration des Zielsystems unzulässig ist. Es wurde offenbar übersehen, dass eine entsprechende Verpflichtung bereits unmittelbar aus dem Recht auf Gewährleistung von Integrität und Vertraulichkeit informationstechnischer Systeme folgt. Dieses ist nicht nur Abwehrrecht des Bürgers gegen den Staat. Es enthält auch einen verfassungsrechtlichen Schutz- und Gewährleistungsauftrag zur Verwirklichung der Wertvorstellungen des Grundrechts.[122]

Dem kann nur durch einen expliziten Ausschluss der Ausnutzung unbekannter Sicherheitslücken zum Zweck der Durchführung der Maßnahmen entsprochen werden.

2. Sog. „kleine Online-Durchsuchung" (§ 100a Abs. 2 S. 3 StPO)

§ 100a Abs. 2 S. 3 StPO ist verfassungswidrig, da er einen verfassungsrechtlich nicht gerechtfertigten Eingriff in das Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme vermittelt.

[121] Vgl. auch *Buermeyer*, Stellungnahme, S. 21f. mit Formulierungsvorschlag auf S. 23.
[122] *Heckmann*, in: Heckmann, jurisPK-Internetrecht, 5. Aufl. 2017, Kap. 5 Rn. 125

a. Eingriff

Die Gestattung der sog. „kleinen Online-Durchsuchung“ durch § 100a Abs. 1 S. 3 StPO, wonach bei der Quellen-Telekommunikationsüberwachung nicht nur auf laufende, sondern auch auf gespeicherte (also „ruhende“) Kommunikation zugegriffen werden darf, wenn diese *„während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können*“ stellt einen Eingriff in das Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme dar.

Das Gericht hat mit Blick auf die Durchführung sog. Quellen-Telekommunikationsüberwachungsmaßnahmen bereits im Jahr 2008 ausdrücklich festgehalten,

> *„Art. 10 Abs. 1 GG ist hingegen der alleinige grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zu einer „Quellen-Telekommunikationsüberwachung“, wenn sich die Überwachung* ***ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt****. Dies muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein.*“[123]

Diese Grenze zwischen Art. 10 Abs. 1 GG und dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme wird mit der Befugnis zur heimlichen „retrograden“ Erhebung von gespeicherten Kommunikationsinhalten (und -umständen) überschritten.

b. Fehlende verfassungsrechtliche Rechtfertigung

Der durch § 100a Abs. 2 S. 3 StPO gestattete Eingriff ist verfassungsrechtlich nicht gerechtfertigt.

Die Regelung des § 100a Abs. 2 S. 3 StPO ist an den gleichen Maßstäben zu messen wie die durch § 100b Abs. 1 StPO gestattete Online-Durchsuchung. Diesen Anforderungen

[123] BVerfGE 120, 274 (309 - Rn. 190) - Hervorhebung nur hier.

wird § 100a Abs. 2 S. 3 StPO bereits deshalb[124] nicht gerecht, da er als Eingriffsanlass das Vorliegen eines einfachen Verdachts einer der vielfältigen Anlasstaten nach § 100a Abs. 2 StPO ausreichen lässt. Die im Katalog des § 100a Abs. 2 StPO[125]genannten Taten knüpfen vielfach nicht, wie vom Gericht gefordert[126], an überragend wichtige Rechtsgütern an[127].

In der Gesetzesbegründung[128] wird ein Abweichen von diesen strengen Eingriffsvoraussetzungen mit der unzutreffenden Argumentation zu legitimierenden versucht, dass die Eingriffsintensität der Maßnahme aufgrund der Beschränkung der Datenerhebung auf Telekommunikationsinhalte und -umstände gegenüber einer umfassenden Online-Durchsuchung nach § 100b StPO deutlich abgesenkt sei. Es bestünde eine Vergleichbarkeit mit Telekommunikationsüberwachungsmaßnahmen („funktionale Äquivalenz"), sodass die Eingriffsvoraussetzungen für eine kleine Online-Durchsuchung entsprechend abgesenkt werden dürften.

Diese Argumentation ist offensichtlich nicht tragfähig:

- Die Figur der „*funktionalen Äquivalenz*" ist kein Topos, der ein Abweichen von den verfassungsrechtlich gebotenen Eingriffsschwellen für eine Online-Durchsuchung rechtfertigen könnte (**aa**).
- Zudem verkennt der Gesetzgeber die *drastischen Grundrechtsbelastungen*, die Maßnahmen nach § 100a Abs. 2 S. 3 StPO vermitteln können; diese stehen einer Online-Durchsuchung nach § 100b StPO nicht nach (**bb**).
- Im Übrigen führt die Möglichkeit einer „kleinen" Online-Durchsuchung zu einer verfassungswidrigen *Aushebelung* des verfassungsrechtlich garantierten Rechts auf kommunikativen *Selbstschutz* (**cc**).
- Nur vorsorglich sei darauf hingewiesen, dass eine durch § 100a Abs. 2 S. 3 StPO ermöglichte „rückwirkende" Datenerhebung für den Zeitraum zwischen Maßnahmeanordnung und Installation der Späh-Software nicht erforderlich ist (**dd**).

[124] Die o.g. Ausführungen zur Online-Durchsuchung gelten für die „kleine Online-Durchsuchung" entsprechend.
[125] Vgl. zum Katalog der Anlasstaten für eine Online-Durchsuchung bereits oben D.II.1.c.aa).
[126] BVerfGE 120, 274 (328 - Rn. 247).
[127] Beispielhaft seien die §§ 108e, 146, 151, 244, 260, 260a, 263, 264, 265e StGB genannt.
[128] BT-Drs. 18/12785, S. 50 f.

aa) Keine Einschränkungen des Grundrechtsschutzes bei „funktionaler Äquivalenz“

Die Schutzbereiche des Fernmeldegeheimnisses und des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme sind komplementär angelegt[129]. Sobald die engen Grenzen des technisch gesicherten Zugriffs allein auf die *laufende* Kommunikation überschritten werden (Quellen-Telekommunikationsüberwachung), liegt eine Online-Durchsuchung vor, die wesentlich höheren verfassungsrechtlichen Schranken unterliegt. Dazwischen sind mit Blick auf die zu erhebenden Daten keine weiteren Abstufungen der Schutzwürdigkeit möglich.

Der Argumentationsansatz der „funktionalen Äquivalenz“ verkennt die Bedeutung der Privilegierung des Zugriffs auf nur *laufende* Kommunikationsinhalte. Diese beruht darauf, dass die den Schutzbereich des Fernmeldegeheimnisses prägenden Risiken der Datenübermittlung durch Dritte auf das informationstechnische System erweitert werden.[130]

Dagegen unterfallen auf dem System bereits perpetuierte Kommunikationsinhalte dem spezifischen Gewährleistungsgehalt des neuen Grundrechts. Der Schutzgehalt dieses Grundrechts wird bereits mit der Infiltration des Systems aktiviert[131]. Ob und welche Daten im Anschluss daran erhoben werden, ist dagegen irrelevant. Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gewährt den Schutz der auf dem „gekaperten“ System gespeicherten Daten *um ihrer selbst willen*. – Unabhängig davon, ob diese Daten ebenso auf andere Weise rechtmäßig und ggf. unter geringeren Eingriffsvoraussetzungen erhoben werden könnten. Die These von der „funktionalen Äquivalenz“ dagegen zielt unzulässig allein auf das möglicherweise identische Ergebnis der Überwachung ab und nimmt spezifische Gefährdungslagen, wie veritable Missbrauchsrisiken, die durch die Infiltration des Systems vermittelt werden aus dem Blick. Nähme man sie ernst, könnte man eine Online-Durchsuchung auch unter den Voraussetzungen der §§ 94 ff. StPO ermöglichen,

[129] *Buermeyer*, StV 2013, 470 (473).
[130] So auch *Buermeyer*, StV 2013, 470 (473).
[131] Vgl. BVerfGE 120, 274 (309 - Rn. 188).

geht es doch um die Gewinnung genau derselben Daten, nämlich all derer, die auf dem informationstechnischen Zielsystem gespeichert sind.

bb) Tatsächliche Eingriffsintensität der „kleinen" Online-Durchsuchung

In der Gesetzesbegründung wird ausschließlich die Notwendigkeit der Regelung in Bezug auf die Erfassung von Kommunikationsinhalten angesprochen, die mit Hilfe von *Messenger-Diensten* ausgetauscht werden. Faktisch geht die Regelung aber weit über die Erhebung solcher Daten hinaus und unterscheidet sich, was die Reichweite und den Umfang der erhebbaren Daten (Telekommunikationsinhalte und –umstände) betrifft, im Ergebnis nicht von einer „herkömmlichen" Online-Durchsuchung. Es werden Eingriffe von gleicher Intensität ermöglicht und das unter verfassungsrechtlich völlig unzureichenden Eingriffsvoraussetzungen und prozeduralen Sicherungen.

Nach dem Wortlaut der Norm wird die Erhebung *aller Telekommunikationsdaten* gestattet, die ab dem Zeitpunkt der Anordnung auf dem informationstechnischen System generiert werden. Entscheidend für die Eingriffsintensität der Maßnahme ist der – strittige – Begriff der Telekommunikation. In einem Nichtannahmebeschluss aus dem Jahre 2016 geht die Dritte Kammer des Zweiten Senats des *BVerfG* von einem denkbar *weiten Begriffsverständnis* aus[132]:

Das Telekommunikationsgeheimnis schütze davor, dass staatliche Stellen sich in die Kommunikation einschalten und Kenntnisse über die Kommunikationsbeziehungen oder Kommunikationsinhalte gewinnen. Da auch bei der Nutzung des Internets ein solches Gefährdungspotential besteht, erstrecke sich der Schutzbereich des Art. 10 GG auch auf das *„Surfen" bzw. Abrufen* von Web-Seiten. Den Einwand der Literatur[133], dass für eine schützenswerte Telekommunikation Voraussetzung ist, dass Individuen miteinander kommunizieren, lässt das Gericht nicht gelten. Der Schutz der Vertraulichkeit knüpfe nicht an die Beteiligten der Kommunikation, sondern an den

[132] BVerfG, 2. Senat 3. Kammer, Nichtannahmebeschluss v. 6.7.2016 – 2 BvR 1454/13; ähnlich *Bäcker*, Die Vertraulichkeit der Internetkommunikation, in: Rensen/Brink (Hrsg.), Linien der Rechtsprechung des Bundesverfassungsgerichts – erörtert von den wissenschaftlichen Mitarbeitern, S. 99 (109 f.).
[133] Etwa *Böckenförde*, JZ 2008, 925 (937); *Hiéramente*, StraFo 2013, 96 (99); *Meinicke*, in: Taeger, Law as a Service – Recht im Internet- und Cloud-Zeitalter, 2013, 969 (971); *Albrecht/Braun*, HRRS 2013, 500 (503); *Braun*, jurisPR-ITR 18/2013 Anm. 5; *Albrecht/Dienst,* JurPC Web-Dok. 5/2012 Abs. 22.

Übermittlungsvorgang und das dabei genutzte Medium an. Ein empfängergesteuerter Abruf von Informationen aus dem Netz sei eine Übermittlung von Informationen an einen individuellen Rezipienten, was in Abgrenzung zu einem nicht geschützten, rein maschinellen Datenaustausch [134] ausreiche, um einen schützenswerten Kommunikationsvorgang anzunehmen. Zudem sei das schutzauslösende spezifische Gefährdungspotenzial für die Privatheit der Kommunikation vorhanden, da willensgesteuert auf konkrete Kommunikationsinhalte zugegriffen werde. Damit sei auch das „Surfen" im Internet unter das Fernmeldegeheimnis zu subsumieren und vom Begriff der Telekommunikation in § 100a StPO erfasst.

Damit wird die „kleine" Online-Durchsuchung, die den Zugriff auf ebendiese Telekommunikationsinhalte gestattet zu einer „großen". Sie erfasst nicht nur, wie die Gesetzesbegründung unzutreffend suggeriert[135], die typischen Kommunikationsinhalte (etwa mittels Messenger-Diensten), sondern alle Informationen, die willensgesteuert von einer Person über das Internet abgerufen und übermittelt wurden. Die Datenmenge und Datenqualität, die regelmäßig durch eine längerfristige Überwachung der Internetaktivitäten der Zielperson gem. § 100a Abs. 2 S. 3 StPO gewonnen werden kann, befähigt zu einer Kumulation und Kombination der erhobenen Information, durch die ein umfassendes Persönlichkeitsprofil erstellt werden kann.

Es lassen sich – wie dargelegt – durch eine Auswertung des Surfverhaltens (Nutzung von Suchmaschinen, E-Commerce- und E-Government-Anwendungen, Soziale Netzwerke, Musik- und Videoplattformen usw.) umfassende Rückschlüsse auf die Persönlichkeit ziehen (z.B. soziale Aktivitäten, sexuelle Vorlieben, Gesundheitszustand usw.), die oftmals an Detailgenauigkeit nicht einmal engsten Freunden und Familienangehörigen bekannt sein dürften[136] Ebenso ermöglicht wird die Ausleitung aller Inhalte, die über Cloud-Computing-Dienste transferiert wurden.

Die Eingriffsintensität wird zudem durch die Dauer der Überwachung ganz wesentlich verstärkt. In einem üblichen Zeitraum von drei Monaten (vgl. § 100e Abs. 1 S. 4 StPO)

---

[134] Hierzu BVerfG, Beschluss vom 22.10.2006 – 2 BvR 1345/03 - IMSI-Catcher.
[135] BT-Drs. 18/12785, S. 50 f.
[136] *Hieramente*, StraFo 2013, 96, *Albrecht/Braun*, HRRS 2013, 500 (503) *Braun*, jurisPR-ITR 18/2013 Anm. 5.

kann eine solche Masse an personenbezogenen Daten erhoben werden, dass sie einem Auslesen des gesamten informationstechnischen Systems nicht nachsteht.

So illustriert das *BVerfG* die immense Eingriffsqualität einer Online-Durchsuchung auch und gerade damit, dass durch eine Infiltration des Rechners des Betroffenen massenhaft sensible Daten über seine *Online*-Aktivitäten gewonnen werden können. Das Gericht erkennt die besondere Schwere des Eingriffs darin, dass durch eine Online-Durchsuchung die Möglichkeit bestehe, *„die gesamte Internetkommunikation des Betroffenen über einen längeren Zeitraum mit zu verfolgen*“[137]. Genau dies wird durch die gegenständliche „kleine“ Online-Durchsuchung ermöglicht.

Soweit man einen graduellen Unterschied zu einem „Vollzugriff“ auf die auf einem informationstechnischen System gespeicherten Daten nach § 100b StPO erkennen wollte, ist dieser nur mit Blick auf Inhalte, die keine „Telekommunikation“ i.S.d. § 100a StPO darstellen und Telekommunikationsinhalte, die vor Erlass der zugriffseröffnenden Anordnung auf dem System gespeichert wurden, erkennbar. Eine andere Bewertung lassen diese marginalen Unterschiede indes nicht zu. Zudem ist zu erinnern, dass mit Blick auf den derzeitigen Stand der Technik und den üblichen Nutzungsgepflogenheiten derartige Inhalte regelmäßig über das Internet transferiert und damit als „Telekommunikation“ zum Zielobjekt von Maßnahmen nach § 100a Abs. 2 S. 3 StPO werden können; man denke etwa an regelmäßige Synchronisierungen zwischen mehreren Endgeräten oder Zugriffe auf in den Anbieter-Clouds (z.B. iCloud, Dropbox) abgelegte Dateien, Back-Ups usw. Im Übrigen sind Internetnutzer auf eine Datenspeicherung im eigenen informationstechnischen System ohnehin immer weniger angewiesen. Mittels Cloud-Computing-Anwendungen kann nahezu die gesamte Rechneraktivität in virtuelle Speicher, auf die ein ortsunabhängiger Zugriff möglich ist, verlegt werden. Dabei werden die in der Vergangenheit auf stationären Festplatten vorgehaltenen Speicherkapazitäten durch „virtuelle“ Speicher ersetzt. Jeder Zugriff auf diese ausgelagerten Festplatten stellt einen Telekommunikationsvorgang dar, der durch eine „kleine“ Online-Durchsuchung überwacht werden könnte.

[137] BVerfGE 120, 274 (324 - Rn. 235).

cc) Aushebelung von verfassungsrechtlich garantierten Selbstschutzmöglichkeiten

§ 100a Abs. 2 S. 3 StPO enthält die „Einschränkung", dass eine Überwachung und Aufzeichnung der Telekommunikation nur erfolgen darf, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätte überwacht und aufgezeichnet werden können.

Die Regelung besagt zweierlei: Nämlich, dass ausschließlich auf Inhalte zugegriffen werden darf, die auch durch eine (Quellen-)Telekommunikationsüberwachung hätten erhoben werden dürfen und dass solche Maßnahmen gegenüber einer sog. „kleinen" Online-Durchsuchung vorrangig sind; es sei denn, ein Zugriff ist mangels Verschlüsselung nicht möglich. Diese Voraussetzungen werden regelmäßig erfüllt sein. Eine vollständige Überwachung der Internetkommunikation soll – nach hier vertretener Ansicht: unzutreffend[138] – nach einem Kammerbeschluss des *BVerfG* von der Vorschrift der Ermächtigung des § 100a Abs. 1 StPO gedeckt sein (sog. IP-basierte Telekommunikationsüberwachung oder DSL-Überwachung)[139]. Lässt sich eine solche umfassende Überwachung aufgrund des Einsatzes von Verschlüsselungstechniken – sei es partiell durch den Anbieter von Internetkommunikationsdiensten oder umfassend durch den Beschuldigten, der seine gesamte Internetkommunikation verschlüsselt – nicht bewerkstelligen, stünde eine „kleine" Online-Durchsuchung offen.

In diesem Zusammenhang wird die Widersinnigkeit der Vorschrift evident. Letztlich besagt der Passus, dass *derjenige, der im Internet verschlüsselt kommuniziert, zugleich Anlass dafür gibt, dass jetzt sein informationstechnisches System infiltriert wird* – ohne dass hierfür die Eingriffsvoraussetzungen im Vergleich zu einer Telekommunikationsüberwachung erhöht sein müssten.

Damit werden verfassungsrechtlich garantierte *Selbstschutzmöglichkeiten* verletzt. Die behördliche Infiltration und die damit einhergehende Manipulation eines informationstechnischen Systems führt dazu, dass das aus dem Grundrecht auf Informationelle Selbstbestimmung abgeleitete Recht auf Selbstschutz als wesentliches Element eigenbestimmter Kommunikationsteilnahme durch verschlüsselte

[138] *Eidam*, NJW 2016, 3508, 3511; ff.; *Hieramente*, HRRS 2016, 448; *Braun*, jurisPR-ITR 1/2017 Anm. 2.
[139] BVerfG, Beschluss vom 6.7.2016 – 2 BvR 1454/13 - NJW 2016, 3508 m. abl. Anm. *Eidam.*

Kommunikation unterlaufen wird.[140] Auch diese zusätzliche Grundrechtsbeeinträchtigung verwehrt einen „Gleichlauf" der Eingriffsvoraussetzungen mit denen einer Telekommunikationsüberwachung und fordert die vom *BVerfG* für eine Online-Durchsuchung formulierten strengen Eingriffshürden.

Dieser Argumentation kann nicht entgegengehalten werden, dass das *BVerfG* für Fälle einer – zumindest abstrakt – denkbaren Quellen-Telekommunikationsüberwachung fehlende Selbstschutzmöglichkeiten nicht zum Anklang gebracht hat. Das Gericht hatte in seiner Entscheidung aus dem Jahre 2008 ausschließlich Kommunikationsformen, wie VOIP-Dienste im Blick, auf die ein Zugriff aus technischen Gründen, unabhängig von Selbstschutzvorkehrungen des Betroffenen, eine Überwachung ausgeschlossen war. Unter strengen Voraussetzungen, insbesondere wirksamen technischen Sicherungsvorkehrungen vor einem Zugriff auf andere Inhalte, sah das Gericht eine Infiltration mit dem eingeschränkten Ziel der Erhebung der „laufenden" Kommunikation vor.

Eine Bewertung *sämtlicher* willensgesteuerter Nutzungen des Internet als „Telekommunikation", wie es heute teilweise vertreten wird, und damit auch eine Erstreckung von Telekommunikationsüberwachungsmaßnahmen auf diese Inhalte, hatte das Gericht damals nicht vor Augen (auch geht der erste Senat noch immer von einem engeren Begriffsverständnis aus[141]). War es Betroffenen insoweit noch möglich auf andere Kommunikationsformen auszuweichen, verbleibt nach Maßgabe des weiten Begriffs der Telekommunikation als Selbstschutzmöglichkeit nur, auf die Nutzung des Internets gänzlich zu verzichten. Das freilich kann darunter wohl kaum verstanden werden.

dd) Unverhältnismäßige „rückwirkende" Datenerhebungen

§ 100b Abs. 2 S. 3 StPO ermöglicht Zugriffe auf Telekommunikationsinhalte- und Umstände, die auf dem zu überwachenden informationstechnischen System ab dem Zeitpunkt der richterlichen Anordnung generiert werden. Auf den Zeitpunkt der

[140] *Hoffmann-Riem*, JZ 2008, 1109 (1118).
[141] BVerfGE 141, 220 (312 f. - Rn. 238).

tatsächlichen Infiltration des informationstechnischen Systems durch die Überwachungssoftware kommt es dagegen nicht an. Innerhalb des Geltungszeitraums der Anordnung können also auch rückwirkende Datenerhebungen mit der Ausschlussgrenze des Anordnungszeitpunktes vorgenommen werden. Begründet wird dies mit dem Ziel der Regelung. In der Gesetzesbegründung wird dieses als ein „funktionales Äquivalent" zur möglichen herkömmlichen Ausleitung der Telekommunikation, die bei den Telekommunikationsunternehmen im öffentlichen Telekommunikationsnetz mit dem Vorliegen des Beschlusses sofortige Zugriffe ermöglicht[142]nur schwammig zum Ausdruck gebracht.

Der dargestellte zeitliche Ansatzpunkt der Überwachung ist unverhältnismäßig. Ein Bedürfnis für eine entsprechende rückwirkende Überwachung ist nicht erkennbar. Es geht vorliegend um die Gewinnung von Erkenntnissen zur *Strafverfolgung*. Anders als im Rahmen der Gefahrenabwehr ist kein besonderes Eilbedürfnis erkennbar, bei der für die Informationsgewinnung wenige Stunden oder Tage ausschlaggebend wären. Zudem ist die regelmäßige Anordnungsdauer der Maßnahme von drei Monaten (mit mehrmaliger Möglichkeit der Verlängerung, vgl. § 100e Abs. 1 StPO) in jedem Falle ausreichend um eine ggf. zeitaufwändige Infiltration des zu überwachenden Informationstechnischen Systems zu kompensieren.

3. Quellen-Telekommunikationsüberwachung (§ 100a Abs. 2 S. 2 StPO)

Auch die nach § 100a Abs. 2 S. 2 StPO gestattete Quellen-Telekommunikationsüberwachung ist als verfassungsrechtlich nicht gerechtfertigter Eingriff in das Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme zu bewerten.

§ 100a Abs. 2 S. 2 StPO gestattet de facto eine (nur beweisthematisch begrenzte) Online-Durchsuchung, da technisch nicht ausgeschlossen werden *kann*, dass neben der „laufenden Kommunikation" auch weitere persönlichkeitsrelevante Informationen erhoben werden (hierzu bereits oben A.III.5). Mit Blick auf ein entsprechendes Vorbringen im Zusammenhang mit § 20k BKAG a.F. hat das *BVerfG* vertreten, dass

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

> *„Sollten zum gegenwärtigen Zeitpunkt diese Anforderungen nicht erfüllbar sein, liefe die Vorschrift folglich bis auf weiteres leer. Auch dies machte sie jedoch nicht widersprüchlich und verfassungswidrig,* ***weil damit nicht ausgeschlossen ist, dass die nötigen technischen Voraussetzungen in absehbarer Zukunft geschaffen werden können****."*[143]

Das Gericht hat, wie der letzte Halbsatz suggeriert, im damaligen Verfahren den Eindruck gewonnen, dass die technische Unmöglichkeit der Beschränkung einer Trojanersoftware auf die Überwachung der laufenden Kommunikation „*in absehbarer Zukunft*" überwunden werden könnte. Das ist nicht der Fall.

Es ist seit dem Jahr 2008 nicht gelungen und wird auch in absehbarer (und auch ferner) Zukunft nicht möglich sein, eine Trojanersoftware zu entwickeln, die allein die „laufende Kommunikation" überwacht.[144] Es handelt sich bei § 100a Abs. 2 S. 2 StPO also nicht nur um eine – nach Auffassung des Gerichts zulässige[145] – Gesetzgebung „auf Vorrat", sondern um eine Regelung die eine Maßnahme gestattet, die technisch so niemals umsetzbar sein wird.

Die Regelung läuft also nicht „bis auf weiteres leer", sie läuft ad infinitum leer. Sie ist dementsprechend „*widersprüchlich und verfassungswidrig*", da „*ausgeschlossen ist, dass die nötigen technischen Voraussetzungen in absehbarer Zukunft geschaffen werden können*".

Dass der Gesetzgeber offenbar selbst davon ausgeht, dass sich eine Quellen-Telekommunikationsüberwachung nicht auf die „*laufende Kommunikation*" begrenzen lässt, wird mit § 100a Abs. 5 S. 1 Nr. 1 StPO verdeutlicht. Der Gesetzgeber gibt zu erkennen, dass er eine Quellen-Telekommunikationsüberwachung und eine „kleine Online-Durchsuchung" (§ 100a Abs. 1 S. 3 StPO) als einheitliche Maßnahme betrachtet, wenn er von „*Maßnahmen nach Absatz 1 Satz 2* ***und*** *3*" spricht.

---

[143] BVerfGE 141, 220 (311 f. – Rn. 234) - Hervorhebung nur hier.
[144] Vgl. nochmals *Hornung*, Stellungnahme, S. 6.
[145] A.A. *Tomerius*, NVwZ 2015, 412 (414), *Roggan*, LKV 2015, 14 (16 f.).

Der Versuch, die Vorgabe des *BVerfG* einzuhalten, die Quellen-Telekommunikationsüberwachung „rechtlich" auf die laufende Telekommunikation „zu begrenzen" schlägt fehl. Nach § 100a Abs. 5 S. 1 Nr. 1 StPO ist nämlich (lediglich!)

> „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)**,".

Wie *Roggan* zutreffend bemerkt, handelt es sich hierbei um „*nicht weniger als die Manifestation, dass die Spionagesoftware technisch* ***mehr*** *können darf als verfassungsgerichtlich gestattet*"[146].

Unabhängig davon, dass die Vorgaben des § 100a Abs. 5 StPO an die technische Gestaltung der Trojanersoftware zur Durchführung einer Maßnahme nach § 100a Abs. 1 S. 2 und 3 StPO unzulänglich sind, fehlt eine Vorgabe dazu, wie die Einhaltung der gesetzlichen Anforderungen sichergestellt werden soll. Das betrifft auch die weiteren Vorgaben des § 100a Abs. 5 StPO.

Wie das *BVerfG* festgehalten hat, ist mit der Installation der Trojanersoftware

> „*die entscheidende Hürde genommen, um das System insgesamt auszuspähen. Die dadurch bedingte Gefährdung geht weit über die hinaus, die mit einer bloßen Überwachung der laufenden Telekommunikation verbunden ist.*"[147]

Dementsprechend ist es verfassungsrechtlich nicht hinnehmbar, wenn unklar bleibt, ob und wer die Einhaltung der „*technischen Vorgaben*" überwacht. Die Beurteilung wird dem die Maßnahme anordnenden Gericht schon tatsächlich nicht möglich sein. Sie kann

[146] *Roggan*, StV 2017, 821 (824) - Hervorhebung im Original.
[147] BVerfGE 120, 274 (308 - Rn. 188).

und darf aber nicht in das Belieben der mit der Durchführung der Maßnahmen betrauten Stellen überantwortet werden.

Es ist vielmehr eine unabhängige Stelle zu benennen, die die jeweils als Mittel der Wahl auserkorene Software überprüft. Diesbezüglich ist zwingend vorzusehen, dass der überprüfenden Stelle alle dazu erforderlichen Unterlagen (z.B. Programmdokumentation) – einschließlich des Quellcodes – vorgelegt werden, da nur so eine Nachprüfung sinnvoll möglich ist.[148] Da dies nicht geschehen ist, ist die Regelung auch aus diesem Grunde unverhältnismäßig und verfassungswidrig.

III. Unvereinbarkeit mit dem Fernmeldegeheimnis (Art. 10 Abs. 1 GG)

1. Online-Durchsuchung (§ 100b StPO)

Die durch § 100b Abs. 1 StPO gestattete Online-Durchsuchung stellt einen ungerechtfertigten Eingriff in Art. 10 Abs. 1 GG dar.

Eine Online-Durchsuchung impliziert stets auch eine Telekommunikationsüberwachung.

Da eine Online-Durchsuchung nur bei Bestehen einer Internetverbindung möglich ist und bei einer solchen permanent und in Echtzeit auch Inhalte und Umstände der Telekommunikation erhoben werden (wozu nach einem Nichtannahmebeschluß des *BVerfG* bereits das Aufrufen von Webseiten gehören soll[149]), ist ein Eingriff in den Schutzbereich gegeben. So wie es technisch nicht möglich ist, über eine Trojanersoftware ausschließlich sog. „*laufende Kommunikation*“ zu überwachen, ist es technisch ebenso wenig möglich lediglich die „nur“ in den Schutzbereich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme fallenden Informationen (also diejenigen, die nicht bereits durch Art. 10 GG erfasst werden[150]) zu erheben und zu überwachen.

---

[148] Vgl. BfDI, Bericht, S. 20.
[149] BVerfG, Beschluss vom 6.7.2016 – 2 BvR 1454/13 - Rn. 37 f. - allerdings im Widerspruch zu BVerfGE 141, 220 (312f. - Rn. 238) wo das „*Nach- oder Mitverfolgen der Bewegungen im Internet*“ als Beispiel für eine Online-Durchsuchung (in Abgrenzung zur TKÜ) genannt wird.
[150] Das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme füllt die „Schutzlücke“, die Art. 10 Abs. 1 GG offen lässt (vgl. BVerfGE 120, 274 (308 - Rn. 187)).

Dass eine Online-Durchsuchung (auch) einen Eingriff in das Fernmeldegeheimnis gestattet, hat der Gesetzgeber nicht berücksichtigt. Jedenfalls wurde Art. 10 Abs. 1 GG im Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens nicht als eingeschränktes Grundrecht genannt. Dort heißt es in Art. 17 lediglich: „*Durch Artikel 3 Nummer 8 wird das Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) eingeschränkt.*“ Der Art. 3 Nr. 8 enthält indes nur die Änderungen des § 100a StPO.

Die Regelung ist also wegen Verstoßes gegen das Zitiergebot (Art. 19 Abs. 1 S. 2 GG) verfassungswidrig.

2. Quellen-Telekommunikationsüberwachung (§ 100a Abs. 1 S. 2, 3 StPO)

Möchte man die Befugnis zur Quellen-Telekommunikationsüberwachung entgegen der hier vertretenen Auffassung nicht an Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, sondern „nur“ an Art. 10 Abs. 1 GG messen wollen, wäre diese dennoch als unverhältnismäßige Einschränkung anzusehen.

a. Ungeeignetheit

Die im Rahmen einer repressiven Quellen-Telekommunikationsüberwachung erhobenen Daten müssen technisch über eine Trojanersoftware digital erhoben und weitergeleitet werden. Da durch die Installation der Software das Zielsystem kompromittiert wird und eine Manipulation der Daten ohne weiteres ermöglicht, haben die ausgeleiteten Informationen keinen Beweiswert. Das Ziel einer Telekommunikationsüberwachung, nämlich die Gewinnung von (verwertbaren) Beweisen, kann nicht erreicht werden.

b. Fehlende Erforderlichkeit

Wie die Online-Durchsuchung auch ist insbesondere die „retrograde“ Erhebung von gespeicherten Inhalten „laufender Kommunikation“ nicht erforderlich. Es liegen mit der Beschlagnahme und Durchsuchung weniger einschneidende und mit Blick auf den Beweiswert besser geeignete Mittel zur Zielerreichung vor.

c. Unangemessenheit

Die Regelungen zur Quellen-Telekommunikationsüberwachung in § 100a StPO sind auch unangemessen.

aa) Begleitmaßnahmenschwelle

Dies betrifft insbesondere die Zulassung der mit den für die Quellen-Telekommunikationsüberwachung verbundenen Begleitmaßnahmen. Die hierfür angesetzte Schwelle entspricht nicht den verfassungsrechtlichen Maßstäben.

§ 100a Abs. 1 S. 2 StPO gestattet einen „Eingriff" in das vom Betroffenen „genutzte" informationstechnische System, *„wenn dies notwendig ist, um die Überwachung und Aufzeichnung [...] zu ermöglichen*".

Durch die Anforderung einer schlichten „Notwendigkeit" wird der mit einer Quellen-Telekommunikationsüberwachung einhergehende massive Eingriff in das informationstechnische Zielsystem nicht hinreichend verfassungsrechtlich eingehegt. Um der erhöhten Intensität der Maßnahme und der Ausstrahlungswirkung des Rechts auf Integrität und Vertraulichkeit informationstechnischer Systeme Genüge zu tun, wäre neben der schlichten „Notwendigkeit" eine obligatorische Prüfung der Angemessenheit im konkreten Fall explizit zu regeln gewesen. Der durch § 100a Abs. 2 StPO gestattete Eingriff in das informationstechnische System muss wenigstens (!) „in einem angemessenen Verhältnis zur Bedeutung der Sache" stehen, wie dies z.B. bei der einfachen Verkehrsdatenerhebung in § 100g Abs. 1 StPO niedergeschrieben wurde.

bb) Unzureichender technischer Schutz

Wie bei Maßnahmen einer Online-Durchsuchung auch, besteht keine ausreichende Gewähr dafür, dass das Zielsystem nicht über das für die Durchführung der Maßnahme „notwendige" Maß hinaus kompromittiert wird. Die in § 100a Abs. 5 StPO vorgesehenen Verpflichtungen sind für einen wirksamen Grundrechtsschutz nicht ausreichend, da nicht festgelegt wird, wer oder wie die eingesetzte Trojanersoftware auf die Einhaltung der dort vorgesehenen Vorgaben überwacht wird. Auch hier wäre eine Prüfung durch

eine unabhängige Stelle vorzusehen gewesen. Insbesondere hätte gesetzlich angeordnet werden müssen, dass der prüfenden Stelle alle hierfür erforderlichen Informationen (insbesondere der Quellcode der einzusetzenden Software) zur Verfügung gestellt werden.

cc) Unzureichender Schutz der IT-Sicherheit

Auch die Zulassung eines Eingriffs in informationstechnische Systeme zur Durchführung einer Quellen-Telekommunikationsüberwachung durch § 100a Abs. 1 S. 2 StPO ist verfassungswidrig. Es wird pauschal ein Eingriff in informationstechnische Systeme gestattet, ohne dass die technischen Wege der Infiltration begrenzt wären. Zur Vermeidung von Wiederholungen sei auf die Ausführungen unter II.1.d verwiesen.

Das fehlende Verbot der Ausnutzung und „Beschaffung" unbekannter Sicherheitslücken steht zu den Zwecken der Quellen-Telekommunikationsüberwachung in noch stärkerem Widerspruch als dies bei der Online-Durchsuchung der Fall ist. Eine Quellen-Telekommunikationsüberwachung ist bereits zur Bekämpfung von Straftaten möglich, die nicht einmal die Qualität der in § 100b Abs. 2 StPO genannten Anlasstaten erreichen müssen. Dass eine Gefährdung der IT-Sicherheit lebenswichtiger Einrichtungen zu Zwecken der Aufklärung z.B. eines Sportwettbetrugs (vgl. § 100a Abs. 2 Nr. 1 p StPO) in Missverhältnis steht, ist offensichtlich.

IV. Unvereinbarkeit mit dem Wohnungsgrundrecht (Art. 13 Abs. 1 GG)

Die Online-Durchsuchung stellt einen Eingriff in Art. 13 Abs. 1 GG dar, der verfassungsrechtlich nicht gerechtfertigt ist.

1. Eingriff

Das (auch passive) Beobachten und Abhören der Wohnung der Zielperson über sein informationstechnisches System, stellt einen Eingriff in Art. 13 Abs. 1 GG dar. In solchen Fällen verdrängt Art. 13 Abs. 1 GG das Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme.[151]

[151] *Papier*, in: Maunz/Dürig, GG, Art. 13 Rn. 145 m.w.N.

Technisch ist im Rahmen einer Online-Durchsuchung die heimliche Inbetriebnahme einer mit dem informationstechnischen System verbundenen Kamera und/oder eines mit diesem verbundenen Mikrofons möglich. Hierbei muss es sich nicht notwendigerweise um eine eingebaute Kamera handeln. So findet die Überwachung von „Haus und Hof" mittels sog. IP-Kameras immer weitere Verbreitung.[152] Diese Kameras sind über entsprechende Anwendungsprogramme permanent mit dem Smartphone des Nutzers verbunden und können von diesem gesteuert werden. Nach erfolgreicher Installation einer Trojanersoftware ist das Abgreifen der von dieser Kamera übertragenen Signale und das eigenständige Ansteuern der Kamera durch die Ermittlungsbehörden möglich.

Aus der Gesetzesbegründung folgt, dass die Online-Durchsuchung gerade dazu dienen soll, das „*gesamte Nutzungsverhalten einer Person*" zu überwachen.[153] Diese „Live-Rundumüberwachung" betrifft auch den durch Art. 13 Abs. 1 GG geschützten Wohnraum.

2. Fehlende verfassungsrechtliche Rechtfertigung

Bereits das alleinige Mithören des gesprochenen Worts in einer Wohnung über das informationstechnische System wäre deswegen verfassungswidrig, weil das § 100b StPO einführende Gesetz in Art. 17 das Wohnungsgrundrecht nicht als eingeschränkt bezeichnet (vgl. Wortlaut bereits oben) .[154]

Das im Rahmen der Online-Durchsuchung ermöglichte *optische* Überwachen des Wohnraums ist verfassungsrechtlich nicht zu rechtfertigen, da Art. 13 Abs. 3 GG derartige Eingriffe ausschließt.

---

[152] Vgl. z.B. *Ladenthin/Wiesmüller*, Durchblick: Überwachungskameras mit WLAN im Test, computerbild.de v. 17. 6. 2018, http://www.computerbild.de/artikel/cb-Tests-Vernetztes-Wohnen-Ueberwachung-Kameras-Test-WLAN-IP-15610039.html.
[153] BT-Drs. 18/12785, S. 54.
[154] *Roggan*, StV 2017, 821 (826).

Es wären aus Gründen der Bestimmbarkeit des Befugnisumfangs für die Rechtsanwender entgegenwirkende Kautelen ausdrücklich vorzusehen gewesen.[155]

Auch die absolute Unverwertbarkeit von Daten, die unter Verletzung von Art. 13 Abs. 1 GG erlangt wurden, hätte gesetzgeberisch klargestellt werden müssen.[156]

Da dies nicht geschehen ist, ist § 100b StPO mit dem Wohnungsgrundrecht unvereinbar.

V. Unvereinbarkeit mit der Garantie effektiven Rechtsschutzes (Art. 19 Abs. 4 GG)

Die hier gegenständlichen Regelungen – insbesondere die Absätze 5 und 6 des § 100a StPO – sind mit der Garantie effektiven Rechtsschutzes (Art. 19 Abs. 4 GG) unvereinbar. Sowohl die Online-Durchsuchung als auch die Quellen-Telekommunikationsüberwachung sind Ermittlungsmaßnahmen die letztlich der Beweiserhebung im Strafverfahren dienen.

Ob diese Beweiserhebung rechtskonform durchgeführt wird, ist de facto durch den Betroffenen nicht nachprüfbar. Im Gegenteil: Im Rahmen der Infiltration des informationstechnischen Systems mit einer nicht näher von einer unabhängigen Stelle geprüften Trojanersoftware wird dieses System insgesamt kompromittiert.

Es besteht ab dem Zeitpunkt der Infiltration die erhöhte Gefahr einer Manipulation durch Dritte. Die in den §§ 100a Abs. 5 und Abs. 6 StPO enthaltenen Vorgaben zur technischen Gestaltung der Software und zur Protokollierung des Einsatzes sind für den Betroffenen de facto wertlos.

Eine Überprüfung der Einhaltung der gesetzeskonformen Ausgestaltung der Software durch eine unabhängige Stelle ist nicht explizit gesetzlich vorgesehen und kann auch auf Grund der fehlenden Bekanntgabe des Quellcodes praktisch nicht erfolgen. Es ist gerichtlich nicht überprüfbar, ob zum Beweis vorgelegte Kopien von auf dem System des

[155] *Sinn*, Stellungnahme, S. 10; *Roggan*, StV 2017, 821 (826).
[156] *Roggan*, StV 2017, 821 (826) der zudem darauf hinweist, dass die Erkenntnisse auch nicht als Spurenansatz in Betracht kommen.

Betroffenen erhoben Daten tatsächlich von diesem stammen, ob diese gegebenenfalls verändert wurden sowie wer und wann tatsächlich auf das System Zugriff hatte. Damit widersprechen die gegenständlichen Regelungen grundlegenden Anforderungen[157] an die Transparenz und Nachvollziehbarkeit heimlicher Maßnahmen.

VI. Fazit

Nach alledem sind die § 100a Abs. 1 S. 2 und 3, Abs. 3 bis 6, § 100b sowie § 100d Abs. 1 bis 3 und 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.) wegen Verstoßes gegen die Menschenwürde (Art. 1 Abs. 1 GG), jedenfalls aber wegen Verstoßes gegen das Recht auf Integrität und Vertraulichkeit informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), das Fernmeldegeheimnis (Art. 10 Abs. 1 GG), das Wohnungsgrundrecht (Art. 13 Abs. 1 GG) sowie die Garantie effektiven Rechtsschutzes (Art. 19 Abs. 4 GG) mit dem Grundgesetz für unvereinbar und nichtig zu erklären.

Prof. Dr. Frank Braun Prof. Dr. Jan Roggenkamp

[157] Hierzu ausführlich BVerfGE 141, 220 (282 f.).