DeutscherAnwaltVerein

Stellungnahme

des Deutschen Anwaltvereins durch den Ausschuss Verfassungsrecht, den Ausschuss Gefahrenabwehrrecht und den Ausschuss Strafrecht

zur Verfassungsbeschwerde
1 BvR 180-23
(Quellen-Telekommunikationsüberwachung – § 100a Abs. 1 ff. StPO)

Stellungnahme Nr.: 59/2023 Berlin, im August 2023

Mitglieder des Ausschusses Verfassungsrecht

- RA Prof. Dr. Christian Winterhoff, Hamburg (Vorsitzender)
- RAin Dr. Antje Wittmann, Münster (stellvertretende Vorsitzende)
- RAin Dr. Maria Marquard, Stuttgart (Berichterstatterin)
- RA Dr. Sebastian Nellesen, Bonn
- RA Stefan von Raumer, Berlin
- RAin Dr. Roya Sangi, Berlin (nicht an der Stellungnahme mitgewirkt)
- RAin Dr. Ricarda Schelzke, Frankfurt a. M.
- RA Dr. Sebastian Schmuck, Leipzig
- RA Dr. Michael Schramm, Düsseldorf (Berichterstatter)
- RAin Dr. Inga Schwertner, Köln (Berichterstatterin)

Zuständig in der DAV-Geschäftsstelle

- RA Max Gröning, Geschäftsführer, Berlin
- RAin Katharina Schmidt-Matthäus, Referentin, Berlin

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

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Mitglieder des Ausschusses Gefahrenabwehrrecht

- RAin Lea Voigt, Bremen (Vorsitzende)
- RA Wilhelm Achelpöhler, Münster
- RA Dr. David Albrecht, Berlin
- RA Dr. Eren Basar, Düsseldorf
- RAin Prof. Dr. Annika Dießner, Berlin (ständiges Gastmitglied im Ausschuss)
- RA Dr. Nikolas Gazeas, LL.M., Köln (nicht an der Stellungnahme mitgewirkt)
- RA Dr. Andreas Grözinger, Köln (Berichterstatter)
- RA Dr. Mayeul Hieramente, Hamburg (Berichterstatter)
- RA Dr. Saleh Ihwas, Frankfurt am Main
- RA Prof. Dr. Stefan König, Berlin
- RAin Dr. Regina Michalke, Frankfurt
- RAin Dr. Vivien Veit, Mönchengladbach
- RA Prof. Dr. Mark A. Zöller, München (ständiges Gastmitglied im Ausschuss)

Zuständig in der DAV-Geschäftsstelle

- RA Max Gröning, Geschäftsführer, Berlin
- RAin Katharina Schmidt-Matthäus, Referentin, Berlin

Mitglieder des Ausschusses Strafrecht

- RA Dr. Rainer Spatscheck, München (Vorsitzender)
- RA Stefan Conen, Berlin
- RAin Dr. Gina Greeve, Frankfurt a.M.
- RA Kai Kempgens, Berlin (Berichterstatter)
- RA Prof. Dr. Stefan Kirsch, Frankfurt a.M.
- RAin Dr. Jenny Lederer, Essen
- RA Prof. Dr. Bernd Müssig, Bonn
- RA Prof. Dr. Ali B. Norouzi, Berlin (Stellvertretender Vorsitzender)
- RAin Dr. Anna Oehmichen, Berlin
- RAin Gül Pinar, Hamburg
- RA Martin Rubbert, Berlin
- RAin Dr. Heide Sandkuhl, Potsdam

Zuständig in der DAV-Geschäftsstelle

- RAin Tanja Brexl, Geschäftsführerin, Berlin
- RAin Evelyn Westhoff, Referentin, Berlin

Verteiler

- Bundesverfassungsgericht
- Ausschuss Recht des Deutschen Bundestages
- Ausschuss für Inneres und Heimat des Deutschen Bundestages
- Vors. des Rechtsausschusses des Deutschen Bundestages
- Vors. des Innenausschusses des Deutschen Bundestages
- Digitalausschuss des Deutschen Bundestages
- Fraktionen des Deutschen Bundestages
- Arbeitsgruppe Inneres der im Deutschen Bundestag vertretenen Parteien
- Bundesministerium der Justiz
- Bundesministerium des Innern und für Heimat
- Justizministerien und Senatsverwaltungen der Bundesländer
- Innenministerien und Senatsverwaltungen der Bundesländer
- Bundesgerichtshof
- Bundesanwaltschaft
- Bundesrechtsanwaltskammer
- Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
- Landesdatenschutzbeauftragte
- Deutscher Richterbund
- Bundesverband der Freien Berufe
- Deutsches Institut für Menschenrechte
- Gesellschaft für Freiheitsrechte
- Deutscher Strafverteidiger e. V.
- Regionale Strafverteidigervereinigungen
- Organisationsbüro der Strafverteidigervereinigungen und -initiativen
- Bund Deutscher Kriminalbeamter
- Arbeitskreise Recht der im Bundestag vertretenen Parteien
- Prof. Dr. Jürgen Wolter, Universität Mannheim
- ver.di, Bereich Recht und Rechtspolitik
- Deutscher Juristentag (Präsident und Generalsekretär)

- Mitglieder des Vorstandes des Deutschen Anwaltvereins
- Vorsitzenden der Landesverbände des Deutschen Anwaltvereins
- Vorsitzenden der Gesetzgebungsausschüsse des Deutschen Anwaltvereins
- Ausschuss Verfassungsrecht des Deutschen Anwaltvereins
- Ausschuss Gefahrenabwehrrecht des Deutschen Anwaltvereins
- Strafrechtsausschuss des Deutschen Anwaltvereins
- Geschäftsführender Ausschuss der Arbeitsgemeinschaft Strafrecht des Deutschen Anwaltvereins
- Strafrechtsausschuss der Bundesrechtsanwaltskammer
- Vors. des Strafrechtsausschusses des KAV, BAV
- Forum Junge Anwaltschaft

<u>Presse:</u>

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

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV versammelt mehr als 60.000 Rechtsanwältinnen und Rechtsanwälte sowie Anwaltsnotarinnen und Anwaltsnotare, die in 253 lokalen Anwaltvereinen im In- und Ausland organisiert sind. Er vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene. Der DAV ist im Lobbyregister für die Interessenvertretung gegenüber dem Deutschen Bundestag und der Bundesregierung zur Registernummer R000952 eingetragen.

Inhaltsverzeichnis

1. Teil: Zusammenfassung 9

2. Teil: Inhalt der Regelungen 11

A. § 100a Abs. 1 S. 2, 3, Abs. 3, 5-6 StPO – Quellen-Telekommunikations-überwachung 11

B. § 100b StPO – Online-Durchsuchung 12

C. § 100d Abs. 1 bis 4 StPO – Kernbereichsschutz 13

D. § 100d Abs. 5 StPO – Schutz zeugnisverweigerungsberechtigter Personen 13

I. Berufsgeheimnisträger (§ 53 Abs. 1 StPO) 14

II. Berufshelfer (§ 53a StPO) und Angehörige (§ 52 StPO) 14

3. Teil: Begründetheit/Unbegründetheit der Verfassungsbeschwerde 16

A. § 100a Abs. 1 S. 2, 3, Abs. 3, 5-6 StPO – Quellen-Telekommunikationsüberwachung 16

I. § 100a Abs. 1 Satz 2 StPO (Eingriff in Art. 10 Abs. 1 GG) 16

1. Wortlaut und Auslegung 16

2. Verfassungsrechtliche Vorgaben 17

a) Schutzbereich des Art. 10 Abs. 1 GG eröffnet 17

b) Eingriff und verfassungsrechtliche Rechtfertigung 19

aa) Eingriffstiefe 19

(1) „Surfen im Internet“ **20**

(2) Cloud-Computing **21**

bb) Verfassungsrechtliche Rechtfertigung 23

c) Technische Möglichkeit und technische Sicherung 26

d) „Nachrichtenmittler“ / „Nichtbeschuldigte“ 27

e) Richtervorbehalt 28

f) Fehlende zeitliche Obergrenze 29
g) Schutzpflichten für die IT-Sicherheit (Ausnutzung und Aufrechterhaltung von technischen Lücken) 30
h) Relevanz in der Praxis 31
II. § 100a Abs. 1 Satz 3 StPO 32
1. Wortlaut und Auslegung 32
2. Verfassungsrechtliche Anforderungen 33
a) Schutzbereich des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG und Eingriff 33
b) Verfassungsrechtliche Rechtfertigung 33
c) Weiterer Vortrag 36
B. § 100b StPO – Online-Durchsuchung 36
I. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG: Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme („IT-Grundrecht“) 36
1. Schutzbereich 36
2. Eingriff 37
a) Bedeutung von Daten auf IT-Systemen 38
b) Zugriff auf Datenmassen 39
c) Live-Überwachung des Nutzerverhaltens 39
d) Heimlichkeit der Maßnahme 40
e) Notwendigkeit ungeschlossener Sicherheitslücken 40
f) Unzureichende Regelungen zum Umgang mit Daten(-massen) 41
g) Streubreite 42
3. Keine Rechtfertigung 42
a) Maßstäbe des BverfG 42
b) Verletzung des IT-Grundrechts durch § 100b StPO 44
aa) Geeignetheit 44
bb) Erforderlichkeit 44
cc) Unvereinbarkeit mit Verhältnismäßigkeitsmaßstab des BVerfG 44

dd) Unzulässige Übertragung des Straftatenkatalogs aus § 100c Abs. 2 StPO a.F. 45
ee) Unzureichende Subsidiaritätsklausel 45
ff) Fehlendes Erfordernis der Erfolgsaussicht 46
gg) Fehlende Maßnahmen zum Schutz vor Vollüberwachung 46
hh) Fehlende Kontrolle durch eine unabhängige Stelle 46
ii) Fehlende Kontrolle der eingesetzten Remote Forensic Software 47
jj) Fehlende Regelungen zur Vorbeugung der Erstellung eines vollständigen Persönlichkeitsprofils 47
II. Art. 13 Abs. 1 GG: Unverletzlichkeit der Wohnung 47
C. § 100d Abs. 1 bis 4 StPO – Kernbereichsschutz 49
I. Allgemeine Maßstäbe des Bundesverfassungsgerichts 49
II. Entscheidung zu § 20k Abs. 7 BKAG 50
III. Kein ausreichender Kernbereichsschutz auf Erhebungsebene bei § 100b StPO 52
IV. Kein ausreichender Kernbereichsschutz auf Auswertungsebene bei § 100b StPO 54
V. Bindungswirkung der gerichtlichen Entscheidung bei § 100b StPO 55
VI. Kernbereichsschutz bei Quellen-TKÜ 56
D. § 100d Abs. 5 StPO – Schutz zeugnisverweigerungsberechtigter Personen 58
I. Uneinheitliche Regelung zum Schutz von zeugnisverweigerungsberechtigten Personen 58
II. Keine Überschreitung des verfassungsrechtlichen Gestaltungsspielraums 59
1. Kein verfassungsrechtliches Gebot des absoluten Schutzes von Zeugnisverweigerungsberechtigten 60

2. Ausgestaltung des Schutzes von Berufshelfern ist verfassungsgemäß 61
3. Strenge Anforderungen an die Verwertung von Erkenntnissen aus der Kommunikation mit Berufshelfern 62
4. Auch im Übrigen bestehen keine verfassungsrechtlichen Bedenken 63

1. Teil: Zusammenfassung

Die Beschwerdeführer wenden sich gegen die gesetzliche Ausgestaltung der Quellen-Telekommunikationsüberwachung in **§ 100a Abs. 1 S. 2, 3 StPO**. Die Verfassungskonformität der Regelungen hängt maßgeblich von der Auslegung der Vorschriften und der Reichweite des strafprozessualen Telekommunikationsbegriffs ab. Jedenfalls bei einem weiten Verständnis der Norm, insbesondere bei Einbeziehung der Überwachung des Surfverhaltens und des Cloud-Computings, ist die Verfassungskonformität der Regelungen zweifelhaft. Zwar steht dem Gesetzgeber ein gewisser Beurteilungsspielraum zu. Will dieser indes weitgehende Überwachungen des Datentransfers zwischen Endgeräten und Cloud zulassen und die gesamte Nutzung des Internets überwachen, so hat er die Verhältnismäßigkeit im engeren Sinne zu wahren. Selbst wenn eine derartige Befugnis nicht von der Vorschrift erfasst sein sollte, dürfte es verfassungsrechtlich geboten sein, Verfahrensvorschriften für eine Datenselektion vorzusehen.

Die Beschwerdeführer wenden sich weiter gegen die Regelungen zur Onlinedurchsuchung gem. **§ 100b StPO**. Die Verfassungsbeschwerde ist aus Sicht des Deutschen Anwaltsvereins begründet. Nach hiesigem Standpunkt sind hinsichtlich der Eingriffstiefe insbesondere die seit der im Jahr 2008 ergangenen Grundsatzentscheidung massiv gewachsene Datendichte, die rasante Verbreitung und Vernetzung von Endgeräten sowie die deutliche Zunahme der Bedeutung digitaler Daten für das Individuum zu berücksichtigen. Zudem fehlen jedwede Regelungen zur Auswertung der gemäß § 100b StPO erhobenen Daten. Da die nach ihrer Konzeption heimlich stattfindenden und eine umfangreiche, breit streuende Live-Überwachung und zeitlich unbegrenzte Datenbeschlagnahme ermöglichenden Onlinedurchsuchungen vor diesem Hintergrund in ihrer Wirkung deutlich über die Reichweite von Maßnahmen nach § 100c StPO hinausgehen, erscheinen weder der Straftatenkatalog des § 100c Abs. 2 StPO a.F. angemessen, noch gewährleistet die konkrete Ausgestaltung der Umsetzungsregeln (insbesondere auch hinsichtlich des Kernbereichsschutzes in Erhebungs- und Auswertungsphase) mangels einer ausreichend konkreten Schutzkonzeption einen für die Wahrung der Verhältnismäßigkeit ausreichenden Grundrechtsschutz.

Die Beschwerdeführer rügen einen unzureichenden Kernbereichsschutz. Zutreffend ist, dass der Kernbereichsschutz bei der Online-Durchsuchung unzureichend ausgestaltet ist. In **§ 100d Abs. 3 StPO** fehlt es an einer Regelung zum Abbruch bzw. Unterbrechung der Online-Durchsuchung. Insoweit genügt die Regelung den verfassungsrechtlichen Maßstäben zum Schutz des Kernbereichs privater Lebensgestaltung auf Erhebungsebene nicht. Auf Auswertungsebene wird § 100d Abs. 3 Satz 2 StPO den verfassungsrechtlichen Anforderungen ebenfalls nicht gerecht. Es fehlt an einer Sichtung durch eine unabhängige Stelle, da die erste Sichtung den Ermittlungsbehörden (selbst) vorbehalten bleibt. Problematisch ist auch die Bindungswirkung der gerichtlichen Entscheidung nach § 100d Abs. 3 Satz 3 StPO. Die Bindungswirkung gilt nach dem Wortlaut der Norm auch für das Haupt- und Rechtsmittelverfahren. Dies ist mit Blick auf den Menschenwürdegehalt des Kernbereichsschutzes verfassungsrechtlich nicht zu rechtfertigen. § 100d Abs. 3 Satz 3 StPO ist daher so zu fassen, dass die Entscheidung des Gerichts über die Verwertbarkeit für das weitere Verfahren nur bindend ist, soweit die Verwertbarkeit abgelehnt wurde.

Die Beschwerdeführer wenden sich ferner gegen **§ 100d Abs. 5 StPO**. Die in der Norm enthaltene Differenzierung zwischen dem absoluten Schutz von Berufsgeheimnisträgern durch ein absolutes Beweis*erhebung*sverbot und dem Schutz anderer zeugnisverweigerungsberechtigter Personen im Sinne der §§ 52, 53a StPO durch ein nur relatives Beweis*verwertung*sverbot sei nicht gerechtfertigt.

Die Regelung schafft im Vergleich zu anderen Normen der StPO in der Tat ein uneinheitliches Regelungsgefüge zum Schutz zeugnisverweigerungsberechtigter Personen und relativiert damit letztlich den absoluten Schutz der Berufsgeheimnisträger selbst. Mit der getroffenen Regelung überschreitet der Gesetzgeber indes nicht die verfassungsrechtlichen Grenzen. Dem Gesetzgeber steht bei der Ausgestaltung des Schutzes zeugnisverweigerungsberechtigter Personen ein weiter Gestaltungsspielraum zu. Dabei ist er verfassungsrechtlich verpflichtet, den Kernbereich privater Lebensgestaltung zu schützen, der in engem Zusammenhang mit dem Schutz der Kommunikation mit bestimmten Berufsgruppen (§§ 53, 53a StPO) und nahen Angehörigen (§ 52 StPO) steht. Er ist darüber hinaus aber nicht verpflichtet, alle

Zeugnisverweigerungsberechtigten im Rahmen von Ermittlungsmaßnahmen unter einen absoluten Schutz zu stellen.

2. Teil: Inhalt der Regelungen

A. § 100a Abs. 1 S. 2, 3, Abs. 3, 5-6 StPO – Quellen-Telekommunikations-überwachung

§ 100a Abs. 1 S. 2, 3 StPO regelt die sog. Quellen-Telekommunikationsüberwachung. Danach darf auch ohne Wissen des Betroffenen die laufende Telekommunikation überwacht werden, wenn (1.) bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine im Folgeabsatz 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. § 100a Abs. 2 StPO regelt einen abschließenden Katalog an Straftaten, die der Gesetzgeber als schwer einstuft. Die Vorschrift erlaubt die Sicherung von Daten und eine „Live-Überwachung“ der Telekommunikation. In der Praxis ist umstritten, wie der Telekommunikationsbegriff des § 100a StPO zu interpretieren ist.

Zur Umgehung etwaiger Verschlüsselung erlaubt § 100a Abs. 1 Satz 2 StPO eine Infiltration des Endgeräts zur Ermöglichung der der Überwachung und Aufzeichnung der laufenden Telekommunikation (vgl. § 100a Abs. 5 Nr. 1 a) StPO) in unverschlüsselter Form. Die Regelung soll damit den Entwicklungen der modernen Technik im Bereich der Transportverschlüsselung Rechnung tragen. Darüber hinaus erlaubt § 100a Abs. 1 Satz 3 StPO auch den Zugriff auf gespeicherte Inhalts- und Verkehrsdaten, wenn diese auch während des laufenden Übertragungsvorgags im öffentlichen Telekommunikationsnetzt in verschlüsselter Form hätten überwacht und aufgezeichnet werden können. Dabei ist sicherzustellen, dass nur Inhalte und Umstände der Kommunikation nach Anordnung überwacht und aufgezeichnet werden (vgl. § 100a Abs. 5 Nr. 1 b) StPO). § 100a Abs. 5 StPO regelt die notwendigen technischen Sicherungen. § 100a Abs. 6 StPO normiert Protokollierungspflichten. .

B. § 100b StPO – Online-Durchsuchung

§ 100b StPO regelt die Online-Durchsuchung. Danach darf auch ohne Wissen des Betroffenen 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 im Folgeabsatz 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.

§ 100b Abs. 2 StPO regelt einen Katalog besonders schwerer Straftaten i.S.d. § 100b Abs. 1 Nr. 1 StPO, der inhaltsgleich mit dem Straftatenkatalog für die Wohnraumüberwachung in § 100c Abs. 2 StPO a.F. ist. Die Vorschrift erlaubt die „Erhebung von Daten“, weshalb § 100b Abs. 1 StPO nicht nur einen punktuellen Eingriff auf das IT-System des Betroffenen, sondern ausweislich der Vorschrift des § 100e Abs. 2 S. 4 bis 6 StPO und der Gesetzesbegründung auch einen dauerhaften Zugriff und somit auch eine umfassende Überwachung des Nutzerverhaltens zulässt. Auf Grundlage von § 100b Abs. 1 StPO kann somit nicht nur der gesamte Datenbestand eines IT-Systems heimlich „beschlagnahmt“ werden. § 100b Abs. 1 StPO erlaubt darüber hinaus eine fortdauernde „Live-Überwachung“ des Systems. In der Praxis bedeutet dies, dass die Strafverfolgungsbehörden dem Beschuldigten „beim Denken“ zuschauen können, etwa wenn dieser beispielsweise eine Nachricht entwirft, diese dann aber löscht, anstatt sie zu versenden, was der Überwachung eines Selbstgesprächs gleichkommt.

Auch wenn nach der herrschenden Auffassung in der Literatur ein selbstständiges Aktivieren von Sensoren (z.B. Kamera oder Mikrofon) durch die Strafverfolgungsbehörden (angesichts der gesetzlichen Formulierung „*daraus*“) nicht umfasst sein soll, soll eine Erhebung sensorgenerierter Daten zulässig sein, wenn der Nutzer die Sensoren selbsttätig aktiviert bzw. diese systemseitig ohnehin aktiv sind. Gemäß § 100b StPO sollen demnach auch aktuell systemseitig vorhandene Sensordaten, wie z.B. aktuelle Videoaufzeichnungen einer Webcam, erhoben werden dürfen (*Rückert*, in: MüKo-StPO, 2. Aufl. 2023, § 100b, Rn. 45 f. m.w.N.).

C. § 100d Abs. 1 bis 4 StPO – Kernbereichsschutz

§ 100d Abs. 1 bis 4 StPO enthält Regelungen zum Kernbereichsschutz. Nach § 100d Abs. 1 StPO ist eine Maßnahme unzulässig, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch eine Maßnahme nach den §§ 100a bis 100c StPO allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden. Nach § 100d Abs. 2 StPO dürfen Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach den §§ 100a bis 100c StPO erlangt wurden, nicht verwertet werden. Aufzeichnungen über solche Erkenntnisse sind unverzüglich zu löschen (Satz 2). Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren (Satz 3).
§ 100d Abs. 3 StPO enthält eine Spezialregelung zum Kernbereichsschutz bei Online-Durchsuchungen. Die Regelung lautet:

> *„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.“*

§ 100d Abs. 1 bis 4 StPO fasst die bislang in den Einzelermächtigungsgrundlagen gesondert geregelten Vorschriften über den Kernbereichsschutz zusammen. Nach der Gesetzesbegründung wurde die Vorschrift nach der Schwere des Eingriffs systematisiert und auf die Maßnahmen der Online-Durchsuchung erstreckt (BT-Drs. 18/12785, S. 55).

D. § 100d Abs. 5 StPO – Schutz zeugnisverweigerungsberechtigter Personen

§ 100d Abs. 5 StPO übernimmt die zuvor in § 100c Abs. 6 StPO aF enthaltene Regelung zum Schutz zeugnisverweigerungsberechtigter Personen bei der akustischen Wohnraumüberwachung, insbesondere von Berufsgeheimnisträgern.[1] Sie gilt nunmehr

[1] S. insoweit die Regelung des § 100c Abs. 6 aF, die mit *Gesetz zur Umsetzung des Urteils des Bundesverfassungsgerichts vom 3. März 2004* vom 24. Juni 2005 (BGBl. I, S. 1841 ff.) eingeführt und bis Inkrafttreten des Gesetzes vom 17. August 2017 in Kraft

auch für Maßnahmen der Online-Durchsuchung (§ 100b StPO). § 100d Abs. 5 StPO geht als *lex specialis* dem allgemeinen Schutz zeugnisverweigerungsberechtigter Berufsgeheimnisträger vor strafprozessualen Ermittlungsmaßnahmen nach § 160a StPO vor.

Die Vorschrift differenziert hinsichtlich der Maßnahmenbeschränkungen gegenüber Zeugnisverweigerungsberechtigten zwischen Berufsgeheimnisträgern (§ 53 StPO) einerseits und Angehörigen (§ 52 StPO) und Berufshelfern (§ 53a StPO) andererseits.

I. Berufsgeheimnisträger (§ 53 Abs. 1 StPO)

Nach § 100d Abs. 5 StPO sind Maßnahmen der Wohnraumüberwachung und der Online-Durchsuchung *"in den Fällen des § 53"* unzulässig. Die Vorschrift des § 53 StPO regelt das Zeugnisverweigerungsrecht sogenannter Berufsgeheimnisträger, d.h. bestimmter Berufsgruppen, denen im Rahmen ihrer Tätigkeit vertrauliche Informationen offenbart werden.

Für das Berufsgeheimnis unterfallende Erkenntnisse gilt nach § 100d Abs. 5 S. 1 StPO ein Beweiserhebungsverbot, das bereits bei der Anordnung der Maßnahme zu beachten ist.[2] Ergibt sich erst später, dass ein Fall des § 53 StPO vorliegt, folgt nach § 100d Abs. 5 S. 1 Hs. 2 StPO ein absolutes Beweisverwertungsverbot nach § 100d Abs. 2 StPO entsprechend. Aufzeichnungen sind unverzüglich zu löschen, was zu dokumentieren ist.

Sind die zur Verweigerung des Zeugnisses Berechtigten in die Straftat verstrickt, so entfällt gem. § 100d Abs. 5 S. 3 i.V.m § 160 a Abs. 4 StPO das Überwachungs- und Verwertungsverbot der S. 1 und 2.

II. Berufshelfer (§ 53a StPO) und Angehörige (§ 52 StPO)

Berufshelfer (§ 53a StPO) und Angehörige (§ 52 StPO) sind nicht durch ein absolutes Beweiserhebungsverbot geschützt. Für die Kommunikation mit diesen Personen gilt

---

war:*"In den Fällen des § 53 Abs. 1 ist eine Maßnahme nach § 100 c Abs. 1 Nr. 3 unzulässig. Dies gilt auch; wenn zu erwarten ist, daß sämtliche aus der Maßnahme zu gewinnenden Erkenntnisse einem Verwertungsverbot unterliegen. In den Fällen der §§ 52 und 53 a dürfen aus einer Maßnahme nach § 100 c Abs. 1 Nr. 3 gewonnene Erkenntnisse nur verwertet werden, wenn dies unter Berücksichtigung der Bedeutung des zugrundeliegenden Vertrauensverhältnisses nicht außer Verhältnis zum Interesse an der Erforschung des Sachverhaltes oder der Ermittlung des Aufenthaltsortes des Täters steht.".*

[2] Handkommentar Gesamtes Strafrecht /*Arthur-Hartmann*, 5. Aufl. 2022, StPO § 100d, Rn. 19.

insoweit nur das Erhebungsverbot des Abs. 1 bzw. speziell für die akustische Wohnraumüberwachung das Erhebungsverbot des Abs. 4. Nach § 100d Abs. 5 StPO dürfen Erkenntnisse aus Maßnahmen nach § 100b und 100c StPO nur verwertet werden, wenn dies unter Berücksichtigung der Bedeutung des zugrunde liegenden Vertrauensverhältnisses nicht außer Verhältnis zu den legitimen Zwecken der Maßnahme steht (relatives Beweisverwertungsverbot).[3] Die Verstrickungsregelung des § 100d Abs. 5 S. 3 i.V.m § 160a Abs. 4 StPO gilt für Berufshelfer und Angehörige gleichermaßen.

[3] Vgl. etwa Handkommentar Gesamtes Strafrecht /*Arthur-Hartmann*, 5. Aufl. 2022, StPO § 100d, Rn. 18.

3. Teil: Begründetheit/Unbegründetheit der Verfassungsbeschwerde

Es folgen Ausführungen zur Begründetheit/Unbegründetheit der Verfassungsbeschwerde. Dabei soll zunächst die Quellen-Telekommunikationsüberwachung beleuchtet werden (dazu unter A.). Der danach folgende Abschnitt befasst sich mit der Online-Durchsuchung (dazu unter B.). Es folgen Ausführungen zum Kernbereichsschutz (dazu unter C.) und zum Schutz zeugnisverweigerungsberechtigter Personen (dazu unter D.).

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

I. § 100a Abs. 1 Satz 2 StPO (Eingriff in Art. 10 Abs. 1 GG)

Die Beschwerdeführer rügen, dass die Befugnis zur Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) sowohl in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs.1 GG i.V.m. Art. 1 Abs.1 GG) als auch in das Fernmeldegeheimnis in nicht zu rechtfertigender Weise eingreife. Die Regelung laufe aufgrund des derzeitigen technischen Standes leer und gewährleiste angesichts der Infiltration des informationstechnischen Systems keinen hinreichenden technischen Schutz und Schutz der IT-Sicherheit.

1. Wortlaut und Auslegung

Gem. § 100a Abs. 1 Satz 2 StPO darf die Überwachung und Aufzeichnung der Telekommunikation i.S.d. § 100a Abs. 1 Satz 1 StPO 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. Dabei ist nach § 100a Abs. 5 Satz 1 Nr. 1 lit. a StPO technisch sicherzustellen, dass ausschließlich die laufende Telekommunikation überwacht und aufgezeichnet werden kann. Weiter sieht § 100a Abs. 5 Satz 2 und 3 StPO vor, dass das eingesetzte Mittel nach dem Stand der Technik gegen unbefugte Nutzung sowie kopierte Daten nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen sind. Protokollierungspflichten sind in § 100a Abs. 6 StPO geregelt.

Anders als die Beschwerdeführer vortragen, ergibt sich aus dem Wortlaut und der Systematik des § 100a Abs. 5 StPO, dass es sich bei den durch § 100a Abs. 1 Satz 2 und § 100a Abs. 1 Satz 3 StPO eröffneten Eingriffsbefugnissen nicht um eine einheitliche Maßnahme handelt (VB, S. 76 f.). Das bestätigt die Gesetzesbegründung (BT-Drs. 18/12785, S. 53 und 51), nach der der neu gestaltete § 100a Abs. 5 StPO die an unterschiedlichen Stellen geregelten technischen Voraussetzungen der Durchführung einer Quellen-Telekommunikationsüberwachung in einer Vorschrift zusammen fasst und diese an die differenziert ausgestalteten Ermächtigungsgrundlagen anpasst.

2. Verfassungsrechtliche Vorgaben

a) Schutzbereich des Art. 10 Abs. 1 GG eröffnet

§ 100a Abs. 1 Satz 2 StPO begründet als sog. Quellen-TKÜ grundsätzlich ausschließlich einen Eingriff in Art. 10 Abs. 1 GG. Zwar ist es technisch zwingend erforderlich, dass das informationstechnische System zum Zwecke der Telekommunikationsüberwachung infiltriert wird und damit die Hürde genommen ist, das System insgesamt auszuspähen. Das begründet eine über die bloße Überwachung der laufenden Telekommunikation hinausgehende Gefährdung.

Allerdings ist auch in diesen Fällen Art. 10 Abs. 1 GG 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 (BVerfGE 120, 274 [309]). § 100a Abs. 1 Satz 2 StPO ermöglicht ausschließlich Überwachungen, die sich auf den laufenden Telekommunikationsvorgang beschränken. Zugriff auf weitere inhaltliche Informationen des informationstechnischen Systems gestattet die Vorschrift nicht, sodass sie grundsätzlich nicht am Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu messen ist.

Nach dem Willen des Gesetzgebers ist mit § 100a Abs. 1 Satz 2 StPO kein Zugriff auf Entwürfe von Nachrichten verbunden (BT-Drs. 18/12785, S. 51; vgl. dazu auch Graf, in: BeckOK StPO mit RiStBV und MiStra, 47. Edition, Stand: 01.01.2023, § 100a Rn. 127).

Diese Begrenzung wird jedoch dann faktisch ausgehebelt, wenn man – mit der nachfolgend unter b) aa) (2) dargestellten Literaturansicht – die Kommunikation zwischen Endgerät und „Cloud“ selbst als Kommunikation versteht. Dies soll an einem einfachen Beispiel illustriert werden: Wenn ein Nutzer eines gängigen E-Mail-Programms (z.B. Outlook, Mail) auf dem Smartphone einen E-Mail-Entwurf fertigt, erfolgt eine automatische Synchronisation, so dass der gleiche Nutzer auf dem Laptop diesen Entwurf sehen und bearbeiten kann. Es erfolgt ein automatisierter Datenaustausch zwischen Smartphone und Cloud-Laptop. Sofern Staatsanwaltschaften und Fachgerichte den automatisierten Datenaustausch mit der Cloud als Telekommunikation einstufen, ist die für die (soziale) Telekommunikation geforderte Differenzierung zwischen dem (nur dem Nutzer bekannten) Erstellen des Entwurfs und der (Nutzer und Empfänger) bekannten Telekommunikation obsolet.

Anders als bei der „klassischen“ Kommunikation stellt die Überwachung des automatisierten Datenaustauschs zwischen Endgerät und Cloud einen Eingriff in das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme dar. So betrifft die Erhebung zwar nicht Daten, die auf der Festplatte des Endgeräts gespeichert sind. Werden diese Daten indes automatisiert mit der Cloud synchronisiert, erlaubt eine Quellen-TKÜ faktisch den Zugriff auf die Daten, deren Vertraulichkeit gerade besonders geschützt werden soll. Im BKAG-Urteil hatte der Erste Senat des Bundesverfassungsgerichts § 20k BKAG a.F. zu überprüfen, der zu einem „*Zugriff auf informationstechnische Systeme [ermächtigt] und erlaubt die geheime Durchführung von Online-Durchsuchungen, mit denen private, von den Betroffenen auf eigenen oder vernetzten fremden Computern (wie etwa der sogenannten Cloud) abgelegte oder hinterlassene Daten erhoben und deren Verhalten im Netz nachvollzogen werden kann*.“ Hierzu führte der Erste Senat aus:

> *„Dabei befinden sich die Daten, auf deren Vertraulichkeit die Betroffenen angewiesen sind und auch vertrauen, in weitem Umfang nicht mehr nur auf eigenen informationstechnischen Systemen, sondern auf denen Dritter. Das Grundrecht auf*

Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme schützt dementsprechend vor einem geheimen Zugriff auf diese Daten und damit insbesondere vor Online-Durchsuchungen, mit denen private Computer wie sonstige informationstechnische Systeme manipuliert und ausgelesen, sowie persönliche Daten, die auf externen Servern in einem berechtigten Vertrauen auf Vertraulichkeit ausgelagert sind, erfasst und Bewegungen der Betroffenen im Netz verfolgt werden.“

(BVerfG, Urt. v. 20.4.2016, 1 BvR 966/09, 1 BvR 1140/09, Rn. 210).

Sofern man mit einer Literaturansicht annimmt, § 100a Abs. 1 Satz 2 StPO erlaube den Zugriff auf den Datenaustausch mit der Cloud, liegt insoweit ein Eingriff in das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme vor.

b) Eingriff und verfassungsrechtliche Rechtfertigung

Eine Überwachung der Telekommunikation begründet schwerwiegende Eingriffe, wobei die Heimlichkeit des Zugriffs die Eingriffsintensität noch einmal erhöht. Dabei ist in Rechnung zu stellen, dass § 100a Abs. 1 Satz 2 StPO den Straftatenkatalog des § 100a Abs. 2 StPO übernommen hat. Zu berücksichtigen ist jedoch zugleich, dass § 100a Abs. 1 Satz 2 StPO lediglich die Aufgabe hat, den technischen Entwicklungen der Informationstechnik zu folgen und eine Telekommunikationsüberwachung auch dort zu ermöglichen, wo dies mittels der alten Überwachungstechnik nicht mehr möglich ist (so zur Quellen-TKÜ im BKAG BVerfGE 141, 220 [309]).

Diese Eingriffe sind verfassungsrechtlich nur zum Teil gerechtfertigt.

aa) Eingriffstiefe

Für die an die verfassungsrechtliche Rechtfertigung zu stellenden Maßstäbe kommt es zunächst auf die Eingriffstiefe an. Für die Bewertung der Eingriffstiefe einer Maßnahme nach § 100a Abs. 1 Satz 2 StPO ist maßgeblich, welche Auslegung des Begriffes der Telekommunikation in der Praxis vorgenommen wird. Insoweit kann dahinstehen, ob diese Auslegung „richtig“ oder „falsch“ ist. Maßgeblich ist insoweit einzig, ob eine derartige Auslegung durch die Staatsanwaltschaften und Fachgerichte als vertretbar eingestuft wird. Dies betrifft u.a. die Fallkonstellation des „Surfens im Internet“ (dazu unter (1)) und die Frage einer Zulässigkeit der Überwachung des automatisierten Datenaustausches zwischen Endgerät und Cloud (dazu unter (2)).

(1) „Surfen im Internet“

Staatsanwaltschaften und Fachgerichte vertreten in der Praxis die Auffassung, unter Telekommunikation iSd § 100a StPO sei auch das „Surfen“ im Internet zu fassen. Diese Rechtsauffassung ist zwar umstritten, wird aber in der strafprozessualen Literatur und von Fachgerichten vertreten. Eine (vollständige) Überwachung der Internetnutzung stellt einen besonders schwerwiegenden Eingriff in die Privatsphäre des Betroffenen dar, da die Internetnutzung zum einen besonders sensible Themen (z.B. Krankheit, sexuelle Vorlieben, politische Ausrichtung) betrifft und zum anderen regelmäßig ohne soziale Interaktion erfolgt. Der Nutzer des Internets kann berechtigterweise erwarten, dass sein Nutzungsverhalten Dritten – selbst Familie und Freunden – nicht bekannt wird und kann insoweit auf dem Endgerät sogar Vorkehrungen treffen (z.B. Löschen des Browserverlaufs, etc.). Die Erwartung besonderer Vertraulichkeit der Internetnutzung ist auch grundsätzlich schutzwürdig. Der DAV hat bereits in der Stellungnahme SN 23/22 im Verfahren 1 BvR 1345/21 u.a. darauf hingewiesen, dass eine Überwachung der Internetnutzung im 21. Jahrhundert sehr tiefe Einblicke in die Privatsphäre sowie den Kernbereich ermöglicht und insoweit ausgeführt:

> *„Die Überwachung des Surfverhaltens des modernen Internetnutzers kann tiefgehende Einblicke in den (psychischen) Gesundheitszustand, die politischen und sexuellen Vorlieben und die berufliche Tätigkeit ermöglichen. Eine kürzlich von der ARD ausgestrahlte Dokumentation (Made to Measure: Eine digitale Spurensuche, 1. September 2021, abrufbar unter: https://www.ardmediathek.de/video/wdr-dok/made-to-measure-eine-digitalespurensuche/wdr/Y3JpZDovL3dkci5kZS9CZWl0cmFnLWYwZGQwNTgwLWMyNDUtNGIwZC1iNjE5LTljY2YwNDM5NmVhMQ) veranschaulicht, dass allein über die Rekonstruktion von Google-Suchen einer Person intime Erkenntnisse über Suizidgedanken, Abtreibungen und Essstörungen ermittelt werden konnten.*
>
> *Hierbei handelte es sich um Erkenntnisse, die die betroffene Person nicht mit Dritten geteilt haben muss. Beispiele sind u.a. der Besuch anonymer Foren, z.B. für Opfer von Gewalt- und Sexualverbrechen, Recherchen zu medizinischen Symptomen (66 Prozent der Deutschen haben im Jahr 2019 derartige Recherchen zu eigenen Symptomen angestellt, vgl. https://de.statista.com/infografik/8497/nutzung-des-*

internets-fuer-gesundheitsinformationen/) oder die Nutzung pornographischer Angebote im Internet (ca. 14 Mio. Deutsche sind regelmäßige Nutzer, vgl. https://de.statista.com/infografik/8869/pornografie-im-internet/). Angesichts einer durchschnittlichen Internet-Nutzungsdauer von 269 Minuten/Tag in der Altersgruppe 14-29 (vgl. https://de.statista.com/statistik/daten/studie/1073613/umfrage/taeglichenutzungsdauer-des-medialen-internets-nach-altersgruppen-in-deutschland/) ermöglicht die Überwachung von Datenströmen eine umfassende Überwachung von Interessen und Neigungen der Bürgerinnen und Bürger."

Die obigen Ausführungen betreffen sowohl die Quellen-TKÜ iSd § 100a Abs. 1 Satz 2 StPO als auch die „normale" Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 1 StPO. In beiden Fällen greift die Maßnahme tief in die Grundrechte der Bürgerinnen und Bürger ein. Bei der Quellen-TKÜ nach § 100a Abs. 1 Satz 2 StPO kann sich der Eingriff noch einmal vertiefen. Zwar ist die Nutzung von Verschlüsselungen in der modernen Informationstechnologie ubiquitär. Kommerzielle Anbieter bieten nämlich standardmäßig eine Transportverschlüsselung an (vgl. z.B. im Bereich der Messenger WhatsApp, Signal, Telegram). Dennoch kann eine Verwendung bestimmter Verschlüsselungstechniken gerade dann zum Einsatz kommen, wenn eine sensible (legale) Nutzung des Internets erfolgt und der Nutzer eine Zurückverfolgung verhindern will. Dies können z.B. bestimmte (legale aber in Teilen der Gesellschaft nicht akzeptierte) sexuelle Vorlieben sein. Weit verbreitet ist der Einsatz von besonderen Transport-Verschlüsselungen aber auch im Bereich des investigativen Journalismus oder bei Personen, die Repressalien zu befürchten haben (z.B. Whistleblower). Dementsprechend kann die Kombination aus einer weiten Auslegung des Telekommunikationsbegriffs in Kombination mit der Quellen-TKÜ zu hochsensiblen Einblicken in die Privatsphäre führen.

(2) Cloud-Computing

In der Literatur wird zum Teil die Ansicht vertreten, über § 100a StPO könne auch der – zum Teil automatisierte – Datenaustausch zwischen einem Endgerät und der Cloud überwacht werden. So vertreten u.a. *Henrichs* und *Weingast* (KK-StPO/*Henrichs/Weingast*, 9. Aufl. 2023, StPO § 100a Rn. 4), ihres Zeichens Oberstaatsanwalt und Staatsanwältin beim Bundesgerichtshof, die Ansicht, § 100a StPO erfasse auch den Datenaustausch mit der Cloud. Sie begründen es u.a. damit,

dass *„[b]ei der Überwachung des Datenverkehrs mit der Cloud […] nur ein auf den aktuellen Datenfluss beschränkter Zugriff [erfolge].“* Dieser Befund ist zwar im Grundsatz zutreffend [vgl. zur zeitlichen Dimension aber auch unter f)], suggeriert aber – in vielen Fällen zu Unrecht – einen relativ beschränkten Datenzugriff. Bereits bei der einfachsten Form der Cloud-Nutzung, der Nutzung als externes Speichermedium (Cloud Storage), ist der Zugriff auf Daten erheblich. So verfügen moderne Endgeräte (Smartphones, Laptops, etc.) über verhältnismäßig – im Verhältnis zum stetig wachsenden Bedarf an Speicherplatz angesichts hochauflösender Bilder, Filme, Dokumente – geringe lokale Speicherkapazitäten. Dementsprechend werden zahlreiche Daten nicht mehr lokal gespeichert, sondern auf die Cloud ausgelagert. Sofern ein Dokument lokal benötigt wird, wird es anlassbezogen auf das Endgerät heruntergeladen. Eine Speicherung in der Cloud erfolgt bei vielen Anbietern routinemäßig auch zum Schutz der Daten vor ungewolltem Datenverlust. Zahlreiche Anbieter bieten insoweit eine ständige Datensynchronisation an, so dass jegliche Datenveränderung auf dem Endgerät automatisch in die Cloud übertragen wird. Darüber hinaus besteht bei der modernen Nutzung von Endgeräten die Erwartung, dass sämtliche Endgeräte miteinander vernetzt sind. So soll eine Änderung auf dem Laptop (z.B. ein Kalendereintrag oder ein neues Bild) auch automatisch auf dem über einen Account vernetzten Smartphone abrufbar sein. Beide Endgeräte kommunizieren in einem solchen Fall (automatisch) mit der Cloud, um den Datenbestand abzugleichen.

Darüber hinaus bieten zahlreiche Anbieter „in der Cloud“ auch Dienstleistungen an (Cloud as a Service). In einem solchen Fall muss eine Software nicht mehr heruntergeladen und lokal genutzt werden. Der Datenverarbeitungsprozess der Software erfolgt „in der Cloud“. Auch hier erfolgt ein automatisierter Datenaustausch. Während früher die lokale Datenverarbeitung die Regel war, wird eine Auslagerung von Datenverarbeitungsprozessen „in die Cloud“ aufgrund begrenzter Ressourcen der Endgeräte zunehmend zur Regel. Ein „Offline“-Betrieb ist nur noch eingeschränkt möglich.

Der Durchschnittsnutzer hat insoweit in der Praxis wenig bis keinen Handlungsspielraum. Er ist selbst bei der alltäglichen Nutzung von Endgeräten (Smartphones und Laptops) auf onlinebasierte Speicher- und Dienstleistungsanbieter angewiesen.

bb) Verfassungsrechtliche Rechtfertigung

Das BVerfG hat wiederholt betont, dass die Telekommunikationsüberwachung den legitimen öffentlichen Zweck der Aufklärung und Verfolgung schwerer Straftaten verfolgt. Dabei wurden die unabweisbaren Bedürfnisse einer wirksamen Strafverfolgung hervorgehoben, das öffentliche Interesse an einer möglichst vollständigen Wahrheitsermittlung im Strafverfahren betont und die wirksame Aufklärung gerade schwerer Straftaten als wesentlicher Auftrag eines rechtsstaatlichen Gemeinwesens bezeichnet (BVerfGE 107, 299 [316 m.w.N.]). Dabei wird grundsätzlich eine Straftat von erheblicher Bedeutung und ein konkreter Tatverdacht verlangt (vgl. BVerfGE 107, 299 [321]), wobei eine Straftat von erheblicher Bedeutung mindestens dem Bereich der mittleren Kriminalität zuzurechnen sein, den Rechtsfrieden empfindlich stören und dazu geeignet sein muss, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen (BVerfGE 103, 21 [34]).

Nach diesen Maßstäben unterliegt der Straftatenkatalog grundsätzlich keinen verfassungsrechtlichen Bedenken, da die gesetzgeberische Einstufung der in § 100a Abs. 2 StPO aufgenommenen Straftatbestände als „schwer“ bei einer Gesamtschau vertretbar ist. Das hat das BVerfG bereits im Jahre 2011 festgestellt (BVerfGE 129, 208 [241 ff.]). Zwar ist der Katalog des § 100a Abs. 2 StPO mittlerweile erweitert worden. Im Ergebnis dürfte der dem Gesetzgeber zustehende Beurteilungsspielraum jedoch nicht überschritten worden sein.

Im Grundsatz begegnet daher die Übernahme des Straftatenkatalogs des § 100a Abs. 2 StPO auf § 100a Abs. 1 Satz 2 StPO keinen verfassungsrechtlichen Bedenken. Obwohl es sich bei Maßnahmen nach § 100a Abs. 1 Satz 2 StPO um schwerwiegende Grundrechtseingriffe handelt, dürfte die Übernahme des Katalogs noch verhältnismäßig sein. Denn neben dem dem Gesetzgeber eröffneten Beurteilungsspielraum bei der Entscheidung darüber, welche Straftaten Anlass für bestimmte strafprozessuale Ermittlungsmaßnahmen sind, setzen Eingriffe in das Fernmeldegeheimnis die Qualifizierung einer Straftat nur als schwer voraus (BVerfGE 129, 208 [243]). Zudem ist der besonderen Eingriffstiefe im Rahmen der Prüfung der "Schwere im Einzelfall“ Rechnung zu tragen.

Verfassungsrechtliche Bedenken bestehen allerdings, soweit die Vorschrift des § 100a Abs. 1 Satz 2 StPO den Zugriff auf das Internetnutzungsverhalten ermöglicht. Dabei handelt es sich um einen Eingriff, der deutlich schwerwiegender ist als die Überwachung des sozialen Kommunikationsverhaltens (s. unter 1. a)). Die Beschwerdeführer rügen insoweit zu Recht, dass die fachgerichtliche Rechtspraxis, die gesamte Internetkommunikation zu überwachen, nicht verhältnismäßig im engeren Sinne ist. Die Literatur, die sich für die Zulässigkeit einer Überwachung des Surfverhaltens ausspricht, beruft sich insoweit auf eine Kammerentscheidung des Zweiten Senats (BVerfG, Beschluss vom 6. Juli 2016 - 2 BvR 1454/13). Dabei wird außen vorgelassen, dass die Kammerentscheidung die Rechtsprechung des Ersten Senats unzureichend gewürdigt hat. Der DAV hat bereits in der Stellungnahme SN 33/2022 zum Verfahren 1 BvR 1345/21 BVerfG darauf hingewiesen. Im BKAG-Urteil des Ersten Senats heißt es zur Telekommunikationsüberwachung – wenn auch nicht im Rahmen der Prüfung der Verhältnismäßigkeit im engeren Sinne – nämlich:

> *„Allerdings ist die Telekommunikationsüberwachung ihrem Gesamtcharakter nach nicht in gleicher Weise durch ein Eindringen in die Privatsphäre geprägt wie die Wohnraumüberwachung oder auch die Online-Durchsuchung (vgl. BVerfGE 113, 348 <391>). Sie erfasst Kommunikation aller Art in allen Situationen, die immer technisch vermittelt ist. Höchstvertrauliche Kommunikation ist ein kleiner Teil von ihr, der bei der Überwachung miterfasst zu werden droht, nicht aber - wie die Überwachung des Rückzugsbereichs der privaten Wohnung - typusprägend ist. Sie unterscheidet sich insoweit auch von Online-Durchsuchungen. Denn während diese oft gesamthaft über lange Zeit angesammelte Informationen einschließlich höchstprivater Aufzeichnungen erfassen und dabei unter Umständen durch deren Verknüpfung sowie das Nach- oder Mitverfolgen der Bewegungen im Internet auch geheim gehaltene Schwächen und Neigungen erschließen können, bezieht sich die Telekommunikationsüberwachung auf einzelne Akte unmittelbarer Kommunikation. Ihre Kernbereichsnähe beschränkt sich vor allem darauf, dass sie hierbei auch den höchstpersönlichen Austausch zwischen Vertrauenspersonen umfasst (vgl. BVerfGE 129, 208 <247>).“*
>
> (BVerfG, Urt. v. 20.4.2016, 1 BvR 966/09, 1 BvR 1140/09, Rn. 238. Hervorhebung hier.).

Legt man diesen, vom Ersten Senat dargestellten Maßstab zu Grunde, kann eine Überwachung der gesamten Internetnutzung nicht für den ganzen Katalog des § 100a Abs. 2 StPO verfassungsrechtlich gerechtfertigt sein.

Eine verfassungskonforme (restriktive) Auslegung des § 100a Abs. 1 StPO dürfte insoweit unzureichend sein. So dürfte es – wie Befürworter einer extensiven Auslegung des § 100a StPO zu Recht hervorheben – aus technischen Gründen grundsätzlich nicht möglich sein, bei der Erhebung durch Ausleitung des Datenstroms zwischen sozialer Interaktion und anderweitiger Internetnutzung zu differenzieren. Die Regelung des § 100a StPO dürfte insoweit nur verfassungskonform ausgestaltet sein, wenn – ähnlich wie beim Kernbereichsschutz – ausdrückliche Verwendungsbeschränkungen und Löschungspflichten durch den Gesetzgeber definiert werden. Etwas anderes dürfte gelten, wenn bei einem Einsatz nach § 100a Abs. 1 Satz 2 StPO eine technische Differenzierung möglich wäre (z.B. indem das reine Surfen im World Wide Web von der Überwachung und Sicherung ausgenommen wird). Bei einer – hier nicht verfahrensgegenständlichen – Überwachung nach § 100a Abs. 1 Satz 1 StPO ist eine Differenzierung nicht möglich, da insoweit vom Diensteanbieter der gesamte Datenstrom ausgeleitet wird.

Verfassungsrechtliche Bedenken bestehen ferner, soweit die Vorschrift des § 100a Abs. 1 Satz 2 StPO faktisch Zugriff auf den automatisierten Datenaustausch mit der Cloud ermöglicht. Insoweit liegt ein Eingriff in das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme vor. Die Eingriffstiefe ist immens, da auf diesem Weg regelmäßig u.a. Zugriff auf private Fotos, Videos, digitale Tagebücher, private Notizen und weitere, in der Erwartung besonderer Vertraulichkeit gespeicherte Daten zu ermöglichen. Das Bundesverfassungsgericht hat sich insoweit zwar noch nicht eindeutig zu der Frage positioniert, ob für einen derartigen mittelbaren Zugriff auf Daten, die auf dem Endgerät oder einem externen Datenspeicher – ohne gleichzeitigen Vollzugriff auf das Endgerät die gleichen verfassungsrechtlichen Hürden gelten, wie für die Online-Durchsuchung. Da ein Zugriff auf derartige Daten unter den tatsächlichen Rahmenbedingungen des modernen Cloud-Computings von der Eingriffstiefe einem Vollzugriff zumindest nahekommt bzw. kommen kann, bietet es sich jedoch an, insoweit die gleichen verfassungsrechtlichen Hürden zu fordern. Jedenfalls dürften die in § 100a Abs. 1 S. 2, Abs. 2 StPO niedergelegten Anforderungen für einen derartigen Zugriff

verfassungsrechtlich unvertretbar sein. Die Eingriffstiefe geht über eine klassische Telekommunikationsüberwachung weit hinaus.

Auch insoweit dürfte eine verfassungskonforme (restriktive) Auslegung des § 100a Abs. 1 StPO unzureichend sein. Dies dürfte im Ergebnis von der Funktionsweise der jeweiligen Cloud-Anwendung sowie der von den Ermittlungsbehörden eingesetzten Software abhängen. Würde die Behördensoftware ermöglichen, bereits vor Erhebung der Daten eine Differenzierung vorzunehmen, wäre die Regelung wohl einer verfassungskonformen Auslegung zugänglich. Dafür wäre allerdings notwendig, dass die Software ganze Anwendungen von der Sicherung und Überwachung ausnimmt (z.B. bestimmte Cloud-spezifische Anwendungen wie z.B. die icloud von Apple oder One Drive von Microsoft) und bei anderen Anwendungen nach der Art des Datentransfers differenziert (z.B. bei Verwendung eines E-Mail-Postfaches zwischen Versendung einer E-Mail und automatisierter Speicherung des E-Mail-Entwurfes im eigenen Postfach in der Cloud). Sofern eine solche Differenzierung auf Erhebungsebene technisch nicht umsetzbar ist, bedürfte es einer spezifischen gesetzlichen Regelung von Verwendungsbeschränkungen und Löschungspflichten.

c) Technische Möglichkeit und technische Sicherung

Ob und inwieweit die Quellen-TKÜ überhaupt technisch möglich ist, betrifft nicht die Geltung, sondern die Anwendung der Norm, sodass insoweit keine verfassungsrechtlichen Bedenken bestehen (BVerfGE 141, 220 [311 Rn. 234]). Jedenfalls verfügt das BKA nach Eigenangaben (mittlerweile) sowohl über eigenentwickelte als auch über kommerzielle Software zur Durchführung von Maßnahmen zur Quellen-TKÜ. Die jeweilige Software werde erst nach einem umfangreichen Testverfahren und Feststellung der Konformität zum Einsatz freigegeben und in Abhängigkeit von der operativen Bedarfslage kontinuierlich weiterentwickelt.[4]

Da in § 100 Abs. 5 Satz 1 Nr. 2 und 3 und Satz 2 und 3 StPO weiter die Pflicht geregelt ist, technisch sicherzustellen, dass an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind,

[4] https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html, zuletzt abgerufen am 30.06.2023.

und die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden sowie das eingesetzte Mittel gegen unbefugte Nutzung und kopierte Daten gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme – jeweils nach dem Stand der Technik – zu schützen sind, wird der Gefahr des Missbrauchs, der Fehlfunktion sowie der Beweismittelmanipulation gesetzlich entgegengewirkt. In diesem Zusammenhang hat das BVerfG auch betont, dass es auf die Aufhebung der Begrenzung auf eine Erfassung der laufenden Telekommunikation nicht ankommt, sondern nur darauf, ob das Programm so ausgestaltet ist, dass es hinreichend abgesichert auch gegenüber Dritten den mit der Überwachung betrauten Mitarbeiterinnen und Mitarbeitern inhaltlich eine ausschließlich auf die laufenden Kommunikationsinhalte begrenzte Kenntnisnahme ermöglicht (BVerfGE 141, 220 [311 Rn. 234]). Gerade dies gewährleisten die Regelungen in § 100a Abs. 1 Satz 2, Abs. 5 StPO.

Die weitergehende Rüge der Beschwerdeführer, es würden Selbstschutzmöglichkeiten umgangen, ist zutreffend. Ohne die Umgehung würde jedoch der wesentliche Auftrag des Rechtsstaats an der Strafverfolgung konterkariert. Gleichwohl zeigt die Umgehung der Selbstschutzmöglichkeiten, dass die Quellen-TKÜ schwerwiegende Grundrechtseingriffe ermöglicht, die über die einer klassischen TKÜ hinausgehen.

d) „Nachrichtenmittler“ / „Nichtbeschuldigte“

Nach § 100a Abs. 3 StPO darf sich die Anordnung 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.

Dass der Beschuldigte Adressat der Anordnung ist, ist verfassungsrechtlich nicht zu beanstanden. Verfassungsrechtliche Bedenken bestehen auch nicht hinsichtlich der Erstreckung auf sog. Nachrichtenmittler. Zu der Vorschrift des § 20l Abs. 1 Satz 1 Nr. 3 und 4 BKAG, die eng an § 100a Abs. 3 StPO angelegt ist, hat das BVerfG entschieden, dass sie hinreichend auslegungsfähig ist und den Anforderungen des Bestimmtheitsgrundsatzes genügt (BVerfGE 141, 220 [311 Rn. 233]). Gleiches dürfte

im Ergebnis für § 100a Abs. 3 StPO gelten. Denn – ebenso wie die Regelung im BKAG – erlaubt § 100a Abs. 3 StPO keine Überwachungsmaßnahmen ins Blaue hinein für alle Personen, die mit der Zielperson Nachrichten ausgetauscht haben, sondern setzt bei verfassungskonformer Auslegung eigene, in der Anordnung darzulegende Anhaltspunkte dafür voraus, dass der Nachrichtenmittler von der Zielperson in die Tatdurchführung eingebunden wird und somit eine besondere Tat- oder Gefahrennähe aufweist. Problematisch ist in der fachgerichtlichen Praxis allerdings, dass die Ermittlungsbehörden und Fachgerichte die vom Bundesverfassungsgericht geforderte restriktive Auslegung des Begriffs des Nachrichtenmittlers wiederholt ignorieren und eine Telekommunikationsüberwachung auf Anschlüsse erstrecken, aus deren Überwachung sie sich irgendwelche verfahrensrelevanten Erkenntnisse versprechen. Dies zeigt eindrücklich der Beschluss der 2. Kammer des Zweiten Senats des BVerfG vom 21.3.2023 – 2 BvR 626/20. Hier musste das Bundesverfassungsgericht erneut in Erinnerung rufen, dass vage Anhaltspunkte und bloße Vermutungen für eine Anordnung gegen Nichtbeschuldigte nicht ausreichen. (Verfassungsrechtlich) Erforderlich ist, dass aufgrund der Lebenserfahrung oder der kriminalistischen Erfahrung fallbezogen aus Zeugenaussagen, Observationen oder anderen sachlichen Beweisanzeichen auf die Eigenschaft als Nachrichtenmittler geschlossen werden kann. Dem DAV sind diverse Fälle bekannt, bei denen – wie in dem, dem Kammerbeschluss zugrundeliegenden Fall – eine weitgehend konturenlose Interpretation des Nachrichtenmittlers erfolgt. U.a. sind aus Steuerstrafverfahren Gerichtsbeschlüsse bekannt, mit denen sogar die Überwachung von normalen Kunden-Hotlines und die Überwachung von Mitarbeitern genehmigt wurden, um das Geschäftsmodell des Unternehmens nachzuvollziehen.

Ob § 100a Abs. 3 StPO angesichts der, die verfassungsgerichtliche Rechtsprechung oftmals ignorierende Praxis noch immer einer verfassungskonformen Auslegung zugänglich ist, erscheint zumindest fraglich.

e) Richtervorbehalt

Aus verfahrensrechtlicher Sicht bestehen im Grundsatz keine Bedenken gegen § 100a Abs. 1 Satz 2 StPO. Nach der Rechtsprechung des BVerfG (BVerfGE 125, 260 [337 f.]) kann bei Ermittlungsmaßnahmen, die einen schwerwiegenden Grundrechtseingriff bewirken, verfassungsrechtlich eine vorbeugende Kontrolle durch eine unabhängige

Instanz geboten sein. Dies gilt insbesondere, wenn der Grundrechtseingriff – wie hier – heimlich erfolgt und für den Betroffenen unmittelbar nicht wahrnehmbar ist. Dann sind die Maßnahmen aufgrund der Eingriffsintensität zwingend unter den Vorbehalt richterlicher Anordnung zu stellen. Denn Richter können aufgrund ihrer persönlichen und sachlichen Unabhängigkeit und ihrer ausschließlichen Bindung an das Gesetz die Rechte des Betroffenen im Einzelfall am besten und sichersten wahren.

§ 100e Abs. 1. StPO normiert einen solchen Richtervorbehalt. Es ist demnach Aufgabe und Pflicht des Gerichts, sich eigenverantwortlich ein Urteil darüber zu bilden, ob die beantragte heimliche Maßnahme den gesetzlichen Voraussetzungen entspricht. Nichts anderes folgt aus § 100e Abs. 3 und 4 StPO, der explizit regelt, welche Angaben in der Entscheidungsformel und in der Begründung enthalten sein müssen. Die Darlegung der bestimmten Tatsachen, die den Verdacht begründen, sowie der wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme verdeutlichen, dass alle rechtlich maßgeblichen Gesichtspunkte tragfähig dargelegt werden müssen (vgl. BVerfGE 141, 220 [299 Rn. 194]).

Nach diesen Maßstäben ist gerichtlich auch der jeweilige „Stand der Technik“ i.S.d. § 100a Abs. 5 Satz 2 und 3 StPO als gesetzliche Voraussetzung der Maßnahme zu prüfen. Soweit die Beschwerdeführer hierzu vortragen, die Beurteilung sei dem anordnenden Gericht schon tatsächlich nicht möglich, sondern nur einer unabhängigen Stelle, greift dieses Argument nicht durch. Denn erstens sind durch die antragstellende Behörde vollständige Informationen über den zu beurteilenden Sachstand darzulegen und zweitens ist es Sache der Landesjustizverwaltung und des Präsidiums des zuständigen Gerichts, die jeweils notwendigen sachlichen und personellen Voraussetzungen zu schaffen (BVerfGE 141, 220 [275 f. Rn. 118 m.w.N.]). Dass dies nicht möglich ist, insbesondere zur Beurteilung des jeweiligen Standes der Technik, wird auch von den Beschwerdeführern nicht behauptet.

f) Fehlende zeitliche Obergrenze

Soweit § 100e StPO eine zeitliche Obergrenze nicht verbindlich regelt, sondern die wiederholte Anordnung ohne entsprechende Obergrenze zulässt, ist dies verfassungsrechtlich ebenfalls unbedenklich. Denn eine zeitliche Begrenzung ist

gegebenenfalls einzelfallbezogen aus Verhältnismäßigkeitsgesichtspunkten herzuleiten (BVerfGE 141, 220 [299 Rn. 195]; 109, 279 [362 Rn. 284]).

g) Schutzpflichten für die IT-Sicherheit (Ausnutzung und Aufrechterhaltung von technischen Lücken)

Eingriffe im Sinne des § 100a Abs. 1 Satz 2 StPO erfolgen dergestalt, dass die von dem Betroffenen genutzten informationstechnischen Systeme mittels einer Software infiltriert werden, um die Telekommunikation (unverschlüsselt) zu überwachen und aufzuzeichnen (vgl. BT-Drs. S. 51).

Der Erste Senat des Bundesverfassungsgerichts hat in seinem Beschluss vom 8. Juni 2021 – 1 BvR 2771/18 –, festgestellt, dass sich aus dem Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme eine Pflicht des Staates ergibt, dazu beizutragen, dass die Schutzgüter gegen Angriffe Dritter geschützt werden. Wisse der Staat von Sicherheitslücken, die den Herstellern und Nutzern unbekannt sind, verdichte sich sein allgemeiner Schutzauftrag zu einer konkreten Verpflichtung, die Nutzerinnen und Nutzer informationstechnischer Systeme davor zu schützen, dass Dritte über unbekannte Sicherheitslücken die genutzten Systeme infiltrieren (BVerfG, Beschluss vom 8. Juni 2021 – 1 BvR 2771/18 –, Rn. 35).

Diese Schutzpflicht schließe zwar die Ausnutzung von Sicherheitslücken für eine Quellen-Telekommunikationsüberwachung nicht aus, verlange aber, dass der Gesetzgeber den Umgang der Polizeibehörden mit Sicherheitslücken, die den Herstellern nicht bekannt sind, regelt (BVerfG, Beschluss vom 8. Juni 2021 – 1 BvR 2771/18 –, Rn. 35, 41 ff.). Andernfalls bestünde die Gefahr, dass es die Behörde im Interesse der Durchführung ihr übertragener Überwachungsbefugnisse unterlässt, Sicherheitslücken zu melden oder sogar aktiv darauf hinwirkt, dass diese unerkannt bleiben (BVerfG, Beschluss vom 8. Juni 2021 – 1 BvR 2771/18 –, Rn. 42).

Demgegenüber hat die 2. Kammer des Ersten Senats des BVerfG mit Nichtannahmebeschluss vom 7.04.2023 – 1 BvR 176/23, 1 BvR 178/23, Rn. 4 ff. entschieden, dass sich im Falle der Behauptung einer gesetzgeberischen Schutzpflichtverletzung spezifische Darlegungslasten dahingehend ergeben, dass über den Vortrag angeblicher Unzulänglichkeiten der Rechtslage hinaus der gesetzliche Regelungszusammenhang insgesamt erfasst sein muss, wozu – je nach Fallgestaltung

– zumindest gehört, dass die einschlägigen Regelungen des als unzureichend beanstandeten Normkomplexes jedenfalls in Grundzügen dargestellt werden und begründet wird, warum vom Versagen der gesetzgeberischen Konzeption ausgegangen wird. Dem genügt die Verfassungsbeschwerde nicht, weshalb es an der hinreichenden Darlegung der Möglichkeit einer Schutzpflichtverletzung fehlt. Denn die Beschwerdeführer rügen die Ausnutzung von Sicherheitslücken und die damit verbundene Gefährdung bzw. den unzureichenden Schutz der IT-Sicherheit. Nicht betrachtet wurden jedoch § 500 Abs. 1 StPO, der u.a. auf § 67 BDSG verweist. Danach ist möglicherweise eine Datenschutz-Folgenabwägung vorzunehmen. Hinzu kommt, dass gem. § 68 BDSG i.V.m. § 500 Abs. 2 Nr. 2 StPO mit der oder dem Landesbeauftragten für Datenschutz zusammenzuarbeiten ist. Dass diese Regelungen dem Schutz der IT-Sicherheit nicht gerecht werden, ist nicht erkennbar. Jedenfalls mangelt es aber insoweit an einer hinreichenden Darlegung der Beschwerdeführer.

h) Relevanz in der Praxis

Dass die von den Beschwerdeführern befürchteten grenzenlosen Zugriffsmöglichkeiten nach § 100a Abs. 1 Satz 2 und 3 StPO tatsächlich nicht bestehen, verdeutlicht die „Übersicht Telekommunikationsüberwachung für 2020“, Stand: August 2022, des Bundesamtes für Justiz.[5] Danach wurden im Jahr 2020 25 Eingriffe in ein vom Betroffenen genutztes Informationstechnisches System gem. § 100a Abs. 1 Sätze 2 und 3 StPO angeordnet, jedoch lediglich 14 tatsächlich durchgeführt. Dem stehen insgesamt 17.731 Erst- und Verlängerungsanordnungen für Überwachungen gegenüber.

Dies zeigt: Die Relevanz in der Praxis ist untergeordnet, was möglicherweise an den zusätzlichen rechtlichen und technischen Anforderungen des § 100a StPO liegen dürfte.

[5] https://www.bundesjustizamt.de/SharedDocs/Downloads/DE/Justizstatistiken/Uebersicht_TKUE_2020.pdf?__blob=publicationFile&v=6, zuletzt abgerufen am 30.06.2023.

II. § 100a Abs. 1 Satz 3 StPO

Unabhängig von der Bezeichnung, ob es sich bei § 100a Abs. 1 Satz 3 StPO ebenfalls um eine „Quellen-TKÜ“, eine „kleine Systemüberwachung“ oder um eine „kleine Online-Durchsuchung“ handelt, ist allein der materielle Gehalt der Vorschrift relevant.

1. Wortlaut und Auslegung

Nach § 100a Abs. 1 Satz 3 StPO dürfen auf dem informationstechnischen System des Betroffenen gespeicherte Inhalte und Umstände der Kommunikation überwacht und aufgezeichnet werden, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können. Dabei ist nach § 100a Abs. 5 Satz 1 Nr. 1 lit. b StPO technisch sicherzustellen, dass ausschließlich Inhalte und Umstände der Kommunikation, die ab dem Zeitpunkt der (richterlichen) Anordnung nach § 100e Abs. 1 StPO auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz hätten überwacht und aufgezeichnet werden können. Weiter sieht § 100a Abs. 5 Satz 2 und 3 StPO vor, dass das eingesetzte Mittel nach dem Stand der Technik gegen unbefugte Nutzung sowie kopierte Daten nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen sind. Protokollierungspflichten sind in § 100a Abs. 6 StPO geregelt.

§ 100a Abs. 1 Satz 3 StPO beschränkt sich demnach nicht auf die laufende Kommunikation, sondern erfasst auch solche Inhalte und Umstände der Kommunikation, bei denen der Übertragungsvorgang bereits abgeschlossen ist und die auf dem informationstechnischen System des Betroffenen in einer Anwendung gespeichert sind (BT-Drs. 18/12785, S. 51). § 100a Abs. 1 Satz 3 StPO ermöglicht allerdings weder inhaltlich noch zeitlich einen uneingeschränkten Zugriff auf ein informationstechnisches System. Aus inhaltlicher Sicht darf nur auf solche Inhalte und Umstände der Kommunikation zugegriffen werden, die auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können. Aus zeitlicher Sicht ist nach § 100a Abs. 5 Satz 1 Nr. 1 lit. b StPO technisch sicherzustellen, dass Inhalte und Umstände der Kommunikation erst ab dem Zeitpunkt der Anordnung durch das Gericht ausgeleitet werden dürfen.

2. Verfassungsrechtliche Vorgaben

a) Schutzbereich des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG und Eingriff

Der der § 100a Abs. 1 Satz 3 StPO ermöglichte Zugriff auf ein informationstechnisches System ist als Eingriff in das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG zu werten. Davon geht auch der Gesetzgeber aus (BT-Drs. 18/12785, S. 50). Die Eingriffstiefe des § 100a Abs. 1 Satz 3 StPO hängt auch hier von der Frage ab, wie der einfachgesetzliche Telekommunikationsbegriff zu interpretieren ist. Würde man hier auch das „Surfen im Internet“ erfassen, könnten die Ermittlungsbehörden z.B. den Browserverlauf auslesen (zur Eingriffstiefe s. unter I. 2. b) aa)). Würde man auch den Datentransfer mit der Cloud als erfasst ansehen, könnten die Ermittlungsbehörden rekonstruieren, welche automatisierten Datentransfers es ab Anordnung des Gerichts gegeben hat und könnten diese Daten auslesen.

b) Verfassungsrechtliche Rechtfertigung

Das BVerfG hat wiederholt betont, dass heimliche Überwachungsmaßnahmen verfassungsrechtlich gerechtfertigt sein können. Das setzt den Schutz oder die Bewehrung hinreichend gewichtiger Rechtsgüter voraus, wobei es bei Maßnahmen, die der Strafverfolgungen dienen, auf das Gewicht der verfolgten Straftaten ankommt. Insoweit nimmt das BVerfG Bezug auf die Einordnung der besonders schweren und schweren Straftaten sowie Straftaten von erheblicher Bedeutung (BVerfGE 141, 220 [270 Rn. 107]; vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 251).

Für Fälle präventiver Gefahrenabwehr sind Eingriffe nur zum Schutz besonders gewichtiger Rechtsgüter zulässig, wozu namentlich Leib, Leben und Freiheit der Person sowie der Bestand oder die Sicherheit des Bundes oder eines Landes gehören (BVerfGE 141, 220 [270 Rn. 108]; 120, 274 [328 Rn. 247]).

Diese Maßstäbe gelten allerdings nicht uneingeschränkt, auch nicht hinsichtlich strafprozessualer Maßnahmen. Vielmehr hat das BVerfG bereits im Jahre 2008 festgestellt, dass auch bei einem heimlichen Zugriff auf informationstechnische

Systeme die Eingriffsintensität und das Gewicht des gesetzlich geregelten Eingriffsanlasses entscheidend sind (BVerfGE 120, 274 [322 ff.]). Das hat das BVerfG wiederholt – auch jüngst – noch einmal zum Bereich der Gefahrenabwehr bestätigt. Wie streng die Verhältnismäßigkeitsanforderungen an heimliche Überwachungsbefugnisse sind, bestimmt sich nach dem jeweiligen Eingriffsgewicht, wobei im Grundsatz gilt, dass der Zugriff auf informationstechnische Systeme besonders tief in die Privatsphäre eingreift (BVerfG, Urteil vom 26. April 2022 – 1 BvR 11619/17 – Rn. 174; BVerfGE 141, 220 [269 Rn. 105]).

Vor diesem Hintergrund ist hier in Rechnung zu stellen, dass die Zugriffsmöglichkeiten des § 100a Abs. 1 Satz 3 StPO sowohl inhaltlich als auch zeitlich begrenzt sind. Denn es geht dem Gesetzgeber maßgeblich darum, ein „funktionales Äquivalent“ zur Telekommunikationsüberwachung zu schaffen (BT-Drs. 18/12785, S. 49 ff.). Die Notwendigkeit der in § 100a Abs. 1 Satz 3 StPO geschaffenen „ergänzenden“ Regelung ist darin begründet, dass insbesondere Textnachrichten und sonstige Botschaften, die über Messenger-Dienste versandt werden, ebenso wie Sprach- und Videotelefonate Kommunikationsinhalte enthalten, die IP-basiert und in der Regel verschlüsselt über das Datennetz übertragen werden. Anders als bei der Sprach- und Videotelefonie in Echtzeit ist jedoch der Übertragungsvorgang mit dem Zugang der Nachricht auf dem Endgerät des Betroffenen abgeschlossen, sodass zum Auslesen dieser Nachrichten ein Zugriff auf das informationstechnische System erforderlich ist. Das hat jedoch zugleich zur Folge, dass der Schutzbereich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme eröffnet ist. Es geht daher auch bei § 100a Abs. 1 Satz 3 StPO ausschließlich darum, den technischen Entwicklungen der Informationstechnik Rechnung zu tragen und – ohne Zugriff auf weitere gespeicherte Inhalte des informationstechnischen Systems – eine Telekommunikationsüberwachung auch dort zu ermöglichen, wo dies mittels der alten Überwachungstechnik nicht mehr möglich ist (BT-Drs. 18/12785, S. 50).

Zudem sind Maßnahmen nach § 100a Abs. 1 Satz 3 StPO nur insoweit zulässig, als die Telekommunikation „*auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können.*“ Diese Voraussetzung ist vom anordnenden Gericht zu prüfen. Verfassungskonform ist das Tatbestandsmerkmal dahingehend auszulegen,

dass nur solche Inhalte und Umstände überwacht und aufgezeichnet werden dürfen, die auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden dürfen, für die also ebenfalls die Voraussetzungen des § 100a Abs. 1 Satz 1 StPO vorgelegen hätten. Vom anordnenden Gericht ist demnach die hypothetische Zulässigkeit nach § 100a Abs. 1 Satz 1 StPO (inzident) zu prüfen. Damit ist verfassungsrechtlich sichergestellt, dass § 100 Abs. 1 Satz 3 StPO ein funktionales Äquivalent zu § 100a Abs. 1 Satz 1 StPO darstellt und keine verstärkte Eingriffsintensität aufweist.

Ausgehend von diesem Verständnis ist es verfassungsrechtlich dann grundsätzlich nicht zu beanstanden, wenn der Gesetzgeber zur Rechtfertigung auf den Verdacht einer schweren Straftat i.S.d. § 100a Abs. 2 StPO abstellt. Verfassungsrechtlich grundsätzlich zulässig ist auch die Zugriffsmöglichkeit ab dem Zeitpunkt der richterlichen Anordnung. Ab diesem Zeitpunkt ist der Zugriff zulässig, sodass die von den Beschwerdeführern vorgetragene rückwirkende Datenerhebung aufgrund der erst späteren tatsächlichen Infiltration aus rechtlicher Sicht nicht besteht. Verfassungsrechtlich bedenklich ist jedoch das damit verbundene Auslesen des „Zeitstempels“. Der DAV hat bereits in seiner Stellungnahme SN 44/17 zur Einführung der Online-Durchsuchung und Quellen-TKÜ in der StPO, dort S. 10 f., ausgeführt, dass sich Maßnahmen nach § 100a Abs. 1 Satz 3 StPO nur auf Daten beziehen dürfen, die nach Anordnung der Maßnahme durch das Gericht hätten ausgeleitet werden können. Auf dem Endgerät eines Kommunikationsinhabers sind jedoch unter Umständen auch Nachrichten gespeichert, die sich auf Zeiträume vor der Anordnung erstrecken. Die einzusetzende Software muss daher so programmiert sein, dass sie anhand der zu den einzelnen Nachrichten hinterlegten Meta-Daten, die etwa die Absende-, Empfangs- und Lesezeitpunkte enthalten, nur die erst ab dem Zeitpunkt der Anordnung ein- und ausgehenden Nachrichten ausleitet.

Inwieweit dies technisch überhaupt möglich ist, kann vom DAV nicht beantwortet werden. Aus verfassungsrechtlicher Sicht bestehen jedoch insoweit Bedenken, als der Zugriff bzw. die mit dem Auslesen des Zeitstempels verbundene Durchsuchung der Meta-Daten aller gespeicherten Daten tiefer in die Rechte Betroffener eingreift als eine

Quellen-TKÜ. Gleichwohl erkennt der Gesetzgeber auch insoweit keine höheren verfassungsrechtlichen Hürden.

Im Übrigen gilt das zur Eingriffstiefe der Überwachung der Internetnutzung und der Überwachung des automatisierten Datentransfers im Rahmen des Cloud Computing Gesagte. Insoweit ist die Vorschrift verfassungswidrig, sofern die behördlicherseits eingesetzte Software nicht ausnahmsweise eine Differenzierung vor Erhebung der Daten ermöglicht (s. dazu unter I. 2. b) bb)).

c) Weiterer Vortrag

Im Übrigen wird auf die Ausführungen unter I. 2. c) bis h) verwiesen.

B. § 100b StPO – Online-Durchsuchung

I. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG: Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme („IT-Grundrecht“)

1. Schutzbereich

Das IT-Grundrecht ist eine besondere Ausprägung des allgemeinen Persönlichkeitsrechts aus Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG.

Der Erste Senat des Bundesverfassungsgerichts begründete das Bedürfnis dieser seinerzeit neuen Ausprägung des allgemeinen Persönlichkeitsrechts in seiner maßgeblichen Entscheidung vom 27. Februar 2008 wie folgt:

> *„Aus der Bedeutung der Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung und aus den Persönlichkeitsgefährdungen, die mit dieser Nutzung verbunden sind, folgt ein grundrechtlich erhebliches Schutzbedürfnis. Der Einzelne ist darauf angewiesen, dass der Staat die mit Blick auf die ungehinderte Persönlichkeitsentfaltung berechtigten Erwartungen an die Integrität und Vertraulichkeit derartiger Systeme achtet. Die grundrechtlichen Gewährleistungen der Art. 10 und Art. 13 GG wie auch die bisher in der Rechtsprechung des BVerfG entwickelten Ausprägungen des allgemeinen Persönlichkeitsrechts tragen dem*

durch die Entwicklung der Informationstechnik entstandenen Schutzbedürfnis nicht hinreichend Rechnung.“

(BVerfG NJW 2008, 822, Rz. 181)

In persönlicher Hinsicht schützt das IT-Grundrecht jedermann. Dem Schutzbereich unterfallen daher alle natürlichen Personen. Auch inländische juristische Personen können sich nach den Maßgaben des Art. 19 Abs. 3 GG auf das IT-Grundrecht berufen.

In materieller Hinsicht schützt es den persönlichen und privaten Lebensbereich der Grundrechtsträger vor staatlichem Zugriff im Bereich der Informationstechnik.
Der Anwendungsbereich des IT-Grundrechts ist im Hinblick auf Systeme eröffnet, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten (BVerfG NJW 2008, 822, Rz. 203).

Das IT-Grundrecht schützt die Vertraulichkeit, also das Interesse des Nutzers, dass die von einem vom Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben (BVerfG NJW 2008, 822, Rz. 204).

Geschützt wird darüber hinaus die Integrität des geschützten IT-Systems, so dass ein Eingriff anzunehmen ist, wenn auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können. Dann – so der Erste Senat des BVerfG – sei die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen (BVerfG NJW 2008, 822, Rz. 204).

2. Eingriff

Die Online-Durchsuchung gemäß § 100b StPO greift in den Schutzbereich des IT-Grundrechts ein. Der Eingriff ist von erheblicher Intensität. Diesbezüglich sind folgende Aspekte hervorzuheben.

a) Bedeutung von Daten auf IT-Systemen

Die besondere Intensität des Eingriffs folgt zunächst aus der enormen Bedeutung persönlicher IT-Systeme im gesellschaftlichen Alltag und der Menge der auf diesen Systemen bewusst oder unbewusst gespeicherten Daten. Aus den auf dem Smartphone gespeicherten Daten lässt sich heute ohne Weiteres ein umfassendes Persönlichkeitsprofil ableiten. So geben die dort gespeicherten Daten nicht nur Auskunft über die Bestandsdaten einer Person, sondern auch über deren Interessen, höchstpersönlichen inneren Überlegungen und Gefühle, Beziehungen, Interessen, persönliche und sexuelle Vorlieben.

Mit voranschreitendem technischem Fortschritt erhört sich die Dichte dieses „digitalen Datenabbildes“ ganz erheblich. Dies folgt aus der Verlagerung der zwischenmenschlichen Interaktion in den digitalen Raum, die steigende technische Leistungsfähigkeit und Kapazität persönlicher IT-Systeme (wie moderne Smartphones) und die wachsende Anzahl von technischen Sensoren und Schnittstellen solcher Geräte und Zubehöreinheiten (z.B. Kameras, Mikrofonarray, LiDAR-Scanner, Gesichtserkennungsmodul, Barometer, 3-Achsen-Drehratensensor/Gyrometer, Beschleunigungssensor, Annäherungssensor, Umgebungslichtsensor, Kompass, GPS-Modul, Mobilfunkmodul, WLAN-Modul, Bluetooth-Modul, NFC-Sensor, optische und elektrische Herzsensoren, Blutsauerstoff-Sensor, Körpertemperatursensor, Atemfrequenzmessung, Sprachassistenten). Der Datenanfall erfolgt dabei immer weniger bewusst infolge einer bewussten Aktivierung durch den Nutzer, sondern automatisch anlässlich der alltäglichen Nutzung solcher informationstechnischen Geräte. Auch die Entscheidung über die Speicherung und Löschung der auf diesem Wege anfallenden Daten (beispielsweise auch in Clouddiensten) steht immer weniger im Machtbereich des Individuums.

Durch die Vernetzung mit anderen IT-Systemen erhöht sich die Eingriffsintensität der Online-Durchsuchung um ein Vielfaches. Dies gilt gerade im Falle der Online-Durchsuchung eines Smartphones, das über sog. Apps und Smart-Home-Anwendungen nicht nur mit anderen digitalen Geräten des „Internet of things (IoT)“, wie des Haushalts (TV, Musikanlage, Kühlschrank, Thermostate) oder des Autos, sondern auch etwa Sexspielzeugen verbunden sein kann. Die Strafverfolgungsbehörden

erhalten somit auf Basis eines bloßen Anfangsverdachts einen vollständigen Zugriff auf das digital abgebildete Leben des Nutzers.

b) Zugriff auf Datenmassen

Die Online-Durchsuchung ist weiter besonders eingriffsintensiv, weil sie die Erhebung von Datenmassen erlaubt, ohne dass der Zugriff in zeitlicher, in sachlicher oder in sonstiger Hinsicht auf bestimmte Daten beschränkt werden müsste.

Gemäß § 100b Abs. 1 StPO können Daten ohne Rücksicht auf das Datum ihrer Entstehung erhoben werden, so dass es sich dabei um Daten über den Zeitraum von Jahren oder Jahrzehnten handeln kann. Den Strafverfolgungsbehörden soll es danach erlaubt sein, auf Daten zuzugreifen, die lange vor der möglichen Tatbegehung entstanden sind. Die Maßnahme bietet dadurch ein erhebliches Missbrauchspotential in Hinblick auf eine ohne weiteres mögliche – und möglicherweise auch kaum vermeidbare – Suche nach bzw. Entdeckung von Zufallsfunden („*fishing expedition*“).

Auch in sachlicher Hinsicht fehlen Beschränkungen des Zugriffs. So können nicht nur Gedankenäußerungen wie Textdateien, sondern auch Bild-, Ton-, Videodateien und zahllose weitere Datenarten erhoben werden. In der Praxis wird dies dazu führen, dass der gesamte Datenbestand eines IT-Systems heimlich gespiegelt wird. In ihrer Intensität geht die Maßnahme damit auch weit über eine (heimliche) Durchsuchung hinaus, weil keine Selektion der erhobenen Daten zum Zeitpunkt des Erstzugriffs erfolgt. Damit verlagert sich eine mögliche Selektion vollständig auf die Ebene der Durchsicht von Daten. Hierfür fehlt es im Hinblick auf § 100b StPO an einer Regelung, weil § 110 StPO nicht auf die Online-Durchsuchung anwendbar sein dürfte. Und auch § 110 StPO enthielte im Falle einer entsprechenden Anwendung keine begrenzenden Verfahrensregelungen zum Umgang mit den erhobenen Daten und keine präventive richterliche Kontrolle für die Sichtung.

c) Live-Überwachung des Nutzerverhaltens

Besonders eingriffsintensiv ist die Online-Durchsuchung aufgrund der Möglichkeit der Live-Überwachung des Nutzerverhaltens, die es den Strafverfolgungsbehörden erlaubt, dem Nutzer beim Denken und Fühlen „über die Schulter“ zu schauen. So können die Strafverfolgungsbehörden nicht nur das Surfverhalten des Nutzers im Internet und das

Nutzungsverhalten von Geräten „live“ überwachen, sondern beispielsweise auch solche Nachrichten lesen, die der Nutzer löscht, anstatt sie wie zunächst geplant abzuschicken. Anders als eine „klassische“ physische einmalige offene Durchsuchung des Ist-Zustandes ist so eine fortlaufende Beobachtung und Auswertung aller Systemzustände und damit eine Teilnahme am „digitalen Leben“ des Nutzers möglich.

Zudem erlaubt die Maßnahme die Erhebung aktuell generierter Videodaten, wie z.B. von einer Webcam, sofern der Nutzer die Webcam selbsttätig eingeschaltet hat oder diese ohnehin aktiviert ist. Befindet sich der Nutzer zum Zeitpunkt der Aktivierung der Webcam in seiner Wohnung, führt dies zu einer heimlichen Wohnraumüberwachung. Auch auf den Datenanfall weiterer – zum Großteil standardmäßig aktivierter – IT-Sensoriken kann durch diese Maßnahme zugegriffen werden. Moderne Smartphone-Betriebssysteme vermitteln dem Nutzer vielfach ebenso wenig Kenntnis der derzeit aktiven Sensoren und Schnittstellen, wie den genauen Gegenstand der fortlaufend erhobenen und verarbeiteten Daten.

d) Heimlichkeit der Maßnahme

Die Online-Durchsuchung kann „*ohne Wissen des Betroffenen*“ und somit heimlich durchgeführt werden. Dies erfolgt in der Regel, indem das Zielsystem im Wege eines Fernzugriffs „gehackt“, also mittels einer sog. Remote Forensic Software („Trojaner“) infiltriert wird.

Mit der Heimlichkeit der Maßnahme steigt zugleich das Missbrauchspotential. Dass diese Missbrauchsgefahr durchaus real ist, zeigen Fälle aus der Vergangenheit, etwa die heimliche Aufzeichnung (und Transkription) von Telefonsex und Sexgesprächen durch das BKA.[6]

e) Notwendigkeit ungeschlossener Sicherheitslücken

Darüber hinaus schafft § 100b StPO einen Anreiz, Softwareherstellern behördenseitig bekanntgewordene Sicherheitslücken nicht zu melden, weil diese sich dazu veranlasst sehen würden, die für Jedermann exponierte Sicherheitslücke zu schließen und damit

[6] https://www.spiegel.de/netzwelt/netzpolitik/datenschutzbericht-bka-speicherte-per-trojaner-telefonsex-mitschnitte-a-816435.html (Stand: 13.07.2023).

eine Ausnutzung dieser Sicherheitslücke zur Durchführung einer Online-Durchsuchung unmöglich zu machen.

Anders ausgedrückt: § 100b StPO schafft ein staatliches und privates Interesse an der Existenz gravierender Sicherheitslücken und an der Geheimhaltung solcher Sicherheitslücken.

f) Unzureichende Regelungen zum Umgang mit Daten(-massen)

Die besondere Eingriffsintensität der Online-Durchsuchung folgt weiter aus dem Umstand, dass die StPO keine Verfahrensregelungen zum Umgang mit den durch die Online-Durchsuchung erhobenen Daten vorhält. § 110 StPO, der nach seinem Zuschnitt schon nicht auf § 100b StPO, sondern nur auf im Rahmen einer Durchsuchung nach den §§ 102, 103 StPO vorläufig sichergestellten Daten anwendbar sein dürfte, regelt zwar die Zulässigkeit der Durchsicht von Daten, also das „Ob“. Auch hier fehlen jedoch gänzlich Regelungen zur Frage, „wie“ Daten durchgesehen werden dürfen. Dadurch besteht eine erhebliche Rechtsunsicherheit, insbesondere für die Anwaltschaft und sonstige Berufsgeheimnisträger, weil unklar ist, wie und ob überhaupt Vorkehrungen getroffen werden, um besonders geschützte Kommunikationsbeziehungen vor unberechtigten Zugriffen durch die Strafverfolgungsbehörden zu schützen.

Das Fehlen von gesetzlichen Regelungen zum Verfahren bei der Durchsicht von Daten strahlt auf die Frage der Verhältnismäßigkeit von Daten*erhebungen* aus, weil die Durchsicht sich der Online-Durchsuchung naturgemäß anschließt und sich der Eingriff durch die Durchsicht nicht nur perpetuiert, sondern vertieft. Das gilt umso mehr in Fällen, in denen es – wie bei der Online-Durchsuchung – um die Erhebung von Datenmassen geht.

Hinzu kommt, dass eine Selektion der Daten bei der Online-Durchsuchung bei lebensnaher Anschauung erstmalig im Rahmen der Durchsicht – und nicht wie bei der offenen Durchsuchung im Rahmen der Maßnahme an sich – erfolgen wird. Denn es ist für die Strafverfolgungsbehörden wesentlich einfacher, sämtliche Daten auf einem IT-System zu spiegeln, als das IT-System im Wege eines Fernzugriffs zu durchsuchen,

der zudem nur bei aktiver Internetverbindung funktioniert und zudem das Entdeckungsrisiko und das Risiko des Fehlschlags der Maßnahme erhöht.

g) Streubreite

Durch die Online-Durchsuchung werden nicht nur Daten des Nutzers erhoben, sondern regelmäßig auch Daten einer Vielzahl völlig unbeteiligter Personen – vom Arbeitskollegen bis zum Neugeborenen. Die Erhebung von Daten Unbeteiligter dürfte bei der Online-Durchsuchung gerade der Regelfall sein.

3. Verfassungsrechtliche Rechtfertigung

a) Maßstäbe des BVerfG

Mit Urteil vom 27.02.2008 hat der Erste Senat des BVerfG erstmals Maßstäbe für die Zulässigkeit einer präventiven Online-Durchsuchung festgelegt Hierzu heißt es:

> „*Ein derartiger Eingriff darf nur vorgesehen werden, wenn die Eingriffsermächtigung ihn davon abhängig macht, dass tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut vorliegen. Überragend wichtig sind zunächst Leib, Leben und Freiheit der Person. Ferner sind überragend wichtig solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Hierzu zählt etwa auch die Funktionsfähigkeit wesentlicher Teile existenzsichernder öffentlicher Versorgungseinrichtungen.*
>
> *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, die ihm das jeweils anwendbare Fachrecht im präventiven Bereich einräumt*“
>
> (BVerfG NJW 2008, 822, Rz. 247 f.).

Für die Online-Durchsuchung zu Zwecken der Strafverfolgung wurden dagegen bislang noch keine Maßstäbe formuliert. Ob und inwieweit die Maßstäbe zur präventiven Online-Durchsuchung entsprechend herangezogen werden können, ist nicht abschließend geklärt. Vor dem Hintergrund, dass die Online-Durchsuchung im Rahmen der Gefahrenabwehr dazu dient, einen (noch) nicht eingetretenen, aber möglichen Schaden abzuwenden, bei der Online-Durchsuchung zur Strafverfolgung der Schaden jedoch schon eingetreten ist und ein Schutz individualschützender Rechtsgüter durch die Online-Durchsuchung nicht mehr erreicht werden kann, ist jedoch dafür zu plädieren, die dargestellten Maßstäbe zur präventiven Online-Durchsuchung insoweit heranzuziehen, als die repressive Online-Durchsuchung nur zur Verfolgung von Delikten zulässig sein kann, die dem Schutz der dargestellten überragend wichtigen Rechtsgüter dienen.

Ferner sind die zur präventiven Online-Durchsuchung mit Urteil vom 27. Februar 2008 ergangenen Maßstäbe vor dem Hintergrund zu sehen, dass diese zu einem Zeitpunkt formuliert worden sind, zu dem Smartphones gerade erst im Erscheinen und nicht ansatzweise so vernetzt waren wie heute. So wurde das „iPhone“ des Apple-Konzerns erstmals am 29. Juni 2007 und somit gerade einmal etwa ein halbes Jahr vor Veröffentlichung der Entscheidung des Ersten Senats der Weltöffentlichkeit vorgestellt.

Die rasante technologische Entwicklung und die Verbreitung von Smartphones und sonstigen vernetzten Endgeräten wie Cloud-Diensten, Smartwatches, Smarthome- und KI-Anwendungen sowie die Allgegenwärtigkeit von Smartphones im gesellschaftlichen Alltag waren seinerzeit schwer vorhersehbar und drängen daher nach hiesiger Auffassung zu einer restriktiven Anwendung dieser Maßstäbe.

Dies gilt umso mehr vor dem Hintergrund der oben beschriebenen Zunahme der „Datendichte“ sowie wachsender Speicherkapazitäten und Leistungsfähigkeit, zunehmender Vernetzung und der rasant zunehmenden Popularität von Cloud-Diensten, die durch die Auslagerung von Speicherkapazitäten das zu einem Nutzer vorhandene Datenvolumen weiter erhöhen.

b) Verletzung des IT-Grundrechts durch § 100b StPO

Die Regelung des § 100b Abs. 1 StPO verletzt das IT-Grundrecht als Ausprägung des allgemeinen Persönlichkeitsrechts aus Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG. Sie ist insbesondere unverhältnismäßig.

aa) Geeignetheit

Soweit die Beschwerdeführer diesbezüglich bereits auf eine Ungeeignetheit entsprechender Maßnahmen abstellen, verfängt dies allerdings (noch) nicht. Zwar ist dem Vortrag zuzugeben, dass in Hinblick auf die meist schwere Realisierbarkeit der Einhaltung der Grundsätze der Computerforensik in vielen Fällen von einer Schwächung des Beweiswertes entsprechend erhobener Daten auszugehen sein dürfte. Die Absprache jeglichen Beweiswertes wird indes weder der regelmäßigen Spruchpraxis der Fachgerichte noch dem verfassungsrechtlichen Rahmen der Verwendung entsprechender Beweise gerecht. Es existiert keine verfassungsrechtliche oder normative Beweisregel, dass ein Schuldspruch ausschließlich auf (vorhandene) digitale Rohdaten gestützt werden könne (vgl. dazu beispielsweise die Erwägungen in BVerfG, Beschluss vom 20.06.2023 - 2 BvR 1167/20).

bb) Erforderlichkeit

Ähnlich verhält es sich mit dem Vortrag der Beschwerdeführer zur Erforderlichkeit. Selbstverständlich handelt es sich bei der offenen Beschlagnahme und Auswertung informationstechnischer Zielsysteme um eine weniger grundrechtsinvasive Maßnahme. Dieser Vorgehensweise ist als milderes Mittel der Vorrang zu geben, § 100b Abs. 1 Nr. 3 StPO. Dass es sich dabei grundsätzlich um ein *wirksameres* Mittel handeln soll, dürfte den Erfahrungen der kriminalistischen Praxis bei heimlichen Telekommunikationsüberwachungsmaßnahmen entgegenstehen.

cc) Unvereinbarkeit mit Verhältnismäßigkeitsmaßstab des BVerfG

Zunächst sind eine Vielzahl der in § 100b Abs. 2 StPO genannten Straftaten keine Delikte, die in Bedeutung oder Schwere den vom Ersten Senat des BVerfG postulierten Maßstäben gerecht werden würden. Vielmehr wäre § 100b Abs. 2 StPO auf solche Delikte zu beschränken gewesen, die die dort bezeichneten überragend wichtigen Rechtsgüter wie Leib, Leben und Freiheit der Person schützen.
Für einen erheblichen Teil der in § 100b Abs. 2 StPO enthaltenen Delikte wie etwa die Verleitung zur missbräuchlichen Asylantragstellung (Nr. 2 a) dürfte dies nicht zutreffen.

Auch Delikte wie die gewerbsmäßige Hehlerei oder der besonders schwere Fall der Geldwäsche stehen nicht im Einklang mit den vom BVerfG formulierten Maßstäben.

dd) Unzulässige Übertragung des Straftatenkatalogs aus § 100c Abs. 2 StPO a.F.

Die Übertragung des Straftatenkatalogs des § 100c Abs. 2 StPO a.F. ist nicht mit den verfassungsrechtlichen Maßstäben in Einklang zu bringen. Insbesondere ist der Eingriff durch § 100b StPO um ein Vielfaches grundrechtsinvasiver als eine Wohnraumüberwachung nach § 100c StPO.

Dies folgt bereits aus den Maßnahmen selbst. So erlaubt § 100c StPO nur eine *Überwachung* und somit grundsätzlich nur eine Erfassung und Aufzeichnung von Beginn der Anordnung an. § 100b StPO erlaubt dagegen eine (vollständige) Datenerhebung und damit nicht nur eine Live-Überwachung der Nutzung, sondern auch die heimliche und unbeschränkte Beschlagnahme vorhandener Datenbestände. Zudem ist der Zugriff bei § 100c Abs. 1 StPO auf *akustische* Daten und allein auf das Ziel der Erlangung von *Beschuldigtenäußerungen* beschränkt. Heimliche Videoaufzeichnungen von Wohnungen werden durch § 100c Abs. 1 StPO gerade nicht erfasst. § 100b Abs. 1 StPO sieht dagegen keine Beschränkungen im Hinblick auf die Art der Daten und Informationen vor. Namentlich können Dateien in Audio-, Video-, Text-, Bild- und sonstigem Format erhoben werden.

ee) Unzureichende Subsidiaritätsklausel

Die gewählte Subsidiaritätsklausel wird der gegenüber § 100c Abs. 1 StPO deutlich höheren Eingriffstiefe nicht gerecht. Während eine Maßnahme im Sinne von § 100b Abs. 1 StPO lediglich voraussetzt, dass die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten „*auf andere Weise wesentlich erschwert oder aussichtslos wäre*“, steht die Anordnung der akustischen Wohnraumüberwachung i.S.v. § 100a Abs. 1 StPO unter dem (weitergehenden) Vorbehalt, dass dies „*unverhältnismäßig erschwert oder aussichtlos wäre*“. Die Subsidiaritätskonstruktion des § 100b Abs. 1 StPO wird den vom Bundesverfassungsgericht konstituierten Maßstäben nicht gerecht. Angesichts der massiven Eingriffstiefe hätte nur eine mit § 100c Abs. 1 Nr. 4 StPO vergleichbare Ultima-Ratio-Klausel den Vorgaben gerecht werden können.

ff) Fehlendes Erfordernis der Erfolgsaussicht

Darüber hinaus hätte es der Normierung einer mit § 100c Abs. 1 Nr. 3 StPO vergleichbaren Erwartungsklausel bedurft. Während die dortige Voraussetzungskonstruktion vorsieht, dass (neben der absoluten Subsidiarität gegenüber anderen Maßnahmen) „*aufgrund tatsächlicher Anhaltspunkte*“ anzunehmen sein muss, dass durch die Maßnahmen „*Äußerungen des Beschuldigten erfasst werden, die für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Mitbeschuldigten von Bedeutung sind*“, lassen die Anordnungsvoraussetzungen des § 100b Abs. 1 StPO eine solche Anforderung vermissen. Einer solchen Bedingung hätte es aber bei der eingriffsintensiveren Maßnahme des § 100b Abs. 1 StPO bedurft, um die verfassungsrechtliche Rechtfertigung der besonderen Eingriffstiefe zu gewährleisten.

gg) Fehlende Maßnahmen zum Schutz vor Vollüberwachung

Der Gesetzgeber hat versäumt, Regelungen zum Schutz vor einer Komplettüberwachung zu treffen. Wie bereits dargelegt sind Zugriffe gemäß § 100b StPO weder auf Daten aus einem bestimmten Zeitraum noch auf Daten einer bestimmten Gattung zu beschränken. Zudem kann die Online-Durchsuchung ohne Weiteres auf mehrere Endgeräte erstreckt werden.

Zwar kann der Ermittlungsrichter im Rahmen seiner Anordnungskompetenz theoretisch entsprechende Vorgaben machen – dies wird aber mangels ex-ante Kenntnis der genauen technischen Begebenheiten des Zielsystems selten erfolgen können. Auch weiß er zum Zeitpunkt der Anordnung nicht, mit welchen weiteren Endgeräten das zum Gegenstand der Online-Durchsuchung gemachte Endgerät seinerseits verbunden ist.

Da solche Regelungen fehlen, ist die Gefahr einer vollständigen und damit nicht mehr zu rechtfertigen Ausforschung erheblich. Der Gesetzgeber hätte klarere Regelungen zum Schutz vor einer solchen Maßnahmenintensität treffen müssen.

hh) Fehlende Kontrolle durch eine unabhängige Stelle

§ 100b StPO bietet aufgrund des damit einhergehenden umfassenden Datenzugriffs ein erhebliches Missbrauchspotential. Allein der Richtervorbehalt im Hinblick auf die Anordnung der Maßnahme ist nicht geeignet, eine effektive Kontrolle sicherzustellen. Sowohl auf der Ebene der Umsetzung der Maßnahme als auch auf der Ebene der

Auswertung der Daten bedarf es einer unabhängigen und fachkundigen Stelle, die die Rechtmäßigkeit der Maßnahme kontrolliert.

ii) Fehlende Kontrolle der eingesetzten Remote Forensic Software

Der Gesetzgeber hätte klare Regelungen zur Auswahl, Beschaffung und Ausgestaltung der einzusetzenden Remote Forensic Software schaffen müssen. Gegenwärtig ist unklar, welche Software eingesetzt wird und welches Überwachungspotential die Software besitzt. Gerade das neu aufgekommene und vordringliche Phänomens der Künstlichen Intelligenz und die damit einhergehende Möglichkeit der Vernetzung von Informationen gebietet eine entsprechende gesetzliche Regelung
Es fehlen zudem Regelungen, nach welcher Methodik Online-Durchsuchungen rechtmäßig und ohne dauerhafte Schädigung des Zielsystems durchzuführen sind. So bleibt auch die Frage offen, ob, einmal in das IT-System des Betroffenen eingedrungen, auch dessen vernetzte Geräte – wie etwa aktive Cloud-Verbindungen – ebenfalls infiltriert werden dürfen. Sofern dies zu bejahen wäre, würde die Online-Durchsuchung des Smartphones zum digitalen „Superspreader“, weil das Smartphone häufig mit diversen anderen Endgeräten, wie gerade Cloud-Speichern, verbunden ist.

jj) Fehlende Regelungen zur Vorbeugung der Erstellung eines vollständigen Persönlichkeitsprofils

Eine strafprozessuale Online-Durchsuchung setzt klare gesetzliche Regeln zum Umgang mit den erhobenen Daten voraus. Gegenwärtig fehlen Regelungen zur Auswertung umfangreicher Datensätze. Dies wirkt sich auch auf die Datenerhebung aus. Eine Online-Durchsuchung kann – wenn überhaupt – nur verfassungskonform normiert werden, wenn klare Regelung zum Umgang mit Daten geschaffen wurden.

II. Art. 13 Abs. 1 GG: Unverletzlichkeit der Wohnung

§ 100b Abs. 1 StPO lässt technische Maßnahmen zu, die ohne verfassungsrechtliche Rechtfertigung in den Schutzbereich des Art. 13 GG eingreifen.

Das Grundrecht aus Art. 13 GG garantiert die Unverletzlichkeit der Wohnung. Es sichert einen elementaren Lebensraum in Form eines Rückzugsraums, in dem der Einzelne ohne Angst vor Überwachung sich selbst zum Ausdruck bringen kann. Eine staatliche Überwachung innerhalb dieses Schutzraums greift in dieses Grundrecht ein (vgl. BVerfG, Beschluss vom 03.03.2004 - 1 BvR 2378/98).

Im Wege der gem. § 100b Abs. 1 StPO zulässigen fortdauernden Echtzeitüberwachung darf auf Kameramodule zugegriffen werden, die sich innerhalb von grundrechtlich geschützten Wohnungen befinden. Nach der hier vertretenen Auffassung ist zwar kein aktives Aktivieren von Kameras oder Mikrofonen zulässig, in vielen Fällen werden sich in technischen Systemen allerdings automatisch im Hintergrund ohne aktive Ingangsetzung des Nutzers aktive entsprechende Module vorfinden lassen (beispielsweise zur Realisierung von Sprachassistenten und Gesichts- bzw. Iriserkennungen).

Soweit auf diesem Wege eine akustische Wohnraumüberwachung aus der Ferne durch technische Infiltration der an entsprechenden Orten vorhandenen und aktiven IT-technischen Geräte möglich ist, kommt es neben dem Eingriff in das IT-Grundrecht zu einem Eingriff in Art. 13 GG, ohne dass dies in Art. 17 des einführenden Gesetzes benannt wäre und damit gegen Art. 19 Abs. 1 Satz 2 GG verstößt.

Die gleichfalls mögliche visuelle Wohnraumüberwachung aus der Ferne durch technische Infiltration des informationstechnischen Systems ist zu strafprozessualen repressiven Zwecken durch Art. 13 GG ausgeschlossen. Gleichwohl wurde weder eine Erhebungs- noch eine Verwendungsbeschränkung vorgesehen.

Akustische und optische Überwachung sind nicht die einzigen Maßnahmen, die den grundrechtlichen Schutzbereich des Art 13 GG betreffen können. Angesichts der weiten Streubreite von Maßnahmen im Sinne von § 100b Abs. 1 StPO - insbesondere durch die Nutzung weiterer Sensoriken - sind weitere Überwachungsbereiche denkbar, die gleichfalls geeignet sind, in den Schutzbereich der Unverletzlichkeit der Wohnung einzugreifen.

Zur Gewährleistung des Schutzes des Wohnungsgrundrechts hätte es konkret bestimmter Regelungen zur Beschränkung von Maßnahmen im Sinne von § 100b Abs. 1 StPO bedurft, die sich von der Erhebungsstufe über die Durchsichtstufe bis zur Verwertungsstufe erstrecken.

C. § 100d Abs. 1 bis 4 StPO – Kernbereichsschutz

I. Allgemeine Maßstäbe des Bundesverfassungsgerichts

Der verfassungsrechtliche Schutz des Kernbereichs privater Lebensgestaltung gewährleistet dem Individuum einen Bereich höchstpersönlicher Privatheit gegenüber Überwachung. Er wurzelt in den von den jeweiligen Überwachungsmaßnahmen betroffenen Grundrechten in Verbindung mit Art. 1 Abs. 1 GG und sichert einen dem Staat nicht verfügbaren Menschenwürdekern grundrechtlichen Schutzes gegenüber solchen Maßnahmen. Selbst überragende Interessen der Allgemeinheit können einen Eingriff in diesen absolut geschützten Bereich privater Lebensgestaltung nicht rechtfertigen (BVerfGE 141, 220-378, juris Rn. 120; B. v. 09.12.2022 – 1 BvR 1345/21 – juris Rn. 102).

Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung gehört die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen. Geschützt ist insbesondere die nichtöffentliche Kommunikation mit Personen des höchstpersönlichen Vertrauens, die in der berechtigten Annahme geführt wird, nicht überwacht zu werden. Zu diesen Personen gehören insbesondere Ehe- oder Lebenspartner, Geschwister und Verwandte in gerader Linie, vor allem, wenn sie im selben Haushalt leben, und können Strafverteidiger, Ärzte, Geistliche und enge persönliche Freunde zählen. Solche Gespräche verlieren dabei nicht schon dadurch ihren Charakter als insgesamt höchstpersönlich, dass sich in ihnen Höchstpersönliches und Alltägliches vermischen (BVerfGE 141, 220-378, juris Rn. 121; B. v. 09.12.2022 – 1 BvR 1345/21 –, juris Rn. 102).

Der Schutz des Kernbereichs privater Lebensgestaltung ist strikt und darf nicht durch Abwägung mit Sicherheitsinteressen nach Maßgabe des Verhältnismäßigkeitsgrundsatzes relativiert werden. Dies bedeutet zwar nicht, dass jede tatsächliche Erfassung von höchstpersönlichen Informationen stets einen Verfassungsverstoß oder gar eine Menschenwürdeverletzung begründet. Jedoch muss dem Kernbereichsschutz bei der Durchführung von Überwachungsmaßnahmen auf zwei Ebenen Rechnung getragen werden:

Zum einen sind auf der Ebene der **Datenerhebung** Vorkehrungen zu treffen, die nach Möglichkeit ausschließen, dass Kernbereichsinformationen miterfasst werden. Ein Eindringen in den Kernbereich ist zu vermeiden, soweit dies mit praktisch zu bewältigendem Aufwand möglich ist (BVerfGE 141, 220-378, juris Rn. 128). Weiter ist schon auf der Ebene der Datenerhebung der Abbruch der Maßnahme vorzusehen, wenn erkennbar wird, dass eine Überwachung in den Kernbereich privater Lebensgestaltung eindringt (BVerfGE 141, 220-378, juris Rn. 128; B. v. 09.12.2022 – 1 BvR 1345/21 –, juris Rn. 113).

Zum anderen sind auf der Ebene der nachgelagerten **Auswertung und Verwertung** die Folgen eines dennoch erfolgten Eindringens in den Kernbereich privater Lebensgestaltung strikt zu minimieren. Der Gesetzgeber hat für den Fall, dass die Erfassung von kernbereichsrelevanten Informationen nicht vermieden werden konnte, in der Regel die Sichtung der erfassten Daten durch eine unabhängige Stelle vorzusehen, die die kernbereichsrelevanten Informationen vor deren Verwendung durch die Sicherheitsbehörden herausfiltert (BVerfGE 141, 220-378, juris Rn. 129; B. v. 09.12.2022 – 1 BvR 1345/21 –, juris Rn. 117).

II. Entscheidung zu § 20k Abs. 7 BKAG

In der BKAG-Entscheidung vom 20.04.2016 hat der Erste Senat des Bundesverfassungsgerichts entschieden, dass der Kernbereichsschutz für Online-Durchsuchungen in § 20k Abs. 7 BKAG (a.F.) nicht in jeder Hinsicht den verfassungsrechtlichen Anforderungen genügt. § 20k Abs. 7 BKAG (a.F.) lautete:

> *„Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch die Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Soweit möglich, ist technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Erhobene Daten sind unter der Sachleitung des anordnenden Gerichts nach Absatz 5 unverzüglich vom Datenschutzbeauftragten des Bundeskriminalamtes und zwei weiteren Bediensteten des Bundeskriminalamtes, von denen einer die Befähigung zum Richteramt hat, auf kernbereichsrelevante Inhalte durchzusehen. Der Datenschutzbeauftragte ist bei Ausübung dieser Tätigkeit weisungsfrei und darf deswegen nicht benachteiligt werden. Daten, die den Kernbereich privater*

Lebensgestaltung betreffen, dürfen nicht verwertet werden und sind unverzüglich zu löschen. Die Tatsachen der Erfassung der Daten und der Löschung sind zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.“

Das Bundesverfassungsgericht hat festgestellt, dass der heimliche Zugriff auf informationstechnische Systeme typischerweise die Gefahr einer Erfassung auch höchstvertraulicher Daten in sich trägt und damit eine besondere Kernbereichsnähe aufweist. Daher bedürfe es ausdrücklicher gesetzlicher Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung. Die diesbezüglichen Anforderungen seien dabei mit denen der Wohnraumüberwachung nicht in jeder Hinsicht identisch. Der Schutz werde ein Stück weit von der Erhebungsebene auf die nachgelagerte Aus- und Verwertungsebene verschoben. Dies habe seinen Grund in dem spezifischen Charakter des Zugriffs auf informationstechnische Systeme. Schutzmaßnahmen vor Kernbereichsverletzungen zielten hier nicht primär auf die Verhinderung des Erfassens und Festhaltens eines nur flüchtigen, höchstvertraulichen Moments an einem Ort privater Zurückgezogenheit, sondern auf die Verhinderung des Auslesens höchstvertraulicher Informationen aus einem Gesamtdatenbestand von ohnehin digital vorliegenden Informationen, die in ihrer Gesamtheit typischerweise nicht schon als solche den Charakter der Privatheit wie das Verhalten oder die Kommunikation in einer Wohnung aufwiesen. Die Überwachung vollziehe sich hier nicht als ein zeitlich gegliedertes Geschehen an verschiedenen Orten, sondern als Zugriff mittels eines Ausforschungsprogramms, sodass – bezogen auf den Zugriff selbst – weitgehend die Alternativen von ganz oder gar nicht bestehen.

Dementsprechend seien die Anforderungen an den Kernbereichsschutz auf der Erhebungsebene ein Stück weit zurückgenommen. Allerdings sei auch hier vorzusehen, dass die Erhebung von Informationen, die dem Kernbereich zuzuordnen sind, soweit wie informationstechnisch und ermittlungstechnisch möglich unterbleibt. Insbesondere seien verfügbare informationstechnische Sicherungen einzusetzen. Könnten mit deren Hilfe höchstvertrauliche Informationen aufgespürt und isoliert werden, sei der Zugriff auf diese untersagt.

Weiter habe der Gesetzgeber dem Schutzbedarf der Betroffenen durch Sicherungen auf der Aus- und Verwertungsebene Rechnung zu tragen und die Auswirkungen eines solchen Zugriffs zu minimieren. Entscheidende Bedeutung hierfür komme einer Sichtung durch eine unabhängige Stelle zu, die kernbereichsrelevante Informationen vor ihrer Kenntnisnahme und Nutzung durch das Bundeskriminalamt herausfiltere (BVerfGE 141, 220-378, juris Rn. 218 - 220).

Ausgehend von diesem Maßstab hat das Bundesverfassungsgericht § 20k Abs. 7 Satz 1 und 2 sowie Satz 5 bis 7 BKAG (a.F.). als verfassungskonform erachtet. Unzureichend waren dagegen die Vorkehrungen auf der nachgelagerten Ebene des Kernbereichsschutzes. § 20k Abs. 7 Satz 3 und 4 BKAG (a.F.). sehe keine hinreichende unabhängige Kontrolle vor. Die Sichtung der Daten sei im Wesentlichen Bediensteten des Bundeskriminalamtes selbst überlassen. Dass einer der Bediensteten als behördeninterner Datenschutzbeauftragter weisungsfrei ist, ändere daran ebenso wenig wie die Unterstellung der Sichtung unter eine allgemein bleibende „Sachleitung“ des anordnenden Gerichts (BVerfGE 141, 220-378, juris Rn. 225). Verfassungswidrig sei außerdem die übermäßig kurze Dauer für die Aufbewahrung der Löschungsprotokolle gemäß § 20k Abs. 7 Satz 8 BKAG (a.F).

III. Kein ausreichender Kernbereichsschutz auf Erhebungsebene bei § 100b StPO

Wie oben dargelegt, umfasst die Online-Durchsuchung nach § 100b StPO auch die Überwachung des gegenwärtigen Nutzungsverhaltens. Dadurch wird eine Live-Überwachung möglich. Auf diese Weise können z.B. getippte, aber nicht versendete Nachrichten mitgelesen werden. Auch kann auf bereits aktivierte Kameras und Mikrophone zugegriffen werden.

Auf diese Live-Überwachung können die Maßstäbe des Bundesverfassungsgerichts in der BKAG-Entscheidung nicht uneingeschränkt übertragen werden. Der Kernbereichsschutz hat in diesen Fällen – wie bei der akustischen Wohnraumüberwachung – bereits auf Erhebungsebene stattzufinden. Wie bei der Wohnraumüberwachung ermöglicht die Online-Live-Überwachung das Erfassen und Festhalten „eines nur flüchtigen, höchstvertraulichen Moments an einem Ort privater Zurückgezogenheit“ (vgl. BVerfGE 141, 220-378, juris Rn. 218). Die Online-

Durchsuchung ist daher zu unterbrechen, wenn das gegenwärtig überwachte Nutzungsverhalten Anhaltspunkte liefert, dass kernbereichsrelevante Inhalte betroffen sind (z.B. Chats oder Videounterhaltungen mit Vertrauenspersonen).

§ 100d Abs. 3 StPO sieht – anders als § 100d Abs. 4 Satz 2 StPO – eine entsprechende Regelung zum Abbruch bzw. Unterbrechung der Online-Durchsuchung nicht vor. Insoweit genügt die Regelung den verfassungsrechtlichen Maßstäben zum Schutz des Kernbereichs privater Lebensgestaltung nicht (so auch: Grözinger, Die Überwachung von Cloud-Storage, S. 310).

Die übrigen, von den Beschwerdeführern geltend gemachten verfassungsrechtlichen Bedenken greifen hingegen nicht durch.

Die Beschwerdeführer wenden insbesondere ein, auf Erhebungsebene beschränke sich der Kernbereichsschutz nach § 100d Abs. 3 Satz 1 StPO darauf, „soweit technisch möglich“ sicherzustellen, dass kernbereichsrelevante Daten nicht erhoben werden. Bislang sei dies technisch jedoch unmöglich. Die Einschränkung laufe in der Praxis leer (Verfassungsbeschwerde, S. 63). Die Wirksamkeit der gesetzlichen Regelung sei von künftigen technischen Entwicklungen abhängig. Der Gesetzgeber hätte sicherstellen müssen, dass die Verpflichtung – soweit in Zukunft technisch möglich – eingehalten wird. Dazu hätte es einer Dokumentationspflicht sowie einer Kontrollpflicht durch eine unabhängige Stelle bedurft (Verfassungsbeschwerde, S. 63).

Demgegenüber hat das Bundesverfassungsgericht in seiner BKAG-Entscheidung § 20k Abs. 7 Satz 2 BKAG (a.F.) für verfassungsmäßig erachtet (BVerfGE 141, 220-378, juris Rn. 219, 222). Die Regelung ist nahezu wortgleich mit § 100d Abs. 3 Satz 1 StPO. Auch das Zugriffsverbot auf „allein“ kernbereichsrelevante Daten wurde nicht beanstandet (BVerfGE 141, 220-378, juris Rn. 222). Auch insoweit greift die Verfassungsbeschwerde nicht durch (vgl. Verfassungsbeschwerde, S. 61).

Dass die Regelung mangels technischer Möglichkeiten aktuell leerlaufen mag, macht sie nicht verfassungswidrig. Ob oder wie sich durch technische Maßnahmen sicherstellen lässt, dass ausschließlich die laufende Telekommunikation überwacht und aufgezeichnet wird, betrifft die Anwendung der Norm, nicht aber ihre Gültigkeit. Im

Übrigen ist nicht ausgeschlossen, dass die nötigen technischen Voraussetzungen in absehbarer Zukunft geschaffen werden können (BVerfGE 141, 220-378, juris Rn. 234). Die Online-Durchsuchung schließt es jedenfalls nicht denklogisch aus, dass durch bestimmte Softwareprogramme kernbereichsrelevante Daten ausgeschlossen oder minimiert werden. Denkbar sind z.B. Voreinstellungen, wonach auf Chat-Programme nicht zugegriffen werden kann oder der Zugriff auf Unterhaltungen mit einzelnen, ermittlungsrelevanten Personen beschränkt wird.

IV. Kein ausreichender Kernbereichsschutz auf Auswertungsebene bei § 100b StPO

Nach § 100d Abs. 3 Satz 2 StPO sind Erkenntnisse einer Online-Durchsuchung, die den Kernbereich privater Lebensgestaltung betreffen, unverzüglich zu löschen oder von der Staatsanwaltschaft dem anordnenden Gericht zur Entscheidung über die Verwertbarkeit und Löschung der Daten vorzulegen.

In seiner BKAG-Entscheidung verlangt das Bundesverfassungsgericht ausdrücklich die Sichtung durch eine unabhängige Stelle. Dies diene maßgeblich dem Ziel, kernbereichsrelevante Daten so frühzeitig herauszufiltern, dass sie den Sicherheitsbehörden nach Möglichkeit nicht offenbart werden (BVerfGE 141, 220-378, juris Rn. 224).

Dem wird § 100d Abs. 3 Satz 2 StPO nicht gerecht. Die Regelung geht davon aus, dass sich die Ermittlungsbehörden zunächst selbst ein Bild davon machen, *ob* kernbereichsrelevante Daten im Rahmen der Online-Durchsuchung erhoben wurden. Davon ist in der Regel auszugehen. Anschließend haben die Ermittlungsbehörden zwei Möglichkeiten, *wie* sie mit diesen kernbereichsrelevanten Daten umgehen. Sie können sie entweder selbst löschen oder sie können sie zur weiteren Entscheidung dem anordnenden Gericht vorlegen.

Die Vorlage an das anordnende Gericht ist nicht zu beanstanden. Dabei handelt es sich um eine unabhängige Stelle. Allerdings gewährleistet § 100d Abs. 3 Satz 2 StPO nicht die unabhängige Sichtung „*aller* aus der Online-Durchsuchung gewonnenen Daten“ (so ausdrücklich: BVerfGE 162, 1-178, juris Rn. 315). Dem Gericht werden nur die Daten vorgelegt, die die Ermittlungsbehörde zuvor als kernbereichsrelevant einstuft. Erforderlich ist eine Regelung, wonach alle erhobenen Daten aus der Online-

Durchsuchung unverzüglich dem anordnenden Gericht vorzulegen sind, damit dieses die Daten auf kernbereichsrelevante Inhalte überprüfen kann (vgl. die Formulierung in § 20k BKAG (a.F.), die insoweit über § 100d Abs. 3 Satz 2 StPO hinausgeht).

Aus der in der Gesetzesbegründung (BT-Drs. 18/12785) zitierten Fundstelle (BVerfGK 11, 164-178, juris Rn. 65) ergibt sich nichts anderes. Diese Entscheidung betrifft die akustische Wohnraumüberwachung. Diese ist mit Blick auf ihre Eingriffsintensität mit der Online-Durchsuchung nicht vergleichbar. Insbesondere findet bei der akustischen Wohnraumüberwachung der Kernbereichsschutz maßgeblich auf Erhebungsebene statt, während er bei der Online-Durchsuchung auf die Auswertungsebene verlagert wird (BVerfGE 141, 220-378, juris Rn. 218). Bei der akustischen Wohnraumüberwachung kann auf Erhebungsebene dafür gesorgt werden, dass die Überwachung abgebrochen wird, wenn der Kernbereich privater Lebensgestaltung betroffen ist. Die Ermittlungsbehörden wissen bereits während des Erhebungsvorgangs, ob sie (versehentlich) kernbereichsrelevante Daten „miterhoben“ haben. Über deren Verwertbarkeit muss dann das anordnende Gericht entscheiden. Bei der Online-Durchsuchung wird in den meisten Fällen zunächst ein Datensatz unbekannten Inhalts erhoben. Die Ermittlungsbehörden wissen im Erhebungszeitpunkt meist nicht, ob es sich um kernbereichsrelevante Daten handelt. Dies herauszufinden muss Aufgabe einer unabhängigen Stelle sein.

V. Bindungswirkung der gerichtlichen Entscheidung bei § 100b StPO

Nach § 100d Abs. 3 Satz 3 StPO ist die Entscheidung des Gerichts über die Verwertbarkeit für das weitere Verfahren bindend.

Der Wortlaut der Norm lässt eine Bindungswirkung nicht nur für das Ermittlungsverfahren, sondern auch für das Haupt- und Rechtsmittelverfahren zu. Damit wäre die falsche gerichtliche Entscheidung über die Verwertbarkeit von vermeintlich nicht kernbereichsrelevanten Daten vom Tatgericht sowie vom Rechtsmittelgericht zu beachten. Das ist verfassungsrechtlich bedenklich. Werden kernbereichsrelevante Daten zu Unrecht als verwertbar eingestuft, liegt ein Verstoß gegen den Schutz des Kernbereichs privater Lebensgestaltung vor. Dies begründet einen Eingriff in das unantastbare Grundrecht der Menschenwürde nach Art. 1 Abs. 1 GG. Die Menschenwürde gilt uneingeschränkt. Sie kann nicht mit der durch § 100d Abs. 3 Satz

3 StPO bezweckten Rechtssicherheit und Rechtsklarheit abgewogen werden. Es muss dem Tatgericht und dem Rechtsmittelgericht möglich sein, einen erst später erkannten Verstoß gegen Art. 1 Abs. 1 GG „rückgängig“ zu machen, indem Daten aus dem Kernbereich privater Lebensgestaltung nicht verwertet werden, auch wenn sie vom anordnenden Gericht (rechtskräftig) als verwertbar eingestuft wurden (so auch: Rückert, in: MüKoStPO, 2. Aufl. 2023, § 100d Rn. 22, m.w.N.).

Der Deutsche Anwaltsverein hält eine verfassungskonforme Auslegung des § 100d Abs. 3 Satz 3 StPO nicht für möglich. Würde man den Begriff „Verfahren“ dahingehend auslegen, dass damit nur das weitere Ermittlungsverfahren gemeint ist, würde dies auch die Fälle umfassen, in denen das Gericht die Kernbereichsrelevanz bejaht und die Verwertung untersagt hat. Diese Entscheidung sollte keinesfalls rückgängig gemacht werden können.

§ 100d Abs. 3 Satz 3 StPO ist daher so zu fassen, dass die Entscheidung des Gerichts über die Verwertbarkeit für das weitere Verfahren bindend ist, soweit die Verwertbarkeit abgelehnt wurde.

VI. Kernbereichsschutz bei Quellen-TKÜ

Sofern man die unter F. I. 2. B) aa) (1) und (2) dargestellte Rechtsansicht vertritt, eine Quellen-TKÜ erlaube eine Überwachung des Surfverhaltens und/oder eine Überwachung des (automatisierten) Datenaustauschs zwischen Endgerät und Cloud, bedarf es einer Sonderregelung zum Schutz des Kernbereichs bei der Erhebung und Auswertung von Daten. Hierzu hatte der DAV mit Stellungnahme 33/2022 wie folgt ausgeführt:

> „*In der Entscheidung zum BKA-Gesetz vom 20. April 2016 hat der 1. Senat des Bundesverfassungsgerichts klargestellt, dass jenseits der Online-Durchsuchung bei der Telekommunikationsüberwachung keine kategorische Pflicht zur Prüfung durch eine unabhängige Stelle bestehe (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 240; vgl. bereits BVerfG, Beschluss vom 12. Oktober 2011 – 2 BvR 236/08 u.a. –; Rn. 224). Allerdings hat der 1. Senat offenbar vor allem die Überwachung einzelner Akte unmittelbarer (mündlicher) Kommunikation (mit Vertrauenspersonen) im Blick gehabt (BVerfG, Urteil vom 20. April 2016 – 1 BvR*

966/09, 1 BvR 1140/09 –, Rn. 238, 241). Insoweit hat der 1. Senat eine Möglichkeit gesehen, dass bereits auf der Erhebungsstufe eine Prüfung erfolgt, die die Erfassung höchstprivater Gespräche verhindert (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 239). Zudem hat der 1. Senat eindeutig Folgendes erklärt:

„Erlaubt der Gesetzgeber in dieser Weise auch die Erhebung von Informationen, für die Zweifel bestehen können, ob sie dem Kernbereich privater Lebensgestaltung unterfallen, bedarf es für solche Aufzeichnungen dann aber auch der Sichtung durch eine unabhängige Stelle.“ (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 241).

Seit dem Urteil des 1. Senats aus April 2016 haben sich die Rahmenbedingungen signifikant verändert. So hat u.a. die 3. Kammer des 2. Senats des Bundesverfassungsgerichts im Juli 2016 die fachgerichtliche Entscheidung des LG Ellwangen, dass vom Telekommunikationsbegriff des § 100a StPO auch das Surfen im Internet bzw. das Verwenden einer Suchmaschine („Googlen“) erfasst sei, als verfassungsrechtlich vertretbar eingestuft (BVerfG, Beschluss vom 6. Juli 2016 – 2 BvR 1454/13 –). In Anwendung dieser Rechtsprechung kann eine Telekommunikationsüberwachung neben dem klassischen Telefonat, dem Mitlesen von E-Mails und privaten Chats auch eine vollständige Überwachung der privaten oder gar intimen Internetnutzung erfassen. Die moderne Telekommunikationsüberwachung dient nur zum Teil der Überwachung (mündlichen) Kommunikationsverhaltens, sondern wird in der Praxis regelmäßig auch zur Überwachung des Datenstroms von Mobiltelefonen und Computern eingesetzt. Damit erfasst die Telekommunikationsüberwachung im Wesentlichen gerade die besonders sensiblen Verhaltensweisen, die der 1. Senat noch im April 2016 als für die Online-Durchsuchung typusprägend eingestuft hat („Nach- oder Mitverfolgen der Bewegungen im Internet, Erschließen von geheim gehaltenen Schwächen und Neigungen; vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 –, Rn. 238.). Hinzu kommt, dass bei der Überwachung derartiger Datenströme ein effektiver Kernbereichsschutz auf Ebene der Erhebung regelmäßig ausgeschlossen ist. […]

Diese neuen bzw. gerichtlich neu eingeräumten Möglichkeiten der Auslegung der Vorschriften zur Telekommunikationsüberwachung führen dazu, dass die vom 1. Senat geschilderte Situation eingetreten ist (insb. keine Möglichkeit der Prüfung der Kernbereichsrelevanz auf Erhebungsebene) und eine Sichtung durch eine unabhängige Stelle geboten ist. Dem DAV ist bewusst, dass das Erfordernis der Einbindung einer unabhängigen Stelle im Bereich der (präventiven und repressiven) Telekommunikationsüberwachung mit signifikanten praktischen Hürden für Polizei- und Strafverfolgungsbehörden einhergehen würde. Angesichts der signifikanten Ausweitung behördlicher Befugnisse im Bereich der Telekommunikationsüberwachung ist eine verfassungsrechtliche Einhegung indes, wie der 1. Senat bereits im Grundsatz festgestellt hat, geboten. Die Einbindung einer unabhängigen Stelle ist zumindest dann verfassungsrechtlich zwingend, sofern im Rahmen einer Telekommunikationsüberwachung nicht nur das mündlich gesprochene Wort überwacht wird. Hier ist ein Kernbereichsschutz auf Erhebungsebene regelmäßig nicht umsetzbar.“

Diese zur präventiven Quellen-TKÜ gemachten Ausführungen gelten auch für die repressive Quellen-TKÜ.

D. § 100d Abs. 5 StPO – Schutz zeugnisverweigerungsberechtigter Personen

Die Beschwerdeführer wenden sich ferner gegen § 100d Abs. 5 StPO. Die Rüge ist unbegründet und daher zurückzuweisen.

I. Uneinheitliche Regelung zum Schutz von zeugnisverweigerungsberechtigten Personen

Der Gesetzgeber hat die Chance verpasst, eine einheitliche und klare Regelung zum Schutz zeugnisverweigerungsberechtigter Personen bei Ermittlungsmaßnahmen zu treffen. Insofern ist den Beschwerdeführern darin beizupflichten, dass ein Vergleich des § 100d Abs. 5 StPO mit anderen Normen der StPO ein uneinheitliches Regelungsgefüge zum Schutz zeugnisverweigerungsberechtigter Personen offenbart.

Bei der Online-Durchsuchung und der akustischen Wohnraumüberwachung gilt ein Erhebungsverbot für die Kommunikation des Beschuldigten mit Berufsgeheimnisträgern nach § 53 StPO (§ 100d Abs. 5 StPO). Ein absoluter Schutz von

Berufsgeheimnisträgern ist auch für die Erhebung von Verkehrsdaten vorgesehen (§ 100g Abs. 4 StPO); dieses besondere Erhebungsverbot gilt aber ausdrücklich nur für die Abfrage von Verkehrsdaten nach § 100g Abs. 2 StPO und damit nicht für solche nach § 100g Abs. 1 StPO. Für Maßnahmen nach § 100g Abs. 1 StPO und auch für alle anderen Ermittlungsmaßnahmen gilt wiederum die Generalklausel des § 160a StPO. § 160a Abs. 1 und 2 StPO statuieren Erhebungsverbote nur für einen Teil der Berufsgeheimnisträger und für die dieser Gruppe zuzuordnenden Berufshelfer nach § 53a StPO. Insoweit sind die Berufshelfer stärker geschützt als nach § 100d Abs. 5 StPO. Für alle übrigen Berufsgeheimnisträger (und deren Berufshelfer) sieht § 160a Abs. 3 StPO ein abwägungsoffenes (relatives) Beweiserhebungs- und Beweisverwertungsverbot vor. Im Rahmen der §§ 100b, 100c StPO werden demgegenüber sämtliche Berufshelfer nur durch ein relatives Beweisverwertungsverbot geschützt.

Diese unklare Gesetzeslage wurde bereits im Rahmen des Gesetzgebungsverfahrens 2017 bemängelt und war schon damals nicht neu.[7] Mit der Verabschiedung der Generalklausel des § 160a StPO war ein erster Versuch zur Vereinheitlichung der Regelungen unternommen worden[8], der aber im Hinblick auf die Maßnahmen nach §§ 100b und 100c StPO durch die spezielle Regelung des § 100d Abs. 5 StPO letztlich nicht vollendet wurde.

Die Regelung überzeugt zudem auch deshalb nicht, da ein uneinheitlicher Schutz von Berufsgeheimnisträgern und ihrer Berufshelfer tatsächliche Gegebenheiten und Arbeitsläufe ignoriert und damit letztlich den absoluten Schutz der Berufsgeheimnisträger relativiert (*eingehend unten II.2*).

II. Keine Überschreitung des verfassungsrechtlichen Gestaltungsspielraums

Dem Gesetzgeber steht im Hinblick auf den Schutz zeugnisverweigerungsberechtigter Personen allerdings ein weiter Gestaltungsspielraum zu[9], den er in noch verfassungsmäßiger Weise ausfüllt. Die konkrete Ausgestaltung mag regelungstechnisch unglücklich und die Differenzierung zwischen

[7] Vgl. Überblick zur Kritik bei Löwe-Rosenberg/*Hauck*, 27. Auflage 2019, Rn. 56ff.; so auch: Bundesanwalt b. BGH *Krauss*, Stellungnahme zum Gesetzentwurf zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze, 2017, S. 12.; S. schon zur Vorgängerregelung § 100c Abs. 6 StPO: *Löffelmann*, Das Gesetz zur Umsetzung des Urteils des Bundesverfassungsgerichts vom 3. März 2004 (akustische Wohnraumüberwachung), ZIS 2006, 87, 94.
[8] Vgl. BT-Drucks 16/5846, S. 34 f.; 16/6979 S. 43 (damals noch als § 53b StPO-E aufgeführt).
[9] BVerfGE 141, 220, Rn. 133.

Berufsgeheimnisträgern und ihren Berufshelfern nicht überzeugend sein. Gleichwohl ist der Gesetzgeber verfassungsrechtlich nicht verpflichtet, alle Zeugnisverweigerungsberechtigten im Rahmen heimlicher Überwachungsmaßnahmen dem gleichen (absoluten) Schutz zu unterwerfen.

Das Bundesverfassungsgericht hat im Jahr 2007 die Vereinbarkeit des § 100c Abs. 6 StPO aF im Hinblick auf die akustische Wohnraumüberwachung für mit dem Grundgesetz vereinbar erklärt.[10] Die Regelung wurde vom Gesetzgeber 2017 wortgleich übernommen und auch auf die Online-Durchsuchung erstreckt. Für eine verfassungsrechtliche Neubewertung dürfte heute kein Anlass bestehen.

Insofern ist die Anordnung von Ermittlungsmaßnahmen gegen Berufshelfer verfassungsrechtlich nicht zu beanstanden. Auch im Übrigen wahrt der Gesetzgeber die verfassungsrechtlichen Grenzen.

1. Kein verfassungsrechtliches Gebot des absoluten Schutzes von Zeugnisverweigerungsberechtigten

Der Gesetzgeber hat Regelungen zum Schutz zeugnisverweigerungsberechtigter Personen im Rahmen von Ermittlungsmaßnahmen vorzusehen.[11] Dabei stellt das Bundesverfassungsgericht den absoluten Schutz der Zeugnisverweigerungsberechtigten aber in einen engen Zusammenhang mit dem Kernbereichsschutz[12]. Eingriffe in den Kernbereich privater Lebensgestaltung müssen vermieden werden (*eingehend oben* unter C.). Ein gewichtiges Indiz für die Kernbereichsrelevanz eines Gesprächsinhalts oder einer Kommunikation ist die *"Anwesenheit von Personen des höchstpersönlichen Vertrauens"*.[13] Insbesondere bei einem Zugriff auf die Kommunikation mit Berufsgeheimnisträgern und anderen nach §§ 52, 53a StPO zeugnisverweigerungsberechtigten Personen besteht eine hohe Wahrscheinlichkeit, dass kernbereichsrelevante Erkenntnisse erlangt werden. Diese Erkenntnis muss sich auch in der Regelung der Anordnungsbefugnis widerspiegeln.

Allerdings: *"Die aus dem Kernbereich privater Lebensgestaltung folgenden Abhörverbotes sind nicht identisch mit den in §§ 52 und 53 StPO genannten*

[10] BVerfG, Beschluss vom 11. Mai 2007 – 2 BvR – 543/06; näher hierzu, s. unten.
[11] BVerfGE 141, 220, Rn. 131.; zuvor bereits BVerfGE 109, 279, 321 ff.
[12] BVerfGE 109, 279, 321 ff
[13] BVerfGE 109, 279, 321.

Zeugnisverweigerungsberechtigten".[14] Soweit also der Kontakt zwischen einem Betroffenen und einer zeugnisverweigerungsberechtigten Person den unantastbaren Kernbereich privater Lebensgestaltung berührt, muss ein Eingriff vermieden werden; darüber hinaus besteht aber kein absoluter Schutz aller Zeugnisverweigerungsberechtigten im Rahmen von Ermittlungsmaßnahmen.[15]

Vielmehr muss der Gesetzgeber im Übrigen einen angemessenen Ausgleich zwischen dem Schutz der Berufsgeheimnisträger und dem verfassungsrechtlichen Gebot einer effektiven Strafverfolgung, dem Interesse an einer möglichst vollständigen Wahrheitsermittlung im Strafverfahren und dem staatlichen Auftrag zur effektiven Aufklärung gerade schwerer Straftaten finden.[16] Auch das Gebot der effektiven Strafverfolgung genießt Verfassungsrang. Der Gesetzgeber ist daher sogar verpflichtet, Sachgründe für seine Entscheidung vorzubringen, will er dem Schutz der Zeugnisverweigerungsberechtigten den Vorrang einzuräumen. [17]

2. Ausgestaltung des Schutzes von Berufshelfern ist verfassungsgemäß

Dieser Linie folgend nahm das Bundesverfassungsgericht im Jahr 2007 eine Verfassungsbeschwerde unter anderem gegen die mit § 100d Abs. 5 StPO nahezu wortgleiche Vorschrift des § 100c Abs. 6 StPO[18] nicht zur Entscheidung an.[19] Die Nichtannahmeentscheidung begründete das Bundesverfassungsgericht ausführlich und stellte dabei die Vereinbarkeit der Vorschrift mit dem Grundgesetz fest.[20]

Das Bundesverfassungsgericht hielt insbesondere § 100c Abs. 6 S. 2 StPO, also den nur *"relativen Schutz"* der Zeugnisverweigerungsberechtigten nach §§ 52, 53a StPO, für verfassungsgemäß.[21] Die Gespräche mit Zeugnisverweigerungsberechtigten seien entgegen der Auffassung der Beschwerdeführer keineswegs schutzlos und der Kernbereichsschutz stehe nicht zur Abwägung. Vielmehr seien die Gespräche mit Zeugnisverweigerungsberechtigten bereits vom (allgemeinen) Kernbereichsschutz des

[14] BVerfGE 109, 279, 323.
[15] BVerfGE 141, 220, Rn 132; 129, 208, 259.
[16] BVerfGE 141, 220, Rn 131 ff.
[17] BVerfGE 129, 208, 260.
[18] S. bereits oben Fn. 4.
[19] BVerfG, Beschluss vom 11. Mai 2007 – 2 BvR – 543/06; insb. Rn. 33.
[20] Einige Jahre zuvor hatte das Bundesverfassungsgericht wiederum die Vorgängerregelung zu § 100c Abs. 6 StPO aF, damals noch § 100d Abs. 3 StPO für verfassungswidrig erklärt, da der Gesetzgeber nur unzureichend Eingriffe in den Kernbereich verhindert habe. Daraufhin war dem Gesetzgeber bis zum 30. Juni 2005 aufgegeben worden, eine neue Regelung zu treffen. Dies erfolgte durch das Gesetz zur Umsetzung des Urteils von 3. März 2004, das unter anderem die Vorschrift des 2007 zur Entscheidung gestellten § 100c Abs.6 StPO einführte.
[21] BVerfG, Beschluss vom 11. Mai 2007 – 2 BvR – 543/06, Rn. 20.

§ 100c Abs. 4 StPO aF erfasst. § 100c Abs. 6 StPO regelte *"ergänzend"* ein absolutes Beweiserhebungsverbot für Berufsgeheimnisträger nach § 53 StPO und ein Beweisverwertungsverbot für Gespräche mit Zeugnisverweigerungsberechtigten nach §§ 52, 53a StPO. Insofern sollte *"§ 100c Abs. 6 Satz 2 StPO [...] - eine zulässige Abhörmaßnahme vorausgesetzt - auch den Interessen der durch Zeugnisverweigerungsrechte geschützten Personen Rechnung tragen".*[22]

Die Differenzierung zwischen dem Schutz von Berufshelfern und Angehörigen einerseits und Berufsgeheimnisträgern andererseits hielt das Bundesverfassungsgericht hingegen nicht für bedenklich. Vielmehr betonte das Bundesverfassungsgericht den weiten Gestaltungsspielraum des Gesetzgebers und ging auf die Frage des unterschiedlichen Schutzniveaus von Berufsgeheimnisträgern und Berufshelfern nicht weiter ein.[23]

Mit der Neuregelung im Jahr 2017 wurde die Regelung des § 100c Abs. 6 StPO übernommen und auf die Online-Durchsuchung erstreckt (s. § 100d Abs. 5 StPO). Anlass zu einer anderen verfassungsrechtlichen Bewertung des heutigen § 100d Abs. 5 StPO ergibt sich daraus nicht.

Es bleibt jedoch erneut anzumerken, dass im Zuge der Neuregelung die ursprüngliche Regelung des § 100c Abs. 4 und 5 StPO aF, die den Kernbereichsschutz für die akustische Wohnraumüberwachung vorsah, gerade nicht auf die Online-Durchsuchung übertragen wurde. Dies ist mehr Frage des Kernbereichsschutzes nach § 100d Abs. 1 bis 4 StPO (siehe oben unter C.) und wurde an dieser Stelle bereits ausführlich diskutiert.

3. Strenge Anforderungen an die Verwertung von Erkenntnissen aus der Kommunikation mit Berufshelfern

In der Praxis erfolgt die Kommunikation mit – absolut vor Maßnahmen nach den §§ 100b und 100c StPO geschützten – Berufsgeheimnisträgern allerdings regelmäßig (auch) über etwaige Berufshelfer (wie Sekretariate, Übersetzungsdienste etc.).[24] Wenn

[22] BVerfG, Beschluss vom 11. Mai 2007 – 2 BvR – 543/06, Rn. 52.
[23] BVerfG, Beschluss vom 11. Mai 2007 – 2 BvR – 543/06, vgl. Rn. 42, 45, 54.
[24] Vgl. auch Verfassungsbeschwerde, S. 65.

für den Zugriff auf Berufshelfer niedrigere Schwellen gelten, relativiert dies insgesamt auch den absoluten Schutz der Berufsgeheimnisträger.

Dem ist bei der Entscheidung über die Verwertbarkeit von Erkenntnissen aus Maßnahmen nach den §§ 100b und 100c StPO Rechnung zu tragen. Insbesondere ist § 100d Abs. 5 StPO so auszulegen, dass die Verwertbarkeit der aus der Überwachung von Berufshelfern gewonnenen Erkenntnisse unter dem Vorbehalt umfassender verfassungsrechtlicher Garantien steht. Dies gilt insbesondere, soweit durch die Maßnahme die Religionsfreiheit (Art. 4 Abs. 1 GG), die Pressefreiheit (Art. 5 Abs. 1 GG) und die Berufsfreiheit (Art. 12 Abs. 1 GG), die Rechtsschutzgarantie (Art. 19 Abs. 4 GG) oder die Freiheit des Mandats (At. 38 Abs. 1 GG) betroffen sind.[25]

4. Auch im Übrigen bestehen keine verfassungsrechtlichen Bedenken

Auch über die Rügen der Beschwerdeführer hinaus bestehen gegen § 100d Abs. 5 StPO keine durchgreifenden verfassungsrechtlichen Bedenken.

Offen bleibt die Frage, ob unter den Berufsgeheimnisträgern nach § 53 StPO eine Differenzierung dadurch erfolgt, dass § 100d Abs. 5 StPO insgesamt auf die "*Fälle des § 53*" verweist[26], also auch auf die Einschränkungen für Presseangehörige bei der Ausübung ihres Zeugnisverweigerungsrechts in § 53 Abs. 1 S. 2, Abs. 2 S. 2 StPO. Bei einem solchen Verständnis der Vorschrift unterliegen Presseangehörige im Ergebnis (nur) einem relativen Beweisverwertungsverbot.[27] Dies ist aber letztlich eine Frage der Auslegung des einfachen Rechts und bedarf hier keiner Klärung.

Ein verfassungsrechtliches Gebot, Presseangehörige einem absoluten Schutz zu unterstellen, besteht nicht.[28] Ein solcher Anspruch auf umfassenden Schutz vor heimlichen Ermittlungsmaßnahmen folgt insbesondere nicht aus Art. 5 Abs. 1 Satz 2 GG.[29] Die Medienfreiheit ist nicht abstrakt vorrangig gegenüber dem staatlichen Interesse an der Strafverfolgung.[30]

---

[25] BVerfGE 141, 220, 131 ff.
[26] Bei § 100c Abs. 6 StPO aF hieß es demgegenüber noch *"in den Fällen des § 53 Abs. 1",* s. oben.
[27] Vgl. *Buermeyer*, Gutachterliche Stellungnahme zur Öffentlichen Anhörung zur „Formulierungshilfe" des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKÜ im Strafprozess, 2017, S. 23 f.
[28] BVerfGE 141, 220, Rn. 256.
[29] Vgl. BVerfGE 107, 299, 332 f.
[30] BVerfGE 77, 65, 75 f.

Die Differenzierung zwischen dem Schutz von Berufsgeheimnisträgern und Berufshelfern verstößt überdies auch nicht gegen den allgemeinen Gleichheitssatz des Art. 3 Abs.1 GG. Die Differenzierung ist im Hinblick auf die tatsächlichen Arbeitsvorgänge zwar praxisfremd. Die Grenze einer sachwidrigen Ungleichbehandlung wird dadurch indes nicht überschritten sein. Das Bundesverfassungsgericht räumt dem Gesetzgeber gerade den Spielraum ein, bei verdeckten Ermittlungsmaßnahmen zwischen Berufshelfern und Berufsgeheimnisträgern zu unterscheiden.[31]

[31] S. eingehend II., BVerfGE 141, 220, Rn. 133.