Leitsätze

zum Beschluss des Ersten Senats vom 24. Juni 2025

- 1 BvR 180/23 -

Trojaner II

1. Eine Befugnis zur Überwachung und Aufzeichnung laufender Telekommunikation in der Weise, dass mit technischen Mitteln in von Betroffenen eigengenutzte IT-Systeme eingegriffen wird (Quellen-Telekommunikationsüberwachung, vgl. § 100a Abs. 1 Satz 2 StPO), begründet einen sehr schwerwiegenden Eingriff sowohl in das IT-System-Grundrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) als auch in das durch Art. 10 Abs. 1 GG geschützte Fernmeldegeheimnis.

2. a) Eine Befugnis zur Überwachung und Aufzeichnung der auf einem IT-System Betroffener gespeicherten Inhalte und Umstände der Kommunikation in der Weise, dass mit technischen Mitteln in ein IT-System eingegriffen wird (erweiterte Quellen-Telekommunikationsüberwachung, vgl. § 100a Abs. 1 Satz 3 StPO), ist allein am IT-System-Grundrecht zu messen.

   b) Das Recht auf informationelle Selbstbestimmung schützt nicht nur vor einzelnen Datenerhebungen, sondern auch vor dem Zugriff auf große und dadurch typischerweise besonders aussagekräftige Datenbestände. Ermächtigt aber eine Norm zur Datenerhebung aus einem IT-System, auf das mit technischen Mitteln zugegriffen wird, wird das Recht auf informationelle Selbstbestimmung vom IT-System-Grundrecht verdrängt.

   c) Von diesen beiden Ausprägungen des allgemeinen Persönlichkeitsrechts gewährleistet das IT-System-Grundrecht einen gegenüber dem Recht auf informationelle Selbstbestimmung spezifischen Schutz, der gerade die mit dem Zugriff auf eigengenutzte IT-Systeme verbundene Verletzung ihrer Integrität und Gefährdung der Vertraulichkeit in den Blick nimmt.

3. Eine Befugnisnorm, die dazu ermächtigt, heimlich mit technischen Mitteln in ein von Betroffenen genutztes IT-System einzugreifen und daraus Daten zu erheben, die auch solche der laufenden Fernkommunikation umfassen (Online-Durchsuchung), ermöglicht Eingriffe sowohl in das IT-System-Grundrecht als auch in Art. 10 Abs. 1 GG. Sind beide Grundrechte betroffen, ist die Befugnis zur Online-Durchsuchung an beiden Grundrechten zu messen.

BUNDESVERFASSUNGSGERICHT

- 1 BvR 180/23 -

IM NAMEN DES VOLKES

In dem Verfahren
über
die Verfassungsbeschwerde

1. des Herrn (...),
2. des Herrn (...),
3. des Herrn (...),
4. des Herrn (...),
5. der Frau (...),

- Bevollmächtigte: (...) -

gegen § 100a Absatz 1 Sätze 2 und 3, Absätze 3 bis 6, § 100b sowie § 100d Absätze 1 bis 3 und 5 der Strafprozessordnung (StPO) in der Fassung des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017 (Bundesgesetzblatt I Seite 3202 ff.)

hat das Bundesverfassungsgericht – Erster Senat –

unter Mitwirkung der Richterinnen und Richter

Präsident Harbarth,
Ott,
Christ,
Radtke,
Härtel,
Wolff,
Eifert,
Meßling

am 24. Juni 2025 beschlossen:

1. § 100a Absatz 1 Sätze 2 und 3 in Verbindung mit § 100a Absatz 1 Satz 1 Nummer 1, Absatz 2 Nummer 1 Buchstaben a, c, d und t, Nummer 6 und Nummer 7 Buchstabe b der Strafprozessordnung in der Fassung des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017 (Bundesgesetzblatt I Seite 3202) und in der Fassung späterer Gesetze verstoßen nach Maßgabe der Gründe gegen Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes sowie – nur bezogen auf § 100a Absatz 1 Satz 2 der Strafprozessordnung – auch gegen Artikel 10 Absatz 1 des Grundgesetzes und sind nichtig.

2. § 100b der Strafprozessordnung in der Fassung des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017 und in der Fassung späterer Gesetze ist mit Artikel 10 Absatz 1 in Verbindung mit Artikel 19 Absatz 1 Satz 2 des Grundgesetzes unvereinbar. Die Vorschrift gilt bis zu einer Neuregelung fort.

3. Im Übrigen wird die Verfassungsbeschwerde zurückgewiesen.

4. Die Bundesrepublik Deutschland hat den Beschwerdeführenden zu 1) und 5) ein Drittel, den Beschwerdeführenden zu 2) und 4) ein Sechstel ihrer notwendigen Auslagen aus dem Verfassungsbeschwerdeverfahren zu erstatten.

G r ü n d e :

A.

Gegenstand der Verfassungsbeschwerde sind strafprozessuale Ermächtigungen zur Quellen-Telekommunikationsüberwachung und zur Online-Durchsuchung. 1

I.

Die Beschwerdeführenden wenden sich mit ihrer Verfassungsbeschwerde gegen § 100a Abs. 1 Sätze 2 und 3, Absätze 3 bis 6, § 100b sowie § 100d Absätze 1 bis 3 und 5 StPO in der Fassung des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017 (BGBl I S. 3202), das mit Wirkung zum 24. August 2017 in Kraft getreten ist. Die Vorschriften lauten in ihrer angegriffenen Fassung wie folgt: 2

§ 100a StPO - Telekommunikationsüberwachung

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

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

[2]Die Überwachung und Aufzeichnung der Telekommunikation darf auch in der Weise erfolgen, dass mit technischen Mitteln in von dem Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen. [3]Auf dem informationstechnischen System des Betroffenen gespeicherte Inhalte und Umstände der Kommunikation dürfen überwacht und aufgezeichnet werden, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können.

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

1. aus dem Strafgesetzbuch:
   a) Straftaten des Friedensverrats, des Hochverrats und der Gefährdung des demokratischen Rechtsstaates sowie des Landesverrats und der Gefährdung der äußeren Sicherheit nach den §§ 80a bis 82, 84 bis 86, 87 bis 89a, 89c Absatz 1 bis 4, 94 bis 100a,
   b) Bestechlichkeit und Bestechung von Mandatsträgern nach § 108e,

c) Straftaten gegen die Landesverteidigung nach den §§ 109d bis 109h,

d) Straftaten gegen die öffentliche Ordnung nach den §§ 129 bis 130,

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

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

g) Verbreitung, Erwerb und Besitz kinder- und jugendpornographischer Schriften nach § 184b Absatz 1 und 2, § 184c Absatz 2,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. aus der Abgabenordnung:

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

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

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

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

4. aus dem Asylgesetz:

a) Verleitung zur missbräuchlichen Asylantragstellung nach § 84 Abs. 3,

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

5. aus dem Aufenthaltsgesetz:

a) Einschleusen von Ausländern nach § 96 Abs. 2,

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

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

7. aus dem Betäubungsmittelgesetz:

a) Straftaten nach einer in § 29 Abs. 3 Satz 2 Nr. 1 in Bezug genommenen Vorschrift unter den dort genannten Voraussetzungen,

b) Straftaten nach den §§ 29a, 30 Abs. 1 Nr. 1, 2 und 4 sowie den §§ 30a und 30b,

8. aus dem Grundstoffüberwachungsgesetz:

Straftaten nach § 19 Abs. 1 unter den in § 19 Abs. 3 Satz 2 genannten Voraussetzungen,

9. aus dem Gesetz über die Kontrolle von Kriegswaffen:

a) Straftaten nach § 19 Abs. 1 bis 3 und § 20 Abs. 1 und 2 sowie § 20a Abs. 1 bis 3, jeweils auch in Verbindung mit § 21,

b) Straftaten nach § 22a Abs. 1 bis 3,

9a. aus dem Neue-psychoaktive-Stoffe-Gesetz:

Straftaten nach § 4 Absatz 3 Nummer 1 Buchstabe a,

10. aus dem Völkerstrafgesetzbuch:

a) Völkermord nach § 6,

b) Verbrechen gegen die Menschlichkeit nach § 7,

c) Kriegsverbrechen nach den §§ 8 bis 12,

d) Verbrechen der Aggression nach § 13,

11. aus dem Waffengesetz:

a) Straftaten nach § 51 Abs. 1 bis 3,

b) Straftaten nach § 52 Abs. 1 Nr. 1 und 2 Buchstabe c und d sowie Abs. 5 und 6.

(3) Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss oder ihr informationstechnisches System benutzt.

(4) [1]Auf Grund der Anordnung einer Überwachung und Aufzeichnung der Telekommunikation hat jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt, dem Gericht, der Staatsanwaltschaft und ihren im Polizeidienst tätigen Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) diese Maßnahmen zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen. [2]Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, bestimmt sich nach dem Telekommunikationsgesetz und der Telekommunikations-Überwachungsverordnung. [3]§ 95 Absatz 2 gilt entsprechend.

(5) [1]Bei Maßnahmen nach Absatz 1 Satz 2 und 3 ist technisch sicherzustellen, dass

1. ausschließlich überwacht und aufgezeichnet werden können:

a) die laufende Telekommunikation (Absatz 1 Satz 2), oder

b) Inhalte und Umstände der Kommunikation, die ab dem Zeitpunkt der Anordnung nach § 100e Absatz 1 auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz hätten überwacht und aufgezeichnet werden können (Absatz 1 Satz 3),

2. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und

3. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.

[2]Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. [3]Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(6) Bei jedem Einsatz des technischen Mittels sind zu protokollieren

1. die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,

2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,

3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und
4. die Organisationseinheit, die die Maßnahme durchführt.

§ 100b StPO - Online-Durchsuchung

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

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

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

1. aus dem Strafgesetzbuch:
   a) Straftaten des Hochverrats und der Gefährdung des demokratischen Rechtsstaates sowie des Landesverrats und der Gefährdung der äußeren Sicherheit nach den §§ 81, 82, 89a, 89c Absatz 1 bis 4, nach den §§ 94, 95 Absatz 3 und § 96 Absatz 1, jeweils auch in Verbindung mit § 97b, sowie nach den §§ 97a, 98 Absatz 1 Satz 2, § 99 Absatz 2 und den §§ 100, 100a Absatz 4,
   b) Bildung krimineller Vereinigungen nach § 129 Absatz 1 in Verbindung mit Absatz 5 Satz 3 und Bildung terroristischer Vereinigungen nach § 129a Absatz 1, 2, 4, 5 Satz 1 erste Alternative, jeweils auch in Verbindung mit § 129b Absatz 1,
   c) Geld- und Wertzeichenfälschung nach den §§ 146 und 151, jeweils auch in Verbindung mit § 152, sowie nach § 152a Absatz 3 und § 152b Absatz 1 bis 4,
   d) Straftaten gegen die sexuelle Selbstbestimmung in den Fällen des § 176a Absatz 2 Nummer 2 oder Absatz 3 und, unter den in § 177 Absatz 6 Satz 2 Nummer 2 genannten Voraussetzungen, des § 177,
   e) Verbreitung, Erwerb und Besitz kinderpornografischer Schriften in den Fällen des § 184b Absatz 2,
   f) Mord und Totschlag nach den §§ 211, 212,
   g) Straftaten gegen die persönliche Freiheit in den Fällen der §§ 234, 234a Absatz 1, 2, der §§ 239a, 239b und Menschenhandel nach § 232 Absatz 3, Zwangsprostitution und Zwangsarbeit nach § 232a Absatz 3, 4 oder 5 zweiter Halbsatz, § 232b Absatz 3 oder 4 in Verbindung mit § 232a Absatz 4 oder 5 zweiter Halbsatz und Ausbeutung unter Ausnutzung einer Freiheitsberaubung nach § 233a Absatz 3 oder 4 zweiter Halbsatz,

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

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

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

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

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

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

2. aus dem Asylgesetz:

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

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

3. aus dem Aufenthaltsgesetz:

a) Einschleusen von Ausländern nach § 96 Absatz 2,

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

4. aus dem Betäubungsmittelgesetz:

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

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

5. aus dem Gesetz über die Kontrolle von Kriegswaffen:

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

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

6. aus dem Völkerstrafgesetzbuch:

a) Völkermord nach § 6,

b) Verbrechen gegen die Menschlichkeit nach § 7,

c) Kriegsverbrechen nach den §§ 8 bis 12,

d) Verbrechen der Aggression nach § 13,

7. aus dem Waffengesetz:

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

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

(3) [1]Die Maßnahme darf sich nur gegen den Beschuldigten richten. [2]Ein Eingriff in informationstechnische Systeme anderer Personen ist nur zulässig, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass

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

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

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

§ 100d StPO - Kernbereich privater Lebensgestaltung; Zeugnisverweigerungsberechtigte

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

(2) [1]Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach den §§ 100a bis 100c erlangt wurden, dürfen nicht verwertet werden. [2]Aufzeichnungen über solche Erkenntnisse sind unverzüglich zu löschen. [3]Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren.

(3) [1]Bei Maßnahmen nach § 100b ist, soweit möglich, technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. [2]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. [3]Die Entscheidung des Gerichts über die Verwertbarkeit ist für das weitere Verfahren bindend.

(4) [...]

(5) [1]In den Fällen des § 53 sind Maßnahmen nach den §§ 100b und 100c unzulässig; ergibt sich während oder nach Durchführung der Maßnahme, dass ein Fall des § 53 vorliegt, gilt Absatz 2 entsprechend. [2]In den Fällen der §§ 52 und 53a dürfen aus Maßnahmen nach den §§ 100b und 100c gewonnene Erkenntnisse nur verwertet werden, wenn dies unter Berücksichtigung der Bedeutung des zugrunde liegenden Vertrauensverhältnisses nicht außer Verhältnis zum Interesse an der Erforschung des Sachverhalts oder der

Ermittlung des Aufenthaltsortes eines Beschuldigten steht. [3]§ 160a Absatz 4 gilt entsprechend.

II.

1. Mit dem Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017 wurden erstmals die Rechtsgrundlagen für eine Quellen-Telekommunikationsüberwachung (§ 100a Abs. 1 Sätze 2 und 3 StPO) und eine Online-Durchsuchung (§ 100b Abs. 1 StPO) in der Strafprozessordnung geschaffen. Nach der Begründung des Gesetzentwurfs sollen die neuen Befugnisse die Effizienz der Strafverfolgung steigern und dadurch eine funktionstüchtige Strafrechtspflege gewährleisten. Aufgrund der fortschreitenden Entwicklung der Informationstechnik sei festzustellen, dass informationstechnische Systeme (im Folgenden: IT-Systeme) allgegenwärtig seien und ihre Nutzung für die Lebensführung der meisten Bürger von zentraler Bedeutung sei. Dies gelte vor allem für die Nutzung mobiler Geräte in Form von Smartphones oder Tablet-PCs. Deren Leistungsfähigkeit sei ebenso gestiegen wie die Kapazität ihrer Arbeitsspeicher und der mit ihnen verbundenen Speichermedien, bei denen es sich immer häufiger um externe Speicher in sogenannten Clouds handele. Das Internet öffne Nutzern den Zugriff auf eine Fülle von Informationen und stelle zahlreiche neuartige Kommunikationsdienste zur Verfügung. Herkömmliche Formen der Fernkommunikation würden in weitem Umfang auf das Internet verlagert (vgl. BTDrucks 18/12785, S. 46). Aufgrund ihrer weiten Verbreitung spielten IT-Systeme daher auch eine wichtige Rolle bei der Aufklärung von Straftaten. 3

Die bisherige Regelung des § 100a StPO genüge insoweit nicht. Sie enthalte zwar eine Rechtsgrundlage zur Erhebung derjenigen Kommunikationsinhalte, die während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz überwacht und aufgezeichnet werden könnten. Nachdem inzwischen aber ein Großteil der Kommunikation internetprotokollbasiert erfolge und zahlreiche „Voice-over-IP"- und Messenger-Dienste die Kommunikationsinhalte mit einer Verschlüsselung versähen, würden den Ermittlungsbehörden oft nur noch verschlüsselte Daten geliefert. Deren Entschlüsselung sei entweder nicht möglich oder aber sehr langwierig und kostenintensiv. Eine effektive Strafverfolgung müsse sich diesen technischen Veränderungen stellen und ihre Ermittlungsmaßnahmen dem technischen Fortschritt anpassen (vgl. BTDrucks 18/12785, S. 48). Mit der Quellen-Telekommunikationsüberwachung und der Online-Durchsuchung sollten daher Überwachungstechniken in die Strafprozessordnung eingeführt werden, die zur Gefahrenabwehr bereits zulässig seien (vgl. BTAusschussdrucks 18<6>334, A). Mit beiden Maßnahmen könne auf die Kommunikation schon „an der Quelle", das heiße vor der Verschlüsselung beim Absender oder nach der Entschlüsselung beim Empfänger, durch eine verdeckt installierte Software Zugriff genommen werden (vgl. BTDrucks 18/12785, S. 48 f.). Mit einer Online-Durchsuchung könnten zudem auch alle auf einem IT-System gespeicherten Inhalte sowie das gesamte Nutzungsverhalten einer Person überwacht werden (vgl. BTDrucks 18/12785, S. 54). 4

2. § 100a Abs. 1 Sätze 2 und 3 und § 100b Abs. 1 StPO erlauben zum Zweck der Strafverfolgung eine heimliche Überwachung von IT-Systemen. 5

a) Während die herkömmliche Telekommunikationsüberwachung (§ 100a Abs. 1 Satz 1 StPO) das heimliche Überwachen und Aufzeichnen von Telekommunikation insbesondere unter Einbezug derjenigen ermöglicht, die Telekommunikationsdienste erbringen oder daran mitwirken (aa), erfolgt mit der Quellen-Telekommunikationsüberwachung ein Zugriff auf das IT-System selbst. Dabei unterscheiden die beiden hier angegriffenen Befugnisse zur Quellen-Telekommunikationsüberwachung danach, ob über den Zugriff auf das IT-System laufende Telekommunikation (§ 100a Abs. 1 Satz 2 StPO) (bb) oder auf dem System gespeicherte, vormals laufende Telekommunikation (§ 100a Abs. 1 Satz 3 StPO) (cc) überwacht und aufgezeichnet werden soll. 6

aa) § 100a Abs. 1 Satz 1 StPO erlaubt die heimliche Überwachung und Aufzeichnung der Telekommunikation der Betroffenen, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in § 100a Abs. 2 StPO genannte schwere Straftat begangen, zu begehen versucht oder durch eine Straftat vorbereitet hat (vgl. § 100a Abs. 1 Satz 1 Nr. 1 StPO). Die Tat muss auch im Einzelfall schwer wiegen und die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsorts des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos sein (§ 100a Abs. 1 Satz 1 Nummern 2 und 3 StPO). Nach § 100a Abs. 3 StPO darf sich die Anordnung einer Überwachung nur gegen Beschuldigte oder gegen Personen richten, von denen aufgrund bestimmter Tatsachen anzunehmen ist, dass sie für Beschuldigte bestimmte oder von diesen herrührende Mitteilungen entgegennehmen oder weitergeben (sog. Nachrichtenmittler) oder dass Beschuldigte ihren Anschluss oder ihr IT-System benutzen (sog. Anschluss- oder Endgeräteüberlasser). Nach § 100a Abs. 4 StPO ist jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt, auf Anordnung verpflichtet, eine Überwachungsmaßnahme zu ermöglichen und die erforderlichen Auskünfte zu erteilen, also die überwachten Kommunikationsinhalte und -umstände an die Ermittlungsbehörden auszuleiten. 7

Beschränkungen hinsichtlich der Art der Telekommunikation enthält die Vorschrift nicht. In der Praxis leiten die verpflichteten Diensteanbieter nach den hier vorliegenden Stellungnahmen (vgl. Rn. 65, 68, 80) den gesamten Rohdatenstrom aus. Umfasst sind nicht nur Inhalte und Umstände der Telekommunikation zwischen Personen, sondern alle über das Internet transportierten Daten (vgl. zur Fernmeldeaufklärung des BND BVerfGE 154, 152 <181 Rn. 10> – BND – Ausland-Ausland-Fernmeldeaufklärung), wobei ein Großteil der Inhalte des Rohdatenstroms verschlüsselt und daher praktisch nicht lesbar ist (vgl. BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 8 – Trojaner I; vgl. die Stellungnahmen der Bundesregierung, unten Rn. 65, der Bayerischen Staatsregierung und der Landesregierung Schleswig-Holstein, unten Rn. 68, sowie des Generalbundesanwalts, unten Rn. 80). 8

bb) Die Quellen-Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 2 StPO ermächtigt unter den Voraussetzungen nach § 100a Abs. 1 Satz 1, Abs. 3 StPO zur Überwachung und Aufzeichnung der Telekommunikation auch in der Weise, dass mit technischen Mitteln in von Betroffenen genutzte IT-Systeme eingegriffen wird. Die Überwachung erfolgt mit dem Ziel, auch solche Inhalte einer Kommunikation zu erfassen, die bei einer bloßen Telekommunikationsüberwachung aufgrund ihrer Verschlüsselung nicht oder jedenfalls nicht mit praktisch vertretbarem Aufwand ausgewertet werden können. Der Zugriff darf in solchen Fällen vor der Verschlüsselung beim Sendegerät oder nach der Entschlüsselung beim Empfangsgerät erfolgen. Zu diesem Zweck darf die Polizei mit technischen Mitteln in das von der betroffenen Person genutzte IT-System eingreifen; erlaubt ist insbesondere der Einsatz einer Überwachungssoftware (sog. Trojaner; vgl. BTDrucks 18/12785, S. 48 f.). Ein Systemeingriff darf aber nur erfolgen, wenn durch technische Maßnahmen sichergestellt ist, dass ausschließlich die laufende Telekommunikation überwacht und aufgezeichnet wird (vgl. § 100a Abs. 5 Satz 1 Nr. 1 Buchstabe a StPO). Auch muss der Eingriff in das System gemäß § 100a Abs. 1 Satz 2 StPO notwendig sein, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen. Die Anordnung einer Quellen-Telekommunikationsüberwachung ist insoweit subsidiär (vgl. auch BTDrucks 18/12785, S. 51). 9

Nach § 100a Abs. 5 Satz 1 Nummern 2 und 3 StPO sind Veränderungen an dem IT-System auf das für die Datenerhebung Unerlässliche zu beschränken und nach Beendigung der Maßnahme, soweit technisch möglich, wieder automatisiert rückgängig zu machen. § 100a Abs. 6 StPO regelt die bei jedem Einsatz technischer Mittel geltenden Protokollierungspflichten. Damit sollen nach Vorstellung des Gesetzgebers die notwendigen Vorkehrungen geschaffen werden, um die nachträgliche Überprüfung einer durchgeführten Maßnahme zu gewährleisten. Dies soll einen effektiven Grundrechtsschutz der Betroffenen und die Gerichtsfestigkeit der erhobenen Beweise sicherstellen (vgl. BTDrucks 18/12785, S. 53). Insbesondere soll dadurch die Prüfung ermöglicht werden, ob eine Software verwendet wurde, die den Anforderungen des § 100a Abs. 5 Satz 1 Nr. 1 Buchstabe b StPO genügt (vgl. BTDrucks 18/12785, S. 52). Darüber hinaus besteht ein Prüfungsrecht des behördlichen Datenschutzbeauftragten sowie der Bundesdatenschutzbeauftragten im Rahmen ihrer gesetzlichen Kompetenzen (vgl. BTDrucks 18/12785, S. 52). 10

Nach der Begründung des Gesetzentwurfs darf der Zugriff auf ein IT-System in Form der Aufbringung einer Überwachungssoftware grundsätzlich nur auf technischem Wege oder mittels kriminalistischer List erfolgen; die Befugnis zur Quellen-Telekommunikationsüberwachung umfasse nicht das zu diesem Zweck heimliche Betreten der Wohnung (vgl. BTDrucks 18/12785, S. 52). 11

Eine Quellen-Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 2 StPO erfasst – wenngleich in lesbarer Form – technisch und rechtlich die gleichen Daten wie eine 12

„klassische“ Telekommunikationsüberwachung (vgl. Rn. 8) und damit nach den hier vorliegenden Stellungnahmen der Äußerungsberechtigten und sachkundigen Dritten den gesamten ein- und ausgehenden Datenstrom des überwachten Endgeräts (vgl. Rn. 65, 68, 80).

cc) Die Quellen-Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 3 StPO ermächtigt unter den Voraussetzungen nach § 100a Abs. 1 Satz 1, Abs. 3 StPO dagegen zur Überwachung und Aufzeichnung der auf dem IT-System Betroffener gespeicherten Inhalte und Umstände der Kommunikation, und zwar ebenfalls in der Weise, dass mit technischen Mitteln in ein IT-System eingegriffen wird. Nach der Vorstellung des Gesetzgebers ergänzt § 100a Abs. 1 Satz 3 StPO eine Quellen-Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 2 StPO insoweit, als auch auf solche Inhalte und Umstände einer Kommunikation zugegriffen werden darf, bei denen der Übertragungsvorgang bereits abgeschlossen ist und die auf dem IT-System der Betroffenen in einer Anwendung noch gespeichert sind (vgl. BTDrucks 18/12785, S. 51). Der staatliche Zugriff ist damit von einem unmittelbaren Übertragungsvorgang losgelöst, wobei aber nach § 100a Abs. 5 Satz 1 Nr. 1 Buchstabe b StPO sicherzustellen ist, dass ausschließlich Inhalte und Umstände einer Kommunikation überwacht werden können, die ab dem Zeitpunkt der richterlichen Anordnung auch während des laufenden Übertragungsvorgangs hätten überwacht werden können (vgl. auch BTDrucks 18/12785, S. 51 f.). Mit der auf gespeicherte Daten erweiterten Quellen-Telekommunikationsüberwachung will der Gesetzgeber den Ermittlungsbehörden ermöglichen, technische Schwierigkeiten bei der Vollziehung der Quellen-Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 2 StPO auszugleichen, weil nach deren Anordnung ein gewisser Zeitraum bis zum Beginn der Überwachung verstreichen kann. Durch § 100a Abs. 1 Satz 3 StPO sollen also einzig Kommunikationsdaten, die bis zu diesem Zeitpunkt anfallen, ausgeleitet werden können (vgl. BTDrucks 18/12785, S. 51 f.; Hauck, in: Löwe-Rosenberg, StPO, 27. Aufl. 2019, § 100a Rn. 140, 142). 13

Eine Quellen-Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 3 StPO erfasst daher ausschließlich Inhalte und Umstände einer Kommunikation, die nach Anordnung der Maßnahme angefallen und zum Zeitpunkt des Zugriffs noch gespeichert sind (vgl. auch Rn. 235). Flüchtige, nicht gespeicherte Kommunikationsinhalte etwa eines Telefongesprächs können nicht ausgeleitet werden (vgl. dazu Stellungnahme der GDD, Rn. 98). 14

b) Die Online-Durchsuchung nach § 100b Abs. 1 StPO erlaubt es, in ein von Betroffenen genutztes IT-System einzugreifen und daraus Daten zu erheben, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in § 100b Abs. 2 StPO genannte besonders schwere Straftat begangen oder zu begehen versucht hat (vgl. § 100b Abs. 1 Nr. 1 StPO). Dabei muss die Tat auch im Einzelfall besonders schwer wiegen und die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsorts des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos sein (vgl. § 100b Abs. 1 15

Nummern 2 und 3 StPO). Die Anordnung einer Online-Durchsuchung ist daher subsidiär; vor ihrer Durchführung ist etwa zu prüfen, ob nicht eine offene Durchsuchung und Beschlagnahme in Betracht kommen (vgl. BTDrucks 18/12785, S. 55). Nach § 100b Abs. 4 StPO gelten § 100a Absätze 5 und 6 StPO mit Ausnahme von § 100a Abs. 5 Satz 1 Nr. 1 StPO entsprechend (vgl. dazu Rn. 10).

Eine Online-Durchsuchung darf sich nach § 100b Abs. 3 StPO grundsätzlich nur gegen Beschuldigte richten. Ein Eingriff in IT-Systeme anderer Personen ist nur zulässig, wenn aufgrund bestimmter Tatsachen anzunehmen ist, dass Beschuldigte deren IT-Systeme benutzen und die Durchführung des Eingriffs in IT-Systeme der Beschuldigten allein nicht zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsorts von Mitbeschuldigten führen wird. Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden (vgl. § 100b Abs. 3 Satz 3 StPO). 16

Im Gegensatz zur Quellen-Telekommunikationsüberwachung ermöglicht die Online-Durchsuchung einen Zugriff auf das gesamte IT-System. Das Nutzungsverhalten einer Person einschließlich der Inhalte und Umstände laufender Kommunikation sowie alle dort gespeicherten Daten werden vollständig erfasst. Zentrales gesetzgeberisches Anliegen ist es, die Nutzung des Systems umfassend zu überwachen und seine Speichermedien auszulesen (vgl. BTDrucks 18/12785, S. 47, 54). 17

c) Der Schutz des Kernbereichs privater Lebensgestaltung und der Schutz von Vertrauensverhältnissen, aus denen Zeugnisverweigerungsrechte folgen können, werden in verschiedenen Vorschriften geregelt. 18

aa) § 100d Absätze 1 bis 4 StPO enthalten Vorgaben zum Schutz des Kernbereichs privater Lebensgestaltung. Nach § 100d Abs. 1 StPO dürfen insbesondere Maßnahmen nach §§ 100a, 100b StPO nicht durchgeführt werden, sofern tatsächliche Anhaltspunkte vorliegen, dass hierdurch allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden. Nach der Begründung des Gesetzentwurfs kann ein solcher ausschließlicher Kernbereichsbezug vor allem angenommen werden, wenn Betroffene mit Personen in Kontakt treten, zu denen sie in einem besonderen, den Kernbereich betreffenden Vertrauensverhältnis stehen – wie engsten Familienangehörigen, Geistlichen, Telefonseelsorgenden, Strafverteidigerinnen und Strafverteidigern oder im Einzelfall auch Ärztinnen und Ärzten (vgl. BTDrucks 18/12785, S. 56). Soweit ein derartiges Vertrauensverhältnis für Ermittlungsbehörden erkennbar ist, dürfen Maßnahmen nicht durchgeführt werden. Allein der Umstand, dass eine Maßnahme auch Tatsachen mit erfassen kann, die den Kernbereich berühren, ist dagegen unbeachtlich. Werden Erkenntnisse aus dem Kernbereich erlangt, dürfen sie nicht verwertet werden; Aufzeichnungen sind unverzüglich zu löschen und sowohl deren Erlangung als auch die Löschung zu dokumentieren (vgl. § 100d Abs. 2 StPO). 19

Im Fall einer Online-Durchsuchung ist nach § 100d Abs. 3 StPO darüber hinaus schon auf der Erhebungsebene technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Entsprechende Erkenntnisse, die dennoch erlangt werden, sind unverzüglich zu löschen oder dem anordnenden Gericht zur Entscheidung über die Verwertbarkeit und Löschung der Daten vorzulegen. 20

bb) Der Schutz von Vertrauensverhältnissen, aus denen Zeugnisverweigerungsrechte folgen können (§§ 52 ff. StPO), ist an unterschiedlichen Stellen geregelt. 21

Für die Telekommunikations- und Quellen-Telekommunikationsüberwachung nach § 100a StPO sind die allgemeinen Vorschriften anwendbar. So leitet die Praxis aus § 148 StPO für die Kommunikation zwischen Beschuldigten und Verteidigern ein absolutes Erhebungsverbot ab. Gleichwohl erlangte Erkenntnisse dürfen nicht gegen Beschuldigte verwertet werden (vgl. etwa BGHSt 53, 257 <261 f. Rn. 13 f.>; Kämpfer/Travers, in: Münchener Kommentar zur StPO, 2. Aufl. 2023, § 148 Rn. 19, 26). Eine Verwertung in Strafverfahren gegen Verteidiger ist zwar denkbar, aber aufgrund des hiermit einhergehenden Eingriffs in die Berufsfreiheit anhand des Einzelfalls zu beurteilen (vgl. BVerfG, Beschluss der 2. Kammer des Zweiten Senats vom 20. Mai 2010 - 2 BvR 1413/09 -, Rn. 8 ff.). Daneben sieht § 160a StPO bei beruflich zeugnisverweigerungsberechtigten Personen und ihren Berufshelfern Erhebungs- sowie Verwertungsbeschränkungen vor, die nach der konkret in Rede stehenden Gruppe von Berufsgeheimnisträgern differenzieren. 22

Online-Durchsuchungen nach § 100b StPO werden ebenfalls durch §§ 148, 160a StPO begrenzt (vgl. Rückert, in: Münchener Kommentar zur StPO, 2. Aufl. 2023, § 100b Rn. 72 ff.). Darüber hinaus sieht § 100d Abs. 5 Satz 1 StPO vor, dass Maßnahmen in den Fällen eines gemäß § 53 StPO bestehenden Zeugnisverweigerungsrechts von beruflich Geheimnisverpflichteten unzulässig sind; eine Online-Durchsuchung darf sich daher etwa nicht gegen Verteidiger richten, sofern diese nicht selbst im Verdacht stehen, in die Tat oder ein Anschlussdelikt verstrickt zu sein (vgl. § 100d Abs. 5 Satz 3 i.V.m. § 160a Abs. 4 StPO). Gleichwohl erlangte Erkenntnisse aus der Kommunikation mit Berufsgeheimnisträgern unterliegen einem umfassenden Verwertungsverbot (vgl. § 100d Abs. 5 Satz 1 Halbsatz 2 i.V.m. § 100d Abs. 2 StPO). § 100d Abs. 5 Satz 2 StPO sieht schließlich in „den Fällen der §§ 52 und 53a“ (Angehörige von Beschuldigten, Berufshelfern) ein relatives, abwägungsgebundenes Beweisverwertungsverbot vor. 23

d) Maßnahmen nach § 100a StPO unterliegen nach § 100e Abs. 1 Satz 1 StPO einem Richtervorbehalt. Die Anordnung ist auf höchstens drei Monate zu befristen und darf um jeweils nicht mehr als drei Monate verlängert werden (vgl. § 100e Abs. 1 Sätze 4 und 5 StPO). Eine Online-Durchsuchung nach § 100b StPO darf nur von der in § 74a Abs. 4 GVG genannten Kammer des Landgerichts angeordnet werden und ist auf höchstens einen Monat zu befristen; eine Verlängerung ist um jeweils einen Monat zulässig, wobei nach einer 24

Verlängerung auf insgesamt sechs Monate eine weitere Verlängerung nur durch das Oberlandesgericht angeordnet werden darf (vgl. § 100e Abs. 2 StPO).

3. Der Gesetzgeber hat die §§ 100a, 100b StPO seit August 2017 mehrfach geändert. Die Änderungen betreffen ausschließlich die Kataloge der Anlassstraftaten in § 100a Abs. 2 und § 100b Abs. 2 StPO. §§ 100d, 100e StPO sind unverändert geblieben. 25

III.

Die Beschwerdeführenden wenden sich gegen die strafprozessualen Befugnisse zur Quellen-Telekommunikationsüberwachung und Online-Durchsuchung (§ 100a Abs. 1 Sätze 2 und 3, § 100b Abs. 1 StPO) einschließlich der sie flankierenden Regelungen in § 100a Absätze 3 bis 6, § 100b Absätze 2 bis 4 und § 100d Absätze 1 bis 3 und 5 StPO. Sie rügen eine Verletzung von Art. 1 Abs. 1, Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 (Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme), Art. 10 Abs. 1, Art. 13 Abs. 1 und Art. 19 Abs. 4 GG. 26

1. Die Beschwerdeführenden seien durch die angegriffenen Befugnisse selbst, gegenwärtig und unmittelbar betroffen. 27

Der Beschwerdeführer zu 1) sei unter anderem Rechtsanwalt, investigativer Journalist und Kuratoriumsmitglied der Internationalen Liga für Menschenrechte. In den Jahren 1970 bis 2008 sei er wegen unterstellter Kontakte zu „linksextremistischen" beziehungsweise „linksextremistisch beeinflussten" Personen und Gruppierungen durch das Bundesamt für Verfassungsschutz wegen behaupteter verfassungsfeindlicher Bestrebungen heimlich beobachtet worden. Als Rechtsanwalt und Journalist stehe er in Kontakt zu potentiellen Zielpersonen einer Überwachung nach § 100a Abs. 1 Sätze 2 und 3, § 100b Abs. 1 StPO. 28

Der Beschwerdeführer zu 2) kommuniziere als Rechtsanwalt und Strafverteidiger täglich mit Personen, denen schwere und schwerste Straftaten vorgeworfen würden, sowie mit deren Familienangehörigen. Verfahrensrelevante Daten übermittele und speichere er auf den von ihm (und seinen Berufshelfern) genutzten informationstechnischen Geräten, die er auch für private Belange nutze. 29

Der Beschwerdeführer zu 3) trete unter seinem Künstlernamen „(...)" auf. Sein Anliegen sei es, Menschen digital zu „ermündigen". Seit vielen Jahren betreibe er zudem mit der Beschwerdeführerin zu 5) einen Tor-Server, der es seinen Nutzern ermögliche, im Internet anonym zu bleiben. Dies nutzten auch Kriminelle aus. In Zusammenhang mit beiden Tätigkeiten sei er bereits mehrfach auch schwerster Straftaten beschuldigt und Hausdurchsuchungen unterworfen worden. 30

Der Beschwerdeführer zu 4) sei unter anderem Rechtsanwalt, Strafverteidiger, Honorarprofessor, Autor und Herausgeber. Als Bürgerrechtler und beruflich habe er mit Personen zu tun, gegen die sich Maßnahmen nach § 100a Abs. 1 Sätze 2 und 3, § 100b Abs. 1 StPO richten könnten. 31

Die Beschwerdeführerin zu 5) sei Mitglied im Vorstand des (...) e.V. In dieser Funktion recherchiere und erhalte sie vertrauliche Informationen aus Behörden, zivilgesellschaftlichen Organisationen und Unternehmen. Mitunter bewegten sich ihre Informanten im Bereich der in § 100a Abs. 2 und § 100b Abs. 2 StPO genannten Straftaten. Darüber hinaus betreibe sie gemeinsam mit dem Beschwerdeführer zu 3) einen Tor-Server. Die hinterlegte IP-Adresse führe daher technikbedingt auch zu ihr als Zugangsvermittlerin, sodass kriminelles Verhalten der Servernutzenden bisweilen, wie in der Vergangenheit schon geschehen, ihr zugeschrieben werde. 32

Die Beschwerdeführenden befürchten, aufgrund dieser Umstände unmittelbar oder mittelbar in unterschiedlich geltend gemachtem Umfang staatlich überwacht werden zu können. Alle Beschwerdeführenden nutzten IT-Systeme und kommunizierten über diese teilweise verschlüsselt. Die Nutzung erfolge auch und gerade im privaten Bereich. Sie recherchierten Informationen zu unterschiedlichen privaten Themen im Internet und tauschten sich anonym in Internetforen aus. Alle Beschwerdeführenden nutzten Smartphones mit Kameras, GPS-Funktionen und eingebautem Mikrofon. Bei Bedarf und Vertrauen überließen sie IT-Systeme auch Dritten zur Mitnutzung. Die Beschwerdeführenden selbst nutzten auch IT-Systeme Dritter. 33

2. Die angegriffenen Vorschriften verletzten ihre Grundrechte. 34

a) § 100a Abs. 1 Sätze 2 und 3, § 100b Abs. 1 StPO verstießen gegen Art. 1 Abs. 1 GG. Die Befugnisnormen ermöglichten einen heimlichen Zugriff auf Informationen, die der unantastbaren Intimsphäre Betroffener zuzuordnen seien. Denn die überwachten IT-Systeme seien nicht nur Arbeitsgeräte, sondern spiegelten mit Blick auf Art und Umfang der – auch unbewusst und automatisiert – verarbeiteten Daten den höchstpersönlichen Bereich eines Menschen wider. Die Befugnisnormen ermöglichten, die Gedankenwelt Betroffener auszulesen und die Tiefen ihrer Persönlichkeit auszuforschen. Dadurch könnten allumfassende Persönlichkeitsbilder – unter Einschluss der den Betroffenen selbst nicht bewussten persönlichkeitsprägenden Merkmale – gezeichnet werden. Mit der Überwachung von IT-Systemen werde daher denknotwendigerweise der Kernbereich privater Lebensgestaltung zum Ziel staatlicher Ermittlungen gemacht, was absolut ausgeschlossen sei. 35

b) Sowohl die Quellen-Telekommunikationsüberwachung nach § 100a Abs. 1 Sätze 2 und 3 StPO (aa) als auch die Online-Durchsuchung nach § 100b Abs. 1 StPO (bb) verstießen gegen das aus dem allgemeinen Persönlichkeitsrecht nach Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG abgeleitete Grundrecht auf Gewährleistung der Integrität und 36

Vertraulichkeit informationstechnischer Systeme (im Folgenden: IT-System-Grundrecht) sowie – in Bezug auf § 100a Abs. 1 Sätze 2 und 3 StPO jedenfalls hilfsweise – gegen das durch Art. 10 Abs. 1 GG geschützte Fernmeldegeheimnis. Alle Befugnisnormen seien zudem mit der Schutzdimension des IT-System-Grundrechts nicht zu vereinbaren (cc).

aa) § 100a Abs. 1 Sätze 2 und 3 StPO seien am IT-System-Grundrecht, hilfsweise jedenfalls am Fernmeldegeheimnis zu messen. 37

(1) § 100a Abs. 1 Satz 2 StPO greife in das IT-System-Grundrecht ein, denn es könne technisch nicht ausgeschlossen werden, dass neben der laufenden Kommunikation auch weitere persönlichkeitsrelevante Informationen erhoben würden. Die Regelung sei daher widersprüchlich und verfassungswidrig, da ausgeschlossen sei, dass die technische Beschränkung auf die Überwachung laufender Kommunikation in absehbarer Zukunft geschaffen werden könne (unter Verweis auf BVerfGE 141, 220 <311 Rn. 234>). 38

Nach § 100a Abs. 1 Satz 3 StPO dürfe nicht nur auf laufende, sondern auch auf dort gespeicherte „ruhende" Kommunikation zugegriffen werden. Die Grenze zwischen Art. 10 Abs. 1 GG und dem IT-System-Grundrecht werde mit dieser Befugnis zur heimlichen „retrograden" Erhebung gespeicherter Kommunikation überschritten. 39

(2) Diese Grundrechtseingriffe seien unverhältnismäßig und damit nicht gerechtfertigt. Eine Quellen-Telekommunikationsüberwachung sei bereits nicht zur Aufklärung von Straftaten geeignet, denn die erhobenen Daten hätten wegen ihrer möglichen Manipulation keinen Beweiswert. Insbesondere die Überwachung nach § 100a Abs. 1 Satz 3 StPO sei auch nicht erforderlich. Denn mit der (offenen) Durchsuchung und Beschlagnahme lägen mildere und besser geeignete Mittel vor. Die Regelungen seien auch nicht angemessen. 40

(a) Der Gesetzgeber habe nicht sichergestellt, dass die Angemessenheit der Maßnahme auch im Einzelfall geprüft werde. Der mit der Quellen-Telekommunikationsüberwachung einhergehende „massive" Eingriff in ein IT-System müsse in einem angemessenen Verhältnis zur Bedeutung der Sache stehen. 41

(b) Da die nach § 100a Abs. 1 Sätze 2 und 3 StPO eröffnete Quellen-Telekommunikationsüberwachung im Hinblick auf ihre Eingriffsintensität mit einer Online-Durchsuchung vergleichbar sei, gälten auch die gleichen strengen Anforderungen an ihre verfassungsrechtliche Rechtfertigung (dazu Rn. 49 ff.). Die Quellen-Telekommunikationsüberwachung umfasse nämlich alle Informationen, die willensgesteuert von einer Person über das Internet abgerufen und übermittelt würden, und demgemäß vor allem eine vollständige Überwachung der Internetnutzung. Zu bedenken sei auch die Gepflogenheit, den gesamten Inhalt eines IT-Systems regelmäßig zwischen mehreren Endgeräten oder der Cloud zu synchronisieren. Jeder Zugriff auf diese „ausgelagerten Festplatten" stelle Telekommunikation dar, die durch eine Quellen-Telekommunikationsüberwachung erfasst werden könne. Auch 42

könnten alle Inhalte ausgeleitet werden, die über Cloud-Dienste transferiert würden. Selbst in kurzen Überwachungszeiträumen könnten dadurch Daten in einem Umfang und einer Vielfalt erhoben werden, die die Erstellung eines umfassenden Persönlichkeitsprofils ermöglichten. Es verbleibe daher ein allenfalls marginaler Unterschied zu einem „Vollzugriff" nach § 100b Abs. 1 StPO, weil Systeminhalte durch einen regelmäßigen Transfer über das Internet zu Telekommunikation würden (etwa regelmäßige Synchronisierungen zwischen Endgeräten, Zugriffe auf Daten in der Cloud oder Backups).

Angesichts dieser hohen Eingriffsintensität werde die Quellen-Telekommunikationsüberwachung den verfassungsrechtlichen Anforderungen nicht gerecht, weil als Eingriffsanlass lediglich der einfache Tatverdacht für eine der vielfältigen Anlasstaten nach § 100a Abs. 2 StPO vorausgesetzt werde, die nicht einmal die Qualität der in § 100b Abs. 2 StPO genannten Anlassstraftaten erreichen müssten. Die in dem Katalog nach § 100a Abs. 2 StPO genannten Taten knüpften vielfach nicht an überragend wichtige Rechtsgüter an (näher Rn. 49). 43

(c) Auch die verfahrensrechtlichen Absicherungen seien unzureichend. Es fehlten Vorgaben, wie die Einhaltung der technisch erforderlichen Beschränkungen der Quellen-Telekommunikationsüberwachung nach § 100a Abs. 5 StPO sichergestellt werden solle. Unklar sei, ob und wer dies überwache. Dem anordnenden Gericht werde dies nicht möglich sein. Erforderlich sei eine unabhängige Stelle, die die jeweilige Software überprüfe. Hierfür müsse auch zwingend vorgesehen werden, dass der überprüfenden Stelle alle dazu erforderlichen Unterlagen einschließlich des jeweiligen Quellcodes vorgelegt würden. 44

(d) Im Übrigen griffen die gegenüber § 100b StPO erhobenen Rügen (dazu im Folgenden) auch hinsichtlich § 100a Abs. 1 Sätze 2 und 3 StPO durch. 45

bb) § 100b Abs. 1 StPO verletze nicht nur das IT-System-Grundrecht, sondern auch Art. 10 Abs. 1 GG, denn eine Online-Durchsuchung impliziere stets auch eine Telekommunikationsüberwachung. Die Regelung sei unter anderem unverhältnismäßig, insbesondere unangemessen. 46

(1) § 100b StPO sei zur Aufklärung von Straftaten bereits ungeeignet. Die gewonnenen Informationen hätten keinen Beweiswert, denn Ermittlungsbehörden hätten nach einer Infiltration gegebenenfalls monatelang Zugriff auf das gesamte IT-System, das bewusst oder unbewusst manipuliert werden könnte. Gerichtsfeste Beweise könnten daher nicht erhoben werden. Eine Datenerhebung im Wege der Online-Durchsuchung sei auch nicht erforderlich, da jedenfalls für repressive Zwecke die offene Beschlagnahme des IT-Systems regelmäßig gleich wirksam, aber grundrechtsschonender sei. Mit der Durchsuchung nach §§ 102 ff. StPO und der anschließenden Beschlagnahme sowie Auswertung eines IT-Systems nach §§ 94 ff. StPO könne auf denselben Datenbestand wie bei einer heimlichen Online-Durchsuchung zugegriffen werden. 47

(2) Die Befugnis nach § 100b Abs. 1 StPO sei angesichts der gestiegenen Bedeutung von IT-Systemen in der modernen Gesellschaft auch unangemessen. 48

(a) Der Katalog von Anlassstraftaten in § 100b Abs. 2 StPO sei verfassungsrechtlich unzureichend. Es müsse ein Gleichlauf mit den Anforderungen an eine präventive Online-Durchsuchung bestehen, weshalb die Anlassstraftaten von einem Gewicht sein müssten, das mit den Anforderungen an die zu schützenden „überragend wichtigen Rechtsgüter" korreliere. Viele der in § 100b Abs. 2 StPO geregelten Straftatbestände knüpften indes nicht an überragend wichtige Rechtsgüter an, weshalb eine präventive Online-Durchsuchung zu deren Verhinderung unzulässig wäre. 49

(b) Auch die Eingriffsschwelle genüge nicht den Vorgaben des Bundesverfassungsgerichts zur präventiven Online-Durchsuchung, denn § 100b StPO setze nur einen qualifizierten Anfangsverdacht voraus. Dies bedeute de facto nicht mehr als einen bloßen Anfangsverdacht. Von Verfassungs wegen erforderlich sei aber ein Verdacht, der einem „hinreichenden" Tatverdacht „angenähert" sei beziehungsweise ein „hinreichend schwerer Tatverdacht". Denn wie im präventiven Bereich gehe es um die strukturell vergleichbare, wenn nicht sogar identische Prognose einer hinreichenden Wahrscheinlichkeit, die bei einer präventiven Maßnahme zukunftsgerichtet und bei einer Maßnahme der Strafverfolgung vergangenheitsbezogen sei. Es bedürfe jeweils in der Gegenwart festgestellter Tatsachen, die die Prognose tragen müssten. 50

Die Defizite des nur einfachen Tatverdachts würden verschärft, soweit § 100b Abs. 2 StPO – namentlich im Bereich der Terrorismusbekämpfung – auch an Straftaten anknüpfe, die weit im Vorfeld konkreter Rechtsgutsverletzungen ansetzten. Damit werde im Ergebnis Gefahrenabwehr betrieben. Prognoseschwierigkeiten seien virulent und führten zu starken Spekulationen. Insofern würden die Grenzen zwischen Gefahrenabwehr und Strafverfolgung verwischt. 51

(c) Hinzu komme, dass § 100b StPO den Zugriff auf IT-Systeme insbesondere „anderer Personen" nicht von einer auf Tatsachen basierenden Erfolgsprognose abhängig mache. Es könnten vielmehr alle IT-Systeme überwacht werden, die Beschuldigte nutzten, ohne dass die Ermittlungsbehörden Anhaltspunkte dafür haben müssten, dass dort auch verfahrensgegenständliche Informationen gespeichert oder generiert würden. Dies sei nicht nur unverhältnismäßig, sondern missachte zudem, dass eine Online-Durchsuchung gegenüber nicht selbst beschuldigten Dritten nur subsidiär und unter strengen Voraussetzungen möglich sein dürfe. Ein Zugriff auf IT-Systeme anderer Personen setze nach § 100b Abs. 3 Satz 2 Nr. 2 StPO aber lediglich voraus, dass ein Zugriff auf das IT-System des Beschuldigten allein nicht zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes eines Mitbeschuldigten führen werde. Dies genüge nicht. Erforderlich sei vielmehr, dass aufgrund 52

bestimmter Tatsachen anzunehmen sei, dass nur so Daten erhoben werden könnten, die für die Erforschung des Sachverhalts von maßgeblicher Bedeutung seien.

(d) Die allgemeine in § 100b Abs. 1 Nr. 3 StPO vorgesehene Subsidiaritätsklausel vertiefe die Unangemessenheit. Sie belege, dass der Gesetzgeber die Eingriffsintensität einer Online-Durchsuchung fehleingeschätzt habe. Diese stehe einer Wohnraumüberwachung nicht nach und sei deutlich grundrechtsbelastender als eine Telekommunikationsüberwachung, sodass der Gesetzgeber – auch im Vergleich mit § 100a Abs. 1 Satz 1 Nr. 3 StPO – jedenfalls die in § 100c Abs. 1 Nr. 4 StPO enthaltene Ultima-Ratio-Klausel in § 100b StPO hätte integrieren müssen. Hinzu komme, dass das inhaltliche Prüfprogramm der Subsidiaritätsklausel unpräzise sei. 53

(e) Der Gesetzgeber habe auch die Belastungswirkung additiver Grundrechtseingriffe verkannt. Die durch die Strafprozessordnung eröffneten heimlichen Überwachungsmaßnahmen begründeten die Gefahr einer „Totalüberwachung". Diese könne auch nicht auf Rechtsanwendungsebene verhindert werden. Denn dafür müsste das anordnende Gericht Kenntnis von allen repressiven und präventiven Maßnahmen haben, die gegen Betroffene vollzogen würden. Dies sei nicht gewährleistet. 54

(f) Die gesetzliche Möglichkeit der Anordnung einer Dauerüberwachung impliziere eine menschenunwürdige Totalüberwachung und sei unverhältnismäßig. Zwar sei die Anordnungsdauer in § 100e Abs. 2 Satz 4 StPO auf einen Monat begrenzt. Anordnungen könnten aber durch die Kammer des Landgerichts bis zu einer Gesamtdauer von sechs Monaten und darüber hinaus durch das Oberlandesgericht theoretisch unbegrenzt verlängert werden. Es fehle eine absolute Höchstdauer. 55

(3) Der Kernbereichsschutz sei verfassungsrechtlich unzureichend ausgestaltet. Auf Erhebungsebene bestehe faktisch kein Schutz, obwohl bei einer Online-Durchsuchung kernbereichsrelevante Inhalte nicht nur am Rande, sondern typischerweise erfasst würden. § 100d Abs. 1 StPO laufe leer, da er voraussetze, dass allein Erkenntnisse aus dem Kernbereich erlangt würden, was kaum denkbar sei. Eine Online-Durchsuchung dürfe vielmehr nur angeordnet werden, wenn aufgrund tatsächlicher Anhaltspunkte anzunehmen sei, dass kernbereichsrelevante Daten in nur unerheblichem Umfang erhoben würden. Bei privat genutzten Smartphones sei eine Online-Durchsuchung damit regelmäßig ausgeschlossen. Auch § 100d Abs. 3 Satz 1 StPO, nach dem technisch – soweit möglich – sicherzustellen sei, dass kernbereichsrelevante Daten nicht erhoben würden, laufe leer, weil dies bislang technisch gerade nicht möglich sei. In Bezug auf die eingesetzten technischen Sicherungen fehlten Dokumentations- und Kontrollpflichten. Auch hätte es einer Regelung wie in § 100d Abs. 4 StPO bedurft, wonach eine Überwachung, die in Echtzeit durchgeführt werde, unterbrochen werden müsse und eine Fortführung einer Entscheidung durch ein Gericht bedürfe. Die Regelungen auf der Verwertungsebene enthielten keine Vorgaben für 56

den Fall, dass wider Erwarten in nicht nur unerheblichem Umfang höchstpersönliche Informationen erfasst würden.

(4) Auch der Schutz von Berufsgeheimnisträgern sei unzureichend. § 100d Abs. 5 StPO gewähre in verfassungswidriger Weise keinen absoluten Schutz für deren Berufshelfer. Die Regelung enthalte lediglich ein absolutes Beweiserhebungsverbot in Bezug auf die Berufsgeheimnisträger selbst. Für die ebenso schutzwürdige Kommunikation der Berufshelfer im Sinne des § 53a StPO werde in § 100d Abs. 5 Satz 2 StPO lediglich ein relatives Beweisverwertungsverbot normiert. 57

(5) Da eine Online-Durchsuchung nach § 100b Abs. 1 StPO zugleich zu einem Eingriff in Art. 10 Abs. 1 GG ermächtige, dieses Grundrecht aber in dem Gesetz, mit dem § 100b StPO eingeführt wurde, nicht genannt worden sei, sei die Regelung wegen Verstoßes gegen das Zitiergebot nach Art. 19 Abs. 1 Satz 2 GG verfassungswidrig. 58

cc) § 100a Abs. 1 Sätze 2 und 3 sowie § 100b Abs. 1 StPO verletzten das IT-System-Grundrecht auch im Hinblick auf seine Schutzdimension, da sie pauschal einen Eingriff in IT-Systeme gestatteten, ohne die technischen Wege der Infiltration zu begrenzen. Durch Schaffung der Regelungen habe der Gesetzgeber vielmehr Anreize gesetzt, IT-Sicherheitslücken auszunutzen anstatt sie zu schließen. Dadurch werde die IT-Sicherheit gefährdet, obwohl der Gesetzgeber gehalten sei, diese zu gewährleisten. 59

c) Die Online-Durchsuchung nach § 100b StPO verletze darüber hinaus die durch Art. 13 Abs. 1 GG geschützte Unverletzlichkeit der Wohnung. Schon das passive Abhören der Wohnung einer Zielperson unter Nutzung des infiltrierten IT-Systems stelle einen Eingriff dar, der mangels Beachtung des Zitiergebots verfassungswidrig sei. Darüber hinaus sei aber auch das aktive Ansteuern von Peripheriegeräten technisch möglich. Nach der Gesetzentwurfsbegründung solle die Online-Durchsuchung gerade dazu dienen, das „gesamte Nutzungsverhalten einer Person“ zu überwachen. Das insoweit ermöglichte optische Überwachen des Wohnraums sei aber nach Art. 13 Abs. 3 GG ausgeschlossen. 60

d) Der Gesetzgeber habe auch Art. 19 Abs. 4 GG missachtet. Die Rechtsweggarantie sei aufgrund unzureichender Sicherungsmechanismen – vor allem in § 100a Absätze 5 und 6 StPO – verletzt. Es sei für Betroffene de facto nicht nachprüfbar, ob hier in Rede stehende Beweiserhebungen rechtskonform durchgeführt worden seien. Es bestehe ab dem Zeitpunkt der Infiltration eine erhöhte Gefahr der Manipulation durch Dritte. Die Vorgaben in § 100a Absätze 5 und 6 StPO seien praktisch wertlos. Es sei nicht explizit vorgesehen, dass durch eine unabhängige Stelle überprüft werde, dass die Software gesetzeskonform ausgearbeitet sei. Eine solche Überprüfung könne auch aufgrund der fehlenden Bekanntgabe des Quellcodes nicht erfolgen. Insofern sei die Authentizität vorgelegter Beweise nicht nachprüfbar. 61

IV.

Von der im Verfassungsbeschwerdeverfahren eingeräumten Möglichkeit zur Stellungnahme haben der Bundesgerichtshof, der (damalige) Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, der Generalbundesanwalt beim Bundesgerichtshof, der Bund Deutscher Kriminalbeamter e.V., der Chaos Computer Club e.V., die Deutsche Polizeigewerkschaft im DBB, der Deutsche Anwaltverein e.V., der Deutsche Journalisten-Verband e.V., der Deutsche Richterbund e.V., die Gesellschaft für Freiheitsrechte e.V. und die Gewerkschaft der Polizei Gebrauch gemacht. 62

Den ergänzend übersandten Fragenkatalog zur Nutzung von Cloud-Services, zur Bedeutung von Erkenntnissen aus Maßnahmen nach § 100a Abs. 1 StPO für die Strafverfolgung und zu praktischen Erfahrungswerten bei der Durchführung einer Quellen-Telekommunikationsüberwachung haben die Bundesregierung, mehrere Landesregierungen, die Datenschutzaufsichtsbehörden des Bundes und der Länder, der Generalbundesanwalt, das Statistische Bundesamt, der Chaos Computer Club, die Gesellschaft für Datenschutz und Datensicherheit e.V. und die Gesellschaft für Freiheitsrechte beantwortet. 63

1. Die Äußerungsberechtigten nach § 94 Abs. 4 in Verbindung mit § 77 Nr. 1 BVerfGG, die zu der Verfassungsbeschwerde und den ergänzend gestellten Fragen Stellung genommen haben, haben sich wie folgt geäußert: 64

a) Die Bundesregierung teilt zu den Fragen des Senats mit, dass bei der Telekommunikationsüberwachung eine Ausleitung aller Inhalte und Umstände laufender Kommunikation erfolge, die über die Verbindung vom Endgerät zum Telekommunikationsanbieter laufe. Das betreffe auch sämtliche Internetkommunikation inklusive des Aufrufens von Webseiten und der Cloud-Kommunikation. Es gelte das Prinzip der vollständigen Überwachungskopie. In der Regel sei der gesamte Internetverkehr standardmäßig verschlüsselt. Die mit einer Telekommunikationsüberwachung erlangten Daten seien daher in der Regel nicht les- oder auswertbar. 65

Nach Angaben des Bundesamts für Sicherheit in der Informationstechnik sei die Bandbreite an Cloud-Diensten sehr groß und umfasse quasi jeden Bereich der Nutzung von Informationstechnologie. Privatpersonen nutzten Cloud-Services direkt oder indirekt in verschiedensten Kontexten. Dabei arbeiteten Cloud-Services oft im Hintergrund und ermöglichten die Nutzung der eigentlichen Software-Anwendung oder des Produkts. Hierzu zählten unter anderem die Nutzung von Cloud-Services, die standardmäßig durch die Betriebssysteme mobiler Endgeräte wie Smartphones oder Tablets genutzt oder zur Verfügung gestellt würden (etwa Android, iOS), und Cloud-Services, die zur Nutzung von Internet-of-Things-Geräten benötigt würden (z.B. Smarthome-Anwendungen, digitale Sprachassistenten und smarte Haushaltsgeräte), aber auch vernetzte Fahrzeuge, Datenaustauschdienste wie Dropbox, Google Drive und Bild- und Textverarbeitungsprogramme sowie Messenger- 66

Dienste und Videokonferenzlösungen. Unternehmen nutzten die genannten Cloud-Services in noch breiterer Varietät, etwa als Datenbanken oder für Management-Anwendungen. Konkrete Daten zur Nutzung könne man verschiedenen Umfragen entnehmen. Nach den Erhebungen des Bitkom e.V. und des KPMG Cloud-Monitor nutze ein großer Teil der Unternehmen Cloud-Services. Eine Studie der Convios Consulting GmbH im Auftrag von web.de und GMX gehe davon aus, dass 62 % der Privatinternetnutzenden Cloud-Speicher nutzten. Insgesamt habe sich die Nutzung von Cloud-Services in den letzten zehn Jahren stark erhöht, was mit einer Verdoppelung der Smartphone-Nutzenden von 41 % im Jahr 2013 auf 82,2 % im Jahr 2023 einhergehe. Der Datenaustausch mit Cloud-Diensten erfolge in der Regel verschlüsselt. Die Zeitabstände für Backups hingen vom Service und der Art der Daten ab. Den am häufigsten genutzten Diensten sei eine Echtzeit-Aktualisierung und ein kontinuierlicher Upload gemeinsam, um Änderungen sofort zu erfassen.

Die Bundesregierung teilt mit, dass im Jahr 2022 deutschlandweit in 94 Fällen Quellen-Telekommunikationsüberwachungen nach § 100a Abs. 1 Sätze 2 und 3 StPO angeordnet und in 49 Fällen durchgeführt worden seien. Die Maßnahmen beträfen grundsätzlich das gesamte Spektrum des Katalogs von § 100a Abs. 2 StPO. Für Maßnahmen des Bundeskriminalamts lägen in einem Großteil der Fälle mehrere Tage bis Wochen zwischen Anordnung und tatsächlicher Umsetzung einer Maßnahme. 67

b) Nach Angaben der Bayerischen Staatsregierung werden bei einer Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 1 StPO alle Daten, die bei der Kommunikation über einen überwachten Telekommunikationsanschluss anfallen, technisch ausgeleitet. Dabei sei auch die Kommunikation mit einem Cloud-Service oder mit Software-as-a-Service erfasst. Im Falle einer verschlüsselten Datenübermittlung könnten grundsätzlich keine Inhalte textlich gelesen oder ausgewertet werden. Gleiches teilen auch die Sächsische Staatsregierung und die Landesregierung Schleswig-Holstein mit. Letztere gibt weiter an, bei einer Telekommunikationsüberwachung gebe es keine Filterung der ausgeleiteten Daten, sodass auch der Austausch mit einem Cloud-Service über ein Mobilfunknetz umfasst sei. Es werde nur noch ein sehr geringer Anteil im Internetdatenstrom unverschlüsselt übertragen. Die Landesregierung Rheinland-Pfalz gibt an, dass die Telekommunikationsunternehmen eine Überwachungskopie des gesamten am überwachten Anschluss ein- und ausgehenden Datenstroms ausleiteten, darunter auch „Sprach- und Internetdaten“. 68

Die Bayerische Staatsregierung teilt weiter mit, in der Praxis sei bei der Datenübertragung mit Cloud-Services die Transportverschlüsselung Standard. Die Ende-zu-Ende-Verschlüsselung werde weniger genutzt. Die Einstellung von System-Backups in die Cloud sowie deren Häufigkeit variierten nach individuellen Bedürfnissen und der genutzten Software. Auch die Landesregierung Schleswig-Holstein betont, dass der Datenaustausch zwischen einem Cloud-Service und dem Endgerät grundsätzlich verschlüsselt erfolge, sodass übermittelte Inhalte nicht lesbar seien. Die Regierung des Saarlandes berichtet, aus der 69

Ermittlungsarbeit der Staatsanwaltschaften ergebe sich, dass die gängigen Mobiltelefone eine Verbindung zu Cloud-Speichern vorinstalliert hätten und daher alle Nutzenden eines solchen Smartphones über einen entsprechenden Speicher verfügten – teilweise ohne sich dessen bewusst zu sein. Es sei daher von einer privaten Nutzung von Cloud-Speichern bei mehr als 90 % der Bevölkerung auszugehen. Nach den Ermittlungen der Staatsanwaltschaften in Ransomware-Verfahren, in denen Unternehmen ihre IT-Infrastruktur offenlegten, nutzten auch Unternehmen Cloud-Speicher im großen Stil. Neben einer Nutzung von Speicherdiensten für E-Mails und zur Speicherung von Dateien würden Unternehmen die Cloud für Office-Anwendungen, den Einsatz weiterer Software und Datenbanken gebrauchen. Auch im kriminellen Milieu sei die Nutzung von Cloud-Speicherdiensten angestiegen, weil die Dienste der Identitätsverschleierung dienten und ganzen Tätergruppen Zugriff auf bestimmte Daten ermöglichten.

Nach Angaben der Bayerischen Staatsregierung besteht auch bei verschlüsselten Daten die Möglichkeit einer Klassifizierung der jeweiligen Anwendung aus dem Datenstrom. So könnten der genutzte Dienst oder die entsprechende Software identifiziert werden. Denn der Datenstrom enthalte nicht nur verschlüsselte Daten, die nicht gelesen oder ausgewertet werden könnten, sondern auch Rand-, Verkehrs- und Metadaten, aus denen sich weitere Hinweise zur Telekommunikation ergeben könnten. Auch nach Auffassung der Niedersächsischen Landesregierung bieten Maßnahmen der Telekommunikationsüberwachung trotz weitreichender Inhaltsverschlüsselung noch immer Ermittlungsansätze hinsichtlich Metadaten oder der Feststellung von Kommunikationsbeziehungen als solchen. 70

Die Landesregierung Baden-Württemberg merkt an, dass der Telekommunikationsüberwachung bei der Verfolgung und Aufklärung schwerer Straftaten in vielen Deliktsfeldern herausragende Bedeutung zukomme. Die Quellen-Telekommunikationsüberwachung sei in Anbetracht zunehmend verschlüsselter Kommunikation für die Strafverfolgung unverzichtbar. In Fällen schwerer und schwerster Kriminalität, unter anderem Organisierter Kriminalität, würden die Behörden nur durch sie in die Lage versetzt, der (früheren) klassischen Telekommunikationsüberwachung entsprechende Erkenntnisse zu erhalten. Nach Angaben der Bayerischen Staatsregierung kommt der Überwachung der Telekommunikation im Bereich der Kapitaldelikte, Eigentumsdelikte und bei schweren Betäubungsmitteldelikten in der Praxis eine besondere Bedeutung zu. Die Landesregierung Rheinland-Pfalz gibt an, dass Maßnahmen der Telekommunikationsüberwachung am häufigsten im Bereich von Betäubungsmitteldelikten genutzt würden. Weitere Anlassdelikte seien regelmäßig Betrugsdelikte, Kapitaldelikte und Straftaten gegen die öffentliche Ordnung. Aufgrund der hohen technischen und taktischen Anforderungen werde eine Quellen-Telekommunikationsüberwachung überwiegend erst bei Straftaten mit erheblicher Schwere, zum Beispiel bei Kapitaldelikten, beziehungsweise bei besonders konspirativem Täterverhalten eingesetzt. Die Niedersächsische Landesregierung weist darauf hin, dass bei Straftaten, die über das Internet begangen würden, im Regelfall außer der Telekommunikations- 71

überwachung keine anderen Beweismittel zur Verfügung stünden. Die Quellen-Telekommunikationsüberwachung könne insbesondere für technisch anspruchsvollere Serverüberwachungen im Bereich Cybercrime genutzt werden. Nach Angaben der Landesregierung Schleswig-Holstein seien in den letzten fünf Jahren fast die Hälfte aller Maßnahmen der Telekommunikationsüberwachung im Deliktsbereich der Betäubungsmittelkriminalität erfolgt. Danach folgten Betrug, Bandendiebstahl/Wohnungseinbruchsdiebstahl und Kapitaldelikte sowie in 7,5 % der Fälle die Gefahrenabwehr. Amtshilfe des Bundeskriminalamts für die Quellen-Telekommunikationsüberwachung sei nur bei bestimmten Deliktsfeldern (Staatsschutz, Organisierte Kriminalität, Betäubungsmittelkriminalität) in Anspruch genommen worden. Für das Amtshilfeersuchen sei in der Regel eine mehrwöchige Vorbereitungszeit erforderlich, da die Ausleitungssoftware an die Hard- und Software des Zielgeräts angepasst werden müsse. Der Gerichtsbeschluss werde in der Regel erst nach Umsetzungsreife der Maßnahme beantragt.

Der Senat der Freien und Hansestadt Hamburg teilt mit, Maßnahmen nach § 100a Abs. 1 Sätze 2 und 3 StPO seien in den Jahren ab 2021 nur in wenigen Fällen angeordnet und durchgeführt worden, wobei nicht stets beide Varianten der Quellen-Telekommunikationsüberwachung angeordnet und durchgeführt worden seien. Nach Angaben der Landesregierung Niedersachsen wurden im Jahr 2023 in keinem und im Jahr 2024 in einem Ermittlungsverfahren eine Quellen-Telekommunikationsüberwachung angeordnet und durchgeführt. 72

2. Der Bundesgerichtshof teilt mit, dass der 3. Strafsenat wiederholt mit Ermittlungsverfahren befasst gewesen sei, denen Erkenntnisse zugrunde gelegen hätten, die mittels einer Quellen-Telekommunikationsüberwachung oder einer Online-Durchsuchung gewonnen worden seien (Verweis etwa auf BGH, Beschluss vom 30. November 2021 - AK 49/21 -, Rn. 15). 73

3. Die angehörten sachkundigen Dritten, die zur Verfassungsbeschwerde und den ergänzenden Fragen Stellung genommen haben, äußern sich wie folgt. 74

a) Der (damalige) Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hält die angegriffenen Vorschriften für verfassungswidrig, weil sie unverhältnismäßig seien. § 100a Abs. 1 Sätze 2 und 3 StPO griffen in das IT-System-Grundrecht ein. Die Eingriffsintensität sei hoch, weil auch die Nutzung von Cloud-Diensten Kommunikation darstelle und daher die „Kommunikation der überwachten Person mit sich selbst“ erfasst sei. Durch den von § 100a Abs. 1 Satz 3 StPO ermöglichten Zugriff auf gespeicherte Kommunikation werde die Grenze der Telekommunikationsüberwachung zugunsten einer echten Online-Durchsuchung überschritten. Die Eingriffe in das IT-System-Grundrecht durch § 100a Abs. 1 Sätze 2 und 3, § 100b StPO seien nicht gerechtfertigt. Es müssten mindestens dieselben Anforderungen gelten, wie sie das Bundesverfassungsgericht im Bereich der 75

Gefahrenabwehr zugrunde lege. Daher bedürfe es einer Überwachung zugunsten eines überragend wichtigen Rechtsguts, dem die Straftatenkataloge in § 100a Abs. 2 und § 100b Abs. 2 StPO nicht durchgehend genügten. Bedenklich sei auch, dass nicht nur staatliche Software-Entwicklungen eingesetzt werden dürften und die Software überschießende Funktionalitäten aufweisen könne.

b) Zu den Fragen des Senats führt für die Datenschutzaufsichtsbehörden des Bundes und der Länder die Landesbeauftragte für Datenschutz Schleswig-Holstein aus, dass die meisten Betriebssysteme bei privater Nutzung automatisch eine bereits implementierte Cloud-Lösung anböten. Die Verschlüsselung auf dem Transportweg sei mittlerweile Standard. Bei der Speicherung von Daten in der Cloud wirke diese Art der Verschlüsselung nicht gegen den Cloud-Anbieter selbst, sondern könne nur gegen bestimmte externe und interne Angriffe (z.B. durch Mitarbeitende) schützen. Vor diesem Hintergrund lägen den Cloud-Betreibern im Falle einer Transportverschlüsselung die dort gespeicherten Daten rein technisch in auswertbarer Form vor. Soweit dieser Betreiber mit den Ermittlungsbehörden kooperiere, bestehe für Überwachungsmaßnahmen kein technisches Hindernis. Ein heimlicher Zugriff mittels Staatstrojaner könne sich daher erübrigen. Mit Blick auf die zahlreichen höchstpersönlichen Daten auf diversen Cloud-Servern verschiedener Anbieter dürfe ein Zugriff der Ermittlungsbehörden nicht ohne neue Schranken erfolgen. 76

c) aa) Nach Auffassung des Generalbundesanwalts (GBA) sind § 100a Abs. 1 Sätze 2 und 3 und § 100b StPO verfassungsgemäß. 77

§ 100a Abs. 1 Sätze 2 und 3 StPO seien aus dem IT-System-Grundrecht ausgeklammert. Auch im Hinblick auf § 100a Abs. 1 Satz 3 StPO liege der Fokus auf der Kommunikationsüberwachung, denn es könne nur auf Kommunikation zugegriffen werden, die auf dem infiltrierten System während des angeordneten Überwachungszeitraums anfalle. Damit gleiche die Vorschrift aus, wenn die Datenausleitung nicht schon ab Beginn des angeordneten Überwachungszeitraums, sondern erst verzögert erfolge; hierzu könne es etwa bei technischen Hindernissen infolge des Einsatzes von Verschlüsselungstechniken bei Messenger-Diensten kommen. Weder Intensität noch zeitlicher Umfang des bereits durch § 100a Abs. 1 Satz 2 StPO erlaubten Eingriffs würden durch § 100a Abs. 1 Satz 3 StPO geändert. Auch im letzteren Fall sei die funktionale Äquivalenz mit der klassischen Telekommunikationsüberwachung gewährleistet, weil der Zugriff so beschränkt sei, dass kein Einblick in wesentliche Teile der Lebensgestaltung einer Person genommen werde. Art. 10 Abs. 1 GG sei allerdings nicht betroffen, da nur der Zugriff auf gespeicherte Kommunikationsdaten gestattet werde. § 100a Abs. 1 Satz 3 StPO müsse daher am Recht auf informationelle Selbstbestimmung gemessen werden. Dieser Eingriff sei ebenso wie derjenige durch § 100a Abs. 1 Satz 2 StPO gerechtfertigt. Denn in der Sache werde nur mit Blick auf die aktuellen Entwicklungen in der Informationstechnik eine Telekommunikationsüberwachung auch dort ermöglicht, wo dies mit alter Überwachungstechnik mittlerweile ausscheide. Die 78

Quellen-Telekommunikationsüberwachung könne dabei technisch auf laufende Kommunikation begrenzt werden.

§ 100b StPO sei ebenfalls nicht zu beanstanden. An eine Online-Durchsuchung zu repressiven Zwecken seien keine höheren gesetzlichen Anforderungen zu stellen als an eine entsprechende Maßnahme zu präventiven Zwecken. Die staatliche Pflicht zum Schutz individueller und kollektiver Rechtsgüter vor drohenden Gefahren habe von Verfassungs wegen keine größere Bedeutung als die ebenfalls verfassungsrechtlich gebotene Wahrung der Funktionstüchtigkeit der Strafrechtspflege. Unabhängig davon diene die Strafverfolgung im Rahmen der Spezial- und Generalprävention auch dem Schutz derselben Rechtsgüter. Der Straftatenkatalog des § 100b Abs. 2 StPO sei nicht zu beanstanden; er umfasse nur solche Straftatbestände, die dem Schutz überragend wichtiger Rechtsgüter dienten. Die Beschwerdeführenden übersähen, dass die beispielhafte Aufzählung von entsprechenden Rechtsgütern durch das Bundesverfassungsgericht nicht ausschließe, dass der Gesetzgeber auch den Schutz anderer Rechtsgüter verfolgen dürfe. Anderenfalls würden bestimmte Formen schwerster, bisweilen organisierter, Kriminalität wie schwerste Eigentumsdelikte nicht erfasst. Zudem sei bei der Auswahl der Straftatbestände neben anderen Gesichtspunkten auch die gesetzgeberische Wertung zu berücksichtigen, die in der Bemessung der jeweiligen Höchststrafe zum Ausdruck komme. Schließlich sei auch das Zitiergebot nicht deshalb verletzt, weil der Gesetzgeber Art. 10 Abs. 1 GG nicht als durch § 100b StPO eingeschränktes Grundrecht genannt habe. Der hier vorliegende Grundrechtseingriff bemesse sich ausschließlich am IT-System-Grundrecht, das Art. 10 Abs. 1 GG verdränge. 79

bb) Zu den Fragen des Senats berichtet der Generalbundesanwalt, dass aufgrund einer Anordnung nach § 100a Abs. 1 Satz 1 StPO alle ein- und ausgehenden Daten ausgeleitet würden und zwar aufgrund einer Verpflichtung des Mobilfunkbetreibers beziehungsweise Providers des Festnetzanschlusses, über den das WLAN laufe, oder einer Verpflichtung etwa des Anbieters des Cloud-Services oder des Software-as-a-Service-Dienstes. Werde der Telekommunikationsdiensteanbieter verpflichtet, seien nur die klassische Telefonie und SMS lesbar. Relevante Inhalte, insbesondere solche von Cloud- und E-Mail-Diensten, seien regelmäßig verschlüsselt und daher nicht lesbar. Auch die Ausleitung verschlüsselter Inhalte biete aber die Möglichkeit einer sogenannten Rohdatenanalyse bezüglich Metadaten und im Hinblick darauf, welche Dienste von den Betroffenen genutzt würden. Diese Informationen könnten weitere Maßnahmen vorbereiten. Im Falle einer Verpflichtung von Cloud- oder Software-as-a-Service-Betreibern sei regelmäßig eine unverschlüsselte Ausleitung möglich. Problematisch sei allerdings, dass eine Vielzahl von Betreibern ihren Sitz im Ausland habe, weshalb Rechtshilfeersuchen notwendig seien. Auch bei einer Verpflichtung des E-Mail-Providers erfolge eine komplette Ausleitung des gesamten (auch ruhenden) E-Mail-Verkehrs. Alles in allem habe die klassische Telekommunikationsüberwachung weiterhin eine erhebliche Bedeutung. 80

Durch eine Maßnahme nach § 100a Abs. 1 Satz 2 StPO würden alle ein- und ausgehenden Daten unverschlüsselt ausgeleitet und seien dann lesbar. Der gesamte Datenverkehr könne identifiziert und im Klartext mitgeschnitten werden; dieser umfasse auch den Datenaustausch mit Cloud-Services. Die Umsetzung der Quellen-Telekommunikationsüberwachung erfordere einige Zeit. In der Regel würden zwischen Anordnung und Umsetzung jedenfalls einige Tage vergehen. Die Verzögerung ergebe sich aus der notwendigen Anpassung an die Hard- und Software des jeweiligen Endgeräts. Die Möglichkeit der zeitlich begrenzten rückwirkenden Erhebung über § 100a Abs. 1 Satz 3 StPO gleiche diesen zeitlichen Aufwand aus. 81

Die Quellen-Telekommunikationsüberwachung sei eine der wenigen Maßnahmen, mit denen derzeit gerade im Bereich schwerer beziehungsweise Organisierter Kriminalität noch effektiv oder überhaupt verfahrensrelevante Kommunikationsdaten erhoben werden könnten. In diesem Bereich würden regelmäßig gezielt Mittel der verschlüsselten Kommunikation eingesetzt. 82

d) Das Statistische Bundesamt hat auf die Fragen des Senats die dort vorliegenden Statistiken zur Cloud-Nutzung mitgeteilt. 83

e) Nach Auffassung des Bunds Deutscher Kriminalbeamter greift § 100a Abs. 1 Satz 3 StPO in das IT-System-Grundrecht ein und ist daher an den gleichen Maßstäben zu messen wie die durch § 100b StPO gestattete Online-Durchsuchung, weshalb der in § 100a Abs. 2 StPO abgebildete Straftatenkatalog nur teilweise den verfassungsrechtlichen Anforderungen entspreche. § 100a Abs. 1 Satz 2 StPO sei dagegen allein an Art. 10 Abs. 1 GG zu messen. Die Begrenzbarkeit der Quellen-Telekommunikationsüberwachung auf die laufende Kommunikation betreffe nur die Anwendung, nicht aber die Gültigkeit der Norm. Diese Maßnahme sei zwischenzeitlich auch technisch begrenzbar. 84

f) aa) Der Chaos Computer Club kritisiert, dass der Einsatz von Staatstrojanern nunmehr als eine Standardmaßnahme strafprozessualer Überwachung auch gegenüber Alltagskriminalität mit niedriger Eingriffsschwelle definiert worden sei. Infolge der Digitalisierung der Gesellschaft seien IT-Systeme dichter an den einzelnen Menschen herangerückt und elementarer Teil der gesamten Lebens- und Arbeitspraxis geworden. Auch die Gesellschaft sei zunehmend vernetzter geworden, weil solche Systeme unverzichtbarer Teil aller gesellschaftlichen Infrastrukturen seien. Dadurch sei das Smartphone zu einer Schaltzentrale für alle Lebensbereiche geworden und spiegele die persönlichste Lebensführung wider. Digitale Dienste seien daher mittlerweile auch im Regelfall verschlüsselt. 85

Hinsichtlich einer Infiltration von IT-Systemen müsse klar sein, dass das Zielsystem dadurch wesentlich verändert und so dessen Integrität dauerhaft unterminiert sowie auch anderen Angreifern der ungewollte und unbemerkte Zugang erleichtert werde. Grundsätzlich sei die Schwächung der Gerätesicherheit unvermeidbar. Im Rahmen welcher 86

konkreten Ermittlungsmaßnahme eine Infiltration erfolge, sei technisch irrelevant. Es sei ferner zu besorgen, dass die Befugnisse weitreichende Auswirkungen auf die Betreiber und Administratoren von Kommunikationsinfrastrukturen hätten. Schwere Kollateralschäden und eine unzulässig weitreichende Auswertung der Daten betroffener Zielpersonen seien zu befürchten, gerade weil unbefugte Dritte durch Missbrauch neu geschaffener Sicherheitslücken einen grenzenlosen Einblick in Inhalts- und Verkehrsdaten gewönnen. Hinzu komme, dass es an einer hinreichenden Prüfung der technischen Details der verwendeten Trojaner fehle. Vor allem eine Prüfung des Quellcodes sei nötig. Eine gerichtliche Einzelfallkontrolle genüge nicht, da Gerichte typischerweise technisch nicht ausreichend vorbereitet seien, um sie sinnvoll vornehmen zu können. Ein Vertrauen nur auf die Aussagen der Anbieter komme nicht in Betracht, da deren Wahrheitsgehalt nicht hinreichend prüfbar sei.

bb) Auf die Fragen des Senats teilt der Chaos Computer Club mit, dass der Trend zu Cloud-Services weitergehe, da Unternehmen, aber auch Behörden den Zugang zu skalierbaren IT-Ressourcen schlicht benötigten. Die Nutzung sei mittlerweile weit verbreitet. In Unternehmen würden System-Backups mindestens täglich durchgeführt, oft auch mehrfach täglich. Viele Softwarepakete, die in der Wirtschaft zum Einsatz kämen, seien nur noch über die Cloud zu erreichen. Insbesondere durch Smartphones und die von deren Herstellern angebotenen Cloud-Lösungen habe auch die Privatnutzung stark zugenommen. Viele Arten von Cloud-Services seien unbewusst in den Alltag einbezogen und müssten nicht mehr bewusst abgerufen werden. Private Endnutzer verließen sich in der Regel auf die Voreinstellungen ihrer Softwareanbieter. Bei iPhones sei das Cloud-Backup zum Beispiel standardmäßig aktiviert und finde täglich statt. Der ganz überwiegende Teil der Nutzer ändere dies nicht. Bisweilen sei eine dauerhafte Speicherung außerhalb der Cloud überhaupt nicht mehr vorgesehen. Die Art der Daten, die heute über verschiedenste Cloud-Services mit und ohne Wissen der Betroffenen automatisiert verarbeitet würden, sei mannigfaltiger, voluminöser und persönlicher denn je. Ein Großteil der Menschen schiebe persönlichste Daten unbewusst zwischen Computersystemen „hin und her“. 87

g) Nach Auffassung der Deutschen Polizeigewerkschaft im DBB sind Quellen-Telekommunikationsüberwachung und Online-Durchsuchung unerlässliche Instrumente einer effektiven Verbrechensbekämpfung zur Wahrnehmung des grundgesetzlichen Schutzauftrags des Staates. Das Kommunikationsverhalten von Straftätern sei im Zeitalter der Digitalisierung rasanten Veränderungsprozessen unterworfen. Dem müssten sich die Sicherheitsbehörden stellen. 88

Die Quellen-Telekommunikationsüberwachung bedeute zwar einen sehr schwerwiegenden Eingriff in Persönlichkeitsrechte Einzelner, allerdings müssten sich die Sicherheitsbehörden eben auch einer nie dagewesenen Situation der Bedrohung durch Kriminalität und Terror stellen. Mit ihr sei auch keine grundsätzlich neue eingriffsintensivere 89

Maßnahme geschaffen worden, sondern die Strafverfolgungsbehörden seien nur in den „Stand vorher" zurückversetzt worden, als Telefonie noch über klassische Systeme abgewickelt worden sei. Mittlerweile sei die Verschlüsselung von Fernkommunikation technischer Standard, sodass eine effektive Strafverfolgung mehr als eine klassische Telekommunikationsüberwachung brauche. Die Quellen-Telekommunikationsüberwachung habe sich in Bund und Ländern als Instrument der Gefahrenabwehr mittlerweile etabliert und werde erfolgreich angewendet.

h) Der Deutsche Anwaltverein hält die Verfassungsbeschwerde teilweise für aussichtsreich. Die Quellen-Telekommunikationsüberwachung knüpfe grundsätzlich verfassungsrechtlich unbedenklich an die in § 100a Abs. 2 StPO genannten Straftatbestände an. Bedenken bestünden jedoch, soweit § 100a Abs. 1 Sätze 2 und 3 StPO auch eine Überwachung der Internetnutzung ermöglichten. Dies wiege deutlich schwerer als eine Überwachung der sozialen Kommunikation. Die vollständige Überwachung der Internetnutzung sei nicht für den gesamten Katalog des § 100a Abs. 2 StPO verfassungsrechtlich gerechtfertigt. Darüber hinaus bestünden verfassungsrechtliche Bedenken, soweit der eingriffsintensive Zugriff auf den Datenaustausch mit der Cloud faktisch ermöglicht werde. Dies lege nahe, dieselben verfassungsrechtlichen Anforderungen wie an eine Online-Durchsuchung zugrunde zu legen. 90

Die Online-Durchsuchung nach § 100b StPO sei nicht verhältnismäßig. Es seien die Maßstäbe wie zur Rechtfertigung präventiver Online-Durchsuchungen heranzuziehen. Eine repressive Online-Durchsuchung sei daher nur zur Verfolgung solcher Delikte zulässig, die dem Schutz überragend wichtiger Rechtsgüter dienten. Dem genügten nicht alle in § 100b Abs. 2 StPO genannten Straftatbestände. 91

Der Gesetzgeber habe auch versäumt, die Subsidiarität hinreichend zu regeln. § 100c StPO sehe eine strengere Subsidiaritätsklausel vor, obwohl die durch § 100b StPO vermittelte Eingriffstiefe größer sei. Dies sei nicht angemessen. Zudem böten § 100d Absätze 1 bis 4 StPO keinen ausreichenden Kernbereichsschutz auf Erhebungsebene. Angesichts der durch § 100b StPO ermöglichten Echtzeit-Überwachung müsse eine Online-Durchsuchung wie auch eine akustische Wohnraumüberwachung unterbrochen werden, wenn das überwachte Nutzungsverhalten Anhaltspunkte dafür liefere, dass kernbereichsrelevante Inhalte betroffen seien. § 100d Abs. 3 StPO mache jedoch keine entsprechenden Vorgaben. 92

i) Der Deutsche Journalisten-Verband weist darauf hin, dass Daten heute durch generative Künstliche Intelligenz ausgewertet werden könnten, was die Erstellung intimster Persönlichkeitsprofile erlaube. Das Gesetz sehe ein Eingreifen bei nicht ausreichend schweren Straftaten vor und missachte, dass die Quellen-Telekommunikationsüberwachung technisch nicht auf die laufende Kommunikation begrenzbar sei. Darüber hinaus sei die Pressefreiheit durch § 100a Abs. 1 Sätze 2 und 3, Abs. 3 StPO wegen eines mangelhaften 93

Informantenschutzes und eines unzureichenden Schutzes von Berufsgeheimnisträgern im Bereich von Presse und Rundfunk verletzt.

j) Der Deutsche Richterbund (DRB) hält die angegriffenen Vorschriften für verfassungsgemäß. Wegen der zunehmenden Digitalisierung des Täterhandelns seien die neu eingeführten Maßnahmen zur Aufklärung schwerwiegender Straftaten insbesondere im Bereich der Organisierten Kriminalität und des Staatsschutzes unverzichtbar. § 100b StPO sei durch eine ausreichende Eingriffsschwelle und Beschränkung auf Straftaten, die dem Schutz überragend wichtiger Rechtsgüter dienen, angemessen begrenzt. Der Gesetzgeber habe bei deren Auswahl einen gewissen Spielraum und sei nicht auf Taten gegen Leib, Leben und Freiheit der Person beschränkt. 94

Der Gesetzgeber habe mit der Befugnis zur Quellen-Telekommunikationsüberwachung kein gegenüber der herkömmlichen Telekommunikationsüberwachung neues Ermittlungsinstrument mit größerer Eingriffstiefe geschaffen. Er habe nur die „Überwachungslücke" durch die technisch bedingte Verlagerung der Telekommunikation in das Internet schließen wollen. Es liege kein Eingriff in das IT-System-Grundrecht vor, denn es werde technisch sichergestellt, dass nur Inhalte und Umstände der laufenden Kommunikation ausgeleitet würden. Dies sei auch kontrollierbar. Wegen der technischen Beschränkung des eingesetzten Überwachungstools der Quellen-Telekommunikationsüberwachung sei diese allein an Art. 10 Abs. 1 GG zu messen. Ob dies auch für § 100a Abs. 1 Satz 3 StPO gelte oder hier das Recht auf informationelle Selbstbestimmung betroffen sei, könne dahinstehen. Entscheidend sei der Gedanke der „hypothetischen Kommunikationsüberwachung", denn es sollten lediglich die technischen Schwierigkeiten ausgeglichen werden, die bei Umsetzung der Maßnahme nach Erlass der Überwachungsanordnung aufträten. 95

k) Nach Angaben der Gesellschaft für Datenschutz und Datensicherheit (GDD) auf die Fragen des Senats steigt der Umfang der Cloud-Nutzung kontinuierlich an. Insbesondere bei Privatnutzenden sei von einer erheblichen Zunahme auszugehen, weil viele soziale Medien und Messenger-Dienste cloudbasiert seien. Auch viele Softwareanbieter hätten in den letzten zehn Jahren auf rein cloudbasierte Lösungen umgestellt. Für Datenübertragungen in die Cloud sei mittlerweile mindestens eine Transportverschlüsselung technischer Standard. Zur Datensynchronisierung und zum Backup seien keine statistischen Aussagen bekannt. Cloud-Kollaborationslösungen, bei denen parallel an Dokumenten oder Daten gearbeitet werde, synchronisierten in der Regel sofort. Bei reinen Cloud-Speicherlösungen könne die Synchronisation auch mit einer gewissen Zeitverzögerung stattfinden, etwa in dem Rhythmus, in dem ein Nutzer seine Dokumente manuell dort speichere oder die Anwendungen selbst ein automatisches Speichern auslösten. Die Frequenz des automatischen Speicherns lasse sich in einigen Office-Anwendungen manuell festlegen. Wie oft System-Backups durchgeführt würden, könne zwischen den Extremen – mehrmals am Tag und praktisch nie – stark variieren. Die üblichen Cloud-Speicher synchronisierten Daten 96

unmittelbar nach ihrer Speicherung. Die Daten würden also erst lokal gespeichert und dann synchronisiert. Die Häufigkeit von System-Backups könne auch insoweit stark variieren. Es lasse sich nicht von Standardverfahren oder einer Standardhäufigkeit sprechen.

Bei der klassischen Telekommunikationsüberwachung dürften die an die und von der Cloud übertragenen Inhaltsdaten aufgrund ihrer Verschlüsselung nicht lesbar sein. Sämtliche Metadaten einer Datenübertragung dürften aber zu sehen sein; darunter fielen zum Beispiel IP-Adressen der Endnutzer und des Cloud-Diensts, die für die Kommunikation verwendeten Ports, das verwendete Übertragungsprotokoll und die Kryptozertifikate der Kommunikationsbeteiligten. 97

Was Maßnahmen nach § 100a Abs. 1 Satz 3 StPO betreffe, erfolge die Überwachung nicht auf der Strecke, sondern nur am Endgerät. Ein Zugriff sei daher nur möglich, soweit ehemals laufende Kommunikation noch auf dem Endgerät vorhanden sei. Dies könne bei Cloud-Diensten (nur) in Form von lokalen Synchronisationsdaten der Fall sein, wie bei lokalen Zwischenkopien und Dateien im Cache (Arbeitsspeicher). Zudem könnten lokale Logdaten auf dem Endgerät vorhanden sein, die Aufschluss über Zeitstempel, IP-Adressen der Kommunikationsbeteiligten, die verwendeten Protokolle und Namen der übertragenen Dateien (z.B. bei Cloud-Speichern) enthalten könnten. Durch die Überwachung auf dem Endgerät könnten – sofern sie das System im Klartext speichere – auch Zugangsdaten zu den jeweiligen Cloud-Diensten erlangt werden. Potentiell könnten auch Zugangsschlüssel für die jeweiligen in der Cloud verschlüsselt gespeicherten Daten dazugehören. 98

l) aa) Die Gesellschaft für Freiheitsrechte ist der Ansicht, § 100a Abs. 1 Sätze 2 und 3 StPO seien als Eingriffe in das IT-System-Grundrecht verfassungsrechtlich nicht gerechtfertigt. Es bestehe das Risiko einer Ausspähung der Persönlichkeit. Die bislang formulierten präventiv-polizeilichen Anforderungen seien auf den repressiven Bereich zu übertragen. Denn bei der Strafverfolgung gehe es nicht darum, eine Rechtsgutsverletzung zu verhindern, sondern nur um die Sanktionierung einer bereits eingetretenen. Es fehle schon an hinreichenden verfahrensrechtlichen Regelungen in § 100e Absätze 3 und 4 StPO. Es sei nämlich schon nicht geregelt, dass das einzusetzende „technische Mittel" benannt und technisch spezifiziert werde. Es werde den Ermittlungsbehörden vertraut, die Staatstrojaner nach „Gutdünken" einsetzen könnten. Ein ausreichender Überprüfungsmechanismus sei aber rechtsstaatlich geboten. Erschwerend sei, dass die Software von externen Anbietern stammen könne, sodass die Ermittlungsbehörden mitunter selbst nicht einschätzen könnten, welche Funktionen sie habe. 99

Die Verantwortung für die Einhaltung der rechtlichen Anforderungen dürfe nicht auf die anordnenden Gerichte abgewälzt werden. Es bedürfe einer verpflichtenden Kontrolle auf Ebene des Quelltextes durch eine unabhängige Stelle, weil nur dadurch eine neutrale Begutachtung der Software gewährleistet werde. Ein Gesetz müsse im Lichte des 100

Wesentlichkeitsgrundsatzes eine unabhängige technische Überprüfung der einzusetzenden Staatstrojaner vorschreiben.

bb) Auf die Fragen des Senats berichtet die Gesellschaft für Freiheitsrechte, dass im privaten Bereich Clouds oft unbewusst genutzt würden, weil diese auf dem Betriebssystem vorinstalliert seien. Bei Betriebssystemen und Apps sei die Synchronisation oft automatisch aktiviert. Es seien tägliche Backups üblich und standardisiert eingestellt. Seriöse Cloud-Anbieter nutzten mindestens eine Transportverschlüsselung. 101

m) Die Gewerkschaft der Polizei hält die angegriffenen Befugnisse für praxisgerecht und verfassungsgemäß. Neue Verschlüsselungstechniken machten Ergänzungen bei strafprozessualen Eingriffsbefugnissen notwendig. Nur so könnten Strafverfolgungsbehörden weiterhin ihren gesetzlichen Aufgaben gerecht werden. Diese hätten Verfassungsrang, denn eine funktionstüchtige Strafrechtspflege sei Teil des Rechtsstaatsprinzips und letztlich auch Ausdruck der Wehrhaftigkeit der Demokratie. Rechtsfreie Räume der Kommunikation seien nicht hinzunehmen. Vielmehr müsse sichergestellt sein, dass strafrechtlich relevantes Handeln auch verfolgbar sei. Befugnisse zur Quellen-Telekommunikationsüberwachung und Online-Durchsuchung seien gerade in den Bereichen terroristischer, organisierter und allgemeiner schwerster Kriminalität nötig, um Netzwerkstrukturen zu durchdringen. 102

B.

Die fristgerecht am 7. August 2018 erhobene Verfassungsbeschwerde ist zu einem Teil unzulässig. In Bezug auf § 100b Abs. 2 Nr. 1 Buchstabe l StPO in der angegriffenen Fassung fehlt den Beschwerdeführenden das Rechtsschutzbedürfnis (I). Der Beschwerdeführer zu 3) hat seine Verfassungsbeschwerde nicht formgerecht eingelegt (II). Die übrigen in unterschiedlichem Umfang betroffenen Beschwerdeführenden haben die Möglichkeit einer Grundrechtsverletzung nur teilweise aufgezeigt (III). Im verbleibenden Umfang genügt die Verfassungsbeschwerde den Anforderungen der Subsidiarität (IV). Soweit die Verfassungsbeschwerde insgesamt zulässig ist (V), ist die Zuständigkeit des Bundesverfassungsgerichts gegeben (VI). 103

I.

In Bezug auf § 100b Abs. 2 Nr. 1 Buchstabe l StPO in der angegriffenen Fassung fehlt den Beschwerdeführenden das Rechtsschutzbedürfnis. Die Regelung ist nach Erhebung der Verfassungsbeschwerde mit dem Gesetz zur Verbesserung der strafrechtlichen Bekämpfung der Geldwäsche vom 9. März 2021 (BGBl I S. 327) mit Wirkung zum 18. März 2021 geändert worden (vgl. nunmehr § 100b Abs. 2 Nr. 1 Buchstabe m StPO). Aufgrund des dieser Änderung auch zukommenden materiellen Gewichts sind die Beschwerdeführenden durch die Altfassung nicht mehr beschwert (vgl. auch BVerfGE 87, 181 <194 f.>; 100, 271 <281 f.>; 104

108, 370 <383>). Sie haben ihre Verfassungsbeschwerde daraufhin weder auf die Neufassung umgestellt (vgl. BVerfGE 87, 181 <194>), noch ist ersichtlich, dass die Altfassung verfassungsrechtliche Fragen von grundsätzlicher Bedeutung aufwerfen könnte, die nicht ungeklärt bleiben dürften (vgl. auch BVerfGE 100, 271 <281 f.>).

II.

Die Verfassungsbeschwerde erlaubt, soweit sie den Beschwerdeführer zu 3) betrifft, nicht die erforderliche verlässliche Zurechnung des Erklärungsinhalts zum Urheber der Erklärung (vgl. BVerfGE 15, 288 <291 f.>; BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 48 m.w.N.). Der Beschwerdeschrift kann hier nicht ausreichend zuverlässig die Person entnommen werden, die die Verfassungsbeschwerde eingelegt hat. Der Beschwerdeführer zu 3) verwendet einen Künstlernamen, der die erforderliche hinreichende Individualisierung der Person für sich genommen nicht zulässt. Auch hat er zu solchermaßen individualisierenden Umständen nicht substantiiert ausgeführt; insbesondere fehlt eine nachvollziehbare und nicht nur vage bleibende Beschreibung seines künstlerischen Werdegangs und seiner Werke, anhand derer die Figur „(...)" personalisiert und ihre Verkehrsgeltung für die Öffentlichkeit erkennbar sein könnte. Insoweit kann auch der nach Ablauf der Jahresfrist gemäß § 93 Abs. 3 BVerfGG nachgereichte Schriftsatz vom 12. Juni 2023 der Verfassungsbeschwerde nicht mehr zur Zulässigkeit verhelfen (vgl. auch BVerfGE 169, 130 <167 f. Rn. 75> – Hessisches Verfassungsschutzgesetz). 105

III.

Die Beschwerdebefugnis der übrigen Beschwerdeführenden ist teilweise gegeben. 106

Nach Art. 94 Abs. 1 Nr. 4a GG, § 90 Abs. 1 BVerfGG setzt die Zulässigkeit einer Verfassungsbeschwerde unter anderem die Behauptung voraus, durch einen Akt der öffentlichen Gewalt in Grundrechten oder grundrechtsgleichen Rechten verletzt zu sein (vgl. BVerfGE 140, 42 <54 Rn. 47>). Dazu müssen sowohl die Möglichkeit der Grundrechtsverletzung als auch die eigene, unmittelbare und gegenwärtige Betroffenheit den Begründungsanforderungen nach § 23 Abs. 1 Satz 2, § 92 BVerfGG entsprechend dargelegt sein. Richtet sich die Verfassungsbeschwerde gegen ein Gesetz, das Sicherheitsbehörden zu heimlichen Überwachungsmaßnahmen ermächtigt, bestehen insoweit besondere Zulässigkeitsanforderungen (näher BVerfGE 165, 1 <30 ff. Rn. 39 ff.> – Polizeiliche Befugnisse nach SOG MV; stRspr). 107

1. Danach haben die Beschwerdeführenden nicht aufgezeigt, dass eine sich insbesondere aus dem IT-System-Grundrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) ergebende grundrechtliche Schutzpflicht verletzt sein könnte. Es fehlt an der verfassungsrechtlich gebotenen Darlegung (vgl. dazu BVerfGE 158, 170 <191 f. Rn. 51> – IT-Sicherheitslücken), dass unter Berücksichtigung des gesetzlichen Regelungszusammenhangs vom Versagen der gesetzgeberischen Konzeption auszugehen sein könnte. Insoweit nehmen sie insbesondere 108

die gesetzlichen Regelungen des zum Schutz von IT-Systemen anwendbaren Strafprozess-, Datenschutz- und Cybersicherheitsrechts nicht in den Blick (vgl. auch BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 53; Beschluss der 2. Kammer des Ersten Senats vom 17. April 2023 - 1 BvR 176/23 u.a. -, Rn. 6).

2. Die Möglichkeit einer Verletzung des IT-System-Grundrechts in seiner abwehrrechtlichen Dimension sowie des Art. 10 Abs. 1 GG wird teilweise aufgezeigt. 109

Die Beschwerdeführenden haben dargelegt, dass die Befugnisse zur Quellen-Telekommunikationsüberwachung nach § 100a Abs. 1 Sätze 2 und 3 StPO das IT-System-Grundrecht sowie in Bezug auf § 100a Abs. 1 Satz 2 StPO zugleich Art. 10 Abs. 1 GG verletzen könnten, soweit die Befugnisnormen – gemessen an ihrem Eingriffsgewicht – die Verfolgung nicht hinreichend gewichtiger Straftaten erlauben (a). Dargetan wird auch, dass die Befugnis zur Online-Durchsuchung in § 100b Abs. 1 StPO wegen ihres Eingriffs in das IT-System-Grundrecht sowie in Art. 10 Abs. 1 GG verfassungswidrig sein könnte, weil im Hinblick auf den Eingriff in Art. 10 Abs. 1 GG das Zitiergebot missachtet worden und im Hinblick auf beide Grundrechte ein nicht in jeder Hinsicht genügender Kernbereichsschutz vorgesehen sein könnte (b). 110

a) Die Beschwerdeführenden haben die Möglichkeit einer Grundrechtsverletzung aufgezeigt, soweit sie in Bezug auf die Quellen-Telekommunikationsüberwachung nach § 100a Abs. 1 Sätze 2 und 3 StPO ein nicht hinreichendes Gewicht der in § 100a Abs. 2 StPO genannten Straftaten rügen. Im Übrigen genügt ihr gegen § 100a Abs. 1 Sätze 2 und 3 in Verbindung mit § 100a Absätze 3 bis 6, § 100d Absätze 1, 2 und 5 StPO gerichteter Vortrag nicht den Darlegungsanforderungen. 111

aa) Die Beschwerdeführenden haben dargetan, dass die Quellen-Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 2 StPO sowohl in das IT-System-Grundrecht als auch in Art. 10 Abs. 1 GG eingreifen könnte. 112

Mit Blick auf § 100a Abs. 1 Satz 3 StPO haben sie dagegen nur einen möglichen Eingriff in das IT-System-Grundrecht aufgezeigt, nicht aber auch eine Betroffenheit des Fernmeldegeheimnisses aus Art. 10 Abs. 1 GG. So schützt Art. 10 Abs. 1 GG allein vor den spezifischen Gefahren, die mit einer räumlich distanzierten Kommunikation einhergehen, da diese auf einen technischen Übermittlungsvorgang angewiesen ist, der nicht im ausschließlichen Einflussbereich Betroffener liegt, weshalb sie in besonderer Weise einer Kenntnisnahme durch Dritte ausgesetzt ist (vgl. BVerfGE 115, 166 <182, 186>; näher BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 87 f. m.w.N.). Der Grundrechtsschutz aus Art. 10 Abs. 1 GG erstreckt sich daher nicht auf die außerhalb eines laufenden Kommunikationsvorgangs im Herrschaftsbereich der Betroffenen – also nach Abschluss des Übertragungsvorgangs – gespeicherten Inhalte und Umstände einer Kommunikation (vgl. BVerfGE 115, 166 <183 f.>; 120, 274 <307 f.>; 124, 43 <54>). Unter Zugrundelegung dieses 113

Maßstabs haben die Beschwerdeführenden nicht aufgezeigt, dass die nach § 100a Abs. 1 Satz 3 StPO erlaubte Überwachung und Aufzeichnung der auf dem IT-System Betroffener gespeicherten Inhalte und Umstände früherer Kommunikation den Gewährleistungsgehalt des Art. 10 Abs. 1 GG verkürzen könnte. Sie haben sich schon nicht damit auseinandergesetzt, dass der den grundrechtsspezifischen Schutzbedarf begründende Übertragungsvorgang bereits abgeschlossen ist und sich die Daten im Herrschaftsbereich der Betroffenen befinden.

bb) Die Beschwerdeführenden haben aufgezeigt, dass die dargelegten Grundrechtseingriffe nicht gerechtfertigt sein könnten, soweit die Befugnisse nach § 100a Abs. 1 Sätze 2 und 3 StPO Quellen-Telekommunikationsüberwachungen bereits zur Verfolgung von – gemessen an ihrem Eingriffsgewicht – nicht hinreichend gewichtigen Straftaten erlauben. Im Übrigen genügt ihr Vortrag nicht den Darlegungsanforderungen. 114

(1) Soweit die Beschwerdeführenden rügen, § 100a Abs. 1 Satz 2 StPO sei widersprüchlich und verfassungswidrig, da ausgeschlossen sei, dass die nach § 100a Abs. 5 Satz 1 Nr. 1 StPO erforderliche technische Beschränkung der Überwachung auf laufende Kommunikation in absehbarer Zukunft geschaffen werden könne, differenzieren sie weder danach, inwieweit es für die Frage der Beschränkbarkeit auf den möglichen Datenzugriff durch die eingesetzte Überwachungssoftware selbst oder auf die Ermöglichung der Kenntnisnahme durch die Überwachungspersonen ankommt, noch stellen sie eine entsprechende Beschränkbarkeit der Quellen-Telekommunikationsüberwachung in tatsächlicher Hinsicht substantiiert infrage (vgl. auch BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 59 ff.). 115

(2) Soweit die Beschwerdeführenden die Unverhältnismäßigkeit der Befugnis zur Quellen-Telekommunikationsüberwachung rügen, ist ihr Vortrag nur hinsichtlich einer möglichen Unangemessenheit wegen eines teilweise fehlenden hinreichenden Gewichts der in Bezug genommenen Straftaten hinreichend substantiiert. 116

(a) Der gegen die Eignung der Quellen-Telekommunikationsüberwachung gerichtete Vortrag genügt nicht den Darlegungsanforderungen. Vor dem Hintergrund, dass für die Eignung im verfassungsrechtlichen Sinne bereits die Möglichkeit genügt, durch die gesetzliche Regelung den Gesetzeszweck zu erreichen, und eine Regelung daher erst dann nicht mehr geeignet ist, wenn sie die Erreichung des Gesetzeszwecks in keiner Weise fördern kann oder sich sogar gegenläufig auswirkt (vgl. BVerfGE 161, 299 <367 f. Rn. 166> – Impfnachweis <Covid-19> m.w.N.), haben die Beschwerdeführenden nicht aufgezeigt, dass die hier angegriffenen Befugnisse die von § 100a StPO bezweckte Strafverfolgung nicht zumindest fördern könnten. Zwar geht mit der Durchführung einer Quellen-Telekommunikationsüberwachung regelmäßig eine Infiltration mit einer Überwachungssoftware und damit eine technische Veränderung des Zielsystems einher (vgl. Rn. 194; vgl. auch BVerfG, 117

Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 114 m.w.N.; BKA, Standardisierende Leistungsbeschreibung für Software zur Durchführung von Maßnahmen der Quellen-Kommunikationsüberwachung und der Online-Durchsuchung, 2018, S. 5). Auch haben Ermittlungsbehörden über eine längere Zeit einen tatsächlichen Zugriff auf das gesamte System, dessen Inhalt sie bewusst oder unbewusst manipulieren könnten. Gleichwohl haben die Beschwerdeführenden nicht substantiiert dargelegt, dass der Beweiswert der mittels einer Quellen-Telekommunikationsüberwachung gewonnenen Daten regelmäßig „gleich Null" sein könnte. Denn ungeachtet dessen, dass der Nachweis der Authentizität von Daten bei einer Erhebung mittels einer Überwachungssoftware technisch schwierig sein kann, haben sie nicht aufgezeigt, dass mittels einer Überwachungssoftware nach § 100a Abs. 1 Sätze 2 oder 3 StPO niemals Beweise gewonnen werden könnten, auf die ein Strafgericht – nach Beweiswürdigung unter gegebenenfalls sachverständiger Hilfe – seine Überzeugung im Sinne von § 261 StPO und eine Verurteilung (mit-)stützen könnte (vgl. dazu auch Hauck, in: Löwe-Rosenberg, StPO, 27. Aufl. 2019, § 100b Rn. 92; Rückert, in: Münchener Kommentar zur StPO, 2. Aufl. 2023, § 100b Rn. 13, 75). Dagegen führt ein möglicherweise begrenzter Beweiswert von Erkenntnissen, die mittels eines solchen Zugriffs gewonnen werden können, nicht zur Ungeeignetheit (vgl. BVerfGE 120, 274 <320 f.>).

(b) Die Beschwerdeführenden haben auch nicht aufgezeigt, dass die Befugnisse nach § 100a Abs. 1 Sätze 2 und 3 StPO nicht im verfassungsrechtlichen Sinne erforderlich wären. Soweit sie auf die offene Durchsuchung und anschließende Auswertung sichergestellter IT-Systeme gemäß §§ 94 ff., 102 ff. StPO als mögliche mildere Mittel hinweisen, ist nicht dargetan, dass diese gleich wirksam (vgl. dazu BVerfGE 161, 299 <378 Rn. 187>) sein können. Insoweit fehlt schon eine Auseinandersetzung damit, dass der offene Zugriff auf ein IT-System zum Beispiel an Zugangssicherungen und Speicherverschlüsselungen scheitern könnte. Jedenfalls aber haben die Beschwerdeführenden nicht berücksichtigt, dass der offene Zugriff auf ein IT-System zum einen überhaupt nur eine Maßnahme nach § 100a Abs. 1 Satz 3 StPO ersetzen kann, da nur diese – anders als eine Maßnahme nach § 100a Abs. 1 Satz 2 StPO – auf gespeicherte frühere und nicht erst auf künftig stattfindende Kommunikation gerichtet ist. Zum anderen legen Behörden mit Maßnahmen nach §§ 94 ff., 102 ff. StPO ihre Ermittlungen offen, wodurch Beschuldigte sowie ein mögliches kriminelles Umfeld gewarnt und veranlasst werden könnten, Verdunkelungsmaßnahmen zu ergreifen. 118

(c) Die Beschwerdeführenden haben aber dargelegt, dass die Befugnisse zur Quellen-Telekommunikationsüberwachung nach § 100a Abs. 1 Sätze 2 und 3 StPO verfassungswidrig sein könnten, soweit sie in § 100a Abs. 1 Satz 1 Nr. 1, Abs. 2 StPO an – gemessen an ihrem Eingriffsgewicht – nicht hinreichend gewichtige Straftaten anknüpfen. Im Übrigen genügt ihr Vortrag nicht den Darlegungsanforderungen. 119

(aa) Die Beschwerdeführenden rügen, die Befugnisse in § 100a Abs. 1 Sätze 2 und 3 StPO knüpften nicht an hinreichend gewichtige Straftaten an. Die Befugnisse zur Quellen-Telekommunikationsüberwachung seien aufgrund ihres sehr hohen Eingriffsgewichts nicht verhältnismäßig, weil § 100a Abs. 1 Satz 1 Nr. 1 StPO als Eingriffsanlass lediglich den Tatverdacht für eine der vielfältigen Anlasstaten nach § 100a Abs. 2 StPO voraussetze, die nicht die Qualität der in § 100b Abs. 2 StPO genannten Anlassstraftaten erreichen müssten. Dieser Vortrag erfüllt die Darlegungsanforderungen. Da sich die Beschwerdeführenden allerdings nicht mit dem Gewicht der einzelnen in § 100a Abs. 2 StPO genannten Straftatbestände auseinandergesetzt haben, gilt dies nur insoweit, als das Gewicht der dort genannten Straftaten ohne Weiteres etwa anhand ihrer Strafrahmen bestimmt werden kann. Soweit es dagegen für die Bestimmung des Straftatengewichts auf weitere Umstände wie das geschützte Rechtsgut, Begehungsmerkmale oder Tatfolgen ankommt, fehlen Darlegungen dazu, warum die konkret in § 100a Abs. 2 StPO genannten Straftaten auf Grundlage der insoweit anwendbaren verfassungsrechtlichen Maßstäbe (vgl. BVerfGE 109, 279 <344>; 129, 208 <243 f.>; 169, 130 <220 Rn. 206>; dazu Rn. 207 ff.) nicht besonders schwer wiegen könnten. Schon mangels Rechtsschutzbedürfnisses ausgenommen ist darüber hinaus § 100b Abs. 2 Nr. 1 Buchstabe l StPO in der angegriffenen Fassung (dazu Rn. 104). 120

(bb) Dass die angegriffenen Regelungen in § 100a Abs. 1 Sätze 2 und 3 StPO auch deshalb verfassungswidrig sein könnten, weil die anordnende Stelle nicht gesetzlich verpflichtet wird, die Anforderungen der Angemessenheit bei Anordnung einer konkreten Maßnahme zu beachten, ist nicht hinreichend dargetan. Zwar stellen die Beschwerdeführenden insoweit nicht in Abrede, dass das anordnende Gericht – auch ohne eine entsprechende gesetzliche Regelung – verpflichtet ist, in jedem Einzelfall zu prüfen, ob eine Maßnahme insgesamt verhältnismäßig ist (vgl. dazu auch BVerfGE 141, 220 <266 f. Rn. 97> – Bundeskriminalamtgesetz I; 162, 1 <131 Rn. 288> – Bayerisches Verfassungsschutzgesetz). Warum es aber geboten sein könnte, dass diese schon von Verfassungs wegen bestehende Pflicht zusätzlich im Fachrecht abgesichert wird, haben sie allein mit ihrem Hinweis auf die Eingriffsintensität der Maßnahme und die „Ausstrahlungswirkung" des IT-System-Grundrechts nicht substantiiert dargelegt. Unabhängig davon wird § 100e Abs. 4 Satz 1, Satz 2 Nr. 2 StPO nicht in den Blick genommen, wonach die Anordnung einer Quellen-Telekommunikationsüberwachung einzelfallbezogen die wesentlichen Erwägungen zur Verhältnismäßigkeit der Maßnahme angeben muss. Warum daraus nicht folgen könnte, dass das anordnende Gericht zuvor diese Verhältnismäßigkeit auch zu prüfen hat, wird nicht erörtert. 121

(cc) Auch verfassungsrechtliche Mängel bezüglich der von den Beschwerdeführenden als nicht zureichend gerügten unabhängigen Vorabkontrolle werden nicht aufgezeigt. Insoweit fehlt schon eine selbstständig tragende verfassungsrechtliche Herleitung einer neben dem gesetzlichen Richtervorbehalt (vgl. § 100e Abs. 1 Satz 1 StPO) erforderlichen unabhängigen Vorabkontrolle zur Prüfung der Voraussetzungen des § 100a Abs. 5 StPO (vgl. auch BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 70). 122

Soweit die Beschwerdeführenden eine effektive Prüfung durch den Richtervorbehalt nicht gewährleistet sehen, haben sie sich insbesondere nicht damit auseinandergesetzt, dass es Aufgabe und Pflicht des anordnenden Gerichts ist, sich eigenverantwortlich ein Urteil darüber zu bilden, ob die beantragte Überwachungsmaßnahme den gesetzlichen Voraussetzungen entspricht (vgl. BVerfGE 109, 279 <359>; 141, 220 <275 Rn. 118>).

(dd) Soweit die Beschwerdeführenden schließlich zur Begründung der Unangemessenheit der Befugnisse zur Quellen-Telekommunikationsüberwachung pauschal auf ihre gegenüber § 100b StPO erhobenen Rügen Bezug nehmen, haben sie diese nicht in Bezug auf § 100a Abs. 1 Sätze 2 und 3 StPO aufbereitet. Ungeachtet dessen sind die gegen § 100b StPO insoweit erhobenen Rügen unzulässig (vgl. unten Rn. 132 ff.), ohne dass dargelegt oder sonst ersichtlich wäre, warum hinsichtlich § 100a Abs. 1 Sätze 2 und 3 StPO eine andere Beurteilung geboten sein könnte. 123

(3) Die Beschwerdeführenden haben auch nicht aufgezeigt, dass § 100a Abs. 1 Sätze 2 und 3 StPO nicht den besonderen Anforderungen genügen könnten, die sich aus den jeweiligen Grundrechten in Verbindung mit Art. 1 Abs. 1 GG für die Durchführung von besonders eingriffsintensiven Überwachungsmaßnahmen an den Schutz des Kernbereichs privater Lebensgestaltung ergeben. Entsprechendes gilt, soweit die Beschwerdeführenden Art. 1 Abs. 1 GG isoliert gerügt haben. 124

(a) Es fehlt schon eine Auseinandersetzung mit den verfassungsgerichtlich ausformulierten Maßstäben zum grundrechtlichen Würdeanspruch im Allgemeinen und bei heimlichen Überwachungsmaßnahmen im Besonderen. Auch die verfassungsrechtlichen Maßstäbe zum Schutz des Kernbereichs haben die Beschwerdeführenden nicht näher in den Blick genommen. Soweit dieser einer freien, seine Bedeutung relativierenden Abwägung mit staatlichen Sicherheitsinteressen nicht zugänglich ist, berücksichtigen sie nicht, dass nicht jede tatsächliche Erhebung von höchstpersönlichen Informationen stets eine Menschenwürdeverletzung begründet. Absolut ausgeschlossen ist es zwar, den Kernbereich zum Ziel staatlicher Ermittlungen zu machen und diesbezügliche Informationen in irgendeiner Weise zu verwerten oder sonst zur Grundlage weiterer Ermittlungen zu machen (vgl. BVerfGE 141, 220 <278 Rn. 125>). Im Übrigen aber ist auf der Erhebungsebene ein Eindringen in den Kernbereich grundsätzlich nur insoweit zu vermeiden, als dies mit praktisch zu bewältigendem Aufwand möglich ist (vgl. BVerfGE 141, 220 <279 Rn. 128>; 165, 1 <61 Rn. 111>; stRspr); erst auf der Verwertungsebene sind die Folgen einer dennoch erfolgten Erhebung strikt zu minimieren (vgl. BVerfGE 141, 220 <278 f. Rn. 124, 126>). 125

(b) Dass die in § 100d Abs. 1 StPO für die Erhebungsebene geregelten Sicherungen des Kernbereichs dem nicht genügen könnten, haben die Beschwerdeführenden mit ihrer allein mit Blick auf § 100b Abs. 1 StPO näher begründeten Rüge nicht aufgezeigt. Insbesondere berücksichtigen sie nicht, dass die verfassungsrechtlichen Anforderungen an den 126

Kernbereichsschutz im Hinblick auf verschiedene Überwachungsmaßnahmen unterschiedlich ausfallen können (vgl. dazu BVerfGE 141, 220 <279 Rn. 127>) und der Schutz abhängig von dem Charakter einer bestimmten Maßnahme auch zu einem großen Teil von der Erhebungsebene auf die nachgelagerte Aus- und Verwertungsebene verschoben sein kann (vgl. BVerfGE 141, 220 <306 f. Rn. 218 f.>; 162, 1 <129 f. Rn. 284>). Die Beschwerdeführenden hätten insoweit konkret darzulegen gehabt, inwieweit unter Berücksichtigung des spezifischen Charakters einer Quellen-Telekommunikationsüberwachung eine Verschärfung des auf Erhebungsebene bestehenden Kernbereichsschutzes geboten sein könnte. Eine solche Darlegung ist nicht erfolgt. Soweit sie auch einen mangelnden Schutz auf der Verwertungsebene rügen, übersehen sie das in § 100d Abs. 2 StPO geregelte absolute Verwertungsverbot; in Bezug auf die gegen § 100d Abs. 5 StPO gerichtete Rüge kann auf die Ausführungen zur Online-Durchsuchung verwiesen werden (unten Rn. 152).

b) Der gegen die Befugnis zur Online-Durchsuchung nach § 100b Abs. 1 StPO gerichtete Vortrag genügt in weiten Teilen nicht den Begründungsanforderungen. 127

Die Beschwerdeführenden zeigen zwar auf, dass die angegriffene Regelung nicht nur in das IT-System-Grundrecht, sondern auch in Art. 10 Abs. 1 GG eingreifen und deshalb das Zitiergebot missachtet worden sein könnte (aa). Eine mögliche Unverhältnismäßigkeit der Eingriffe in beide Grundrechte ist aber weitgehend nicht dargetan (bb). Lediglich in Bezug auf einen Teilaspekt des Kernbereichsschutzes genügt ihr Vortrag den Darlegungsanforderungen (cc). 128

aa) Die Beschwerdeführenden haben hinreichend dargelegt, dass Art. 10 Abs. 1 GG deshalb verletzt sein könnte, weil der Gesetzgeber dieses Grundrecht bei Einführung der Online-Durchsuchung nach § 100b Abs. 1 StPO unter Missachtung des Zitiergebots (Art. 19 Abs. 1 Satz 2 GG) nicht als eingeschränkt genannt hat. 129

bb) Der gegen die Verhältnismäßigkeit der Maßnahme gerichtete Vortrag genügt dagegen nicht den Darlegungsanforderungen. 130

(1) Eine möglicherweise fehlende Eignung des § 100b Abs. 1 StPO wird nicht aufgezeigt (vgl. zu § 100a Abs. 1 Sätze 2 und 3 StPO näher Rn. 117). Dies gilt auch für die als fehlend gerügte Erforderlichkeit (vgl. Rn. 118), wobei die Beschwerdeführenden in Bezug auf die Online-Durchsuchung zudem auch deren gegenüber offenen Maßnahmen potentiell höheren Aufklärungserfolg nicht in den Blick genommen haben. Denn eine Online-Durchsuchung ermöglicht – anders als etwa eine Durchsuchung und Beschlagnahme eines IT-Systems – nicht nur einen Zugriff auf einen bestehenden Datenbestand, sondern eine darüber hinausgehende künftige Überwachung, weil nach Aufspielen einer Überwachungssoftware auch erst später erzeugte Daten ausgeleitet werden können. 131

(2) Die Beschwerdeführenden haben auch nicht aufgezeigt, dass die Online-Durchsuchung nach § 100b Abs. 1 StPO unverhältnismäßig im engeren Sinne sein könnte. 132

(a) Mögliche verfassungsrechtliche Mängel im Hinblick auf das Gewicht der in § 100b Abs. 2 StPO genannten Straftaten sind nicht dargetan. 133

(aa) Dies gilt zunächst für die Rüge, das Gewicht einer Vielzahl der in § 100b Abs. 2 StPO genannten Straftaten korreliere nicht mit den Anforderungen an die bei einer präventiven Online-Durchsuchung zu schützenden überragend wichtigen Rechtsgüter; eine repressive Online-Durchsuchung dürfe aber nur zugunsten solcher Rechtsgüter erfolgen, die hinreichend gewichtig seien, um eine vergleichbare präventive Maßnahme zu rechtfertigen. Insoweit fehlt schon eine Auseinandersetzung mit der verfassungsgerichtlichen Rechtsprechung: Danach kommt es für Maßnahmen, die der Strafverfolgung dienen und damit repressiven Charakter haben, auf das Gewicht der Straftaten an, die der Gesetzgeber in – jeweils näher bestimmte – erhebliche, schwere und besonders schwere Straftaten eingeteilt hat (vgl. BVerfGE 141, 220 <270 Rn. 107> mit Bezugnahme auf BVerfGE 109, 279 <343 ff.>; vgl. auch BVerfGE 162, 1 <118 Rn. 251>; 169, 130 <218 Rn. 202>). Maßgeblich für die Schwere des tatbestandlichen Unrechts sind der Rang des verletzten Rechtsguts und andere tatbestandlich umschriebene, gegebenenfalls auch in einem Qualifikationstatbestand enthaltene Begehungsmerkmale und weitere Tatfolgen. Sie allein müssen die besondere, deutlich über dem Durchschnitt liegende Schwere des jeweiligen Straftatbestandes begründen (BVerfGE 109, 279 <344>). Dabei gibt der Strafrahmen einer Deliktsnorm einen maßgebenden Anhaltspunkt dafür, ob es sich abstrakt um eine – wie hier erforderliche – besonders schwere Straftat handelt (vgl. BVerfGE 109, 279 <347>; 125, 260 <329>; 169, 130 <218 f. Rn. 202>). Ausgehend vom Strafrahmen einer Strafnorm liegt die besondere Schwere einer Straftat jedenfalls dann vor, wenn sie mit einer Höchstfreiheitsstrafe von mehr als fünf Jahren bedroht ist (vgl. BVerfGE 109, 279 <347 f., 349>; 165, 1 <93 Rn. 179>; 169, 130 <219 Rn. 203>). 134

(bb) Auch die konkrete Einordnung einzelner in § 100b Abs. 2 StPO genannter Straftatbestände als besonders schwer wird nicht substantiiert gerügt. Die verfassungsrechtlichen Maßstäbe, nach denen sich bemisst, ob der Gesetzgeber in zulässiger Ausfüllung seines Spielraums einen bestimmten Straftatbestand als besonders schwer bewertet hat, sind geklärt (vgl. zuletzt BVerfGE 169, 130 <218 ff. Rn. 201 ff.> m.w.N.; näher Rn. 209 ff.). Dass die einzelnen in § 100b Abs. 2 StPO genannten Katalogtaten hinter diesen Maßstäben zurückbleiben könnten, haben die Beschwerdeführenden nicht aufgezeigt. 135

(b) Die Rüge, der Gesetzgeber habe eine Online-Durchsuchung in § 100b Abs. 1 Nr. 1 StPO nur von einem qualifizierten Anfangsverdacht und damit von einer zu niedrigen Eingriffsschwelle abhängig gemacht, genügt nicht den Darlegungsanforderungen. Zwar ist neben der Schwere der Tat auch die Stärke des Tatverdachts mitentscheidend dafür, ob eine 136

strafprozessuale Ermittlungsmaßnahme in einem angemessenen Verhältnis zu dem Gewicht der Grundrechtsbeeinträchtigung steht (vgl. BVerfGE 107, 299 <322>). Die Beschwerdeführenden haben aber nicht aufgezeigt, dass es in Anbetracht der Eingriffsintensität einer Online-Durchsuchung verfassungsrechtlich geboten sein könnte, die Maßnahme vom Vorliegen eines höheren, insbesondere „hinreichend schweren Tatverdachts“ abhängig zu machen. Insoweit fehlt schon eine vertiefte Auseinandersetzung mit der verfassungsgerichtlichen Rechtsprechung, wonach der qualifizierte Anfangsverdacht („bestimmte Tatsachen den Verdacht begründen“) einerseits einen Tatverdacht darstellt, der jedenfalls über einen Anfangsverdacht hinausreicht, wie er Voraussetzung für die Einleitung eines Ermittlungsverfahrens ist (vgl. BVerfGE 109, 279 <350 f.>; 129, 208 <268>; Rückert, in: Münchener Kommentar zur StPO, 2. Aufl. 2023, § 100b Rn. 51), und andererseits einen Verdachtsgrad aufweist, der für die vergleichbar eingriffsintensive Wohnraumüberwachung eine hinreichende Eingriffsschwelle bildet (vgl. BVerfGE 109, 279 <350 f.>). Zudem wird nicht in den Blick genommen, dass es gerade Sinn und Zweck eines Ermittlungsverfahrens ist, den zunächst nur zureichenden Verdacht im Sinne des § 152 Abs. 2 StPO zu einem für die Anklageerhebung erforderlichen Tatverdacht gemäß § 170 Abs. 1 StPO zu erhärten oder den Beschuldigten zu entlasten. Als Mittel der Sachverhaltserforschung sollen daher Ermittlungsmaßnahmen wie die Quellen-Telekommunikationsüberwachung den für eine Anklageerhebung (§ 170 Abs. 1 StPO) oder später den Eröffnungsbeschluss (§ 203 StPO) erforderlichen hinreichenden oder gar den für die Verhängung der Untersuchungshaft (§ 112 Abs. 1 Satz 1 StPO) geforderten dringenden Tatverdacht erst noch erbringen. Sie können ihn deshalb nicht schon für ihre Zulässigkeit voraussetzen (vgl. dazu auch BVerfGE 109, 279 <351 f.>). Letztlich haben die Beschwerdeführenden auch nicht substantiiert aufgezeigt, weshalb es verfassungsrechtlich zu beanstanden sein könnte, dass das anordnende Gericht bei der Tatverdachtsprognose einen Spielraum hat (vgl. dazu BVerfG, Vorprüfungsausschuss, Beschluss vom 8. November 1983 - 2 BvR 1138/83 -, NJW 1984, S. 1451 <1452>).

(c) Die weitere Rüge der Beschwerdeführenden, eine Online-Durchsuchung sei unverhältnismäßig, weil der Zugriff auf IT-Systeme „anderer Personen“ nicht subsidiär ausgestaltet und nicht von einer auf Tatsachen basierenden Erfolgsprognose abhängig sei, leidet an einer unvollständigen Auseinandersetzung mit dem Normtext von § 100b StPO und der bisherigen Rechtsprechung des Bundesverfassungsgerichts. Für die Einbeziehung von Dritten in heimliche Überwachungsmaßnahmen ergeben sich besondere Anforderungen aus dem Grundsatz der Verhältnismäßigkeit (vgl. BVerfGE 109, 279 <356 f.>; 141, 220 <274 Rn. 115>; 162, 1 <99 f. Rn. 210 f.>). Voraussetzung hierfür ist, dass der Zugriff allein auf die IT-Systeme der eigentlich beschuldigten Person nicht zur Erreichung des Ermittlungsziels ausreicht; die Anordnung einer Online-Durchsuchung, die auf das IT-System von Dritten zielt, muss insofern subsidiär sein. Darüber hinaus bedarf es tatsächlicher Anhaltspunkte dafür, dass dort ermittlungsrelevante Informationen gespeichert sind und die Überwachungsmaßnahme daher der Sachverhaltsaufklärung dienlich sein wird. Bloße 137

Vermutungen genügen insoweit nicht; eine Überwachung „ins Blaue hinein", allein getragen von der Hoffnung auf Erkenntnisse, ist ausgeschlossen.

Dass der Gesetzgeber diesen besonderen Anforderungen nicht entsprochen haben könnte, haben die Beschwerdeführenden nicht aufgezeigt. § 100b Abs. 3 Satz 2 Nr. 2 StPO verbürgt ausdrücklich die verfassungsrechtlich verlangte Subsidiarität. Im Hinblick auf das Erfordernis einer tatsachengestützten Erfolgsprognose setzt zwar § 100b Abs. 3 Satz 2 Nr. 1 StPO lediglich tatsächliche Anhaltspunkte dafür voraus, dass der Beschuldigte das IT-System der anderen Person nutzt. Die Beschwerdeführenden haben sich aber weder damit auseinandergesetzt, ob eine tatsachenbasierte Auffindewahrscheinlichkeit relevanter Informationen aus Gründen der Verhältnismäßigkeit nicht schon bei Anwendung der Vorschrift vorausgesetzt werden muss (vgl. BVerfGE 141, 220 <292 Rn. 168>; vgl. auch BVerfGE 113, 29 <57>; 115, 166 <197>), noch damit, inwiefern die Regelung dahin ausgelegt werden könnte, dass zugleich eine hinreichende Wahrscheinlichkeit bestehen muss, durch einen Zugriff auf dieses System verfahrensrelevante Informationen zu gewinnen (vgl. BVerfGE 141, 220 <291 f. Rn. 167 f., 297 f. Rn. 188, 310 f. Rn. 233>). 138

(d) Die Beschwerdeführenden haben auch nicht aufgezeigt, dass die in § 100b Abs. 1 Nr. 3 StPO enthaltene Subsidiaritätsklausel, wonach die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsorts des Beschuldigten „auf andere Weise wesentlich erschwert oder aussichtslos" sein muss, nicht den Anforderungen der Verhältnismäßigkeit genügen könnte. 139

(aa) Es ist nicht dargetan, dass die Strafverfolgungsbehörden allein aufgrund der identischen Formulierungen in § 100a Abs. 1 Satz 1 Nr. 3 und § 100b Abs. 1 Nr. 3 StPO frei zwischen der Anordnung einer Telekommunikationsüberwachungsmaßnahme und einer Online-Durchsuchung wählen könnten. Insoweit haben die Beschwerdeführenden nicht erwogen, dass Strafverfolgungsbehörden schon aus Gründen der Verhältnismäßigkeit im Einzelfall verfassungsrechtlich gehalten sein könnten, zunächst eine Maßnahme auf Grundlage von § 100a Abs. 1 StPO in Betracht zu ziehen. Denn lässt sich ein Sachverhalt erwartungsgemäß mit mehreren Ermittlungsmaßnahmen gleich effektiv erforschen, ist es Ausfluss der Verhältnismäßigkeit, derjenigen Maßnahme den Vorzug zu geben, die den relativ milderen Eingriff darstellt (vgl. auch Hauck, in: Löwe-Rosenberg, StPO, 27. Aufl. 2019, § 100a Rn. 45, § 110a Rn. 37; Henrichs/Weingast, in: Karlsruher Kommentar zur StPO, 9. Aufl. 2023, § 110a Rn. 22). Entsprechend ist auch der Gesetzgeber davon ausgegangen, dass die gegenüber Telekommunikationsmaßnahmen eingriffsintensivere Online-Durchsuchung nur angewendet wird, wenn andere Ermittlungsmaßnahmen versagen (vgl. BTAusschussdrucks 18<6>334, S. 25). 140

(bb) Auch dass der Gesetzgeber das Rangverhältnis zwischen § 100b StPO und § 100c StPO im Hinblick auf die unterschiedlichen Subsidiaritätsklauseln in § 100b Abs. 1 Nr. 3 StPO 141

(„wesentlich erschwert oder aussichtslos“) und in § 100c Abs. 1 Nr. 4 StPO („unverhältnismäßig erschwert oder aussichtslos“) verfassungsrechtlich unzureichend geregelt haben könnte, liegt nicht nahe.

142 So haben die Beschwerdeführenden schon im Ausgangspunkt nicht aufgezeigt, warum eine mögliche Subsidiarität von § 100c StPO gegenüber § 100b StPO ein verfassungsrechtliches Problem sein könnte. Beide Maßnahmen haben eine jedenfalls vergleichbare Eingriffsintensität (vgl. BVerfGE 141, 220 <298 f. Rn. 192, 304 Rn. 210, 338 Rn. 316>; vgl. auch BTDrucks 18/12785, S. 54). Dies vermag auch die Verfassungsbeschwerde unbeschadet der steigenden gesellschaftlichen Relevanz von IT-Systemen nicht substantiiert infrage zu stellen. Insbesondere zeigt sie nicht auf, dass mit einem Bedeutungszuwachs von IT-Systemen zwingend ein Bedeutungsverlust der Wohnung als dem von Art. 13 Abs. 1 GG geschützten Objekt einherginge und die Wohnung nicht mehr den zentralen und grundrechtlich besonders geschützten privaten Rückzugsort, in dem Individuen ihre eigene Persönlichkeit frei entfalten können, bildete (vgl. insoweit BVerfGE 109, 279 <313 f.>). Wenn aber der Gesetzgeber vor diesem Hintergrund die Wohnraumüberwachung gegenüber der Online-Durchsuchung als grundsätzlich subsidiär ausgestaltet haben sollte, so hätten sich die Beschwerdeführenden mit dem naheliegenden Argument befassen müssen, ob es nicht vom gesetzgeberischen Gestaltungsspielraum gedeckt sein könnte, unter vergleichbar eingriffsintensiven Maßnahmen eine Vorrangentscheidung zu treffen.

143 Unabhängig hiervon fehlt es auch an Ausführungen dazu, ob und inwieweit § 100c Abs. 1 Nr. 4 und § 100b Abs. 1 Nr. 3 StPO tatsächlich eine Subsidiarität der Wohnraumüberwachung gegenüber der Online-Durchsuchung zum Ausdruck bringen. So ließe sich der Wortlaut des § 100c Abs. 1 Nr. 4 StPO schon damit erklären, dass der Gesetzgeber erkennbar nur die entsprechende Formulierung in Art. 13 Abs. 3 GG aufgreifen wollte (vgl. auch BVerfGE 109, 279 <341>). Hierauf sind die Beschwerdeführenden aber ebenso wenig eingegangen wie auf Ansichten im Schrifttum, wonach § 100b Abs. 1 Nr. 3 und § 100c Abs. 1 Nr. 4 StPO dahingehend auszulegen seien, dass zwischen der Online-Durchsuchung und der Wohnraumüberwachung gerade kein vom Einzelfall gelöstes Subsidiaritätsverhältnis bestehe (vgl. Ruppert, in: Dietrich/Fahrner/Gazeas et al., Handbuch Sicherheits- und Staatsschutzrecht, 2022, § 23 Rn. 77 f.; vgl. auch Rückert, in: Münchener Kommentar zur StPO, 2. Aufl. 2023, § 100c Rn. 38).

144 (e) Die Rüge, der Gesetzgeber habe ausreichende Absicherungen vor einer Totalüberwachung aufgrund additiver Grundrechtseingriffe unterlassen, genügt ebenfalls nicht den Darlegungsanforderungen. Das Bundesverfassungsgericht hat ausdrücklich entschieden, dass Behörden das Verbot einer Rundumüberwachung als Ausprägung des Verhältnismäßigkeitsgrundsatzes unmittelbar von Verfassungs wegen im Rahmen ihrer Befugnisse von sich aus zu beachten haben und dass es insoweit keiner weiteren gesetzlichen Konkretisierungen bedarf (vgl. BVerfGE 141, 220 <317 f. Rn. 254>; 162, 1 <130 f. Rn. 287 f.>).

Warum in Abänderung dieser Rechtsprechung weitere gesetzliche Schutzvorkehrungen gegen additive Grundrechtseingriffe erforderlich sein könnten, haben die Beschwerdeführenden nicht substantiiert dargelegt.

Nichts anderes gilt für die weitere Rüge, es bedürfe einer gesetzlichen Verpflichtung, dem anordnenden Gericht Auskunft über alle bereits ergriffenen und geplanten repressiven und präventiven heimlichen Überwachungsmaßnahmen gegen Betroffene zu geben sowie die daraus gewonnenen Erkenntnisse detailliert mitzuteilen. Die Beschwerdeführenden haben schon nicht erörtert, ob die dadurch erstrebte Verbesserung unabhängiger Kontrolle in einem angemessenen Verhältnis zu den Grundrechtsbelastungen stünde, die damit verbunden sein könnten. Zwar kann davon ausgegangen werden, dass die hierfür erforderliche Koordination innerhalb der jeweiligen Ermittlungsbehörde selbst gewährleistet ist (vgl. dazu BVerfGE 162, 1 <131 Rn. 288>) und diese dem anordnenden Gericht ohne Weiteres entsprechende Auskünfte erteilen kann. Sollte aber sichergestellt werden, dass dem anordnenden Gericht auch behördenübergreifend sämtliche gegen einen Betroffenen bereits ergriffene und geplante repressive und präventive (einschließlich nachrichtendienstliche) heimliche Überwachungsmaßnahmen nebst daraus gewonnenen Erkenntnissen mitgeteilt werden, könnte dies ein erhebliches grundrechtliches Gefährdungspotential begründen. Denn würde zu diesem Zweck etwa eine bundesweite Zentraldatei eingerichtet, in der diese Informationen personenbezogen gebündelt dargestellt und umfassend abgefragt werden könnten, ginge das damit verbundene Gefährdungspotential für die Betroffenen deutlich über das etwa des staatsanwaltschaftlichen Verfahrensregisters (§§ 492 ff. StPO; vgl. hierzu BVerfGE 112, 304 <320>) hinaus. Damit aber haben sich die Beschwerdeführenden nicht auseinandergesetzt. 145

(f) Auch die Rüge einer zeitlich nicht begrenzten Gesamtanordnungsdauer ist unzulässig. Es wird nicht aufgezeigt, dass eine absolute Höchstdauer heimlicher Überwachungsmaßnahmen von Verfassungs wegen geboten sein könnte. Insoweit fehlt eine Auseinandersetzung mit der Rechtsprechung des Bundesverfassungsgerichts (vgl. BVerfGE 109, 279 <361 f.>; 141, 220 <245 Rn. 22, 306 Rn. 216>) und insbesondere mit den in § 100e Abs. 2 Sätze 4 bis 6, Abs. 4 Satz 2 Nr. 2, Abs. 5 StPO geregelten Sicherungen der Verhältnismäßigkeit der Maßnahme. So ist nach § 100b Abs. 1 in Verbindung mit § 100e Abs. 2 Sätze 4 und 5 StPO die Anordnung einer Online-Durchsuchung nicht nur auf höchstens einen Monat zu befristen, sondern auch eine Verlängerung nur unter Berücksichtigung der bislang gewonnenen Ermittlungsergebnisse um jeweils nicht mehr als einen Monat zulässig. Bei einer Verlängerung bestehen daher sowohl für die beantragende Staatsanwaltschaft als auch für das anordnende Gericht Prüfungs- und Begründungspflichten im Hinblick auf die bisherigen Ergebnisse der Maßnahme und die weitere Erfolgsprognose (vgl. BVerfGE 109, 279 <361>). Darüber hinaus muss das anordnende Gericht bei der Entscheidung über eine Verlängerung berücksichtigen, seit wann die Überwachungsmaßnahme bereits vollzogen wird. Insofern gebietet der Grundsatz der Verhältnismäßigkeit im Einzelfall eine 146

richterliche Kontrolle, die der mit zunehmender Dauer ansteigenden Eingriffsintensität der Maßnahme gerecht wird (vgl. BVerfGE 109, 279 <362>). Die Maßgeblichkeit des Einzelfalls kommt auch in § 100e Abs. 5 Satz 1 StPO zum Ausdruck, wonach Überwachungsmaßnahmen unverzüglich und nicht erst zum Ablauf der angeordneten Dauer zu beenden sind, sobald die Voraussetzungen ihrer Anordnung nicht mehr vorliegen.

(g) Ein von den Beschwerdeführenden gerügtes Verschwimmen der Grenzen zwischen Prävention und Repression (dazu Rn. 51) lässt keine Unangemessenheit von § 100b Abs. 1 StPO nebst den flankierenden Vorschriften erkennen. 147

Soweit die Beschwerdeführenden rügen, die Polizei als Gefahrenabwehr- und Strafverfolgungsbehörde könne eine Maßnahme wahlweise auf das Gefahrenabwehrrecht oder die Strafprozessordnung stützen und daher spezifische Grundrechtssicherungen umgehen, indem sie jeweils das Regime mit den geringeren Eingriffsvoraussetzungen wähle, haben sie nicht dargelegt, inwiefern damit eine Verfassungswidrigkeit der hier konkret angegriffenen Befugnis nach § 100b Abs. 1 StPO einhergehen könnte. Auch soweit sie Straftaten in den Blick nehmen, die im Vorfeld konkreter Rechtsgutsverletzungen ansetzen, wie dies bei Vorfeldstraftaten (etwa § 89a StGB) oder bei Organisationsdelikten (etwa § 129a Absätze 1 und 2, § 129b Abs. 1 StGB) der Fall ist, und eine insoweit nicht hinreichende Eingriffsschwelle rügen, kann dies keine mögliche Grundrechtsverletzung aufzeigen. Zwar kann im Gefahrenabwehrrecht dann, wenn der Gesetzgeber an Straftatbestände anknüpft, die Vorbereitungshandlungen oder bloße Rechtsgutsgefährdungen zum Gegenstand haben, der Eingriffsanlass zu weit im Vorfeld einer in ihren Konturen noch nicht absehbaren konkreten Gefahr für Schutzgüter der Norm liegen (näher dazu BVerfGE 165, 1 <51 f. Rn. 92> m.w.N.). Die Beschwerdeführenden haben aber nicht substantiiert dargelegt, dass auch im repressiven Bereich bei Anknüpfung an die vorgenannten Straftaten der Eingriffsanlass abgeschwächt zu werden droht. Insbesondere berücksichtigen sie nicht, dass jede strafprozessuale Ermittlungsmaßnahme einen qualifizierten Anfangsverdacht für eine begangene Straftat voraussetzt und die hier gerügten, in § 100b Abs. 2 Nr. 1 Buchstaben a und b StPO in der angegriffenen Fassung genannten Straftatbestände bereits verwirklichtes kriminelles Unrecht nachzeichnen. 148

cc) Hinreichend dargelegt wird dagegen, dass § 100b Abs. 1 StPO nicht den besonderen Anforderungen an den Schutz des Kernbereichs privater Lebensgestaltung genügen könnte, soweit für Überwachungen in Echtzeit kein Abbruchgebot – wie etwa in § 100d Abs. 4 Satz 2 StPO – vorgesehen ist. Im Übrigen aber erfüllt der Vortrag zum Kernbereichsschutz (1) ebenso wenig wie der zum Schutz von Berufsgeheimnisträgern (2) die Darlegungsanforderungen. 149

(1) Es fehlt bereits eine Auseinandersetzung mit den verfassungsgerichtlich ausformulierten Maßstäben zum Kernbereichsschutz bei heimlichen Überwachungsmaßnahmen 150

(vgl. Rn. 254 ff.). Soweit die Beschwerdeführenden konkret den in § 100d Abs. 1 StPO geregelten Erhebungsschutz als unzureichend rügen, wonach eine Überwachung unterbleiben muss, wenn angenommen werden kann, dass „allein" Erkenntnisse aus dem Kernbereich erlangt werden, haben sie nicht aufgezeigt, dass für eine Online-Durchsuchung eine Negativprognose – so wie für eine Wohnraumüberwachung (vgl. dazu BVerfGE 162, 1 <128 Rn. 280 f., 137 f. Rn. 305>) – geboten sein könnte. Es fehlt auch hier eine Auseinandersetzung damit, dass die verfassungsrechtlichen Anforderungen an den Kernbereichsschutz im Hinblick auf verschiedene Überwachungsmaßnahmen unterschiedlich ausfallen können und abhängig von dem spezifischen Charakter einer bestimmten Maßnahme der Schutz auch zu einem großen Teil von der Erhebungsebene auf die nachgelagerte Aus- und Verwertungsebene verschoben sein kann (vgl. Rn. 126, vgl. auch Rn. 257, 261), wie dies insbesondere bei einer Online-Durchsuchung der Fall sein kann (vgl. BVerfGE 141, 220 <307 f. Rn. 222>; 162, 1 <141 Rn. 314>). Der unter den Vorbehalt des Möglichen gestellte technische Kernbereichsschutz in § 100d Abs. 3 Satz 1 StPO wird ebenfalls nicht substantiiert gerügt. Insoweit wird nicht berücksichtigt, dass bei einer Online-Durchsuchung bereits von Verfassungs wegen gesetzlich vorzusehen ist, dass die Erhebung kernbereichsrelevanter Informationen, soweit informationstechnisch und ermittlungstechnisch möglich, unterbleibt und verfügbare Sicherungen einzusetzen sind (vgl. BVerfGE 141, 220 <307 Rn. 219>). Eine verfassungsrechtliche Herleitung der geforderten, hierüber hinausgehenden Dokumentationspflicht und unabhängigen Überprüfung dieser technischen Sicherungen fehlt.

Die auf die Auswertungs- und Verwertungsebene abzielende Rüge, der Gesetzgeber habe keine Vorgaben für den Fall vorgesehen, dass wider Erwarten in nicht nur ganz unerheblichem Umfang höchstpersönliche, dem Kernbereich unterfallende Informationen erfasst würden, übersieht das in § 100d Abs. 2, Abs. 3 Satz 2 StPO geregelte Verwertungsverbot und die dort ebenfalls geregelten Löschungs- sowie Dokumentationsvorgaben. 151

(2) Soweit die Beschwerdeführenden rügen, dass § 100d Abs. 5 Satz 2 StPO für die sogenannten Berufshelfer der Berufsgeheimnisträger keinen absoluten Schutz vorsieht, haben sie sich abermals nicht mit einschlägiger verfassungsgerichtlicher Rechtsprechung auseinandergesetzt. Danach hat der Gesetzgeber einen erheblichen Einschätzungsspielraum bei beweisbezogenen Regelungen; absolute Beweiserhebungs-, Beweisverwertungs- und Beweisverwendungsverbote dürfen zugunsten einer effektiven Strafverfolgung auf eng begrenzte Ausnahmen beschränkt sein (vgl. BVerfGE 129, 208 <259 ff.>; 141, 220 <318 f. Rn. 256, 258>). Inwiefern daher der für Berufshelfer nur relative Verwertungsschutz nach § 100d Abs. 5 Satz 2 StPO und der nach § 160a Abs. 3 StPO in Betracht kommende Erhebungsschutz verfassungsrechtlich – unbeschadet weiterer Schutzvorgaben – unzureichend sein könnten, wird nicht dargetan. 152

3. Die Rüge einer möglichen Verletzung des Art. 13 Abs. 1 GG durch § 100b StPO genügt nicht den Darlegungsanforderungen. Schon ein Eingriff in das Wohnungsgrundrecht wird nicht aufgezeigt. 153

a) Soweit die Beschwerdeführenden einen Eingriff in die durch Art. 13 Abs. 1 GG geschützte Unverletzlichkeit der Wohnung damit begründen, dass Ermittlungsbehörden Kameras und Mikrofone über das infiltrierte IT-System eigenständig ansteuern und so aktiv Daten generieren könnten, haben sie nicht substantiiert dargelegt, dass § 100b Abs. 1 StPO eine solche Nutzungsmöglichkeit überhaupt rechtlich eröffnet. Dies wäre aber erforderlich gewesen. Denn schon nach seinem Wortlaut erlaubt § 100b Abs. 1 StPO lediglich die Erhebung von Daten aus dem System selbst („dürfen Daten daraus erhoben werden"), was dagegen spricht, dass das IT-System auch zur Datenerzeugung genutzt werden darf. Entsprechend wird auch im Schrifttum die Ansicht vertreten, dass § 100b Abs. 1 StPO nicht zur eigenständigen Anfertigung von Videos oder Audioaufnahmen von Sachverhalten außerhalb des IT-Systems ermächtige (vgl. Singelnstein/Derin, NJW 2017, S. 2646 <2647>; Rückert, in: Münchener Kommentar zur StPO, 2. Aufl. 2023, § 100b Rn. 45 m.w.N.; Köhler, in: Schmitt/Köhler, StPO, 68. Aufl. 2025, § 100b Rn. 2). Hierauf dürfte auch hinweisen, dass der Gesetzgeber die Maßnahme als „Online-Durchsuchung" legaldefiniert hat (vgl. § 100b Abs. 1 StPO) und eine Durchsuchung stets auf Vorhandenes und somit auf das begrenzt ist, was die Ermittlungsbehörden als von der Zielperson geschaffen vorfinden. Letztlich haben die Beschwerdeführenden überdies nicht erörtert, dass ein Eingriff in Art. 13 Abs. 1 GG ein Eigengewicht aufweist, das schon wegen der spezifischen verfassungsrechtlichen Rechtfertigungsanforderungen eine spezielle Ermächtigungsgrundlage erfordern dürfte (vgl. dazu BVerfGE 165, 363 <389 ff. Rn. 54, 66 ff., 77> – Automatisierte Datenanalyse). 154

b) Soweit die Beschwerdeführenden darüber hinaus rügen, schon das passive Abgreifen von Audio- und Videosignalen eines IT-Systems, das sich in einer Wohnung befindet, begründe einen Eingriff in Art. 13 Abs. 1 GG, haben sie sich insbesondere nicht mit der verfassungsgerichtlichen Rechtsprechung auseinandergesetzt (vgl. etwa BVerfGE 120, 274 <310 f.>). 155

4. Schließlich ist auch die Rüge betreffend Art. 19 Abs. 4 GG unzulässig erhoben. Soweit die Beschwerdeführenden beanstanden, insbesondere § 100a Absätze 5 und 6 StPO seien mit der Garantie effektiven Rechtsschutzes nicht vereinbar und insoweit lediglich auf die verfassungsrechtlichen Transparenzanforderungen (vgl. BVerfGE 141, 220 <282 ff. Rn. 134 ff.>) verweisen, genügt dies nicht für eine Auseinandersetzung mit den einschlägigen verfassungsrechtlichen Maßstäben. Ungeachtet dessen lässt die Behauptung, eine auf den §§ 100a, 100b StPO beruhende Beweiserhebung sei nicht nachprüfbar, eine Berücksichtigung insbesondere des in § 101 Abs. 7 Sätze 2 bis 4 StPO geregelten nachträglichen Rechtsschutzes vermissen. Warum dieser mit Blick auf Art. 19 Abs. 4 Satz 1 GG verfassungsrechtlich unzureichend sein könnte, ist nicht dargetan. Auch haben die 156

Beschwerdeführenden nicht gewürdigt, dass eine inzidente gerichtliche Kontrolle der Rechtmäßigkeit von Ermittlungsmaßnahmen in einem Haupt- und Rechtsmittelverfahren erfolgen kann.

5. Die Beschwerdeführenden zu 1), 2), 4) und 5) haben ihre Betroffenheit in unterschiedlichem Umfang dargelegt. 157

Für die Darlegung der unmittelbaren sowie der eigenen und gegenwärtigen Betroffenheit gelten bei einer Verfassungsbeschwerde gegen eine gesetzliche Ermächtigung zu heimlichen Überwachungsmaßnahmen nach der Rechtsprechung des Bundesverfassungsgerichts besondere Anforderungen (näher BVerfGE 165, 1 <31 f. Rn. 41 ff.>). 158

a) Danach sind die Beschwerdeführenden von §§ 100a, 100b StPO im verfassungsprozessrechtlichen Sinne unmittelbar betroffen. Die Regelungen ermöglichen heimliche Ermittlungsmaßnahmen. Die in § 101 Abs. 4 Satz 1 Nummern 3 und 4 StPO vorgesehenen Benachrichtigungspflichten wirken dieser Heimlichkeit nur teilweise entgegen. Denn § 101 Abs. 4 Satz 1 Nr. 4, Sätze 3 bis 5, Abs. 5 und Abs. 6 Satz 3 StPO schränken die Benachrichtigungspflichten ein oder lassen sie vollständig entfallen. Auch der Auskunftsanspruch nach § 491 Abs. 2 StPO in Verbindung mit § 57 Abs. 1 Satz 1 des Bundesdatenschutzgesetzes (BDSG) unterliegt nach § 57 Abs. 4 in Verbindung mit § 56 Abs. 2 BDSG weitgehenden Einschränkungen. Würde eine Auskunft erteilt, hätte sie wegen dieser Einschränkungen nur begrenzte Aussagekraft und könnte nicht zuverlässig belegen, ob Beschwerdeführende von einer Maßnahme nach §§ 100a, 100b StPO betroffen sind oder nicht (vgl. dazu BVerfGE 162, 1 <56 f. Rn. 107>). 159

b) Ihre mögliche eigene und gegenwärtige Betroffenheit mussten die Beschwerdeführenden hier näher begründen, weil die Streubreite der angegriffenen Maßnahmen nach §§ 100a, 100b StPO rechtlich und tatsächlich eingeschränkt ist (aa). Im Ergebnis ist ihnen dies in unterschiedlichem Umfang gelungen (bb). 160

aa) Maßnahmen nach §§ 100a, 100b StPO haben eine eingeschränkte Streubreite. Im Hinblick auf eine mögliche Überwachung als Zielperson ist sie durch spezifische Eingriffsschwellen und ein erhöhtes Gewicht der Katalogstraftaten erheblich beschränkt. Zusätzlich wird die Einhaltung der Eingriffsvoraussetzungen institutionell durch einen Richtervorbehalt abgesichert, der bei einer Online-Durchsuchung sogar eine Anordnung durch eine aus drei Berufsrichtern bestehende Kammer am Landgericht erfordert (§ 100e Abs. 1 Satz 1, Abs. 2 Satz 1 StPO). Eine Betroffenheit als Dritter kann hingegen an geringere Darlegungslasten geknüpft sein. Insoweit ist die Streubreite der hier angegriffenen Befugnisse nicht in gleichem Maße beschränkt, da auch solche Personen von einer Überwachung betroffen sein können, die mit potentiellen Zielpersonen etwa lediglich elektronisch kommunizieren, ohne selbst in einer unmittelbaren Beziehung zu einer aufzuklärenden Straftat zu 161

stehen (vgl. BVerfGE 113, 348 <383>; BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 74 m.w.N.).

bb) Danach haben die Beschwerdeführenden zu 1) und 5) ihre Betroffenheit als Zielperson dargelegt. Ihr Vortrag belegt, dass sie deutlich aus dem Kreis der Allgemeinheit herausgehoben sind, für die angesichts der eingeschränkten Streubreite von Maßnahmen nach §§ 100a, 100b StPO nur ein theoretisches, eine mögliche Selbstbetroffenheit nicht tragendes Risiko besteht, mit einiger Wahrscheinlichkeit Zielperson einer Quellen-Telekommunikationsüberwachung oder Online-Durchsuchung zu werden. Ihr Vortrag zu ihrem Umfeld begründet auch eine mögliche Betroffenheit als unvermeidbar mitbetroffene Dritte. 162

Die Beschwerdeführer zu 2) und 4) haben dagegen ihre Betroffenheit als Zielperson nicht hinreichend dargetan. Soweit sie Überwachungsmaßnahmen im Zusammenhang mit ihrer Tätigkeit als Rechtsanwalt und Strafverteidiger befürchten, haben sie sich nur unvollständig mit den einfachrechtlichen Schutzvorschriften zugunsten von Berufsgeheimnisträgern auseinandergesetzt. Warum sie unbeschadet der § 100d Abs. 5 Satz 1, § 148, § 160a StPO mit einiger Wahrscheinlichkeit als Zielperson überwacht werden könnten, wird nicht näher ausgeführt. Die vom Beschwerdeführer zu 4) geäußerte Befürchtung, wegen eines Verdachts der Geldwäsche Zielperson werden zu können, genügt aufgrund ihrer Pauschalität auch unter Berücksichtigung des Umstands, dass keine Pflicht zur Selbstbezichtigung besteht (vgl. BVerfGE 162, 1 <53 Rn. 97>), für eine substantiierte Darlegung nicht. Insbesondere geht das Vorbringen insoweit nicht über die bloße Nennung des entsprechenden Straftatbestands hinaus. Auch fehlt substantiierter Vortrag zu § 100a Abs. 3 und § 100b Abs. 3 StPO. Anders liegen die Dinge im Hinblick auf mögliche Maßnahmen gegen einen ihrer Mandanten als potentielle Zielperson, denn diesen werden nach Angaben der Beschwerdeführer Katalogtaten im Sinne von § 100a Abs. 2 und § 100b Abs. 2 StPO vorgeworfen beziehungsweise könnten ihnen vorgeworfen werden. Als deren Kommunikationspartner könnten daher beide Beschwerdeführer mit einiger Wahrscheinlichkeit in eine heimliche Überwachung einbezogen werden und damit als Dritte betroffen sein (vgl. auch BVerfGE 165, 1 <38 Rn. 59>). 163

IV.

Soweit die Beschwerdeführenden beschwerdebefugt sind, sind die sich aus der Subsidiarität der Verfassungsbeschwerde ergebenden Anforderungen gewahrt. Ausgehend von den einschlägigen verfassungsrechtlichen Maßstäben (dazu BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 78 f. m.w.N.) bedarf es keiner fachgerichtlichen Vorbefassung. Unabhängig von der Statthaftigkeit eines fachgerichtlichen Rechtsbehelfs stellen sich hier spezifisch verfassungsrechtliche Fragen, ohne dass von einer vorherigen fachgerichtlichen Klärung verbesserte Entscheidungsgrundlagen zu erwarten wären. 164

V.

Im Ergebnis ist die Verfassungsbeschwerde daher zulässig, soweit sie sich gegen die § 100a Abs. 1 Sätze 2 und 3 in Verbindung mit § 100a Abs. 1 Satz 1 Nr. 1, Abs. 2 StPO wendet und ein nicht hinreichendes Straftatengewicht rügt. Im Übrigen ist sie – auch mit Blick auf die flankierenden Regelungen in § 100a Absätze 3 bis 6 StPO – unzulässig, wobei es zu § 100a Abs. 4 StPO schon an einem Vortrag fehlt. 165

Die gegen § 100b Abs. 1 StPO gerichtete Verfassungsbeschwerde ist zulässig, soweit sie einen Verstoß gegen das Zitiergebot (Art. 19 Abs. 1 Satz 2 GG) sowie einen unzureichenden Kernbereichsschutz wegen eines fehlenden Abbruchgebots rügt. Im Übrigen ist sie, soweit sie sich gegen § 100b Absätze 2 bis 4 StPO wendet, unzulässig. 166

Die gegen die flankierenden Regelungen in § 100d Absätze 1 bis 3 und 5 StPO gerichteten Rügen sind ebenfalls unzulässig. Soweit sie unmittelbar angegriffen werden, ergibt sich dies zudem daraus, dass die Regelungen selbst lediglich Beschränkungen zugunsten des Kernbereichsschutzes enthalten und allein die Befugnisnormen nach § 100a Abs. 1 Sätze 2 und 3 und § 100b Abs. 1 StPO zu belastenden, weitergehenden Eingriffen ermächtigen (vgl. dazu BVerfGE 169, 130 <161 Rn. 58, 165 Rn. 68>). 167

VI.

Das Bundesverfassungsgericht ist für die Prüfung der Vereinbarkeit der angegriffenen Normen mit den Grundrechten des Grundgesetzes zuständig, obwohl diese Normen auch Bezüge zu datenschutzrechtlichen Bestimmungen in Rechtsakten der Europäischen Union wie der JI-Richtlinie (Richtlinie <EU> 2016/680) haben. Es handelt sich jedenfalls nicht um die Umsetzung zwingenden Unionsrechts, denn Rechtsakte der Europäischen Union enthalten keine Bestimmungen, die die hier angegriffenen repressiven Überwachungsbefugnisse erforderten oder gar abschließend regelten; die Befugnisse sind nicht vollständig unionsrechtlich determiniert. Unberührt bleibt hiervon die Frage, ob sich weitere rechtliche Anforderungen unmittelbar aus dem Sekundärrecht der Europäischen Union ergeben und ob die angegriffenen Regelungen mit diesen vereinbar sind (vgl. BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 83 m.w.N.). 168

C.

Die Verfassungsbeschwerde ist, soweit sie zulässig ist, überwiegend begründet. 169

Die angegriffenen Befugnisse ermächtigen die Ermittlungsbehörden zum Zweck der Strafverfolgung zur heimlichen Erhebung personenbezogener Daten in der Weise, dass mit technischen Mitteln in ein von Betroffenen genutztes IT-System eingegriffen wird. Sie begründen damit Eingriffe in das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG in seiner Ausprägung als Grundrecht auf Gewährleistung der 170

Vertraulichkeit und Integrität informationstechnischer Systeme (IT-System-Grundrecht) und in seiner Ausprägung als Recht auf informationelle Selbstbestimmung sowie in das durch Art. 10 Abs. 1 GG geschützte Fernmeldegeheimnis; diese Eingriffe genügen nur zu einem Teil den Anforderungen an ihre verfassungsrechtliche Rechtfertigung.

I.

Die durch die Quellen-Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 2 StPO bewirkten Grundrechtseingriffe sowohl in das IT-System-Grundrecht als auch in Art. 10 Abs. 1 GG (1) sind nicht gerechtfertigt, soweit § 100a Abs. 1 Satz 2 in Verbindung mit § 100a Abs. 1 Satz 1 Nr. 1, Abs. 2 StPO an nicht hinreichend gewichtige Katalogstraftaten als Eingriffsvoraussetzung anknüpft (2). Soweit nur ein Eingriff in Art. 10 Abs. 1 GG vorliegt, begegnet § 100a Abs. 1 Satz 2 StPO keinen verfassungsrechtlichen Bedenken (3). 171

1. Die Befugnis zur Quellen-Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 2 StPO begründet Eingriffe in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-System-Grundrecht) sowie in das durch Art. 10 Abs. 1 GG geschützte Fernmeldegeheimnis. 172

Das IT-System-Grundrecht schützt als Ausprägung des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) vor Zugriffen auf IT-Systeme in ihrer ganzen Breite. Sein Schutzgegenstand sind eigengenutzte IT-Systeme, die aufgrund ihrer technischen Funktionalität allein oder durch ihre technische Vernetzung Daten einer betroffenen Person in einem Umfang und in einer Vielfalt vorhalten 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. Grundrechtlich gewährleistet ist die Vertraulichkeit und Integrität des geschützten IT-Systems (näher BVerfGE 120, 274 <313 ff.>; BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 97 ff. m.w.N. – Trojaner I). Das Fernmeldegeheimnis (Art. 10 Abs. 1 GG) schützt demgegenüber die unkörperliche Übermittlung von Informationen mit Hilfe des Telekommunikationsverkehrs, und zwar vor den spezifischen Gefahren, die mit einer räumlich distanzierten Kommunikation einhergehen. Dies umfasst auch den kommunikationsbezogenen Zugriff auf ein Endgerät (näher BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 87 m.w.N.). 173

Die Befugnis zur Quellen-Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 2 StPO ermächtigt zur Überwachung und Aufzeichnung laufender Telekommunikation auch in der Weise, dass mit technischen Mitteln in von Betroffenen genutzte IT-Systeme eingegriffen wird. Begründet werden dadurch Eingriffe sowohl in das IT-System-Grundrecht als auch in das durch Art. 10 Abs. 1 GG geschützte Fernmeldegeheimnis. § 100a Abs. 1 Satz 2 StPO ist an beiden Grundrechten zu messen (vgl. zu § 20c Abs. 1 i.V.m. Abs. 2 PolG NRW 174

BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 85 ff., 105 ff. m.w.N.).

Allein ein Eingriff in Art. 10 Abs. 1 GG liegt dagegen vor, wenn eine Person zwar von einer Überwachung nach § 100a Abs. 1 Satz 2 StPO betroffen ist, dieser Überwachung aber etwa kein Zugriff auf ein von ihr eigengenutztes und hinreichend qualifiziertes IT-System zugrunde liegt (vgl. Rn. 173). Insoweit gewährleistet das IT-System-Grundrecht keinen Schutz (vgl. BVerfGE 120, 274 <315>; Rückert, Digitale Daten als Beweismittel im Strafverfahren, 2023, S. 180; vgl. auch Hoffmann-Riem, JZ 2008, S. 1009 <1012, 1019>). Es schützt daher keine Dritten, die von einer Quellen-Telekommunikationsüberwachung etwa allein deshalb betroffen sind, weil sie mit einer Person, deren IT-System überwacht wird, in Kontakt stehen. Auch etwa der Zugriff auf das von einem Nachrichtenmittler nach § 100a Abs. 3 StPO eigengenutzte IT-System begründet nur diesem gegenüber einen Eingriff in das IT-System-Grundrecht, nicht aber auch gegenüber dem Beschuldigten. Der Schutz des in solchen Fällen allein beeinträchtigten Fernmeldegeheimnisses kann allerdings nicht weiter reichen als derjenige aus einer gleichzeitigen Betroffenheit des IT-System-Grundrechts (vgl. dazu BVerfGE 109, 279 <326>; näher Rn. 218). 175

2. Die durch den Zugriff auf eigengenutzte IT-Systeme begründeten Eingriffe sowohl in das IT-System-Grundrecht als auch in Art. 10 Abs. 1 GG sind nicht gerechtfertigt, soweit eine Quellen-Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 2 in Verbindung mit § 100a Abs. 1 Satz 1 Nr. 1, Abs. 2 StPO auch die Aufklärung solcher Straftaten erlaubt, die eine Höchstfreiheitsstrafe von drei Jahren oder weniger vorsehen und damit nur dem einfachen Kriminalitätsbereich zuzuordnen sind. 176

a) Die Verfassungsmäßigkeit von heimlichen Überwachungsmaßnahmen richtet sich nach den jeweils betroffenen Grundrechten und dabei vor allem nach den Anforderungen der Verhältnismäßigkeit (vgl. BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 123 ff. m.w.N.). Sowohl für Eingriffe in das IT-System-Grundrecht, das der Schrankentrias des Art. 2 Abs. 1 GG untersteht und gleichermaßen zu präventiven wie zu repressiven Zwecken beschränkbar ist (vgl. BVerfGE 120, 274 <315>), als auch für solche in Art. 10 Abs. 1 GG (vgl. BVerfGE 100, 313 <373 ff.>; 113, 348 <385 ff.>) gelten hierbei keine Besonderheiten. Überwachungsbefugnisse müssen einen legitimen Zweck verfolgen und zur Erreichung dieses Zwecks geeignet, erforderlich und verhältnismäßig im engeren Sinne sein (vgl. BVerfGE 141, 220 <265 Rn. 93> m.w.N.). Maßgebliche Begrenzungen ergeben sich insbesondere aus den Anforderungen der Verhältnismäßigkeit im engeren Sinne. Wie streng diese Anforderungen im Einzelnen sind, bestimmt sich nach dem jeweiligen Eingriffsgewicht und dem Gewicht des öffentlichen Interesses (vgl. BVerfGE 141, 220 <269 Rn. 105>). 177

Verfassungsrechtliche Anforderungen richten sich dabei an die Eingriffsschwelle und – bei repressiven Maßnahmen – an das Gewicht der Straftaten, die den Anlass der Überwachung bilden. Als Eingriffsschwelle bedarf es einer gesicherten Tatsachenbasis sowohl für die Annahme eines Tatverdachts als auch für die Erstreckung der Maßnahme auf Dritte (vgl. BVerfGE 129, 208 <242>). Daneben kommt es für Maßnahmen, die der Strafverfolgung dienen und damit repressiven Charakter haben, auf das Gewicht der Straftaten an, die der Gesetzgeber in – jeweils näher bestimmte – erhebliche, schwere und besonders schwere Straftaten eingeteilt hat (vgl. BVerfGE 141, 220 <270 Rn. 107>). Das erforderliche Gewicht der verfolgten Straftat bestimmt sich maßgeblich nach der Eingriffsintensität (vgl. BVerfGE 141, 220 <269 ff. Rn. 104 ff.>; 169, 130 <172 Rn. 87 f.>; BVerfG, Beschluss des Ersten Senats vom 14. November 2024 - 1 BvL 3/22 -, Rn. 74; näher Rn. 201 ff.). Die jeweils geregelten Eingriffsvoraussetzungen stehen dabei allerdings nicht unverbunden nebeneinander. Es bedarf vielmehr einer Gesamtschau der Kombination von Gewicht der Straftat und Stärke des Tatverdachts unter Berücksichtigung insbesondere der Intensität des Grundrechtseingriffs (vgl. BVerfGE 109, 279 <351>; vgl. auch BVerfGE 165, 1 <86 Rn. 161, 90 f. Rn. 173>; BVerfG, Beschluss des Ersten Senats vom 14. November 2024 - 1 BvL 3/22 -, Rn. 75 ff.). 178

b) Danach genügt die angegriffene Regelung in § 100a Abs. 1 Satz 2 StPO im Hinblick auf das erforderliche Straftatengewicht teilweise nicht den Anforderungen der Verhältnismäßigkeit im engeren Sinne. 179

aa) § 100a Abs. 1 Satz 2 StPO dient allerdings einem legitimen Zweck (1) und ist zur Erreichung dieses Zwecks auch geeignet und erforderlich (2). 180

(1) Die hier angegriffene Befugnis zur Quellen-Telekommunikationsüberwachung dient dem Zweck, den Ermittlungsbehörden ein Aufklärungsmittel an die Hand zu geben, mit dem jedenfalls schwere Straftaten effektiver verfolgt werden können. Sie soll die Behörden in die Lage versetzen, Telekommunikation auch dann zu überwachen, wenn sie – was zunehmend der Fall ist (vgl. dazu auch Rn. 4, 8) – verschlüsselt erfolgt und deshalb mittels einer klassischen Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 1 StPO keine lesbaren Inhaltsdaten mehr gewonnen werden können (dazu Rn. 8). Die Bereitstellung von insoweit wirksamen Überwachungsmaßnahmen ist ein legitimer Zweck (vgl. BVerfGE 129, 208 <241 f.>; vgl. auch BVerfGE 133, 277 <321 Rn. 106; 333 f. Rn. 133>; 169, 332 <374 Rn. 101>). Sie steigert die Effizienz der Strafverfolgung (vgl. BVerfGE 115, 166 <192>), der nach dem Grundgesetz eine hohe Bedeutung zukommt (vgl. BVerfGE 100, 313 <388>; 113, 29 <54>), die auch auf der verfassungsrechtlichen Pflicht des Staates gründet, eine funktionstüchtige Strafrechtspflege zu gewährleisten (vgl. BVerfGE 122, 248 <272 f.>; 130, 1 <26>). 181

(2) § 100a Abs. 1 Satz 2 StPO ist zur Erreichung dieses Ziels im verfassungsrechtlichen Sinn auch geeignet und erforderlich. Die Befugnisnorm eröffnet Polizeibehörden ein Mittel zur Aufklärung, das dazu beitragen kann, Straftaten effektiver zu verfolgen. Ein milderes 182

Mittel, das gleichermaßen effektiv eine ebenso weitgehende Aufklärung ermöglichte, ist abstrakt nicht ersichtlich. Dies lässt allerdings unberührt, dass auch die Anordnung einer Quellen-Telekommunikationsüberwachung im konkreten Einzelfall geeignet und erforderlich sein muss (vgl. § 100a Abs. 1 Satz 1 Nr. 3 StPO; vgl. auch BVerfGE 141, 220 <266 f. Rn. 97>).

bb) § 100a Abs. 1 Satz 2 StPO genügt allerdings nicht vollständig den besonderen Anforderungen an heimliche Überwachungsmaßnahmen, die sich aus der Verhältnismäßigkeit im engeren Sinne ergeben. Die Befugnis ermöglicht sehr schwerwiegende Grundrechtseingriffe (1). Den deshalb hohen Anforderungen an ihre Rechtfertigung im Hinblick auf das erforderliche Gewicht aufzuklärender Straftaten (2) genügt jedenfalls ein Teil der in § 100a Abs. 2 StPO genannten Straftaten nicht (3). 183

(1) § 100a Abs. 1 Satz 2 StPO ermöglicht sehr schwerwiegende Grundrechtseingriffe. 184

(a) Das Eingriffsgewicht einer Befugnis zur Datenerhebung wird vor allem durch Art, Umfang und denkbare Verwendung der Daten sowie die Gefahr ihres Missbrauchs bestimmt (vgl. BVerfGE 65, 1 <45 f.>; 109, 279 <353 f.> m.w.N.). Maßgebliche Kriterien sind insbesondere die Zahl der Betroffenen und die Intensität der Beeinträchtigungen (vgl. BVerfGE 100, 313 <376>), die sich vor allem nach der Aussagekraft und den Verwendungsmöglichkeiten der Daten bestimmt, also danach, welche Nachteile Grundrechtsberechtigten aus der weiteren Verwendung der erhobenen Daten drohen oder von ihnen nicht ohne Grund befürchtet werden müssen (vgl. BVerfGE 162, 1 <76 Rn. 157> m.w.N.). Auch die Heimlichkeit einer staatlichen Eingriffsmaßnahme erhöht das Eingriffsgewicht in der Regel erheblich (vgl. BVerfGE 155, 119 <178 f. Rn. 129> m.w.N. – Bestandsdatenauskunft II). Das Gewicht eines Eingriffs wird ebenso dadurch geprägt, wie lange die Überwachungsmaßnahme andauert, weil mit zunehmender Dauer der Eingriff in das allgemeine Persönlichkeitsrecht immer intensiver wird (vgl. BVerfGE 141, 220 <293 Rn. 171>; 162, 1 <92 Rn. 191>). Zudem hängt das Eingriffsgewicht einer Maßnahme davon ab, wie weitgehend die Persönlichkeit erfasst werden kann, ob besonders private Informationen erlangt werden können oder ob berechtigte Vertraulichkeitserwartungen überwunden werden (vgl. BVerfGE 141, 220 <269 Rn. 105>; 155, 119 <229 Rn. 253>; BVerfG, Beschluss des Ersten Senats vom 14. November 2024 - 1 BvL 3/22 -, Rn. 93; stRspr). Nicht zuletzt beeinflusst aber auch die Art und Weise der Datenerhebung die Eingriffsintensität (vgl. dazu BVerfGE 165, 363 <404 Rn. 90>). Eingriffsverstärkend wirkt insoweit, wenn die Datenerhebung als solche etwa mit besonderen Belastungen oder Gefährdungen für Betroffene oder auch Dritte einhergehen kann (vgl. BVerfGE 120, 274 <325>; Rückert, Digitale Daten als Beweismittel im Strafverfahren, 2023, S. 302). 185

(b) Danach wiegt der von § 100a Abs. 1 Satz 2 StPO ausgehende Eingriff in beide Grundrechte sehr schwer. 186

(aa) Art und Umfang der erhobenen Daten wirken schon für sich genommen eingriffsverstärkend, denn die Quellen-Telekommunikationsüberwachung ermöglicht Ermittlungsbehörden den Zugang zu einem Datenbestand, der herkömmliche Informationsquellen an Umfang und Vielfältigkeit bei weitem übertreffen kann. 187

Die nach § 100a Abs. 1 Satz 2, Abs. 5 Satz 1 Nr. 1 StPO erlaubte Überwachung und Aufzeichnung der laufenden Telekommunikation umfasst – nach der maßgeblichen materiellen Betrachtung der von dieser Befugnis eröffneten rechtlichen und tatsächlichen Nutzungsmöglichkeiten (vgl. BVerfGE 162, 1 <147 Rn. 326>; 165, 363 <429 Rn. 149>) – die Ausleitung des gesamten Rohdatenstroms. Dieser kann – anders als bei der klassischen Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 1 StPO (vgl. Rn. 8) – trotz einer etwaigen Verschlüsselung vollständig ausgewertet werden; alle Daten des im Rahmen einer Maßnahme nach § 100a Abs. 1 Satz 2 StPO ausgeleiteten Rohdatenstroms sind für die Ermittlungsbehörden lesbar (vgl. Stellungnahme des GBA, oben Rn. 81). Die Befugnis nach § 100a Abs. 1 Satz 2 StPO hat damit insbesondere unter den heutigen Bedingungen der Informationstechnik und ihrer Bedeutung für die Kommunikationsbeziehungen eine außerordentliche Reichweite. So wird mit den erfassten Datenströmen nicht nur eine unübersehbare Zahl von Formen elektronischer Kommunikation transportiert und der Auswertung zugeführt. Angesichts der ubiquitären und vielfältigen Nutzung von IT-Systemen findet inzwischen auch zunehmend jede Art individuellen Handelns und zwischenmenschlicher Kommunikation in elektronischen Signalen ihren Niederschlag und wird so insbesondere der Quellen-Telekommunikationsüberwachung zugänglich. Die Überwachung erfasst damit auch tief in den Alltag hineinreichende, auch höchst private und spontane Kommunikationsvorgänge einschließlich gespeicherter Bilder und Dokumente. Erfasst werden letztlich alle über das Internet transportierten Daten, so etwa das Nutzerverhalten im World Wide Web und die hierbei zum Ausdruck kommenden Interessen, Wünsche und Vorlieben (vgl. auch BVerfGE 154, 152 <243 Rn. 151>). Dabei wird – wie sich insbesondere aus den Stellungnahmen der Äußerungsberechtigten (vgl. Rn. 65, 68) und der im Verfahren gehörten sachkundigen Dritten (vgl. Rn. 75, 80 f., 90, 98) ergibt – auch der gesamte Datenaustausch mit Dienstleistungen überwacht, die über das Internet zur Speicherung von Daten oder zur Nutzung von Softwareleistungen zur Verfügung stehen (Cloud-Services und Software-as-a-Service). Dies kann nicht nur große Datenmengen in unterschiedlichsten Formaten (etwa Sprach-, Text-, Bild- und Videodateien) betreffen. Die Daten können auch detaillierte Informationen über die persönlichen Verhältnisse und die Lebensführung der Betroffenen, die über verschiedene Kommunikationswege geführte private und geschäftliche Korrespondenz oder auch tagebuchartige persönliche Aufzeichnungen umfassen; es können alle – privaten und privatesten – Lebensbereiche betroffen sein (vgl. bereits BVerfGE 120, 274 <323>; vgl. auch BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 113 m.w.N.). Lesbar können zum Beispiel die Zugangsdaten zu Online-Diensten wie Cloud-Services, Online-Banking oder Gesundheitsservices (vgl. BVerfGE 120, 274 <324>) sowie die Daten sogenannter Fitnesstracker sein. Findet im Anordnungs- 188

zeitraum ein Cloud-Backup statt, können in Abhängigkeit der hersteller- beziehungsweise nutzerseitigen Voreinstellungen potentiell alle auf dem IT-System zunächst nur gespeicherten, ruhenden Daten (einschließlich dort gespeicherter früherer Kommunikationsdaten) als Telekommunikation erfasst werden.

IT-Systeme werden nach heutigen Nutzungsgepflogenheiten typischerweise auch bewusst zum Speichern persönlicher Daten von gesteigerter Sensibilität, etwa in Form privater Text-, Bild- oder Tondateien, genutzt (vgl. schon BVerfGE 120, 274 <322 f.>). Sie haben mittlerweile alle Lebensbereiche erfasst und spielen für die Lebensführung der Mehrzahl der Menschen eine unverzichtbare Rolle (vgl. BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 113 m.w.N.; vgl. auch VfGH Österreich, Erkenntnis vom 14. Dezember 2023 - G 352/2021-46 -, Rn. 37, 66 ff.; EuGH, Urteil vom 4. Oktober 2024, Bezirkshauptmannschaft Landeck, C-548/21, EU:C:2024:830, Rn. 93 f.). Insbesondere die Nutzung von Cloud-Services einschließlich Cloud-Speichern gehört für viele Menschen und Unternehmen zunehmend zum Alltag (vgl. Stellungnahmen, oben Rn. 66, 69, 87, 96). So geht etwa der Branchenverband der Telekommunikationsbranche Bitkom auf Grundlage einer Unternehmensbefragung davon aus, dass im Jahr 2024 rund 81 % aller Unternehmen Cloud-Services nutzten und 14 % dies planten oder diskutierten (vgl. Bitkom, Cloud Report 2024, S. 2). Ähnliche Zahlen haben sowohl das Statistische Bundesamt für das Jahr 2023 (vgl. Statistisches Bundesamt, Erhebung über die Nutzung von Informations- und Kommunikationstechnologien in Unternehmen) als auch der KPMG Cloud-Monitor für das Jahr 2024 ermittelt. Im Bereich der Privatnutzung von Cloud-Services liegen zwar keine vergleichbar belastbaren Daten vor. In ihren Stellungnahmen sind sich die Äußerungsberechtigten und sachkundigen Dritten aber darin einig, dass ein großer und zunehmender Teil der Bevölkerung schon aufgrund der Voreinstellungen der ubiquitär verbreiteten Smartphones und der darauf installierten Software Cloud-Services nutzt (vgl. oben Rn. 66, 69, 87, 96). 189

(bb) Ein staatlicher Zugriff auf einen derart umfassenden Datenbestand ist auch vor dem Hintergrund, dass die Analysemöglichkeiten gestiegen und heute sehr weitreichend sind (vgl. insoweit BVerfGE 154, 152 <243 Rn. 151>), mit dem naheliegenden Risiko verbunden, dass die erhobenen Daten in einer Gesamtschau einen umfassenden Einblick in das Privatleben Betroffener und eine weitgehende Erfassung der Persönlichkeit bis hin zu einer Erstellung von Verhaltens- und Kommunikationsprofilen ermöglichen (vgl. insoweit BVerfGE 120, 274 <323>). Wegen der oft höchstpersönlichen Natur dieser Daten, die sich insbesondere auch aus deren Verknüpfung ergibt, ist der Eingriff in die hier betroffenen Grundrechte daher von besonderer Intensität (vgl. zur Online-Durchsuchung BVerfGE 141, 220 <304 Rn. 210>). 190

(cc) Soweit Daten erhoben werden, die Aufschluss über die Kommunikation mit Dritten geben, wird die Intensität der Grundrechtseingriffe weiter erhöht. Solche Datenerhebungen weisen eine beträchtliche, das Gewicht der Eingriffe erhöhende Streubreite auf, da 191

Dritte erfasst werden, ohne dass es darauf ankäme, ob in deren Person die Voraussetzungen für einen derartigen Zugriff vorliegen (vgl. BVerfGE 120, 274 <323>).

(dd) Eingriffsverstärkend wirkt auch, dass eine Quellen-Telekommunikationsüberwachung nicht nur heimlich erfolgt, sondern mit dem Zugriff auf ein IT-System gezielt Sicherungsmechanismen wie insbesondere der Einsatz von Verschlüsselungstechnologie umgangen werden. Die Vereitelung solchen informationellen Selbstschutzes erhöht das Gewicht der Grundrechtseingriffe (vgl. insoweit BVerfGE 120, 274 <324 f.>). Mit dem Zugriff auf das IT-System werden zudem berechtigte Erwartungen in dessen Integrität und Vertraulichkeit beeinträchtigt. Verbunden ist damit ein hohes Gefährdungspotential. Einmal in das IT-System eingedrungen, ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems überwunden (vgl. auch BVerfGE 120, 274 <314>). 192

(ee) Das Gewicht des Eingriffs wird schließlich dadurch erhöht, dass infolge des Zugriffs Gefahren für die Integrität des IT-Systems sowie für Rechtsgüter der Betroffenen und einer unbestimmten Vielzahl Dritter begründet werden. 193

Schon mit dem Zugriff als solchem geht das Risiko einer funktionellen Beeinträchtigung des IT-Systems einher. Dabei ist zu beachten, dass es einen rein lesenden Zugriff jedenfalls bei Infiltration eines IT-Systems mit einer Überwachungssoftware nicht gibt. Sowohl die Ermittlungsbehörde als auch von ihr mit der Durchführung betraute Dritte können Datenbestände versehentlich oder durch gezielte Manipulationen löschen, verändern oder neu anlegen (vgl. BVerfGE 120, 274 <325>). Zu berücksichtigen sind auch die mit dem Zugriff auf ein IT-System mittelbar einhergehenden Gefährdungen. Denn Ermittlungsbehörden dürfen insbesondere mit einer Überwachungssoftware auf ein Zielsystem zugreifen und dafür unbekannte IT-Sicherheitslücken ausnutzen (sog. Zero-Day-Exploits). So wirkt sich auf das Eingriffsgewicht aus, dass schon die Existenz dieser Befugnis einen Anreiz für Ermittlungsbehörden schafft, ihnen bekannte Sicherheitslücken offenzuhalten, um sie für eine Infiltration nutzen zu können (vgl. BVerfGE 120, 274 <326>; 158, 170 <188 f. Rn. 42>; 162, 1 <142 Rn. 316>; Rückert, Digitale Daten als Beweismittel im Strafverfahren, 2023, S. 192). In der Folge besteht die Gefahr, dass die Ermittlungsbehörde es etwa unterlässt, gegenüber anderen Stellen Maßnahmen zur Schließung solcher Sicherheitslücken anzuregen, oder sie sogar aktiv darauf hinwirkt, dass die Lücken unerkannt bleiben (BVerfGE 120, 274 <326>). 194

(ff) Eingriffsverstärkend wirkt, dass § 100a Abs. 1 Satz 2 StPO nicht nur eine einmalige und punktuelle Datenerhebung, sondern eine längerfristige Überwachung der Telekommunikation einschließlich der gesamten Internetkommunikation erlaubt (vgl. dazu auch BVerfGE 120, 274 <324>). Eingriffsmindernd wirkt jedoch, dass die Maßnahme als solche zeitlich befristet ist. § 100e Abs. 1 Satz 4 StPO sieht bei einer richterlichen Anordnung eine 195

Begrenzung auf höchstens drei Monate vor. Diese Anordnung kann zwar unbegrenzt oft verlängert werden; dies ist aber jeweils nur um denselben Höchstzeitraum möglich und bedarf erneut richterlicher Anordnung (vgl. § 100e Abs. 1 Satz 5 StPO; vgl. auch BVerfGE 165, 1 <49 Rn. 88>). Dabei besteht eine gesetzliche Verpflichtung, die Maßnahme bei Entfallen der Anordnungsvoraussetzungen unverzüglich abzubrechen (vgl. § 100e Abs. 5 StPO).

(gg) In einer Gesamtschau begründet die Quellen-Telekommunikationsüberwachung daher einen sehr schwerwiegenden Eingriff sowohl in Art. 10 Abs. 1 GG als auch in das IT-System-Grundrecht. 196

Ausgangspunkt ist insoweit, dass jede heimliche Überwachung der Telekommunikation grundsätzlich einen schweren Eingriff jedenfalls in Art. 10 Abs. 1 GG darstellt, weil dabei Kommunikation erfasst wird, die oftmals privaten und unter Umständen auch höchstvertraulichen Charakter hat (vgl. BVerfGE 129, 208 <240>; 154, 152 <241 Rn. 147>; BVerfG, Beschluss des Ersten Senats vom 8. Oktober 2024 - 1 BvR 1743/16 u.a. -, Rn. 157). 197

Obwohl es bei allen Varianten der Telekommunikationsüberwachung nach § 100a Abs. 1 StPO final um das Abschöpfen von Kommunikationsdaten geht, kommt der Quellen-Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 2 StPO aber schon aufgrund der Art und des Umfangs der verwertbaren Daten (Rn. 187 ff.) ein insbesondere gegenüber der klassischen Telekommunikationsüberwachung (vgl. Rn. 8, 188) deutlich erhöhtes Eingriffsgewicht zu. Eine Überwachung nach § 100a Abs. 1 Satz 2 StPO kann eine ungleich größere und aussagekräftigere Datenmenge betreffen. Hinzu kommt, dass Ermittlungsbehörden dabei nicht nur einen vulnerablen Moment einer auf Distanz geführten Kommunikationsbeziehung ausnutzen, sondern zugleich zu deren Schutz ergriffene Sicherheitsvorkehrungen überwinden, und damit nicht nur die Integrität von IT-Systemen beeinträchtigen, sondern zugleich auch deren Vertraulichkeit gefährden. 198

Gleichwohl wirkt die gegenständliche Beschränkung auf die laufende Telekommunikation – insbesondere im Vergleich zur Online-Durchsuchung nach § 100b StPO – noch eingriffsmindernd, denn die auf dem IT-System erzeugten, verarbeiteten und gespeicherten oder von dort aus zugänglichen Daten können jedenfalls nicht vollständig überwacht werden. Zum einen hängt es ganz maßgeblich vom Nutzerverhalten ab, ob und inwieweit insbesondere typischerweise lokal gespeicherte Daten (Videos, Bilder, Textdokumente) etwa aufgrund eines Cloud-Backups auch als laufende Telekommunikation erfasst werden können. Die Ergiebigkeit einer Überwachung ist daher im Einzelnen nicht vorhersehbar (vgl. dazu BVerfGE 154, 152 <241 Rn. 148>). Auch können die Betroffenen den Umfang des Datenzugriffs im Vergleich zur Online-Durchsuchung in höherem Maße selbst beeinflussen, indem sie etwa die Nutzung von auf Internetkommunikation basierenden Diensten minimieren. Zum anderen ermöglicht § 100a Abs. 1 Satz 2 StPO jedenfalls keine 199

Echtzeitüberwachung des gesamten IT-Systems in der Weise, dass etwa alle Bearbeitungsschritte beim Erstellen eines Textes erfasst werden können. Der Zugriff auf die laufende Telekommunikation mittels einer Quellen-Telekommunikationsüberwachung kann daher nicht mit dem Vollzugriff auf ein IT-System gleichgesetzt werden (vgl. Wissenschaftliche Dienste des Deutschen Bundestages, Ausarbeitung WD 3 - 3000 - 293/20 <2021>, S. 16; Henrichs/Weingast, in: Karlsruher Kommentar zur StPO, 9. Aufl. 2023, § 100a Rn. 42).

Im Ergebnis begründet eine Quellen-Telekommunikationsüberwachung aber gleichwohl – vor allem im Vergleich zur herkömmlichen Telekommunikationsüberwachung, aber auch aus sich heraus betrachtet – unter den heutigen Bedingungen der Nutzung von IT-Systemen einen sehr schwerwiegenden Eingriff sowohl in das IT-System-Grundrecht als auch in Art. 10 Abs. 1 GG (anders noch BVerfGE 141, 220 <310 Rn. 229, 312 Rn. 237>). 200

(2) Ausgehend von dem sehr hohen Eingriffsgewicht der von § 100a Abs. 1 Satz 2 StPO erlaubten Quellen-Telekommunikationsüberwachung muss diese aus Gründen der Verhältnismäßigkeit im engeren Sinne auf die Verfolgung besonders schwerer Straftaten beschränkt sein. 201

(a) Sehr schwerwiegende Eingriffe sind nur verhältnismäßig im engeren Sinne, wenn die entgegenstehenden Belange entsprechend gewichtig sind. Das Gewicht des Strafverfolgungsinteresses ist insbesondere von der Schwere und der Bedeutung der aufzuklärenden Straftat abhängig (vgl. BVerfGE 100, 313 <375 f., 392>; 107, 299 <321>). Danach bildet die Eingriffsintensität der jeweiligen Maßnahme den zentralen Bezugspunkt bei der Beantwortung der Frage, ob der Gesetzgeber ein verfassungsrechtlich zureichendes Straftatengewicht vorgesehen hat. Zu berücksichtigen ist aber auch, ob und inwieweit der Gesetzgeber die Eingriffsvoraussetzungen im Übrigen begrenzt hat. Erst im Rahmen einer solchen Gesamtschau kann beurteilt werden, ob er sich mit der Wahl einer bestimmten Kategorie von Straftaten (erheblich, schwer, besonders schwer) innerhalb des ihm zukommenden Spielraums bewegt. 202

(b) Danach muss eine wie in § 100a Abs. 1 Satz 2 StPO ausgestaltete Quellen-Telekommunikationsüberwachung der Verfolgung besonders schwerer Straftaten dienen. Anderenfalls wären die sehr schwerwiegenden Eingriffe in das IT-System-Grundrecht und in Art. 10 Abs. 1 GG materiell nicht mehr angemessen begrenzt. 203

Für Maßnahmen, die der Strafverfolgung dienen, kommt es auf das Gewicht der verfolgten Straftaten an, die der Gesetzgeber in erhebliche, schwere und besonders schwere Straftaten eingeteilt hat (vgl. BVerfGE 169, 130 <218 Rn. 202>; vgl. auch BVerfGE 141, 220 <270 Rn. 107> m.w.N.; 162, 1 <118 Rn. 251>). So bedarf es etwa für die Durchführung einer Wohnraumüberwachung des Verdachts einer besonders schweren Straftat (vgl. Art. 13 Abs. 3 GG; BVerfGE 109, 279 <343 ff.>), für die Durchführung einer Telekommunikationsüberwachung des Verdachts einer schweren Straftat (vgl. BVerfGE 125, 260 <328 f.>; 129, 204

208 <243>) und für die Durchführung einer Observation etwa durch einen GPS-Sender einer Straftat von erheblicher Bedeutung (vgl. BVerfGE 107, 299 <321 f.>; 112, 304 <315 f.>; 141, 220 <270 Rn. 107>). Hinzu tritt als vierte Kategorie die Ermächtigung zu Ermittlungsmaßnahmen zugunsten der Aufklärung einer jeden Straftat.

Die nach § 100a Abs. 1 Satz 2 StPO erlaubte Quellen-Telekommunikationsüberwachung erfordert wegen ihres hohen Eingriffsgewichts eine Begrenzung ihres Einsatzes auf die Verfolgung besonders schwerer Straftaten im verfassungsrechtlichen Sinne. Insofern gebietet auch eine Gesamtschau der Eingriffsvoraussetzungen keine Absenkung des erforderlichen Gewichts der verfolgten Straftaten. Denn der von § 100a Abs. 1 Satz 2 in Verbindung mit § 100a Abs. 1 Satz 1 Nr. 1 StPO verlangte qualifizierte Anfangsverdacht (vgl. Rn. 7) begegnet zwar für sich genommen keinen verfassungsrechtlichen Bedenken, umreißt aber auch keine besonders ausgeprägte Eingriffsschwelle. Auch der Subsidiaritätsvorbehalt, wonach die Strafverfolgung auf andere Weise wesentlich erschwert oder aussichtslos sein muss (vgl. § 100a Abs. 1 Satz 1 Nr. 3 StPO; dazu Rn. 7), begrenzt zwar die Maßnahme, darf in seiner Wirkung angesichts seiner normativen Weite aber nicht überschätzt werden. 205

Auch der Umstand, dass der Gesetzgeber die Quellen-Telekommunikationsüberwachung als funktionales Äquivalent zur klassischen Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 1 StPO ausgestaltet hat, um der Entwicklung Rechnung zu tragen, dass laufende Kommunikation zunehmend verschlüsselt erfolgt (vgl. BTDrucks 18/12785, S. 50 ff.; vgl. oben Rn. 4, 8), ändert an dem Erfordernis einer besonders schweren Straftat als Eingriffsanlass nichts. Zwar wollte der Gesetzgeber ausschließen, dass solche Daten erhoben werden dürfen, die auf dem infiltrierten System verarbeitet werden oder dort gespeichert sind, jedoch im Überwachungszeitraum nicht Teil der laufenden Kommunikation sind (vgl. Rückert, in: Münchener Kommentar zur StPO, 2. Aufl. 2023, § 100a Rn. 220). Insbesondere aber wegen Art und Umfang der heute mit dieser Maßnahme erhebbaren Daten (vgl. Rn. 188 f.) sowie wegen der mit einem Zugriff auf ein IT-System einhergehenden Integritätsverletzung und Vertraulichkeitsgefährdung ist eine Maßnahme nach § 100a Abs. 1 Satz 2 StPO nicht mehr mit einer klassischen Telekommunikationsüberwachung vergleichbar. 206

(c) Das danach erforderliche Gewicht der Anlassstraftaten ist vom Gesetzgeber vorzugeben (aa). Von den Ermittlungsbehörden sowie im Rahmen der unabhängigen Kontrolle (vgl. BVerfGE 141, 220 <275 f. Rn. 117 f.>) ist das Vorliegen eines entsprechenden Gewichts auch im Einzelfall zu überprüfen (bb). 207

(aa) Erfordert eine Befugnis zur Strafverfolgung den durch bestimmte Tatsachen begründeten Verdacht einer Straftat, die ein bestimmtes Gewicht aufweisen muss, bedarf dies näherer Konkretisierung. Welche Straftatbestände hiervon umfasst sein sollen, hat der Gesetzgeber selbst festzulegen. Ihm kommt hierbei ein Spielraum zu. Er kann entweder auf 208

bestehende Kataloge zurückgreifen oder einen eigenen Katalog schaffen, etwa um Straftaten, die für die konkrete Maßnahme besondere Bedeutung haben, zu erfassen (vgl. BVerfGE 125, 260 <328 f.>; 154, 152 <269 Rn. 221>). Die Qualifizierung einer Straftat als schwer oder besonders schwer muss aber in der Strafnorm selbst einen objektivierten Ausdruck finden (vgl. BVerfGE 109, 279 <343 ff.>; 125, 260 <329>; 169, 130 <220 Rn. 206>), also insbesondere in deren Strafrahmen und gegebenenfalls in tatbestandlich umschriebenen oder in einem Qualifikationstatbestand enthaltenen Begehungsmerkmalen und Tatfolgen (vgl. BVerfGE 109, 279 <344>; 169, 130 <220 Rn. 206>). Dabei ist der Gesetzgeber nicht auf Tatbestände beschränkt, die als Verbrechen im Sinne des § 12 StGB einzuordnen sind. Auch die Aufnahme von Vergehen in einen Katalog ist zulässig, wenn die Tatbestände das Merkmal der besonders schweren Straftat ausfüllen (vgl. BVerfGE 109, 279 <345>; 169, 130 <220 Rn. 207>). Werden für unbenannte schwere oder minderschwere Fälle abweichende Höchstfreiheitsstrafen angedroht, ist der jeweilige Grundtatbestand maßgeblich (vgl. BVerfGE 109, 279 <349>). Eine Generalklausel oder lediglich die abstrakte Verweisung auf Straftaten von besonderer Schwere reichen nicht aus (vgl. BVerfGE 125, 260 <329>).

Ausgehend vom Strafrahmen einer Strafnorm liegt die besondere Schwere einer Straftat jedenfalls dann vor, wenn sie mit einer Höchstfreiheitsstrafe von mehr als fünf Jahren bedroht ist (vgl. BVerfGE 109, 279 <347 f., 349>; 165, 1 <93 Rn. 179>; 169, 130 <219 Rn. 203>). Nach der gesetzlichen Systematik wird in Tatbeständen mit einem fünf Jahre übersteigenden oberen Strafrahmen sogleich eine Höchststrafe von zehn Jahren Freiheitsentzug oder mehr normiert. Sie ist denjenigen Delikten vorbehalten, die ein besonders schweres Tatunrecht aufweisen und damit den Bereich der mittleren Kriminalität eindeutig verlassen (vgl. BVerfGE 109, 279 <348>). 209

Dagegen qualifiziert eine Höchstfreiheitsstrafe von mindestens fünf Jahren eine Straftat weder als schwer (vgl. BVerfGE 129, 208 <243>; 141, 220 <338 Rn. 316>) noch als besonders schwer. Erfasst sind damit nämlich auch Straftaten mit einer Höchstfreiheitsstrafe von fünf Jahren, die allenfalls dem mittleren Kriminalitätsbereich zuzuordnen sind (vgl. BVerfGE 109, 279 <348>; 124, 43 <64>; 129, 208 <243>); dazu zählen auch Delikte der Massenkriminalität wie etwa der einfache Diebstahl, die öffentliche Verleumdung oder die einfache Körperverletzung (vgl. BVerfGE 141, 220 <338 Rn. 316>). Die besondere Schwere der Straftat wird allerdings nicht allein durch den Strafrahmen indiziert (vgl. BVerfGE 109, 279 <344>). Von daher kann jedenfalls eine Straftat mit einer angedrohten Höchstfreiheitsstrafe von mindestens fünf Jahren dann als besonders schwer eingestuft werden, wenn dies nicht nur unter Berücksichtigung des jeweils geschützten Rechtsguts und dessen Bedeutung für die Rechtsgemeinschaft, sondern auch unter Berücksichtigung der Tatbegehung und Tatfolgen vertretbar erscheint (vgl. BVerfGE 169, 130 <219 f. Rn. 205>). 210

Sind Straftaten allerdings nur mit einer Höchstfreiheitsstrafe von bis zu drei Jahren oder mit Geldstrafe bewehrt und damit dem einfachen Kriminalitätsbereich zuzuordnen, 211

schließt dies die Einordnung als besonders schwere Straftat von vornherein aus (vgl. BVerfGE 169, 130 <221 Rn. 208>).

(bb) Über die abstrakte Festlegung eines entsprechenden Straftatenkatalogs hinaus hat der Gesetzgeber zudem sicherzustellen, dass bestimmte Tatsachen den Verdacht begründen, dass die Tat auch im Einzelfall das erforderliche Gewicht aufweist (vgl. BVerfGE 125, 260 <329> m.w.N.). Denn angesichts der Vielgestaltigkeit des Lebens sind Fallgestaltungen denkbar, in denen ein abstrakt betrachtet etwa besonders schwerer oder auch nur schwerer Straftatbestand durch ein im Einzelfall in Rede stehendes Verhalten ausgefüllt wird, ohne dass dieser Sachverhalt einen Unrechtsgehalt aufweist, der die Durchführung eingriffsintensiver heimlicher Überwachungsmaßnahmen rechtfertigen könnte. 212

(3) Danach sind die durch § 100a Abs. 1 Satz 2 StPO begründeten Grundrechtseingriffe nicht gerechtfertigt, soweit eine Quellen-Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 2 in Verbindung mit § 100a Abs. 1 Satz 1 Nr. 1, Abs. 2 StPO auch zur Aufklärung solcher Straftaten erlaubt ist, die eine Höchstfreiheitsstrafe von drei Jahren oder weniger vorsehen und damit nur dem einfachen Kriminalitätsbereich zuzuordnen sind. 213

(a) Insoweit nicht von Belang ist allerdings, dass der Gesetzgeber selbst in § 100a Abs. 1 Satz 1 Nr. 1 StPO lediglich eine so bezeichnete „schwere Straftat" voraussetzt sowie solche „schweren Straftaten" abschließend in § 100a Abs. 2 StPO bestimmt und dass er in § 100a Abs. 1 Satz 1 Nr. 2 StPO lediglich voraussetzt, dass die Tat auch im Einzelfall „schwer" wiegen muss. Denn maßgeblich ist insoweit nur der materielle Gehalt der dort genannten Straftaten, den diese abstrakt und gleichermaßen auch konkret aufweisen müssen. 214

(b) Unter Zugrundelegung einer erforderlichen Begrenzung auf die Verfolgung von besonders schweren Straftaten genügen jedenfalls die in § 100a Abs. 2 StPO genannten Straftatbestände nicht den verfassungsrechtlichen Anforderungen, die lediglich eine Höchstfreiheitsstrafe von drei Jahren oder weniger vorsehen und damit dem einfachen Kriminalitätsbereich zuzuordnen sind. Diese Straftaten haben von vornherein kein besonders schweres Gewicht, weshalb sie die Anordnung einer so eingriffsintensiven Maßnahme wie die Quellen-Telekommunikationsüberwachung nicht rechtfertigen können. Im Einzelnen handelt es sich – soweit zulässig angegriffen – um die folgenden in § 100a Abs. 2 Nr. 1 Buchstaben a, c, d und t, Nr. 6 und Nr. 7 Buchstabe b StPO in der angegriffenen Fassung vom 17. August 2017 (BGBl I S. 3202) genannten Straftatbestände: § 85 Abs. 2 StGB, § 86 Absätze 1 und 2 StGB, § 97 Abs. 2 StGB, § 97b Abs. 1 Satz 1 in Verbindung mit § 97 Abs. 2 StGB, § 109g Abs. 1 in Verbindung mit Abs. 4 Satz 1 StGB, § 109g Abs. 2 StGB, § 129 Abs. 1 Satz 2 StGB, § 129 Abs. 1 Satz 2 in Verbindung mit § 129b StGB, § 130 Absätze 2, 4 und 5 StGB, § 310 Abs. 1 Nr. 4 in Verbindung mit § 309 Abs. 6 StGB, § 313 Abs. 2 in Verbindung mit § 308 Abs. 6 StGB, § 17 Abs. 5 AWG, § 18 Abs. 5a AWG, § 30b BtMG in Verbindung mit § 129 215

Abs. 1 Satz 2 StGB, § 30b BtMG in Verbindung mit § 129 Abs. 1 Satz 2 in Verbindung mit § 129b StGB.

Anders als im Gefahrenabwehrrecht sind die dem einfachen Kriminalitätsbereich zuzuordnenden Straftatbestände auch keiner ergänzenden Rechtsgutsbetrachtung zugänglich; auch eine zusätzliche Qualifizierung etwa als terroristische Straftat im Einzelfall wäre ohne Belang (vgl. dazu BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 138). Im repressiven Bereich kommt es vielmehr allein auf das Gewicht der verfolgten Straftaten an, das – neben dem Vorliegen einer hinreichenden Eingriffsschwelle – das staatliche Strafverfolgungsinteresse auslöst und dadurch repressive Ermittlungsmaßnahmen rechtfertigt. Straftatbeständen mit einer Höchstfreiheitsstrafe von nicht mehr als drei Jahren liegt jedoch selbst nach Einschätzung des Gesetzgebers prinzipiell kein tatbestandliches Unrecht zugrunde, das diese als besonders schwer erscheinen lassen könnte. 216

Soweit dagegen einzelne der in § 100a Abs. 2 StPO genannten Straftatbestände eine Höchstfreiheitsstrafe von fünf Jahren vorsehen und damit allenfalls dem mittleren Kriminalitätsbereich zuzuordnen sind, handelt es sich dabei zwar nicht von vorherein um besonders schwere Straftaten (vgl. Rn. 210). Mangels einer insoweit auf einzelne Straftatenbestände bezogenen Rüge (Rn. 120), sind diese jedoch nicht Prüfungsgegenstand. Bei allen übrigen in § 100a Abs. 2 StPO genannten Straftatbeständen handelt es sich schließlich um solche, für die eine Höchstfreiheitsstrafe von mehr als fünf Jahren angedroht wird, und damit um von vornherein besonders schwere Straftaten (vgl. Rn. 209). 217

3. Soweit die Befugnis zur Quellen-Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 2 StPO allein in Art. 10 Abs. 1 GG eingreift, weil etwa das betroffene IT-System nicht als eigenes genutzt wird und das IT-System-Grundrecht daher nicht betroffen ist (vgl. Rn. 173, 175), ist der Eingriff hingegen gerechtfertigt. Das insofern einer Überwachung nach § 100a Abs. 1 Satz 2 StPO zukommende Eingriffsgewicht entspricht insbesondere im Hinblick auf Art und Umfang der Daten (vgl. Rn. 187 ff.) und Art und Weise der Datenerhebung (Rn. 193 f.) bei weitem nicht einer gegen das eigengenutzte IT-System gerichteten Maßnahme, sondern ist eher mit einer Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 1 StPO vergleichbar. Es ist daher aus Gründen der Verhältnismäßigkeit insoweit zureichend, dass die Befugnis nach § 100a Abs. 1 Satz 2 in Verbindung mit § 100a Abs. 1 Satz 1 Nr. 1, Abs. 2 StPO auf die Verfolgung von „schweren Straftaten" beschränkt ist. Der Frage, ob und inwieweit allen in § 100a Abs. 2 StPO genannten Taten ein auch im verfassungsrechtlichen Sinne hinreichend schweres Gewicht zukommt, ist mangels entsprechender Rüge nicht nachzugehen. 218

II.

Der durch § 100a Abs. 1 Satz 3 StPO bewirkte Eingriff in das IT-System-Grundrecht ist ebenfalls nicht gerechtfertigt, soweit eine Quellen-Telekommunikationsüberwachung 219

nach § 100a Abs. 1 Satz 3 in Verbindung mit § 100a Abs. 1 Satz 1 Nr. 1, Abs. 2 StPO auch zur Aufklärung von Straftaten erlaubt ist, die eine Höchstfreiheitsstrafe von bis zu drei Jahren vorsehen und damit nur dem einfachen Kriminalitätsbereich zuzuordnen sind.

1. Die Befugnis zur Quellen-Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 3 StPO begründet ebenfalls einen Eingriff in das IT-System-Grundrecht, soweit auf ein eigengenutztes IT-System zugegriffen wird (a). Zwar betrifft § 100a Abs. 1 Satz 3 StPO auch den Schutzbereich des Rechts auf informationelle Selbstbestimmung (b). Dieses tritt hier jedoch zurück (c). 220

a) Eine Quellen-Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 3 StPO greift in das IT-System-Grundrecht ein (vgl. Hauck, in: Löwe-Rosenberg, StPO, 27. Aufl. 2019, § 100a Rn. 99, 146; Rückert, Digitale Daten als Beweismittel im Strafverfahren, 2023, S. 192; vgl. auch BTDrucks 18/12785, S. 50), denn Ermittlungsbehörden dürfen insoweit mit technischen Mitteln dergestalt auf IT-Systeme zugreifen, dass deren Leistungen, Funktionen und Speicherinhalte potentiell genutzt werden können. Ermöglicht wird ein Zugriff auf IT-Systeme in ihrer ganzen Breite. Unerheblich ist dabei, dass die Überwachung und Aufzeichnung nach § 100a Abs. 1 Satz 3, Abs. 5 Satz 1 Nr. 1 Buchstabe b StPO auf vormals laufende Telekommunikation ab dem Anordnungszeitpunkt begrenzt ist. Denn diese gegenständliche und zeitliche Begrenzung lässt unberührt, dass das Gefährdungspotential, das mit dem Zugriff unter Verwendung technischer Mittel unmittelbar einhergeht, die Vertraulichkeitserwartung an das IT-System insgesamt unterläuft. Einmal in das System eingedrungen, ist die Vertraulichkeit aller dort erzeugten, verarbeiteten und gespeicherten oder von dort aus zugänglichen Daten erheblich gefährdet (vgl. auch BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 103). Ein Eingriff in das IT-System-Grundrecht scheidet dagegen aus, sofern das IT-System etwa nicht eigengenutzt wird oder nicht hinreichend qualifiziert ist (vgl. BVerfGE 120, 274 <315>; näher Rn. 173, 175). 221

b) § 100a Abs. 1 Satz 3 StPO betrifft aber auch den Schutzbereich des Rechts auf informationelle Selbstbestimmung. 222

aa) Das Recht auf informationelle Selbstbestimmung schützt als Ausprägung des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) die Befugnis Einzelner, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden (vgl. BVerfGE 65, 1 <42>; 115, 320 <341>; 150, 1 <106 Rn. 219>). Der Schutzbereich ist auf die individuelle Selbstbestimmung Einzelner über ihre personenbezogenen Daten ausgerichtet (vgl. BVerfGE 115, 320 <341 f.>). Dementsprechend schützt das Recht auf informationelle Selbstbestimmung vor der unbegrenzten Erhebung, Speicherung, Verwendung und Weitergabe personenbezogener Daten (vgl. BVerfGE 65, 1 <43>; 115, 166 <188>; 115, 320 <341>; 120, 274 <312>; 169, 332 <364 Rn. 81>). Dieser vorgangsbezogene Schutz ist rein prozedural, also keiner Materialisierung 223

nach Stärke der Persönlichkeitsrelevanz zugänglich. So kommt es weder auf die Qualität und Sensibilität der Daten (vgl. BVerfGE 65, 1 <45>; 120, 378 <398>) noch auf den Speicherort (vgl. auch Rückert, Digitale Daten als Beweismittel im Strafverfahren, 2023, S. 153) an. Auch der Umfang der Daten ist nicht von Bedeutung. Das Recht auf informationelle Selbstbestimmung ist vielmehr bei jeder Erhebung, Speicherung, Verwendung oder Weitergabe personenbezogener Daten betroffen. Es schützt daher nicht nur vor einzelnen Datenerhebungen, sondern auch vor dem Zugriff auf große und dadurch typischerweise besonders aussagekräftige Datenbestände (vgl. Britz, DÖV 2008, S. 411 <412>; Hornung, CR 2008, S. 299 <301 f.>; Epping/Lenz/Leydecker, Grundrechte, 10. Aufl. 2024, Rn. 642); an seiner insoweit möglicherweise abweichenden Rechtsprechung im Urteil vom 27. Februar 2008 (BVerfGE 120, 274 <313>) hält der Senat nicht fest. Denn Schutzgegenstand des Rechts auf informationelle Selbstbestimmung ist nicht nur das einzelne Datum. Es schützt vielmehr gerade vor einer umfassenden Persönlichkeitsgefährdung durch (moderne) Informationstechnologie und die Kombination von Einzeldaten aus verschiedenen Quellen (vgl. dazu BVerfGE 65, 1 <42>; 165, 363 <388 f. Rn. 50, 394 Rn. 65, 396 ff. Rn. 69 f.>). Daher sind nicht nur individualisierbare Datenerhebungsvorgänge, sondern auch Zugriffe auf umfassende Datenbestände erfasst (vgl. zur Beschlagnahme des gesamten Datenbestands einer Rechtsanwaltskanzlei schon BVerfGE 113, 29 <45 f.>). Insofern ändert auch der Umstand, dass die Erhebung besonders vieler Daten einen besonders gravierenden Eingriff begründet, nichts. Anderenfalls stünde zu besorgen, dass gerade ein Zugriff auf große, aussagekräftige Datenmengen, insbesondere dann, wenn weder das IT-System-Grundrecht noch Art. 10 Abs. 1 GG betroffen sind, keinen spezifischen Grundrechtsschutz erfährt.

bb) § 100a Abs. 1 Satz 3 StPO betrifft deshalb auch den Schutzbereich des Rechts auf informationelle Selbstbestimmung. Die Befugnisnorm erlaubt die Erhebung von Daten aus Kommunikationsvorgängen, die nach deren Abschluss – und damit außerhalb des Schutzbereichs des Art. 10 Abs. 1 GG (vgl. dazu BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 88 m.w.N.; vgl. auch Rn. 113) – noch auf einem IT-System gespeichert sind. 224

c) Das Recht auf informationelle Selbstbestimmung tritt hier allerdings hinter dem IT-System-Grundrecht zurück. 225

aa) In dem für das IT-System-Grundrecht grundlegenden Urteil zur Online-Durchsuchung aus dem Jahr 2008 wurde das Konkurrenzverhältnis zwischen beiden Grundrechten letztlich noch nicht festgelegt. Das auf eine Online-Durchsuchung angewendete IT-System-Grundrecht wurde als notwendige weitere Ausprägung des allgemeinen Persönlichkeitsrechts angesichts neuer Gefährdungen für die freie Entfaltung der Persönlichkeit begründet. Damit ist aber keine Bestimmung eines Vorrangs für den Fall der Betroffenheit weiterer Grundrechtsgewährleistungen verbunden (vgl. mit Blick auf das Verhältnis des IT- 226

System-Grundrechts zu Art. 10 Abs. 1 GG BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 108 f.; vgl. auch Bäcker, in: Rensen/Brink, Linien der Rechtsprechung des Bundesverfassungsgerichts, Band 1, 2009, S. 99 <132>).

bb) Ermächtigt eine Norm zur Datenerhebung aus einem IT-System, auf das mit technischen Mitteln zugegriffen wird, verdrängt das IT-System-Grundrecht das ebenfalls betroffene Recht auf informationelle Selbstbestimmung. Von diesen beiden Ausprägungen des allgemeinen Persönlichkeitsrechts gewährleistet das IT-System-Grundrecht einen gegenüber dem Recht auf informationelle Selbstbestimmung spezifischen Schutz, der gerade die mit dem Zugriff auf eigengenutzte IT-Systeme verbundene Verletzung ihrer Integrität und Gefährdung der Vertraulichkeit in den Blick nimmt (vgl. im Ergebnis Bäcker, in: Rensen/Brink, Linien der Rechtsprechung des Bundesverfassungsgerichts, Band 1, 2009, S. 99 <132>; Hauser, Das IT-Grundrecht, 2015, S. 198 ff., insb. S. 203; Rühs, Durchsicht informationstechnischer Systeme, 2022, S. 189 f. m.w.N.; Rückert, Digitale Daten als Beweismittel im Strafverfahren, 2023, S. 177 f., 197; El-Ghazi, in: Verhandlungen des 74. Deutschen Juristentages, Band 1, Gutachten, 2024, C 50 m.w.N.) und jedenfalls bei einer auf diesem Weg erfolgenden Datenerhebung vorrangig ist. 227

Zwar dienen beide Grundrechte insbesondere der Verhaltensfreiheit und Privatheit und begegnen insoweit Gefährdungen der Persönlichkeit mit Blick auf den staatlichen Zugriff auf personenbezogene Daten. Das IT-System-Grundrecht hat aber als formalen Anknüpfungspunkt einen spezifischen Schutzgegenstand. Es knüpft an den vergegenständlichten Schutzraum eines eigengenutzten IT-Systems an, während das Recht auf informationelle Selbstbestimmung allgemein vor dem Zugriff auf personenbezogene Daten schützt, und zwar sowohl innerhalb als auch außerhalb des digitalen Raums sowie auf jedwedem IT-System oder im Cyberraum, unabhängig von der Zuordnung der betroffenen IT-Systeme (vgl. zum Wohnungsgrundrecht BVerfGE 51, 97 <105>; 109, 279 <325 f.>; 113, 29 <45>; 118, 168 <184>; zu möglichen Ausnahmen vgl. BVerfGE 115, 166 <187 f.>). Dabei schützt das IT-System-Grundrecht nicht nur die Vertraulichkeit der Daten, die durch Datenerhebungsvorgänge beeinträchtigt wird, sondern verlagert diesen Vertraulichkeitsschutz nach vorne. Vom Schutzbereich erfasst wird schon die abstrakt-systembezogene Vertraulichkeitserwartung im Vorfeld konkreter Datenerhebungen (vgl. BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 100 f.), wodurch ein insoweit spezifischer vorgelagerter Schutz der Persönlichkeit begründet wird. 228

Bereits die spezifische Gefährdungslage, die durch den Zugriff auf ein IT-System geschaffen wird, ist grundrechtsprägend und der Schutzbereich auf ein auf dieses System insgesamt bezogenes Gefährdungspotential ausgelegt (vgl. BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 100). Das IT-System-Grundrecht nimmt damit eine systembezogene, von der tatsächlichen Erhebung personenbezogener Daten 229

unabhängige Vertypung vor, mittels derer die Gefährdung des Persönlichkeitsrechts hervorgehoben und so die Eingriffsschwelle besonders deutlich markiert wird.

cc) Sind die Gewährleistungsbereiche beider Grundrechte betroffen, ist daher das IT-System-Grundrecht lex specialis. Raum für eine Anwendung des Rechts auf informationelle Selbstbestimmung bleibt allerdings auch bei Zugriffen auf IT-Systeme. So kann die informationelle Selbstbestimmung alleiniger Prüfungsmaßstab sein, wenn eine Datenerhebung aus einem infiltrierten IT-System nicht vom Gewährleistungsgehalt des IT-System-Grundrechts erfasst wird, weil etwa ein IT-System nicht hinreichend qualifiziert ist oder nicht als eigenes genutzt wird (vgl. Rn. 173; vgl. auch Hauser, Das IT-Grundrecht, 2015, S. 201). Bei einer Quellen-Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 3 GG, die lediglich den Zugriff auf gespeicherte Daten erlaubt, betrifft dies etwa auf dem IT-System gespeicherte Kommunikationsdaten Dritter, da hier auch Art. 10 Abs. 1 GG als spezielle Garantie nicht betroffen sein kann. Der Schutz aus dem Recht auf informationelle Selbstbestimmung kann insofern allerdings nicht weiter reichen als derjenige aus dem IT-System-Grundrecht (vgl. dazu auch BVerfGE 109, 279 <326>; vgl. näher Rn. 239). 230

2. Der durch einen Zugriff auf eigengenutzte IT-Systeme begründete Eingriff in das IT-System-Grundrecht ist nicht gerechtfertigt, soweit die Quellen-Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 3 in Verbindung mit § 100a Abs. 1 Satz 1 Nr. 1, Abs. 2 StPO auch zur Aufklärung von Straftaten erlaubt ist, die eine Höchstfreiheitsstrafe von drei Jahren oder weniger vorsehen und damit nur dem einfachen Kriminalitätsbereich zuzuordnen sind. 231

§ 100a Abs. 1 Satz 3 StPO genügt insoweit nicht den besonderen Anforderungen an die Rechtfertigung heimlicher Überwachungsmaßnahmen, die sich aus der Verhältnismäßigkeit im engeren Sinne ergeben (dazu Rn. 177 ff.). Gemessen an der Eingriffsintensität der Maßnahme (a) genügt das von § 100a Abs. 1 Satz 3 in Verbindung mit § 100a Abs. 1 Satz 1 Nr. 1, Abs. 2 StPO vorausgesetzte Gewicht der aufzuklärenden Straftaten nicht durchgängig den verfassungsrechtlichen Anforderungen (b). 232

a) Einer Quellen-Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 3 StPO kommt ebenfalls ein sehr schweres, wenngleich auch für sich genommen gegenüber § 100a Abs. 1 Satz 2 StPO leicht gemindertes Eingriffsgewicht zu. 233

Das Eingriffsgewicht, das sich vor allem nach Art, Umfang und denkbarer Verwendung der erhobenen Daten sowie der Gefahr ihres Missbrauchs, aber auch nach der Art und Weise der Datenerhebung als solcher bestimmt (näher Rn. 185), wiegt bei einer Quellen-Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 3 StPO ähnlich schwer wie das einer solchen nach § 100a Abs. 1 Satz 2 StPO. Infolge der technologischen Entwicklungen und der geänderten Nutzungsweise von IT-Systemen können auch nach § 100a Abs. 1 Satz 3 StPO 234

grundsätzlich Daten in einer Art und einem Umfang abgegriffen werden, die weitreichende persönlichkeitssensible Schlüsse zulassen (vgl. dazu Rn. 187 ff.).

Eingriffsmindernd wirkt allerdings, dass § 100a Abs. 1 Satz 3 StPO keinen generellen Zugriff auf gespeicherte Daten zulässt. Erlaubt ist nach § 100a Abs. 5 Satz 1 Nr. 1 Buchstabe b StPO nur die Überwachung von Inhalten und Umständen einer Kommunikation, die ab dem Zeitpunkt einer Anordnung nach § 100e Abs. 1 StPO angefallen und auf dem IT-System in einer Anwendung (noch) gespeichert sind. Maßgeblich ist insoweit die Anordnung der Quellen-Telekommunikationsüberwachung (vgl. dazu Hauck, in: Löwe-Rosenberg, StPO, 27. Aufl. 2019, § 100a Rn. 140, 142; Stellungnahme von Sinn, BTAusschussprotokoll des Ausschusses für Recht und Verbraucherschutz, Protokoll-Nr. 18/152, S. 129 f.) und nicht etwa eine im selben Ermittlungsverfahren zuvor ergangene Anordnung nach § 100a Abs. 1 Satz 1, § 100e Abs. 1 StPO, die eine rückwirkende Erhebung über einen potentiell sehr langen Zeitraum ermöglichte. Ausgeschlossen ist daher eine Erhebung von Daten, die vor der gerichtlichen Anordnung der Quellen-Telekommunikationsüberwachung gespeichert wurden (vgl. BTDrucks 18/12785, S. 52). Zu berücksichtigen ist allerdings, dass auch in kurzen Zeiträumen eine große Menge persönlichkeitssensibler Datenmengen anfallen können. Da aber eine Quellen-Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 3 StPO jedenfalls nach Vorstellung des Gesetzgebers (vgl. BTDrucks 18/12785, S. 51) nur ergänzend zu einer Maßnahme nach § 100a Abs. 1 Satz 2 StPO angeordnet werden soll, erfasst sie insoweit nur diejenigen Kommunikationsdaten, die auf dem IT-System im Zeitraum zwischen Anordnung und Zugriff in Form der Aktivierung der Überwachungssoftware gespeichert worden sind (vgl. insoweit zu § 11 Abs. 1a Satz 2 G10 BVerwGE 177, 327 <332 Rn. 14>). Dementsprechend dürfte eine Quellen-Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 3 StPO nach den in diesem Verfahren eingeholten Stellungnahmen der Äußerungsberechtigten regelmäßig nur einige Tage bis Wochen wirksam werden (dazu oben Rn. 67, 81). 235

Das Gewicht des Eingriffs wird auch dadurch vermindert, dass § 100a Abs. 1 Satz 3 StPO keine laufende, durch das Fernmeldegeheimnis geschützte Telekommunikation erfasst. Erlaubt ist lediglich die Überwachung und Aufzeichnung der gespeicherten Inhalte und Umstände früherer Telekommunikation, die vor allem über Messenger-Dienste geführt wurde (vgl. BTDrucks 18/12785, S. 50 f.; Graf, in: Graf, BeckOK StPO, § 100a Rn. 135 <Jan. 2025>). Dabei können technisch – anders als im Falle des § 100a Abs. 1 Satz 2 StPO – „flüchtige" Kommunikationsdaten, wie etwa Inhalte der Sprach- und Videotelefonie, nicht erfasst werden, soweit davon keine Aufzeichnungen auf den betroffenen IT-Systemen dauerhaft oder temporär gespeichert sind. Auch etwa der Datenverkehr mit Cloud-Diensten kann nach den Angaben der im Verfahren als sachkundige Dritte angehörten Gesellschaft für Datenschutz und Datensicherheit (vgl. Rn. 98) nur insoweit ausgeleitet werden, als er in Form von lokalen Synchronisationsdaten (wie etwa lokalen Zwischenkopien und temporär gespeicherten Daten) noch vorhanden ist. 236

Letztlich wirkt aber der auch mit einer Quellen-Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 3 StPO verbundene Systemzugriff deutlich eingriffsverstärkend (vgl. Rn. 193 f.). Dieser unterscheidet sie nicht nur maßgeblich von einer klassischen Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 1 StPO, sondern rückt die Maßnahme von ihrem Eingriffsgewicht her auch insgesamt näher an die Quellen-Telekommunikationsüberwachung nach § 100a Abs. 1 Satz 2 StPO heran. Im Vergleich zu dieser dürfte der Systemzugriff letztlich auch ein technisch höheres Gefährdungspotential aufweisen, weil eine Überwachungssoftware rein strukturell auf den gesamten Speicher des IT-Systems zugreifen kann und muss, um die gespeicherten Kommunikationsdaten zu finden und herauszufiltern. 237

b) Danach muss auch eine wie in § 100a Abs. 1 Satz 3 StPO ausgestaltete Quellen-Telekommunikationsüberwachung unter Berücksichtigung ihres Eingriffsgewichts der Verfolgung besonders schwerer Straftaten dienen. Anderenfalls wäre der sehr schwerwiegende Eingriff in das IT-System-Grundrecht materiell nicht mehr angemessen begrenzt. Dem genügen jedenfalls die in § 100a Abs. 2 Nr. 1 Buchstaben a, c, d und t, Nr. 6 und Nr. 7 Buchstabe b StPO in der angegriffenen Fassung vom 17. August 2017 (BGBl I S. 3202) genannten Straftatbestände nicht, die eine Höchstfreiheitsstrafe von drei Jahren oder weniger vorsehen (vgl. Rn. 215). 238

3. Soweit die Befugnis zur Quellen-Telekommunikationsüberwachung keinen Eingriff in das IT-System-Grundrecht begründet (vgl. Rn. 230) und deshalb am Recht auf informationelle Selbstbestimmung zu messen ist, ist ein Eingriff hingegen gerechtfertigt. Das insofern der Überwachung nach § 100a Abs. 1 Satz 3 StPO zukommende Eingriffsgewicht entspricht auch hier bei weitem nicht demjenigen einer gegen ein eigengenutztes IT-System gerichteten Maßnahme (vgl. Rn. 218). Es ist daher aus Gründen der Verhältnismäßigkeit insoweit zureichend, dass Eingriffe auf Grundlage des § 100a Abs. 1 Satz 3 in Verbindung mit § 100a Abs. 1 Satz 1 Nr. 1, Abs. 2 StPO auf die Verfolgung von „schweren Straftaten" begrenzt sind. Der Frage, ob und inwieweit allen in § 100a Abs. 2 StPO genannten Taten ein auch im verfassungsrechtlichen Sinne hinreichend schweres Gewicht zukommt, ist mangels entsprechender Rüge auch hier nicht nachzugehen. 239

III.

§ 100b Abs. 1 StPO verletzt Art. 10 Abs. 1 in Verbindung mit Art. 19 Abs. 1 Satz 2 GG (1), weil der Gesetzgeber das Zitiergebot nicht beachtet hat (2). Das Fehlen einer gesetzlichen Abbruchpflicht bei einer in Echtzeit durchgeführten Online-Durchsuchung führt hingegen weder zu einer Verletzung des IT-System-Grundrechts noch des Rechts auf informationelle Selbstbestimmung (3). 240

1. Die Befugnis zur Online-Durchsuchung nach § 100b Abs. 1 StPO ermöglicht Eingriffe sowohl in das IT-System-Grundrecht als auch in Art. 10 Abs. 1 GG, soweit das IT-System, auf 241

das zugegriffen wird, als eigenes genutzt wird. Sind beide Grundrechte betroffen, ist die Online-Durchsuchung an beiden Grundrechten zu messen.

§ 100b Abs. 1 StPO ermächtigt dazu, heimlich mit technischen Mitteln in ein von Betroffenen genutztes IT-System einzugreifen und daraus Daten zu erheben (Online-Durchsuchung). Die Erhebung umfasst alle im IT-System erzeugten, verarbeiteten und gespeicherten oder von dort aus zugänglichen Daten, womit das gesamte Nutzerverhalten nachvollzogen werden soll (vgl. BTDrucks 18/12785, S. 47, 54). Die Vorschrift begründet damit einen Eingriff in das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) in seiner Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-System-Grundrecht) (vgl. auch BVerfGE 120, 274 <302>; 141, 220 <303 Rn. 209>; 162, 1 <139 f. 307 f.>; 165, 1 <69 Rn. 128>) soweit das IT-System auch als eigenes genutzt wird (vgl. BVerfGE 120, 274 <315>). 242

Daneben liegt ein Eingriff in Art. 10 Abs. 1 GG vor, denn § 100b Abs. 1 StPO erlaubt auch die Überwachung der laufenden Fernkommunikation, die unter Nutzung eines IT-Systems stattfindet (allgemein dazu BVerfGE 120, 274 <307>; vgl. auch BVerfGE 158, 170 <184 Rn. 28>). Sind beide Grundrechte betroffen, stehen diese zueinander in Idealkonkurrenz (vgl. BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 105 ff. m.w.N.). Dies gilt auch mit Blick auf die Online-Durchsuchung (vgl. ausdrücklich offenlassend BVerfGE 120, 274 <340>; in der Sache offenlassend BVerfGE 141, 220 <303 Rn. 209>; 165, 1 <69 Rn. 128>; klarstellend zu BVerfGE 162, 1 <140 Rn. 308>). 243

Wird dagegen das überwachte IT-System nicht als eigenes genutzt – wie etwa bei einer Erhebung von Daten unvermeidbar betroffener Dritter (vgl. § 100b Abs. 3 Satz 3 StPO) – oder wird der Gewährleistungsgehalt des IT-System-Grundrechts aus anderen Gründen nicht berührt (vgl. Rn. 173; vgl. BVerfGE 120, 274 <314 f.>), können sich von einer Datenerhebung Betroffene, soweit die Erhebung die laufende Fernkommunikation betrifft, auf Art. 10 Abs. 1 GG und, soweit etwa nur gespeicherte Daten erhoben werden, auf das Recht auf informationelle Selbstbestimmung berufen (vgl. zur nicht eigengenutzten Wohnung BVerfGE 109, 279 <326>; in Bezug auf die Online-Durchsuchung wurden die vorgenannten Fallkonstellationen bisher erkennbar nicht in den Blick genommen, vgl. BVerfGE 141, 220 <303 Rn. 209>; 165, 1 <69 Rn. 128>; vgl. auch zur Überprüfung einer von vornherein auf eigengenutzte IT-Systeme beschränkten Ermächtigung BVerfGE 162, 1 <139 f. Rn. 307 f.> sowie im Übrigen Rn. 243). 244

2. § 100b Abs. 1 StPO ist schon aus formellen Gründen nicht mit der Verfassung vereinbar. Die Vorschrift genügt, soweit sie (auch) zu Eingriffen in Art. 10 Abs. 1 GG ermächtigt, nicht dem Zitiergebot des Art. 19 Abs. 1 Satz 2 GG. 245

a) Nach Art. 19 Abs. 1 Satz 2 GG muss ein Gesetz dasjenige Grundrecht unter Angabe seines Artikels benennen, das durch dieses Gesetz oder aufgrund dieses Gesetzes eingeschränkt 246

wird. Dieses sogenannte Zitiergebot findet Anwendung auf Grundrechte, die aufgrund ausdrücklicher Ermächtigung vom Gesetzgeber eingeschränkt werden dürfen (vgl. BVerfGE 64, 72 <79 f.>; 113, 348 <366>; 129, 208 <236>). Es erfüllt eine Warn- und Besinnungsfunktion (vgl. BVerfGE 113, 348 <366>; 120, 274 <343>). Durch die Benennung des Eingriffs im Gesetzeswortlaut soll gesichert werden, dass der Gesetzgeber nur Eingriffe vornimmt, die ihm als solche bewusst sind und über deren Auswirkungen auf die betroffenen Grundrechte er sich Rechenschaft ablegt (vgl. BVerfGE 85, 386 <404>; 113, 348 <366>; 129, 208 <236 f.>). Keiner Nennung bedürfen vor diesem Hintergrund allerdings Grundrechte, die nicht zielgerichtet zumindest mittelbar eingeschränkt werden. Denn eine Erstreckung des Zitiergebots auf solche Einschränkungen führte regelmäßig zur vorsorglichen Nennung einer Vielzahl etwaig berührter Grundrechte und entwertete damit die Warn- und Besinnungsfunktion des Zitiergebots (vgl. BVerfG, Urteil des Ersten Senats vom 26. November 2024 - 1 BvL 1/24 -, Rn. 97 m.w.N.).

Das Zitiergebot ist gerade dann verletzt, wenn der Gesetzgeber ausgehend von einer bestimmten Auslegung des Schutzbereichs ein Grundrecht als nicht betroffen erachtet und deshalb nicht als eingeschränkt benennt. Dann nämlich fehlt es an seinem Bewusstsein, zu Grundrechtseingriffen zu ermächtigen, und seinem Willen, sich über deren Auswirkungen Rechenschaft abzulegen (vgl. BVerfGE 154, 152 <237 Rn. 135>). Zudem entzieht sich der Gesetzgeber so einer öffentlichen Debatte, in der Notwendigkeit und Ausmaß von Grundrechtseingriffen zu klären sind (vgl. BVerfGE 85, 386 <403 f.>; 113, 348 <366>; 129, 208 <236 f.>; 154, 152 <237 Rn. 135>). Dem Zitiergebot ist daher nur Rechnung getragen, wenn das Grundrecht im Gesetzestext des einschränkenden Gesetzes selbst oder des dieses einführenden Gesetzes ausdrücklich als eingeschränkt benannt wird; selbst ein Hinweis in der Begründung des Gesetzentwurfs genügt nicht (vgl. etwa BVerfGE 113, 348 <367>). Das Bewusstsein, in Grundrechte einzugreifen, muss sich im Gesetzestext niedergeschlagen haben (vgl. BVerfGE 120, 274 <343>). 247

b) Danach genügt § 100b Abs. 1 StPO, der auch zu Eingriffen in Art. 10 Abs. 1 GG ermächtigt, nicht dem Zitiergebot nach Art. 19 Abs. 1 Satz 2 GG (für die Online-Durchsuchung nach § 5 Abs. 2 Nr. 11 VSG NRW a.F. noch offenlassend BVerfGE 120, 274 <340>). 248

aa) Das Grundrecht auf Wahrung des Fernmeldegeheimnisses steht nach Art. 10 Abs. 2 Satz 1 GG unter einem ausdrücklichen Gesetzesvorbehalt. Das Zitiergebot gilt daher auch für Einschränkungen des Art. 10 Abs. 1 GG (vgl. BVerfGE 113, 348 <366>; 154, 152 <236 Rn. 134>; vgl. auch Gersdorf, in: Gersdorf/Paal, BeckOK Informations- und Medienrecht, GG Art. 10 Rn. 47 <Nov. 2024>; Kaufhold, in: Dreier, GG, 4. Aufl. 2023, Art. 19 Abs. 1 Rn. 40; Wischmeyer, in: Dreier, GG, 4. Aufl. 2023, Art. 10 Rn. 104). Unbeachtlich ist insoweit, ob neben Art. 10 Abs. 1 GG noch weitere Grundrechte betroffen sind (vgl. etwa zu Art. 2 Abs. 2 Satz 1 GG und Art. 12 Abs. 1 GG BVerfGE 161, 299 <348 Rn. 121 f., 403 Rn. 255>). Art. 19 249

Abs. 1 Satz 2 GG gilt daher auch, soweit nicht allein Art. 10 Abs. 1 GG (vgl. insoweit Rn. 244 f.), sondern daneben das IT-System-Grundrecht anwendbar ist (vgl. Rn. 242 f.).

bb) § 100b Abs. 1 StPO genügt dem Zitiergebot nicht. Obgleich die Befugnis auch zu Eingriffen in das durch Art. 10 Abs. 1 GG geschützte Fernmeldegeheimnis ermächtigt (vgl. Rn. 242 ff.), nennen weder die Strafprozessordnung noch das § 100b StPO einführende Gesetz den Art. 10 Abs. 1 GG als durch § 100b StPO eingeschränkt. So zitiert das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017 (BGBl I S. 3202), mit dem die repressive Befugnis zur Online-Durchsuchung nach § 100b StPO erstmalig eingeführt wurde, in seinem Art. 17 den Art. 10 Abs. 1 GG lediglich im Hinblick auf Änderungen in § 100a StPO. 250

cc) Eine verfassungskonforme Auslegung, welche die Verfassungswidrigkeit von § 100b StPO vermeiden könnte, kommt nicht in Betracht. Grundsätzlich kann zwar einer solchen Auslegung der Vorrang vor einer Feststellung der Verfassungswidrigkeit zu geben sein (vgl. BVerfGE 130, 151 <204>). Dies setzt aber eine Auslegungsfähigkeit der bemakelten Bestimmung dahin voraus, dass sie nicht das Grundrecht einschränkt, dessen Nichtzitierung den Verstoß gegen Art. 19 Abs. 1 Satz 2 GG begründet. Eine Auslegung des § 100b StPO dahin, dass die Vorschrift nicht zu Eingriffen in Art. 10 Abs. 1 GG und damit nicht zur Überwachung der insbesondere auch über das Internet geführten Telekommunikation ermächtigt, ist jedoch nicht möglich. Sie träte in Widerspruch zu dem klar erkennbar geäußerten Willen des Gesetzgebers (vgl. dazu BVerfGE 128, 157 <179>; 162, 1 <171 Rn. 387>), der in den Gesetzgebungsmaterialien ausdrücklich davon ausgegangen ist, dass mit der Online-Durchsuchung eines IT-Systems das gesamte Nutzungsverhalten einer Person überwacht werden soll (vgl. BTDrucks 18/12785, S. 47, 54). 251

3. § 100b Abs. 1 StPO genügt dagegen – soweit zulässig gerügt – den verfassungsrechtlichen Anforderungen an den Schutz des Kernbereichs privater Lebensgestaltung, die sich aus den betroffenen Grundrechten in Verbindung mit Art. 1 Abs. 1 GG für die Durchführung von wie hier besonders eingriffsintensiven heimlichen Überwachungsmaßnahmen schon für die Erhebungsphase ergeben. Der Gesetzgeber musste insbesondere kein Abbruchgebot für den Fall vorsehen, in dem erkennbar wird, dass eine Überwachung in den Kernbereich privater Lebensführung eindringt. Hiervon unberührt bleibt, dass ein Abbruch bei Anwendung der Maßnahme im Einzelfall geboten sein kann (vgl. zur Anwendung nicht verletzungsgeneigter Überwachungsbefugnisse Rn. 255). 252

Die verfassungsrechtlichen Anforderungen an einen hinreichenden Kernbereichsschutz bei eingriffsintensiven Maßnahmen können zwar grundsätzlich auch ein gesetzlich geregeltes Abbruchgebot erfordern (a). Dies gilt aufgrund ihres spezifischen Charakters aber nicht für die Online-Durchsuchung (b). 253

a) aa) Neben den verfassungsrechtlichen Anforderungen an die allgemeinen Eingriffsvoraussetzungen ergeben sich aus den jeweiligen Grundrechten in Verbindung mit Art. 1 Abs. 1 GG für die Durchführung besonders eingriffsintensiver Maßnahmen besondere Anforderungen an den Schutz des Kernbereichs privater Lebensgestaltung. Dieser Schutz gewährleistet einen Bereich höchstpersönlicher Privatheit des Individuums gegenüber staatlichen Überwachungsmaßnahmen. Selbst überragende Interessen der Allgemeinheit können einen Eingriff in diesen absolut geschützten Bereich nicht rechtfertigen (vgl. BVerfGE 141, 220 <276 Rn. 119 f.>; 165, 1 <56 Rn. 102>; stRspr). 254

Der Kernbereich privater Lebensgestaltung beansprucht gegenüber allen Überwachungsmaßnahmen Beachtung. Können sie typischerweise zur Erhebung kernbereichsrelevanter Daten führen, muss der Gesetzgeber Regelungen schaffen, die einen wirksamen Schutz normenklar gewährleisten. Außerhalb solch verletzungsgeneigter Befugnisse bedarf es eigener Regelungen nicht. Grenzen, die sich im Einzelfall auch hier gegenüber einem Zugriff auf höchstpersönliche Informationen ergeben können, sind bei deren Anwendung unmittelbar von Verfassungs wegen zu beachten (vgl. BVerfGE 141, 220 <277 f. Rn. 123>; 162, 1 <127 Rn. 278>). 255

Der Schutz des Kernbereichs privater Lebensgestaltung ist strikt und darf nicht durch Abwägung mit den Sicherheitsinteressen nach Maßgabe des Verhältnismäßigkeitsgrundsatzes relativiert werden (vgl. BVerfGE 109, 279 <314>; 120, 274 <339>; stRspr). Dies bedeutet jedoch nicht, dass jede tatsächliche Erfassung von höchstpersönlichen Informationen stets einen Verfassungsverstoß oder eine Menschenwürdeverletzung begründet. Angesichts der Handlungs- und Prognoseunsicherheiten, unter denen Sicherheitsbehörden ihre Aufgaben wahrnehmen, kann ein unbeabsichtigtes Eindringen in den Kernbereich privater Lebensgestaltung im Rahmen von Überwachungsmaßnahmen nicht für jeden Fall von vornherein ausgeschlossen werden (vgl. BVerfGE 120, 274 <337 f.>). Die Verfassung verlangt jedoch für die Ausgestaltung der Überwachungsbefugnisse die Achtung des Kernbereichs als eine strikte, nicht frei durch Einzelfallerwägungen überwindbare Grenze (BVerfGE 141, 220 <278 Rn. 124>). 256

Absolut ausgeschlossen ist damit zunächst, den Kernbereich zum Ziel staatlicher Ermittlungen zu machen (vgl. BVerfGE 141, 220 <278 Rn. 125>, 165, 1 <60 Rn. 110>). Des Weiteren folgt hieraus, dass bei der Durchführung von Überwachungsmaßnahmen dem Kernbereichsschutz auf zwei Ebenen Rechnung getragen werden muss. Zum einen sind auf der Ebene der Datenerhebung Vorkehrungen zu treffen, die eine unbeabsichtigte Miterfassung von Kernbereichsinformationen nach Möglichkeit ausschließen. Zum anderen sind auf der Ebene der nachgelagerten Aus- und Verwertung die Folgen eines dennoch erfolgten Eindringens in den Kernbereich privater Lebensgestaltung strikt zu minimieren (vgl. BVerfGE 141, 220 <278 f. Rn. 126>; 165, 1 <59 f. Rn. 108>; stRspr). 257

bb) In diesem Rahmen kann der Gesetzgeber den Schutz des Kernbereichs privater Lebensgestaltung in Abhängigkeit von der Art der Befugnis und deren Nähe zum absolut geschützten Bereich privater Lebensgestaltung für die verschiedenen Überwachungsmaßnahmen verschieden ausgestalten (vgl. BVerfGE 120, 274 <337>; 129, 208 <245>; 141, 220 <279 Rn. 127>). 258

Auf der Ebene der Datenerhebung ist bei Maßnahmen, die typischerweise zur Erhebung kernbereichsrelevanter Daten führen, durch eine vorgelagerte Prüfung sicherzustellen, dass die Erfassung von kernbereichsrelevanten Situationen oder Gesprächen jedenfalls insoweit ausgeschlossen ist, als sich diese mit praktisch zu bewältigendem Aufwand im Vorfeld vermeiden lässt (vgl. BVerfGE 141, 220 <279 Rn. 128>; 154, 152 <264 Rn. 206>; 165, 1 <61 Rn. 111>; stRspr). Die gesetzliche Regelung hat etwa darauf hinzuwirken, dass die Erhebung kernbereichsrelevanter Daten soweit wie informationstechnisch und ermittlungstechnisch möglich unterbleibt (vgl. für die Online-Durchsuchung BVerfGE 120, 274 <338>). Schon auf der Ebene der Datenerhebung ist auch der Abbruch einer Überwachungsmaßnahme vorzusehen, wenn erkennbar wird, dass die Überwachung in den Kernbereich privater Lebensgestaltung eindringt (vgl. BVerfGE 141, 220 <279 Rn. 128>; 165, 1 <62 Rn. 113>). Dies gilt insbesondere bei einer Wohnraumüberwachung (vgl. BVerfGE 109, 279 <318, 324, 331>; 141, 220 <300 Rn. 199>; 162, 1 <128 Rn. 281>) sowie grundsätzlich auch für den Einsatz von Vertrauenspersonen und verdeckt Ermittelnden (vgl. BVerfGE 165, 1 <62 f. Rn. 113 ff.>). Ein Abbruchgebot gilt aber weder ausnahmslos (vgl. insoweit BVerfGE 165, 1 <63 Rn. 115>) noch unterschiedslos für alle Überwachungsmaßnahmen. Unter Berücksichtigung der Art der Informationserhebung und der durch sie erfassten Informationen (vgl. insoweit BVerfGE 129, 208 <245>) ist ein Abbruchgebot nur dann vorzusehen, wenn sich damit die Erhebung kernbereichsrelevanter Informationen auch mit praktisch zu bewältigendem Aufwand vermeiden lässt. So kann es etwa bei einer Telekommunikationsüberwachung praktisch schwierig sein, kernbereichsrelevante Inhalte überhaupt zu erkennen und als solche einzuordnen (vgl. dazu BVerfGE 129, 208 <248 f.>). 259

b) Danach ist es aufgrund des spezifischen Charakters einer Online-Durchsuchung nicht geboten, zum Schutz des Kernbereichs ein gesetzliches Abbruchgebot vorzusehen. 260

aa) Da der heimliche Zugriff auf IT-Systeme typischerweise die Gefahr einer Erfassung auch höchstvertraulicher Daten in sich trägt und damit eine besondere Nähe zum Kernbereich privater Lebensgestaltung aufweist, bedarf es ausdrücklicher gesetzlicher Vorkehrungen zu dessen Schutz. Die diesbezüglichen Anforderungen sind allerdings mit denen der Wohnraumüberwachung nicht in jeder Hinsicht identisch und verschieben den Schutz ein Stück weit von der Erhebungsebene auf die nachgelagerte Aus- und Verwertungsebene (vgl. BVerfGE 120, 274 <335 ff.>; 141, 220 <306 Rn. 218>; 162, 1 <129 f. Rn. 284>). Dies hat seinen Grund in dem technischen Charakter des Zugriffs auf informationstechnische Systeme. Der Schutz vor Kernbereichsverletzungen zielt hier darauf, zu verhindern, dass 261

höchstvertrauliche Informationen aus einem Gesamtdatenbestand von ohnehin digital vorliegenden Informationen ausgelesen werden, die in ihrer Gesamtheit, typischerweise aber nicht schon als solche, den Charakter der Privatheit wie das Verhalten oder die Kommunikation in einer Wohnung aufweisen. Dementsprechend sind die Anforderungen an den Kernbereichsschutz auf der Erhebungsebene etwas geringer (BVerfGE 162, 1 <129 f. Rn. 284>; vgl. auch BVerfGE 141, 220 <306 f. Rn. 218 f.>).

Allerdings ist auch für eine Online-Durchsuchung vorzusehen, dass die Erhebung von Informationen, die dem Kernbereich zuzuordnen sind, soweit wie informationstechnisch und ermittlungstechnisch möglich, unterbleibt. Insbesondere sind verfügbare informationstechnische Sicherungen einzusetzen; können mit deren Hilfe höchstvertrauliche Informationen aufgespürt und isoliert werden, ist der Zugriff auf diese untersagt (vgl. BVerfGE 120, 274 <338>; 141, 220 <307 Rn. 219>; 162, 1 <130 Rn. 285>). 262

Können aber in der konkreten Anwendung kernbereichsrelevante Daten vor oder bei der Datenerhebung nicht ausgesondert werden, ist ein Zugriff auf das informationstechnische System auch dann zulässig, wenn hierbei eine Wahrscheinlichkeit besteht, dass am Rande auch höchstpersönliche Daten miterfasst werden. Der Gesetzgeber hat insofern dem Schutzbedarf der Betroffenen durch Sicherungen auf der Aus- und Verwertungsebene Rechnung zu tragen und die Auswirkungen eines solchen Zugriffs zu minimieren (vgl. BVerfGE 120, 274 <338 f.>; 141, 220 <307 Rn. 220>; 162, 1 <130 Rn. 286>). 263

bb) Danach genügen die für die Erhebungsebene in § 100d StPO vorgesehenen Bestimmungen zum Kernbereichsschutz den verfassungsrechtlichen Anforderungen an eine Online-Durchsuchung. Neben den vorgesehenen Sicherungen des Kernbereichs privater Lebensgestaltung in § 100d Abs. 1 StPO und § 100d Abs. 3 Satz 1 StPO (vgl. dazu BVerfGE 141, 220 <308 Rn. 222>; 162, 1 <141 Rn. 314>) bedarf es keiner weiteren gesetzlichen Sicherung in Form eines Abbruchgebots (vgl. im Ergebnis BVerfGE 120, 274 <338>; 141, 220 <307 f. Rn. 222>; 162, 1 <141 Rn. 314>; zur Auslandsfernmeldeaufklärung vgl. BVerfGE 154, 152 <264 Rn. 206>; BVerfG, Beschluss des Ersten Senats vom 8. Oktober 2024 - 1 BvR 1743/16 u.a. -, Rn. 167>). 264

Ein gesetzliches Abbruchgebot ist unter Berücksichtigung des spezifischen Charakters der Online-Durchsuchung nach § 100b StPO nicht geboten. Wegen der Art der Informationserhebung und der durch sie erfassten Informationen lässt sich – jenseits der vorgenannten Sicherungen – ein Eindringen in den Kernbereich bei Durchführung einer Online-Durchsuchung nicht mit praktisch zu bewältigendem Aufwand vermeiden. Insoweit ist zunächst zu berücksichtigen, dass die Datenerhebung im Rahmen eines technischen Zugriffs auf IT-Systeme schon aus technischen Gründen überwiegend automatisiert erfolgt. Die Automatisierung erschwert es jedoch – jenseits technischer Sicherungen – im Vergleich zu einer durch Personen durchgeführten Maßnahme, bereits bei der Erhebung Daten mit und ohne 265

Bezug zum Kernbereich zu unterscheiden (vgl. BVerfGE 120, 274 <337>). Selbst wenn aber der Datenzugriff unmittelbar durch Personen durch (paralleles) Mithören oder -lesen in Echtzeit erfolgt, stößt der Kernbereichsschutz – der in Echtzeit in der Regel nur punktuell stattfinden kann (vgl. zur Telekommunikationsüberwachung BVerfGE 129, 208 <248>) – auf praktische Schwierigkeiten. So kann die Kernbereichsrelevanz schon während der Erhebung vielfach nicht abgeschätzt werden, weil es sich etwa um fremdsprachige oder schlecht verständliche, über das Internet geführte Gespräche handelt (vgl. BVerfGE 120, 274 <338>; 129, 208 <248>) oder weil nicht beurteilt werden kann, in welchen persönlichen Beziehungen Kommunikationspartner zueinanderstehen (vgl. BVerfGE 129, 208 <248 f.>).

Die größte Herausforderung für einen Kernbereichsschutz schon auf der Ebene der Datenerhebung ergibt sich aber daraus, dass bei der Überwachung eines IT-Systems, auf das mit technischen Mitteln heimlich zugegriffen werden darf, aufgrund dessen zunehmender Nutzungsmöglichkeiten nicht nur zahlreiche und verschiedenartige Daten erfasst werden können, sondern diese zudem in gleichzeitig stattfindenden Prozessen erzeugt, verarbeitet oder gespeichert werden. Anders als etwa bei der Überwachung des in der Wohnung gesprochenen Worts fehlt es daher an einem klar fassbaren Bezugspunkt. Und anders als bei dem Einsatz von Vertrauenspersonen und verdeckt Ermittelnden besteht auch keine konkrete, von den eingesetzten Überwachungspersonen grundsätzlich gestaltbare Kommunikations- oder Interaktionsbeziehung (vgl. dazu BVerfGE 165, 1 <62 Rn. 113>). Für die Nutzung eines IT-Systems ist es vielmehr geradezu typisch, dass eine Vielzahl unterschiedlicher digitaler Anwendungen parallel Datenströme produziert und dies sowohl veranlasst durch die Nutzenden selbst als auch fremdgesteuert oder systembedingt. Erfasst daher eine Maßnahme kernbereichsrelevante Daten aus einer spezifischen Nutzung oder Anwendung eines IT-Systems, kann dasselbe System weiter zu zahlreichen Zwecken ohne Kernbereichsrelevanz genutzt werden. Wird erkennbar, dass eine Überwachung in den Kernbereich privater Lebensgestaltung eindringt, ist es verfassungsrechtlich aber nicht geboten, zwangsläufig die gesamte Maßnahme zu beenden (vgl. zum Einsatz von Vertrauenspersonen und verdeckt Ermittelnden BVerfGE 165, 1 <62 Rn. 113>). Doch auch ein nur teilweiser Abbruch kann – insbesondere aufgrund der verschiedenartigen Kommunikations- und Interaktionsbeziehungen sowie der unterschiedlichen Arten der Daten – vor allem in seiner Reichweite praktisch kaum sinnvoll abgegrenzt und durchgeführt werden. 266

Werden bei einer Überwachungsmaßnahme trotz der Sicherungen in § 100d Abs. 1, Abs. 3 Satz 1 StPO kernbereichsrelevante Daten erfasst, bieten – ungeachtet dessen, dass es dazu an einer zulässigen Rüge fehlt (vgl. Rn. 151) – § 100d Abs. 2, Abs. 3 Satz 2 StPO insofern einen nachgelagerten Schutz auf der Aus- und Verwertungsebene, als Kommunikationsinhalte des höchstpersönlichen Bereichs nicht verwertet werden dürfen, sondern unverzüglich zu löschen sind (vgl. dazu BVerfGE 113, 348 <392>). 267

c) Soweit eine Online-Durchsuchung nach § 100b Abs. 1 StPO nicht vom IT-System-Grundrecht erfasst wird, weil etwa Dritte betroffen sind, kann der Schutz des in solchen Fällen allein beeinträchtigten Fernmeldegeheimnisses oder Rechts auf informationelle Selbstbestimmung (vgl. Rn. 244) nicht weiter reichen (vgl. dazu auch BVerfGE 109, 279 <326>). 268

D.

I.

Im Ergebnis genügen die zulässig angegriffenen Normen den verfassungsrechtlichen Anforderungen teilweise nicht. 269

1. § 100a Abs. 1 Sätze 2 und 3 in Verbindung mit § 100a Abs. 1 Satz 1 Nr. 1, Abs. 2 StPO in der angegriffenen Fassung vom 17. August 2017 sind verfassungswidrig, soweit auf in § 100a Abs. 2 Nr. 1 Buchstaben a, c, d und t, Nr. 6 und Nr. 7 Buchstabe b StPO genannte Straftatbestände Bezug genommen wird, die eine Höchstfreiheitsstrafe von bis zu drei Jahren vorsehen (§ 85 Abs. 2 StGB, § 86 Absätze 1 und 2 StGB, § 97 Abs. 2 StGB, § 97b Abs. 1 Satz 1 in Verbindung mit § 97 Abs. 2 StGB, § 109g Abs. 1 in Verbindung mit Abs. 4 Satz 1 StGB, § 109g Abs. 2 StGB, § 129 Abs. 1 Satz 2 StGB, § 129 Abs. 1 Satz 2 in Verbindung mit § 129b StGB, § 130 Absätze 2, 4 und 5 StGB, § 310 Abs. 1 Nr. 4 in Verbindung mit § 309 Abs. 6 StGB, § 313 Abs. 2 in Verbindung mit § 308 Abs. 6 StGB, § 17 Abs. 5 AWG, § 18 Abs. 5a AWG, § 30b BtMG in Verbindung mit § 129 Abs. 1 Satz 2 StGB, § 30b BtMG in Verbindung mit § 129 Abs. 1 Satz 2 in Verbindung mit § 129b StGB). Die Regelungen verletzen die Beschwerdeführenden zu 1) und 5) in ihrem IT-System-Grundrecht und – soweit § 100a Abs. 1 Satz 2 StPO betroffen ist – zugleich in Art. 10 Abs. 1 GG. 270

2. § 100b Abs. 1 StPO ist verfassungswidrig. Die Regelung verletzt die Beschwerdeführenden zu 1), 2), 4) und 5) aufgrund eines Verstoßes gegen das Zitiergebot in ihrem Grundrecht aus Art. 10 Abs. 1 GG in Verbindung mit Art. 19 Abs. 1 Satz 2 GG. Damit geht allerdings nicht die Verfassungswidrigkeit des gesamten Gesetzes – hier des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017 (BGBl I S. 3202 ff.) – einher, sondern sie beschränkt sich auf die Bestimmung, die den gerügten Verstoß gegen das Zitiergebot begründet. 271

II.

1. Die Feststellung der Verfassungswidrigkeit gesetzlicher Vorschriften führt grundsätzlich zu deren Nichtigkeit. Allerdings kann sich das Bundesverfassungsgericht, wie sich aus § 31 Abs. 2 Sätze 2 und 3 sowie § 79 Abs. 1 und § 93c Abs. 1 Satz 3 BVerfGG ergibt (vgl. BVerfGE 166, 1 <88 Rn. 187> – Kinderehe), auch darauf beschränken, eine verfassungswidrige Norm nur für mit der Verfassung unvereinbar zu erklären. Es verbleibt dann bei einer 272

bloßen Beanstandung der Verfassungswidrigkeit ohne den Ausspruch der Nichtigkeit. Die Unvereinbarkeitserklärung kann das Bundesverfassungsgericht dabei zugleich mit der Anordnung einer befristeten Fortgeltung der verfassungswidrigen Regelung verbinden. Dies kommt in Betracht, wenn die sofortige Ungültigkeit der zu beanstandenden Norm dem Schutz überragender Güter des Gemeinwohls die Grundlage entziehen würde und eine Abwägung mit den betroffenen Grundrechten ergibt, dass der Eingriff für eine Übergangszeit hinzunehmen ist (BVerfGE 165, 1 <100 Rn. 201> m.w.N.; stRspr).

2. a) Danach sind § 100a Abs. 1 Sätze 2 und 3 StPO im Umfang ihrer Verfassungswidrigkeit (dazu Rn. 270) für mit der Verfassung unvereinbar und nichtig zu erklären. Sie genügen insoweit nicht den verfassungsrechtlichen Anforderungen. Eine verfassungsmäßige Regelung mit vergleichbarem Regelungsgehalt kann der Gesetzgeber auch durch Nachbesserung nicht herbeiführen. 273

Die Gründe, die zur teilweisen Nichtigkeit von § 100a Abs. 1 Sätze 2 und 3 StPO in der angegriffenen Fassung vom 17. August 2017 (BGBl I S. 3202) führen, treffen hinsichtlich der in § 100a Abs. 2 StPO genannten Straftatbestände, die eine Höchstfreiheitsstrafe von drei Jahren oder weniger vorsehen (vgl. Rn. 270), ebenso auf alle nachfolgenden Fassungen zu. Gemäß § 78 Satz 2 BVerfGG, der auch im Verfassungsbeschwerdeverfahren und auf zeitlich nachfolgende Gesetzesfassungen anwendbar ist (vgl. BVerfGE 133, 377 <423 Rn. 106>), sind insoweit daher auch die Fassungen späterer Gesetze im Interesse der Rechtsklarheit für mit dem Grundgesetz unvereinbar zu erklären. Dies betrifft alle von der Nichtigkeitserklärung konkret erfassten Straftatbestände, und zwar unabhängig davon, an welcher Stelle sie in § 100a Abs. 2 StPO katalogmäßig erfasst werden. Unerheblich ist daher, dass etwa § 100a Abs. 2 Nr. 1 Buchstabe t StPO, der in der angegriffenen Fassung die Straftatbestände in § 310 Abs. 1 Nr. 4 in Verbindung mit § 309 Abs. 6 StGB und § 313 Abs. 2 in Verbindung mit § 308 Abs. 6 StGB nennt, zwischenzeitlich als § 100a Abs. 2 Nr. 1 Buchstabe u StPO in der Fassung des Gesetzes gegen illegale Beschäftigung und Sozialleistungsmissbrauch vom 11. Juli 2019 (BGBl I S. 1066) neu bezeichnet wurde. 274

b) Demgegenüber ist § 100b Abs. 1 StPO lediglich für mit der Verfassung unvereinbar zu erklären. Die Gründe für die Verfassungswidrigkeit dieser Regelung betreffen nicht den Kern der mit ihr eingeräumten Befugnis, sondern einen einzelnen Aspekt ihres rechtsstaatlichen Zustandekommens. Der Gesetzgeber kann die verfassungsrechtliche Beanstandung beseitigen und damit die mit der Vorschrift verfolgten Ziele in einem verfassungsmäßigen Verfahren verwirklichen (vgl. BVerfGE 150, 309 <344 f. Rn. 97>), indem er sich nach den Vorgaben des Art. 19 Abs. 1 Satz 2 GG bewusst macht, dass er eine Befugnis zur Online-Durchsuchung auch im Lichte des Art. 10 Abs. 1 GG regeln muss, und sich darüber Rechenschaft ablegt (vgl. auch BVerfGE 5, 13 <16>; 154, 152 <237 Rn. 135>). Die Verfassungswidrigkeit der zu beanstandenden Regelung ist für eine Übergangszeit hinzunehmen. Die Befugnis zur Online-Durchsuchung hat für die Strafverfolgung unter Berücksichtigung der 275

Entwicklungen in der Informationstechnik eine große Bedeutung. Durch eine Nichtigerklärung oder eine vorläufige Außerkraftsetzung würden erhebliche Risiken eingegangen. Angesichts der ihrerseits großen Bedeutung der Strafverfolgung ist eine vorübergehende Fortgeltung der verfassungswidrigen Vorschrift eher hinzunehmen als deren Beseitigung bis zu einer Neuregelung, mit der absehbar zu rechnen ist.

Die Unvereinbarkeitserklärung betrifft zunächst § 100b Abs. 1 StPO. Da damit aber für die Regelungen in § 100b Absätze 2 bis 4 StPO kein selbständiger Anwendungsbereich mehr verbleibt, ist § 100b StPO in Gänze für mit der Verfassung unvereinbar zu erklären. Die Gründe, die zur Verfassungswidrigkeit von § 100b StPO in der angegriffenen Fassung führen, treffen ebenso auf alle nachfolgenden Fassungen zu, die daher im Interesse der Rechtsklarheit auch für mit dem Grundgesetz unvereinbar zu erklären sind (vgl. Rn. 274). 276

3. Die Auslagenentscheidung beruht auf § 34a Abs. 2 BVerfGG. Eine Auslagenerstattung zugunsten des Beschwerdeführers zu 3) war nicht auszusprechen, weil dessen Verfassungsbeschwerde unzulässig ist (Rn. 105). 277

Harbarth Ott Christ

Radtke Härtel Wolff

Eifert Meßling