Formulierungshilfe der Bundesregierung für einen **15.05.2017**

Änderungsantrag

der Fraktionen CDU/CSU und SPD

zu dem Gesetzentwurf der Bundesregierung

– Drucksache 18/11272 –

Deutscher Bundestag
Ausschuss für
Recht und Verbraucherschutz

Ausschussdrucksache
18(6)334

15. Mai 2017

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

Artikel 1

Änderung der Strafprozessordnung

Die Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 3 Absatz 5 des Gesetzes vom 23. Dezember 2016 (BGBl. I S. 3346) geändert worden ist, wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

   a) Die Angabe zu § 100b wird wie folgt gefasst:

   „§ 100b Online-Durchsuchung“.

   b) Die Angaben zu den §§ 100d und 100e werden wie folgt gefasst:

   „§ 100d Kernbereich privater Lebensgestaltung; Zeugnisverweigerungsberechtigte

   § 100e Verfahren bei Maßnahmen nach den §§ 100a bis 100c“.

   c) Die Angabe zu § 101b wird wie folgt gefasst:

   „§ 101b Statistische Erfassung; Berichtspflichten“.

2. § 100a wird wie folgt geändert:

   a) Absatz 1 Satz 1 werden folgende Sätze angefügt:

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

   b) In Absatz 3 werden nach dem Wort „Anschluss“ die Wörter „oder ihr informationstechnisches System“ eingefügt.

c) Absatz 4 wird durch die folgenden Absätze 4 bis 6 ersetzt:

„(4) 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. Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, bestimmt sich nach dem Telekommunikationsgesetz und der Telekommunikations-Überwachungsverordnung. § 95 Absatz 2 gilt entsprechend.

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

1. ausschließlich überwacht und aufgezeichnet werden können:

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

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

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

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

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

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

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

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

3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und

4. die Organisationseinheit, die die Maßnahme durchführt.“

3. § 100b wird wie folgt gefasst:

„§ 100b

Online-Durchsuchung

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

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete besonders schwere Straftat begangen oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat,

2. die Tat auch im Einzelfall besonders schwer wiegt und

3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

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

1. aus dem Strafgesetzbuch:

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

b) Bildung krimineller Vereinigungen nach § 129 Absatz 1 in Verbindung mit Absatz 4 zweiter Halbsatz 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, §§ 239a, 239b und Menschenhandel nach § 232 Absatz 3, Zwangsprostitution und Zwangsarbeit nach § 232a Absatz 3, 4 oder 5 zweiter Halbsatz, § 232b Absatz 3 oder 4 in Verbindung mit § 232a Absatz 4 oder 5 zweiter Halbsatz und Ausbeutung unter Ausnutzung einer Freiheitsberaubung nach § 233a Absatz 3 oder 4 zweiter Halbsatz,

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

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

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

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

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

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

2. aus dem Asylgesetz:

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

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

3. aus dem Aufenthaltsgesetz:

a) Einschleusen von Ausländern nach § 96 Absatz 2,

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

4. aus dem Betäubungsmittelgesetz:

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

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

5. aus dem Gesetz über die Kontrolle von Kriegswaffen:

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

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

6. aus dem Völkerstrafgesetzbuch:

a) Völkermord nach § 6,

b) Verbrechen gegen die Menschlichkeit nach § 7,

c) Kriegsverbrechen nach den §§ 8 bis 12,

d) Verbrechen der Aggression nach § 13,

7. aus dem Waffengesetz:

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

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

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

1. der in der Anordnung nach § 100e Absatz 3 bezeichnete Beschuldigte informationstechnische Systeme der anderen Person benutzt, und

2. die Durchführung des Eingriffs in informationstechnische Systeme des Beschuldigten allein nicht zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes eines Mitbeschuldigten führen wird.

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

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

4. § 100c wird wie folgt geändert:

a) In Absatz 1 Nummer 1 wird nach den Wörtern „eine in“ die Angabe „§ 100b“ eingefügt.

b) Absatz 2 wird aufgehoben.

c) Absatz 3 wird Absatz 2 und in Satz 2 Nummer 1 die Angabe „§ 100d Abs. 2“ durch die Angabe „§ 100e Absatz 3“ ersetzt.

d) Die Absätze 4 bis 7 werden aufgehoben.

5. Die §§ 100d und 100e werden wie folgt gefasst:

„§ 100d

Kernbereich privater Lebensgestaltung; Zeugnisverweigerungsberechtigte

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

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

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

(4) Maßnahmen nach § 100c dürfen nur angeordnet werden, soweit auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass durch die Überwachung Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, nicht erfasst werden. Das Abhören und Aufzeichnen ist unverzüglich zu unterbrechen, wenn sich während der Überwachung Anhaltspunkte dafür ergeben, dass Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden. Ist eine Maßnahme unterbrochen worden, so darf sie unter den in Satz 1 genannten Voraussetzungen fortgeführt werden. Im Zweifel hat die Staatsanwaltschaft über die Unterbrechung oder Fortführung der Maßnahme unverzüglich eine Entscheidung des Gerichts herbeizuführen; § 100e Absatz 5 gilt entsprechend. Auch soweit für bereits erlangte Erkenntnisse ein Verwertungsverbot nach Absatz 2 in Betracht kommt, hat die Staatsanwaltschaft unverzüglich eine Entscheidung des Gerichts herbeizuführen. Absatz 3 Satz 4 gilt entsprechend.

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

§ 100e

Verfahren bei Maßnahmen nach den §§ 100a bis 100c

(1) Maßnahmen nach § 100a dürfen nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden. Bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft getroffen werden. Soweit die Anordnung der Staatsanwaltschaft nicht binnen drei Werktagen von dem Gericht bestätigt wird, tritt sie außer Kraft. Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei Monate ist zulässig, soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen.

(2) Maßnahmen nach den §§ 100b und 100c dürfen nur auf Antrag der Staatsanwaltschaft durch die in § 74a Absatz 4 des Gerichtsverfassungsgesetzes genannte Kammer des Landgerichts angeordnet werden, in dessen Bezirk die Staatsanwaltschaft ihren Sitz hat. Bei Gefahr im Verzug kann diese Anordnung auch durch den Vorsitzenden getroffen werden. Dessen Anordnung tritt außer Kraft, wenn sie nicht binnen drei Werktagen von der Strafkammer bestätigt wird. Die Anordnung ist auf höchstens einen Monat zu befristen. Eine Verlängerung um jeweils nicht mehr als einen Monat ist zulässig, soweit die Voraussetzungen unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen. Ist die Dauer der Anordnung auf insgesamt sechs Monate verlängert worden, so entscheidet über weitere Verlängerungen das Oberlandesgericht.

(3) Die Anordnung ergeht schriftlich. In ihrer Entscheidungsformel sind anzugeben:

1. soweit möglich, der Name und die Anschrift des Betroffenen, gegen den sich die Maßnahme richtet,

2. der Tatvorwurf, auf Grund dessen die Maßnahme angeordnet wird,

3. Art, Umfang, Dauer und Endzeitpunkt der Maßnahme,

4. die Art der durch die Maßnahme zu erhebenden Informationen und ihre Bedeutung für das Verfahren,

5. bei Maßnahmen nach § 100a die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgerätes, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist; im Fall des § 100a Absatz 1 Satz 2 und 3 eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das eingegriffen werden soll,

6. bei Maßnahmen nach § 100b eine möglichst genaue Bezeichnung des informationstechnischen Systems, aus dem Daten erhoben werden sollen,

7. bei Maßnahmen nach § 100c die zu überwachende Wohnung oder die zu überwachenden Wohnräume.

(4) In der Begründung der Anordnung oder Verlängerung von Maßnahmen nach den §§ 100a bis 100c sind deren Voraussetzungen und die wesentlichen Abwägungsgesichtspunkte darzulegen. Insbesondere sind einzelfallbezogen anzugeben:

1. die bestimmten Tatsachen, die den Verdacht begründen,

2. die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme,

3. bei Maßnahmen nach § 100c die tatsächlichen Anhaltspunkte im Sinne des § 100d Absatz 4 Satz 1.

(5) Liegen die Voraussetzungen der Anordnung nicht mehr vor, so sind die auf Grund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden. Das anordnende Gericht ist nach Beendigung der Maßnahme über deren Ergebnisse zu unterrichten. Bei Maßnahmen nach den §§ 100b und 100c ist das anordnende Gericht auch über den Verlauf zu unterrichten. Liegen die Voraussetzungen der Anordnung nicht mehr vor, so hat das Gericht den Abbruch der Maßnahme anzuordnen, sofern der Abbruch nicht bereits durch die Staatsanwaltschaft veranlasst wurde. Die Anordnung des Abbruchs einer Maßnahme nach den §§ 100b und 100c kann auch durch den Vorsitzenden erfolgen.

(6) Die durch Maßnahmen nach den §§ 100b und 100c erlangten und verwertbaren personenbezogenen Daten dürfen für andere Zwecke nach folgenden Maßgaben verwendet werden:

1. Die Daten dürfen in anderen Strafverfahren ohne Einwilligung der insoweit überwachten Personen nur zur Aufklärung einer Straftat, auf Grund derer Maßnahmen nach § 100b oder § 100c angeordnet werden könnten, oder zur Ermittlung des Aufenthalts der einer solchen Straftat beschuldigten Person verwendet werden.

2. Die Verwendung der Daten, auch solcher nach § 100d Absatz 5 Satz 1 Halbsatz 2, zu Zwecken der Gefahrenabwehr ist nur zur Abwehr einer im Einzelfall bestehenden Lebensgefahr oder einer dringenden Gefahr für Leib oder Freiheit einer Person, für die Sicherheit oder den Bestand des Staates oder für Gegenstände von bedeutendem Wert, die der Versorgung der Bevölkerung dienen, von kulturell herausragendem Wert oder in § 305 des Strafgesetzbuches genannt sind, zulässig. Die Daten dürfen auch zur Abwehr einer im Einzelfall bestehenden dringenden Gefahr für sonstige bedeutende Vermögenswerte verwendet werden. Sind die Daten zur Abwehr der Gefahr oder für eine vorgerichtliche oder gerichtliche Überprüfung der zur Gefahrenabwehr getroffenen Maßnahmen nicht mehr erforderlich, so

sind Aufzeichnungen über diese Daten von der für die Gefahrenabwehr zuständigen Stelle unverzüglich zu löschen. Die Löschung ist aktenkundig zu machen. Soweit die Löschung lediglich für eine etwaige vorgerichtliche oder gerichtliche Überprüfung zurückgestellt ist, dürfen die Daten nur für diesen Zweck verwendet werden; für eine Verwendung zu anderen Zwecken sind sie zu sperren.

3. Sind verwertbare personenbezogene Daten durch eine entsprechende polizeirechtliche Maßnahme erlangt worden, dürfen sie in einem Strafverfahren ohne Einwilligung der insoweit überwachten Personen nur zur Aufklärung einer Straftat, auf Grund derer die Maßnahmen nach § 100b oder § 100c angeordnet werden könnte, oder zur Ermittlung des Aufenthalts der einer solchen Straftat beschuldigten Person verwendet werden."

6. In § 100f Absatz 4 werden die Wörter „§ 100b Abs. 1, 4 Satz 1 und § 100d Abs. 2 gelten" durch die Angabe „§ 100e Absatz 1, 3, 5 Satz 1 gilt" ersetzt.

7. In § 100i Absatz 3 werden die Wörter „§ 100b Abs. 1 Satz 1 bis 3, Abs. 2 Satz 1 und Abs. 4 Satz 1" durch die Wörter „§ 100e Absatz 1 Satz 1 bis 3, Absatz 3 Satz 1 und Absatz 5 Satz 1" ersetzt.

8. § 101 wird wie folgt geändert:

   a) In Absatz 1 wird die Angabe „100a, 100c bis 100f" durch die Angabe „100a bis 100f" ersetzt.

   b) In Absatz 2 wird vor der Angabe „100c" die Angabe „100b" und ein Komma eingefügt.

   c) Absatz 4 Satz 1 wird wie folgt geändert:

      aa) Nach Nummer 3 wird folgende Nummer 4 eingefügt:

         „4. des § 100b die Zielperson sowie die erheblich mitbetroffenen Personen,".

      bb) Die bisherigen Nummern 4 bis 11 werden die Nummern 5 bis 12.

   d) In Absatz 6 Satz 5 werden die Wörter „Im Fall des § 100c" durch die Wörter „Bei Maßnahmen nach den §§ 100b und 100c" ersetzt.

9. § 101a Absatz 1 wird wie folgt geändert:

   a) Satz 1 wird wie folgt geändert:

      aa) In dem Satzteil vor Nummer 1 werden die Wörter „§ 100a Absatz 3 und § 100b Absatz 1 bis 4" durch die Wörter „§ 100a Absatz 3 und 4 und § 100e" ersetzt.

      bb) In Nummer 1 werden die Wörter „100b Absatz 2 Satz 2" durch die Wörter „100e Absatz 3 Satz 2" ersetzt.

      cc) In Nummer 2 werden die Wörter „100b Absatz 3 Satz 1" durch die Wörter „100a Absatz 4 Satz 1" ersetzt.

   b) In Satz 2 werden die Wörter „100b Absatz 1 Satz 2 und 3" durch die Wörter „100e Absatz 1 Satz 2".

   c) In Satz 3 werden die Wörter „100b Absatz 2 Satz 2 Nummer 2" durch die Wörter „100e Absatz 3 Satz 2 Nummer 5" ersetzt.

10. § 101b wird wie folgt gefasst:

„§ 101b

Statistische Erfassung; Berichtspflichten

(1) Die Länder und der Generalbundesanwalt berichten dem Bundesamt für Justiz kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres über in ihrem Zuständigkeitsbereich angeordnete Maßnahmen nach den §§ 100a, 100b, 100c und 100g. Das Bundesamt für Justiz erstellt eine Übersicht zu den im Berichtsjahr bundesweit angeordneten Maßnahmen und veröffentlicht diese im Internet. Über die im jeweils vorangegangenen Kalenderjahr nach § 100c angeordneten Maßnahmen berichtet die Bundesregierung dem Deutschen Bundestag vor der Veröffentlichung im Internet.

(2) In den Übersichten über Maßnahmen nach § 100a sind anzugeben:

1. die Anzahl der Verfahren, in denen Maßnahmen nach § 100a Absatz 1 angeordnet worden sind;

2. die Anzahl der Überwachungsanordnungen nach § 100a Absatz 1, unterschieden nach Erst- und Verlängerungsanordnungen;

3. die jeweils zugrunde liegende Anlassstraftat nach der Unterteilung in § 100a Absatz 2,

4. die Anzahl der Verfahren, in denen ein Eingriff in ein von dem Betroffenen genutztes informationstechnisches System nach § 100a Absatz 1 Satz 2 und 3

   a) im richterlichen Beschluss angeordnet wurde und

   b) tatsächlich durchgeführt wurde.

(3) In den Übersichten über Maßnahmen nach § 100b sind anzugeben:

1. die Anzahl der Verfahren, in denen Maßnahmen nach § 100b Absatz 1 angeordnet worden sind;

2. die Anzahl der Überwachungsanordnungen nach § 100b Absatz 1, unterschieden nach Erst- und Verlängerungsanordnungen;

3. die jeweils zugrunde liegende Anlassstraftat nach Maßgabe der Unterteilung in § 100b Absatz 2,

4. die Anzahl der Verfahren, in denen ein Eingriff in ein vom Betroffenen genutztes informationstechnisches System tatsächlich durchgeführt wurde.

(4) In den Berichten über Maßnahmen nach § 100c sind anzugeben:

1. die Anzahl der Verfahren, in denen Maßnahmen nach § 100c Absatz 1 angeordnet worden sind;

2. die jeweils zugrunde liegende Anlassstraftat nach Maßgabe der Unterteilung in § 100b Absatz 2;

3. ob das Verfahren einen Bezug zur Verfolgung organisierter Kriminalität aufweist;

4. die Anzahl der überwachten Objekte je Verfahren nach Privatwohnungen und sonstigen Wohnungen sowie nach Wohnungen des Beschuldigten und Wohnungen dritter Personen;

5. die Anzahl der überwachten Personen je Verfahren nach Beschuldigten und nichtbeschuldigten Personen;

6. die Dauer der einzelnen Überwachung nach Dauer der Anordnung, Dauer der Verlängerung und Abhördauer;

7. wie häufig eine Maßnahme nach § 100d Absatz 4, § 100e Absatz 5 unterbrochen oder abgebrochen worden ist;

8. ob eine Benachrichtigung der Betroffenen (§ 101 Absatz 4 bis 6) erfolgt ist oder aus welchen Gründen von einer Benachrichtigung abgesehen worden ist;

9. ob die Überwachung Ergebnisse erbracht hat, die für das Verfahren relevant sind oder voraussichtlich relevant sein werden;

10. ob die Überwachung Ergebnisse erbracht hat, die für andere Strafverfahren relevant sind oder voraussichtlich relevant sein werden;

11. wenn die Überwachung keine relevanten Ergebnisse erbracht hat: die Gründe hierfür, differenziert nach technischen Gründen und sonstigen Gründen;

12. die Kosten der Maßnahme, differenziert nach Kosten für Übersetzungsdienste und sonstigen Kosten.

(5) In den Übersichten über Maßnahmen nach § 100g sind anzugeben:

1. unterschieden nach Maßnahmen nach § 100g Absatz 1, 2 und 3

   a) die Anzahl der Verfahren, in denen diese Maßnahmen durchgeführt wurden;

   b) die Anzahl der Erstanordnungen, mit denen diese Maßnahmen angeordnet wurden;

   c) die Anzahl der Verlängerungsanordnungen, mit denen diese Maßnahmen angeordnet wurden;

2. untergliedert nach der Anzahl der zurückliegenden Wochen, für die die Erhebung von Verkehrsdaten angeordnet wurde, jeweils bemessen ab dem Zeitpunkt der Anordnung

   a) die Anzahl der Anordnungen nach § 100g Absatz 1;

   b) die Anzahl der Anordnungen nach § 100g Absatz 2;

   c) die Anzahl der Anordnungen nach § 100g Absatz 3;

   d) die Anzahl der Anordnungen, die teilweise ergebnislos geblieben sind, weil die abgefragten Daten teilweise nicht verfügbar waren;

   e) die Anzahl der Anordnungen, die ergebnislos geblieben sind, weil keine Daten verfügbar waren.“

11. In § 160a Absatz 5 wird die Angabe „100c Absatz 6“ durch die Angabe „100d Absatz 5“ ersetzt.

12. In § 161 Absatz 2 Satz 2 wird die Angabe „§ 100d Abs. 5 Nr. 3“ durch die Wörter „§ 100e Absatz 6 Nummer 3“ ersetzt.

13. In § 163d Absatz 2 Satz 3 wird die Angabe „§ 100b Abs. 1 Satz 3“ durch die Wörter „§ 100e Absatz 1 Satz 3“ ersetzt.

14. In § 163e Absatz 4 Satz 4 wird die Angabe „§ 100b Abs. 1 Satz 3“ durch die Wörter „§ 100e Absatz 1 Satz 3“ ersetzt.

15. In § 163f Absatz 3 Satz 3 werden die Wörter „§ 100b Abs. 1 Satz 4 und 5, Abs. 2 Satz 1“ durch die Wörter „§ 100e Absatz 1 Satz 4 und 5, Absatz 3 Satz 1“ ersetzt.

16. In § 477 Absatz 2 Satz 4 wird die Angabe „§ 100d Abs. 5“ durch die Angabe „§ 100e Absatz 6“ ersetzt.

Artikel 2

Änderung des Einführungsgesetzes zur Strafprozessordnung

Dem Einführungsgesetz zur Strafprozessordnung in der im Bundesgesetzblatt Teil III, Gliederungsnummer 312-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 3 des Gesetzes vom 8. Juli 2016 (BGBl. I S. 1610) geändert worden ist, wird folgender § …[einsetzen: nächste bei der Verkündigung freie Zählbezeichnung] angefügt:

„§ …[einsetzen: nächste bei der Verkündigung freie Zählbezeichnung]

Übergangsregelung zum Gesetz […]“

„Die Übersichten nach § 101b der Strafprozessordnung sind erstmalig für das Berichtsjahr … [einsetzen: Jahreszahl des zweiten auf die Verkündung folgenden Kalenderjahres] zu erstellen. Für die vorangehenden Berichtsjahre sind § 100b Absatz 6, § 100e Absatz 2 und § 101b Nummer 2 der Strafprozessordnung in der bis zum …[einsetzen: Datum des Inkrafttretens nach Artikel 10 dieses Gesetzes] geltenden Fassung weiter anzuwenden.“

Artikel 3

Änderung des Antiterrordateigesetzes

In § 4 Absatz 3 Satz 1 Nummer 2 des Antiterrordateigesetzes vom 22. Dezember 2006 (BGBl. I S. 3409), das zuletzt durch Artikel 1 des Gesetzes vom 18. Dezember 2014 (BGBl. I S. 2318; 2016 I 48) geändert worden ist, wird die Angabe „§ 100c“ durch die Wörter den „§§ 100b und 100c“ ersetzt.

Artikel 4

Änderung des Rechtsextremismus-Datei-Gesetzes

In § 4 Absatz 3 Satz 1 Nummer 2 des Rechtsextremismus-Datei-Gesetzes vom 20. August 2012 (BGBl. I S. 1798), das durch Artikel 2 des Gesetzes vom 18. Dezember 2014 (BGBl. I S. 2318; 2016 I 48) geändert worden ist, wird die Angabe „§ 100c“ durch die Wörter „den §§ 100b und 100c“ ersetzt.

Artikel 5

Änderung des Artikel 10-Gesetzes

In § 17 Absatz 1 des Artikel 10-Gesetzes vom 26. Juni 2001 (BGBl. I S. 1254, 2298), das zuletzt durch Artikel 3 Absatz 3 des Gesetzes vom 23. Dezember 2016 (BGBl. I S. 3346) geändert worden ist, wird die Angabe „100b“ durch die Angabe „100e“ ersetzt.

Artikel 6

Änderungen des Gerichtsverfassungsgesetzes

Das Gerichtsverfassungsgesetz in der Fassung der Bekanntmachung vom 9. Mai 1975 (BGBl. I S. 1077), das zuletzt durch Artikel 2 Absatz 2 des Gesetzes vom 22. Dezember 2016 (BGBl. I S. 3150) geändert worden ist, wird wie folgt geändert:

1. In § 74a Absatz 4 wird die Angabe „§ 100c“ durch die Wörter „den §§ 100b und 100c“ ersetzt.

2. In § 120 Absatz 4 Satz 2 wird die Angabe „§ 100d Abs. 1 Satz 6“ durch die Wörter „§ 100e Absatz 2 Satz 6“ ersetzt.

Artikel 7

Änderungen des IStGH-Gesetzes

In § 59 Absatz 2 IStGH-Gesetz vom 21. Juni 2002 (BGBl. I S. 2144), das zuletzt durch Artikel 15 Absatz 4 des Gesetzes vom 21. November 2016 (BGBl. I S. 2591) geändert worden ist, wird die Angabe „§§ 100c, 100f“ durch die Wörter „§§ 100b, 100c und 100f“ ersetzt.

Artikel 8

Änderung des Wertpapierhandelsgesetzes

In § 4 Absatz 3c Satz 2 des Wertpapierhandelsgesetzes in der Fassung der Bekanntmachung vom 9. September 1998 (BGBl. I S. 2708), das zuletzt durch Artikel 2 des Gesetzes vom 30. Juni 2016 (BGBl. I S. 1514) geändert worden ist, werden die Wörter „§ 100a Absatz 3 und § 100b Absatz 1 bis 4 Satz 1“ durch die Angabe „§ 100a Absatz 3 und 4, § 100e Absatz 1 und 3 sowie 5 Satz 1“ ersetzt.

Artikel 9

Änderung des Strafgesetzbuchs

In § 129 Absatz 4 des Strafgesetzbuchs in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 2 Absatz 4 des Gesetzes vom 22. Dezember 2016 (BGBl. I S. 3150) geändert worden ist, wird die Angabe „100c“ durch „100b“ ersetzt.

Artikel 10

Änderungen des Zollfahndungsdienstgesetzes

Das Zollfahndungsdienstgesetz vom 16. August 2002 (BGBl. I S. 3202), das zuletzt durch Artikel 2 Absatz 5 des Gesetzes vom 22. Dezember 2016 (BGBl. I S. 3150) geändert worden ist, wird wie folgt geändert:

1. In § 22a Absatz 3 Nummer 2 wird in dem Satzteil vor Satz 2 die Angabe „100c“ durch die Angabe „100b Absatz 2“ ersetzt.

2. In § 32a Absatz 3 Nummer 2 wird in dem Satzteil vor Satz 2 die Angabe „100c“ durch die Angabe „100b Absatz 2“ ersetzt.

Artikel 11

Änderungen der Telekommunikations-Überwachungsverordnung

Die Telekommunikations-Überwachungsverordnung vom 3. November 2005 (BGBl. I S. 3136), die zuletzt durch Artikel 4 des Gesetzes vom 25. Dezember 2008 (BGBl. I S. 3083) geändert worden ist, wird wie folgt geändert:

1. In § 1 Nummer 1 Buchstabe a wird die Angabe „100b“ durch die Angabe „100e“ ersetzt.

2. § 2 wird wie folgt geändert:

   a) In Nummer 1 wird die Angabe „100b“ durch die Angabe „100e“ ersetzt.

b) In Nummer 3 wird die Angabe „§ 100b Abs. 3 Satz 1“ durch die Wörter „§ 100a Absatz 4 Satz 1“ ersetzt.

c) In Nummer 15 wird die Angabe „100b“ durch die Angabe „100e“ ersetzt.

3. In der Überschrift des Teils 2 wird die Angabe „100b“ durch die Angabe „100e“ ersetzt.

4. In § 3 Absatz 2 Satz 4 wird die Angabe „§ 100b Abs. 3 Satz 1“ durch die Wörter „§ 100a Absatz 4 Satz 1“ ersetzt.

5. In § 5 Absatz 1 wird die Angabe „100b“ durch die Angabe „100e“ ersetzt.

Artikel 12

Einschränkung eines Grundrechts

Durch Artikel 1 Nummer 2 wird das Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) eingeschränkt.

Artikel 13

Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Begründung

A. Allgemeiner Teil

Die fortschreitende Entwicklung der Informationstechnik hat dazu geführt, dass informationstechnische Systeme allgegenwärtig sind und ihre Nutzung für die Lebensführung der meisten Bürgerinnen und Bürger von zentraler Bedeutung ist. Dies gilt vor allem für die Nutzung mobiler Geräte in Form von Smartphones oder Tablet-PCs. Die Leistungsfähigkeit derartiger Geräte ist dabei 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 handelt. Die Nutzung dieser mobilen Geräte ersetzt zunehmend die herkömmlichen Formen der Telekommunikation. Das Internet als komplexer Verbund von Rechnernetzen öffnet dem Nutzer eines angeschlossenen Systems nicht nur den Zugriff auf eine praktisch unübersehbare Fülle von Informationen, die von anderen Netzrechnern zum Abruf bereitgehalten werden. Es stellt ihm daneben zahlreiche neuartige Kommunikationsdienste zur Verfügung, mit deren Hilfe er über das Internet aktiv soziale Verbindungen aufbauen und pflegen kann, ohne herkömmliche Formen der Telekommunikation in Anspruch nehmen zu müssen. Zudem führen technische Konvergenzeffekte dazu, dass auch herkömmliche Formen der Fernkommunikation in weitem Umfang auf das Internet verlagert werden können (vgl. dazu schon das Bundesverfassungsgericht (BVerfG), Urteil vom 27. Februar 2008 – 1 BvR 370/07, Rn. 171 ff.).

Die weite Verbreitung informationstechnischer Systeme führt dazu, dass sie auch eine wichtige Rolle spielen, wenn es um die Verhinderung und um die Aufklärung von Straftaten geht. Im Bereich der Gefahrenabwehr wird den Polizeibehörden schon seit längerer Zeit ausdrücklich die Möglichkeit eingeräumt, schwere Gefahren durch den Einsatz von Überwachungstechniken abzuwehren. Im Bereich der Strafverfolgung ist umstritten, inwieweit die Überwachung insbesondere verschlüsselter Kommunikation über das Internet zulässig ist. Die Möglichkeit eines verdeckten Eingriffs in informationstechnische Systeme zum Zweck ihrer Durchsuchung besteht bislang für die Strafverfolgungsbehörden nicht.

Mit den vorgeschlagenen Änderungen werden Rechtsgrundlagen für die Quellen-Telekommunikationsüberwachung und die Online-Durchsuchung und in der Strafprozessordnung geschaffen.

Als Online-Durchsuchung wird der verdeckte staatliche Zugriff auf fremde informationstechnische Systeme über Kommunikationsnetze mittels einer Überwachungssoftware bezeichnet. Bei der Quellen-Telekommunikationsüberwachung wird ebenfalls ein fremdes informationstechnisches System infiltriert, um mit einer eigens für diesen Zweck entwickelten Überwachungssoftware die Kommunikation zwischen den Beteiligten überwachen und aufzeichnen zu können. Dies geschieht aus technischen Gründen, weil die Kommunikation nach dem geltenden Recht zwar im öffentlichen Telekommunikationsnetz ausgeleitet werden könnte, den Ermittlungsbehörden dann aber nur in verschlüsselter Form vorliegen würde. Die Entschlüsselung ist entweder extrem zeitaufwändig oder sogar gänzlich ausgeschlossen.

Beide Maßnahmen sind nach der Rechtsprechung des Bundesverfassungsgerichts grundsätzlich zulässig (vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, Rn. 1 ff.).

Angesichts der mit diesen Maßnahmen verbundenen spezifischen Grundrechtseingriffe sind an deren Rechtfertigung insbesondere mit Blick auf die Verhältnismäßigkeit allerdings hohe Anforderungen zu stellen, die das Bundesverfassungsgericht in der genannten Entscheidung im Einzelnen dargelegt hat. Je tiefer Überwachungsmaßnahmen in das Privatleben hineinreichen und mit berechtigten Vertraulichkeitserwartungen kollidieren, desto

strenger sind diese Anforderungen; der absolute Kernbereich der Persönlichkeit darf nicht ausgeforscht werden. Besonders tief in die Privatsphäre dringen nach der Rechtsprechung des Bundesverfassungsgerichts die Wohnraumüberwachung sowie der Zugriff auf informationstechnische Systeme (BVerfG a.a.O., Rn. 104).

Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung gehört die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen (vgl. BVerfGE 109, 279, 313; 120, 274, 335; ständige Rechtsprechung). Geschützt ist insbesondere die nichtöffentliche Kommunikation mit Personen des höchstpersönlichen Vertrauens, die in der berechtigten Annahme geführt wird, nicht überwacht zu werden, wie es insbesondere bei Gesprächen im Bereich der Wohnung der Fall ist. Zu diesen Personen gehören Ehe- oder Lebenspartner, Geschwister und Verwandte in gerader Linie, vor allem, wenn sie im selben Haushalt leben, und können Strafverteidiger, Ärzte, Geistliche und enge persönliche Freunde zählen (vgl. BVerfGE 109, 279, 321 ff.). Dieser Kreis deckt sich nur teilweise mit dem der Zeugnisverweigerungsberechtigten. Solche Gespräche verlieren dabei nicht schon dadurch ihren Charakter als insgesamt höchstpersönlich, dass sich in ihnen Höchstpersönliches und Alltägliches vermischen (vgl. BVerfGE 109, 279, 330; 113, 348, 391 f.).

Weil vor und während der Durchführung die Transparenz der Datenerhebung und -verarbeitung sowie individueller Rechtsschutz bei heimlichen Überwachungsmaßnahmen nur sehr eingeschränkt sichergestellt werden können, ist es umso wichtiger, eine effektive Kontrolle und Aufsicht im Nachhinein zu gewährleisten. Der Verhältnismäßigkeitsgrundsatz stellt für tief in die Privatsphäre reichende Überwachungsmaßnahmen deshalb an eine wirksame Ausgestaltung dieser Kontrolle sowohl auf der Ebene des Gesetzes als auch der Verwaltungspraxis gesteigerte Anforderungen (vgl. BVerfG, Urteil vom 24. April 2013 – 1 BvR 1215/07 – Rn. 214). Zur Gewährleistung von Transparenz und Kontrolle bedarf es schließlich einer gesetzlichen Regelung von Berichtspflichten (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 – Rn. 142 ff.).

Bei der heimlichen Infiltration eines informationstechnischen Systems im Rahmen einer Online-Durchsuchung können die Nutzung des Systems umfassend überwacht und seine Speichermedien ausgelesen werden. Dies stellt einen Eingriff in das allgemeine Persönlichkeitsrecht nach Artikel 2 Absatz 1 i.V.m. Artikel 1 Absatz 1 des Grundgesetzes (GG) in seiner eigenständigen Ausprägung als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme dar (vgl. BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 – Rn. 201). Für den präventiven Bereich hat das Bundesverfassungsgericht festgelegt, dass Eingriffe in den Schutzbereich dieses Grundrechts nur dann erfolgen dürfen, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Von seinem Intensitätsgrad und wegen der oft höchstpersönlichen Natur der auf einem informationstechnischen System gespeicherten Daten vergleicht es den Eingriff seinem Gewicht nach mit dem (heimlichen) Eingriff in die Unverletzlichkeit der Wohnung (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 – Rn. 210 a.E.). Der Grundrechtsschutz ist dementsprechend auch durch geeignete Verfahrensvorkehrungen abzusichern: Die heimliche Infiltration eines informationstechnischen Systems ist unter den Vorbehalt richterlicher Anordnung zu stellen. Das Gesetz, das zu einem solchen Eingriff ermächtigt, muss Vorkehrungen enthalten, um den Kernbereich privater Lebensgestaltung zu schützen. Zudem sind flankierende Vorschriften über die Verwendung und Löschung der mittels einer Online-Durchsuchung erlangten Informationen erforderlich.

Werden im Zuge einer heimlichen Infiltration eines informationstechnischen Systems hingegen lediglich laufende Telekommunikationsvorgänge überwacht und aufgezeichnet, ist in erster Linie der Schutzbereich des Fernmeldegeheimnisses nach Artikel 10 Absatz 1 GG betroffen. Zur Abgrenzung führt das Bundesverfassungsgericht aus, dass ein Eingriff in das aus dem allgemeinen Persönlichkeitsrecht nach Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG hergeleitete Grundrecht auf Gewährleistung der Vertraulichkeit und In-

tegrität informationstechnischer Systeme vorliege, wenn mit der Infiltration des informationstechnischen Systems die entscheidende Hürde genommen sei, um das System – etwa im Sinne einer Online-Durchsuchung – insgesamt auszuspähen (vgl. BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 – Rn. 188). Artikel 10 Absatz 1 GG sei hingegen der alleinige grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zu einer "Quellen-Telekommunikationsüberwachung", wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt. Dies müsse indes durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein (vgl. BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 – Rn. 190).

Das Bundesverfassungsgericht hat die genannten Maßstäbe im Bereich des Rechts der Nachrichtendienste und der Gefahrenabwehr entwickelt. Nichtsdestoweniger müssen sie auch im Bereich der Strafverfolgung berücksichtigt werden, wobei einzelne Elemente wegen der unterschiedlichen Natur der jeweiligen Eingriffe modifiziert werden müssen. Der Vorschlag zur künftigen Ausgestaltung der Strafprozessordnung enthält daher zunächst eine Erweiterung des § 100a StPO auf die Fälle der Quellen-Telekommunikationsüberwachung, und zwar unter Einbeziehung der über Messenger-Dienste versandten Kommunikationsinhalte, soweit sie funktionale Äquivalente zu laufender Kommunikation mittels SMS darstellen. Die Rechtsgrundlage für die Online-Durchsuchung ist in § 100b StPO-E vor der vergleichbar grundrechtsintensiven Regelung zur Wohnraumüberwachung in § 100c in der Entwurfsfassung (StPO-E), verortet.

Regelungssystematisch soll § 100a StPO-E überwiegend Eingriffe in Artikel 10 GG und ergänzend in Artikel 2 Absatz 1 i.V.m. 1 Absatz 1 GG erfassen, die Regelung zur Online-Durchsuchung in § 100b StPO-E überwiegend Eingriffe in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nach Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG rechtfertigen und die Regelung des § 100c wie bisher als Ermächtigungsgrundlage für Eingriffe in die Unverletzlichkeit der Wohnung gemäß Artikel 13 GG dienen. Das Vorhaben wird darüber hinaus zum Anlass genommen, die Vorschriften zum Schutz des Kernbereichs privater Lebensgestaltung und der Zeugnisverweigerungsberechtigten in eine Vorschrift zusammenzuführen und klarer zu fassen. Die Verfahrensvorschriften werden ebenfalls zusammengefasst, wobei die für die Wohnraumüberwachung geltenden hohen Anforderungen auf die Online-Durchsuchung erstreckt werden. Schließlich werden die Verwendungs- und Löschungsregelungen sowie die statistische Erfassung und die Berichtspflichten angepasst.

B. Besonderer Teil

Zu Artikel 1 (Änderung der Strafprozessordnung)

Zu Nummer 1

Die Inhaltsübersicht mit Paragraphenbezeichnung in der Strafprozessordnung wird an die Änderungen angepasst.

Zu Nummer 2

Mit den vorgeschlagenen Änderungen wird eine Rechtsgrundlage für die Quellen-Telekommunikationsüberwachung geschaffen.

Die Regelung des § 100a StPO enthält derzeit unstreitig eine Rechtsgrundlage zur Erhebung derjenigen Kommunikationsinhalte, die während der Übertragung von einem Kommunikationsteilnehmer zu einem anderen während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz überwacht und aufgezeichnet werden können. Die Überwachung und Aufzeichnung erfolgt hier nicht bei den Kommunikationsteilnehmern

selbst, sondern über Dritte, in der Regel bei den Telekommunikationsunternehmen. Die Anbieter öffentlich zugänglicher Telekommunikationsdienste sind nach den geltenden Regelungen in der Strafprozessordnung, dem Telekommunikationsgesetz (TKG) und der Telekommunikationsüberwachungs-Verordnung (TKÜV) verpflichtet, Maßnahmen der Telekommunikationsüberwachung zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen.

Nachdem inzwischen ein Großteil der Kommunikation Internetprotokoll-(IP)-basiert erfolgt und zahlreiche „Voice-over-IP“ (VoIP)- und Messenger-Dienste die Kommunikationsinhalte mit einer Verschlüsselung versehen, werden den Ermittlungsbehörden bei der Überwachung und Aufzeichnung im öffentlichen Telekommunikationsnetz oft nur verschlüsselte Daten geliefert. Deren Entschlüsselung ist entweder derzeit gar nicht möglich, oder aber langwierig und kostenintensiv. Eine Verpflichtung der Anbieter öffentlich zugänglicher Telekommunikationsdienste zur Herausgabe der automatisch generierten, temporären Schlüssel bzw. die Implementierung sogenannter Hintertüren für Behörden bereits in den Programmen durch deren Anbieter (back doors) ist derzeit nicht denkbar. Nach den Grundsätzen der von der Bundesregierung verfolgten Kryptopolitik wird im Gegenteil aus Gründen des Schutzes vertraulicher Daten vor den Zugriffen Dritter sogar eine Stärkung der Verschlüsselungstechnologien und deren häufige Anwendung befürwortet. Dem gegenüber steht das Gebot effektiver Strafverfolgung, die ohne Telekommunikationsüberwachung in den vom Gesetz genannten Katalogtaten nicht mehr gewährleistet ist. Eine effektive, am Gebot der Rechtsstaatlichkeit ausgerichtete und der Notwendigkeit des Datenschutzes angemessen Rechnung tragende Strafverfolgung muss sich diesen technischen Veränderungen stellen und ihre Ermittlungsmaßnahmen dem technischen Fortschritt anpassen. Soll die Überwachung und Aufzeichnung von Kommunikationsinhalten im Rahmen der Strafverfolgung wie bisher bei schweren Straftaten möglich sein, kommt daher nur ein Ausleiten der Kommunikation „an der Quelle“ in Betracht, d.h. noch vor deren Verschlüsselung auf dem Absendersystem oder nach deren Entschlüsselung beim Empfänger. Technisch kann die Ausleitung der Kommunikation vor der Verschlüsselung über eine spezielle Software erfolgen, die auf dem Endgerät des Betroffenen verdeckt installiert wird.

Ob das Überwachen und Aufzeichnen der Kommunikation am Endgerät des Betroffenen vor dem Hintergrund der Rechtsprechung des Bundesverfassungsgerichts bereits jetzt auf § 100a StPO gestützt werden kann, ist umstritten. In der Rechtsprechung der Instanzgerichte und Teilen der Literatur wurde die Auffassung vertreten, dass die Quellen-Telekommunikationsüberwachung auf der Grundlage der geltenden Fassung der §§ 100a, 100b StPO möglich sei, wenn eine Beschränkung auf ausschließlich für die Überwachung der Telekommunikation notwendige Eingriffe in das Endgerät erfolge (LG Landshut, Beschluss vom 20.01.2011 – 4 Qs 346/10, MMR 2011, 690 f. m. zust. Anm. Bär; LG Hamburg, Beschluss vom 13.09.2010 – 608 Qs 17/10, MMR 2011, 693 ff.; AG Bayreuth, Beschluss vom 17.09.2009 – Gs 911/09, MMR 2010, 266 f.; Bär, in: KMR/StPO, § 100a Rn. 31a; Schmitt, in: Meyer-Goßner/Schmitt, Strafprozessordnung, 58. Aufl. 2015, § 100a Rn. 7b; Bruns, in: Karlsruher Kommentar zur Strafprozessordnung, 7. Aufl. 2013, § 100a Rn. 27 f.; Graf, in: Beck‘scher Online-Kommentar zur Strafprozessordnung, 2015, § 100a Rn. 107c). Hiergegen wurde allerdings eingewandt, dass mit der verdeckten Installation einer Software zur Ausleitung der laufenden Kommunikation zwangsläufig ein Eingriff in die Integrität des Zielsystems vorliege. Der Eingriff wiege im Gegensatz zur herkömmlichen Telefonüberwachung beim Telekommunikationsanbieter schon deshalb qualitativ schwerer und erfordere eine eigene Ermächtigungsgrundlage (Becker/Meinicke StV 2011, 50, 51; Beukelmann NJW 2012, 2617, 2620 f.; Brodowski JR 2011, 533, 535 ff.; Gercke GA 2012, 474, 488; Klesczewski ZStW 123 (2011), 737, 743 f.; Popp ZD 2012, 51, 54; Sankol CR 2008, 13, 14 ff.; Skistims/Roßnagel ZD 2012, 3, 6; Singelnstein NStZ 2012, 593, 599; Stadler MMR 2012, 18, 20; Wolter/Greco, in: Systematischer Kommentar zur Strafprozessordnung, 5. Aufl. 2016, § 100a Rn. 27 ff.). Auch seien die technischen Vorkehrungen, unter denen die Quellen-Telekommunikationsüberwachung rechtlich zulässig sei, für Maßnahmen zum Zwecke

der Strafverfolgung keineswegs eindeutig im Gesetz klargestellt (Buermeyer, StV 2013, 470, 472; Popp, ZD 2012, 51, 53; Singelnstein, NStZ 2012, 593, 599).

Mit den vorgeschlagenen Änderungen wird ausdrücklich festgelegt, dass Telekommunikationsinhalte auch auf dem Endgerät des Betroffenen überwacht und aufgezeichnet werden dürfen. Dabei muss den Anforderungen des Bundesverfassungsgerichts entsprechend technisch sichergestellt sein, dass nur solche Kommunikationsinhalte erfasst werden, die auch auf herkömmlichem Wege ausgeleitet werden können. Innerhalb dieses Rahmens stellt § 100a StPO-E je nach Kommunikationsform sowohl eine Ermächtigungsgrundlage für Eingriffe in Artikel 10 Absatz 1 GG (verschlüsselte Sprach- und Videotelefonie) als auch für Eingriffe in Artikel 2 Absatz 1 i.V.m. 1 Absatz 1 GG (verschlüsselte Nachrichten über Messenger-Dienste) dar.

Der Schutzbereich des Artikel 10 Absatz 1 GG ist in zweifacher Hinsicht begrenzt. Zum einen ist in funktionaler Hinsicht mit Blick auf den Gegenstand der Überwachung Artikel 10 GG der alleinige grundrechtliche Maßstab, wenn sich die Überwachung mittels einer Infiltration des Endgeräts auf Kommunikationsinhalte aus einem laufenden Telekommunikationsvorgang beschränkt und eine Gefahr der Ausspähung des gesamten übrigen Systems nicht vorliegt. Zum anderen wird der Schutzbereich des Artikel 10 GG vom Schutzbereich des Art. 2 Absatz 1 i.V.m. 1 Absatz 1 GG nach „Herrschaftssphären“ abgegrenzt. Wird die Kommunikation zeitlich während des Übertragungsvorgangs überwacht, ist der Schutzbereich des Artikel 10 GG, vor Beginn und nach Abschluss des Übertragungsvorgangs hingegen der Schutzbereich des Artikel 2 Absatz 1 i.V.m. 1 Absatz 1 GG betroffen. Der Schutz des Fernmeldegeheimnisses endet in dem Moment, in dem die Nachricht beim Empfänger angekommen und der Übertragungsvorgang beendet ist.

Je nach Kommunikationsform sind bei einer Überwachung und Aufzeichnung auf dem Endgerät folglich unterschiedliche Schutzbereiche betroffen. Bei der Überwachung und Aufzeichnung von Sprach- und Videotelefonie fallen die Ausleitung durch die Software und die Übertragung der Kommunikation zeitlich regelmäßig zusammen. Die Ausleitung erfolgt daher noch „während der Übertragung“ und nicht nach Beendigung des Übertragungsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers. Anders liegt es bei der Beschlagnahme von E-Mails. Sind diese auf dem Server eines Host-Providers (z.B. Googlemail, GMX, web.de) end- oder zwischengespeichert, ist bei einem Eingriff dort der Schutzbereich des Artikels 10 GG eröffnet. Ist die E-Mail dagegen auf dem Endgerät des Betroffenen angekommen und in seinem Mailprogramm (z.B. Outlook) gespeichert, befindet sie sich in seinem Herrschaftsbereich. Weil der Übertragungsvorgang unmittelbar mit der Ankunft der E-Mail auf dem Endgerät abgeschlossen ist, unterliegt ein Ausleiten dieser Kommunikation aus einem informationstechnischem System des Betroffenen nicht mehr dem Fernmeldegeheimnis (BVerfG, Beschluss vom 16. Juni 2009 – 2 BvR 902/06 – Rn. 45). Textnachrichten und sonstige Botschaften, die über Messenger-Dienste versandt werden, enthalten ebenso wie Sprach- und Videotelefonate Kommunikationsinhalte, die IP-basiert und in der Regel verschlüsselt über das Datennetz übertragen werden können. Sie werden heute häufig als funktionales Äquivalent zu SMS-Nachrichten verwendet um Texte, Bilder oder andere Inhalte (auch aufgezeichnete Sprachnachrichten) an Kommunikationspartner zu übermitteln. Anders als bei der Sprach- und Videotelefonie in Echtzeit ist jedoch der Übertragungsvorgang mit dem Zugang der Nachricht auf dem Endgerät des Betroffenen abgeschlossen. Wie bei E-Mails ist die Nachricht im Herrschaftsbereich des Betroffenen angekommen und der Schutzbereich des Persönlichkeitsrechts eröffnet.

Soweit daher über Messenger-Dienste versandte Nachrichten auf dem Endgerät mittels einer speziell dazu entwickelten Software ausgelesen werden sollen, liegt keine unmittelbar am Maßstab des Artikels 10 GG zu messende „laufende Telekommunikation“ vor. Vielmehr erfolgt ein Eingriff in das Grundrecht aus Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 GG in seiner Ausprägung als Grundrecht auf informationelle Selbstbestimmung oder als Grundrecht in die Integrität und Vertraulichkeit eigener informationstechnischer Systeme.

Soweit das Bundesverfassungsgericht höhere Anforderungen an die Rechtfertigung von Eingriffen in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gestellt hat, betrafen diese nicht den Fall, dass die Überwachung und Aufzeichnung auf neu ankommende oder abgesendete Messenger-Nachrichten auf dem Endgerät begrenzt und technisch ausgeschlossen wird, dass die Gefahr des Auslesens des gesamten Systems oder auch nur der gesamten gespeicherten Kommunikation nicht besteht. In diesem Fall weist der Eingriff eine erheblich geringere Intensität und Reichweite auf, erfasst keine nur dem Betroffenen (und nicht auch Kommunikationspartnern) bekannten Inhalte und geht nicht über das hinaus, was die Strafverfolgungsbehörden mit einer herkömmlichen Telefonüberwachung ermittelt haben würden, wenn der Betroffene diesen Kommunikationsweg gewählt hätte. Dann erscheint es verfassungsrechtlich nicht geboten, die wegen der besonderen Sensibilität informationstechnischer Systeme für die Ermittlung von Persönlichkeitsprofilen des Betroffenen liegenden Gefährdung aufgestellten höheren Anforderungen des Bundesverfassungsgerichts anzuwenden. Hinreichend, aber notwendig erweisen sich vielmehr die ebenfalls strengen Anforderungen, die aus Artikel 10 GG für die Telefonüberwachung folgen.

Der Entwurf sieht deshalb in mehrfacher Hinsicht enge Begrenzungen der Quellen-Telekommunikationsüberwachung vor. Gespeicherte Nachrichten dürfen nicht erhoben werden, wenn sie nicht mehr als aktuelle Kommunikation im Zeitraum nach Ergehen der Anordnung (vgl. dazu sogleich) gelten können. Ebenso wie bei der Sprach- und Videotelefonie darf das Ausleiten von Messenger-Nachrichten am Endgerät nur dann erfolgen, wenn dies ein funktionales Äquivalent zur Überwachung und Ausleitung der Nachrichten aus dem Telekommunikationsnetz darstellt. Die vorgeschlagenen Änderungen setzen folglich ausschließlich das Ziel um, den technischen Entwicklungen der Informationstechnik Rechnung zu tragen und – ohne Zugriff auf weitere gespeicherte Inhalte des informationstechnischen Systems – eine Telekommunikationsüberwachung auch dort zu ermöglichen, wo dies mittels der alten Überwachungstechnik nicht mehr möglich ist.

Um die funktionale Äquivalenz auch in zeitlicher Hinsicht zu gewährleisten, ist technisch sicherzustellen, dass über Messenger-Dienste versandte Nachrichten erst ab dem Zeitpunkt der Anordnung durch das Gericht bzw. – in Eilfällen – der Staatsanwaltschaft ausgeleitet werden dürfen. Auch im Rahmen der herkömmlichen Telekommunikationsüberwachung können Kommunikationsinhalte erst von diesem Zeitpunkt an ausgeleitet werden. Auf dem Endgerät eines Kommunikationsinhabers sind jedoch unter Umständen auch Nachrichten gespeichert, die sich auf Zeiträume vor der Anordnung erstrecken. Die einzusetzende Software muss daher so programmiert sein, dass sie anhand der zu den einzelnen Nachrichten hinterlegten Meta-Daten, die etwa die Absende-, Empfangs- und Lesezeitpunkte enthalten, die ein- und ausgehenden Nachrichten erst ab dem Zeitpunkt der Anordnung ausleitet.

Soll hingegen eine Ausleitung aller Nachrichten in zeitlich unbegrenzter Hinsicht erfolgen, würde das über die herkömmlichen Möglichkeiten der Telekommunikationsüberwachung weit hinausgehen und eine – wenngleich auf Kommunikationsinhalte eines Kommunikationsdienstes begrenzte – „kleine“ Online-Durchsuchung darstellen. Das Ausleiten von Nachrichten, die vor dem Anordnungszeitpunkt abgesendet oder empfangen wurden, findet seine Rechtsgrundlage folglich nicht in § 100a StPO, sondern in der für die Online-Durchsuchung neu geschaffenen Ermächtigungsgrundlage des § 100b StPO.

Zu Buchstabe a

§ 100a Absatz 1 Satz 2 und 3 StPO-E enthält nunmehr in Ergänzung zu den in Satz 1 auch für die herkömmliche Telekommunikationsüberwachung genannten Voraussetzungen besondere Ermächtigungsgrundlagen für die Überwachung und Aufzeichnung von Kommunikationsinhalten auf einem informationstechnischen System des Betroffenen. Dabei bildet Satz 2 die Rechtsgrundlage für Eingriffe in Artikel 10 GG, wenn sich die Überwachung und Aufzeichnung auf dem informationstechnischen System auf „laufende Kommunikation“

noch während des Übertragungsvorgangs bezieht. Satz 3 erfasst darüber hinaus die Fälle, in denen ein Eingriff in Artikel 2 Absatz 1 i.V.m. Artikel 1 Absatz 1 GG vorliegt, weil sich die Überwachung und Aufzeichnung zwar ebenfalls ausschließlich auf Kommunikationsinhalte bezieht, der Übertragungsvorgang in dem Moment der Überwachung jedoch bereits abgeschlossen ist.

Mit dem neu geschaffenen Satz 2 wird ausdrücklich festgelegt, dass die Überwachung und Aufzeichnung der Telekommunikation auch in der Weise erfolgen darf, dass in von dem Betroffenen genutzte informationstechnische Systeme mit technischen Mitteln eingegriffen wird. Insoweit liegt gegenüber der herkömmlichen Telekommunikationsüberwachung, die beim Telekommunikationsunternehmen erfolgt, ein zusätzlicher Grundrechtseingriff für den Betroffenen vor, weil dessen technische Geräte mittels einer Software infiltriert und damit verändert werden. Die Strafverfolgungsbehörden erhalten die Befugnis, mit Hilfe einer Überwachungssoftware, die den Anforderungen des § 100a Absatz 5 Satz 1 Nummer 1 Buchstabe a StPO-E genügen muss (dazu unter Buchstabe c), eine von den Kommunikationspartnern verschlüsselt geführte Kommunikation in unverschlüsselter Form zu überwachen und aufzuzeichnen. Hierzu können sie die notwendigen technischen Maßnahmen ergreifen, z.B. die Audiosignale an Mikrofon oder Headset bei einem laufenden Telekommunikationsvorgang abgreifen. Der Hinweis auf die besondere Notwendigkeit des Eingriffs zur Ermöglichung der Überwachung und Aufzeichnung der Kommunikation stellt eine besondere Ausprägung des Verhältnismäßigkeitsgrundsatzes dar. Die Quellen-Telekommunikationsüberwachung ist im Verhältnis zur herkömmlichen Telekommunikationsüberwachung grundsätzlich nur subsidiär zulässig. Den Hauptanwendungsfall der Maßnahme bildet dabei die Sicherstellung der Aufzeichnung von Telekommunikation in unverschlüsselter Form.

Satz 3 trifft eine ergänzende Regelung und stellt klar, dass auch solche Inhalte und Umstände der Kommunikation mittels einer Überwachungssoftware überwacht und aufgezeichnet werden dürfen, bei denen der Übertragungsvorgang bereits abgeschlossen ist und die auf dem informationstechnischen System des Betroffenen in einer Anwendung gespeichert sind. Dies betrifft konkret die über Messenger-Dienste versandten und mittlerweile regelmäßig verschlüsselten Nachrichten. Um die funktionale Äquivalenz mit der herkömmlichen Telekommunikationsüberwachung zu gewährleisten, dürfen nur solche Kommunikationsinhalte und -umstände erhoben werden, die auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form erhoben werden könnten. Die zu verwendende Software muss demnach entsprechend konstruiert sein und außerdem in technischer Hinsicht den Anforderungen des § 100a Absatz 5 Satz 1 Nummer 1 Buchstabe b StPO-E genügen (vgl. dazu Buchstabe c). Damit gewährleistet die Vorschrift einerseits eine Beschränkung auf „Kommunikationsinhalte“ in Abgrenzung zu den sonstigen auf dem informationstechnischen System befindlichen gespeicherten Daten. Zum anderen wird klargestellt, dass ein Ausleiten der Inhalte und Umstände der Kommunikation nur für den Fall der Verschlüsselung zulässig ist (Subsidiarität), da ansonsten die Kommunikation auch während des laufenden Übertragungsvorgangs im öffentlichen Rechnernetz ausgeleitet werden könnte. Der Begriff der Verschlüsselung erfasst jede Form der technischen Unbrauchbarmachung, die eine Kenntnisnahme vom Inhalt der Nachricht im Falle der herkömmlichen Ausleitung beim Verpflichteten tatsächlich unmöglich macht. Erfasst werden danach nicht nur die Ende-zu-Ende-Verschlüsselung, sondern auch alle sonstigen Formen der Unkenntlichmachung etwa durch eine Transport-Verschlüsselung oder durch das Aufspalten und Versenden einer Nachricht in vielen kleinen unlesbaren Einheiten.

Jeder Zugriff auf ein informationstechnisches System des Betroffenen zum Zweck der Aufbringung der Überwachungssoftware darf grundsätzlich nur auf technischem Wege oder mittels kriminalistischer List erfolgen. Eine Befugnis, die Wohnung des Betroffenen zu diesem Zweck heimlich zu betreten, ist mit der Befugnis nach § 100a Absatz 1 Satz 2 StPO nicht verbunden.

Zu Buchstabe b

Die Anordnung einer Telekommunikationsüberwachung darf sich nur gegen bestimmte Personen richten. Die bisherige Regelung erstreckt sich auf den Beschuldigten und sogenannte Nachrichtenmittler, d.h. Personen, von denen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder dass der Beschuldigte ihren Anschluss benutzt (zur Verfassungskonformität der vergleichbaren Regelung im präventiven Bereich BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 – Rn. 233). Die Regelung wird durch die Einbeziehung der Quellen-Telekommunikationsüberwachung nunmehr ergänzt um die Fälle, in denen anzunehmen ist, dass der Beschuldigte sich eines fremden informationstechnischen Systems bedient.

Zu Buchstabe c

Absatz 4

Absatz 4 entspricht, abgesehen von geringfügigen redaktionellen Änderungen, der geltenden Fassung des § 100b Absatz 3 StPO und enthält die Verpflichtung der Telekommunikationsunternehmen zur Mitwirkung im Rahmen der herkömmlichen Telekommunikationsüberwachung.

Absatz 5

Der neu gestaltete Absatz 5 des § 100a fasst die in § 20l Absatz 2 Satz 1 Nummer 1 und § 20k Absatz 2 BKAG g.F. (§§ 50 Absatz 2 Satz 1 Nummer 1, 48 Absatz 2 BKAG-E) für den präventiven Bereich an unterschiedlichen Stellen geregelten technischen Voraussetzungen der Durchführung einer Quellen-Telekommunikationsüberwachung in einer Vorschrift zusammen und passt diese an die differenziert ausgestalteten Ermächtigungsgrundlagen in Absatz 1 Satz 2 und 3 StPO-E an.

Absatz 5 Satz 1 Nummer 1 formuliert die technischen Anforderungen an die zu verwendende Software im Sinne der vom Bundesverfassungsgericht vorgegebenen „funktionalen Äquivalenz“ zur herkömmlichen Telekommunikationsüberwachung durch Ausleiten beim Telekommunikationsunternehmen (s.o. Begründung zu Nummer 2).

Die Software muss danach in den Fällen des Absatz 1 Satz 2 gewährleisten, dass ausschließlich „laufende Kommunikation“ erfasst wird (Nummer 1 Buchstabe a).

In den Fällen des Absatzes 1 Satz 3 muss die Software so entwickelt werden, dass nur solche Inhalte und Umstände der Kommunikation erhoben werden, die auch auf während der Übertragung im öffentlichen Rechnernetz hätte überwacht und aufgezeichnet werden können (Nummer 1 Buchstabe b). Um die funktionale Äquivalenz zur herkömmlichen Telekommunikationsüberwachung auch in zeitlicher Hinsicht zu gewährleisten, dürfen nur zukünftige Kommunikationsinhalte erhoben werden, d.h. solche, die ab dem Zeitpunkt der Anordnung nach § 100e Absatz 1 StPO anfallen. Die für die Ausleitung von mit Messenger-Diensten übertragenen Nachrichten einzusetzende Software muss daher anhand der zu den einzelnen Textnachrichten hinterlegten Meta-Daten, die etwa die Absende-, Empfangs- und Lesezeitpunkte enthalten, unterscheiden können, damit Nachrichten erst ab dem Zeitpunkt der Anordnung überwacht und aufgezeichnet werden können. Ältere Messenger-Nachrichten dürfen nur im Rahmen einer Maßnahme nach § 100b StPO-E (Online-Durchsuchung) ausgeleitet werden.

Soweit eine den Anforderungen des Absatz 5 Satz 1 Nummer 1 genügende Software, die eine entsprechende Trennung der laufenden Kommunikation von den übrigen Systeminhalten bzw. eine Trennung der Messenger-Kommunikationsinhalte anhand der zu den

Nachrichten hinterlegten Metadaten nicht zur Verfügung stehen sollte, weil sie – unter Umständen für jede Anwendung gesondert – erst entwickelt werden muss, ist die Maßnahme unter den Voraussetzungen des § 100a StPO-E unzulässig. Insoweit kommt allerdings die Durchführung einer Online-Durchsuchung gemäß § 100b StPO-E in Betracht – wenn deren Voraussetzungen im Übrigen vorliegen.

Absatz 5 Satz 1 Nummer 2 und 3 und Satz 2 stellt eine Ausprägung des Verhältnismäßigkeitsgrundsatzes dar und entsprechen § 20k Absatz 2 BKAG g.F. (§ 48 Absatz 2 BKAG-E). Danach haben die Strafverfolgungsbehörden bestimmte technische Schutzvorkehrungen zu treffen, um den Eingriff in das vom Betroffenen zu Kommunikationszwecken genutzte informationstechnische System auf das unbedingt erforderliche Mindestmaß zu begrenzen und die Datensicherheit zu gewährleisten.

Absatz 6

Gemäß Absatz 6 gelten für Maßnahmen, bei denen technische Mittel eingesetzt werden, zusätzliche Protokollierungsvorschriften, um einen effektiven Grundrechtsschutz des Betroffenen und die Gerichtsfestigkeit der erhobenen Beweise zu gewährleisten. Insoweit gelten nach dem neu eingefügten § 100a Absatz 6 die in § 20k Absatz 3 Satz 1 BKAG g.F. (§ 79 Absatz 1 und Absatz 2 Nummer 6 Buchstabe b BKAG-E) enthaltenen Bestimmungen für die Quellen-Telekommunikationsüberwachung im Bereich der Strafverfolgung entsprechend. In der durch den Bund und die Länder erarbeiteten Standardisierenden Leistungsbeschreibung ist das Verfahren für eine umfassende Protokollierung ergänzend festgelegt. Durch die Dokumentation des Quellcodes, des Prozesses der Programmerzeugung aus diesem Quellcode und des Programms selbst kann im Nachhinein der Funktionsumfang der jeweils eingesetzten Überwachungssoftware abschließend nachvollzogen werden. Soweit in § 20k Absatz 3 Satz 3 BKAG g.F. auch Verwendungs- und Löschungsvorschriften für die Protokollierung vorgesehen sind (insoweit in § 79 Absatz 4 Satz 2 BKAG-E bereits angepasst), werden diese nicht in die Strafprozessordnung übernommen, weil im Bereich der Strafverfolgung die Kontrolle der Rechtmäßigkeit des eingesetzten Mittels bis zum Abschluss des Strafverfahrens durch die Gerichte möglich sein muss. Danach gelten die Löschungs- und Dokumentationsvorschriften des § 101 Absatz 8 StPO.

Zu Nummer 3

Mit den vorgeschlagenen Änderungen wird erstmals eine Rechtsgrundlage für die Online-Durchsuchung in der Strafprozessordnung geschaffen.

Die Online-Durchsuchung im Sinne eines verdeckten staatlichen Zugriffs auf ein fremdes informationstechnisches System mit dem Ziel, dessen Nutzung zu überwachen und gespeicherte Inhalte aufzuzeichnen, ist derzeit zu Strafverfolgungszwecken nicht gestattet. Möglich sind die „offene“ Durchsuchung und Beschlagnahme der auf informationstechnischen Geräten gespeicherten Daten nach den §§ 94 ff., 102 ff. StPO sowie die „heimliche“ Telekommunikationsüberwachung, die sich auf Kommunikationsinhalte bezieht. Der mit der Online-Durchsuchung verbundene Eingriff wiegt in verschiedener Hinsicht erheblich schwerer. Im Unterschied zur offenen Durchsuchung und Beschlagnahme eines informationstechnischen Systems erfolgt der Zugriff heimlich und kann nicht nur einmalig und punktuell stattfinden, sondern sich auch über einen längeren Zeitraum erstrecken. In Abgrenzung zur ebenfalls „heimlichen“ Telekommunikationsüberwachung können nicht nur neu hinzukommende Kommunikationsinhalte, sondern alle auf einem informationstechnischen System gespeicherten Inhalte sowie das gesamte Nutzungsverhalten einer Person überwacht werden.

Die Online-Durchsuchung stellt für den Betroffenen einen Eingriff in den Schutzbereich des Grundrechts auf Integrität und Vertraulichkeit informationstechnischer Systeme als eigen-

ständiger Ausprägung des Rechts auf informationelle Selbstbestimmung nach Artikel 2 Absatz 1 i.V.m. Artikel 1 Absatz 1 GG dar. Das Recht auf informationelle Selbstbestimmung trägt den Persönlichkeitsgefährdungen nicht vollständig Rechnung, die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist und dabei dem System persönliche Daten anvertraut oder schon allein durch dessen Nutzung zwangsläufig liefert. Ein Dritter, der auf ein solches System zugreift, kann sich einen potentiell äußerst großen und aussagekräftigen Datenbestand verschaffen, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein. Ein solcher Zugriff geht in seinem Gewicht für die Persönlichkeit des Betroffenen über einzelne Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützt, weit hinaus (vgl. BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 – Rn. 200).

Eingriffe in den Schutzbereich des Grundrechts auf Integrität und Vertraulichkeit informationstechnischer Systeme können grundsätzlich gerechtfertigt sein, stehen jedoch unter strengen Bedingungen. Insoweit sind hohe Anforderungen an die Rechtfertigung des Eingriffs zu stellen. Der Intensität des Grundrechtseingriffs ist im Recht der Gefahrenabwehr etwa dadurch Rechnung zu tragen, dass die Online-Durchsuchung nur durchgeführt werden darf, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Im Bereich der Strafverfolgung muss die Maßnahme in einem angemessenen Verhältnis zur Schwere und Bedeutung der Straftat stehen. Insoweit ist insbesondere zu berücksichtigen, dass das Bundesverfassungsgericht die Eingriffsintensität einer Online-Durchsuchung mit der Eingriffsintensität einer Wohnraumüberwachung vergleicht (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 – Rn. 210 a.E.).

Die vorgeschlagene Regelung des § 100b StPO als Rechtsgrundlage für die Online-Durchsuchung orientiert sich daher sowohl hinsichtlich der Voraussetzungen für die Anordnung der Maßnahme als auch hinsichtlich der verfahrensrechtlichen Sicherungen, dem Schutz des Kernbereichs privater Lebensgestaltung, sowie der Verwendung und Löschung der mit der Maßnahme erlangten Erkenntnisse grundsätzlich an der bereits bestehenden und vom Bundesverfassungsgericht bereits geprüften Regelung zur akustischen Wohnraumüberwachung (§§ 100c, 100d StPO g.F.; BVerfG, Nichtannahmebeschluss vom 11. Mai 2007 – 2 BvR 543/06 – Rn. 64 ff.). Im Übrigen werden die technischen Sicherungen, die auch im Rahmen der Quellen-Telekommunikationsüberwachung gelten, auch auf die Online-Durchsuchung übertragen.

Absatz 1

Absatz 1 enthält die eigentliche Ermächtigungsgrundlage zur Durchführung der Online-Durchsuchung.

Nach Absatz 1 Nummer 1 darf auch ohne Wissen des Betroffenen in ein von dem Betroffenen genutztes informationstechnisches System eingegriffen und dürfen Daten daraus erhoben werden, wenn 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.

Während die Telekommunikationsüberwachung grundsätzlich bei „schweren Straftaten“ zulässig ist, darf die Online-Durchsuchung ebenso wie die akustische Wohnraumüberwachung nur beim Verdacht einer „besonders schweren Straftat“ angeordnet werden. Der Katalog der Straftaten, bei denen eine Online-Durchsuchung erfolgen darf, entspricht daher vollständig dem Katalog der Straftaten, bei denen bislang eine akustische Wohnraumüberwachung angeordnet werden darf.

Darüber hinaus muss die Tat auch im Einzelfall besonders schwer wiegen (Absatz 1 Nummer 2) und die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des

Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos sein (Absatz 1 Nummer 3). Diese Voraussetzungen stellen eine Ausprägung des Verhältnismäßigkeitsgrundsatzes dar. Die Maßnahme ist nur zulässig, wenn eine Tat nicht nur im Allgemeinen, sondern auch im konkreten Fall besonders schwer wiegt. Im Übrigen ist die Maßnahme subsidiär, d.h. sie darf nur angewendet werden, wenn andere Ermittlungsmaßnahmen versagen. Vor der Durchführung einer Online-Durchsuchung ist daher insbesondere zu prüfen, ob nicht auch eine offene Durchsuchung und Beschlagnahme in Betracht kommt.

Absatz 2

Der Katalog der Straftaten entspricht dem für die Wohnraumüberwachung geltenden Katalog in § 100c Absatz 2 StPO g.F.

Die in Nummer 1 Buchstabe a) aufgeführten §§ 98 Abs. 1 Satz 2, 99 Absatz 2 StGB schließen elektronische Angriffe fremder Mächte ein, für deren Verfolgung die Ermittlung von Angriffsvektoren über dazu genutzte informationstechnische Systeme besonders bedeutsam ist. Dies gilt nicht nur für Fälle der Cyberspionage von beachtlichem Gewicht (vgl. etwa den Angriff auf den Deutschen Bundestag), sondern umfasst insbesondere auch Wirtschaftsspionage durch fremde Mächte, wenn sie wegen der erheblichen volkswirtschaftlichen Schäden typischerweise besonders schwere Fälle darstellen.

Absatz 3

Absatz 3 ist § 100c Absatz 3 nachgebildet. Die Maßnahme der Online-Durchsuchung darf sich grundsätzlich nur gegen den Beschuldigten richten. Andere Personen werden nur erfasst, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass der Beschuldigte ihre informationstechnischen Systeme selbst benutzt. Auch in diesen Fällen ist ein Zugriff auf das Gerät der anderen Person jedoch nur dann zulässig, wenn der Zugriff auf Geräte des Beschuldigten selbst allein nicht zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes eines Mitbeschuldigten genügt.

Absatz 4

In Absatz 4 wird auf die bei der Telekommunikationsüberwachung geltenden technischen Sicherungen und Protokollierungsvorschriften verwiesen, soweit diese auch auf die Online-Durchsuchung Anwendung finden sollen. Entsprechend anzuwenden sind insoweit sämtliche Vorschriften mit Ausnahme der für die Quellen-Telekommunikationsüberwachung spezifischen Voraussetzung der Gewährleistung der funktionalen Äquivalenz zur herkömmlichen Telekommunikationsüberwachung in § 100a Absatz 5 Satz 1 Nummer 1 StPO-E.

Zu Nummer 4

Nachdem der bisherige Straftatenkatalog für die Wohnraumüberwachung nunmehr unverändert in § 100b Absatz 2 StPO-E aufgenommen wurde, wird in § 100c Absatz 1 Nummer 1 auf § 100b Absatz 2 StPO-E verwiesen. Der bisherige Absatz 3 wird Absatz 2, der im bisherigen Absatz 3 enthaltene Verweis auf § 100d Absatz 2 als Folgeänderung angepasst. Der Inhalt der Absätze 4 bis 7 ist nunmehr Gegenstand des § 100d StPO-E.

Zu Nummer 5

In § 100d StPO-E werden die bislang in den einzelnen Ermächtigungsgrundlagen gesondert geregelten Vorschriften über den Schutz des Kernbereichs privater Lebensgestaltung sowie die Zeugnisverweigerungsberechtigten zusammengefasst, nach der Schwere des Eingriffs systematisiert und auf die Maßnahmen der Online-Durchsuchung erstreckt. In § 100e StPO-E sind die für das Verfahren geltenden Vorschriften für Maßnahmen nach den §§ 100a bis 100c StPO-E zusammengefasst.

§ 100d StPO-E

Nach der Rechtsprechung des Bundesverfassungsgerichts müssen bei eingriffsintensiven Maßnahmen mit genereller Relevanz für den Kernbereich privater Lebensgestaltung einer Person sowohl auf der Erhebungsebene als auch in der Auswertungsphase hinreichende Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung getroffen werden (vgl. BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 – Rn. 257; Beschluss vom 12. Oktober 2011 – 2 BvR 236/08 – Rn. 209).

In Absatz 1 wird insoweit auf der Erhebungsebene der Grundsatz vorangestellt, dass sämtliche Maßnahmen nach §§ 100a bis 100c StPO-E generell unzulässig sind, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden (vgl. §§ 100a Absatz 4 S. 1, 100c Absatz 4 S. 1 StPO g.F.; dazu BVerfG, Beschluss vom 12. Oktober 2011 – 2 BvR 236/08 – Rn. 209; Urteil vom 20. April 2016 – 1 BvR 966/09 – Rn. 119 ff., 125). Ein ausschließlicher Kernbereichsbezug kann vor allem dann angenommen werden, wenn der Betroffene mit Personen in Kontakt tritt, zu denen er in einem besonderen, den Kernbereich betreffenden Vertrauensverhältnis – wie zum Beispiel engsten Familienangehörigen, Geistlichen, Telefonseelsorgern, Strafverteidigern oder im Einzelfall auch Ärzten – steht (vgl. BVerfG, Beschluss vom 12. Oktober 2011 – 2 BvR 236/08 – Rn. 215). Soweit ein derartiges Vertrauensverhältnis für Ermittlungsbehörden erkennbar ist, dürfen Maßnahmen nicht durchgeführt werden. Umgekehrt besagt der in Absatz 1 vorangestellte Grundsatz nicht, dass Maßnahmen nach §§ 100a bis 100c schon deshalb von vornherein unterlassen werden müssen, weil auch Tatsachen mit erfasst werden können, die den Kernbereich des Persönlichkeitsrechts berühren (BVerfG a.a.O., Rn 216). Der Schutz des Kernbereichs privater Lebensgestaltung wird in diesen Fällen durch ergänzende Vorkehrungen in der Erhebungs- und Auswertungsphase (Absätze 2 bis 4) sichergestellt.

Absatz 2 sieht entsprechend den Vorgaben des Bundesverfassungsgerichts Schutzvorkehrungen auf der Verwertungsebene vor. Nach der für sämtliche Maßnahmen nach den §§ 100a bis 100c StPO-E geltenden Verwertungsregelung dürfen Erkenntnisse aus dem Kernbereich privater Lebensgestaltung nicht verwertet werden. Die Vorschrift enthält das Gebot der unverzüglichen Löschung solcher Erkenntnisse und flankierende Dokumentations- und Löschungspflichten. Diese galten bislang für die Telekommunikationsüberwachung und die Wohnraumüberwachung (§§ 100a Absatz 4 S. 2 bis 4, § 100c Absatz 5 S. 2 bis 4 StPO g.F.), werden nunmehr in einer Vorschrift zusammengefasst und auf die Online-Durchsuchung erstreckt. Die Dokumentation über die Erlangung und Löschung entsprechender Erkenntnisse (Löschungsprotokoll) wird zu den Akten genommen, um die Kontrolle der Rechtmäßigkeit der Maßnahme bis zum Abschluss des Strafverfahrens durch die Gerichte zu ermöglichen (zur Verwahrung der Unterlagen bei der Staatsanwaltschaft vgl. § 101 Abs. 2 Satz 1 StPO-E). Insoweit gelten die Löschungs- und Dokumentationsvorschriften des § 101 Absatz 8 StPO.

Absatz 3 enthält einen an die Regelung des Kernbereichsschutzes im Rahmen der Wohnraumüberwachung angelehnten, den Besonderheiten der Online-Durchsuchung Rechnung tragenden ergänzenden Schutz auf der Erhebungs- und Auswertungsebene (vgl. dazu BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 – Rn. 217 ff., 223 ff.). Bei der Erhebung von Erkenntnissen im Rahmen einer Online-Durchsuchung ist, soweit möglich, technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Erkenntnisse, die durch Maßnahmen nach § 100b erlangt wurden und den Kernbereich privater Lebensgestaltung betreffen, sind unverzüglich zu löschen oder von der Staatsanwaltschaft dem anordnenden Gericht als einer unabhängigen Stelle (vgl. Nichtannahmebeschluss vom 11. Mai 2007 – 2 BvR 543/06 – Rn. 23, 64 ff.) zur Entscheidung über die Verwertbarkeit und Löschung der Daten vorzulegen. Die Entscheidung des Gerichts über die Verwertbarkeit ist für das weitere Verfahren bindend.

Absatz 4 fasst die bisher in § 100c Absatz 4, 5 und 7 StPO g.F. enthaltenen Vorschriften zum Schutz des Kernbereichs privater Lebensgestaltung bei der Wohnraumüberwachung in einer ergänzenden Regelung für die Erhebungs- und Auswertungsebene zusammen. Maßnahmen nach § 100c g.F. dürfen bereits nur dann angeordnet werden, soweit auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass durch die Überwachung Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, nicht erfasst werden. Diese tatsächlichen Anhaltspunkte sind im richterlichen Beschluss gesondert darzulegen (vgl. § 100e Absatz 4 Nummer 3 StPO-E). Auf der Erhebungsebene ist das Abhören und Aufzeichnen ferner unverzüglich zu unterbrechen, soweit sich während der Überwachung Anhaltspunkte dafür ergeben, dass Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden. Ist eine Maßnahme unterbrochen worden, so darf sie nur unter den in Satz 1 genannten Voraussetzungen fortgeführt werden. Bestehen Zweifel, so hat die Staatsanwaltschaft über die Unterbrechung oder Fortführung der Maßnahme unverzüglich eine Entscheidung des Gerichts herbeizuführen. Auch soweit für bereits erlangte Erkenntnisse ein Verwertungsverbot nach Absatz 2 in Betracht kommt, ist von der Staatsanwaltschaft unverzüglich eine Entscheidung des Gerichts einzuholen; diese Entscheidung ist für das weitere Verfahren bindend.

Nicht in die Neuregelung aufgenommen wurde § 100c Absatz 4 Satz 1 Halbsatz 3, Satz 2 und 3 StPO g.F. Die Frage, ob auf Grund tatsächlicher Anhaltspunkte der Kernbereich privater Lebensgestaltung betroffen sein könnte, ist jeweils konkret vom Gericht unter Berücksichtigung aller Umstände des Einzelfalles zu würdigen. Die Art der zu überwachenden Räumlichkeiten – Betriebs-/Geschäftsräume oder Privatwohnung – oder das Verhältnis der zu überwachenden Personen zueinander kann in diesem Zusammenhang von Bedeutung sein, liefert allgemein aber allenfalls Indizien gegen eine Vertraulichkeit. Generell kann der Kernbereich privater Lebensgestaltung auch in einem Geschäftsraum betroffen sein. Die Subsumtion ist eine Frage des jeweiligen Einzelfalls. Die o.g. Vorschriften werden deshalb in der Literatur als „problematisch“ und „weitreichend misslungen“ bezeichnet (vgl. Hauck, in: Löwe-Rosenberg, Strafprozessordnung, 26. Auflage, § 100c Rn. 115 ff.; Wolter, in: SK/StPO, 5. Auflage 2016, § 100c Rn. 54). Sie sind nach der Rechtsprechung des Bundesverfassungsgerichts zur negativen Kernbereichsprognose auch nicht erforderlich (vgl. Nichtannahmebeschluss vom 11. Mai 2007 – 2 BvR 543/06 –, juris, Rn. 41 ff., 44).

Absatz 5 enthält die bisher in § 100c Absatz 6 StPO g.F. enthaltene Regelung zum Schutz von Zeugnisverweigerungsberechtigten, insbesondere Berufsgeheimnisträgern. Diese wird auf Maßnahmen der Online-Durchsuchung erstreckt.

§ 100e StPO-E

Die Vorschriften über das Verfahren sind in § 100e StPO-E dem Schweregrad des Eingriffs bei den jeweiligen Maßnahmen entsprechend abgestuft.

Absatz 1 entspricht § 100b Absatz 1 StPO g.F. Danach dürfen Maßnahmen der Telekommunikationsüberwachung vom Ermittlungsrichter auf Antrag der Staatsanwaltschaft, in Eilfällen auch von der Staatsanwaltschaft selbst angeordnet werden kann, sofern sie binnen drei Tagen vom Gericht bestätigt wird. Die Maßnahme ist auf drei Monate zu befristen und darf verlängert werden, soweit die Voraussetzungen für ihre Anordnung fortbestehen.

Absatz 2 entspricht § 100d Absatz 1 StPO g.F., wobei die dort für die Wohnraumüberwachung geltenden besonderen Verfahrenssicherungen nunmehr auch auf Maßnahmen der Online-Durchsuchung erstreckt werden. An die Stelle des Ermittlungsrichters tritt die in § 74a Absatz 4 des Gerichtsverfassungsgesetzes genannte Kammer des Landgerichts, in dessen Bezirk die Staatsanwaltschaft ihren Sitz hat. Diese ist für die Anordnung und fortlaufende Kontrolle der Maßnahmen zuständig. Bei Gefahr im Verzug kann die Anordnung selbst auch durch den Vorsitzenden getroffen werden, muss aber binnen drei Werktagen von der Strafkammer bestätigt werden. Die Anordnung ist auf höchstens einen Monat zu

befristen. Auch hinsichtlich der Fristen ist daher der Gleichlauf mit der Wohnraumüberwachung gegeben, wobei nicht verkannt werden soll, dass die Durchführung einer geplanten Online-Durchsuchung vor dem Hintergrund der zu schaffenden technischen Voraussetzungen regelmäßig zeitlich aufwändiger ist als die Durchführung einer akustischen Wohnraumüberwachung. Eine Verlängerung um jeweils nicht mehr als einen Monat ist allerdings auch nach der bisher geltenden Regelung zulässig, soweit die Voraussetzungen unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen. Ist die Dauer der Anordnung auf insgesamt sechs Monate verlängert worden, so entscheidet über weitere Verlängerungen das Oberlandesgericht.

In Absatz 3 sind die für den Inhalt der Entscheidungsformel geltenden Bestimmungen für Maßnahmen nach den §§ 100a bis 100c StPO-E zusammengefasst. Absatz 1 Nummer 1 bis 3 galt bereits zuvor für Maßnahmen nach den §§ 100a und 100c StPO g.F., Absatz 3 Nummer 4 galt vorher nur für Maßnahmen nach den §§ 100c, so dass die Regelung eine moderate Ausweitung der Anforderungen für alle heimlichen Maßnahmen enthält. Absatz 3 Nummer 5 enthält spezielle Anforderungen für die Anordnung der Telekommunikationsüberwachung. Über die in § 100b Absatz 2 Satz 2 Nummer 1 bis 3 StPO g.F. enthaltenen Angaben hinaus muss die Anordnung in den Fällen des § 100a Absatz 1 Satz 2 und 3 StPO-E nunmehr auch eine möglichst genaue Bezeichnung des informationstechnischen Systems, in das zur Überwachung und Aufzeichnung der Kommunikation ggf. eingegriffen werden soll, enthalten. Die Bezeichnung des informationstechnischen Systems, in das eingegriffen und aus dem Daten erhoben werden sollen, ist nach Absatz 3 Nummer 6 auch bei Maßnahmen der Online-Durchsuchung erforderlich. Absatz 3 Nummer 7 entspricht § 100d Absatz 2 Nummer 3 StPO g.F.

Absatz 4 enthält entsprechend der für die Wohnraumüberwachung bisher geltenden Regelung in § 100d Absatz 3 StPO g.F. Anforderungen an die Begründung der Anordnung. Diese werden mit Ausnahme von Absatz 4 Nummer 3, welche speziell auf die Kernbereichsregelung für die Wohnraumüberwachung zugeschnitten ist, auf Maßnahmen nach den §§ 100a und 100b StPO erstreckt. Für Maßnahmen der Telekommunikationsüberwachung war dies bislang zwar nicht ausdrücklich gesetzlich vorgeschrieben, allerdings hat das Bundesverfassungsgericht nunmehr für die Parallelvorschrift in § 20l BKAG ausdrücklich eine Mitteilung der Gründe einer solchen Anordnung verlangt (BVerfG, Urteil vom 20. April 2016, – 1 BvR 966/09, 1 BvR 1140/09 – Rn. 235).

Absatz 5 fasst die Vorschriften über die Beendigung und die Verlaufskontrolle (bisher die §§ 100b Absatz 4 und 100d Absatz 4 StPO g.F.) zusammen und erstreckt die für die Wohnraumüberwachung geltenden – erweiterten – Bestimmungen auf die Online-Durchsuchung.

Absatz 6 enthält die bisher in § 100d Absatz 5 StPO g.F. geregelte umfassende Verwendungsregelung für personenbezogene Daten aus Maßnahmen der Wohnraumüberwachung, welche die allgemeinen Verwendungsregelungen in § 161 Absatz 2 und 3 und § 477 Absatz 2 StPO ergänzt und aufgrund der Eingriffstiefe der Wohnraumüberwachung spezielle Anforderungen an die weitere Verwendung personenbezogener Daten stellt. Diese Anforderungen werden aufgrund der vergleichbaren Eingriffstiefe auf Maßnahmen der Online-Durchsuchung erstreckt und im Übrigen geringfügig inhaltlich und redaktionell angepasst.

Zu Nummer 6

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Nummer 7

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Nummer 8

Die Verfahrensregelungen bei verdeckten Maßnahmen in § 101 StPO g.F. werden mit Blick auf die Einführung der Online-Durchsuchung entsprechend erweitert, insbesondere wird die Verwahrungspflicht für Unterlagen in Absatz 2 auf Maßnahmen des § 100b StPO-E ausgedehnt und die Benachrichtigungspflicht auf den Beschuldigten und erheblich mitbetroffene Personen bei Online-Durchsuchungen erstreckt.

Zu Nummer 9

Es handelt sich um redaktionelle Folgeänderungen.

Zu Nummer 10

Die geltenden jährlichen Pflichten zur statistischen Erfassung für Maßnahmen nach §§ 100a bis 100c StPO-E und § 100g g.F. sowie die Einzelheiten der in Artikel 13 Absatz 6 GG vorgeschriebenen Berichtspflicht für Maßnahmen der akustischen Wohnraumüberwachung werden in § 101b StPO-E zusammengefasst.

Absatz 1 Satz 1 und 2 entspricht § 100b Absatz 5 StPO g.F., Absatz 1 Satz 3 entspricht § 100e Absatz 1 Satz 2 StPO g.F.

Absatz 2 entspricht § 100b Absatz 6 StPO g.F., wobei die im Gesetzentwurf der Bundesregierung zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens geringfügig geänderten Berichtspflichten in Nummer 2 bereits berücksichtigt sind. Nach der neu angefügten Nummer 4 ist zudem nach Abschluss des Verfahrens in der Statistik sowohl die Anzahl der Verfahren anzugeben, in denen eine Quellen-Telekommunikationsüberwachung im richterlichen Beschluss angeordnet wurde, als auch die Anzahl der Verfahren, in denen die Maßnahme tatsächlich durchgeführt wurde.

Absatz 3 betrifft Maßnahmen der neu eingeführten Online-Durchsuchung nach § 100b StPO-E. Anzugeben sind insoweit die Anzahl der Verfahren, in denen Maßnahmen nach § 100b Absatz 1 StPO-E angeordnet worden sind, die Anzahl der Überwachungsanordnungen unterschieden nach Erst- und Verlängerungsanordnungen, die jeweils zugrunde liegende Anlassstraftat nach Maßgabe der Unterteilung in § 100b Absatz 2 StPO-E, sowie die Anzahl der Verfahren, in denen ein Eingriff in ein vom Betroffenen genutztes informationstechnisches System tatsächlich durchgeführt wurde.

Absatz 4 entspricht § 100e Absatz 2 StPO g.F. und betrifft Maßnahmen der Wohnraumüberwachung.

Absatz 5 entspricht § 101b StPO g.F., wobei die im Gesetzentwurf der Bundesregierung zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens geringfügig geänderten Berichtspflichten in Nummer 2 bereits berücksichtigt wurden.

Zu Nummer 11 bis 16

Es handelt sich um redaktionelle Folgeänderungen.

Zu Artikel 2 (Änderung des Einführungsgesetzes zur Strafprozessordnung)

§ …[…] des Einführungsgesetzes zur Strafprozessordnung in der Entwurfsfassung enthält eine Übergangsregelung für die Statistik- und Berichtspflichten.

Zu Artikel 3 (Änderung des Antiterrordateigesetzes)

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Artikel 4 (Änderung des Rechtsextremismus-Datei-Gesetzes)

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Artikel 5 (Änderung des Artikel 10-Gesetzes)

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Artikel 6 (Änderungen des Gerichtsverfassungsgesetzes)

Es handelt sich um redaktionelle Folgeänderungen.

Zu Artikel 7 (Änderungen des IStGH-Gesetzes)

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Artikel 8 (Änderung des Wertpapierhandelsgesetzes)

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Artikel 9 (Änderung des Strafgesetzbuchs)

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Artikel 10 (Änderungen des Zollfahndungsdienstgesetzes)

Es handelt sich um redaktionelle Folgeänderungen.

Zu Artikel 11 (Änderungen der Telekommunikations-Überwachungsverordnung)

Es handelt sich um redaktionelle Folgeänderungen.

Zu Artikel 12 (Einschränkung eines Grundrechts)

Mit der Vorschrift wird dem in Artikel 19 Absatz 1 Satz 2 GG enthaltenen Zitiergebot Rechnung getragen.

Zu Artikel 13 (Inkrafttreten)

Die Vorschrift regelt das Inkrafttreten des Gesetzes.