HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

BACHELORARBEIT

Frau
Antonia Leibl

Online-Durchsuchung und Quellen-TKÜ nach §§ 100b, 100a StPO als Instrumentarien der Strafverfolgung

2018

Fakultät
Angewandte Computer- und Biowissenschaften

BACHELORARBEIT

Online-Durchsuchung und Quellen-TKÜ nach §§ 100b, 100a StPO als Instrumentarien der Strafverfolgung

Autorin:
Antonia Leibl

Studiengang:
Allgemeine und Digitale Forensik

Seminargruppe:
FO15w3-B

Erstprüfer:
Prof. Dr. jur. Frank Czerner

Zweitprüfer:
Prof. Dr. rer. nat. Christian Hummert

Mittweida, August 2018

Bibliografische Angaben

Leibl, Antonia: Online-Durchsuchung und Quellen-TKÜ nach §§ 100b, 100a StPO als Instrumentarien der Strafverfolgung

45 Seiten, 4 Abbildungen, 1 Anlage mit Drucksachen des Bundestags und Bundesrats, Hochschule Mittweida (FH), Fachbereich Angewandte Computer- und Biowissenschaften

Bachelorarbeit, 2018

Referat

Der Inhalt dieser Arbeit beschreibt die Online-Durchsuchung und Quellen-Telekommunikationsüberwachung. Diese Maßnahmen im Kontext der Strafverfolgung wurden 2017 vom Gesetzgeber in §§ 100b, 100a StPO neu gefasst. Es handelt sich um einen verdeckten Zugriff auf ein informationstechnisches System durch eine Überwachungssoftware, um im Rahmen der Online-Durchsuchung sämtliche Inhalte einsehen und bei der Quellen-Telekommunikationsüberwachung die Kommunikation aufzeichnen zu können.

Diese Arbeit erläutert einleitend die historische Entwicklung der Maßnahmen, die zum Gesetzgebungsverfahren geführt haben. Darauf aufbauend werden die rechtlichen Aspekte der Online-Durchsuchung und Quellen-Telekommunikationsüberwachung behandelt. Dazu zählen die betroffenen Grundrechte, die Straftatenkataloge und die Verfahrensvorschriften. Ein weiteres Themengebiet beschreibt die technischen Grundlagen im Hinblick auf die benötigte Funktionalität der Spähprogramme und Möglichkeiten zur Systeminfiltration. Der letzte Teil der Arbeit geht darauf ein, inwieweit diese Maßnahmen schon Einzug in die Strafverfolgung gefunden haben und welche Probleme noch überwunden werden müssen.

Abstract

The content of this thesis describes the online search and source telecommunication surveillance. In the context of prosecution, these measures were redifined by legislation in §§ 100b, 100a StPO in 2017. The online search and source telecommunication surveillance regulate secret access to an information technology system with a surveillance software in order to get a view on all the data inside and to record the communication respectively.

The introduction of this thesis explains the historical development of the measures which led to the legislative procedure. On this basis, the legal aspects of the online search and source telecommunication surveillance are clarified in conjunction with the affected fundamental rights, the offense catalog and the rules of procedure. Another topic deals with the technical principals in regards to the required functionality of the spy programs and its possibilities for system infiltration. The last section of this thesis examines in what extent these measures are already in use by prosecution and what are the problems still to be solved.

I. Inhaltsverzeichnis

II. Abbildungsverzeichnis

III. Abkürzungsverzeichnis

AES	Advanced Encryption Standard
aF	alte Fassung
AsylG	Asylgesetz
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtgesetz
BND	Bundesnachrichtendienst
BR	Bundesrat
BT	Bundestag
BtMG	Betäubungsmittelgesetz
BVerfG	Bundesverfassungsgericht
BVerfGE	Sammlung der Entscheidungen des BVerfG
bzw.	beziehungsweise
CCC	Chaos Computer Club
C+C-Server	Command-and-Control-Server
CDU	Christlich Demokratische Union
CSU	Christlich Soziale Union
Drs.	Drucksache
DSL	Digital Subscriber Line
EU-DSGVO	Europäische Datenschutzgrundverordnung
f.	folgende
ff.	fortfolgende
gem.	gemäß
GG	Grundgesetz
IDS	Intrusion Detection System
IP	Internet Protocol
i.S.d.	im Sinne des
IT-System	Informationstechnisches System
i.V.m.	in Verbindung mit
LKA	Landeskriminalamt
nF	neue Fassung
Nr.	Nummer(n)
PC	Personalcomputer
PKS	Polizeiliche Kriminalstatistik
PSIS	Programm zur Stärkung der Inneren Sicherheit
RCIS 1.0	Remote Control Interception Software 1.0
Rn.	Randnummer(n)
S.	Seite(n)
SMS	Short Message Service

SPD	Sozialdemokratische Partei Deutschlands
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
VoIP	Voice-over-IP
z. B.	zum Beispiel
ZITiS	Zentrale Stelle für Informationstechnik im Sicherheitsbereich

A. Einleitung

Bei Ermittlungen gegen die Neonazigruppe „Oldschool Society“ im Jahr 2015 ist es dem BKA gelungen, den Account dieser Vereinigung beim Messagingdienst Telegram zu hacken.[1] Das Verfahren des BKA, bei dem in die als sicher geltende App eingedrungen wird, beruht darauf, den Account eines Verdächtigen auf einem Gerät der Strafverfolgungsbehörde zu registrieren.[2] Dabei wird die an die Zielperson verschickte SMS mit dem Authentifizierungscode im Rahmen einer bestehenden TKÜ abgefangen.[3] Ab diesem Zeitpunkt verfügt das BKA über die Möglichkeit, die gesamte unverschlüsselte Kommunikation mitzulesen. Die Durchführung des kompletten Verfahrens beruht auf der rechtlichen Grundlage einer richterlich angeordneten, klassischen TKÜ nach § 100a StPO aF.[4] Gegen dieses Vorgehen sind rechtliche Bedenken geäußert worden, weil die Methode Elemente einer Quellen-TKÜ, die bis dato weder präventiv noch repressiv geregelt gewesen ist, enthalte.[5] Dieser Fall ist ein gutes Beispiel für die kriminalistische List des BKA, durch die bestehende Sicherheitslücken in Apps ausgenutzt werden. Aus Sicht der digitalen Forensik und des technischen Fortschritts ist zu überlegen, ob die neuen Instrumentarien der Online-Durchsuchung und Quellen-TKÜ umfangreichere Erkenntnisse insbesondere im Bereich der verschlüsselten Kommunikation über die Neonazigruppe „Oldschool Society“ ergeben hätten.

Die Reform der StPO 2017 mit der Einführung der Online-Durchsuchung und Quellen-TKÜ zur Strafverfolgung hat in der Presse eine Resonanz hinterlassen, indem Begriffe wie Bundestrojaner und staatliches Hacking aufgekommen sind. Aufgrund der Aktualität und der noch nicht endgültig geklärten Fragen in diesem Bereich stellt sich das Thema dieser Arbeit als sehr reizvoll und interessant dar. Die Bedeutung für die digitale Forensik besteht darin, wissenschaftliche Methoden anzuwenden, um Daten als Beweismittel online zu erheben. Die Online-Durchsuchung und Quellen-TKÜ nach den §§ 100b, 100a StPO als Instrumentarien der Strafverfolgung sollen sowohl nach rechtlichen Aspekten als auch im Zusammenhang mit technischen Grundlagen erläutert und diskutiert werden.

Die Arbeit setzt sich mit folgenden Schwerpunkten auseinander. Da in der Presse[6] von Eilverfahren und Einschmuggeln der Änderungen in einen anderen Gesetzesentwurf die

[1] Vgl. Lipp/Hoppenstedt, 2016.
[2] Vgl. Rebiger, 2016.
[3] Vgl. Lipp/Hoppenstedt, 2016.
[4] Vgl. Lipp/Hoppenstedt, 2016.
[5] Vgl. Lipp/Hoppenstedt, 2016.
[6] Vgl. Grunert, 2017.

Rede ist, um eine politische Diskussion und öffentliche Debatte zu umgehen, soll das Gesetzgebungsverfahren beleuchtet werden. Dabei sollen die Fragen, inwieweit dieses Thema bereits früher diskutiert worden ist und wie der Ablauf von Gesetzesentwurf bis zur Verkündung im Bundesgesetzblatt stattgefunden hat, beantwortet werden.
Im Zusammenhang mit der Online-Durchsuchung und Quellen-TKÜ bemängeln zahlreiche Stellungnahmen von Juristen die massiven Eingriffe in die Grundrechte des Betroffenen. Die Arbeit soll ausführen, welche Grundrechte betroffen sind, wie sich die Eingriffe durch die Maßnahmen darstellen und wann sie gerechtfertigt sind.
Nach einem Blick ins Grundgesetz sollen die Regelungen der §§ 100a, 100b StPO in den Fokus gerückt werden. Mit der Arbeit soll die Frage beantwortet werden, in welchen Fällen die Maßnahmen der Online-Durchsuchung und Quellen-TKÜ angeordnet werden dürfen. Dazu sollen die Straftatenkataloge beider Instrumentarien analysiert und die Unterschiede hervorgehoben werden, um die Abgrenzung von § 100a und § 100b StPO herauszustellen.
Für beide Maßnahmen ergibt sich die Frage, welche Anforderungen das Gesetz nach § 100d StPO an den Schutz des Kernbereichs und an das Zeugnisverweigerungsrecht stellt. Außerdem soll ausgeführt werden, welche Voraussetzungen für die richterliche Anordnung gem. § 100e StPO vorliegen müssen.
Einen weiteren Schwerpunkt der Arbeit stellen die technischen Grundlagen dar. Informationen zur Software sollen darüber zusammengetragen werden, wie die Software auf welche Geräte unbemerkt gelangt, welche Funktionen die Software enthalten soll und ob diese selbst programmiert oder kommerziell erworben wird.
Es soll die Frage diskutiert werden, ob die repressiven Instrumentarien der Online-Durchsuchung und Quellen-TKÜ technisch geeignet sind, sinnvolle Ergebnisse für den Ermittlungserfolg zu liefern. Dazu soll die tatsächliche und rechtliche Sicht beleuchtet werden.
Zum Schluss sollen die wesentlichen Ergebnisse der Arbeit zusammengefasst werden. Daraus soll ein Fazit gezogen und ein Ausblick gegeben werden, inwieweit Verbesserungsbedarf hinsichtlich der Software und der rechtlichen Ausgestaltung von Online-Durchsuchung und Quellen-TKÜ besteht.

B. Gesetzgebungsverfahren

Zunächst soll die Entstehungsgeschichte der Regelungen für die Online-Durchsuchung und Quellen-TKÜ dargestellt werden. Dazu wird auf Gegenstand und Ablauf des Gesetzgebungsverfahrens eingegangen.

I. Historische Entwicklung

Um die Jahrtausendwende haben Computer in alle Bereiche des Lebens und der Wirtschaft bereits so stark Einzug gehalten, dass für die üblichen Ermittlungsmethoden Handlungsbedarf herrschte. Die versuchten Kofferbombenanschläge auf Regionalzüge im August 2006 haben politische Diskussionen angefeuert.[7] Daraufhin hat der Haushaltsausschuss des Deutschen Bundestages 2006 das Programm zur Stärkung der Inneren Sicherheit (PSIS) beschlossen.[8] Das Programm sieht die Möglichkeit einer Online-Durchsuchung sowohl im präventiven als auch im repressiven Bereich vor. Durch die Haushaltsmittel sollten innerhalb der restlichen 16. Legislaturperiode operative sowie einsatz- und ermittlungstechnische Instrumentarien entwickelt werden.[9] Die Maßnahme der Online-Durchsuchung wurden im präventiven Bereich eingeführt, was gem. § 20k BKAG durch das Anknüpfen an das Vorliegen einer Gefahr deutlich wird.[10] Das BKA ist nach § 2 VI Nr. 3 BKAG Zentralstelle zur Unterstützung der Polizeien des Bundes und der Länder und damit für die Erforschung von polizeilichen Methoden und Arbeitsweisen der Kriminalitätsbekämpfung, dementsprechend auch für die Prüfung und Bewertung der Eignung von neuen technischen Verfahren zur Strafverfolgung, zuständig.[11] Die historische Entwicklung führte zur Diskussion über den Einsatz der Online-Durchsuchung und Quellen-TKÜ im repressiven Bereich und über die Schaffung von rechtlichen Grundlagen in der StPO. Außerdem hat auch der deutsche Richterbund bereits jahrelang diese Maßnahmen zur Strafverfolgung gefordert.[12]
Es haben keine besonderen Straftaten wie Terroranschläge zur kriminalpolitischen Entschließung eines Gesetzesentwurfs für Online-Durchsuchung und Quellen-TKÜ geführt.

[7] Vgl. Kohlmann, 2012, S. 21.
[8] BT-Drs. 16/3492, 21.11.06.
[9] BT-Drs. 16/3492, 21.11.06, S. 2.
[10] Vgl. Kohlmann, 2012, S. 22 f.
[11] Vgl. Kohlmann, 2012, S. 23.
[12] Vgl. Neuhaus, DRiZ 2017, 192 (192).

Vielmehr haben Praxiserfahrungen der Behörden, so die Auswertung einer Zusammenfassung des BKA zum Ermittlungserfolg der klassischen TKÜ, die weitgehende Wirkungslosigkeit dieser Maßnahme gezeigt.[13] Schlussendlich ist die fortschreitende Entwicklung der Informationstechnik der Entschließungsgrund gewesen. Intention des Gesetzgebers ist es, der Behinderung der Strafverfolgung vor allem bei schweren Straftaten durch technische Innovationen entgegenzuwirken.[14] Der technische Fortschritt bezieht sich in diesem Zusammenhang zum einen auf die Nutzung mobiler Geräte in Form von Smartphones und Tablet-PCs, die in der Gesellschaft, besonders in der jungen Bevölkerungsgruppe, zum Alltag gehören und deshalb die herkömmliche Art der Telekommunikation ersetzen.[15] Ein anderer Aspekt der Entwicklung ist die Form und Größe der Speichermedien anzuführen, wozu die Verbesserung der Kapazität der Arbeitsspeicher und die vermehrte Verwendung von externen Speichern wie Clouds zählen.[16] Außerdem bietet das Internet zahlreiche neue Möglichkeiten der Kommunikation wie z. B. soziale Netzwerke, Messenger-Dienste und Webforen, auf die sich die Fernkommunikation immer mehr verlagert.[17]

Der Koalitionsvertrag zwischen CDU, CSU und SPD für die 18. Legislaturperiode sieht innerhalb des fünften Kapitels „Moderner Staat, innere Sicherheit und Bürgerrechte“ unter dem Punkt „Freiheit und Sicherheit“ grundsätzlich eine effektive Strafverfolgung vor, die durch Vorschläge einer Expertenkommission ausgestaltet werden soll. Für die Quellen-TKÜ ist im Vertrag bereits eine rechtsstaatliche Präzisierung festgelegt.[18]

II. Gegenstand

Diskutiert werden im Gesetzgebungsverfahren die unter §§ 100a, 100b StPO neugefassten Rechtsgrundlagen für die Quellen-TKÜ und die Online-Durchsuchung. Bei der Online-Durchsuchung wird vom Staat verdeckt durch eine Überwachungssoftware auf fremde informationstechnische Systeme über Kommunikationsnetze zugegriffen.[19] Die Quellen-TKÜ stellt auch eine Infiltrierung eines fremden IT-Systems dar, bei der die

[13] Vgl. Neuhaus, DRiZ 2017, 192 (193).
[14] Vgl. Sinn, 2017, S. 1.
[15] Ausschuss-Drs. 18[6]361, 19.06.17, Artikel 3 Nummer 8 ff; BT-Drs. 18/12785, 20.06.17, S.46.
[16] Ausschuss-Drs. 18[6]361, 19.06.17, Artikel 3 Nummer 8 ff; BT-Drs. 18/12785, 20.06.17, S.46.
[17] Ausschuss-Drs. 18[6]361, 19.06.17, Artikel 3 Nummer 8 ff; BT-Drs. 18/12785, 20.06.17, S.46.
[18] Koalitionsvertrag, 18. Legislaturperiode, S. 146.
[19] Ausschuss-Drs. 18[6]361, 19.06.17, Artikel 3 Nummer 8 ff; BT-Drs. 18/12785, 20.06.17, S.46.

Überwachungssoftware aber für die Überwachung und Aufzeichnung der Kommunikation zwischen Beteiligten eingesetzt wird.[20] Zur Abgrenzung beider Maßnahmen ist auf die Ausrichtung abzustellen, die bei der Quellen-TKÜ ausschließlich auf die Erfassung laufender Kommunikation und im Rahmen der Online-Durchsuchung darüber hinaus auf einen Zugriff sämtlicher Inhalte eines Rechners abzielt.[21] Um den Begriff der laufenden Kommunikation zu verdeutlichen, wird in der Abb. 1 der Telekommunikationsvorgang dargestellt.

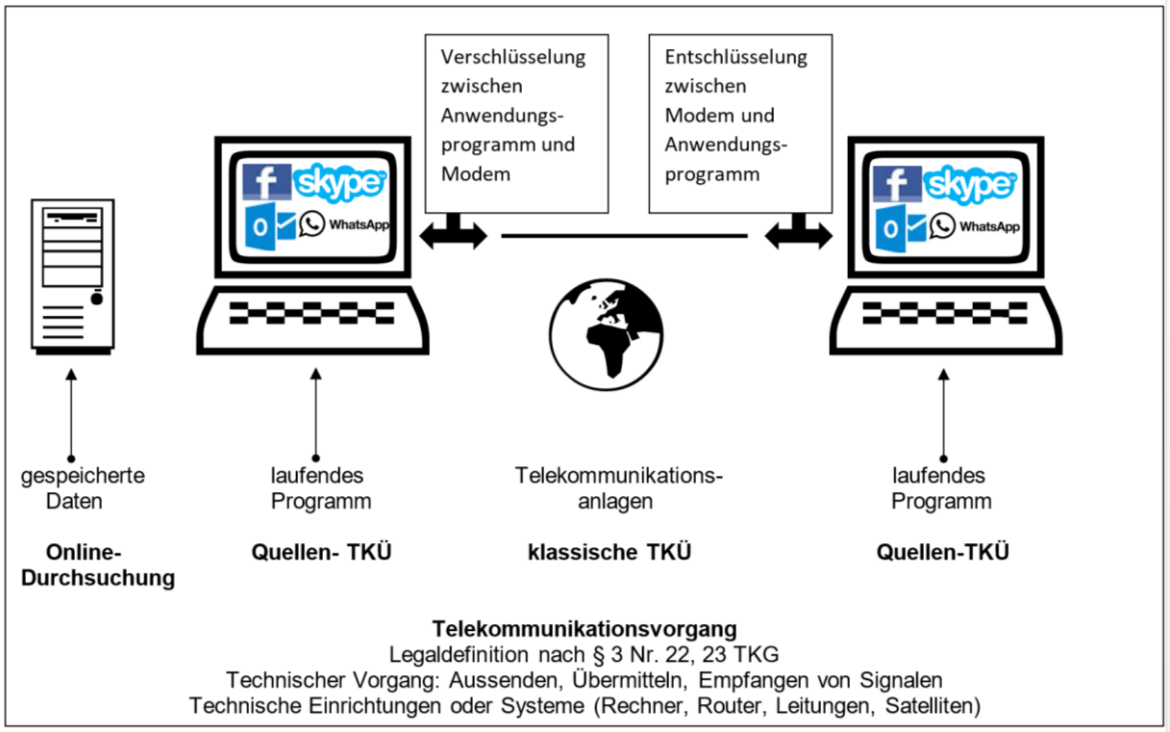

Abb. 1: Begriff Telekommunikationsvorgang, eigene Arbeit.

Der Telekommunikation i.S.d. § 100a StPO wird die Legaldefinition nach § 3 Nr. 22, 23 TKG zugrunde gelegt.[22] Demnach ist Telekommunikation „der technische Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache oder Tönen mittels technischer Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können“.[23] Somit wird unter der klassischen TKÜ der Übertragungsweg vom Verlassen der Signale am Modem des Senders über die Telekommunikationsanlagen der verschiedenen Anbieter bis hin zum

[20] Ausschuss-Drs. 18[6]361, 19.06.17, Artikel 3 Nummer 8 ff; BT-Drs. 18/12785, 20.06.17, S.46.
[21] Vgl. Tinnefeld, ZD 2012, 451 (454).
[22] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100a Rn. 6.
[23] Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100a Rn. 6.

Eingehen am Modem des Empfängers verstanden. Bei der Quellen-TKÜ setzt der Telekommunikationsvorgang früher ein, da der Beginn des Kommunikationsweges bereits im laufenden Anwendungsprogramm, das Outlook oder Skype sein kann, gesehen wird. Damit findet die Überwachung der Kommunikation bei dieser Maßnahme zu einem noch nicht verschlüsselten Zeitpunkt statt. Die Dauer des laufenden Kommunikationsvorgangs beim Sender fängt mit dem Starten des Programms an und geht über das Erfassen bzw. Sprechen der Nachricht. Das Ende liegt dann im Versenden der Daten. Für den Empfänger gilt analog das Starten des Programms als Beginn. Der Telekommunikationsvorgang umfasst auf dieser Seite das Herunterladen der Daten und endet mit dem Lesen oder Hören der Nachricht. Ab dem Zeitpunkt der Speicherung der Daten kann die Maßnahme der Quellen-TKÜ nur im Fall des § 100a I 3 StPO angewendet werden. Ansonsten liegt diese im Bereich der Online-Durchsuchung.

III. Ablauf

Die Regelungen zur Online-Durchsuchung und Quellen-TKÜ im repressiven Bereich sind Gegenstand mehrerer parlamentarischer Verfahren. In den ursprünglichen Gesetzesentwürfen der Bundesregierung vom 22.02.2017, die den Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze (BT-Drs. 18/11272) und den Entwurf eines Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens (BT-Drs. 18/11277) umfassen, waren beide Maßnahmen noch nicht erwähnt. Erst mit einem Änderungsantrag von CDU/CSU und SPD (Ausschussdrucksache 18[6]334 vom 15.05.2017) wurden im laufenden Gesetzgebungsverfahren die beiden Gesetzesentwürfe zusammengefasst und zusätzlich um den Einsatz von Spionagesoftware nach §§ 100a, 100b StPO nF erweitert.[24] Bei einer Sachverständigenanhörung im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages am 31.05.2017 wurden einige Kritikpunkte zum Gesetzesentwurf geäußert. Bei der Online-Durchsuchung wird bemängelt, dass der Einsatz des Staatstrojaners außerordentlich eingriffsintensiv ist und über die akustische Wohnraumüberwachung, die auch als „Großer Lauschangriff“ bezeichnet wird, hinausgeht.[25] Außerdem wird der Straftatenkatalog nach § 100b II StPO als zu weit

[24] Vgl. Beukelmann, NJW-Spezial 2017, 440 (440).
[25] Vgl. Buermeyer, 2017, S. 2.

gefasst angesehen.[26] Die Beschränkung auf die laufende Kommunikation bei der Quellen-TKÜ wird kritisch betrachtet, da dies aus technischer Sicht zeitlich schwer einschränkbar und deshalb die Abgrenzung zur Online-Durchsuchung unscharf ist.[27] Weiterhin bestehen Bedenken bezüglich der fehlenden Regelung zu den technischen Anforderungen an die Überwachungssoftware hinsichtlich der Datensicherheit und Resistenz gegen Manipulationsversuche.[28] Die Tatsache, dass der Staat zur Installation eines Staatstrojaners auch Sicherheitslücken ausnutzt und deshalb eventuell kein Interesse am Schließen dieser Lücken hat, führt zur einer „Kultur der kalkulierten IT-Unsicherheit".[29] Die Auswirkung nicht geschlossener Sicherheitslücken wird in der Stellungnahme mit dem Ausbruch des „wannacry"-Trojaners exemplarisch verdeutlicht. Des Weiteren werden die unzureichenden Regelungen zum Schutz von Berufsgeheimnisträgern wie Journalisten bemängelt.[30] Schließlich wird die Eilbedürftigkeit des Gesetzes angezweifelt.[31] Dennoch erreichte diese Kritik keinen Einfluss in die Beschlussempfehlung des Änderungsantrages der Bundesregierung mit den Beschlüssen des Ausschusses für Recht und Verbraucher (6. Ausschuss) vom 19.06.2017 (Ausschussdrucksache 18[6]361; BT-Drs. 18/12785). Eine Diskussion über das Für und Wider zwischen den Abgeordneten mit ähnlichen Argumenten geht aus dem Plenarprotokoll zur zweiten und dritten Beratung im Bundestag vom 22.06.2017 hervor. Trotz der scharfen Kritik von Sachverständigen hinsichtlich Art und Weise von Zustandekommen und Inhalt des Gesetzes hat der Bundestag den Gesetzentwurf in der Ausschussfassung am 22.06.2017 beschlossen.[32] Dem Bundesrat wurden vom Ausschuss für Agrarpolitik und Verbraucherschutz Empfehlungen (527/1/17) vorgelegt, die auf eine Streichung der Regelungen zur Online-Durchsuchung und Quellen-TKÜ mithilfe eines Vermittlungsausschusses gem. Art. 77 II GG abzielten. Bei der Empfehlung zur Entschließung wurden vom Ausschuss folgende Kritikpunkte angeführt: Fehlende Beteiligung der Länder bei diesen Regelungsbereichen, Eingriffstiefe und Auswirkungen auf den Kernbereich privater Lebensgestaltung sowie eine Vielzahl von zugänglichen personenbezogenen Daten, was umfangreiche Rückschlüsse über die Zielperson zulässt. Der federführende Rechtsausschuss des Bundesrates vertritt die gegensätzliche Meinung und empfiehlt, keinen Antrag gem. Art. 77 II GG zu stellen. Der Bundesrat hat sich dieser Seite angeschlossen und am 07.07.2017 mit

[26] Vgl. Buermeyer, 2017, S. 2.
[27] Vgl. Buermeyer, 2017, S. 2.
[28] Vgl. Buermeyer, 2017, S. 3.
[29] Vgl. Buermeyer, 2017, S. 3.
[30] Vgl. Buermeyer, 2017, S. 3.
[31] Vgl. Buermeyer, 2017, S. 3.
[32] Vgl. Beukelmann, NJW-Spezial 2017, 440 (440).

seinem Beschluss (BR-Drs. 527/17) das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens gebilligt. Zum Abschluss des formellen Gesetzgebungsverfahrens wurde das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens am 23.08.2017 im Bundesgesetzblatt verkündet.

C. Grundrechte

Welche Grundrechte von den repressiven Maßnahmen der Strafverfolgung betroffen sind, soll nun im Folgenden erläutert werden. Dazu wird dargestellt, wie der Schutzbereich der einschlägigen Grundrechte ausgestaltet ist, wie Eingriffe darin durch die Online-Durchsuchung und Quellen-TKÜ vorgenommen werden und wie diese gerechtfertigt werden können. Abb. 2 zeigt die Zusammenhänge von Maßnahmen und Grundrechten.

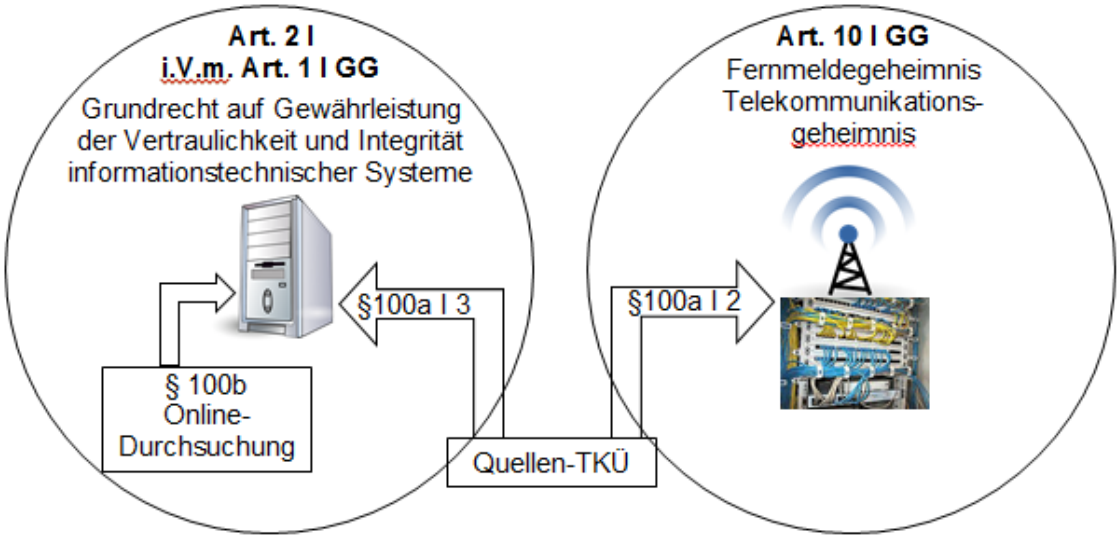

Abb. 2: Eingriff der Online-Durchsuchung und Quellen-TKÜ in die jeweiligen Grundrechte, eigene Arbeit.

Die Online-Durchsuchung nach § 100b StPO greift ausschließlich in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gem. Art. 2 I i.V.m. Art. 1 I GG ein. Die von der Quellen-TKÜ nach § 100a I 2 StPO betroffene Kommunikation liegt während der Übertragung im Schutzbereich des Fernmeldegeheimnisses aus Art. 10 I GG.[33] Die Kommunikationsinhalte befinden sich nach Abschluss des Übertragungsvorgangs im Herrschaftsbereich des Empfängers, welcher durch das Computergrundrecht nach Art. 2 I i.V.m. Art. 1 I GG geschützt ist.[34] Die Quellen-TKÜ in Form des § 100a I 3 StPO greift in dieses ein.[35]

[33] Vgl. Niederhuber, JA 2018, 169 (170).
[34] Vgl. Niederhuber, JA 2018, 169 (171).
[35] Vgl. Niederhuber, JA 2018, 169 (171).

I. Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gem. Art. 2 I i.V.m. Art. 1 I GG

Das aus Art. 2 I i.V.m. Art. 1 I GG abgeleitete allgemeine Persönlichkeitsrecht[36] unterteilt sich je nach besonderen Ausprägungen in spezielle unbenannte Freiheitsrechte, die aufgrund ihrer spezifischen Anforderungen an die Rechtfertigung von Eingriffen eigene Strukturen aufweisen.[37] Diese unbenannten Freiheitsrechte sind allerdings keine eigenständigen Grundrechte, sondern finden ihre normative Grundlage in Art. 2 I GG.[38] Das in verschiedenen Formen vorliegende allgemeine Persönlichkeitsrecht bestimmt sich inhaltlich aus der im Art. 1 I GG garantierten Menschenwürde.[39] Die für das allgemeine Persönlichkeitsrecht abgeleitete Verbindung von Art. 2 I mit Art. 1 I GG verstärkt den Schutz des Grundrechts und grenzt sich insoweit von der allgemeinen Handlungsfreiheit gem. Art. 2 I GG ab, indem es das Sein des Menschen und nicht nur sein Verhalten umfasst.[40] Durch die Unspezifizität des allgemeinen Persönlichkeitsrechts ist es möglich, den durch den wissenschaftlich-technischen Fortschritt entstehenden, neuartigen Gefahren für die Persönlichkeitsentfaltung zu begegnen und den Persönlichkeitsschutz an die wechselnden Bedingungen anzupassen.[41] Das BVerfG misst der Nutzung informationstechnischer Systeme eine zunehmende Bedeutung für die Persönlichkeitsentfaltung bei und sieht deshalb eine besondere Schutzbedürftigkeit vor allem für Computer vor.[42] Was früher nicht absehbar war, hat durch die Fortentwicklung besondere Ausmaße angenommen. Durch die Vernetzung von IT-Systemen haben Dritte Zugriff zum Ausspähen und Manipulieren von Daten, die bewusst oder automatisch erzeugt und gespeichert werden.[43] Anhand dieser Daten können die Eigenschaften und das Verhalten des Nutzers so detailliert eingesehen werden, dass letztlich sogar die Erstellung eines Persönlichkeitsprofils möglich ist.[44] Diese Entwicklung erfordert eine neue Ausprägung des allgemei-

[36] BVerfGE 54, 148 (153).
[37] Vgl. Murswiek/Rixen in: Sachs, 2018, Art. 2 Rn. 65.
[38] Vgl. Murswiek/Rixen in: Sachs, 2018, Art. 2 Rn. 65.
[39] Vgl. Murswiek/Rixen in: Sachs, 2018, Art. 2 Rn. 62.
[40] Vgl. Murswiek/Rixen in: Sachs, 2018, Art. 2 Rn. 62.
[41] Vgl. Murswiek/Rixen in: Sachs, 2018, Art. 2 Rn. 66.
[42] Vgl. Jarass in: Jarass/Pieroth, 2018, Art. 2 Rn. 37a.
[43] Vgl. Murswiek/Rixen in: Sachs, 2018, Art. 2 Rn. 73c.
[44] Vgl. Murswiek/Rixen in: Sachs, 2018, Art. 2 Rn. 73c.

nen Persönlichkeitsrechts, die das BVerfG im Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme formuliert.[45] Dieses bezeichnet man auch als Computergrundrecht.[46]

1. Schutzbereich des Computergrundrechts

Um den Schutzbereich des Computergrundrechts besser zu verstehen, ist es wichtig, zunächst einen Blick auf das geschützte Verhalten nach Art. 2 I i.V.m. 1 I GG im Allgemeinen zu werfen. Das allgemeine Persönlichkeitsrecht gewährleistet den Schutz der privaten Lebensgestaltung zur autonomen Entfaltung und Wahrung der personalen und sozialen Identität.[47] Der Schutzbereich gem. Art. 2 I i.V.m. Art. 1 I GG umfasst verschiedene Gebiete. Neben dem Schutz der Ehre, dem Recht am eigenen Bild bzw. Wort und der informationellen Selbstbestimmung des Einzelnen gibt es den Schutzbereich des Computergrundrechts, welcher für die Online-Durchsuchung und Quellen-TKÜ von Bedeutung ist. Der Schutzbereich des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme erstreckt sich sowohl auf die genutzten Geräte als auch auf die gespeicherten Daten an sich. Zu den Systemen zählen neben dem Personalcomputer auch informationstechnische Komponenten in Telekommunikationsgeräten und weitere elektronische Geräte einschließlich ihrer technischen Vernetzungen.[48] Für die Schutzbedürftigkeit dieser genannten Geräte ist es außerdem maßgeblich, dass sie personenbezogene Daten des Nutzers beinhalten, die bei einem Zugriff auf die Lebensgestaltung und das Persönlichkeitsbild des Betroffenen schließen lassen.[49] Persönliche Daten auf externen Servern sind ebenfalls vom Schutzbereich umfasst.[50] Es geht beim Schutzbereich des Computergrundrechts also um die Vertraulichkeit der erzeugten, verarbeiteten und gespeicherten Daten sowie die Integrität der Systeme.[51] Dabei tritt der Schutz der Vertraulichkeit der Daten hinter dem Integritätsschutz informationstechnischer Systeme zurück, da das informationelle Selbstbestimmungsrecht Zweifel an der Notwendigkeit eines eigenständigen Computergrundrechts aufkommen lässt und die überwiegende Bedeutung dem grundrechtlichen Schutz gegen Ausspähen, Überwachung oder Manipulation der Systeme zukommt.[52] Als Erweiterung zu dem real-räumlichen

[45] BVerfGE 120, 274 Rn. 166 ff.
[46] Vgl. Murswiek/Rixen in: Sachs, 2018, Art. 2 Rn. 73c, 73d.
[47] Vgl. Jarass in: Jarass/Pieroth, 2018, Art. 2 Rn. 39.
[48] Vgl. Jarass in: Jarass/Pieroth, 2018, Art. 2 Rn. 46; BVerfGE 120, 274 Rn. 172 ff.
[49] Vgl. Murswiek/Rixen in: Sachs, 2018, Art. 2 Rn. 73c.
[50] Vgl. Jarass in: Jarass/Pieroth, 2018, Art. 2 Rn. 46.
[51] Vgl. Murswiek/Rixen in: Sachs, 2018, Art. 2 Rn. 73c.
[52] Vgl. Murswiek/Rixen in: Sachs, 2018, Art. 2 Rn. 73d.

Schutzbereich in Art. 13 I GG schützt die Ausprägung von Art. 2 I i.V.m. Art. 1 I GG zudem einen virtuell-informationstechnischen Bereich freier Persönlichkeitsentfaltung.[53] Verschafft sich ein Dritter große und aussagekräftige Datenbestände durch einen Zugriff auf IT-Systeme ohne die Nutzung von Datenerhebungs- und Datenverarbeitungsmaßnahmen, geht diese Vorgehensweise in ihrer Intensität weit über das Recht auf informationelle Selbstbestimmung hinaus.[54]

2. Eingriff in Art. 2 I i.V.m. Art. 1 I GG

Grundsätzlich wird beim allgemeinen Persönlichkeitsrecht, das die Integrität als konkreten Schutzgegenstand beinhaltet, ein weiter Eingriffsbegriff angenommen.[55] Belastende rechtliche Regelungen stellen somit Eingriffe in Art. 2 I i.V.m. Art. 1 I GG dar.[56] In den oben beschriebenen Schutzbereich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme kann ein Eingriff vorgenommen werden, bei dem das Grundrecht beeinträchtigt wird. Ein solcher Eingriff liegt vor, wenn ein Zugriff auf erzeugte, verarbeitete oder gespeicherte Daten eines Systems durch einen Dritten stattfindet.[57] Die Berührung der Integrität im Fall einer Nutzung von Leistungen, Funktionen und Speicherinhalten eines Systems durch einen Dritten ist eine weitere Form eines Eingriffs in den Schutzbereich.[58] Es kommt beim Eingriff in das Computergrundrecht nicht darauf an, ob das IT-System nach seiner Infiltration tatsächlich überwacht wird.[59] Mit der Schaffung von Überwachungsmöglichkeiten durch das Installieren des Bundestrojaners ist bereits die Hürde für ein Ausspähen des Zielsystems erreicht.[60] Charakteristisch für den Eingriff ist der heimliche Zugriff auf informationstechnische Systeme.[61] Außerdem stellt die Verwendung von Daten, die in einem Gerichtsverfahren erhoben werden, einen Eingriff in Art. 2 I i.V.m. Art. 1 I GG dar.[62] Dies trifft auf die Erlangung von Daten bei der Online-Durchsuchung und Quellen-TKÜ zu.

[53] Vgl. Murswiek/Rixen in: Sachs, 2018, Art. 2 Rn. 73d.
[54] BT-Drs. 18/12785, 20.06.17, S. 54; BVerfGE 120, 274 Rn. 200.
[55] Vgl. Murswiek/Rixen in: Sachs, 2018, Art. 2 Rn. 84.
[56] Vgl. Jarass in: Jarass/Pieroth, 2018, Art. 2 Rn. 53.
[57] Vgl. Murswiek/Rixen in: Sachs, 2018, Art. 2 Rn. 88c; BVerfGE 120, 274 Rn. 204.
[58] Vgl. Murswiek/Rixen in: Sachs, 2018, Art. 2 Rn. 88c; BVerfGE 120, 274 Rn. 204.
[59] Vgl. Tinnefeld, ZD 2012, 451 (453).
[60] Vgl. Tinnefeld, ZD 2012, 451 (453). BVerfGE 120, 274 Rn. 188.
[61] Vgl. Jarass in: Jarass/Pieroth, 2018, Art. 2 Rn. 53.
[62] Vgl. Jarass in: Jarass/Pieroth, 2018, Art. 2 Rn. 53a.

3. Rechtfertigung nach Art. 2 I i.V.m. Art. 1 I GG

Grundlage für die Rechtfertigung von Eingriffen in das allgemeine Persönlichkeitsrecht sind die Schranken des Art. 2 I GG.[63] Diese Schranken werden als Schrankentrias bezeichnet, weil sie sich in drei Bereiche, die die verfassungsmäßige Ordnung, die Rechte anderer und das Sittengesetz darstellen, gliedern.[64] Allerdings hat die Schranke des Sittengesetzes keine praktische Bedeutung im Rechtsstaat, da ein Verstoß dagegen immer auch ein Verstoß gegen die unantastbare Menschenwürde nach Art. 1 I GG ist.[65] Somit wird aus der Schrankentrias ein Schrankenduo. Wegen des Inhalts des allgemeinen Persönlichkeitsrechts können Verstöße sowohl gegen das Sittengesetz als auch gegen Rechte Dritter ausgeschlossen werden.[66] Folglich stützt sich die Rechtfertigung von Eingriffen insbesondere auf die Schranke der verfassungsmäßigen Ordnung.[67] Ein passender Begriff wäre somit das Schrankensolo.

Zur Schranke der verfassungsmäßigen Ordnung gehören alle formellen und materiellen Gesetze, also die verfassungsmäßige Rechtsordnung.[68] Es handelt sich dabei um einen einfachen Gesetzesvorbehalt, bei dem Eingriffe einer speziellen gesetzlichen Grundlage bedürfen.[69] Im Fall der Online-Durchsuchung und Quellen-TKÜ stellen §§ 100b, 100a StPO die gesetzliche Grundlage dar. Dabei muss das entsprechende Gesetz die Voraussetzungen und den Umfang der Beeinträchtigung je nach Grad der erforderlichen Bestimmtheit von Art und Schwere des Eingriffs hinreichend klar regeln.[70] Ermächtigungen müssen Normenklarheit und -bestimmtheit bei informationstechnischen Systemen erfüllen.[71] Zu diesem Zweck enthalten §§ 100a, 100b StPO Straftatenkataloge, die die Fälle, bei denen die Maßnahmen angeordnet werden darf, bestimmen.

Die Rechtfertigung von Eingriffen beruht zudem auf dem Verhältnismäßigkeitsgrundsatz. Verhältnismäßigkeit liegt vor, wenn ein legitimer Zweck mit geeigneten, erforderlichen und angemessenen Mitteln erreicht wird.[72] Dies ist stets strikt zu prüfen.[73] Bei der Abwägung der Erforderlichkeit darf es kein gleich geeignetes, aber milderes Mittel geben, um den geforderten Zweck zu erreichen. Hierfür ist in §§ 100a I 1 Nr. 3, 100b I

[63] Vgl. Jarass in: Jarass/Pieroth, 2018, Art. 2 Rn. 58.
[64] Vgl. Murswiek/Rixen in: Sachs, 2018, Art. 2 Rn. 89 – 99.
[65] Vgl. Murswiek/Rixen in: Sachs, 2018, Art. 2 Rn. 99.
[66] Vgl. Murswiek/Rixen in: Sachs, 2018, Art. 2 Rn. 103.
[67] Vgl. Jarass in: Jarass/Pieroth, 2018, Art. 2 Rn. 58; BVerfGE 106, 28 (48); 117, 202 (227).
[68] BVerfGE 96, 10 (21); 90, 145 (171 f.); 103, 197 (215).
[69] Vgl. Jarass in: Jarass/Pieroth, 2018, Art. 2 Rn. 58.
[70] Vgl. Jarass in: Jarass/Pieroth, 2018, Art. 2 Rn. 59.
[71] Vgl. Jarass in: Jarass/Pieroth, 2018, Art. 2 Rn. 59.
[72] BVerfGE 115, 320 (345).
[73] Vgl. Jarass in: Jarass/Pieroth, 2018, Art. 2 Rn. 62.

Nr. 3 StPO jeweils eine Subsidiaritätsklausel enthalten. Danach darf die Maßnahme der Online-Durchsuchung nur angeordnet werden, wenn sie die ultima ratio ist, was bedeutet, dass andere Ermittlungsmaßnahmen gänzlich versagen.[74] Der heimliche Zugriff auf IT-Systeme, der als Eingriff belastender ist als ein offener, erfordert laut BVerfG im Fall der präventiven Maßnahmen tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut.[75] Zu diesen Rechtsgütern zählen „Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt".[76] Im Hinblick auf repressive Maßnahmen ist das Gewicht der verfolgten Straftat entscheidend.[77] Hierzu ist im Straftatenkatalog des § 100b II StPO eine Vielzahl von Delikten aufgezählt, bei denen die für den Verhältnismäßigkeitsgrundsatz geforderte Zwecklimitierung fraglich ist.[78] So ist unter § 100b II Nr. 2 a StPO das Verleiten zur missbräuchlichen Asylantragstellung gem. § 84 III AsylG aus dem Bereich der strafrechtlichen Nebengesetze als Beispiel anzuführen.[79] Das heimliche Aktivieren von Kamera- oder Mikrofonfunktionen in Computern oder Smartphones ist zwar ein Eingriff in ein informationstechnisches System, aber der Wortlaut des § 100b I StPO als gesetzliche Grundlage deckt diese Maßnahme ohnehin nicht, da nur Daten „daraus", also aus dem Zielsystem, erhoben werden dürfen.[80] Zudem verdeutlicht der Begriff „Durchsuchung", dass von Daten passiv Kenntnis genommen werden soll und nicht Funktionen aktiviert werden dürfen, die einem Live-Zugriff gleichkommen.[81] Das Aktivieren von Mikrofon und Kamera stellt außerdem eine ständige Überwachung dar, was einem unzulässigen Spähangriff auf einen Wohnraum entspricht und unter Art. 13 GG fällt.[82]

II. Fernmeldegeheimnis gem. Art. 10 I GG

Bezieht sich die Quellen-TKÜ ausschließlich auf Daten aus einem laufenden Übertragungsvorgang, beurteilt sich die Ermächtigungsgrundlage aus § 100a StPO nach dem Grundrecht des Fernmeldegeheimnisses gem. Art. 10 I GG.[83] Das Fernmeldegeheimnis,

[74] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100b Rn. 6.
[75] Vgl. Jarass in: Jarass/Pieroth, 2018, Art. 2 Rn. 62; BVerfGE 120, 274 Rn. 247.
[76] Stoklas/Wendorf, ZD-Aktuell 2017, 05725; BVerfGE 120, 274, Leitsätze Nr. 2.
[77] Vgl. Stoklas/Wendorf, ZD-Aktuell 2017, 05725.
[78] Vgl. Stoklas/Wendorf, ZD-Aktuell 2017, 05725.
[79] Vgl. Stoklas/Wendorf, ZD-Aktuell 2017, 05725.
[80] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100b Rn. 2.
[81] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100b Rn. 2.
[82] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100b Rn. 2.
[83] Vgl. Roggan, StV 2017, 821 (821).

auch bekannt als Telekommunikationsgeheimnis, ist gegenüber Art. 2 I GG sowie im Verhältnis zum allgemeinen Persönlichkeitsrecht lex specialis.[84] Somit hat Art. 10 I GG in den einschlägigen Fällen Vorrang vor dem allgemeinen Persönlichkeitsrecht gem. Art. 2 I i.V.m. Art. 1 I GG. Das Fernmeldegeheimnis und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme stehen aber grundsätzlich nicht gegenseitig in Konkurrenz. Das aus dem allgemeinen Persönlichkeitsrecht abgeleitete Computergrundrecht soll eine Schutzlücke schließen, die dadurch entsteht, dass Art. 10 I GG nur die laufende Kommunikation betrifft, nicht aber gespeicherte Inhalte nach Abschluss eines Kommunikationsvorgangs.[85]
Im Art. 10 I GG sind neben dem Fernmeldegeheimnis auch das Briefgeheimnis und das Postgeheimnis geregelt, die zusammen ein einheitliches Grundrecht bilden.[86] Das Fernmeldegeheimnis gem. Art. 10 I GG dient dem Schutz einer vertraulichen, individuellen Kommunikation, die aufgrund einer räumlichen Distanz nicht direkt zwischen den Beteiligten erfolgt, sondern die Übermittlung durch Zuhilfenahme Dritter erfordert.[87] Dieses Grundrecht bildet eine Grundlage für den Schutz der Privatsphäre.[88]

1. Schutzbereich des Art. 10 I GG

Vom Schutzbereich des Telekommunikationsgeheimnisses umfasst sind Kommunikationsinhalte, die mündlich oder schriftlich wie per Telefon, Skype oder E-Mail ausgetauscht werden.[89] Der Informations- und Gedankenaustausch kann sich sowohl auf den privaten, geschäftlichen als auch politischen Bereich erstrecken.[90] Zum Schutzbereich des Fernmeldegeheimnisses gehören außerdem Informationen darüber, ob, wann, wie oft und zwischen wem Kommunikation stattfindet oder versucht wird.[91] Das Grundrecht nach Art. 10 I GG schützt jede unkörperliche Übermittlung basierend auf jedweder Übertragungstechnik.[92] Die Übertragung kann über Kabel oder Funk, analog oder digital, durch optische, akustische oder elektromagnetische Signale erfolgen.[93] Umfasst sind folglich alle Formen der Kommunikation wie Telefon, Telefax, Computernetze, SMS

[84] Vgl. Pagenkopf in: Sachs, 2018, Art. 10 Rn. 52; Jarass in: Jarass/Pieroth, 2018, Art. 10 Rn. 2.
[85] Vgl. Pagenkopf in: Sachs, 2018, Art. 10 Rn. 53; BVerfGE 115, 166 (183).
[86] Vgl. Jarass in: Jarass/Pieroth, 2018, Art. 10 Rn. 1.
[87] Vgl. Jarass in: Jarass/Pieroth, 2018, Art. 10 Rn. 1.
[88] Vgl. Jarass in: Jarass/Pieroth, 2018, Art. 10 Rn. 1; BVerfGE 85, 386 (395 f.).
[89] Vgl. Pagenkopf in: Sachs, 2018, Art. 10 Rn. 14.
[90] Vgl. Pagenkopf in: Sachs, 2018, Art. 10 Rn. 14.
[91] Vgl. Pagenkopf in: Sachs, 2018, Art. 10 Rn. 14.
[92] Vgl. Pagenkopf in: Sachs, 2018, Art. 10 Rn. 14a; Jarass in: Jarass/Pieroth, 2018, Art. 10 Rn. 3.
[93] Vgl. Pagenkopf in: Sachs, 2018, Art. 10 Rn. 14a; Jarass in: Jarass/Pieroth, 2018, Art. 10 Rn. 3.

oder Internet.[94] Aufgrund des technischen Fortschritts, der immer wieder neue Kommunikationsmöglichkeiten mit sich bringt, ist der Schutzbereich des Fernmeldegeheimnisses entwicklungsoffen und in einem dynamischen Verständnis gefasst.[95] Der Schutz des Art. 10 I GG ist beschränkt auf die Kommunikation zwischen einzelnen individuellen Personen bzw. -gruppen.[96] Ausgenommen vom Fernmeldegeheimnis sind eine an die Allgemeinheit oder an einen unbestimmten Personenkreis gerichtete Kommunikation wie an jedermann adressierte Inhalte im Internet.[97] Räumlich ist der Schutzbereich des Art. 10 I GG davon abhängig, dass die Aufzeichnung und Überwachung der Kommunikation sowie deren Auswertung in Deutschland erfolgt.[98] In diesem Fall sind sowohl der deutsche als auch der ausländische Kommunikationsteilnehmer vom Grundrecht des Fernmeldegeheimnisses geschützt.[99] Das Fernmeldegeheimnis stellt ein subjektiv öffentliches Recht dar, das als Abwehrrecht ausschließlich gegen den Staat ausgerichtet ist und damit nur die öffentliche Gewalt adressiert ist.[100]

2. Eingriff in Art. 10 I GG

Ein Eingriff in das Fernmeldegeheimnis gem. Art. 10 I GG liegt vor, wenn kommunikative Daten durch einen Grundrechtsverpflichteten erlangt, aufgezeichnet und verwertet werden.[101] Außerdem ist ein Eingriff gegeben, wenn an der Internetkommunikation durch Überwachung zugangsgesicherter Inhalte unautorisiert teilgenommen wird.[102] Dazu müssen die staatlichen Stellen zuvor den betroffenen technischen Zugangsschlüssel gegen oder ohne den Willen der Kommunikationsberechtigten erlangen, z.B. durch Keylogging.[103] Die Maßnahme der Quellen-TKÜ findet heimlich statt, sodass der Betroffene kein Einverständnis geben kann und somit ein Eingriff vorliegt. Des Weiteren stellt die Speicherung der Kommunikation und die daran angeschlossene Informations- und Datenverarbeitung einen Eingriff dar.[104] Da dies bei der Quellen-TKÜ zum notwendigen Prozess gehört, fällt diese Maßnahme unter die Eingriffe.

[94] Vgl. Pagenkopf in: Sachs, 2018, Art. 10 Rn. 14a; Jarass in: Jarass/Pieroth, 2018, Art. 10 Rn. 3.
[95] Vgl. Pagenkopf in: Sachs, 2018, Art. 10 Rn. 6a; Jarass in: Jarass/Pieroth, 2018, Art. 10 Rn. 3.
[96] Vgl. Pagenkopf in: Sachs, 2018, Art. 10 Rn. 14a; Jarass in: Jarass/Pieroth, 2018, Art. 10 Rn. 4.
[97] Vgl. Pagenkopf in: Sachs, 2018, Art. 10 Rn. 14b; Jarass in: Jarass/Pieroth, 2018, Art. 10 Rn. 4.
[98] Vgl. Jarass in: Jarass/Pieroth, 2018, Art. 10 Rn. 5.
[99] Vgl. Pagenkopf in: Sachs, 2018, Art. 10 Rn. 15.
[100] Vgl. Pagenkopf in: Sachs, 2018, Art. 10 Rn. 16.
[101] Vgl. Jarass in: Jarass/Pieroth, 2018, Art. 10 Rn. 11; BVerfGE 124, 43 (58); 125, 260 (310).
[102] Vgl. Pagenkopf in: Sachs, 2018, Art. 10 Rn. 10a.
[103] Vgl. Pagenkopf in: Sachs, 2018, Art. 10 Rn. 10a; BVerfGE 120, 274 Rn. 292.
[104] Vgl. Jarass in: Jarass/Pieroth, 2018, Art. 10 Rn. 11; BVerfGE 100, 313 (359, 366).

3. Rechtfertigung gem. Art. 10 II GG

Gerechtfertigt sind Eingriffe in das Telekommunikationsgeheimnis durch eine formellgesetzliche Ermächtigung, die sich sowohl aus einem förmlichen Gesetz, aber auch aus Rechtsverordnungen ergeben kann.[105] Art. 10 II GG sieht als Schranke des Grundrechts somit einen Gesetzesvorbehalt vor.[106] Zur Rechtfertigung von Eingriffen in Art. 10 I GG durch die repressive Maßnahme des § 100a StPO bedarf es einfachgesetzlicher und sich daraus hinreichend konkret ergebender softwaremäßiger Bedingungen, die die Quellen-TKÜ unter identischen Voraussetzungen und mit dem gleichen Straftatenkatalog der klassischen TKÜ erlauben.[107] Die einfachgesetzlichen Regelungen zur Spionagesoftware im Hinblick darauf, welche Software eingesetzt und welche spezifischen Kriterien für die Zuverlässigkeit der Beweiserhebung erfüllt werden, sind verfassungsrechtlich zu präzisieren und zu konkretisieren.[108]

Ein Grundrechtseingriff ist zudem nur zulässig, wenn ein legitimer Gemeinwohlzweck verfolgt wird.[109] Die repressive Strafverfolgung bei der Quellen-TKÜ nach § 100a StPO ist ein legitimer Zweck, der der Allgemeinheit dient. Erhobene Daten auf Vorrat zu einem unbestimmten Zweck zu speichern, ist nicht erlaubt.[110] Der Eingriff in das Fernmeldegeheimnis, der sowohl als einschränkendes Gesetz aber auch in jeder Maßnahme im Einzelfall vorliegt, muss verhältnismäßig sein.[111] Außerdem soll die Erhebung unnötiger Informationen vermieden werden.[112] Der Verhältnismäßigkeitsgrundsatz bedeutet, dass die Maßnahme geeignet, erforderlich und angemessen sein muss. Dem Kriterium der Erforderlichkeit trägt die Quellen-TKÜ mit ihrem in § 100a I 1 Nr. 3 StPO geregelten Subsidiaritätsgrundsatz Rechnung. Hiernach darf die Überwachung nur durchgeführt werden, wenn sie zur Erforschung des Sachverhalts unentbehrlich ist oder andernfalls die Aufklärung wesentlich erschwert würde.[113] Bei der Abwägung der wesentlichen Erschwernis werden Faktoren wie erheblich größerer Zeitaufwand, damit verbundene Verfahrensverzögerung und ein größerer Arbeitsaufwand, nicht jedoch der Kostenaufwand einbezogen.[114] Bei verschlüsselten Kommunikationsübertragungen ist die Quellen-

[105] Vgl. Jarass in: Jarass/Pieroth, 2018, Art. 10 Rn. 16.
[106] Vgl. Jarass in: Jarass/Pieroth, 2018, Art. 10 Rn. 16.
[107] Vgl. Roggan, StV 2017, 821 (821).
[108] Vgl. Roggan, StV 2017, 821 (824).
[109] Vgl. Jarass in: Jarass/Pieroth, 2018, Art. 10 Rn. 20.
[110] Vgl. Jarass in: Jarass/Pieroth, 2018, Art. 10 Rn. 20.
[111] Vgl. Jarass in: Jarass/Pieroth, 2018, Art. 10 Rn. 21.
[112] Vgl. Jarass in: Jarass/Pieroth, 2018, Art. 10 Rn. 22; BVerfGE 124, 43 (67).
[113] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100a Rn. 13.
[114] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100a Rn. 13.

TKÜ gegenüber der klassischen TKÜ nicht subsidiär, da die Entschlüsselung der Daten einen sehr hohen Zeitaufwand mit sich bringt oder eventuell gar nicht zum Ziel führt.[115]

[115] Vgl. Niederhuber, JA 2018, 169 (170).

D. Straftatenkataloge

In den §§ 100a II, 100b II StPO sind Kataloge mit Straftaten legal definiert, für die die Maßnahmen der Quellen-TKÜ und Online-Durchsuchung angeordnet werden dürfen.

I. Straftatenkatalog Quellen-TKÜ

Gem. § 100a I 1 StPO sind die Voraussetzungen für die Überwachung und Aufzeichnung der Telekommunikation der Tatverdacht (Nr. 1), der konkrete Einzelfall (Nr. 2) sowie der Subsidiaritätsgrundsatz (Nr. 3). Es ist weder ein hinreichender Tatverdacht i.S.d. § 203 StPO noch ein dringender Tatverdacht i.S.d. § 112 I 1 StPO erforderlich.[116] Ein Anfangsverdacht ist somit ausreichend. Dieser darf jedoch nicht unerheblich und muss hinreichend konkret sein, was bedeutet, dass bestimmte Tatsachen vorliegen müssen, die unmittelbar den Verdacht einer Katalog- oder Vorbereitungstat begründen.[117] Vage Anhaltspunkte und bloße Vermutungen sind demnach nicht vom Tatverdacht umfasst.[118]
Gem. § 100a I 1 Nr. 1, 2 StPO bezieht sich die Quellen-TKÜ nur auf schwere Straftaten, auf die sich der Tatverdacht und der konkrete Einzelfall stützen. Die Maßnahme liegt in ihrer Einordnung aufgrund der Eingriffsintensität zwischen den besonders schweren Straftaten der Wohnraumüberwachung nach § 100c I Nr. 1 StPO und den Straftaten von erheblicher Bedeutung bei den verdeckten Ermittlungsmaßnahmen nach §§ 98a ff. StPO.[119] Bei schweren Straftaten stellt der Regelstrafrahmen auf die Obergrenze mit mindestens fünf Jahren ab, in Einzelfällen aber auch auf oberhalb eines Jahres oder weniger bei geschützten Rechtsgütern mit besonderer Bedeutung oder besonderem öffentlichen Interesse nach Einschätzung des Gesetzgebers.[120] In den Katalogstraftaten gem. § 100a II StPO hat der Gesetzgeber diese verschiedenen Strafrahmen im Einzelnen abstrakt bewertet.[121] Darunter fallen unter anderem Mord und Totschlag nach §§ 211, 212 StGB (§ 100a II Nr. 1 h StPO), Straftaten des Raubes und der Erpressung nach §§ 249 bis 255 StGB (§ 100a II Nr. 1 k StPO) sowie Betrug und Computerbetrug unter den Voraussetzungen nach § 263 III 2, V StGB i.V.m. § 263a II StGB.

[116] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100a Rn. 9.
[117] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100a Rn. 9.
[118] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100a Rn. 9.
[119] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100a Rn. 10.
[120] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100a Rn. 10.
[121] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100a Rn. 10.

Für den konkreten Einzelfall, bei dem eine schwere Straftat nicht nur abstrakt angezeigt ist, müssen Anhaltspunkte wie Folgen der Tat, Schutzwürdigkeit des verletzten Rechtsguts oder besondere Umstände vorliegen.[122] Dazu zählen z. B. die faktische Verzahnung mit anderen Katalogstraftaten oder das Zusammenwirken des Beschuldigten mit anderen Straftätern.[123] Eine schwere Straftat i.S.d. § 100a II StPO kann als solche bewertet werden, auch wenn ein minder schwerer Fall wie etwa nach § 176a IV StGB, der gem. § 100a II Nr. 1 f StPO als Katalogstraftat aufgeführt ist, vorliegt.[124]
Der Straftatenkatalog nach § 100a II StPO umfasst in den Nr. 1 bis 11 neben dem StGB, BtMG und Völkerstrafgesetzbuch auch Abgabenordnung, Anti-Doping-Gesetz, Asylgesetz, Aufenthaltsgesetz, Außenwirtschaftsgesetz, Grundstoffüberwachungsgesetz, Gesetz über die Kontrolle von Kriegswaffen, Neue-psychoaktive-Stoffe-Gesetz sowie das Waffengesetz. Eine Erweiterung der ausgewählten Katalogtaten ist nicht möglich und kann auch nicht auf eine Notstandsituation nach § 34 StGB gestützt werden.[125]

II. Straftatenkatalog Online-Durchsuchung

Wie bei der Quellen-TKÜ ist für den Eingriff in informationstechnische Systeme und die Datenerhebung mittels der Online-Durchsuchung auch der Tatverdacht, der konkrete Einzelfall und die Subsidiaritätsklausel nach § 100b I Nr. 1 – 3 StPO erforderlich. Im Gegensatz zu § 100a I, II StPO ist die Anordnung der Online-Durchsuchung nicht auf schwere, sondern auf besonders schwere Straftaten gem. § 100b I, II StPO beschränkt. Aufgrund der stärkeren Eingriffsintensität der Online-Durchsuchung im Vergleich zur Quellen-TKÜ ergeben sich höhere Anforderungen an die Voraussetzungen des Tatverdachts nach § 100b I Nr. 1 StPO. Es muss ein über den Anfangsverdacht hinausgehender qualifizierter Tatverdacht vorliegen, der sich aus konkreten und in gewissem Umfang verdichteten Umständen für eine ausreichende Tatsachengrundlage zur Begründung einer Katalogtat ergibt.[126] Die Prüfung, ob eine besonders schwere Straftat im konkreten Einzelfall gem. § 100b I Nr. 2 StPO vorliegt, erfolgt weder nach abstrakter noch nach schematischer Betrachtung, sondern unter Berücksichtigung der Umstände, die bereits

[122] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100a Rn. 11.
[123] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100a Rn. 11.
[124] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100a Rn. 11.
[125] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100a Rn. 15.
[126] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100b Rn. 4.

für die Quellen-TKÜ erläutert und um die Tatausführung erweitert sind.[127] Die im Straftatenkatalog des § 100b II StPO legal definierten besonders schweren Straftaten sind dem der Wohnraumüberwachung gem. § 100c II StPO aF nachgebildet[128], ersetzen diesen und gelten nunmehr für §§ 100b I Nr.1, 100c I Nr. 1 StPO. Das für die Straftaten in § 100b II StPO vorgesehene Höchstmaß ist eine Freiheitsstrafe von mehr als fünf Jahren[129] ohne Ausnahmen, deren Strafrahmen unter dieser Obergrenze liegen. Die in § 100b II Nr. 1 – 7 StPO enumerativ aufgeführten Straftaten stammen sowohl aus dem StGB als auch aus dem Asylgesetz, Aufenthaltsgesetz, BtMG, Gesetz über die Kontrolle von Kriegswaffen, Völkerstrafgesetzbuch sowie Waffengesetz.

III. Vergleich der Straftatenkataloge aus §§ 100a II, 100b II StPO

Unterschiede zwischen der Online-Durchsuchung und der Quellen-TKÜ liegen nicht in der Methodik, da beide Maßnahmen den „Einsatz technischer Mittel“ regeln, sondern allein im Umfang der erhobenen Daten.[130] Die auf dem Erfassungsmaß der jeweiligen Maßnahme beruhende Eingriffsintensität gebietet unterschiedliche Straftatenkataloge. Der Straftatenkatalog des § 100a II StPO mit der neuen Möglichkeit der Quellen-TKÜ umfasst den kompletten, umfangreichen Katalog der herkömmlichen TKÜ, der vorher schon in § 100a StPO aF enthalten gewesen ist.[131] Im Gegensatz zu § 100a II StPO enthält der Straftatenkatalog des § 100b II StPO nur besonders schwere Straftaten und entspricht dem der akustischen Wohnraumüberwachung nach § 100c I Nr. 1 StPO.[132] Die Abb. 3 gibt einen Gesamtüberblick über die Straftaten aus beiden Katalogen der §§ 100a II, 100b II StPO untergliedert nach den Gesetzen, in denen sie geregelt sind. Dabei sind für Online-Durchsuchung und Quellen-TKÜ zutreffende und nur für eine Maßnahme bestimmte Straftaten farblich gekennzeichnet.

[127] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100b Rn. 5.
[128] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100b Rn. 7.
[129] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100b Rn. 7.
[130] Vgl. Roggan, StV 2017, 821 (825); Singelnstein, 2017.
[131] Vgl. Stoklas/Wendorf, ZD-Aktuell 2017, 05725.
[132] Vgl. Niederhuber, JA 2018, 169 (171).

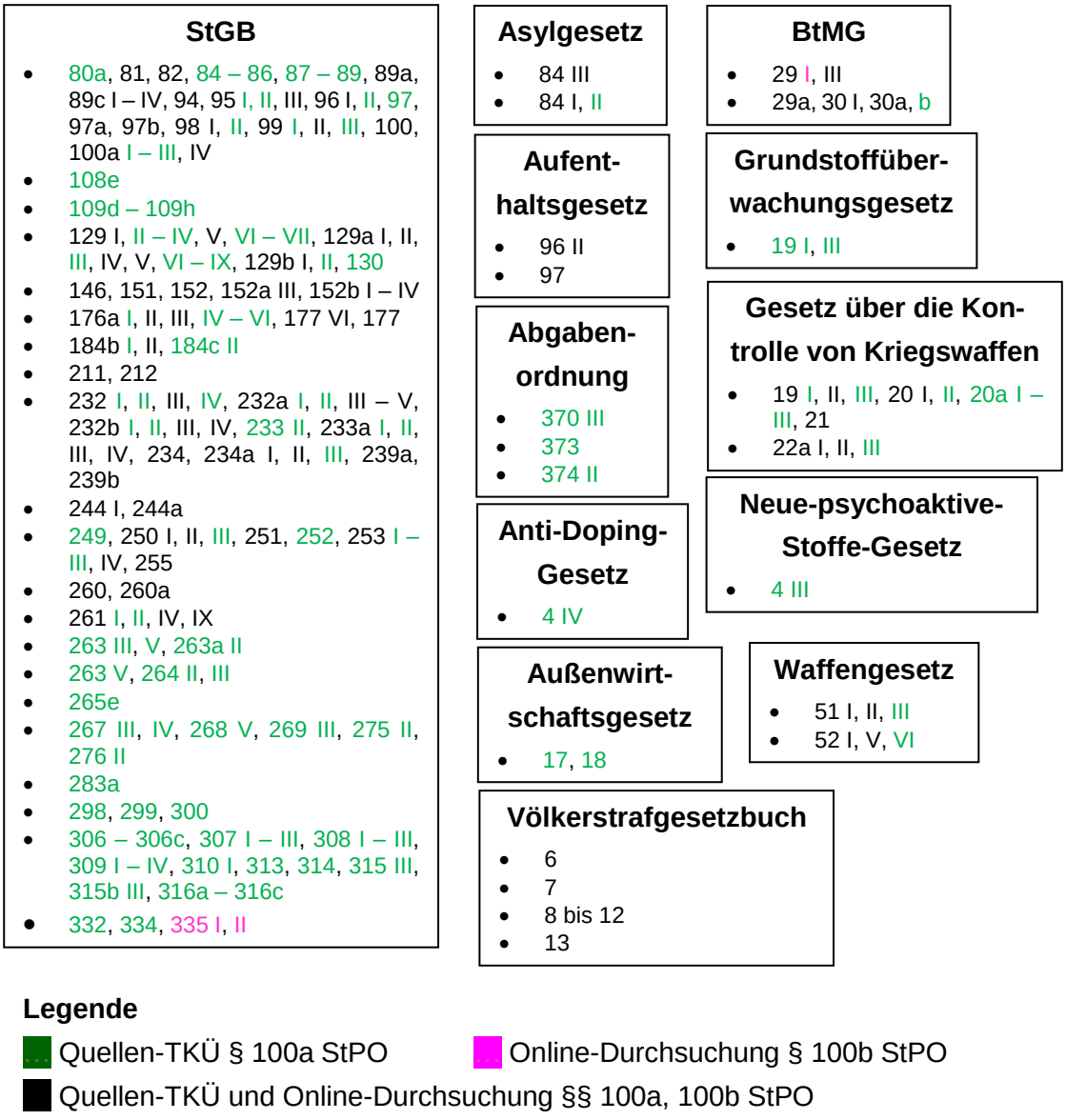

Abb. 3: Übersicht über den Vergleich der Straftatenkataloge von §§ 100a II, 100b II StPO, eigene Arbeit.

Am deutlichsten unterscheiden sich die beiden Straftatenkataloge bezüglich des StGB in den Bereichen von Betrug und Untreue, Urkundenfälschung, Insolvenzstraftaten, Straftaten gegen den Wettbewerb sowie gemeingefährliche Straftaten, die ausschließlich der Maßnahme der Quellen-TKÜ vorbehalten sind. Diese gehören zu den klassischen Einsatzgebieten der TKÜ.[133] Außerdem gibt es strafrechtliche Nebengesetze wie Abgabenordnung, Anti-Doping-Gesetz, Außenwirtschaftsgesetz, Grundstoffüberwachungsgesetz und Neue-psychoaktive-Stoffe-Gesetz, die Straftaten regeln, bei denen nur die Quellen-TKÜ angeordnet werden darf. Hervorzuheben sind die beiden Straftaten der besonders schweren Fälle der Bestechlichkeit und Bestechung aus dem Abschnitt „Straftaten im

[133] Vgl. Greven, 2017, S. 5.

Amt“ des StGB sowie des Gesetzes über den Umgang mit Betäubungsmitteln nach § 29 I BtMG, die exklusive Beispiele der Online-Durchsuchung sind. Von Seiten des Gesetzgebers gibt es innerhalb des Beschlusses keine Begründung für die jeweiligen Bereiche, die sich ausschließlich auf die Quellen-TKÜ oder Online-Durchsuchung beziehen. Vielmehr hat sich der Gesetzgeber anscheinend um eine Orientierung an den Vorgaben des BVerfG in der Entscheidung zum BKAG bemüht.[134] Allgemein lässt sich zur Abgrenzung der Straftatenkataloge anführen, dass sich der Unterschied zwischen schweren und besonders schweren Straftaten aus dem Strafrahmen[135], den geschützten Rechtsgütern[136] und der Strafzumessungsregel mit Regelbeispielen[137] ergibt.

[134] Vgl. Stoklas/Wendorf, ZD-Aktuell 2017, 05725.
[135] Vgl. Krauß, 2017, S. 6, 10.
[136] Vgl. Krauß, 2017, S. 10.
[137] Vgl. Greven, 2017, S. 7.

E. Regelungen für beide Maßnahmen nach §§ 100d, 100e StPO

Die StPO-Reform im Jahr 2017 bringt auch Neuerungen für die §§ 100d, 100e StPO mit sich. Was vorher in §§ 100a IV, 100c IV – VII StPO aF in Einzelvorschriften geregelt worden ist, fasst nun § 100d StPO für die Maßnahmen von § 100a – 100c StPO zusammen.[138] § 100d StPO normiert nun den Umgang mit Erkenntnissen aus dem Kernbereich privater Lebensgestaltung und die Folgen für die Online-Durchsuchung bei Vorliegen eines Zeugnisverweigerungsrechts gem. §§ 52 ff. StPO. Verfahrensvorschriften zu den Maßnahmen nach §§ 100a – c StPO beschreibt § 100e StPO.

I. Kernbereichsschutz und Zeugnisverweigerungsrecht nach § 100d StPO

Der auf dem Grundrecht der Menschenwürde gem. Art. 1 I GG beruhende Schutz des Kernbereichs privater Lebensgestaltung ist in der StPO weder definiert noch allgemein bestimmt, sondern beurteilt sich nach dem jeweiligen Einzelfall.[139] Bei heimlichen Maßnahmen des Staates wird nicht zwingend die Würde des Menschen verletzt, aber die Unantastbarkeit des Kernbereichs privater Lebensgestaltung muss geachtet werden.[140] Dieser Schutz darf nicht mit Strafverfolgungsinteressen nach dem Verhältnismäßigkeitsgrundsatz abgewogen und relativiert werden.[141] Der Begriff des Kernbereichs privater Lebensgestaltung umfasst „Inhalte mit höchstpersönlichem Charakter, welche die Gefühlswelt oder den Intimbereich tangieren“.[142]

Diesen Kernbereichsschutz gewährleisten § 100d I, II StPO als Schutznormen sowohl für die Quellen-TKÜ als auch die Online-Durchsuchung.[143] Die Unzulässigkeit einer Maßnahme nach §§ 100a, 100b StPO und einem damit verbundenen Maßnahmeverbot[144] folgt gem. § 100d I StPO dem Vorliegen tatsächlicher Anhaltspunkte für die alleinige Betroffenheit der Intimsphäre.[145] Für einen alleinigen Kernbereichsbezug spricht, dass

[138] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100d Rn. 1.
[139] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100d Rn. 3.
[140] Vgl. Höfling in: Sachs, 2018, Art. 1 Rn. 45; BVerfGE 109, 279 (313).
[141] Vgl. Höfling in: Sachs, 2018, Art. 1 Rn. 45; BVerfGE 109, 279 (314).
[142] Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100d Rn. 3.
[143] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100d Rn. 4
[144] Vgl. Roggan, StV 2017, 821 (828).
[145] Vgl. Roggan, StV 2017, 821 (828).

eine Kommunikation des Betroffenen mit einem engsten Familienangehörigen, Geistlichen, Telefonseelsorger oder Strafverteidiger, bei denen ein dem Kernbereich betreffendes Vertrauensverhältnis angenommen wird, stattfindet.[146] Wenn sich kein ausschließliches Erheben von Kernbereichsdaten prognostizieren lässt und die Verhinderung von Verletzungen des Kernbereichsschutzes technisch unmöglich ist, wird der Eingriff in den Kernbereich privater Lebensgestaltung folglich planmäßig hingenommen.[147] Nach § 100d II 1 StPO dürfen alle durch die Maßnahmen der Quellen-TKÜ und Online-Durchsuchung erfassten Erkenntnisse aus dem Kernbereich privater Lebensgestaltung nicht verwertet werden. § 100d II 2, 3 StPO ordnet die unverzügliche Löschung dieser Daten und die Dokumentation über diesen Vorgang der Erlangung und Vernichtung an.
Ein § 100b-spezifischer Schutz des Kernbereichs privater Lebensgestaltung befindet sich in § 100d III StPO.[148] Nach § 100d III 1 StPO ist bei Online-Durchsuchungen unter technischer Umsetzbarkeit sicherzustellen, dass den Kernbereich privater Lebensgestaltung betreffende Daten erst gar nicht erhoben werden. Dieser Schutz wird ergänzend dazu gem. § 100d III 2, 3 StPO im Fall einer Kernbereichsverletzung eine Löschungspflicht oder in Zweifelsfällen durch eine Vorlagepflicht gegenüber dem anordnenden Gericht gewährleistet. Für die Löschung kernbereichsgeschützter Daten ist die auswertende Ermittlungsperson i.d.R. zuständig.[149] Bei Zweifelsfällen über den Kernbereichsbezug ist zu beachten, dass dieser Zweifel an das Gericht ohne schuldhaftes Zögern vorzulegen ist, um eine unverzügliche Löschung zu gewährleisten.[150]
§ 100d V StPO bezieht sich auch auf die Online-Durchsuchung nach § 100b StPO beim Vorliegen des Zeugnisverweigerungsrechts. Die Zeugnisverweigerungsberechtigten unterteilen sich in zwei Gruppen nach den Fällen der Berufsgeheimnisträger nach § 53 StPO, für die die Unzulässigkeit der Maßnahme und ein Beweiserhebungsverbot gilt, sowie der gem. § 52 StPO Angehörigen des Betroffenen und gem. § 53a StPO Berufshelfer mit einem relativen Beweisverwertungsverbot.[151] Das Beweiserhebungsverbot für die erste Gruppe bewirkt ein Verwertungsverbot und eine Pflicht zur unverzüglichen Löschung entsprechend dem Kernbereichsschutz der privaten Lebensgestaltung nach

[146] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100d Rn. 5a.
[147] Vgl. Roggan, StV 2017, 821 (828).
[148] Vgl. Roggan, StV 2017, 821 (828).
[149] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100d Rn. 11.
[150] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100d Rn. 11.
[151] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100d Rn. 24, 25.

§ 100d II StPO.[152] Bei dem in der zweiten Gruppe geltenden relativen Beweisverwertungsverbot kann das Eindringen in das Vertrauensverhältnis gegenüber dem Ermittlungsinteresse abgewogen werden, wobei der Kernbereichsschutz unangetastet bleibt.[153]

II. Richterliche Anordnung nach § 100e StPO

Die formellen Voraussetzungen für die Maßnahmen nach §§ 100a, 100b StPO ergeben sich aus § 100e StPO und sind nach dem Schweregrad des jeweiligen Eingriffs abgestuft.[154] Für die Quellen-TKÜ nach § 100a StPO bedarf es gem. § 100e I 1 StPO auf Antrag der Staatsanwaltschaft einer Anordnung durch das Gericht. Bei Gefahr in Verzug kann die Staatsanwaltschaft gem. § 100e I 2 StPO die Maßnahme anordnen. Gem. § 100e I 3 StPO muss in diesem Fall eine Bestätigung durch das Gericht innerhalb von drei Tagen vorliegen, oder die Anordnung tritt außer Kraft. Die Quellen-TKÜ ist zu beenden, wenn die Ermittlungen ohne die Maßnahme nach § 100a StPO fortgeführt werden können bzw. der Ermittlungserfolg mit dem Ausfindigmachen des Aufenthaltsortes des Beschuldigten eingetreten ist.[155] Die Dauer der Anordnung ist nach § 100e I 4, 5 StPO auf höchstens drei Monate befristet und kann um jeweils nicht mehr als drei Monate verlängert werden. Der Fristbeginn ist der Erlass der richterlichen Anordnung.[156] Ein Außerkrafttreten der Anordnung ist bei Nichtverlängern der Frist, die mit dem Anordnungserlass und nicht erst mit dem Vollzug der Maßnahme beginnt, gegeben.[157]
Gem. § 100e II 1 StPO darf auf Antrag der Staatsanwaltschaft die Online-Durchsuchung nach § 100b StPO nur von der Kammer des Landgerichts angeordnet werden. Dabei handelt es sich um die Staatsschutzkammer, die mit drei Richtern besetzt ist.[158] Der Vorsitzende dieser Kammer kann bei Gefahr im Verzug gem. § 100e II 2 StPO die Anordnung treffen, welche wiederum gem. § 100e II 3 StPO binnen drei Werktagen von der Strafkammer zu bestätigen ist, um nicht außer Kraft zu treten. Nach § 100e II 4 StPO gilt eine Befristung der Anordnung auf höchstens einen Monat. Beginn der Frist ist der Zeitpunkt der richterlichen Anordnung, nicht der Anfang der Online-Durchsuchung.[159] Nach

[152] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100d Rn. 24.
[153] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100d Rn. 25.
[154] Vgl. Warken, NZWiSt 2017, 329 (336).
[155] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100e Rn. 5.
[156] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100e Rn. 5.
[157] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100e Rn. 5.
[158] Vgl. Roggan, StV 2017, 821 (828).
[159] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100e Rn. 8.

fünfmaliger Verlängerung um je einen Monat muss gem. § 100e II 5, 6 StPO das Oberlandesgericht über weitere einmonatige Verlängerungen entscheiden. Außerdem ist bei jeder Verlängerung die Erfolgsprognose nach den in § 100e IV 2 Nr. 2 StPO genannten Erwägungen zu überprüfen.[160]
Ein zeitlicher Ablauf über die Regelungen des § 100e I, II StPO ist in Abb. 4 graphisch dargestellt.

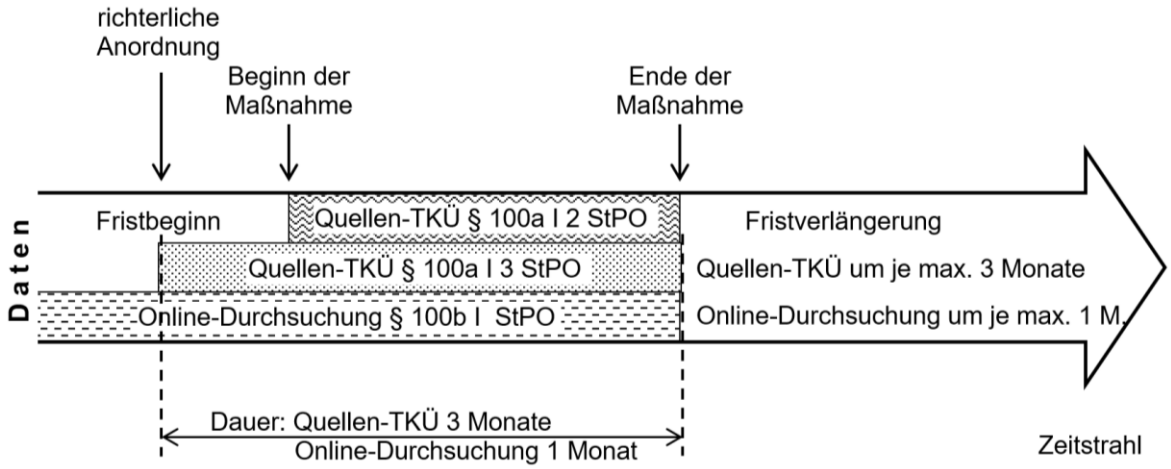

Abb. 4: Zeitstrahl über Fristbeginn, Dauer und Fristverlängerung als Grenze des Datenzugriffs, eigene Arbeit.

§ 100e III StPO enthält Vorgaben zu Form und Inhalt der Anordnung für beide Maßnahmen. Es ist die schriftliche Form nach § 100e III 1 StPO einzuhalten. Die Anordnung muss nach § 100e III 2 StPO folgende Inhaltspunkte umfassen: Name und Anschrift des Betroffenen (Nr. 1), Tatvorwurf (Nr. 2), Art, Umfang und Dauer der Maßnahme (Nr. 3), Art der zu erhebenden Information und ihre Bedeutung für das Verfahren (Nr. 4). Für die Anordnung der Quellen-TKÜ sind nach § 100e III 2 Nr. 5 StPO zudem die Rufnummer sowie das Endgerät bzw. das informationstechnische System anzugeben, während bei der Online-Durchsuchung eine möglichst genaue Bezeichnung des Zielsystems gem. § 100e III 2 Nr. 6 StPO erforderlich ist.

[160] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100e Rn. 8.

F. Technische Grundlagen

Für beide repressiven Maßnahmen der Online-Durchsuchung und Quellen-TKÜ wird dieselbe Technik verwendet. In diesem Kapitel werden die Grundlagen dazu dargelegt. Die Ermittlungsbehörden können nach folgendem Schema[161] vorgehen.

I. Ausspähen des Zielsystems

Zunächst ist es wichtig, alle Informationen über die von der betroffenen Person genutzten Geräte wie PC, Smartphone oder Tablet sowie der Netzwerke und Speicherorte, z.B. zentral im System, lokal auf dem Computer oder extern in einer Cloud, zu sammeln. Dies geschieht über die Umfeldanalyse, die Details über Hardware- und Software-Konfiguration der Zielsysteme liefert.[162] Dabei interessieren Typ, Version, Level und Update-Status von Firewalls, Betriebssystemen sowie Antivirenprogrammen.[163] Varianten der Umfeldanalyse sind Portscan und Social Engineering.[164]

II. Konfiguration einer passenden Durchsuchungssoftware

Zum heutigen Stand gibt es Bundestrojaner, die standardmäßig zur Online-Durchsuchung und Quellen-TKÜ verwendet werden. Es gibt den Trojaner des BKA, der unter dem Namen „Remote Control Interception Software 1.0“ (RCIS 1.0) bekannt ist.[165] Dieser kann lediglich bei Computern eingesetzt werden und auch nur Voice-Over-IP-Programme wie Skype überwachen.[166] Vermutlich beschränkt sich die Spionagesoftware auf Computer mit Betriebssystemen Windows 7 und Windows 8.[167] Für Handys und Tablets gibt es die kommerzielle Überwachungssoftware „FinSpy“ der Firma FinFisher, die das Bundesinnenministerium seit Januar 2018 zum Einsatz freigegeben hat.[168] Damit lässt sich verschlüsselte Kommunikation über Messengerdienste auf Mobiltelefonen überwachen.[169] Falls die Ermittlungsbehörden über die nötigen Mittel und den versierten

[161] Vgl. Kohlmann, 2012, Gliederungspunkte ab S. 43.
[162] Vgl. Kohlmann, 2012, S. 43.
[163] Vgl. Kohlmann, 2012, S. 43.
[164] Vgl. Kohlmann, 2012, S. 43.
[165] Vgl. Flade, 2018.
[166] Vgl. Flade, 2018.
[167] Vgl. Rath, 2017.
[168] Vgl. Flade, 2018.
[169] Vgl. Flade, 2018.

Umgang mit der Software verfügen, kann die Durchsuchungssoftware flexibel gestaltet werden und somit auf spezielle Fallanwendungen zugeschnitten werden, die sich aus dem ausgespähten Zielsystem als notwendig ergeben. Dies könnte es auch ermöglichen, zum Schutz von Unbeteiligten die Maßnahmen auf den vom Betroffenen genutzten Teil des Systems wie etwa im Firmennetzwerk zu begrenzen. Das Spähprogramm sollte folgende Funktionen beherrschen: Analyse des Systems, Zugriff auf dieses, Erstellen von Verzeichnisübersichten, Durchsuchen von Verzeichnissen und angeschlossenen Datenträgern, Herunterladen von Dokumenten, Protokollieren von Tastaturanschlägen, unbemerktes Löschen der eigenen Überwachungssoftware bzw. ihr automatisches Deaktivieren nach bestimmten Zeitablauf.[170] Für die Quellen-TKÜ wäre es zudem von Vorteil, wenn sich die Software automatisch einschalten würde, sobald eine laufende Telekommunikation stattfindet.

III. Installation der Untersuchungssoftware

Zur Installation der Software für die Online-Durchsuchung und Quellen-TKÜ stehen verschiedene Möglichkeiten zur Verfügung.

1. Manuelle Installation

Diese Variante der Installation ist zwar technisch am einfachsten, da die Spähsoftware wie ein normales Programm installiert werden kann, erfordert aber physischen Zugriff auf das Zielsystem. Die Wohnung des Betroffenen als eine nach Art. 13 I GG geschützte Räumlichkeit darf zu diesem Zweck nicht betreten werden.[171] Ein physischer Zugriff auf ein Zielgerät könnte durch verdeckte Ermittlungen wie etwa von einem V-Mann kurzzeitig gelingen. Denkbare Varianten sind das Auffinden des Zielsystems in einem öffentlichen Lokal, abgestellten PKW des Betroffenen oder bei einer polizeilichen bzw. Zoll-Kontrolle. Diese Vorgehensweise bei der praktischen Durchführung der Installation erfordert neben den technischen Mitteln kriminalistische List.[172] Außerdem könnte der Zugriff auf das Gerät des Betroffenen unter gewissen Voraussetzungen durch eine Beschlagnahme nach § 94 StPO erlangt werden und für eine manuelle Installation der Durchsuchungssoftware genutzt werden. Nachteil der letztgenannten Vorgehensweise ist, dass der Betroffene Verdacht auf die Online-Durchsuchung oder Quellen-TKÜ

[170] Vgl. Kohlmann, 2012, S. 44.
[171] Vgl. Roggan, StV 2017, 821 (822).
[172] Vgl. Schmitt in: Meyer-Goßner/Schmitt, 2018, § 100a Rn. 14d.

schöpfen könnte. Die manuelle Installation stellt jedoch generell eine sichere und zielgerichtete Infiltrierung des Zielsystems dar.

2. Entfernte manuelle Installation

Die entfernte manuelle Installation überträgt die Überwachungssoftware via Internet auf das Gerät des Betroffenen, indem unsichere Konfigurationen des Zielsystems, Schwachstellen im Betriebssystem oder Sicherheitslücken in Online-Anwendungen ausgenutzt werden.[173]

Angriffsprogramme auf die dem Hersteller bekannten und publizierten Sicherheitslücken, die als Zero-Day-Exploits[174] bezeichnet werden, eignen sich zur Infizierung des Zielsystems mit der Durchsuchungssoftware, wenn der Betroffene auf seinen genutzten Geräten veraltete Betriebssysteme wie das nicht mehr unterstützte Windows XP von Microsoft verwendet oder auf regelmäßige Updates des Betriebssystems verzichtet. Bei dieser Art der Installation besteht jedoch das Problem, dass die Sicherheitslücken während der auf einen längeren Zeitraum angelegten Maßnahme der Online-Durchsuchung geschlossen werden. Allerdings kann davon ausgegangen werden, dass die Veröffentlichung der Zero-Day-Exploits erst mit Verzögerung von etwa 45 Tagen erfolgt und dass das Schließen dieser Sicherheitslücken durch den Hersteller in Form von Patches oder Updates einige Zeit in Anspruch nimmt.[175]

Less-Than-Zero-Day-Exploits[176] richten sich gegen unveröffentlichte oder dem Hersteller nicht bekannte Sicherheitslücken, die eine weitere Variante der entfernten manuellen Installation ermöglichen. Diese Sicherheitslücken können die Ermittlungsbehörden entweder mit Hilfe von eigenem Personal aufdecken, was sich jedoch aufgrund des fehlenden Know-How der Spezialisten in Deutschland als schwierig bzw. langwierig erweist, oder durch Zukauf bei externen Einzelpersonen oder Firmen, die sich auf das Gebiet der Informationsgewinnung von unveröffentlichten Sicherheitslücken spezialisiert haben.[177] Bei Zukauf solcher Informationen besteht jedoch das Risiko, dass andere Personen, die Kriminelle sein können oder im Bereich der Wirtschaftsspionage tätig sind, von dieser Variante Gebrauch machen und über dieselben Informationen verfügen.[178] Für eine längerfristige Online-Durchsuchung oder Quellen-TKÜ sind die Less-Than-Zero-Day-

[173] Vgl. Kohlmann, 2012, S. 30.
[174] Vgl. Pohl, DuD 2007, 684 (685).
[175] Vgl. Pohl, DuD 2007, 684 (685).
[176] Vgl. Pohl, DuD 2007, 684 (685).
[177] Vgl. Pohl, DuD 2007, 684 (685).
[178] Vgl. Pohl, DuD 2007, 684 (685).

Exploits besser geeignet, da mit einer Veröffentlichung und der damit verbundenen Schließung der Sicherheitslücke auf längere Sicht nicht zu rechnen ist.
Eine andere Möglichkeit zur entfernten manuellen Installation der Überwachungssoftware stellt eine vom Gesetzgeber verordnete Verpflichtung an den Betriebssystemhersteller dar, eine Schnittstelle zum Zugriff auf Computersysteme für Behörden einzubauen.[179] Diese als „Bundes-Backdoor“ bezeichnete Lösung ist aber zu verwerfen, da einerseits der deutsche Gesetzgeber nicht die Handhabe besitzt, international tätigen Konzernen solche Vorgaben zu machen, und auf der anderen Seite der politische Wille fehlt, solche Wege zu beschreiten.[180]
Zur Infizierung von Smartphone und mobile Devices mit der Durchsuchungssoftware eignen sich unsichere Verbindungswege wie Bluetooth und öffentliches WLAN, da hier die Übertragungen ungeschützt ablaufen.

3. Automatische Hintergrundinstallation

Bei der automatischen Hintergrundinstallation wird das Laden der Durchsuchungssoftware in einem anderen im Vordergrund laufenden Prozess versteckt.
Eine Variante davon ist, dass die Software in Dateianhängen von E-Mails eingebaut ist. Nach Öffnen des Anhangs läuft die Installation der Durchsuchungssoftware unbemerkt ab, da der Betroffene nur das Laden der ausführbaren Datei wie Bild oder Musiktrack wahrnimmt. Am erfolgversprechendsten ist diese Methode, wenn das Vertrauen des Betroffenen durch Social Engineering gewonnen wird. Analog kann dieses Vorgehen mittels eines per E-Mail versendeten Links, der auf eine mit der Überwachungssoftware präparierte Webseite verweist, durchgeführt werden.
Es ist auch möglich, auf vom Betroffenen häufig besuchten Webseiten Scriptprogramme zu verstecken, die beim Aufrufen der Webseite die Installation automatisch starten und die Durchsuchungssoftware nachladen.[181] Diese Vorgehensweise ist aber nicht zielgenau, da auch andere Personen, für die keine richterliche Anordnung der Maßnahme vorliegt, auf die Webseite gelangen. Auch Einschränkungen über IP-Adressen und Login-Daten führen nicht zur eindeutigen Identifizierung des Betroffenen, da meist ein dynamisches Vergeben der IP-Adressen in Netzwerken erfolgt und dieselben Login-Daten an Angehörige oder vertraute Personen ausgeliehen werden.[182]

[179] Vgl. Kohlmann, 2012, S. 31.
[180] Vgl. Kohlmann, 2012, S. 31.
[181] Vgl. Kohlmann, 2012, S. 37.
[182] Vgl. Kohlmann, 2012, S. 37.

Für die automatische Hintergrundinstallation stellt speziell bei Smartphones das Verstecken der Überwachungssoftware in Apps eine Möglichkeit dar. Dies ist jedoch noch schwieriger auf die Zielperson zu begrenzen.

IV. Auslesen und Übertragen der Daten vom Zielsystem

Nach erfolgreicher Installation der Überwachungssoftware und dem damit verbundenen Infiltrieren des Systems können Daten einerseits einmalig und punktuell ausgeleitet werden, der Vorgang kann aber auch innerhalb einer Online-Überwachung über einen längeren Zeitraum andauern.[183] Mittels Keylogging oder Screen- bzw. Applicationshots können Passwörter oder Zugangscodes, die zu lediglich kurzzeitig auf dem Zielsystem im Klartext vorliegenden Daten gehören, ausgelesen werden, was der Auswertung von Datenträgern bei einer eventuell späteren Beschlagnahme zugutekommt.[184] Diese Herangehensweise der Datenerhebung wird als „Live-Zugriff“ oder „heimlicher virtueller Blick über die Schulter“ des Betroffenen bezeichnet.[185]
Schwieriger gestaltet sich die Online-Durchsuchung einer Festplatte, weil die Software zunächst die Dateistruktur der Speichermedien an die Ermittlungsbehörde übermitteln muss und spätere Anweisungen benötigt, nach welchen Suchkriterien bzw. Schlüsselwörtern ausgelesen werden soll. Aktuelle Informationen über die staatliche Überwachungssoftware sind wegen Geheimhaltung nicht öffentlich einsehbar. Die folgenden Ausführungen gehen auf die Analyse des Chaos Computer Club (CCC) zurück, dem der Bundestrojaner mit dem Stand von 2011 zur Verfügung gestanden hat. Beim Bundestrojaner findet die Kommunikation zwischen dem Zielsystem und der Behörde über einen „Command-and-Control-Server“ (C+C-Server) statt.[186] Dabei werden nur die ausgehenden Daten nach AES-Verfahren verschlüsselt, während die Anweisungen an die Spähsoftware unverschlüsselt übertragen werden.[187] Dadurch können Dritte die Steuerung der Regierungs-Malware übernehmen, was eine staatlich geschaffene Sicherheitslücke für die Daten auf dem informationellen System des Betroffenen darstellt. Wenn sich der externe C+C-Server wie in diesem untersuchten Fall bei einem Drittanbieter im nichteuropäischen Ausland befindet, muss sichergestellt werden, dass die ausgeleiteten Daten des Betroffenen dem Datenschutz nach der EU-DSGVO entsprechen.

[183] Vgl. Roggan, StV 2017, 821 (825).
[184] Vgl. Henzler, 2017, S. 6.
[185] Vgl. Buermeyer, 2017, S. 5.
[186] Vgl. CCC, 2011, S. 3.
[187] Vgl. CCC, 2011, S. 4.

Sonderfälle stellen externe Festplatten, die nicht ständig mit dem Zielgerät verbunden sind, und auf Cloud basierende Speicher dar. Rechtlich stellt sich die Frage, inwieweit sich die richterliche Anordnung für die Maßnahme der Online-Durchsuchung auf die Speichermedien, die sich sowohl in ihrem Standort als auch Anbieter unterscheiden, bezieht.

Zur Übertragung der Daten mittels der Überwachungssoftware muss eine Internetverbindung zum Zielsystem bestehen. Es sind zwei Varianten denkbar. Die Datenausleitung erfolgt, sobald sich das Gerät mit dem Internet verbindet. Eine DSL-Verbindung mit zu geringer Bandbreite würde das laufende Internetgeschehen beim Übertragen großer Datenmengen im Hintergrund so weit verlangsamen, dass der Betroffene Verdacht schöpfen könnte.[188] Auf der anderen Seite könnte sich die Spähsoftware selbstständig in das Internet einwählen und eine automatische Datenübertragung zu einer Zeit, in der der Betroffene das Gerät nicht nutzt, ablaufen lassen. In diesem Fall könnten aber besondere Routereinstellungen, Firewall oder ein IDS die Übertragung blockieren oder einen Alarm melden.

Um die Sprachdaten wie etwa aus einer Skype-Kommunikation oder VoIP-Telefonie besser übertragen zu können, werden diese komprimiert.[189]

Kritisch anzumerken ist, inwieweit sichergestellt werden kann, dass die ausgeleiteten Daten nicht manipuliert oder verändert worden sind. Da es sich teilweise nur um Mitschnitte bzw. Screenshots handelt, ist der sinnrichtige Kontext gegebenenfalls schwer wiederherzustellen. Um die Beweiskraft der Daten zu gewährleisten, ist zu den ausgeleiteten Daten der Ort und der Zeitpunkt sicherzustellen.[190]

V. Auswertung der Daten

Zur Auswertung der durch die Online-Durchsuchung und Quellen-TKÜ gewonnenen Daten werden allgemein die forensisch üblichen wissenschaftlichen Methoden angewendet. Vom externen Speicherort werden die erhobenen Daten auf einen portablen Datenträger kopiert und offline durch die Behörde untersucht.[191] Von Fall zu Fall ist zu entscheiden, welche Prozesse durch Personal auszuwerten sind und welche automatisiert analysiert werden können, zumal überprüft werden muss, ob die Daten dem Zweck der

[188] Vgl. Kohlmann, 2012, S. 41.
[189] Vgl. CCC, 2011, S. 16.
[190] Vgl. Warken, NZWiSt 2017, 329 (332).
[191] Vgl. Kohlmann, 2012, S. 46.

Beweiserhebung dienen, und bedacht werden muss, dass Wertungsschwierigkeiten auftreten können.[192]

Die gewonnenen Datensätze liegen in unterschiedlichsten Datenformaten vor, die von der Datenquelle abhängig sind.[193] Je nach Maßnahme der Online-Durchsuchung und Quellen-TKÜ wird auf andere Zielsysteme zugegriffen. Als Beispiele für mögliche Datenquellen zu nennen sind: Server, PCs, Tablets, Mobilfunkgeräte, Router, soziale Netzwerke, Streamingdienste, Internetplattformen, Basisstationen oder Speichermedien der Telekommunikation, Videoüberwachungskameras, Buchhaltungssysteme und Bankkonten.[194] Unterschiedliche Datenformate können auch durch die verschiedenen Betriebs- und Dateisysteme sowie Anwendungsprogramme entstehen. Die Datensätze können auch Metadaten enthalten, die als Zusatzinformationen zu bestimmten Datenpaketen meist automatisiert erstellt werden.[195] Außerdem können die erhobenen Daten in komprimierter Form als ZIP-Dateien vorliegen.

Um dieses Rohmaterial in eine auswertbare Form zu transformieren, werden sowohl die jeweilige Software als auch das dazugehörige IT-Wissen benötigt, da oftmals manuell Zwischenschritte umzusetzen sind.[196] Dies führt zu zeitintensiven und personalaufwendigen Aufarbeitungen. Für die weiterführende kriminalistische Analyse und inhaltliche Auswertung ist eine lesbare Form unabdingbar.

Eine weitere Erschwernis der Auswertung stellen in den Geräten verschlüsselt gespeicherte Daten dar. Es geht um vom Betroffenen selbst eingesetzte Verschlüsselungen. Die Dechiffrierung ist von dem verwendeten Kryptoverfahren abhängig und kann durch Ausprobieren der verschiedenen Möglichkeiten gefunden werden. Kommt ein Passwort hinzu, gestaltet sich die Entschlüsselung komplizierter. Das Passwort könnte aber bereits durch einen Keylogger bekannt sein. Sonst bieten sich zur Erlangung des Passworts die üblichen Methoden wie Brute-Force oder Wörterbuchangriffe an, die große Rechenkapazität erfordert.

Bei Daten, die aus einer Cloud oder einem Massenspeicher zur Datensicherung stammen, ist es schwer zu überprüfen, ob der ausgeleitete Datensatz vollkommen identisch mit dem ursprünglich abgelegten ist.[197] Der Grund dafür liegt in der automatischen, geteilten und dynamischen Speicherung der Daten.[198]

---

[192] Vgl. Kohlmann, 2012, S. 46.
[193] Vgl. Warken, NZWiSt 2017, 329 (330).
[194] Vgl. Warken, NZWiSt 2017, 329 (330).
[195] Vgl. Warken, NZWiSt 2017, 329 (331).
[196] Vgl. Warken, NZWiSt 2017, 329 (331).
[197] Vgl. Koops/Goodwin, 2014, S. 23.
[198] Vgl. Koops/Goodwin, 2014, S. 24.

Große Datenmengen, die dem Phänomen Big Data zuzuordnen sind, stellen nicht nur technische Herausforderungen hinsichtlich der Ausleitung dar, sondern führen auch zu einem erhöhten Zeitbedarf bei der Auswertung der Datensätze.[199] Außerdem ist in diesem Zusammenhang der Schutz persönlicher Daten rechtlich bedenklich.[200]

VI. Beenden der Online-Durchsuchung oder Quellen-TKÜ

Das Beenden einer Online-Durchsuchung und Quellen-TKÜ ist in § 100e V StPO geregelt. Demnach müssen die Maßnahmen unverzüglich beendet werden, wenn die Voraussetzungen der richterlichen Anordnung nicht mehr vorliegen. Die Spähsoftware muss dann vom Zielsystem deinstalliert werden. Technisch kann dies umgesetzt werden, indem die Überwachungssoftware entweder einen Befehl zur Deinstallation entgegennimmt oder in ihr eine automatische Deinstallationsroutine integriert wird. Falls keine softwareseitige Beendigung möglich ist, wäre ein physischer Zugriff notwendig. Dies empfiehlt sich jedoch aus kriminalistischer Sicht nicht.

[199] Vgl. Europol, IOCTA 2016, S. 53 f.
[200] Vgl. Europol, IOCTA 2016, S. 54.

G. Diskussion über die Geeignetheit von Online-Durchsuchung und Quellen-TKÜ für den Ermittlungserfolg

Im folgenden Kapitel soll im Rahmen der zur Verfügung stehenden Informationen zu den relativ jungen Regelungen die Geeignetheit der repressiven Maßnahmen zur Strafverfolgung aus technischer Sicht für den Ermittlungserfolg diskutiert werden. Dazu wird sowohl die tatsächliche als auch rechtliche Seite beleuchtet.

I. Tatsächliche Lage

Das BKA besitzt nach eigener Aussage im Sachstandbericht 2018 eine Eigenentwicklung und kommerzielle Software zum Einsatz bei der Quellen-TKÜ sowie eine Software zur Durchführung einer Online-Durchsuchung.[201] Alle zur Verfügung stehenden Spähprogramme müssen ein Testverfahren durchlaufen, um zu zeigen, dass sie mit den rechtlichen Vorgaben konform sind und die Maßstäbe der standardisierten Leistungsbeschreibung erfüllen.[202] Aus einsatztaktischen Gründen gibt das BKA keine Auskünfte über den Entwicklungsstand der Software sowie die tatsächliche Anzahl ihres Einsatzes.[203] Vom Bundesamt für Justiz liegen Statistiken über die TKÜ nur bis zum Jahr 2016 vor.[204] Die PKS 2017[205] enthält nur Informationen über Fälle und Aufklärungsquoten, aber keine Details über die Maßnahmen, die zum Ermittlungserfolg beigetragen haben. Aus dem Bericht der Bundesregierung zum Einsatz von Quellen-TKÜ und Online-Durchsuchung in Ermittlungsverfahren des Generalbundesanwalts geht hervor, dass diese beiden Maßnahmen bis Anfang 2018 in keinem Verfahren angeordnet worden sind.[206] Bisherige Erfolge bei der Online-Kommunikation sind durch kriminalistische List erzielt worden, wie der Fall der Überwachung des Messengerdienstes Telegram, deren Methode zu Beginn dieser Arbeit beschrieben ist, zeigt.[207] Aus journalistischen Kreisen geht hervor, dass eine Installation der vom Bundesinnenministerium seit Februar 2016 freigegebenen Software RCIS 1.0 bzw. deren Versuch nur in wenigen Fällen von angeordneter Quellen-

[201] Vgl. BKA, 2018.
[202] Vgl. BKA, 2018.
[203] Vgl. BKA, 2018.
[204] Abrufbar unter: https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung.html, verfügbar am 09.08.18, 8:51.
[205] Abrufbar unter: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2017/pks2017_node.html, verfügbar am 12.08.18, 19:07.
[206] Vgl. Flade, 2018.
[207] Vgl. Flade, 2018.

TKÜ auf ein Zielgerät erfolgt ist und sich aus Sicht der Ermittler als wenig brauchbar erwiesen hat.[208] Die Ende 2017 erwartete Weiterentwicklung RCIS 2.0 steht immer noch nicht für einen Einsatz zur Verfügung.[209] Eine Durchführung der Quellen-TKÜ mit der kommerziellen Software FinSpy, die vom Bundesinnenministerium im Januar 2018 freigegeben worden ist, hat noch in keinem Fall stattgefunden.[210] Grund für den geringen Einsatz der verschiedenen Bundestrojaner ist vermutlich nicht die Funktionsweise der Software, sondern die Schwierigkeit der heimlichen Installation auf dem Zielsystem.[211] Aufgrund der fehlenden Statistiken kann die Geeignetheit der Maßnahmen aus tatsächlicher Sicht nicht bewertet werden.

II. Rechtliche Sicht

Zur Frage der Geeignetheit der Maßnahmen stellen sich rechtlich folgende Aspekte dar. Mit der Infiltration des Systems gilt es aufgrund der technischen Umstände als kompromittiert.[212] Es könnte den erhobenen Daten die technische Echtheitsbestätigung fehlen.[213] Dies hätte Auswirkungen auf den Beweiswert und würde eventuell nicht revisionsfeste Beweise für ein Strafverfahren liefern.[214] Die rechtliche Sicht ergibt sich jedoch zwingend aus der tatsächlichen. Da bisher noch keine kriminalistischen Erfahrungen bezüglich der Quellen-TKÜ oder Online-Durchsuchungen vorliegen, können auch keine rechtlichen Rückschlüsse auf die Geeignetheit der Maßnahmen gezogen werden.

III. Einschätzung

Es gibt keine zuverlässigen und aussagekräftigen Fakten zur tatsächlichen und rechtlichen Sicht. Dennoch soll eine Einschätzung zur Geeignetheit der Maßnahmen auf technischer Grundlage gegeben werden. Kleinere, auf spezielle Datenerhebungen und Geräte zugeschnittene Programme würden sicherere Ergebnisse liefern, da sie nicht so tief in das Gerät eingreifen. Außerdem müssten wissenschaftliche Methoden entwickelt wer-

[208] Vgl. Flade, 2018.
[209] Vgl. Flade, 2018; Flade, 2017.
[210] Vgl. Flade, 2018; Flade, Ministerium 2018.
[211] Vgl. Flade, 2018.
[212] Vgl. Roggan, StV 2017, 821 (825).
[213] Vgl. Roggan, StV 2017, 821 (825).
[214] Vgl. Roggan, StV 2017, 821 (825); BVerfGE 120, 274 Rn. 223.

den, die den Wahrheitsgehalt der Beweise bestätigen können. Die tatsächliche Einsatzfähigkeit des Bundestrojaners steht und fällt mit zuverlässigen Methoden zur Infiltration auf das jeweilige Zielsystem. Zu berücksichtigen ist, dass mit einem Etablieren der Maßnahmen bei der Strafverfolgung sich auch das Verhalten der Beschuldigten anpassen wird. Die hochintelligente Tätergruppe wird vermehrt Kryptographie einsetzen und sensible Daten an unzugängliche Orte auslagern, um sich der Strafverfolgung zu entziehen.[215]

[215] Vgl. Schaar, 2008, zu Punkt 3.

H. Zusammenfassung

In diesem Kapitel sollen die wesentlichen Ergebnisse aus jedem Kapitel zusammengefasst werden. Die Erkenntnisse werden in einem kurzen Abriss gebündelt dargestellt.
Die Ausführungen zum Gesetzgebungsverfahren haben im historischen Bereich gezeigt, dass das im Jahr 2006 beschlossene PSIS einen Startschuss für einen langen Entwicklungsprozess technischer Voraussetzungen für die Online-Durchsuchung und Quellen-TKÜ gegeben, aber zunächst nur zur präventiven Regelung des § 20k BKAG geführt hat. Letztlich hat ein Gesetzgebungsverfahren in der 18. Legislaturperiode, das von der Ergänzung in einem Änderungsantrag am 15.05.17 bis zur Verkündung im Bundesgesetzblatt am 23.08.17 gedauert hat und trotz zahlreicher kritischer Stellungnahmen unverändert geblieben ist, die repressiven Maßnahmen in §§ 100b, 100a StPO gesetzlich geregelt.
Von der Online-Durchsuchung und Quellen-TKÜ sind das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nach Art. 2 I i.V.m. Art. 1 I GG und das Fernmeldegeheimnis nach Art. 10 I GG als lex specialis betroffen. Das Computergrundrecht gibt es, weil zurecht angenommen wird, dass informationstechnische Systeme mit den gespeicherten Daten und Kommunikationsinhalten so viel über eine Persönlichkeit aussagen, dass eine besondere Schutzbedürftigkeit besteht und deshalb eine weitere Ausgestaltungsform des allgemeinen Persönlichkeitsrechts erfordert.
Im Kapitel der Straftatenkataloge wird erläutert, dass die verschieden tiefe Eingriffsintensität der beiden repressiven Maßnahmen ihren Niederschlag in den Straftatenkatalogen gem. §§ 100a II, 100b II StPO findet. Gleichermaßen fordern §§ 100a I 1 Nr. 1, 2, 100b I Nr. 1, 2 StPO einen Tatverdacht und konkreten Einzelfall, aber beziehen sich einerseits auf eine schwere und zum anderen auf eine besonders schwere Straftaten, die in den Straftatenkatalogen legaldefiniert sind, was im Vergleich zu einem umfangreicheren Straftatenkatalog der Quellen-TKÜ, der dem der klassischen TKÜ nachgebildet ist, und einem enger gefassten Straftatenkatalog der Online-Durchsuchung, der dem der Wohnraumüberwachung nach § 100c StPO entspricht, geführt hat.
§ 100d StPO enthält die zusammengefassten Regeln zum nicht mit dem Strafverfolgungsinteresse relativierbaren Kernbereichsschutz, der entweder zu einer Unzulässigkeit der Maßnahme oder bei Erhebung der nicht von regulären Daten trennbaren Kernbereichsinhalten zu einem Verwertungsverbot und einer Löschungspflicht führt, sowie zum

Zeugnisverweigerungsrecht, das für die Gruppe der Berufsgeheimnisträger ein Beweiserhebungsverbot und für die zweite Gruppe ein relatives Beweisverwertungsverbot vorsieht. Allgemeine Verfahrensvorschriften zur richterlichen Anordnung für die beiden repressiven Maßnahmen finden sich in § 100e StPO, der sowohl die Zuständigkeit, Form und Inhalt als auch den Fristbeginn und die auf Fristverlängerung beruhende, unterschiedliche Dauer der Maßnahmen regelt.

Das Kapitel über die technischen Grundlagen beschreibt die derzeitigen Möglichkeiten, die für die einzelnen Schritte bei der Durchführung der Maßnahme vom Ausspähen des Zielsystems bis zum Deinstallieren des Trojaners zur Verfügung stehen. Besonders intensiv wird auf die vorstellbaren Methoden zum heimlichen Installieren der Überwachungssoftware eingegangen, deren erfolgreiche Anwendung sich bis zum jetzigen Zeitpunkt als problematisch erweist.

Für die Diskussion über die Geeignetheit der Online-Durchsuchung und Quellen-TKÜ für den Ermittlungserfolg aus technischer Sicht fehlt es zur Darstellung der tatsächlichen Lage an Statistiken und offiziellen Auskünften. Recherchierte Nachrichtenquellen ergeben aber, dass die wenigen freigegebenen Spähprogramme zur Durchführung der repressiven Maßnahmen nur geringe Funktionalität aufweisen und bisher nie oder lediglich in wenigen Fällen eingesetzt worden sind, was die Bewertung der Geeignetheit aus rechtlicher Sicht nicht zulässt.

J. Fazit und Ausblick

Ziel der Arbeit ist es gewesen, alle rechtlichen und technischen Aspekte der Online-Durchsuchung und Quellen-TKÜ nach §§ 100b, 100a StPO als Instrumentarien der Strafverfolgung zu untersuchen. Hinsichtlich der Frage, ob das Gesetz eingeschmuggelt worden ist, kann festgestellt werden, dass das Gesetzgebungsverfahren 2017 sehr zügig durchgeführt worden ist. Außer dem technischen Fortschritt gibt es kein besonderes Ereignis, das den Ausschlag für die Gesetzesinitiative gegeben hat. Vielmehr ist anzunehmen, dass die Koalition die Regelungen noch in der 18. Legislaturperiode beschließen wollte, weil der Wahlausgang im September 2017 unvorhersehbar für die künftige Zusammenstellung der Regierungsparteien war. Obwohl die Kürze des Gesetzgebungsverfahrens herausgestellt wurde, begann die Entwicklung der technischen Grundlagen für diese Art der Maßnahmen mit PSIS im Jahr 2006.

Im Bereich der Grundrechte wurden Schutzbereich, Eingriff und Rechtfertigung zu dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und dem Fernmeldegeheimnis ausgeführt. Es hat sich gezeigt, dass die Grundrechte in den verschiedenen Formen der Maßnahmen betroffen sind, weil die Durchführung der Online-Durchsuchung und Quellen-TKÜ Eingriffe darstellen. Die zur Rechtfertigung gebotene verfassungsmäßige Ordnung bzw. einfachgesetzliche Regelung ist mit §§ 100b, 100a StPO gegeben, wenn diese erforderliche Mittel im Sinne des Verhältnismäßigkeitsgrundsatzes sind.

Hinsichtlich der Straftatenkataloge gem. §§ 100a II, 100b II StPO wurden die Fälle der schweren und besonders schweren Straftaten sowie die weiteren Voraussetzungen für eine Anordnung der Maßnahmen dargelegt und analysiert. Jedoch lässt sich kritisch feststellen, dass beim Vergleich der Straftatenkataloge die Abgrenzung nicht eindeutig erkennbar und nicht wirklich konsequent ist, weil der Gesetzgeber auf Straftatenkataloge der klassischen TKÜ und Wohnraumüberwachung zurückgegriffen hat.

Die für die Maßnahmen nach §§ 100a – c StPO zusammengefassten Regelungen zum Kernbereichsschutz, Zeugnisverweigerungsrecht und zur richterlichen Anordnung wurden im Hinblick auf die Online-Durchsuchung und Quellen-TKÜ dargestellt. Da der geforderte Kernbereichsschutz nicht immer technisch umgesetzt werden kann, regelt § 100d II, III StPO ein Verwertungsverbot und eine unverzügliche Löschung, die aber erst im nachgeordneten Stadium der Auswertung erfolgen kann. Damit gehört § 100d II 1 StPO wie § 136a III 2 StPO für Aussagen, die durch verbotene Vernehmungsmethoden

zustande gekommen sind, zu den gesetzlichen Beweisverwertungsverboten. Aus den Erläuterungen zu § 100e StPO geht hervor, dass die unterschiedlich tiefe Eingriffsintensität der Maßnahmen Auswirkungen auf die Instanz des für die richterliche Anordnung zuständigen Gerichts und auf die Dauer der angeordneten Maßnahmen haben.
Bei den technischen Grundlagen konnten für die einzelnen Schritte Möglichkeiten angeführt werden. Ob diese jedoch tatsächlich Anwendung finden, kann aufgrund der Verschwiegenheit der Ermittlungsbehörden nicht zuverlässig beantwortet werden. Hinsichtlich der aufgeworfenen Fragestellungen wurde mit Hilfe der recherchierten Literatur versucht, Installationswege sowie die Software RCIS für Computer und FinSpy für Mobilgeräte mit ihren Einsatzmöglichkeiten zu beschreiben.
Eine Diskussion über die technische Geeignetheit der Online-Durchsuchung und Quellen-TKÜ erwies sich zudem als schwierig, da die zur Verfügung stehenden Informationen Anlass zur Annahme geben, dass entweder ein Einsatz dieser Maßnahmen noch nicht stattgefunden hat oder für den Ermittlungserfolg nicht relevant waren. Vielmehr beruht die erfolgreiche Erhebung unverschlüsselter Daten bisher noch auf kriminalistischer List wie der Fall von Telegram aus der Einleitung zeigt. Da die tatsächliche Lage nur eingeschränkt und die rechtliche Seite nicht diskutiert werden konnte, wurde eine Einschätzung über Argumente, die eine zukünftige Geeignetheit der repressiven Maßnahmen beeinflussen könnten, gegeben.
Die Regelungen zur repressiven Online-Durchsuchung und Quellen-TKÜ nach §§ 100b, 100a StPO sind noch nicht vom BVerfG auf ihre Verfassungsmäßigkeit überprüft worden, weil bisher in keinem Fall relevante Beweismittel durch diese Maßnahmen erhoben werden konnten. Die diskutierten Instrumentarien sind in der Strafverfolgung derzeit noch nicht angekommen. Dies liegt wahrscheinlich daran, dass die wenigen freigegebenen Spähprogramme mit ihren eingeschränkten Funktionen für die behördliche Ermittlung nicht ausreichend sind. Für die Forschung und Entwicklung der Überwachungssoftware gibt es die neugegründete Behörde ZITiS, die sich im Aufbau befindet und noch nicht genügend Personal mit entsprechendem technischem Fachwissen hat. Es wäre wichtig, einen leistungsfähigen Werkzeugkasten mit differenzierten Softwarelösungen zur Verfügung zu haben, um auf die unterschiedlichen Fälle der auszuspähenden IT-Systeme reagieren können. Außerdem müssen die Spähprogramme stets aktualisiert werden, damit sie mit dem schnelllebigen informationstechnischen Bereich Schritt halten können. Die Forderung der Nachrichtendienstler, die Werkzeuge zur geheimdienstlichen Überwachung durch den Verfassungsschutz oder BND zu nutzen, ist gesetzlich noch

nicht geregelt.[216] Dies könnte zu Synergieeffekten führen, bei denen Personal und finanzielle Mittel für die Entwicklung gebündelt werden. Bedeutsam ist dabei auch ein reger Austausch zwischen den Strafverfolgungsbehörden wie BKA und LKA mit dem ZITiS, um zum Einen die Anforderungen der Praktiker besser in die Entwicklungsarbeit einzubringen und andererseits durch Schulungen der Ermittler die Zeitspanne zwischen Programmierung und Anwendung zu verkürzen. Eine Zusammenarbeit mit anderen Ländern in der EU bzw. weltweit kann sich zudem vorteilhaft erweisen, weil einige Staaten wie Amerika oder Großbritannien mit ihrem Kenntnisstand bezüglich Überwachungssoftware Deutschland weit voraus sind. Zum Ausleiten der Daten bei der Online-Durchsuchung und Quellen-TKÜ werden die richtigen Schnittstellen z. B. vor der Verschlüsselung benötigt. Dazu sollten Möglichkeiten überlegt werden, die Hersteller der Anwendungsprogramme und Betriebssysteme zur Kooperation zu bewegen. Dadurch kann die Forschung und Entwicklung der Bundestrojaner durch Insiderwissen über den Quellcode oder Sicherheitslücken der Programme früher und zielgerichteter darauf abgestimmt werden. Sicherheitslücken können auch dazu verwendet werden, das Spähprogramm unbemerkt auf die Geräte zu installieren. Da die Hersteller diese durch Updates immer wieder schließen, woran der Staat auch Interesse hat, ist eine schnelle Umsetzung in die Überwachungssoftware wichtig, um sie eine gewisse Zeit ausnutzen zu können. Das Erwerben von Informationen zu Sicherheitslücken bei kommerziellen Hackern bringt zwar einen Zeitvorsprung für die Entwicklung, erscheint aber bedenklich, da dieses Wissen nicht exklusiv dem Staat, sondern auch kriminellen Kreisen zur Verfügung gestellt wird. Beim Umgang mit Sicherheitslücken steht das Strafverfolgungsinteresse in Konkurrenz mit dem Schutz der Bürger und der Wirtschaft vor Schaden. Fragwürdig erscheint die Doppelmoral in der Gesellschaft, die zum Teil die repressiven Maßnahmen der Online-Durchsuchung und Quellen-TKÜ aufgrund ihrer Eingriffsintensität als Vergeheimdienstlichung[217] des Strafverfahrens sieht, aber in sozialen Medien häufig Details aus ihrem Privatleben sorglos preisgibt und mit ihren persönlichen Daten die kostenlose Nutzung dieser Netzwerke bezahlt.[218] Es sollten diesen Maßnahmen die Zeit und Chance gegeben werden, ihre Effektivität für die Strafverfolgung unter Beweis zu stellen.

[216] Vgl. Flade, 2018.
[217] Vgl. Singelnstein/Derin, NJW 2017, 2646 (2652).
[218] Vgl. Paal/Hennemann, ZRP 2017, 215 (216).

Literaturverzeichnis

Beuckelmann, Stephan: Online-Durchsuchung und Quellen-TKÜ. In: NJW-Spezial 2017, S. 440.

BKA: Quellen-TKÜ und Online-Durchsuchung – Notwendigkeit, Sachstand und Rahmenbedingungen. URL: <https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html>, Version: 2018, verfügbar am 13.03.18, 15:23.

Buermeyer, Ulf: Gutachterliche Stellungnahme zur Öffentlichen Anhörung zur „Formulierungshilfe“ des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKÜ im Strafprozess – Ausschuss-Drucksache 18(6)334. URL: < https://www.bundestag.de/blob/508848/bdf7512e32578b699819a5aa33dde93c/buermeyer-data.pdf>, S. 1 – 26, Version: 29.05.17, verfügbar am 12.08.18, 16:55.

Chaos Computer Club (CCC): Analyse einer Regierungs-Malware. URL: <https://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf>, Version: 08.10.11, verfügbar am 30.07.2018, 14:23.

Europol: The Internet Organised Crime Threat Assessment (IOCTA) 2016. URL: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016>, verfügbar am 31.07.2018, 16:06.

Flade, Florian: Der neue Bundestrojaner? Noch nie im Einsatz!. URL: <https://www.welt.de/politik/deutschland/article173121473/Verdeckte-Ueberwachung-Ministerium-gibt-neuen-Bundestrojaner-fuer-den-Einsatz-frei.html>, Version: 22.09.17, verfügbar am 08.08.18, 12:02.

Flade, Florian: Ministerium gibt neuen Bundestrojaner für den Einsatz frei. URL: <https://www.welt.de/politik/deutschland/article173121473/Verdeckte-Ueberwachung-Ministerium-gibt-neuen-Bundestrojaner-fuer-den-Einsatz-frei.html>, Version: 02.02.18, verfügbar am 08.08.18, 12:02.

Flade, Florian: Bundestrojaner: Kein Einsatz trotz Genehmigung. URL:<https://investigativ.welt.de/2018/02/23/bundestrojaner-kein-einsatz-trotz-genehmigung/>, Version: 23.02.18, verfügbar am 08.08.18, 11:56.

Greven, Michael: Stellungnahme zum Gesetzentwurf zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze. URL: <https://www.bundestag.de/blob/508850/76fc6296143a5eba18aff59fce987bb8/greven_drb-data.pdf>, S. 1 – 12, Version: 29.05.17, verfügbar am 12.08.18, 18:05.

Grunert, Marlene: Bundestrojaner – Durch die Hintertür zur Online-Überwachung. URL: <http://www.faz.net/aktuell/politik/online-durchsuchung-quellen-tkue-bundestrojaner-wird-gesetz-15071053.html>, Version: 22.06.17, verfügbar am 13.03.18, 15:22.

Henzler, Peter: Anhörung des Vizepräsidenten des Bundeskriminalamtes Peter Henzler im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages am 31. Mai 2017

zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze hier: zum Thema Quellen-TKÜ und Online-Durchsuchung in der StPO gem. Formulierungshilfe der BReg. URL: <https://www.bundestag.de/blob/509190/ce315ac513c903afc986b8110078ddea/henzler-data.pdf>, S. 1 – 10, Version: 31.05.17, verfügbar am 12.08.18, 18:40.

Jarass, Hans Dieter ; Pieroth, Bodo: Grundgesetz für die Bundesrepublik Deutschland – Kommentar. 15. Aufl. München: Beck, 2018.

Kohlmann, Diana: Online-Durchsuchungen und andere Maßnahmen mit Technikeinsatz – Bedeutung und Legitimation ihres Einsatzes im Ermittlungsverfahren. 1. Aufl. Baden-Baden: Nomos, 2012.

Koops, Bert-Jaap ; Goodwin, Morag: Cyberspace, the cloud, and cross-border criminal investigation – The limits and possibilities of international law. – 2014. S. 1 – 101. Tilburg, Tilburg University, TILT – Tilburg Institute for Law, Technology, and Society, CTLD – Center for Transboundary Legal Development. URL: <http://www.wodc.nl/binaries/2326-volledige-tekst_tcm28-73009.pdf>, verfügbar am 31.07.2018, 15:40.

Krauß, Matthias: Stellungnahme zum Gesetzentwurf zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze. URL: <https://www.bundestag.de/blob/509046/5aa0ea61c4f3df0429208b5fda260a0a/krauss-data.pdf>, S. 1 – 12, Version: 30.05.17, verfügbar am 12.08.18, 18:10.

Lipp, Sebastian ; Hoppenstedt, Max: Exklusiv: Wie das BKA Telegram-Accounts von Terrorverdächtigen knackt. URL: <https://motherboard.vice.com/de/article/pgk7gv/exklusiv-wie-das-bka-telegram-accounts-von-terrorverdaechtigen-knackt>, Version: 26.08.16, verfügbar am 17.04.18, 16:55.

Meyer-Goßner, Lutz ; Schmitt, Bertram: Strafprozessordnung – Kommentar. 61. Aufl. München: Beck, 2018.

Neuhaus, Heike: Strafverfolger brauchen Zugriff auf verschlüsselte Kommunikation. In: Deutsche Richterzeitung (DRiZ) 2017, Nr. 06, S. 192 – 193.

Niederhuber, Tanja: Die StPO-Reform 2017 – wichtige Änderungen im Überblick. In: Juristische Arbeitsblätter (JA) 2018, Nr. 3, S. 169 – 175.

Paal, Boris P. ; Hennemann, Moritz: Rechtspolitik im digitalen Zeitalter. In: Zeitschrift für Rechtspolitik (ZRP) 2017, Nr. 7, S. 215 – 216.

Pohl, Hartmut: Zur Technik der heimlichen Online-Durchsuchung. In: Datenschutz und Datensicherheit (DuD) 2007, Nr. 31, S. 684 – 688.

Rath, Christian: BKA-Trojaner zur Überwachung – Generalbundesanwalt will Regelung. URL: <http://www.taz.de/!5373564/>, Version: 20.01.17, verfügbar am 17.04.18, 16:44.

Rebiger, Simon: Bundeskriminalamt knackt 44 Telegram-Accounts in zwei Jahren. URL: <https://netzpolitik.org/2016/bundeskriminalamt-knackt-44-telegram-accounts-in-zwei-jahren/>, Version: 08.12.16, verfügbar am 05.08.18, 9:40.

Roggan, Fredrik: Die strafprozessuale Quellen-TKÜ und Online-Durchsuchung: Elektronische Überwachungsmaßnahme mit Risiken für Beschuldigte und die Allgemeinheit. In: Strafverteidiger (StV) 2017, Nr. 12, S. 821 – 829.

Sachs, Michael: Grundgesetz – Kommentar. 8. Aufl. München: Beck, 2018.

Schaar, Peter: Online-Ermittlung in Europa – Überwachung, Fahndung, Rechtliches, Datenschutz, Technik. URL: <https://www.bfdi.bund.de/DE/Infothek/Reden_Interviews/2008/30_01OnlineErmittlungInEuropa.html>, Version: 30.01.08, verfügbar am 09.08.18, 11:16.

Singelnstein, Tobias: Hacken zur Strafverfolgung? Gefahren und Grenzen der strafprozessualen Online-Durchsuchung. URL: <https://verfassungsblog.de/hacken-zur-strafverfolgung-gefahren-und-grenzen-der-strafprozessualen-online-durchsuchung/>, Version: 02.07.17, verfügbar am 13.03.18, 15:52.

Singelnstein, Tobias ; Derin, Benjamin: Das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens – Was ist aus der StPO-Reform geworden. In: Neue Juristische Wochenschrift (NJW) 2017, S. 2646 – 2652.

Sinn, Arndt: Stellungnahme zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze – BT-Drucksache 18/11272 sowie zur Formulierungshilfe der Bundesregierung für einen Änderungsantrag zum o.g. Gesetzentwurf (Ausschussdrucksache 18(6)334). URL: <https://www.bundestag.de/blob/509050/6f72dd42df72be6f2da6a024475b3f8a/sinn-data.pdf>, S. 1 – 12, Version: 30.05.17, verfügbar am 12.08.18, 16:25.

Stoklas, Jonathan ; Wendorf, Joris: Der Staatstrojaner – verhältnismäßig unverhältnismäßig?. In: ZD-Aktuell 2017, Nr. 05725.

Tinnefeld, Marie-Theres: Die „Staatstrojaner“ aus verfassungsrechtlicher Sicht – Gedanken zum Prüfbericht des Bayerischen Landesbeauftragten für den Datenschutz. In: Zeitschrift für Datenschutz (ZD) 2012, Nr. 10, S. 451 – 454.

Warken, Claudia: Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus, Teil 2 – Beweisverwertung im Zeitalter der digitalen Cloud und datenspezifische Regelungen in der StPO. In: Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht (NZWiSt) 2017, S. 329 – 338.

Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Mittweida, 20.08.2018

Anlage

Deutscher Bundestag **Drucksache 16/3492**

16. Wahlperiode 21. 11. 2006

Entschließungsantrag

der Abgeordneten Jürgen Koppelin, Ulrike Flach, Otto Fricke, Dr. Claudia Winterstein, Gisela Piltz, Jens Ackermann, Dr. Karl Addicks, Daniel Bahr (Münster), Uwe Barth, Rainer Brüderle, Angelika Brunkhorst, Ernst Burgbacher, Patrick Döring, Mechthild Dyckmans, Jörg van Essen, Horst Friedrich (Bayreuth), Dr. Edmund Peter Geisen, Hans-Michael Goldmann, Miriam Gruß, Dr. Christel Happach-Kasan, Heinz-Peter Haustein, Birgit Homburger, Dr. Werner Hoyer, Michael Kauch, Hellmut Königshaus, Gudrun Kopp, Heinz Lanfermann, Harald Leibrecht, Michael Link (Heilbronn), Horst Meierhofer, Jan Mücke, Burkhardt Müller-Sönksen, Hans-Joachim Otto (Frankfurt), Detlef Parr, Jörg Rohde, Frank Schäffler, Marina Schuster, Dr. Hermann Otto Solms, Carl-Ludwig Thiele, Christoph Waitz, Dr. Volker Wissing, Hartfrid Wolff (Rems-Murr), Martin Zeil, Dr. Guido Westerwelle und der Fraktion der FDP

zu der dritten Beratung des Gesetzentwurfs der Bundesregierung
– Drucksachen 16/2300, 16/2302, 16/3106, 16/3123, 16/3124, 16/3125 –

Entwurf eines Gesetzes
über die Feststellung des Bundeshaushaltsplans für das Haushaltsjahr 2007
(Haushaltsgesetz 2007)

hier: Einzelplan 06
Geschäftsbereich des Bundesministeriums des Innern

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

1. Mit Datum vom 24. Oktober 2006 hat das Bundesministerium des Innern das „Programm zur Stärkung der inneren Sicherheit“ (PSIS) dem Haushaltsausschuss des Deutschen Bundestages für seine Sitzung am 26. Oktober 2006 vorgelegt. Das Programm wurde nachträglich in das parlamentarische Verfahren zur Beratung über den Haushalt 2007 eingebracht.

   Bei den Beratungen zum Etat des Bundesinnenministeriums am 25. Oktober 2006 lag dem Innenausschuss das PSIS nicht vor. Erst auf Antrag der Opposition wurde das Programm auf die Tagesordnung der Innenausschusssitzung am 8. November 2006 gesetzt und dort ohne Beschlussfassung erörtert.

2. Das PSIS hat das Ziel, der fortbestehenden Bedrohungslage durch den Aufbau der operativen und der einsatz- und ermittlungsunterstützenden Instrumentarien beim Bundesamt für Verfassungsschutz, Bundeskriminalamt, Bundespolizei und Bundesamt für Sicherheit in der Informationstechnik wirksam entgegenzutreten.

   Das Maßnahmenpaket des PSIS sieht ein Gesamtvolumen von 132 Mio. Euro für die Jahre 2007 bis 2009 vor. Für das Bundesamt für Verfassungsschutz wird hierbei ein Mittelbedarf von 64,77 Mio. Euro festgestellt. Auf das Bundeskriminalamt entfällt ein Mittelbedarf von 34,75 Mio. Euro. Für die Bundespolizei sind 28,47 Mio. Euro und für das Bundesamt für Sicherheit in der Informationstechnik 4 Mio. Euro veranschlagt.

3. Die Mittel für die Bundespolizei umfassen u. a. die Beschaffung weiterer Sprengstoffspürhunde sowie die Anschaffung zusätzlicher Hubschrauber mit Wärmebildkameras, um den Schutz der Bahnanlagen vor möglichen Anschlägen zu verstärken.

   Auch die Verstärkung der Kapazitäten des Bundeskriminalamtes für sprachmittlerische Leistungen, insbesondere im arabischen Sprachumfeld, ist Bestandteil des Maßnahmenpakets.

   Die Bereitstellung dieser zusätzlichen Mittel wird begrüßt.

4. Das PSIS sieht weiter vor, die Sicherung der Kommunikationsstrukturen zu verbessern. So soll das Bundesamt für Sicherheit in der Informationstechnik beauftragt werden, eine Konzeption von sicheren und verfügbaren Kommunikationsarchitekturen, ausgerichtet auf die speziellen Anforderungen der Verteilung und Auswertung von Früherkenntnissen aus dem terroristischen Umfeld, zu entwickeln. Dabei sollen Vertraulichkeit, Verfügbarkeit, Mobilität, Schnelligkeit und weltweite Einsatzfähigkeit gewährleistet werden. Der zusätzlich zum BOS-Digitalfunk bestehende Bedarf wird damit begründet, dass der BOS-Digitalfunk nicht für den Einsatz in allen Geheimhaltungsstufen geeignet sei.

5. Das PSIS enthält Mittelanforderung für Maßnahmen, denen eine gesetzliche Grundlage fehlt:

   – So befindet sich zum Beispiel der Gesetzentwurf zu der in „Maßnahme 4 BKA“ enthaltenen Anti-Terror-Datei noch im parlamentarischen Verfahren.

   – Die „Maßnahme 3 BKA“ – Aufbau der Kompetenz/Auswertung und Analyse technischer Messdaten – enthält als Schwerpunkt den Ausbau der technischen Fähigkeit zur Onlineüberwachung. Entfernte PCs sollen auf verfahrensrelevante Inhalte hin durchsucht werden können, ohne tatsächlich am Standort des Geräts anwesend zu sein. Auch hierfür fehlt eine Rechtsgrundlage.

   – Zudem soll das Bundesamt für Sicherheit in der Informationstechnik beauftragt werden, Bildverarbeitungsfunktionen für biometrische Merkmale auszuarbeiten. Es soll eine Software entwickelt werden, welche es den Polizeibehörden ermöglicht, die Aufnahmen von Überwachungskameras anhand automatisierter Verhaltensmustererkennung auszuwerten und die betreffenden Personen anhand einer Gesichtserkennungssoftware mittels biometrischer Daten zu identifizieren. Dieses Verfahren soll auf Verkehrsknotenpunkten wie Bahnhöfen zum Einsatz kommen. Rechtliche Voraussetzungen für diese Maßnahme bestehen nicht.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

1. die Bewilligung von Haushaltsmitteln nicht auf Maßnahmen zu beziehen, denen eine gesetzliche Grundlage fehlt;
2. den Einsatz von automatisierter Gesichtserkennung anhand biometrischer Merkmale bei der Überwachung von Verkehrsknotenpunkten abzulehnen. Insbesondere spricht sich der Deutsche Bundestag gegen die Schaffung einer zentralen Datei mit biometrischen Daten zu diesem Zweck aus. Der Einsatz dieser Technik muss sich an dem Grundsatz der informationellen Selbstbestimmung im Sinne der Rechtsprechung des Bundesverfassungsgerichts orientieren;
3. den BOS-Digitalfunk dahingehend zu prüfen, ob dieser den Anforderungen an eine sichere Kommunikationsinfrastruktur in allen Geheimhaltungsstufen gerecht wird und somit kein weiterer Bedarf an zusätzlichen Kommunikationsinfrastrukturen besteht. Über das Ergebnis der Prüfung ist dem Deutschen Bundestag innerhalb von drei Monaten zu berichten. Die Anforderungen an den BOS-Digitalfunk sind ggf. entsprechend nachzubessern.

Berlin, den 21. November 2006

Dr. Guido Westerwelle und Fraktion

Deutscher Bundestag
Ausschuss für
Recht und Verbraucherschutz

Ausschussdrucksache
18(6)361

19. Juni 2017

Deutscher Bundestag

18.Wahlperiode

Ausschuss für Recht und Verbraucherschutz

16. Juni 2017

Änderungsantrag

der Fraktionen der CDU/CSU und SPD

zu dem Gesetzentwurf der Bundesregierung

Zusammenstellung

des Entwurfs eines Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens

– Drucksache 18/11277 –

mit den Beschlüssen des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss)

Seite 2 – 4 fehlen.

Entwurf	Beschlüsse des 6. Ausschusses
	2. In § 89a Absatz 1 Satz 5 wird die Angabe „§ 454b Abs. 3“ durch die Angabe „§ 454b Absatz 4“ ersetzt.
Artikel *1*	**Artikel 3**
Änderung der Strafprozessordnung	**Änderung der Strafprozessordnung**
Die Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel *2 Absatz 5* des Gesetzes vom *4. November 2016* (BGBl. I S. *2460*) geändert worden ist, wird wie folgt geändert:	Die Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel **3** des Gesetzes vom **13. April 2017** (BGBl. I S. **872**) 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“.
1. § 26 Absatz 1 Satz 2 wird wie folgt gefasst:	**2.** u n v e r ä n d e r t
„Das Gericht kann dem Antragsteller aufgeben, ein in der Hauptverhandlung angebrachtes Ablehnungsgesuch innerhalb einer angemessenen Frist schriftlich zu begründen.“	
2. In § 26a Absatz 1 Nummer 2 werden nach dem Wort „nicht“ die Wörter „oder nicht innerhalb der nach § 26 Absatz 1 Satz 2 bestimmten Frist“ eingefügt.	**3.** u n v e r ä n d e r t

Entwurf	Beschlüsse des 6. Ausschusses
3. § 29 wird wie folgt geändert:	**4.** unverändert
a) Dem Absatz 1 wird folgender Satz angefügt:	
„Wird ein Richter vor Beginn der Hauptverhandlung abgelehnt und würde eine Entscheidung über die Ablehnung den Beginn der Hauptverhandlung verzögern, kann diese vor der Entscheidung über die Ablehnung durchgeführt werden, bis der Staatsanwalt den Anklagesatz verlesen hat.“	
b) Folgender Absatz 3 wird angefügt:	
„(3) Hat das Gericht dem Antragsteller gemäß § 26 Absatz 1 Satz 2 aufgegeben, das Ablehnungsgesuch innerhalb einer bestimmten Frist schriftlich zu begründen, gilt Absatz 2 mit der Maßgabe entsprechend, dass über die Ablehnung spätestens bis zum Beginn des übernächsten Verhandlungstages nach Eingang der schriftlichen Begründung und stets vor Beginn der Schlussanträge zu entscheiden ist.“	
	5. Dem § 81a Absatz 2 wird folgender Satz angefügt:
	„Die Entnahme einer Blutprobe bedarf abweichend von Satz 1 keiner richterlichen Anordnung, wenn bestimmte Tatsachen den Verdacht begründen, dass eine Straftat nach § 315a Absatz 1 Nummer 1, Absatz 2 und 3, § 315c Absatz 1 Nummer 1 Buchstabe a, Absatz 2 und 3 oder § 316 des Strafgesetzbuchs begangen worden ist.“
4. § 81e wird wie folgt geändert:	**6.** unverändert
a) Absatz 1 wird wie folgt gefasst:	

Entwurf	Beschlüsse des 6. Ausschusses
„(1) An dem durch Maßnahmen nach § 81a Absatz 1 oder § 81c erlangten Material dürfen mittels molekulargenetischer Untersuchung das DNA-Identifizierungsmuster, die Abstammung und das Geschlecht der Person festgestellt und diese Feststellungen mit Vergleichsmaterial abgeglichen werden, soweit dies zur Erforschung des Sachverhalts erforderlich ist. Andere Feststellungen dürfen nicht erfolgen; hierauf gerichtete Untersuchungen sind unzulässig.“	
b) Absatz 2 wird wie folgt geändert:	
aa) In Satz 1 wird das Wort „Spurenmaterial“ durch das Wort „Material“ ersetzt.	
bb) In Satz 2 werden die Wörter „Absatz 1 Satz 3“ durch die Wörter „Absatz 1 Satz 2“ ersetzt.	
cc) Folgender Satz wird angefügt:	
„Ist bekannt, von welcher Person das Material stammt, gilt § 81f Absatz 1 entsprechend.“	
5. § 81h wird wie folgt geändert:	**7.** u n v e r ä n d e r t
a) In Absatz 1 werden in dem Satzteil nach Nummer 3 nach den Wörtern „ob das Spurenmaterial von diesen Personen“ die Wörter „oder von ihren Verwandten in gerader Linie oder in der Seitenlinie bis zum dritten Grad“ eingefügt.	
b) Absatz 3 wird wie folgt gefasst:	

Entwurf	Beschlüsse des 6. Ausschusses
„(3) Für die Durchführung der Maßnahme gilt § 81f Absatz 2 entsprechend. Die entnommenen Körperzellen sind unverzüglich zu vernichten, sobald sie für die Untersuchung nach Absatz 1 nicht mehr benötigt werden. Soweit die Aufzeichnungen über die durch die Maßnahme festgestellten DNA-Identifizierungsmuster zur Erforschung des Sachverhalts nicht mehr erforderlich sind, sind sie unverzüglich zu löschen. Die Vernichtung und die Löschung sind zu dokumentieren.“	
c) Absatz 4 Satz 2 wird wie folgt gefasst:	
„Vor Erteilung der Einwilligung sind sie schriftlich auch darauf hinzuweisen, dass	
1. die entnommenen Körperzellen ausschließlich zur Feststellung des DNA-Identifizierungsmusters, der Abstammung und des Geschlechts untersucht werden und dass sie unverzüglich vernichtet werden, sobald sie hierfür nicht mehr erforderlich sind,	
2. das Untersuchungsergebnis mit den DNA-Identifizierungsmustern von Spurenmaterial automatisiert daraufhin abgeglichen wird, ob das Spurenmaterial von ihnen oder von ihren Verwandten in gerader Linie oder in der Seitenlinie bis zum dritten Grad stammt,	
3. das Ergebnis des Abgleichs zu Lasten der betroffenen Person oder mit ihr in gerader Linie oder in der Seitenlinie bis zum dritten Grad verwandter Personen verwertet werden darf und	

Entwurf	Beschlüsse des 6. Ausschusses
4. die festgestellten DNA-Identifizierungsmuster nicht zur Identitätsfeststellung in künftigen Strafverfahren beim Bundeskriminalamt gespeichert werden.“	
	8. § 100a wird wie folgt geändert:
	a) Dem 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:

Entwurf	Beschlüsse des 6. Ausschusses
	„(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

Entwurf	Beschlüsse des 6. Ausschusses
	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.“
6. § 100b *Absatz 6 Nummer 2* wird wie folgt gefasst:	**9.** § 100b wird wie folgt gefasst:
„2. die Anzahl der Überwachungsanordnungen nach § 100a Absatz 1, unterschieden nach Erst- und Verlängerungsanordnungen;“.	**„§ 100b**
	Online-Durchsuchung

Entwurf	Beschlüsse des 6. Ausschusses
	(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,

Entwurf	Beschlüsse des 6. Ausschusses
	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, §§ 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,

Entwurf	Beschlüsse des 6. Ausschusses
	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,

Entwurf	Beschlüsse des 6. Ausschusses
	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,

Entwurf	Beschlüsse des 6. Ausschusses
	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.“
	10. § 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.

Entwurf	Beschlüsse des 6. Ausschusses
	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.
	11. 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.

Entwurf	Beschlüsse des 6. Ausschusses
	(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

Entwurf	Beschlüsse des 6. Ausschusses
	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:

Entwurf	Beschlüsse des 6. Ausschusses
	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,

Entwurf	Beschlüsse des 6. Ausschusses
	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.

Entwurf	Beschlüsse des 6. Ausschusses
	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.“

Seite 23 – 47 fehlen.

Zur Begründung der Beschlussempfehlung

Der Ausschuss hat den Entwurf eines Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens (Drucksache 18/11277) mit dem Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, der Strafprozessordnung, des Jugendgerichtsgesetzes und weiterer Gesetze (Drucksache 18/11272) verbunden und um Regelungen zur Schaffung von Rechtsgrundlagen für die Online-Durchsuchung und die Quellen-Telekommunikationsüberwachung ergänzt (Drucksache 18(6)334 vom 15. Mai 2017).

Zur Begründung der ursprünglichen Inhalte des Entwurfs eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze wird auf die Drucksache 18/11272 verwiesen, soweit diese unverändert übernommen wurden. Dies betrifft die verschärfte Strafbarkeit organisierter Formen von Schwarzarbeit (Artikel 1 Nummer 3), die Erleichterung der Strafzurückstellung bei betäubungsmittelabhängigen Mehrfachtätern (Artikel 3 Nummer 36 und 37), die Schaffung einer gesetzlichen Grundlage für die Datenübermittlung durch die Bewährungshilfe (Artikel 3 Nummer 40 und 41) sowie eine europarechtlich gebotene Erweiterung bestimmter Straftatbestände im Bundesnaturschutzgesetz (Artikel 7).

Für die Erweiterung des Fahrverbots auf alle Straftaten im Allgemeinen Strafrecht und im Jugendstrafrecht (Artikel 1 Nummer 1 und Artikel 2) sind aufgrund der Sachverständigenanhörung am 22. März 2017 eher geringfügige bzw. klarstellende Änderungen vorgesehen, die im Folgenden im Einzelnen begründet werden. Gleiches gilt für die Einschränkung des Richtervorbehalts bei der Blutprobenentnahme im Zusammenhang mit Straßenverkehrsdelikten (Artikel 3 Nummer 5). Insoweit enthält der Regelungstext eine Ergänzung, die Begründung eine Klarstellung. Soweit der Gesetzentwurf in den beiden vorgenannten Punkten unverändert geblieben ist, wird auf die Begründung in der Drucksache 18/11272 verwiesen.

Die neu hinzugekommenen Regelungen zur Schaffung von Rechtsgrundlagen für die Quellen-Telekommunikationsüberwachung und die Online-Durchsuchung in der Strafprozessordnung (Artikel 3 Nummer 8 ff.) werden umfassend begründet.

Der ursprüngliche Entwurf eines Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens enthält lediglich in § 136 Absatz 4 der Strafprozessordnung in der Entwurfsfassung – StPO-E (Artikel 3 Nummer 17 Buchstabe b) eine klarstellende Änderung zur audiovisuellen Aufzeichnung von Beschuldigtenvernehmungen. Die bisher in Artikel 1 Nummer 6 und 7 StPO-E enthaltenen Anpassungen der geltenden jährlichen Berichtspflichten an die aktuellen technischen Entwicklungen haben in den neuen Vorschlag zur Schaffung einer Rechtsgrundlage für die Online-Durchsuchung und die Quellen-Telekommunikationsüberwachung Eingang gefunden; entsprechend wurde auch die Übergangsvorschrift im Einführungsgesetz zur Strafprozessordnung (EGStPO) angepasst.

Zu Artikel 1 (Änderung des Strafgesetzbuches – StGB)

Zu Nummer 1

Zu Buchstabe a Doppelbuchstabe bb (Änderung des § 44 Absatz 1 Satz 2)

Mit der vorgeschlagenen Ergänzung von § 44 Absatz 1 des Strafgesetzbuches in der Entwurfsfassung (StGB-E) um einen neuen Satz 2 soll die von den Sachverständigen Dr. Bode (schriftliche Stellungnahme, S. 2), Ohlenschlager (schriftliche Stellungnahme, S. 4 f.) und mit Einschränkung auch bei Prof. Dr. Schöch (schriftliche Stellungnahme, S. 3) erhobene Forderung aufgegriffen werden, im Gesetz selbst Vorgaben zu machen, wann die Verhängung eines Fahrverbots, insbesondere bei Straftaten ohne Verkehrsbezug, nach der Neuregelung in Betracht kommt. Wenngleich insoweit Bedenken im Hinblick auf den Bestimmtheitsgrundsatz aus den im Gesetzentwurf der Bundesregierung genannten Gründen

Seite 49 – 51 fehlen.

Zu Artikel 3 (Änderung der Strafprozessordnung – StPO)

Zu Nummer 1 (Änderung der Inhaltsübersicht)

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

Zu Nummer 5 (Änderung des § 81a)

Die in Bezug genommenen Straßenverkehrsdelikte des § 315a Absatz 1 Nummer 1 StGB und des § 315c Absatz 1 Nummer 1 Buchstabe a StGB sollen wie der ebenfalls in Bezug genommene § 316 StGB nicht nur Vorsatztaten, sondern auch die Begehungsformen der Fahrlässigkeit und des Versuchs erfassen. Dies wird im Gesetz ergänzend klargestellt.

Es wird nochmals hervorgehoben, dass die Ausnahme der in der Vorschrift genannten Straßenverkehrsdelikte von dem Erfordernis einer vorherigen richterlichen Anordnung eine grundsätzlich gleichrangige Anordnungskompetenz von Staatsanwaltschaft und Polizei zur Folge hat. Die Sachleitungsbefugnis der Staatsanwaltschaft steht dem nicht entgegen und bleibt davon unberührt. Der Staatsanwaltschaft bleibt es unbenommen, in Ausübung ihrer Sachleitungsbefugnis generalisierende Vorgaben zu machen, Fallgruppen zu bilden oder sich die Entscheidung im Einzelfall gänzlich vorzubehalten. Dies entspricht der derzeit gängigen Praxis in den Bundesländern und ermöglicht eine ebenso flexible Handhabung in der Zukunft.

Zu den Nummern 8 bis 16, 20, 21, 24 bis 26, 39 (Änderungen der §§ 100a ff.)

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 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 in Verbindung mit 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 Integrität 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 in Verbindung mit Artikel 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. Die Änderung 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.

Zu Nummer 8 (§ 100a)

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 in Verbindung mit 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 Artikels 2 Absatz 1 in Verbindung mit Artikel 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 Artikels 2 Absatz 1 in Verbindung mit Artikel 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 in Verbindung mit 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.

Die Regelung 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 in Verbindung mit 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.

Die Überwachung und Aufzeichnung von Messenger-Nachrichten nach § 100a Absatz 1 Satz 3 StPO-E ist somit einerseits inhaltlich auf Kommunikationsinhalte begrenzt, die bisher auch im Wege der herkömmlichen Telekommunikationsüberwachung ausgeleitet werden dürfen. Entwürfe von Nachrichten, die noch nicht abgeschickt wurden, werden nicht erfasst.

Die Maßnahme ist zudem zeitlich auf Messenger-Nachrichten begrenzt, die nach dem Ergehen des richterlichen Beschlusses, nach § 100e Absatz 1 Satz 4 StPO-E jedoch zunächst nur für die Dauer von drei Monaten, abgesendet werden. Innerhalb dieses Zeitraums gilt dies unabhängig davon, wann die Software auf das Gerät aufgebracht wird. Ziel der gesetzlichen Regelung ist es, ein funktionales Äquivalent zur derzeit möglichen herkömmlichen Ausleitung der Telekommunikation zu schaffen, die bei den Telekommunikationsunternehmen im öffentlichen Telekommunikationsnetz mit dem Vorliegen des Beschlusses auch faktisch erfolgen kann. Würden die Messenger-Nachrichten folglich unverschlüsselt als SMS versandt, könnten sie derzeit ab Erlass der richterlichen Anordnung überwacht und aufgezeichnet werden; dies soll künftig für die verschlüsselten Nachrichten ebenfalls gelten. Die Gefahr, dass der Zeitraum zwischen dem Erlass des richterlichen Beschlusses und dem Aufbringen der Software unbegrenzt lang ist und ein rückwirkendes Ausleiten daher erhebliche Zeiträume umfasst, besteht aufgrund der obligatorischen Befristung des Überwachungszeitraums nicht. Ein Überwachen und Aufzeichnen ist gemäß § 100e Absatz 1 Satz 4 StPO nur für maximal drei Monate zulässig und kann danach nur bei Fortbestehen der Anordnungsvoraussetzungen verlängert werden. Diese Befristungsregelung entspricht der Regelung im geltenden Recht. Kann innerhalb dieses Zeitraums künftig die Software nicht auf das Gerät aufgebracht werden, wird der Beschluss ungültig und die Maßnahme darf nicht mehr durchgeführt werden.

Ältere Nachrichten, die vor Erlass des richterlichen Beschlusses versandt wurden, dürfen auf der Grundlage des § 100a Absatz 1 Satz 3 StPO-E nicht erhoben werden. Eine solche rückwirkende Erhebung kann vielmehr ausschließlich als Online-Durchsuchung auf der Grundlage des § 100b StPO-E erfolgen, soweit die Voraussetzungen hierfür vorliegen.

Die zeitliche Begrenzung auf Messenger-Nachrichten, die ab dem Zeitpunkt des richterlichen Beschlusses abgesendet wurden, ist, wie in § 100a Absatz 5 Satz 1 Nummer 1 Buchstabe b StPO-E geregelt, auch technisch eindeutig sicherzustellen. Kann eine Trennung der Messenger-Nachrichten nach einzelnen Zeitpunkten durch die Software nicht vorgenommen werden oder existiert eine solche Software (noch) nicht, ist die Maßnahme auf der Grundlage des § 100a Absatz 1 Satz 3 StPO-E unzulässig.

Mit den in § 100a Absatz 6 StPO-E vorgesehenen Protokollierungspflichten werden die notwendigen Vorkehrungen geschaffen, um die nachträgliche Überprüfung zu gewährleisten, dass die Maßnahme von den Strafverfolgungsbehörden in rechtmäßiger Art und Weise durchgeführt wurde. Insbesondere wird dadurch die Prüfung ermöglicht, ob eine Software verwendet wurde, die den Anforderungen des § 100a Absatz 5 Satz 1 Nummer 1 Buchstabe b StPO-E genügt hat. Organisatorisch werden im Zuständigkeitsbereich des Bundes zudem bereits die Durchführung und die Protokollierung der Maßnahme in verschiedenen Einheiten des Bundeskriminalamtes getrennt vorgenommen. So wird bei der Vorbereitung, Durchführung und Nachbereitung der Maßnahme verfahrenstechnisch sichergestellt, dass die Vorgaben des Gesetzes in vollem Umfang eingehalten werden. Darüber hinaus besteht ein Prüfungsrecht des behördlichen Datenschutzbeauftragten sowie der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit im Rahmen ihrer gesetzlichen Kompetenzen.

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

Zu 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.

Zu Absatz 5

Der neu gestaltete Absatz 5 des § 100a fasst die in § 51 Absatz 2 Satz 1 Nummer 1 und § 49 Absatz 2 BKAG 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 (vgl. 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 § 49 Absatz 2 Nummer 1 und 2 und Satz 2 BKAG. 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.

Zu 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 § 82 Absatz 1 und Absatz 2 Nummer 8 Buchstabe b BKAG 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 § 82 Absatz 4 BKAG auch Verwendungs- und Löschungsvorschriften für die Protokollierung vorgesehen sind, 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 9 (§ 100b)

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 eigenständiger Ausprägung des Rechts auf informationelle Selbstbestimmung nach Artikel 2 Absatz 1 in Verbindung mit 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; 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.

Zu 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.

Zu Absatz 2

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

Die in Nummer 1 Buchstabe a aufgeführten §§ 98 Absatz 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.

Zu 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.

Zu 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 10 (§ 100c)

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 11 (§§ 100d, 100e)

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.

Zu § 100d

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 Satz 1, 100c Absatz 4 Satz 1 StPO.; 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 z. B. 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 Satz 2 bis 4, § 100c Absatz 5 Satz 2 bis 4 StPO), 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 Absatz 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 enthaltenen Vorschriften zum Schutz des Kernbereichs privater Lebensgestaltung bei der Wohnraumüberwachung in einer ergänzenden Regelung für die Erhebungs- und Auswertungsebene zusammen. Maßnahmen nach § 100c 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 An-

haltspunkte 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. 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 oben genannten 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 enthaltene Regelung zum Schutz von Zeugnisverweigerungsberechtigten, insbesondere Berufsgeheimnisträgern. Diese wird auf Maßnahmen der Online-Durchsuchung erstreckt.

Zu § 100e

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. 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, 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, 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 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 gegebenenfalls 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.

Absatz 4 enthält entsprechend der für die Wohnraumüberwachung bisher geltenden Regelung in § 100d Absatz 3 StPO. 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 a.F. (§ 51 BKAG g.F.) 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) zusammen und erstreckt die für die Wohnraumüberwachung geltenden – erweiterten – Bestimmungen auf die Online-Durchsuchung.

Absatz 6 enthält die bisher in § 100d Absatz 5 StPO 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 12 (§ 100f Absatz 4)

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Nummer 13 (§ 100i Absatz 3)

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Nummer 14 (§ 101)

Die Verfahrensregelungen bei verdeckten Maßnahmen in § 101 StPO 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 15 (§ 101aAbsatz 1)

Es handelt sich um redaktionelle Folgeänderungen.

Seite 67 – 68 fehlen.

Plenarprotokoll 18/240

Deutscher Bundestag

Stenografischer Bericht

240. Sitzung

Berlin, Donnerstag, den 22. Juni 2017

Inhalt:

Seite 2 – 117 fehlen.

(A) **Vizepräsidentin Ulla Schmidt:**

Vielen Dank. – Frau Kollegin Schwarzer, möchten Sie darauf antworten? – Bitte schön.

Christina Schwarzer (CDU/CSU):

Frau Präsidentin! Liebe Kollegin Hein, Sie haben sich eben Ihre Antwort eigentlich selbst gegeben. Ich glaube, ich habe das auch fünfmal in meiner Rede gesagt. Die Kommunen und die Länder sind dafür verantwortlich.

(Susanna Karawanskij [DIE LINKE]: Das kann man ja ändern!)

Und wenn die Kommunen und die Länder wollen, dass Schulsozialarbeit an jeder Schule stattfindet – Berlin gibt dafür sehr, sehr viel Geld aus;

(Özcan Mutlu [BÜNDNIS 90/DIE GRÜNEN]: Rot-Rot-Grün!)

im Übrigen auch zu Recht –, sollen sie dafür Geld ausgeben. Eine Änderung im SGB VIII, über die wir ja gerade verhandeln, wird es nicht geben.

(Beifall bei Abgeordneten der CDU/CSU – Zurufe von der LINKEN und der SPD)

Vizepräsidentin Ulla Schmidt:

Jetzt schließe ich diese Aussprache, und wir kommen zu den Abstimmungen.

Tagesordnungspunkt 12 a. Der Ausschuss empfiehlt unter Buchstabe a seiner Beschlussempfehlung die Ablehnung des Antrags der Fraktion Die Linke auf Drucksache 18/8420 mit dem Titel „Inklusive Bildung für alle – Ausbau inklusiver Schulen fördern“. Wer stimmt für diese Beschlussempfehlung? – Wer stimmt dagegen? – Wer enthält sich? – Damit ist die Beschlussempfehlung mit den Stimmen der Koalition gegen die Stimmen der Opposition angenommen.

(B)

Unter Buchstabe b seiner Beschlussempfehlung empfiehlt der Ausschuss die Ablehnung des Antrags der Fraktion Die Linke auf Drucksache 18/8421 mit dem Titel „Inklusive Bildung für alle – Ausbau inklusiver Bildung in der beruflichen Bildung umsetzen“. Wer stimmt für diese Beschlussempfehlung? – Wer stimmt dagegen? – Wer enthält sich? – Die Beschlussempfehlung ist mit den Stimmen der Koalition gegen die Stimmen der Opposition angenommen.

Weiterhin empfiehlt der Ausschuss unter Buchstabe c seiner Beschlussempfehlung die Ablehnung des Antrags der Fraktion Die Linke auf Drucksache 18/8889 mit dem Titel „Inklusive Bildung für alle – Ausbau inklusiver Bildung in der Kindertagesbetreuung umsetzen“. Wer stimmt für diese Beschlussempfehlung? – Wer stimmt dagegen? – Wer enthält sich? – Die Beschlussempfehlung ist mit den Stimmen der Koalitionsfraktionen gegen die Stimmen der Opposition angenommen.

Schließlich empfiehlt der Ausschuss unter Buchstabe d seiner Beschlussempfehlung die Ablehnung des Antrags der Fraktion Die Linke auf Drucksache 18/9127 mit dem Titel „Inklusive Bildung für alle – Ausbau inklusiver Hochschulen fördern“. Wer stimmt für diese Beschlussempfehlung? – Wer stimmt dagegen? – Wer enthält sich? – Die Beschlussempfehlung ist mit den Stimmen der Koalitionsfraktionen gegen die Stimmen der Fraktion Die Linke bei Enthaltung der Fraktion Bündnis 90/Die Grünen angenommen. (C)

Unter Tagesordnungspunkt 12 b liegt die Beschlussempfehlung des Ausschusses für Familie, Senioren, Frauen und Jugend zu dem Antrag der Fraktion Die Linke mit dem Titel „Schulsozialarbeit an allen Schulen sicherstellen“ vor. Der Ausschuss empfiehlt in seiner Beschlussempfehlung auf Drucksache 18/11803, den Antrag der Fraktion Die Linke auf Drucksache 18/2013 abzulehnen. Wer stimmt für diese Beschlussempfehlung? – Wer stimmt dagegen? – Wer enthält sich? – Die Beschlussempfehlung ist mit den Stimmen der Koalitionsfraktionen gegen die Stimmen der Fraktion Die Linke bei Enthaltung der Fraktion Bündnis 90/Die Grünen angenommen.

Damit kommen wir zu Zusatzpunkt 7:

– Zweite und dritte Beratung des von der Bundesregierung eingebrachten Entwurfs eines **Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens**

Drucksache 18/11277

– Zweite und dritte Beratung des von der Bundesregierung eingebrachten Entwurfs eines **Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze** (D)

Drucksache 18/11272

Beschlussempfehlung und Bericht des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss)

Drucksache 18/12785

Zu dem Gesetzentwurf zur Ausgestaltung des Strafverfahrens liegt ein Entschließungsantrag der Fraktion Bündnis 90/Die Grünen vor.

Nach einer interfraktionellen Vereinbarung sind für die Debatte 38 Minuten vorgesehen. – Ich höre hier keinen Widerspruch. Dann ist das so beschlossen. – Ich darf Sie bitten, Ihre Plätze einzunehmen.

Ich eröffne die Aussprache. Das Wort hat Bettina Bähr-Losse, SPD-Fraktion.

(Beifall bei der SPD)

Bettina Bähr-Losse (SPD):

Frau Präsidentin! Liebe Kolleginnen und Kollegen! Meine Damen und Herren! Heute soll der Bundestag eines der größten Gesetzesreformpakete dieser Legislaturperiode beschließen. Der vorliegende Entwurf sieht vor, das Gesetz zur effektiveren Ausgestaltung des Strafverfahrens mit den Gesetzen zur Änderung des Strafgesetzbuchs, der Strafprozessordnung, des Jugendgerichtsgesetzes und weiterer Gesetze zu verbinden und um Regelungen zur Schaffung von Rechtsgrundlagen für die

Bettina Bähr-Losse

(A) Onlinedurchsuchung und die Quellen-Telekommunikationsüberwachung zu ergänzen.

Ich gebe zu: Wo viel Licht ist, da ist auch Schatten. Man sollte vielleicht überdenken, ob es immer sinnvoll ist, solche großen Gesetzespakete zu schnüren und im Gesetzgebungsverfahren Einzelpakete als Junktim zu behandeln, oder ob es nicht transparenter wäre, die jeweiligen Gesetzentwürfe einzeln zu behandeln. Nichtsdestotrotz sehe ich in den nun vorliegenden Gesetzentwürfen eine überwältigende Leistung an parlamentarischer Arbeit. Jeder einzelne Gesetzentwurf nimmt gezielt Verbesserungen vor, sei es im Bereich der Strafprozessordnung oder sei es im Bereich der Strafverfolgung. Zum Ende der Legislaturperiode wird damit zum Abschluss gebracht, was sich die Koalition am Anfang vorgenommen hat.

Das Vorhaben geht auf die Vereinbarung aus dem Koalitionsvertrag zurück, das allgemeine und auch das Jugendstrafverfahren effektiver auszugestalten. Der Gesetzentwurf basiert auf der Arbeit einer eigens eingesetzten Expertenkommission.

(Hans-Christian Ströbele [BÜNDNIS 90/DIE GRÜNEN]: Nur wurde nichts übernommen!)

Im Anschluss an die ersten Lesungen der Entwürfe gab es intensive Beratungen, Berichterstattergespräche, Gespräche auf Fraktionsvizeebene und auch Gespräche im Koalitionsausschuss, und es gab zu allen – ich betone: zu allen – Aspekten öffentliche Anhörungen:

(Hans-Christian Ströbele [BÜNDNIS 90/DIE GRÜNEN]: Alles für die Katz!)

(B) zum Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens, zur geplanten Änderung des Strafgesetzbuches, zur geplanten Änderung der Strafprozessordnung, des Jugendgerichtsgesetzes und weiterer Gesetze. Auch die sogenannte Quellen-TKÜ und die Onlinedurchsuchung wurden intensiv erörtert. Insbesondere die Bedenken kritischer Sachverständiger sind in unsere Beratungen eingeflossen. Einige stellen jetzt die Behauptung auf, dieses Gesetz oder Teilaspekte davon seien quasi über Nacht und durch die Hintertür durchs Parlament gedrückt worden.

(Hans-Christian Ströbele [BÜNDNIS 90/DIE GRÜNEN]: Montag!)

Diejenigen, die das tun, verkennen aber, dass es sich um einen fast vierjährigen Prozess handelt,

(Dr. Volker Ullrich [CDU/CSU]: Hört! Hört! – Hans-Christian Ströbele [BÜNDNIS 90/DIE GRÜNEN]: Beweisen Sie das mal!)

an dem ich selber leider nur einige Monate teilnehmen konnte.

(Beifall bei der SPD sowie bei Abgeordneten der CDU/CSU)

Hierzu eine andere Auffassung zu vertreten, ist selbstverständlich legitim. Ich halte den Umstand, dass bis kurz vor Ende einer Legislaturperiode um einzelne Positionen gerungen wird, aber für nachvollziehbar und legitim, wenn es um den schmalen Grat zwischen der Durchsetzung des Strafanspruchs des Staates einerseits und der Wahrung und Gewährleistung von Grundrechten andererseits geht. (C)

(Beifall bei der SPD sowie bei Abgeordneten der CDU/CSU)

Mit einem Nacht-und-Nebel-Gesetz hat das aber rein gar nichts zu tun.

(Hans-Christian Ströbele [BÜNDNIS 90/DIE GRÜNEN]: Aber mit einem Hauruckverfahren!)

Nun zum Inhalt. Ich möchte nur die wichtigsten Aspekte herausstellen.

Ein Teil des Paketes ist die sogenannte StPO-Reform, die ein ehrgeiziges und wichtiges Ziel verfolgt, nämlich die Vereinfachung und Beschleunigung von Strafverfahren in allen Stadien.

(Hans-Christian Ströbele [BÜNDNIS 90/DIE GRÜNEN]: Wo ist die geblieben?)

Es geht hier etwa um Ablehnungsverfahren bei Befangenheitsgesuchen, die Möglichkeit einer Fristsetzung für Beweisanträge und die audiovisuelle Dokumentation von Beschuldigtenvernehmungen, um nur drei Beispiele zu nennen. Der Gesetzgeber begegnet ja häufig der Kritik, dass viel zu viel Zeit zwischen Straftat und Gerichtsverfahren vergeht. Diesem Problem soll im Gesetzentwurf auf der Ebene der Strafprozessordnung begegnet werden.

Ein zweites Ziel, das mit der Reform der Strafprozessordnung verfolgt wird, ist die Anpassung an die rasante technische Entwicklung der letzten Jahre. Hierzu ein kurzer Blick in die Geschichte der Spurensicherung und Strafverfolgung: 1897 überführte Scotland Yard den ersten Täter anhand seiner Fingerabdrücke. Fingerabdrücke als Beweismittel wurden erstmals 1896 in Argentinien und 1901 in Großbritannien vor Gerichten zugelassen. In Großbritannien und den USA ist der genetische Fingerabdruck in Strafprozessen als Beweismittel zur Identifizierung oder zum Ausschluss eines Tatverdächtigen seit 1987 zugelassen. 1997 ist in Deutschland erstmals eine rechtliche Regelung der Voraussetzungen für den Einsatz des genetischen Fingerabdrucks in Kraft getreten. (D)

(Hans-Christian Ströbele [BÜNDNIS 90/DIE GRÜNEN]: Das steht hier ja gar nicht zur Debatte!)

Das liegt nun aber auch schon wieder 20 Jahre zurück, und die Möglichkeiten der DNA-Analyse haben sich rasant weiterentwickelt.

Die Forensik hat wesentliche Fortschritte auf dem Gebiet der DNA-Analyse erzielt. Augen-, Haar- und Hautfarbe einer Person lassen sich mit hoher Wahrscheinlichkeit bestimmen. Denjenigen, die meinen, dass dadurch eine Stigmatisierung bestimmter Gruppen erfolge, halte ich entgegen, dass zahlreiche andere Verdächtige demgegenüber entlastet werden,

(Beifall bei Abgeordneten der SPD und der CDU/CSU)

(A) die vielleicht vorher unter Generalverdacht gestanden haben. Ist der Täter oder die Täterin blond und blauäugig, werden nun einmal die Schwarzhaarigen und die Braunäugigen entlastet. Das hat nichts mit Diskriminierung zu tun. Im Übrigen wäre eine Öffentlichkeitsfahndung ohne klare Benennung von Äußerlichkeiten wenig erfolgversprechend.

(Beifall bei Abgeordneten der SPD)

Drittens wollen wir unseren Strafverfolgungsbehörden mit den Regelungen zur Quellen-TKÜ und zur Onlinedurchsuchung ermöglichen, darauf reagieren zu können, dass auch Kriminelle neue technische Möglichkeiten nutzen. Die vorgeschlagenen Regelungen halten sich streng an die Vorgaben, die auch bei der Wohnraumüberwachung gelten. Traf man sich vor 20 Jahren noch in einer Wohnung, um kriminelle oder terroristische Aktivitäten zu planen, kann man sich heutzutage in einem Chatroom treffen. Der Gesetzgeber muss hierauf eine Antwort finden. Strafverfolger dürfen Kriminellen nicht hinterherhinken.

(Beifall bei der SPD sowie bei Abgeordneten der CDU/CSU)

Oft ist zu hören, dass die Polizei schon jetzt in der Lage sei, die Kommunikation der Bürgerinnen und Bürger zum Zwecke der Verhütung terroristischer Aktivitäten zu überwachen und entsprechend auszuwerten. Das stimmt aber gar nicht. Besonders schwierig wird es für die Ermittler, wenn es um Datenmaterial geht, das durch sogenannte Messengerdienste ausgetauscht wurde. Wenn (B) Behörden keinen Zugriff auf diese Daten haben, entstehen in der Folge Räume, in denen Strafverfolgung unmöglich ist. Das ergibt sich dann von selbst.

Unser Ziel muss also sein, die Behörden überhaupt erst in die Lage zu versetzen, ermitteln zu können. Die technische Entwicklung erlaubt uns dies jetzt erfreulicherweise. Deshalb treten wir mit unserem gemeinsamen Gesetzentwurf dafür ein, dass es künftig eine gesetzliche Regelung gibt, auf deren Grundlage besonders schwere Straftaten durch den Einsatz der sogenannten Quellen-TKÜ verfolgt werden können. Dabei möchte ich einen Aspekt betonen, der uns besonders wichtig ist. Diese Form der Überwachung, die vor der Verschlüsselung von Daten ansetzt, muss den Vorgaben genügen, die das Bundesverfassungsgericht in seinem BKA-Urteil im letzten Jahr aufgestellt hat. Die entworfene Regelung berücksichtigt also insbesondere den Verhältnismäßigkeitsgrundsatz, ist begrenzt auf den Schutz hinreichend wichtiger Rechtsgüter und gewährleistet dabei auch den Schutz Dritter.

(Beifall bei der SPD sowie des Abg. Dr. Patrick Sensburg [CDU/CSU])

Vizepräsidentin Ulla Schmidt:

Frau Kollegin, denken Sie an die Zeit und kommen Sie zum Schluss.

Bettina Bähr-Losse (SPD):

Ich überspringe jetzt einfach einen Teil.

Vizepräsidentin Ulla Schmidt: (C)

Ja, bitte bis zum letzten Satz.

(Heiterkeit bei der CDU/CSU und der SPD)

Bettina Bähr-Losse (SPD):

Mit dem vorliegenden Gesetzentwurf geben wir unserer Justiz Mittel an die Hand, um auf die Herausforderungen der Gegenwart überhaupt reagieren zu können. Ich bitte deshalb um Unterstützung.

(Beifall bei der SPD und der CDU/CSU)

Vizepräsidentin Ulla Schmidt:

Vielen Dank. – Jetzt hat der Kollege Jörn Wunderlich für die Fraktion Die Linke das Wort.

(Beifall bei der LINKEN – Zuruf von der CDU/CSU: Am besten bis zum letzten Satz!)

Jörn Wunderlich (DIE LINKE):

Frau Präsidentin! Liebe Kolleginnen und Kollegen! Führerscheinentzug als Hauptstrafe, Überwachung von Anbahnungsgesprächen des Verteidigers mit inhaftierten Mandanten, Blutentnahmen ohne richterlichen Vorbehalt, Videoaufzeichnung der ersten Vernehmung eines Beschuldigten – all das war Gegenstand des Gesetzes in der ersten Lesung. Daneben gab es noch einige Regelungen zur Veruntreuung von Arbeitsentgelt und zum Naturschutz; Naturschutz haben wir auch positiv gesehen. Alles in allem Pillepalle im Vergleich zu dem, was uns heute vorliegt. (D)

Experten halten es für eines der invasivsten Überwachungsgesetze der vergangenen Jahre. Heute soll hier in diesem Haus dieses Gesetz mit nachträglichen Änderungen verabschiedet werden, Änderungen, welche den Ermittlungsbehörden den Zugriff auf private Geräte, Handys, Laptops und Tablets ermöglichen sollen – heimlich, zur Strafverfolgung, ohne dass sich die Verdächtigen wehren können. Die geplanten Maßnahmen sind noch weitgehender als der große Lauschangriff aus den 90ern.

(Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]: So ist es!)

– Genauso ist es. – Aber wieso findet sich dazu kaum Resonanz in der Bevölkerung? Hier wird wieder einmal mit einem Verfahrenstrick gearbeitet. Diese massiven Grundrechtseingriffe wurden im Wege eines Änderungsantrages bezogen auf ein Gesetz mit ganz anderen Maßnahmen kurzfristig durchgebracht. Die einzige Schnittmenge ist das Wörtchen „StPO“. Das Thema soll eben kleingehalten werden.

Was will die Bundesregierung erreichen? Bei der Quellen-TKÜ wird eine Schadsoftware auf das Gerät eines Verdächtigen aufgespielt, ein sogenannter Staatstrojaner, der die laufende Kommunikation mitliest. Wesentlich eingriffsstärker ist die Onlinedurchsuchung. Aber auch hier muss eine Software auf dem Gerät des Verdächtigen installiert werden, allerdings kann dann auf sämtliche gespeicherte Inhalte zugegriffen werden, also die gesamte Festplatte ausgelesen werden.

Jörn Wunderlich

(A) Wie wird die Software durch Ermittler installiert? In vielen Fällen werden sie bestehende Sicherheitslücken nutzen müssen, um sich von Ferne Zugriff auf das Gerät zu verschaffen. Doch wenn solche Sicherheitslücken notwendig sind, werden staatliche Stellen bestimmt wenig Interesse daran haben, sie den Softwareherstellern zu melden, was wiederum auch Cyberkriminellen die Nutzung dieser Lücken ermöglicht und diesen somit Vorschub leistet. Die Cyberkriminellen können sich vorab schon einmal bei der Bundesregierung bedanken.

Aus einer Ausnahmemaßnahme zur Terrorabwehr soll nun eine Standardmaßnahme der Polizei werden. Wo bislang abgehört wurde, soll nun der Staatstrojaner eingesetzt werden. Das Gesetz sieht nicht nur vor, die laufende Kommunikation mitzulesen, sondern auch, den Zugriff auf gespeicherte Kommunikation zu erlauben. Experten befürchten daher, dass die Quellen-TKÜ so quasi zu einer Onlinedurchsuchung unter viel geringeren Voraussetzungen wird.

Beide Instrumente gibt es im Übrigen schon, sie werden aber kaum angewandt: Die Onlinedurchsuchung darf etwa nur zur Prävention von äußerst schweren Verbrechen, also beispielsweise zur Terrorabwehr, genutzt werden. Auch die Quellen-TKÜ wurde bislang nur vereinzelt zum Einsatz gebracht. Doch nun sollen diese Maßnahmen nicht nur präventiv, sondern auch zur Strafverfolgung genutzt werden, in einem Anwendungsfeld, das seinesgleichen sucht. Man hätte die Anwendung zumindest auf schwerste Straftaten beschränken müssen.

(Beifall bei der LINKEN und dem BÜND-
(B) NIS 90/DIE GRÜNEN)

Schon im Jahr 2008 hat der Erste Senat des Bundesverfassungsgerichts geurteilt, dass Onlinedurchsuchungen nur zur Abwehr von Gefahren – ich zitiere jetzt mal – für „Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt“, dienen dürfe.

(Beifall des Abg. Harald Petzold [Havelland]
[DIE LINKE])

Dass Drogenhandel und Verstöße im Asylverfahrensrecht den Bestand des Staates oder die Grundlagen der Existenz der Menschen bedrohen, das kann mir hier in diesem Hause keiner erklären.

(Beifall bei der LINKEN und dem BÜND-
NIS 90/DIE GRÜNEN)

Schon heute gibt es bei den Strafverfolgungsbehörden Begehrlichkeiten – das wissen wir aus der Stellungnahme des Oberstaatsanwalts beim BGH –, die Eingriffsschwelle zu senken. Er sagte: Die Schwere des Eingriffes kann man eigentlich erst feststellen, wenn man die Beweismittel gesichert hat. – Deswegen: Wenn ich es beantrage, kann ich noch gar nicht die Schwere bejahen. Daher müsste die Regelung zur Schwere des Eingriffes eigentlich aus dem Gesetz heraus.

Ich bin gespannt, was das Verfassungsgericht zu diesem Gesetz sagen wird. Es wird mit Sicherheit vor dem Verfassungsgericht landen; denn es entspricht nicht den Vorgaben der Entscheidung von 2008. Diese Regierung (C) wird aus den Watschen, die sie sich permanent vom Verfassungsgericht holt, nicht klüger;

(Dr. Johannes Fechner [SPD]: Das waren die
Grünen – die letzte Klatsche!)

aber das wundert mich nicht.

Bei der ersten Lesung des Ursprungsgesetzes, Herr Fechner, hatte ich noch die Hoffnung, in den Beratungen etwas retten zu können. Was heute hier von der Koalition im Omnibusverfahren, im Übrigen am Bundesrat vorbei, ohne Beteiligung der Bundesdatenschutzbeauftragten, ohne Beteiligung der Verbände, ohne Diskussion in der Öffentlichkeit, verabschiedet werden soll, ist mit Worten jenseits der Fäkalsprache nicht mehr zu beschreiben.

(Beifall bei der LINKEN und dem BÜND-
NIS 90/DIE GRÜNEN – Zuruf von der CDU/
CSU: Dann lassen Sie es auch sein!)

Vizepräsidentin Ulla Schmidt:

Vielen Dank. – Für die CDU/CSU-Fraktion spricht jetzt Elisabeth Winkelmeier-Becker.

(Beifall bei der CDU/CSU)

Elisabeth Winkelmeier-Becker (CDU/CSU):

Frau Präsidentin! Liebe Kolleginnen und Kollegen! Strafverfolgung ist ein wesentlicher Teil des rechtsstaatlichen Handelns. Wenn Straftaten begangen werden, dann ist der Staat den Opfern schuldig, dafür zu sorgen, (D) dass die Täter ermittelt werden und dass spürbare Sanktionen verhängt werden. Das ergibt sich aus seinen Schutzpflichten, und dafür hat er auch das Gewaltmonopol. Dafür sorgen eine unabhängige Justiz und handlungsfähige Strafverfolgungsbehörden. Aber in der Praxis ist das nicht so einfach, sondern es gibt da offenbar auch Defizite.

Die Praxis zeigt, dass wir da teilweise an den Belastungsgrenzen angekommen sind. Taten werden nicht aufgeklärt. Gestern haben wir in der Anhörung zum Wohnungseinbruchsdiebstahl gehört, dass die Aufklärungsquote bei diesem Delikt unter 20 Prozent liegt. Gerichtsverfahren dauern lange. Es kommt vor, dass Beschuldigte aus der Untersuchungshaft entlassen werden müssen, weil die sechsmonatige Frist nicht eingehalten werden kann. Es werden viel zu viele Verfahren eingestellt, bei denen es eigentlich gut gewesen wäre, eine Gerichtsverhandlung durchzuführen – damit sie einen bleibenden Eindruck bei dem Täter hinterlässt, damit das Opfer ihm in die Augen blicken kann, damit es einen Ausgleich geben kann. Auch unter Gesichtspunkten der Transparenz gegenüber der Öffentlichkeit wäre es besser, wenn nicht so viele Verfahren eingestellt würden.

Es wird kritisiert, dass Deals gemacht werden. Oft ist der Hintergrund, dass die Arbeitsbelastung zu hoch ist, dass sich abzeichnet, dass ein Verfahren rechtlich und auch tatsächlich sehr kompliziert wird. All das trägt natürlich nicht dazu bei, dass sich die Akzeptanz gerichtlicher Entscheidungen in der Bevölkerung erhöht. Es trägt auch nicht zu mehr Gerechtigkeit bei.

Elisabeth Winkelmeier-Becker

(A) Das Problem liegt in einer sehr hohen Arbeitsbelastung der Gerichte, der Ermittler, der Staatsanwälte und der Justizangestellten. Deshalb haben wir uns in Nordrhein-Westfalen für die neue Koalition vorgenommen, hier à la longue ganz deutlich aufzurüsten, sowohl, was die personelle Ausstattung angeht, als auch, was die technische Ausstattung angeht.

(Beifall bei der CDU/CSU)

– Das ist schon mal einen Applaus wert; das finde ich auch.

Dabei zeigt der Vergleich, dass wir mit der Anzahl von 24 Richtern pro 100 000 Einwohner gar nicht so schlecht dastehen. Wir wissen auch, dass sich diese Zahlen nicht beliebig steigern lassen. Deshalb müssen wir auf der einen Seite die Ressourcen verbessern; auf der anderen Seite wird es darauf ankommen, mit den knappen Ressourcen sorgsam umzugehen, diese Ressourcen sinnvoll und vor allem effizient einzusetzen. Das ist ein Beitrag zu mehr Rechtsstaatlichkeit, zu mehr Vertrauen in den Rechtsstaat und auch zu mehr Gerechtigkeit.

(Beifall bei der CDU/CSU)

Es ist durchaus erkennbar, dass bei uns noch Potenzial vorhanden ist. Ein Vergleich: Das Landgericht Hamburg hatte einen Fall abzuurteilen, in dem es um Piraten ging, die am Horn von Afrika ein deutsches Schiff angegriffen hatten. Für das Verfahren waren 106 Hauptverhandlungstage angesetzt, die Kosten: 4,5 Millionen Euro. Bei einem vergleichbaren Fall in Frankreich dauerte die (B) Hauptverhandlung drei Wochen.

(Hans-Christian Ströbele [BÜNDNIS 90/DIE GRÜNEN]: Kommt doch sehr auf die Beweislage an, Frau Kollegin! Man kann doch nicht Äpfel mit Birnen vergleichen!)

Da zeigt sich eine gewissen Unwucht und dass wir in diesem Bereich auf jeden Fall noch Potenzial haben; denn Frankreich wird man sicherlich nicht nachsagen können, dass dort der Rechtsstaat nichts gilt; ganz im Gegenteil. Wir haben deshalb schon im Koalitionsvertrag vereinbart, dass wir in den Strafverfahren, in den Jugendstrafverfahren, unter Wahrung rechtsstaatlicher Grundsätze selbstverständlich, die Verfahren praxistauglicher ausgestalten wollen. Das ist der rote Faden, der sich durch die Regelungen zieht, die wir Ihnen heute zur Abstimmung vorlegen.

Es beginnt beim Ermittlungsverfahren. Wir schaffen – die Kollegin Bähr-Losse hat es schon dargestellt – damit eine sichere Rechtsgrundlage für Quellen-TKÜ und Onlinedurchsuchungen. Es ist einfach Unsinn, wenn die Ermittlungsbehörden bei ihrer Arbeit nicht die Möglichkeit haben, sich daran zu orientieren, wie Täter und Banden heutzutage agieren. Derzeit heißt es zu oft, dass wir dem Täter nicht auf die Spur kommen können. Mit Telekommunikation herkömmlicher Art bekommen wir eigentlich nur noch mit, wer gerade welche Pizza bestellt, wir erfahren aber nicht mehr, was die Bandenmitglieder verabreden, um ein Verbrechen oder einen Angriff zu begehen, möglicherweise sogar einen terroristischen Anschlag zu planen.

Es ist aus den genannten Gründen notwendig, dass wir (C) für die Maßnahmen eine klare Rechtsgrundlage schaffen. Sie beinhalten zugegebenermaßen schon auch Eingriffe in die Grundrechte, aber sie sind an klare Voraussetzungen gebunden, nämlich dass Tatsachen den Verdacht begründen, dass jemand Täter oder Teilnehmer einer schweren Straftat ist. Ein paar Beispiele dafür, um welche Taten es gehen kann: Terrorismus, Geldwäsche, Abgeordnetenbestechung, Kinderpornografie, Mord, Bandendiebstahl. In solchen Fällen können die Maßnahmen wichtige und unverzichtbare Anhaltspunkte liefern, und dann sind sie auch verhältnismäßig, und dann sind sie auch gerechtfertigt. Es sind die hohen rechtlichen Hürden und auch die hohen technischen Hürden, die dafür sorgen, dass eine Maßnahme nie und nimmer zu einer Standardmaßnahme werden kann. Vielmehr handelt es sich um sehr gezielte Maßnahmen, die allenfalls in wenigen Einzelfällen zum Einsatz kommen.

Ich weiß nicht, woher Sie nehmen, dass eine Maßnahme zu einer Standardmaßnahme werden könnte. Weder die rechtlichen Voraussetzungen lassen diesen Schluss zu, noch die Erfahrungen mit diesem Instrument im präventiven Bereich. Mit den Maßnahmen wird sehr restriktiv umgegangen, und genauso wird das – das ist meine feste Überzeugung – hier im Bereich der Ermittlungen, im Bereich der Strafverfolgung geschehen.

(Jörn Wunderlich [DIE LINKE]: Das ist eine falsche Überzeugung!)

Es wird außerdem Vereinfachungen im Ermittlungsverfahren geben. Auf den Richtervorbehalt bei der Blutentnahme im Zusammenhang mit Verkehrsstraftaten (D) kann guten Gewissens verzichtet werden, weil der telefonisch erreichte Richter im Zweifel ohnehin nur das bestätigen kann, was ihm der Polizeibeamte vor Ort schildert.

Wir schaffen die Pflicht von Zeugen, bei der Polizei zu erscheinen. Wir regeln die Erfassung von sogenannten DNA-Beinahetreffern, wo es Sinn macht. Wir hätten gerne auch noch die DNA-Analyse in Bezug auf Merkmale wie Augenfarbe oder Haarfarbe aufgenommen, aber dazu sah sich das Justizministerium leider nicht in der Lage.

In einem nächsten Schritt haben wir Beschleunigungen für den Gang des Verfahrens vorgesehen. Es gibt häufig den Fall, dass Befangenheitsanträge und Beweisanträge eher taktisch gestellt werden. Das Gericht soll blamiert werden, als hilflos vorgeführt werden, indem man mal zuerst mit einem Befangenheitsantrag beginnt und den ganzen Zeitplan durcheinanderbringt.

(Hans-Christian Ströbele [BÜNDNIS 90/DIE GRÜNEN]: Wenn die doch befangen sind, die Richter?)

Wir haben jetzt geregelt, dass wenigstens bis zur Verlesung der Anklageschrift erst einmal weitergemacht werden kann. Danach wird sich alles Weitere finden. Beides führt zu mehr Effizienz ohne substanzielle Eingriffe in die Rechte des Angeklagten oder Nachteile für die Wahrheitsfindung.

Der letzte Schritt. Bei den Sanktionen haben wir in Zukunft die Möglichkeit, ein Fahrverbot als Nebenstrafe festzusetzen; denn häufig ist es so, dass zum Beispiel

(A) eine Bewährungsstrafe doch nur als Freispruch zweiter Klasse empfunden wird. Hier brauchen wir eine zusätzliche Sanktion, die auch für den Täter spürbar ist – ohne die Nachteile einer Haftstrafe.

Vizepräsidentin Ulla Schmidt:

Jetzt müssen Sie zum Schluss kommen.

Elisabeth Winkelmeier-Becker (CDU/CSU):

So bin ich optimistisch, dass wir mit diesem Paket schon einiges erreichen, liebe Frau Präsidentin.

(Beifall bei der CDU/CSU sowie der Abg. Bettina Bähr-Losse [SPD])

Vizepräsidentin Ulla Schmidt:

Vielen Dank. – Jetzt hat der Kollege Hans-Christian Ströbele, Bündnis 90/Die Grünen, das Wort.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN):

Frau Präsidentin! Liebe Kolleginnen und Kollegen! Eigentlich wollten wir hier über die große Strafprozessreform reden, die der Bundesjustizminister schon vor Jahren angekündigt hat. Dabei ist aber nichts rausgekommen, außer ein paar kleinen Mäuschen, die hier schon erwähnt worden sind, wie zum Beispiel, dass der Richtervorbehalt bei der Blutentnahme wegfällt.

(Dr. Johannes Fechner [SPD]: Das ist ein
(B) großer Vorteil für die Praxis!)

– Ja, sensationell; eine wirklich große Leistung. – Oder dass jetzt bei bestimmten – das gilt nur bei Tötungsdelikten – Vernehmungen von Beschuldigten ein Band mitläuft oder eine Tonaufnahme gemacht wird, das ist auch nicht revolutionär, das ist auch keine große Veränderung.

Aber ich will mich an diesen einzelnen Punkten gar nicht mehr aufhalten, weil wir das bereits in der ersten Lesung getan haben. Übrigens haben wir auch den Aspekt behandelt, der weniger die Strafprozessordnung, sondern eher das Strafrecht betrifft, dass man Führerscheinentzug oder Fahrverbot jetzt auch für Nichtverkehrsstraftaten anwenden will.

Das alles wäre hier heute fast nichts gewesen. Deshalb haben Sie noch rechtzeitig – oder vielmehr: nicht mehr rechtzeitig, nämlich nach Dienstschluss am letzten Freitag – einen Änderungsantrag eingebracht und wollten am Montag eine Sondersitzung für die Telekommunikationsüberwachung, also für Onlinedurchsuchungen und Quellen-TKÜ, haben, damit das im Rechtsausschuss noch schnell beschlossen werden kann – das ist nicht gemacht worden. Dann hat man es Dienstag gemacht, wo es schnell durchgepeitscht wurde.

Ich sage Ihnen: Das ist ein Hauruckverfahren,

(Dr. Patrick Sensburg [CDU/CSU]: Das ist
doch wie ein Sondervotum!)

das unzulässig ist, zumindest wenn es darum geht, ein Gesetz zu machen, das mehr in die Grundrechte der Bürgerinnen und Bürger eingreift als damals der große (C) Lauschangriff,

(Beifall beim BÜNDNIS 90/DIE GRÜNEN
und bei der LINKEN)

und zwar nicht nur in die von Verdächtigten und Beschuldigten, sondern möglicherweise auch in die Grundrechte von anderen Personen. Es könnte nämlich sein, dass, wenn es Anhaltspunkte dafür gibt, dass ein Verdächtiger einen PC oder ein Handy von jemand anderem benutzt hat, dann auch der fällig ist, dann auch der in der Überwachung ist.

Es geht hier um einen operativen Eingriff in Grundrechte. Das muss ausführlich beraten werden. Deshalb haben wir gesagt: So kann man das nicht machen.

(Beifall beim BÜNDNIS 90/DIE GRÜNEN
und bei der LINKEN)

Was haben Sie unter der Überschrift „Wir müssen etwas gegen Terrorismus tun“ jetzt gemacht? Da geben wir Ihnen ja recht – auch mit Blick auf die Strafverfolgung; denn hier geht es ja nur um die Strafverfolgung –: Wir müssen etwas gegen Terrorismus tun; das stimmt. Aber wenn man den Gesetzentwurf nun betrachtet, sieht man: Es hat Auswirkungen quer durch das Strafgesetzbuch. Sie wollen es auf insgesamt 70 Paragrafen, glaube ich, anwenden. Erklären Sie mir, wo die schwere Straftat ist,

(Dr. Patrick Sensburg [CDU/CSU]: Kin-
derpornografie zum Beispiel!)

wenn es beispielsweise auf gewerbsmäßige Hehlerei angewendet werden soll. Wird da der Staat aus den Angeln (D) gehoben, oder warum?

(Dr. Patrick Sensburg [CDU/CSU]: Hehlerei
ist nicht okay!)

Daran zeigt sich, dass Sie etwas ganz anderes vorhaben: Sie wollten das Strafgesetzbuch ganz breit erfassen, nahezu alle Delikte. – Hehlerei ist übrigens nicht einmal ein Verbrechenstatbestand, sondern ein Vergehenstatbestand.

(Beifall beim BÜNDNIS 90/DIE GRÜNEN
und bei der LINKEN)

So kann man das nicht machen, und so ist das auch mit der Rechtsprechung des Bundesverfassungsgerichts nicht in Einklang zu bringen.

Das Bundesverfassungsgericht hat insbesondere verlangt: Wenn man solche Onlinedurchsuchungen machen will, dann muss man garantieren, dass dies technisch und rechtlich vorher so geprüft wird und überprüfbar bleibt, dass man feststellen kann, was mit dieser TKÜ wirklich gemacht wird. Wenn es heißt, sie laufe nach drei Monaten aus, muss überprüfbar sein, ob sie tatsächlich ausläuft. Kann das der Richter feststellen? Da reicht der Richtervorbehalt nicht, sondern da braucht man einen Vorbehalt von Datenschutzbeauftragten oder meinetwegen auch von Spezialisten vom Chaos Computer Club, die man da hinzuziehen muss.

(Beifall beim BÜNDNIS 90/DIE GRÜNEN
und bei der LINKEN)

Hans-Christian Ströbele

(A) Mit diesem Gesetz greifen Sie substanziell in das Recht auf informationelle Selbstbestimmung ein, und dies gerade in dem Kernbereich privater Lebensführung. Dazu haben Sie in das Gesetz hineingeschrieben: Wenn allein dieser Kernbereich betroffen ist, dann ist das unzulässig. – Das wird ja fast nie der Fall sein. Selbst bei einem Liebesgeflüster oder selbst beim Gespräch mit einem Psychologen oder Psychiater wird natürlich auch einmal über etwas anderes gesprochen. Das heißt, Sie öffnen selbst diesen Kernbereich der privaten Lebensführung für derartige Onlinedurchsuchungen. Das ist grundgesetzwidrig, das ist mit der Rechtsprechung des Bundesverfassungsgerichts in keiner Weise zu vereinbaren.

(Beifall beim BÜNDNIS 90/DIE GRÜNEN und bei der LINKEN)

Lassen Sie mich einen letzten Punkt ansprechen. Sie sagen zwar: Rechtsanwälte, Ärzte, Pfarrer sollen davon ausgenommen sein. – Aber Sie nehmen die Helfer der Rechtsanwälte nicht aus. Wie stellen Sie sich denn das in meinem Büro als Rechtsanwalt vor? Bei mir dürfen Sie es nicht einsetzen, aber bei einem Mitarbeiter, der da bei mir im Büro sitzt, dürfen Sie es einsetzen. Wie wollen Sie da noch das Anwaltsgeheimnis wahren,

(Beifall beim BÜNDNIS 90/DIE GRÜNEN und bei der LINKEN – Jörn Wunderlich [DIE LINKE]: Das wollen sie ja nicht!)

wie wollen Sie da noch das Arztgeheimnis wahren, wie wollen Sie die Vertraulichkeit des Gesprächs mit Geistlichen, mit Pfarrern oder anderen wahren?

(B) Nein, dieses Gesetz darf so nicht durchkommen. Dieses Gesetz muss spätestens in Karlsruhe fallen.

(Beifall beim BÜNDNIS 90/DIE GRÜNEN und bei der LINKEN)

Vizepräsidentin Ulla Schmidt:

Vielen Dank. – Für die SPD-Fraktion hat jetzt Dr. Johannes Fechner das Wort.

(Beifall bei der SPD)

Dr. Johannes Fechner (SPD):

Frau Präsidentin! Liebe Kolleginnen und Kollegen! Liebe Zuhörerinnen und Zuhörer! Ich möchte gleich vorab sagen: Das Allerwichtigste – bei Strafgesetzen oder der Reform der Strafprozessordnung – ist es, wenn wir die Strafjustiz entlasten wollen, für mehr Personal zu sorgen. Wir brauchen mehr Richterinnen und Richter, wir brauchen mehr Staatsanwälte. Damit können wir der Justiz den größten Dienst erweisen, liebe Kolleginnen und Kollegen.

(Beifall bei der SPD sowie bei Abgeordneten der CDU/CSU)

Wir können die hohe Arbeitsbelastung gerade in der Strafrechtspflege aber auch durch eine effektivere Ausgestaltung des Strafverfahrens erreichen, und genau dem dient dieses Gesetz. So ist es in der Tat – Kollege Wunderlich hat es angesprochen – zukünftig nicht mehr erforderlich, dass für eine Blutalkoholprüfung extra ein Richter seine Anordnung geben muss. Das hat viele (C) Kräfte gebunden, und es wird von allen Berufsverbänden begrüßt, dass wir die Richter hiervon entlasten. Mit dieser Maßnahme erreichen wir beispielhaft das Ziel, die hohe Belastung in der Justiz zu reduzieren.

Wenn sich die biotechnischen Möglichkeiten der DNA-Analyse weiterentwickelt haben, dann sollten wir diese Möglichkeiten auch nicht ungenutzt lassen. Wir wollen deshalb, dass der sogenannte Beinahetreffer auch von der Strafprozessordnung erfasst wird und dort geregelt ist. Das sind Fälle, in denen der Abgleich von Spuren und DNA-Material ergibt, dass die Spuren zwar nicht vom Täter, aber von einem nahen Verwandten stammen. Zukünftig kann also nicht nur auf die völlige Übereinstimmung von Spur und Täter hin untersucht werden, sondern auch, ob es eine Ähnlichkeit gibt, die auf ein Verwandtschaftsverhältnis schließen lässt. Auch das ist ein ganz wesentlicher Vorteil.

Ich persönlich wünsche mir auch, dass wir rasch in der nächsten Legislaturperiode die Frage der Weitergabe von Ergebnissen aus DNA-Analysen an die Polizei regeln, was die persönlichen Merkmale angeht, also etwa Augenfarbe oder Haarfarbe. Dazu hatten wir ein umfangreiches Symposium beim BMJ; herzlichen Dank für diese gelungene Veranstaltung, die den Handlungsbedarf gezeigt hat. Um dies einzuarbeiten, hat jetzt zum Ende der Legislaturperiode die Zeit nicht mehr gereicht. Aber ich finde: Wenn mit Sicherheit gesagt werden kann, wie die Haarfarbe oder die Augenfarbe eines Täters ist, dann sollte die Polizei diese Informationen bekommen, um die Ermittlungskräfte gezielt einsetzen zu können, liebe Kol- (D) leginnen und Kollegen.

(Beifall bei der SPD sowie bei Abgeordneten der CDU/CSU)

Wir gestalten den Strafprozess an vielen Stellen effektiver. Der Verteidiger erhält bei umfangreichen Verfahren die Möglichkeit zu einer sogenannten Opening Speech, und bei Tötungsvorwürfen muss die Beschuldigtenvernehmung zukünftig auf Video aufgenommen werden. Herr Ströbele, Sie haben recht:

(Hans-Christian Ströbele [BÜNDNIS 90/DIE GRÜNEN]: Ich habe immer recht!)

Wir wären hier viel weiter gegangen. Wir hätten die im sehr guten Referentenentwurf vorgesehene Formulierung des § 58a StPO gerne bei allen Straftaten angewandt; denn wir erhalten aus der Praxis immer wieder Hinweise, dass gerade die Opfer von Sexualstraftaten ihre Aussagen leider zurückziehen. Mit der Videoaufzeichnung hätten wir die Möglichkeit, im Prozess auf diese Aussagen zurückzukommen.

(Hans-Christian Ströbele [BÜNDNIS 90/DIE GRÜNEN]: Genau! Das wäre ein Schritt!)

Deswegen geht der Vorwurf an den Koalitionspartner: Wir könnten mehr Vergewaltiger und mehr Menschenhändler verurteilen, wenn Sie diese Regelung nicht blockiert hätten, liebe Kolleginnen und Kollegen.

(Beifall bei der SPD)

(A) Zu der Frage der Verwertung der Ergebnisse von DNA-Analysen. Wir müssen – das habe ich schon ausgeführt – mit dem technischen Fortschritt gehen. Es kann nicht sein, dass nur die eine Seite, dass nur Terroristen und Kriminelle vom technischen Fortschritt profitieren. Nein, auch die Polizei muss hier Schritt halten und auf Augenhöhe mit den Terroristen und Kriminellen agieren können.

Deswegen ist es richtig, dass wir eine klare rechtsstaatliche Grundlage für die TKÜ und die Onlinedurchsuchungen schaffen. Wir orientieren uns dabei an der Wohnungsüberwachung – mit ganz klaren rechtsstaatlichen Grundsätzen. Es kann nicht einfach ins Blaue hinein angeordnet werden, dass ein Handy von der Polizei gehackt wird. Nein, ein Richter muss feststellen, dass Tatsachen vorliegen, die einen Verdacht auf eine ganz bestimmte Straftat, und zwar eine schwere Straftat, die im Gesetz abschließend geregelt ist, begründen.

(Zuruf des Abg. Hans-Christian Ströbele [BÜNDNIS 90/DIE GRÜNEN])

Man kann darüber diskutieren, ob es auch weniger getan hätte; keine Frage. Aber wir haben eine klare Regelung: Nur bei einer schweren Straftat darf dieses Instrument angeordnet werden. Ich finde, das ist eine rechtsstaatliche Lösung. Die Polizei muss auf dem neuesten technischen Stand sein, um mit Terroristen und Kriminellen mithalten zu können.

(B) Weil Frau Künast direkt danach gefragt hat, will ich Folgendes nicht unerwähnt lassen: Ja, wir tun mit diesem Gesetz auch etwas für den Naturschutz. Wir verschärfen das Bundesnaturschutzgesetz, um den illegalen Wildtierhandel zu bekämpfen. Nach dieser Neuregelung macht sich strafbar, wer leichtfertig ein geschütztes Tier tötet oder geschützte Pflanzenarten zerstört. Hierfür erhöhen wir die Höchststrafe von einem auf drei Jahre. Das ist nicht ganz unwichtig, wie ich finde. Deswegen will ich es in dieser Rede zumindest kurz erwähnen. Abschließend sage ich: Ein gutes Gesetz – –

Vizepräsidentin Ulla Schmidt:

Aber jetzt kommen Sie zum Schluss, ja?

Dr. Johannes Fechner (SPD):

Jetzt haben Sie mich im Schlusssatz unterbrochen, Frau Präsidentin. Ich muss noch einmal anfangen.

Vizepräsidentin Ulla Schmidt:

Dann muss man damit früher anfangen.

Dr. Johannes Fechner (SPD):

Abschließend: Das ist ein gutes Gesetz. Stimmen wir also zu!

Herzlichen Dank.

(Beifall bei der SPD sowie bei Abgeordneten der CDU/CSU)

Vizepräsidentin Ulla Schmidt: (C)

Vielen Dank. – Als Nächster hat jetzt Professor Dr. Patrick Sensburg für die CDU/CSU-Fraktion das Wort.

(Beifall bei der CDU/CSU)

Dr. Patrick Sensburg (CDU/CSU):

Sehr geehrte Frau Präsidentin! Liebe Kolleginnen und Kollegen! Ich kann an die Rede meines Vorredners anknüpfen: Das ist ein gutes Gesetz. Wir haben im Koalitionsvertrag vereinbart, das Strafprozessrecht effektiver und praxistauglicher zu gestalten. Das ist ein guter Ansatz gewesen; denn über die Jahre hat sich das Strafprozessrecht aufgrund vieler Gesetzesänderungen auseinanderentwickelt. Das wieder zusammenzuführen, war der Ansatz.

Das ist uns nur in Teilen gelungen; da stimme ich dem Kollegen Ströbele zu. Es wäre mehr möglich gewesen. Der erste Vorschlag der Kommission beim Justizministerium zeigt: Es war größer geplant. Aber wir haben viele Hürden nehmen müssen. Wir haben über einzelne Regelungen gestritten. An dieser Stelle gilt mein Dank dem Justizministerium, dem Justizminister Maas und insbesondere Staatssekretär Lange. Wir haben oft zusammengesessen und über viele Formulierungen und einzelne Wörter diskutiert, debattiert und gestritten. Im Ergebnis haben wir nach meiner Meinung eine wirklich tragbare und gute Lösung für die Reform des Strafprozessrechts gefunden. Dafür ein Dankeschön! (D)

(Beifall des Abg. Dr. Johannes Fechner [SPD])

Die einzelnen Punkte sind erwähnt worden: Mit Befangenheitsanträgen soll nicht mehr erreicht werden können, dass ein Verfahren endlos in die Länge gezogen wird; Beweisanträge müssen bis zum Ende einer Frist gestellt werden; die Erscheinungspflicht des Zeugen wird geregelt – er kann nicht einfach sagen: ach, was interessiert es mich, wenn die Polizei mich zur Befragung lädt –; und die audiovisuelle Vernehmung ermöglicht es, später noch einmal zu schauen, was der Zeuge bei seiner Vernehmung wirklich gesagt hat.

Ob es, wenn das weiter ausgedehnt worden wäre, uns mehr Klarheit und Transparenz gebracht hätte oder mehr Revisionsgründe, das kann man unterschiedlich beleuchten. Wir haben ja Expertenanhörungen zu diesen Themen durchgeführt. Wir haben dreieinhalb Jahre über diese einzelnen Punkte diskutiert. Von daher freue ich mich, dass Frau Kollegin Bähr-Losse die Genese, die Entwicklung dieses Gesetzentwurfs dargestellt hat. Ich verstehe nicht, wie man angesichts dessen als Oppositionspolitiker sagen kann: Dieser Gesetzentwurf ist in wenigen Tagen entstanden.

Herr Kollege Ströbele, Sie waren doch bei der Expertenanhörung, in der auch über die Quellen-TKÜ diskutiert worden ist, dabei. Ich habe in dieser Anhörung selbst die Frage nach der Notwendigkeit der Quellen-TKÜ gestellt. Vielleicht haben Sie das nicht mitbekommen; dann ver-

Dr. Patrick Sensburg

(A) stehe ich, dass Sie sagen: Das kommt jetzt spontan. – Aber das ist doch nicht spontan.

(Hans-Christian Ströbele [BÜNDNIS 90/DIE GRÜNEN]: Das stand im Gesetz überhaupt nicht drin!)

Das war im Gesamtpaket der Strafprozessordnungsreform drin.

(Irene Mihalic [BÜNDNIS 90/DIE GRÜNEN]: Das war im Gesetzentwurf nicht drin!)

Dann ist es herausgenommen und in zwei Teile getrennt worden, weil wir aus der letzten Legislaturperiode den § 81a StPO noch als sogenanntes Leftover, als Überbleibsel, hatten.

(Hans-Christian Ströbele [BÜNDNIS 90/DIE GRÜNEN]: Das war bis Freitag in dem Gesetz überhaupt nicht drin!)

Wir sind froh, dass wir den § 81a StPO in dieser Legislaturperiode durchbekommen haben. Wir beide waren doch gemeinsam mit dem Kollegen van Essen damals Berichterstatter. Wir wären doch beide froh gewesen, hätten wir den § 81a StPO schon damals durchbekommen.

(Elisabeth Winkelmeier-Becker [CDU/CSU]: So, so! – Alexander Hoffmann [CDU/CSU]: Hört! Hört!)

Jetzt ist uns das endlich gelungen, und nun hängen Sie sich an zwei Punkten auf und blockieren dieses gute Gesetz, nämlich an der Quellen-TKÜ und an der Onlinedurchsuchung. Beides sind Bereiche, die wir ohnehin (B) schon haben. Es ist derzeit ohne Weiteres möglich, den Telefonverkehr von Verbrechern und Menschen, die im Verdacht stehen, schwere und schwerste Straftaten begangen zu haben, abzuhören. Das kennt jeder, der schon einmal den *Tatort* gesehen hat.

Nun ist es so, dass im *Tatort* nicht alle Leute per Messenger telefonieren. Aber in der Realität machen das die Menschen inzwischen. Nur noch 15 Prozent der Kommunikation erfolgen unverschlüsselt. Sehen Sie sich einmal an, was die Kids machen; die drücken auf den Hörer bei WhatsApp.

(Hans-Christian Ströbele [BÜNDNIS 90/DIE GRÜNEN]: Dann führen Sie es doch für Terrorismus ein!)

Diese Kommunikation von Verbrechern bzw. Menschen, die im Verdacht stehen, schwere und schwerste Straftaten begangen zu haben, wollen wir genauso erfassen wie die Kommunikation in normalen Telefonaten. Das ist berechtigt. Diese Möglichkeit eröffnen wir jetzt durch die Quellen-TKÜ.

(Beifall bei der CDU/CSU)

Der zweite Bereich ist die Onlinedurchsuchung. Es ist heutzutage Alltag, dass ein Handy, das an einem Tatort gefunden wird, ausgelesen wird; das ergibt sich aus § 110 der StPO. Wenn man kein Handy findet, aber weiß, dass schwerste Straftaten im Raum stehen, deren besondere Schwere sogar festgestellt worden ist und werden muss – das haben Sie eben unterschlagen, Herr Kollege Ströbele; in § 100b des Gesetzes steht nämlich auch drin, (C) dass die besondere Schwere der einzelnen Tat festgestellt werden muss –,

(Hans-Christian Ströbele [BÜNDNIS 90/DIE GRÜNEN]: Die können Sie vorher doch gar nicht feststellen!)

dann muss es auch möglich sein, ein Handy online zu durchsuchen, genauso wie es durchsucht werden kann, wenn es an einem Tatort beschlagnahmt wird. Wir eröffnen damit die Möglichkeit, Straftaten zu verhindern, sie zu verfolgen und die Täter dingfest zu machen. Das ist nichts Aufregendes, und das ist nichts, was man skandalisieren muss. Das sind die Dinge, die in der normalen – nicht der digitalen – Welt schon bisher möglich waren. Diese Möglichkeit eröffnen wir jetzt auch im Hinblick auf die digitale Kommunikation.

(Britta Haßelmann [BÜNDNIS 90/DIE GRÜNEN]: Herr Sensburg, Sie wissen doch, dass das nicht stimmt!)

Herr Kollege Wunderlich, wenn Sie im Jahre 1990 stehen bleiben, dann werden Sie halt Straftaten nicht mehr ermitteln. Täter kommunizieren heute digital. Daher geben wir unserer Polizei und den Strafverfolgungsbehörden die Möglichkeit, auch diese Kommunikation in ganz besonders schweren Fällen abzurufen.

(Jörn Wunderlich [DIE LINKE]: Insbesondere bei Kids, wie Sie gerade gesagt haben!)

Das ist auch richtig so. Deswegen: Unterstützen Sie un- (D) seren Gesetzentwurf!

Danke schön.

(Beifall bei der CDU/CSU)

Vizepräsidentin Ulla Schmidt:

Vielen Dank, vor allen Dingen für die perfekte Einhaltung der Zeit. – Als letzter Redner zu diesem Tagesordnungspunkt hat jetzt der Kollege Alexander Hoffmann für die CDU/CSU-Fraktion das Wort. Er hat den Ehrgeiz, das genauso zu machen wie der Kollege Sensburg.

Alexander Hoffmann (CDU/CSU):

Ich tue, was ich kann. – Sehr geehrte Frau Präsidentin! Geschätzte Kolleginnen und Kollegen! Meine sehr verehrten Damen und Herren! Kollege Fechner, Ihre Aussage, dass wir mit diesem Gesetz mehr Vergewaltiger verurteilen könnten, wenn die Union nicht wäre,

(Dr. Johannes Fechner [SPD]: Ja!)

bedarf natürlich der Kommentierung durch mich;

(Dr. Johannes Fechner [SPD]: Das überrascht mich nicht!)

das wird Sie nicht überraschen. Ich möchte an dieser Stelle schon darauf hinweisen, dass wir heute vor allem deswegen mehr Vergewaltiger verurteilen können, weil

Alexander Hoffmann

(A) wir einen neuen Straftatbestand haben, nämlich den berühmten Grundsatz „Nein heißt Nein“.

(Marianne Schieder [SPD]: Aber bestimmt nicht wegen der Union!)

Für diesen Straftatbestand hat die Union gekämpft,

(Widerspruch bei der SPD)

dafür haben die Frauen in der Union und glücklicherweise auch die Frauen in der SPD gekämpft, aber leider nicht der SPD-Bundesjustizminister. Diese Bemerkung kann ich mir nicht verkneifen.

(Beifall bei der CDU/CSU – Widerspruch bei der SPD – Renate Künast [BÜNDNIS 90/DIE GRÜNEN]: Herr Maas wollte das auch nicht! Da haben Sie recht!)

Aber ich nehme Sie als geläutert wahr. Sollten wir wieder einmal rechtspolitische Koalitionsverhandlungen führen, können wir gerne über die Versuchsstrafbarkeit beim Cyber Grooming verhandeln. Das ist uns nämlich ein großes Anliegen, das aber die ganze Zeit von der SPD blockiert wird.

Liebe Kolleginnen und Kollegen, gestatten Sie mir, dass ich als letzter Redner zwei Teilaspekte aus dem Gesetzespaket, das uns vorliegt, herausgreife. Zunächst noch ein paar Sätze zur effektiveren und praxistaugliche-

(B) ren Ausgestaltung des Strafverfahrens. Der Titel sagt es schon: Es geht um Verfahrensvereinfachung und Verfahrensbeschleunigung. Wir alle kennen ja aus dem Studium den Satz: Die Strafe soll der Tat auf dem Fuße folgen.

Es geht um bestimmte Komponenten, die – ich will es einmal so sagen – eine Straffung des Befangenheitsrechts darstellen, das – die Praktiker wissen das – in der Vergangenheit immer wieder gezielt zur Verfahrungsverzögerung missbraucht worden ist – so muss man es schon fast nennen –, und zwar, wie die Kollegin Winkelmeier-Becker eben gesagt hat, zum Beispiel durch die Formulierung des Ablehnungsgesuchs kurz vor Beginn der Hauptverhandlung. Dem wollen wir einen Riegel vorschieben. Die Hauptverhandlung kann jetzt beginnen und bis zur Verlesung des Anklagesatzes fortgesetzt werden. Zudem hat der Vorsitzende nun die Möglichkeit, eine Fristsetzung für die schriftliche Begründung des Ablehnungsgesuchs zu formulieren. Auch das führt letztlich dazu, dass Verfahren nicht weiter verschleppt werden.

Ich möchte auch noch einige Sätze zur Änderung des Beweisantragsrechts sagen. Auch das ist mittlerweile leider ein sehr missbrauchsanfälliger Bereich. Hier wird neu eingeführt – ich habe das in der ersten Lesung schon skizziert –, dass der Vorsitzende nach Ende der Beweisaufnahme eine angemessene Frist setzen kann, binnen der weitere Beweisanträge gestellt werden dürfen; danach ist das eben einfach nicht mehr möglich.

Zusammenfassend kann ich sagen, dass wir hier einen praxistauglichen Instrumentenkasten haben, der letztendlich dazu führt, dass wir die Strafverfahren werden straffen können.

Im zweiten Teil meiner Rede möchte ich noch ein paar Sätze zum Fahrverbot als Sanktion sagen; das ist die eigentliche Zielsetzung meiner Berichterstattung. (C) Sie kennen die Rechtslage. Bisher ist es so, dass es das Fahrverbot als Sanktion nur dann gibt, wenn die Straftat im Zusammenhang mit dem Straßenverkehr steht. Diese Verbindung wollen wir aufheben, und das aus guten Gründen.

In einem Rechtsstaat manifestiert sich der staatliche Strafanspruch in der Verurteilung. Strafe und auch Nebenstrafe sollen das Tatunrecht sühnen, Genugtuung für das Opfer sein und auf den Täter einwirken. Diese dritte Komponente, diese Spezialprävention, ist im Jugendstrafrecht noch einmal sehr viel intensiver. Hier steht der Erziehungsgedanke über allem. Man will auf den Täter, der im jugendlichen Alter noch formbar ist, einwirken. Deswegen glaube ich, dass es richtig ist, dass nach dem vorliegenden Entwurf der Instrumentenkasten an Nebenstrafen erweitert wird und auch ein Fahrverbot zulässt, wenn die Straftat nicht im Zusammenhang mit dem Straßenverkehr begangen wird.

Das Fahrverbot bleibt Nebenstrafe. Im Erwachsenenstrafrecht wird die Dauer von maximal drei Monaten auf maximal sechs Monate erhöht; im Jugendstrafrecht bleibt es bei drei Monaten, eben wegen des Erziehungsgedankens. Das Fahrverbot soll in Betracht kommen, wenn es zur Einwirkung auf den Täter erforderlich scheint und – das kommt dem Täter ja zugute – zur Vermeidung einer Freiheitsstrafe zielführend ist. Wir erhoffen uns hiermit ein Instrument, das effektiv einwirken kann, nämlich zielgenau, spürbar und der Schuld angemessen. Ich glaube, wir sind hier auf dem richtigen Weg.

Ich will noch ein Missverständnis aus dem Weg räu- (D) men, weil das immer wieder proklamiert wird: Die Anhörung hat sehr deutlich ergeben, dass sich vor allem die Praxis ein solches Instrument wünscht. Das wollen wir heute beschließen. Deswegen bitte ich um Zustimmung.

Vielen Dank.

(Beifall bei der CDU/CSU sowie bei Abgeordneten der SPD)

Vizepräsidentin Ulla Schmidt:

Vielen Dank. – Der Kollege Christian Ströbele hat um das Wort zu einer Kurzintervention gebeten. Bitte, Herr Ströbele.

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN):

Danke, Frau Präsidentin. – Ich will zu dem, was der Kollege Sensburg gesagt hat, zwei Anmerkungen machen.

Erstens. Wir streiten nicht darüber, dass man bei terroristischen Gefahren für alle Eventualitäten Erkenntnis- und Aufklärungsmöglichkeiten schafft. Das habe ich im Rechtsausschuss auch so gesagt. Das heißt, wir können bei solchen Tatbeständen durchaus darüber reden. Ärgerlich und in gewisser Weise auch unwahrhaftig ist, dass Sie mit dieser terroristischen Gefahr geradezu Handel treiben, indem Sie sagen: „Da muss man doch etwas machen“ – da stimmt Ihnen fast jeder zu –, aber wollen, dass die Maßnahmen auch auf eine ganze Serie von

(A) Straftatbeständen im Strafgesetzbuch – die Zählungen gehen auseinander; bei manchen sind es 50, bei anderen 70 – angewandt werden können.

Zweitens. Der Richtervorbehalt hat Sinn und ist auch hier sinnvoll. Darüber streiten wir ja auch nicht, obwohl das von Ihnen in der Diskussion im Rechtsausschuss bestritten worden ist. Allerdings ist angesichts der Tatsache, dass es hier um eine komplizierte und von den technischen Kenntnissen her problematische Angelegenheit geht, die Frage berechtigt, ob eine Richterin oder ein Richter einer Strafkammer, also Juristen, tatsächlich die Expertise haben, um beurteilen zu können, ob dieses Instrument mit den zu erwartenden Folgen wirklich so konzentriert eingesetzt werden kann, wenn der Staatsanwalt den Antrag stellt. Das Bundesverfassungsgericht hat verlangt, dass eine obligatorische, also verpflichtende, unabhängige Prüfung des jeweiligen Verfahrens durchgeführt werden muss. Das muss doch jedem einleuchten. Ich bin nicht so vermessen, und Sie hoffentlich auch nicht, zu sagen: Das kann ich beurteilen. – Das können nur Fachleute beurteilen. Deshalb muss es eine Verpflichtung geben, Datenschutzbeauftragte oder meinetwegen auch andere Fachleute einzubeziehen, die den Richtern beratend und sachkundig zur Seite stehen. Ansonsten ist es eine für die wirklichen Gefahren unwirksame Kontrolle.

(Beifall beim BÜNDNIS 90/DIE GRÜNEN sowie bei Abgeordneten der LINKEN)

Vizepräsidentin Ulla Schmidt:

Vielen Dank. – Herr Kollege Sensburg, möchten Sie
(B) darauf antworten? – Bitte schön.

Dr. Patrick Sensburg (CDU/CSU):

Herr Kollege Ströbele, ich antworte darauf kurz. Es ist richtig, dass Sie gesagt haben, wir müssten darüber reden. Wir reden auch. Sie machen immer ein Redeangebot. Das klingt so versöhnlich, und Herr Kollege Ströbele, ich mag Sie ja auch. Aber man muss irgendwann vom Reden zum Erarbeiten des Gesetzes übergehen, damit man Straftaten verhindern kann. Sie müssen also auch einmal schauen, wie wir gemeinsam zu einem Konsens kommen. Mit unserem Koalitionspartner sind wir zu einem Konsens gekommen.

Ich will Ihnen jetzt nicht den gesamten Straftatenkatalog vorstellen.

(Hans-Christian Ströbele [BÜNDNIS 90/DIE GRÜNEN]: Vier Seiten!)

Aber hier geht es um Straftaten wie die Bildung einer kriminellen Vereinigung, Straftaten gegen die sexuelle Selbstbestimmung, um Kinderpornografie, Mord und Totschlag oder um schweren Raub mit Todesfolge.

(Hans-Christian Ströbele [BÜNDNIS 90/DIE GRÜNEN]: Da steht „gewerbliche Hehlerei“!)

Ich könnte Ihnen alles vorlesen. Sie haben gesagt, es stehe auch etwas zum Asylgesetz drin. Es geht um das Einschleusen mit Todesfolge. Das sind für mich so schwere Straftaten – das hat nichts mit Terrorismus zu tun –, dass wir sie in einem Katalog regeln, sodass wir die Möglichkeit haben, der Polizei hier die digitale Kommunikation zugänglich zu machen. (C)

Es gibt Personen, die im Verdacht stehen, diese Art von schweren Straftaten zu begehen oder begangen zu haben. In diesen Fällen möchten wir nicht nur das normale Telefonat, das kaum einer mehr nutzt, mithören können, sondern auch die Kommunikation über Messenger-Dienste. Sonst macht polizeiliche Ermittlungsarbeit präventiv, aber auch repressiv keinen Sinn. Wir erlauben dieses Instrument, damit Strafverfolgung in der digitalen Welt weiterhin möglich ist, auf richterliche Anordnung und wenn die besondere Schwere der Straftat festgestellt wird. Darauf könnten auch Sie sich einlassen.

Danke schön.

(Beifall bei der CDU/CSU)

Vizepräsidentin Ulla Schmidt:

Vielen Dank.

(Zuruf des Abg. Jörn Wunderlich [DIE LINKE])

– Nein, Herr Wunderlich, ich lasse jetzt keine Beiträge mehr zu. Wir fangen keine Debatte von Tisch zu Tisch an.

Ich beende die Aussprache.

Wir kommen zur Abstimmung über den von der Bundesregierung eingebrachten Gesetzentwurf zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens. Der Ausschuss für Recht und Verbraucherschutz (D) empfiehlt unter Buchstabe a seiner Beschlussempfehlung auf Drucksache 18/12785, den Gesetzentwurf der Bundesregierung auf Drucksache 18/11277 in der Ausschussfassung anzunehmen. Ich bitte diejenigen, die dem Gesetzentwurf in der Ausschussfassung zustimmen wollen, um das Handzeichen. – Das ist die Koalition. Wer stimmt dagegen? – Das sind die Opposition und zwei Abgeordnete aus der SPD-Fraktion. Wer enthält sich? – Keiner. Damit ist der Gesetzentwurf in zweiter Beratung angenommen.

Dritte Beratung

und Schlussabstimmung. Ich bitte diejenigen, die dem Gesetzentwurf zustimmen wollen, sich zu erheben. – Wer stimmt dagegen? – Wer enthält sich? – Der Gesetzentwurf ist in dritter Beratung mit dem gleichen Stimmenverhältnis angenommen.

Wir kommen zur Abstimmung über den Entschließungsantrag der Fraktion Bündnis 90/Die Grünen auf Drucksache 18/12834. Wer stimmt für diesen Entschließungsantrag? – Das ist die Opposition. Wer stimmt dagegen? – Das ist die Koalition. Wer enthält sich? – Niemand. Damit ist der Entschließungsantrag abgelehnt.

Wir kommen zur Abstimmung über die Beschlussempfehlung des Ausschusses für Recht und Verbraucherschutz zu dem Gesetzentwurf der Bundesregierung zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze. Der Ausschuss für Recht und Verbraucherschutz emp-

Vizepräsidentin Ulla Schmidt

(A) fiehlt unter Buchstabe b seiner Beschlussempfehlung auf Drucksache 18/12785, den Gesetzentwurf der Bundesregierung auf Drucksache 18/11272 für erledigt zu erklären. Wer stimmt für diese Beschlussempfehlung? – Wer stimmt dagegen? – Wer enthält sich? – Damit ist die Beschlussempfehlung einstimmig angenommen.

Damit sind wir am Ende dieses Tagesordnungspunktes.

Ich rufe die Tagesordnungspunkte 14 a und 14 b sowie 37 f auf:

14. a) Beratung des Antrags der Abgeordneten Harald Ebner, Nicole Maisch, Friedrich Ostendorff, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Wege zur Pestizidreduktion in der Landwirtschaft

Drucksache 18/12382

Überweisungsvorschlag:
Ausschuss für Ernährung und Landwirtschaft (f)
Ausschuss für Umwelt, Naturschutz, Bau und Reaktorsicherheit

b) Beratung des Antrags der Abgeordneten Harald Ebner, Friedrich Ostendorff, Nicole Maisch, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Bienengiftige Insektizide vollständig verbieten – Bestäuber, andere Tiere und Umwelt wirksam schützen

(B)

Drucksache 18/12384

Überweisungsvorschlag:
Ausschuss für Ernährung und Landwirtschaft

37. f) Beratung des Antrags der Abgeordneten Katharina Dröge, Kerstin Andreae, Oliver Krischer, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Marktkonzentration im Agrarmarkt stoppen – Artenvielfalt und Ernährungssouveränität erhalten

Drucksache 18/12797

Nach einer interfraktionellen Vereinbarung sind für die Aussprache 38 Minuten vorgesehen. – Es gibt keinen Widerspruch. Dann ist so beschlossen.

Ich bitte die Agrarpolitiker und -politikerinnen, jetzt zügig die Plätze einzunehmen, und alle anderen, die nötigen Gespräche außerhalb des Plenarsaals zu führen, damit wir weitermachen können. – Dann eröffne ich die Aussprache. Das Wort hat Harald Ebner, Bündnis 90/Die Grünen.

Harald Ebner (BÜNDNIS 90/DIE GRÜNEN):

Sehr geehrte Frau Präsidentin! Werte Kolleginnen und Kollegen! Ganz aktuell häufen sich dramatische Berichte über den beängstigenden Rückgang der Zahl der Vögel, Bienen und anderen Insekten und von Wildkräutern in unseren Agrar- und Kulturlandschaften. Eine der maßgeblichen Ursachen ist der flächendeckende Pestizideinsatz: 34 000 Tonnen Wirkstoff jedes Jahr in Deutschland. (C) Die Gifte gelangen in die Böden, ins Grundwasser, in die Luft und in unser Essen.

„Wir brauchen eine Kehrtwende in der Agrarpolitik."

(Beifall beim BÜNDNIS 90/DIE GRÜNEN)

Das sagt eine Behörde des Bundes, nämlich das Bundesamt für Naturschutz. „Das System ist jetzt an einer Stelle angekommen, wo es sich nicht weiter selbst korrigieren kann." Das sagt Carl-Albrecht Bartmer, Präsident der Deutschen Landwirtschafts-Gesellschaft.

Wir müssen vermeiden, dass die Agrarwirtschaft weiter an dem Ast sägt, auf dem sie selber sitzt, wenn durch derartige Fehlentwicklungen nicht nur unsere Lebensgrundlagen, sondern auch ihre eigenen Produktionsgrundlagen zerstört werden. Wenn Böden belastet und verdichtet werden und ihre Fruchtbarkeit und damit ihre wichtigen Funktionen verlieren, wenn Ökosysteme zerstört werden und Nützlinge und Bestäuber fehlen, dann lässt sich auch nichts mehr anbauen. Das ist dann das Gegenteil von Nachhaltigkeit, meine lieben Kolleginnen und Kollegen.

(Beifall beim BÜNDNIS 90/DIE GRÜNEN)

Was unternimmt die Bundesregierung, wenn die konventionelle Agrarwirtschaft schon selbst um Hilfe ruft? Nichts, rein gar nichts außer ein paar Versprechungen und Ankündigungen hier und ein paar flotten Bauernregeln da, die dann aber doch lieber schnell wieder einkassiert werden. Das ist nach vier Jahren ein Armutszeugnis. Da gibt es bei Minister Schmidt etwas mit dem wohlklingenden Titel „Nationaler Aktionsplan Pflanzenschutz". Was (D) ist bis jetzt, zum Ende seiner Amtszeit, dabei herausgekommen? Herr Bleser – der Minister ist nicht anwesend; Sie vertreten ihn –, Sie haben uns kürzlich in einer Antwort auf eine Kleine Anfrage mitgeteilt: „Zielquoten für die Reduzierung der Anwendung sowie erreichte Reduktionen können zurzeit noch nicht angegeben werden." Ja wann denn dann bitte? Wie lange wollen Sie denn noch herumlaborieren? Das ist eine Bankrotterklärung. Bis Sie damit fertig sind, sind Vögel und Bienen ausgestorben.

(Beifall beim BÜNDNIS 90/DIE GRÜNEN)

Sie sind ja nicht einmal bereit, in Brüssel einem Verbot der schlimmsten bienengiftigen Pestizide, den Neonikotinoiden, zuzustimmen, wie es die EU-Kommission vorgeschlagen hat. Bei Minister Schmidt und der Großen Koalition sind jedenfalls Bärbel Höhns Bundestagsbienen nicht in guten Händen.

(Beifall beim BÜNDNIS 90/DIE GRÜNEN)

Glyphosat, weltweit das Ackergift Nummer eins, auch in Deutschland, wollen Sie neu zulassen, obwohl nach wie vor weitere und neue Zweifel an seiner Unbedenklichkeit aufkommen. Das ist verantwortungslos. Dabei geht es auch ganz anders in der Landwirtschaft. Der Ökolandbau macht es schon seit Jahrzehnten vor; aber auch die konventionelle Landwirtschaft kann mit wesentlich weniger Pestiziden auskommen.

(Beifall beim BÜNDNIS 90/DIE GRÜNEN sowie bei Abgeordneten der LINKEN)

Seite 130 – 224 fehlen.

Deutscher Bundestag **Drucksache 18/12785**

18. Wahlperiode 20.06.2017

Beschlussempfehlung und Bericht

des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss)

a) zu dem Gesetzentwurf der Bundesregierung
– Drucksache 18/11277 –

Entwurf eines Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens

b) zu dem Gesetzentwurf der Bundesregierung
– Drucksache 18/11272 –

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

A. Problem

Zu Buchstabe a

Der Gesetzentwurf schlägt zur Effektivierung und Steigerung der Praxistauglichkeit des Strafverfahrens zahlreiche Regelungen vor, die der Verfahrensvereinfachung und Verfahrensbeschleunigung dienen. So sollen unter anderem eine Pflicht für Zeugen, bei der Polizei zu erscheinen, Änderungen im Befangenheitsrecht und die Möglichkeit einer Fristsetzung im Beweisantragsrecht eingeführt werden. Der Erprobung neuer Instrumente zur Ermittlung des wahren Sachverhalts soll die Regelung zur verpflichtenden audiovisuellen Aufzeichnung von Beschuldigtenvernehmungen im Ermittlungsverfahren dienen. Schließlich enthält der Entwurf Vorschläge, um durch eine verstärkt kommunikative und transparente Verfahrensführung in umfangreichen Strafverfahren zu einer Effektivierung beizutragen und durch die Stärkung der Beschuldigtenrechte in einigen Bereichen späteren Streitigkeiten in der Hauptverhandlung vorzubeugen. Um die Erfassung des sogenannten DNA-Beinahetreffers bei der DNA-Reihenuntersuchung zu ermöglichen, werden entsprechende Anpassungen der §§ 81e und 81h der Strafprozessordnung vorgeschlagen.

Zu Buchstabe b

Der Gesetzentwurf sieht verschiedene Maßnahmen zur Steigerung der Effizienz der Strafverfolgung vor. Unter anderem soll der Katalog der strafrechtlichen Sanktionen um die Möglichkeit der Verhängung eines Fahrverbots bei allen Straftaten – nicht nur bei solchen, die einen Zusammenhang mit dem Führen eines Kraftfahrzeugs oder einer Pflichtverletzung im Straßenverkehr aufweisen – ergänzt werden, wobei der Charakter des Fahrverbots als Nebenstrafe beibehalten werden soll. Außerdem soll der Straftatbestand des Vorenthaltens und Veruntreuens von Arbeitsentgelt (§ 266a des Strafgesetzbuchs – StGB) um zwei neue Regelbeispiele für besonders schwere Fälle ergänzt werden. Im Strafverfahrensrecht soll für bestimmte Straßenverkehrsdelikte eine Ausnahme von der vorrangigen richterlichen Anordnungskompetenz für die Entnahme von Blutproben geschaffen und die Anordnungskompetenz insoweit auf Staatsanwaltschaft und Polizei übertragen werden. Weitere Änderungsvorschläge betreffen die Möglichkeit der Zurückstellung einer suchtbedingten Freiheitsstrafe auch bei gleichzeitigem Vorliegen nicht suchtbedingter Freiheitsstrafen, die Klarstellung, dass Bewährungshelfern in bestimmten Konstellationen die Befugnis zusteht, personenbezogene Daten unmittelbar an die Polizei sowie an Einrichtungen des Justiz- und Maßregelvollzugs zu übermitteln sowie die Strafbarkeit des leichtfertigen Tötens und Zerstörens von streng geschützten wildlebenden Tier- und Pflanzenarten.

B. Lösung

Zu Buchstabe a

Annahme des Gesetzentwurfs auf Drucksache 18/11277 in geänderter Fassung. Die Änderungen übernehmen zum einen die in dem Gesetzentwurf zu Buchstabe b vorgeschlagenen Regelungen. Daneben werden Rechtsgrundlagen für die Online-Durchsuchung und die Quellen-Telekommunikationsüberwachung geschaffen.

Annahme des Gesetzentwurfs auf Drucksache 18/11277 in geänderter Fassung mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN.

Zu Buchstabe b

Erledigterklärung des Gesetzentwurfs auf Drucksache 18/11272. Die Regelungen des Gesetzentwurfs sind durch den Änderungsantrag zu Buchstabe a mit dem Gesetzentwurf unter Buchstabe a zusammengeführt worden.

Einvernehmliche Erledigterklärung des Gesetzentwurfs auf Drucksache 18/11272.

C. Alternativen

Keine.

D. Kosten

Wurden im Ausschuss nicht erörtert.

Beschlussempfehlung

Der Bundestag wolle beschließen,

a) den Gesetzentwurf auf Drucksache 18/11277 in der aus der nachstehenden Zusammenstellung ersichtlichen Fassung anzunehmen;

b) den Gesetzentwurf auf Drucksache 18/11272 für erledigt zu erklären.

Berlin, den 20. Juni 2017

Der Ausschuss für Recht und Verbraucherschutz

Renate Künast
Vorsitzende

Alexander Hoffmann
Berichterstatter

Dr. Patrick Sensburg
Berichterstatter

Bettina Bähr-Losse
Berichterstatterin

Dr. Johannes Fechner
Berichterstatter

Jörn Wunderlich
Berichterstatter

Hans-Christian Ströbele
Berichterstatter

Zusammenstellung

des Entwurfs eines Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens
– Drucksache 18/11277 –
mit den Beschlüssen des Ausschusses für Recht und Verbraucherschutz (6. Ausschuss)

Entwurf	Beschlüsse des 6. Ausschusses
Entwurf eines Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens	**Entwurf eines Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens**
Vom ...	Vom ...
Der Bundestag hat das folgende Gesetz beschlossen:	Der Bundestag hat das folgende Gesetz beschlossen:
	Artikel 1
	Änderung des Strafgesetzbuches
	Das Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das durch Artikel 1 des Gesetzes vom 13. April 2017 (BGBl. I S. 872) geändert worden ist, wird wie folgt geändert:
	1. § 44 wird wie folgt geändert:
	a) Absatz 1 wird wie folgt geändert:
	aa) In Satz 1 werden nach dem Wort „Straftat“ das Komma und die Wörter „die er bei oder im Zusammenhang mit dem Führen eines Kraftfahrzeugs oder unter Verletzung der Pflichten eines Kraftfahrzeugführers begangen hat,“ gestrichen und wird das Wort „drei“ durch das Wort „sechs“ ersetzt.
	bb) Nach Satz 1 wird folgender Satz eingefügt:
	„Auch wenn die Straftat nicht bei oder im Zusammenhang mit dem Führen eines Kraftfahrzeugs oder unter Verletzung der Pflichten eines Kraftfahrzeugführers begangen wurde, kommt die Anordnung eines Fahrverbots namentlich in Betracht,

Seite 5 – 8 fehlen.

Entwurf	Beschlüsse des 6. Ausschusses
werden und dass sie unverzüglich vernichtet werden, sobald sie hierfür nicht mehr erforderlich sind,	
2. das Untersuchungsergebnis mit den DNA-Identifizierungsmustern von Spurenmaterial automatisiert daraufhin abgeglichen wird, ob das Spurenmaterial von ihnen oder von ihren Verwandten in gerader Linie oder in der Seitenlinie bis zum dritten Grad stammt,	
3. das Ergebnis des Abgleichs zu Lasten der betroffenen Person oder mit ihr in gerader Linie oder in der Seitenlinie bis zum dritten Grad verwandter Personen verwertet werden darf und	
4. die festgestellten DNA-Identifizierungsmuster nicht zur Identitätsfeststellung in künftigen Strafverfahren beim Bundeskriminalamt gespeichert werden.“	
	8. § 100a wird wie folgt geändert:
	a) Dem Absatz 1 werden die folgenden 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

Entwurf	Beschlüsse des 6. Ausschusses
	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

Entwurf	Beschlüsse des 6. Ausschusses
	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.“
6. § 100b *Absatz 6 Nummer 2* wird wie folgt gefasst:	**9.** § 100b wird wie folgt gefasst:
„2. die Anzahl der Überwachungsanordnungen nach § 100a Absatz 1, unterschieden nach Erst- und Verlängerungsanordnungen;“.	**„§ 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

Entwurf	Beschlüsse des 6. Ausschusses
	§ 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

Entwurf	Beschlüsse des 6. Ausschusses
	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,

Entwurf	Beschlüsse des 6. Ausschusses
	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.

Entwurf	Beschlüsse des 6. Ausschusses
	(4) § 100a Absatz 5 und 6 gilt mit Ausnahme von Absatz 5 Satz 1 Nummer 1 entsprechend.“
	10. § 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 wird die Angabe „§ 100d Abs. 2“ durch die Angabe „§ 100e Absatz 3“ ersetzt.
	d) Die Absätze 4 bis 7 werden aufgehoben.
	11. 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.

Entwurf	Beschlüsse des 6. Ausschusses
	(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

Entwurf	Beschlüsse des 6. Ausschusses
	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,

Entwurf	Beschlüsse des 6. Ausschusses
	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

Entwurf	Beschlüsse des 6. Ausschusses
	Aufenthalts der einer solchen Straftat beschuldigten Person verwendet werden.
	2. Die Verwendung der Daten, auch solcher nach § 100d Absatz 5 Satz 1 zweiter Halbsatz, 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.“
	12. In § 100f Absatz 4 werden die Wörter „§ 100b Abs. 1, 4 Satz 1 und § 100d Abs. 2 gelten“ durch die Wörter „§ 100e Absatz 1, 3, 5 Satz 1 gilt“ ersetzt.
	13. 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

Seite 20 – 38 fehlen.

Bericht der Abgeordneten Alexander Hoffmann, Dr. Patrick Sensburg, Bettina Bähr-Losse, Dr. Johannes Fechner, Jörn Wunderlich und Hans-Christian Ströbele

I. Überweisung

Zu Buchstabe a

Der Deutsche Bundestag hat die Vorlage auf **Drucksache 18/11277** in seiner 221. Sitzung am 9. März 2017 beraten und an den Ausschuss für Recht und Verbraucherschutz zur federführenden Beratung und an den Innenausschuss zur Mitberatung überwiesen.

Zu Buchstabe b

Der Deutsche Bundestag hat die Vorlage auf **Drucksache 18/11272** in seiner 221. Sitzung am 9. März 2017 beraten und an den Ausschuss für Recht und Verbraucherschutz zur federführenden Beratung sowie an den Innenausschuss, den Finanzausschuss, den Ausschuss für Familie, Senioren, Frauen und Jugend und an den Ausschuss für Umwelt, Naturschutz, Bau und Reaktorsicherheit zur Mitberatung überwiesen.

II. Stellungnahmen der mitberatenden Ausschüsse

Zu Buchstabe a

Der **Innenausschuss** hat die Vorlage auf Drucksache 18/11277 im Umlaufverfahren am 19. Juni 2017 beraten und empfiehlt mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN die Annahme.

Der **Finanzausschuss** hat die Vorlage auf Drucksache 18/11277 in seiner 118. Sitzung am 20. Juni 2017 gutachtlich beraten und empfiehlt mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN die Annahme.

Der **Ausschuss für Umwelt, Naturschutz, Bau und Reaktorsicherheit** hat die Vorlage auf Drucksache 18/11277 in seiner 121. Sitzung am 20. Juni 2017 gutachtlich beraten und empfiehlt mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN die Annahme mit Änderungen. Der Änderungsantrag der Fraktionen der CDU/CSU und SPD wurde mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN angenommen.

Der **Ausschuss für Familie, Senioren, Frauen und Jugend** hat die Vorlage auf Drucksache 18/11277 in seiner 94. Sitzung am 20. Juni 2017 gutachtlich beraten und empfiehlt mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN die Annahme mit Änderungen. Der Änderungsantrag der Fraktionen der CDU/CSU und SPD wurde mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN angenommen.

Der **Parlamentarische Beirat für nachhaltige Entwicklung** hat sich mit der Vorlage auf Bundesratsdrucksache 796/16 (Bundestagsdrucksache 18/11277) am 30. Januar 2017 befasst und festgestellt, dass eine Nachhaltigkeitsrelevanz des Gesetzentwurfs nicht gegeben sei. Eine Prüfbitte sei daher nicht erforderlich.

Zu Buchstabe b

Der **Innenausschuss** hat die Vorlage auf Drucksache 18/11272 im Umlaufverfahren am 19. Juni 2017 beraten und empfiehlt mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN die Annahme.

Der **Finanzausschuss** hat die Vorlage auf Drucksache 18/11272 in seiner 118. Sitzung am 20. Juni 2017 beraten und empfiehlt einstimmig, die Vorlage für erledigt zu erklären.

Der **Ausschuss für Familie, Senioren, Frauen und Jugend** hat die Vorlage auf Drucksache 18/11272 in seiner 94. Sitzung am 20. Juni 2017 beraten und empfiehlt, die Vorlage für erledigt zu erklären.

Der **Ausschuss für Umwelt, Naturschutz, Bau und Reaktorsicherheit** hat die Vorlage auf Drucksache 18/11272 in seiner 121. Sitzung am 20. Juni 2017 beraten und empfiehlt mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN die Annahme.

Der **Parlamentarische Beirat für nachhaltige Entwicklung** hat sich mit der Vorlage auf Bundesratsdrucksache 792/16 (Bundestagsdrucksache 18/11272) am 30. Januar 2017 befasst und festgestellt, dass eine Nachhaltigkeitsrelevanz des Gesetzentwurfs gegeben sei. Der Bezug zur nationalen Nachhaltigkeitsstrategie ergebe sich hinsichtlich der Indikatoren 5 (Artenvielfalt – Arten erhalten und Lebensräume schützen), 6 (Staatsverschuldung – Haushalt konsolidieren und Generationengerechtigkeit schaffen) und 15 (Kriminalität – Persönliche Sicherheit weiter erhöhen). Die Auswirkungen auf die nachhaltige Entwicklung seien vorbildlich geprüft und dargestellt. Eine Prüfbitte sei daher nicht erforderlich.

III. Beratungsverlauf und Beratungsergebnisse im federführenden Ausschuss

Zu Buchstabe a

Der Ausschuss für Recht und Verbraucherschutz hat die Vorlage auf Drucksache 18/11277 in seiner 131. Sitzung am 8. März 2017 anberaten und beschlossen, eine öffentliche Anhörung durchzuführen, die er in seiner 139. Sitzung am 29. März 2017 durchgeführt hat. An dieser Anhörung haben folgende Sachverständige teilgenommen:

Dr. Axel Boetticher	Richter am Bundesgerichtshof a. D., Bremen
Stefan Conen	Rechtsanwalt, Berlin
Dr. Markus Löffelmann	Richter am Landgericht München I, München
Prof. Dr. Andreas Mosbacher	Richter am Bundesgerichtshof, 5. Strafsenat, Karlsruhe Honorarprofessor an der Universität Leipzig für Strafrecht und Strafprozessrecht, insbesondere Wirtschaftsstrafrecht und Revisionsrecht
Dr. Ali B. Norouzi	Deutscher Anwaltverein e. V. (DAV), Berlin Rechtsanwalt
Prof. Dr. Henning Radtke	Richter am Bundesgerichtshof, 1. Strafsenat, Karlsruhe,
Marc Wenske	Deutscher Richterbund e. V. Richter am OLG Hamburg Hanseatisches Oberlandesgericht

Hinsichtlich der Ergebnisse der Anhörung wird auf das Protokoll der 139. Sitzung vom 29. März 2017 mit den anliegenden Stellungnahmen der Sachverständigen verwiesen.

Zu Buchstabe b

Der Ausschuss für Recht und Verbraucherschutz hat die Vorlage auf Drucksache 18/11272 in seiner 131. Sitzung am 8. März 2017 anberaten und beschlossen, eine öffentliche Anhörung durchzuführen, die er in seiner 136. Sitzung am 22. März 2017 durchgeführt hat. An dieser Anhörung haben folgende Sachverständige teilgenommen:

Dr. Wolfgang Beckstein	Staatsanwaltschaft München I Oberstaatsanwalt, Hauptabteilungsleiter
Dr. Thomas A. Bode	Europa-Universität Viadrina Frankfurt (Oder) Akademischer Mitarbeiter am Lehrstuhl für Strafrecht, Strafprozessrecht und Rechtsinformatik Prof. Dr. Wolf
Erik Ohlenschlager	Staatsanwaltschaft Bamberg Leitender Oberstaatsanwalt

Martin Rubbert	Deutscher Anwaltverein e. V. Rechtsanwalt Berlin
Prof. Dr. Reinhold Schlothauer	Bundesrechtsanwaltkammer (BRAK) Rechtsanwalt/Fachanwalt für Strafrecht, Bremen
Prof. Dr. em. Heinz Schöch	Ludwig-Maximilians-Universität München Lehrstuhl für Strafrecht, Kriminologie, Jugendrecht und Strafvollzug
Prof. Dr. Torsten Verrel	Universität Bonn Fachbereich Rechtswissenschaften Kriminologisches Seminar Geschäftsführender Direktor

Hinsichtlich der Ergebnisse der Anhörung wird auf das Protokoll der 136. Sitzung vom 22. März 2017 mit den anliegenden Stellungnahmen der Sachverständigen verwiesen.

Der Ausschuss für Recht und Verbraucherschutz hat die Vorlage auf Drucksache 18/11272 in seiner 147. Sitzung am 17. Mai 2017 erneut beraten und beschlossen, eine weitere öffentliche Anhörung durchzuführen, die er in seiner 152. Sitzung am 31. Mai 2017 durchgeführt hat. Gegenstand der öffentlichen Anhörung war eine Formulierungshilfe der Bundesregierung auf Ausschussdrucksache 18(6)334. An dieser Anhörung haben folgende Sachverständige teilgenommen:

Dr. Ulf Buermeyer, LL.M. (Columbia)	Richter am Landgericht Berlin
Michael Greven	Deutscher Richterbund e. V. Oberstaatsanwalt beim Bundesgerichtshof Karlsruhe
Peter Henzler	Vizepräsident beim Bundeskriminalamt Wiesbaden
Alfred Huber	Staatsanwaltschaft Nürnberg-Fürth Oberstaatsanwalt, Stellvertretender Behördenleiter und Abteilungsleiter der BtM- und OK-Abteilung
Dr. Matthias Krauß	Oberstaatsanwalt beim Bundesgerichtshof Karlsruhe
Linus Neumann	Berlin
Prof. Dr. Arndt Sinn	Universität Osnabrück Lehrstuhl für Deutsches und Europäisches Straf- und Strafprozessrecht, Internationales Strafrecht sowie Strafrechtsvergleichung Direktor des Zentrums für Europäische und Internationale Strafrechtsstudien (ZEIS)

Hinsichtlich der Ergebnisse der Anhörung wird auf das Protokoll der 152. Sitzung vom 31. Mai 2017 mit den anliegenden Stellungnahmen der Sachverständigen verwiesen.

Zu den Buchstaben a und b

Der **Ausschuss für Recht und Verbraucherschutz** hat die Vorlage auf Drucksache 18/11277 in seiner 154. Sitzung am 20. Juni 2017 abschließend beraten und empfiehlt mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN die Annahme des Gesetzentwurfs in der aus der Beschlussempfehlung ersichtlichen Fassung. Die Änderungen entsprechen einem von den Fraktionen der CDU/CSU und SPD in den Ausschuss eingebrachten Änderungsantrag, der mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN angenommen wurde. Hinsichtlich der Vorlage auf Drucksache 18/11272 hat der **Ausschuss für Recht und Verbraucherschutz** einvernehmlich empfohlen, den Gesetzentwurf für erledigt zu erklären.

Die **Fraktion BÜNDNIS 90/DIE GRÜNEN** kritisierte das Gesetzgebungsverfahren. Mit einem Überraschungscoup werde ein schwerer Grundrechtseingriff eingeführt. Dieser betreffe insbesondere das Grundrecht auf die Integrität informationstechnischer Systeme und das Recht auf informationelle Selbstbestimmung der gesamten Bevölkerung. Die Qualität dieses Eingriffs verändere das ursprüngliche Vorhaben zur Änderung der Strafprozessordnung völlig; er sei noch gravierender und umfassender als der Große Lauschangriff. Angesichts der bestehenden Gefahren bestreite die Fraktion eine gewisse Notwendigkeit zur Schaffung solcher Regelungen nicht. Diese müssten jedoch sehr sorgfältig überlegt und im Einzelnen abgewogen werden. Dies sei vorliegend nicht der Fall, insbesondere seien zu viele Öffnungsklauseln vorgesehen. Außerdem müsse sichergestellt werden, dass neben der richterlichen Überprüfung auch Fachleute an der Technik und Kontrolle der Maßnahmen beteiligt seien. Die Fraktion kritisierte zudem eine Ungleichbehandlung von zeugnisverweigerungsberechtigten Berufsgeheimnisträgern und deren Helfern in § 100d Absatz 5 StPO-E.

Die **Fraktion DIE LINKE.** schloss sich der Kritik daran an, dass die Quellen-Telekommunikationsüberwachung über einen Änderungsantrag in das Gesetz gebracht werde. Die Regelungen zum Führerscheinentzug als Strafe und zum Wegfall des Richtervorbehalts bei der Blutentnahme seien aus richterlicher Sicht unsinnig. Gleiches gelte auch für die Aufzeichnung der Erstvernehmung mit Bild und Ton. Die Überwachung der Anbahnungsgespräche von inhaftierten Mandanten mit Verteidigern werde von der Anwaltschaft abgelehnt. Die Fraktion lehne den Gesetzentwurf, insbesondere auch wegen der „durch die Hintertür" eingeführten Quellen-Telekommunikationsüberwachung, vollumfänglich ab.

Die **Fraktion der CDU/CSU** merkte an, dass Gesetzentwurf und Änderungsantrag Ergebnis einer intensiven Diskussion seien. Eine effektivere und praxistaugliche Ausgestaltung des Strafverfahrens sei bereits im Koalitionsvertrag vorgesehen gewesen. Der Bundesminister der Justiz und für Verbraucherschutz habe zu Beginn der Wahlperiode eine Reform der Strafprozessordnung als den größten Gesetzgebungsakt der Wahlperiode angekündigt. Die einzelnen Elemente des Vorhabens seien gründlich besprochen worden und auch Gegenstand öffentlicher Anhörungen gewesen. Dies gelte für das Fahrverbot – das gerade Vertreter der Praxis gefordert hätten – ebenso wie für die Quellen-Telekommunikationsüberwachung. Inhaltlich könne man sicher unterschiedlicher Meinung sein, doch die Kritik am Verfahren sei nicht nachvollziehbar.

Die **Fraktion der SPD** trat ebenfalls der Behauptung entgegen, es handele sich um einen gesetzgeberischen „Schnellschuss". Sowohl die Aufhebung des Richtervorbehalts bei der Blutentnahme als auch das Fahrverbot als zusätzliche Sanktion seien von verschiedenen Seiten gefordert und umfassend diskutiert worden. Die Schaffung einer Rechtsgrundlage für die Quellen-Telekommunikationsüberwachung in der StPO sei aus Gründen der Rechtssicherheit überfällig; auch dieses Thema sei intensiv beraten worden. Die Strafschärfungen im Bundesnaturschutzgesetz seien ebenfalls wichtige Maßnahmen. Insgesamt handele es sich um ein sinnvolles Gesetz.

Die **Bundesregierung** wies darauf hin, dass die Regelung für die Berufsgeheimnisträger in § 100d Absatz 5 StPO-E der bislang für die Wohnraumüberwachung geltenden Regelung in § 100c Absatz 6 StPO entspreche. Möglicherweise sei der Schutz der Berufsgeheimnisträger in der StPO grundlegend überarbeitungs- und harmonisierungsbedürftig; hierbei handele es sich jedoch um ein Projekt für eine der kommenden Wahlperioden.

Dem Ausschuss für Recht und Verbraucherschutz lagen mehrere Petitionen vor.

IV. Zur Begründung der Beschlussempfehlung

Der Ausschuss hat den Entwurf eines Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens (Drucksache 18/11277) mit dem Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, der Strafprozessordnung, des Jugendgerichtsgesetzes und weiterer Gesetze (Drucksache 18/11272) verbunden und um Regelungen zur Schaffung von Rechtsgrundlagen für die Online-Durchsuchung und die Quellen-Telekommunikationsüberwachung ergänzt (Ausschussdrucksache 18(6)334 vom 15. Mai 2017).

Zur Begründung der ursprünglichen Inhalte des Entwurfs eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze wird auf die Drucksache 18/11272 verwiesen, soweit diese unverändert übernommen wurden. Dies betrifft die verschärfte Strafbarkeit organisierter Formen von Schwarzarbeit (Artikel 1 Nummer 3), die Erleichterung der Strafzurückstellung bei betäubungsmittelabhängigen Mehrfachtätern (Artikel 3 Nummer 36 und 37), die Schaffung einer gesetzlichen Grundlage für die

Datenübermittlung durch die Bewährungshilfe (Artikel 3 Nummer 40 und 41) sowie eine europarechtlich gebotene Erweiterung bestimmter Straftatbestände im Bundesnaturschutzgesetz (Artikel 7).

Für die Erweiterung des Fahrverbots auf alle Straftaten im Allgemeinen Strafrecht und im Jugendstrafrecht (Artikel 1 Nummer 1 und Artikel 2) sind aufgrund der Sachverständigenanhörung am 22. März 2017 eher geringfügige bzw. klarstellende Änderungen vorgesehen, die im Folgenden im Einzelnen begründet werden. Gleiches gilt für die Einschränkung des Richtervorbehalts bei der Blutprobenentnahme im Zusammenhang mit Straßenverkehrsdelikten (Artikel 3 Nummer 5). Insoweit enthält der Regelungstext eine Ergänzung, die Begründung eine Klarstellung. Soweit der Gesetzentwurf in den beiden vorgenannten Punkten unverändert geblieben ist, wird auf die Begründung in der Drucksache 18/11272 verwiesen.

Die neu hinzugekommenen Regelungen zur Schaffung von Rechtsgrundlagen für die Quellen-Telekommunikationsüberwachung und die Online-Durchsuchung in der Strafprozessordnung (Artikel 3 Nummer 8 ff.) werden umfassend begründet.

Der ursprüngliche Entwurf eines Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens enthält lediglich in § 136 Absatz 4 der Strafprozessordnung in der Entwurfsfassung – StPO-E (Artikel 3 Nummer 17 Buchstabe b) eine klarstellende Änderung zur audiovisuellen Aufzeichnung von Beschuldigtenvernehmungen. Die bisher in Artikel 1 Nummer 6 und 7 StPO-E enthaltenen Anpassungen der geltenden jährlichen Berichtspflichten an die aktuellen technischen Entwicklungen haben in den neuen Vorschlag zur Schaffung einer Rechtsgrundlage für die Online-Durchsuchung und die Quellen-Telekommunikationsüberwachung Eingang gefunden; entsprechend wurde auch die Übergangsvorschrift im Einführungsgesetz zur Strafprozessordnung (EGStPO) angepasst.

Zu Artikel 1 (Änderung des Strafgesetzbuches – StGB)

Zu Nummer 1

Zu Buchstabe a Doppelbuchstabe bb (Änderung des § 44 Absatz 1 Satz 2)

Mit der vorgeschlagenen Ergänzung von § 44 Absatz 1 des Strafgesetzbuches in der Entwurfsfassung (StGB-E) um einen neuen Satz 2 soll die von den Sachverständigen Dr. Bode (schriftliche Stellungnahme, S. 2), Ohlenschlager (schriftliche Stellungnahme, S. 4 f.) und mit Einschränkung auch bei Prof. Dr. Schöch (schriftliche Stellungnahme, S. 3) erhobene Forderung aufgegriffen werden, im Gesetz selbst Vorgaben zu machen, wann die Verhängung eines Fahrverbots, insbesondere bei Straftaten ohne Verkehrsbezug, nach der Neuregelung in Betracht kommt. Wenngleich insoweit Bedenken im Hinblick auf den Bestimmtheitsgrundsatz aus den im Gesetzentwurf der Bundesregierung genannten Gründen (Drucksache 18/11272, S. 16) nicht durchgreifend erscheinen (im Ergebnis ebenso Janker, DAR 2017, S. 13; Schöch, a. a. O., S. 3), kann die vorgeschlagene Ergänzung diesbezügliche Zweifel beseitigen und vor allem der Praxis die Rechtsanwendung erleichtern.

Dem Richter sollen mit dieser Ergänzung – in Anlehnung an die bereits in der Begründung des Gesetzentwurfs der Bundesregierung enthaltenen Erläuterungen – im Gesetz selbst Leitlinien für die Entscheidung über die Verhängung eines Fahrverbots an die Hand gegeben werden. Die in § 44 Absatz 1 Satz 2 StGB-E enthaltenen Vorgaben sollen die Fallkonstellationen hervorheben, bei denen die Nebenstrafe vornehmlich („namentlich“) in Betracht kommt. Die Entscheidung, ob tatsächlich ein Fahrverbot neben der Hauptstrafe zu verhängen ist, obliegt weiterhin dem richterlichen Ermessen („kann“). Dabei ist stets zu beachten, dass Haupt- und Nebenstrafe in einer Wechselwirkung stehen und daher zusammen das Maß der Tatschuld nicht überschreiten dürfen (vgl. LK-Geppert, StGB, 12. Auflage, § 44 Rn. 22; Schönke/Schröder/Stree/Kinzig StGB, 29. Auflage 2014, § 44 Rn. 14 mit weiteren Nachweisen).

Die aufgeführten Leitlinien greifen vornehmlich den mit der vorgeschlagenen Ausweitung des Fahrverbots auf alle Straftaten verfolgten Zweck auf, im Bereich kleinerer und mittlerer Kriminalität auch jenseits von verkehrsbezogenen Delikten den Täter durch eine Kombination von Haupt- und Nebenstrafe unter Berücksichtigung der Strafzwecke noch zielgenauer bestrafen zu können. Der Richter hat also auch bei diesen Straftaten nach pflichtgemäßem Ermessen zu entscheiden, ob die Strafzwecke durch eine Hauptstrafe allein oder besser durch deren Verbindung mit einem Fahrverbot erreicht werden können (vgl. zum bisherigen Recht LK-Geppert, a. a. O., mit weiteren Nachweisen).

Seite 44 – 45 fehlen.

Zu Artikel 3 (Änderung der Strafprozessordnung – StPO)

Zu Nummer 1 (Änderung der Inhaltsübersicht)

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

Zu Nummer 5 (Änderung des § 81a)

Die in Bezug genommenen Straßenverkehrsdelikte des § 315a Absatz 1 Nummer 1 StGB und des § 315c Absatz 1 Nummer 1 Buchstabe a StGB sollen wie der ebenfalls in Bezug genommene § 316 StGB nicht nur Vorsatztaten, sondern auch die Begehungsformen der Fahrlässigkeit und des Versuchs erfassen. Dies wird im Gesetz ergänzend klargestellt.

Es wird nochmals hervorgehoben, dass die Ausnahme der in der Vorschrift genannten Straßenverkehrsdelikte von dem Erfordernis einer vorherigen richterlichen Anordnung eine grundsätzlich gleichrangige Anordnungskompetenz von Staatsanwaltschaft und Polizei zur Folge hat. Die Sachleitungsbefugnis der Staatsanwaltschaft steht dem nicht entgegen und bleibt davon unberührt. Der Staatsanwaltschaft bleibt es unbenommen, in Ausübung ihrer Sachleitungsbefugnis generalisierende Vorgaben zu machen, Fallgruppen zu bilden oder sich die Entscheidung im Einzelfall gänzlich vorzubehalten. Dies entspricht der derzeit gängigen Praxis in den Bundesländern und ermöglicht eine ebenso flexible Handhabung in der Zukunft.

Zu den Nummern 8 bis 16, 20, 21, 24 bis 26, 39 (Änderungen der §§ 100a ff.)

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 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 in Verbindung mit 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 Integrität 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 in Verbindung mit Artikel 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. Die Änderung 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.

Zu Nummer 8 (§ 100a)

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 in Verbindung mit 1 Absatz 1 GG (verschlüsselte Nachrichten über Messenger-Dienste) dar.

Der Schutzbereich des Artikels 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 Artikels 10 GG vom Schutzbereich des Artikels 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG nach „Herrschaftssphären“ abgegrenzt. Wird die Kommunikation zeitlich während des Übertragungsvorgangs überwacht, ist der Schutzbereich des Artikels 10 GG, vor Beginn und nach Abschluss des Übertragungsvorgangs hingegen der Schutzbereich des Artikels 2 Absatz 1 in Verbindung mit Artikel 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 in Verbindung mit 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.

Die Regelung 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 in Verbindung mit 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.

Die Überwachung und Aufzeichnung von Messenger-Nachrichten nach § 100a Absatz 1 Satz 3 StPO-E ist somit einerseits inhaltlich auf Kommunikationsinhalte begrenzt, die bisher auch im Wege der herkömmlichen Telekommunikationsüberwachung ausgeleitet werden dürfen. Entwürfe von Nachrichten, die noch nicht abgeschickt wurden, werden nicht erfasst.

Die Maßnahme ist zudem zeitlich auf Messenger-Nachrichten begrenzt, die nach dem Ergehen des richterlichen Beschlusses, nach § 100e Absatz 1 Satz 4 StPO-E jedoch zunächst nur für die Dauer von drei Monaten, abgesendet werden. Innerhalb dieses Zeitraums gilt dies unabhängig davon, wann die Software auf das Gerät aufgebracht wird. Ziel der gesetzlichen Regelung ist es, ein funktionales Äquivalent zur derzeit möglichen herkömmlichen

Ausleitung der Telekommunikation zu schaffen, die bei den Telekommunikationsunternehmen im öffentlichen Telekommunikationsnetz mit dem Vorliegen des Beschlusses auch faktisch erfolgen kann. Würden die Messenger-Nachrichten folglich unverschlüsselt als SMS versandt, könnten sie derzeit ab Erlass der richterlichen Anordnung überwacht und aufgezeichnet werden; dies soll künftig für die verschlüsselten Nachrichten ebenfalls gelten. Die Gefahr, dass der Zeitraum zwischen dem Erlass des richterlichen Beschlusses und dem Aufbringen der Software unbegrenzt lang ist und ein rückwirkendes Ausleiten daher erhebliche Zeiträume umfasst, besteht aufgrund der obligatorischen Befristung des Überwachungszeitraums nicht. Ein Überwachen und Aufzeichnen ist gemäß § 100e Absatz 1 Satz 4 StPO nur für maximal drei Monate zulässig und kann danach nur bei Fortbestehen der Anordnungsvoraussetzungen verlängert werden. Diese Befristungsregelung entspricht der Regelung im geltenden Recht. Kann innerhalb dieses Zeitraums künftig die Software nicht auf das Gerät aufgebracht werden, wird der Beschluss ungültig und die Maßnahme darf nicht mehr durchgeführt werden.

Ältere Nachrichten, die vor Erlass des richterlichen Beschlusses versandt wurden, dürfen auf der Grundlage des § 100a Absatz 1 Satz 3 StPO-E nicht erhoben werden. Eine solche rückwirkende Erhebung kann vielmehr ausschließlich als Online-Durchsuchung auf der Grundlage des § 100b StPO-E erfolgen, soweit die Voraussetzungen hierfür vorliegen.

Die zeitliche Begrenzung auf Messenger-Nachrichten, die ab dem Zeitpunkt des richterlichen Beschlusses abgesendet wurden, ist, wie in § 100a Absatz 5 Satz 1 Nummer 1 Buchstabe b StPO-E geregelt, auch technisch eindeutig sicherzustellen. Kann eine Trennung der Messenger-Nachrichten nach einzelnen Zeitpunkten durch die Software nicht vorgenommen werden oder existiert eine solche Software (noch) nicht, ist die Maßnahme auf der Grundlage des § 100a Absatz 1 Satz 3 StPO-E unzulässig.

Mit den in § 100a Absatz 6 StPO-E vorgesehenen Protokollierungspflichten werden die notwendigen Vorkehrungen geschaffen, um die nachträgliche Überprüfung zu gewährleisten, dass die Maßnahme von den Strafverfolgungsbehörden in rechtmäßiger Art und Weise durchgeführt wurde. Insbesondere wird dadurch die Prüfung ermöglicht, ob eine Software verwendet wurde, die den Anforderungen des § 100a Absatz 5 Satz 1 Nummer 1 Buchstabe b StPO-E genügt hat. Organisatorisch werden im Zuständigkeitsbereich des Bundes zudem bereits die Durchführung und die Protokollierung der Maßnahme in verschiedenen Einheiten des Bundeskriminalamtes getrennt vorgenommen. So wird bei der Vorbereitung, Durchführung und Nachbereitung der Maßnahme verfahrenstechnisch sichergestellt, dass die Vorgaben des Gesetzes in vollem Umfang eingehalten werden. Darüber hinaus besteht ein Prüfungsrecht des behördlichen Datenschutzbeauftragten sowie der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit im Rahmen ihrer gesetzlichen Kompetenzen.

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

Zu 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.

Zu Absatz 5

Der neu gestaltete Absatz 5 des § 100a fasst die in § 51 Absatz 2 Satz 1 Nummer 1 und § 49 Absatz 2 BKAG 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 (vgl. 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 § 49 Absatz 2 Nummer 1 und 2 und Satz 2 BKAG. 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.

Zu 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 § 82 Absatz 1 und Absatz 2 Nummer 8 Buchstabe b BKAG 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 § 82 Absatz 4 BKAG auch Verwendungs- und Löschungsvorschriften für die Protokollierung vorgesehen sind, 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 9 (§ 100b)

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 eigenständiger Ausprägung des Rechts auf informationelle Selbstbestimmung nach Artikel 2 Absatz 1 in Verbindung mit 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; 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.

Zu 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.

Zu Absatz 2

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

Die in Nummer 1 Buchstabe a aufgeführten §§ 98 Absatz 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.

Zu 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.

Zu 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 10 (§ 100c)

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 11 (§§ 100d, 100e)

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.

Zu § 100d

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 Satz 1, 100c Absatz 4 Satz 1 StPO.; 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 z. B. 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 Satz 2 bis 4, § 100c Absatz 5 Satz 2 bis 4 StPO), 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 Absatz 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 enthaltenen Vorschriften zum Schutz des Kernbereichs privater Lebensgestaltung bei der Wohnraumüberwachung in einer ergänzenden Regelung für die Erhebungs- und Auswertungsebene zusammen. Maßnahmen nach § 100c 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. 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 oben genannten 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 enthaltene Regelung zum Schutz von Zeugnisverweigerungsberechtigten, insbesondere Berufsgeheimnisträgern. Diese wird auf Maßnahmen der Online-Durchsuchung erstreckt.

Zu § 100e

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. 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, 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, 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 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 gegebenenfalls 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.

Absatz 4 enthält entsprechend der für die Wohnraumüberwachung bisher geltenden Regelung in § 100d Absatz 3 StPO. 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 a. F. (§ 51 BKAG g. F.) 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) zusammen und erstreckt die für die Wohnraumüberwachung geltenden – erweiterten – Bestimmungen auf die Online-Durchsuchung.

Absatz 6 enthält die bisher in § 100d Absatz 5 StPO 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 12 (§ 100f Absatz 4)

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Nummer 13 (§ 100i Absatz 3)

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Nummer 14 (§ 101)

Die Verfahrensregelungen bei verdeckten Maßnahmen in § 101 StPO 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 15 (§ 101a Absatz 1)

Es handelt sich um redaktionelle Folgeänderungen.

Zu Nummer 16 (§ 101b)

Die geltenden jährlichen Pflichten zur statistischen Erfassung für Maßnahmen nach den §§ 100a bis 100c StPO-E und § 100g 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, Absatz 1 Satz 3 entspricht § 100e Absatz 1 Satz 2 StPO.

Absatz 2 entspricht § 100b Absatz 6 StPO, 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 und betrifft Maßnahmen der Wohnraumüberwachung.

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

Seite 59 – 60 fehlen.

04.07.17

Empfehlungen
der Ausschüsse

R - AV

zu **Punkt 97** der 959. Sitzung des Bundesrates am 7. Juli 2017

Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens

A.

1. Der **Ausschuss für Agrarpolitik und Verbraucherschutz**

empfiehlt dem Bundesrat,

zu dem Gesetz gemäß Artikel 77 Absatz 2 des Grundgesetzes die Einberufung des Vermittlungsausschusses mit dem Ziel zu verlangen, die Regelungen zur Online-Durchsuchung und Quellen-Telekommunikationsüberwachung zu streichen.

Begründung:

Der Bundesrat sieht mit Sorge, dass die im Gesetz vorgesehene weite Befugnis zur Online-Durchsuchung und Quellen-Telekommunikationsüberwachung zu einer massiven Schwächung der IT-Sicherheitsinfrastruktur und damit auch zu einer Gefährdung der Nutzerinnen und Nutzer informationstechnischer Systeme beitragen kann. Das Gesetz sieht vor, dass eine Überwachung von Messenger-Diensten durch den Einsatz eines sogenannten Staatstrojaners möglich sein soll, der tief in das Betriebssystem von Rechnern und Smartphones eindringt und eine umfangreiche Überwachung möglich macht. Der vorgeschlagene Einsatz von Spähsoftware kann dazu führen, dass die für die Installation dieser Software notwendigen Schwachstellen auf den informationstechnischen Geräten von Verbraucherinnen und Verbrauchern auch von Kriminellen entdeckt und missbraucht werden können. Die Ausnutzung von bisher unbekannten Sicherheitslücken eines informationstechnischen Systems zum Einsatz von

...

Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln
Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0720-2946

Überwachungsprogrammen kann erhebliche Sicherheitsinteressen der Verbraucherinnen und Verbraucher beeinträchtigen.

Das vorliegende Gesetz schafft ein Interesse für Sicherheitsbehörden, die Cyber-Sicherheit weltweit zu schwächen, um informationstechnische Systeme von Zielpersonen infiltrieren zu können. Die kalkulierte IT-Unsicherheit erscheint insbesondere vor dem Hintergrund der jüngsten Cyber-Angriffe mithilfe des globalen Erpressungstrojaners "WannaCry" und damit einhergehenden Aufforderungen staatlicher Sicherheitsbehörden an Verbraucherinnen und Verbraucher sowie Unternehmen, die IT-Systeme besser zu sichern, zumindest widersprüchlich.

Die Installation von Überwachungssoftware seitens staatlicher Stellen kann dazu führen, dass Dritte in das System mittels Nachladefunktion eindringen können, indem sie eine unzureichende Authentifizierung und Verschlüsselung ausnutzen. Je öfter die Schwachstelle ausgenutzt wird, desto eher können auch Kriminelle und andere Interessengruppen solche Lücken missbrauchen.

Dem Bundesrat war es nicht möglich, sich im Rahmen der Stellungnahme zu dem Gesetzentwurf der Bundesregierung, der bereits eine Vielzahl von Maßnahmen zur effektiveren und praxistauglichen Ausgestaltung des Strafverfahrens enthielt, hierzu zu positionieren. Das Gesetz bedarf jedoch zum Schutz der Rechte der Verbraucherinnen und Verbraucher einer entsprechenden Änderung.

B.

2. Der **federführende Rechtsausschuss**

empfiehlt dem Bundesrat,

zu dem Gesetz einen Antrag gemäß Artikel 77 Absatz 2 des Grundgesetzes nicht zu stellen.

C.

Der **Ausschuss für Agrarpolitik und Verbraucherschutz**

empfiehlt dem Bundesrat ferner folgende

E n t s c h l i e ß u n g

zu fassen:

3. Der Bundesrat sieht mit Sorge, dass die im Gesetz vorgesehene weite Befugnis zur Online-Durchsuchung und Quellen-Telekommunikationsüberwachung zu einer massiven Schwächung der IT-Sicherheitsinfrastruktur und damit auch zu einer Gefährdung der Nutzerinnen und Nutzer informationstechnischer Systeme beitragen kann. Das Gesetz sieht vor, dass eine Überwachung von Messenger-Diensten durch den Einsatz eines sogenannten Staatstrojaners möglich sein soll, der tief in das Betriebssystem von Rechnern und Smartphones eindringt und eine umfangreiche Überwachung möglich macht. Der vorgeschlagene Einsatz von Spähsoftware kann dazu führen, dass die für die Installation dieser Software notwendigen Schwachstellen auf den informationstechnischen Geräten von Verbraucherinnen und Verbrauchern auch von Kriminellen entdeckt und missbraucht werden können. Die Ausnutzung von bisher unbekannten Sicherheitslücken eines informationstechnischen Systems zum Einsatz von Überwachungsprogrammen kann erhebliche Sicherheitsinteressen der Verbraucherinnen und Verbraucher beeinträchtigen.

4. Der Bundesrat stellt fest, dass das Gesetz im Rahmen der Beratung im Deutschen Bundestag um die weiteren Regelungsbereiche der Online-Durchsuchung und Quellen-Telekommunikationsüberwachung ergänzt worden ist, die weit über den ursprünglichen Wesensgehalt des Gesetzes hinausgehen. Eine umfassende Beteiligung der Länder zu diesen Regelungsbereichen hat nicht stattgefunden. Der Bundesrat bedauert, dass es ihm nicht möglich

war, sich im Rahmen der Stellungnahme zu dem Gesetzentwurf der Bundesregierung, der bereits eine Vielzahl von Maßnahmen zur effektiveren und praxistauglichen Ausgestaltung des Strafverfahrens enthielt, hierzu zu positionieren. Bei einer Regelung dieser Tragweite, Eingriffstiefe und Auswirkung auf die Praxis sowie den Kernbereich privater Lebensgestaltung wäre dies jedoch angemessen gewesen.

5. Der Bundesrat stellt fest, dass mit den vorgelegten Änderungen für den Bereich der Strafverfolgung Rechtsgrundlagen für die Online-Durchsuchung und die Quellen-Telekommunikationsüberwachung geschaffen werden sollen. Nach einem Grundsatzurteil des Bundesverfassungsgerichts waren solche Eingriffe bisher auf Terrorismus-Ermittlungen im Bereich der Gefahrenabwehr beschränkt. Der Bundesrat merkt an, dass der Einsatz von Überwachungsprogrammen durch die Strafverfolgungsbehörden in Form einer Online-Durchsuchung und einer Quellen-Telekommunikationsüberwachung angesichts der Vielzahl damit zugänglicher personenbezogener Daten umfangreichere Rückschlüsse über die Zielperson zulässt als die akustische Wohnraumüberwachung. Dies bedeutet eine völlig neue Schwere des Grundrechtseingriffs und beinhaltet erhebliche datenschutzrechtliche Risiken.

Der Bundesrat sieht die Gefahr, dass das vorliegende Gesetz das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme sowie das Fernmeldegeheimnis verletzt, da es die diesbezüglich vom Bundesverfassungsgericht im Gefahrenabwehrbereich aufgestellten Voraussetzungen nicht erfüllen könnte. Das Bundesverfassungsgericht hat für den präventiven Bereich strenge Voraussetzungen an die Online-Überwachung geknüpft. Diese Maßstäbe müssen auch im Bereich der Strafverfolgung berücksichtigt werden. Das Gesetz begrenzt die Online-Überwachung aber weder auf schwerste Straftaten, noch beschränkt es die Quellen-Telekommunikationsüberwachung auf laufende Kommunikation. Der Bundesrat hat daher erhebliche Zweifel an der Verhältnismäßigkeit des Gesetzes.

Begründung (nur gegenüber dem Plenum):

Das Gesetz schafft ein Interesse für Sicherheitsbehörden, die Cyber-Sicherheit weltweit zu schwächen, um informationstechnische Systeme von Zielpersonen infiltrieren zu können. Die kalkulierte IT-Unsicherheit erscheint insbesondere vor dem Hintergrund der jüngsten Cyber-Angriffe mithilfe des globalen Erpressungstrojaners "WannaCry" und damit einhergehenden Aufforderungen staatlicher Sicherheitsbehörden an Verbraucherinnen und Verbraucher sowie Unternehmen, die IT-Systeme besser zu sichern, zumindest widersprüchlich. So kann die Installation von Überwachungssoftware seitens staatlicher Stellen dazu führen, dass Dritte in das System mittels Nachladefunktion eindringen können, indem sie eine unzureichende Authentifizierung und Verschlüsselung ausnutzen. Je öfter die Schwachstelle ausgenutzt wird, desto eher können auch Kriminelle und andere Interessengruppen solche Lücken missbrauchen.

Künftig sollen Rechner und Smartphones überwacht, deren Mikrofone aktiviert und deren Speicher ausgelesen werden können. Dies bedeutet eine völlig neue Schwere des Grundrechtseingriffs und beinhaltet erhebliche datenschutzrechtliche Risiken.

Das neue Gesetz ermöglicht die Quellen-Telekommunikationsüberwachung und die Online-Durchsuchung zu Strafverfolgungszwecken nicht nur im Fall von schweren Straftaten, sondern etwa auch bei Steuerdelikten, Computerbetrug, Hehlerei, Geld- und Wertzeichenfälschung oder der Verleitung zur missbräuchlichen Asylantragstellung. Dies kann langfristig zu einer ausufernden Anwendung der Online-Überwachung im Verhältnis zum geltenden Rechtszustand führen. Darüber hinaus erlaubt das vorliegende Gesetz den Behörden, gespeicherte Daten auszulesen, auch wenn diese Gegenstand früherer Kommunikation waren. Dies betrifft konkret die über Messenger-Dienste versandten Nachrichten. Die Quellen-Telekommunikationsüberwachung könnte dadurch zu einer Online-Durchsuchung werden.

Bundesrat Drucksache **527/17** (Beschluss)

07.07.17

Beschluss
des Bundesrates

Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens

Der Bundesrat hat in seiner 959. Sitzung am 7. Juli 2017 beschlossen, zu dem vom Deutschen Bundestag am 22. Juni 2017 verabschiedeten Gesetz einen Antrag gemäß Artikel 77 Absatz 2 des Grundgesetzes nicht zu stellen.

Bundesgesetzblatt 3201

Teil I **G 5702**

2017 **Ausgegeben zu Bonn am 23. August 2017** **Nr. 58**

3202 Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 58, ausgegeben zu Bonn am 23. August 2017

Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens

Vom 17. August 2017

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Änderung des Strafgesetzbuches

Das Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 1 des Gesetzes vom 17. Juli 2017 (BGBl. I S. 2442) geändert worden ist, wird wie folgt geändert:

1. § 44 wird wie folgt geändert:
   a) Absatz 1 wird wie folgt geändert:
      aa) In Satz 1 werden nach dem Wort „Straftat“ das Komma und die Wörter „die er bei oder im Zusammenhang mit dem Führen eines Kraftfahrzeugs oder unter Verletzung der Pflichten eines Kraftfahrzeugführers begangen hat,“ gestrichen und wird das Wort „drei“ durch das Wort „sechs“ ersetzt.
      bb) Nach Satz 1 wird folgender Satz eingefügt:
      „Auch wenn die Straftat nicht bei oder im Zusammenhang mit dem Führen eines Kraftfahrzeugs oder unter Verletzung der Pflichten eines Kraftfahrzeugführers begangen wurde, kommt die Anordnung eines Fahrverbots namentlich in Betracht, wenn sie zur Einwirkung auf den Täter oder zur Verteidigung der Rechtsordnung erforderlich erscheint oder hierdurch die Verhängung einer Freiheitsstrafe oder deren Vollstreckung vermieden werden kann.“
   b) Absatz 2 Satz 1 wird wie folgt gefasst:
   „Das Fahrverbot wird wirksam, wenn der Führerschein nach Rechtskraft des Urteils in amtliche Verwahrung gelangt, spätestens jedoch mit Ablauf von einem Monat seit Eintritt der Rechtskraft.“
   c) Folgender Absatz 4 wird angefügt:
   „(4) Werden gegen den Täter mehrere Fahrverbote rechtskräftig verhängt, so sind die Verbotsfristen nacheinander zu berechnen. Die Verbotsfrist auf Grund des früher wirksam gewordenen Fahrverbots läuft zuerst. Werden Fahrverbote gleichzeitig wirksam, so läuft die Verbotsfrist auf Grund des früher angeordneten Fahrverbots zuerst, bei gleichzeitiger Anordnung ist die frühere Tat maßgebend.“
2. In § 129 Absatz 4 wird die Angabe „100c“ durch die Angabe „100b“ ersetzt.
3. § 266a Absatz 4 Satz 2 wird wie folgt geändert:
   a) In Nummer 2 wird das Wort „oder“ am Ende durch ein Komma ersetzt.
   b) Nach Nummer 2 werden die folgenden Nummern 3 und 4 eingefügt:
      „3. fortgesetzt Beiträge vorenthält und sich zur Verschleierung der tatsächlichen Beschäftigungsverhältnisse unrichtige, nachgemachte oder verfälschte Belege von einem Dritten verschafft, der diese gewerbsmäßig anbietet,
      4. als Mitglied einer Bande handelt, die sich zum fortgesetzten Vorenthalten von Beiträgen zusammengeschlossen hat und die zur Verschleierung der tatsächlichen Beschäftigungsverhältnisse unrichtige, nachgemachte oder verfälschte Belege vorhält, oder“.
   c) Die bisherige Nummer 3 wird Nummer 5.

Artikel 2

Änderung des Jugendgerichtsgesetzes

Das Jugendgerichtsgesetz in der Fassung der Bekanntmachung vom 11. Dezember 1974 (BGBl. I S. 3427), das zuletzt durch Artikel 6 Absatz 28 des Gesetzes vom 13. April 2017 (BGBl. I S. 872) geändert worden ist, wird wie folgt geändert:

1. Dem § 8 Absatz 3 wird folgender Satz angefügt:
   „Ein Fahrverbot darf die Dauer von drei Monaten nicht überschreiten.“
2. In § 89a Absatz 1 Satz 5 wird die Angabe „§ 454b Abs. 3“ durch die Angabe „§ 454b Absatz 4“ ersetzt.

Artikel 3

Änderung der Strafprozessordnung

Die Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 11 Absatz 17 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) 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. § 26 Absatz 1 Satz 2 wird wie folgt gefasst:

„Das Gericht kann dem Antragsteller aufgeben, ein in der Hauptverhandlung angebrachtes Ablehnungsgesuch innerhalb einer angemessenen Frist schriftlich zu begründen.“

3. In § 26a Absatz 1 Nummer 2 werden nach dem Wort „nicht“ die Wörter „oder nicht innerhalb der nach § 26 Absatz 1 Satz 2 bestimmten Frist“ eingefügt.

4. § 29 wird wie folgt geändert:

a) Dem Absatz 1 wird folgender Satz angefügt:

„Wird ein Richter vor Beginn der Hauptverhandlung abgelehnt und würde eine Entscheidung über die Ablehnung den Beginn der Hauptverhandlung verzögern, kann diese vor der Entscheidung über die Ablehnung durchgeführt werden, bis der Staatsanwalt den Anklagesatz verlesen hat.“

b) Folgender Absatz 3 wird angefügt:

„(3) Hat das Gericht dem Antragsteller gemäß § 26 Absatz 1 Satz 2 aufgegeben, das Ablehnungsgesuch innerhalb einer bestimmten Frist schriftlich zu begründen, gilt Absatz 2 mit der Maßgabe entsprechend, dass über die Ablehnung spätestens bis zum Beginn des übernächsten Verhandlungstages nach Eingang der schriftlichen Begründung und stets vor Beginn der Schlussanträge zu entscheiden ist.“

5. Dem § 81a Absatz 2 wird folgender Satz angefügt:

„Die Entnahme einer Blutprobe bedarf abweichend von Satz 1 keiner richterlichen Anordnung, wenn bestimmte Tatsachen den Verdacht begründen, dass eine Straftat nach § 315a Absatz 1 Nummer 1, Absatz 2 und 3, § 315c Absatz 1 Nummer 1 Buchstabe a, Absatz 2 und 3 oder § 316 des Strafgesetzbuchs begangen worden ist.“

6. § 81e wird wie folgt geändert:

a) Absatz 1 wird wie folgt gefasst:

„(1) An dem durch Maßnahmen nach § 81a Absatz 1 oder § 81c erlangten Material dürfen mittels molekulargenetischer Untersuchung das DNA-Identifizierungsmuster, die Abstammung und das Geschlecht der Person festgestellt und diese Feststellungen mit Vergleichsmaterial abgeglichen werden, soweit dies zur Erforschung des Sachverhalts erforderlich ist. Andere Feststellungen dürfen nicht erfolgen; hierauf gerichtete Untersuchungen sind unzulässig.“

b) Absatz 2 wird wie folgt geändert:

aa) In Satz 1 wird das Wort „Spurenmaterial“ durch das Wort „Material“ ersetzt.

bb) In Satz 2 werden die Wörter „Absatz 1 Satz 3“ durch die Wörter „Absatz 1 Satz 2“ ersetzt.

cc) Folgender Satz wird angefügt:

„Ist bekannt, von welcher Person das Material stammt, gilt § 81f Absatz 1 entsprechend.“

7. § 81h wird wie folgt geändert:

a) In Absatz 1 werden in dem Satzteil nach Nummer 3 nach den Wörtern „ob das Spurenmaterial von diesen Personen“ die Wörter „oder von ihren Verwandten in gerader Linie oder in der Seitenlinie bis zum dritten Grad“ eingefügt.

b) Absatz 3 wird wie folgt gefasst:

„(3) Für die Durchführung der Maßnahme gilt § 81f Absatz 2 entsprechend. Die entnommenen Körperzellen sind unverzüglich zu vernichten, sobald sie für die Untersuchung nach Absatz 1 nicht mehr benötigt werden. Soweit die Aufzeichnungen über die durch die Maßnahme festgestellten DNA-Identifizierungsmuster zur Erforschung des Sachverhalts nicht mehr erforderlich sind, sind sie unverzüglich zu löschen. Die Vernichtung und die Löschung sind zu dokumentieren.“

c) Absatz 4 Satz 2 wird wie folgt gefasst:

„Vor Erteilung der Einwilligung sind sie schriftlich auch darauf hinzuweisen, dass

1. die entnommenen Körperzellen ausschließlich zur Feststellung des DNA-Identifizierungsmusters, der Abstammung und des Geschlechts untersucht werden und dass sie unverzüglich vernichtet werden, sobald sie hierfür nicht mehr erforderlich sind,
2. das Untersuchungsergebnis mit den DNA-Identifizierungsmustern von Spurenmaterial automatisiert daraufhin abgeglichen wird, ob das Spurenmaterial von ihnen oder von ihren Verwandten in gerader Linie oder in der Seitenlinie bis zum dritten Grad stammt,
3. das Ergebnis des Abgleichs zu Lasten der betroffenen Person oder mit ihr in gerader Linie oder in der Seitenlinie bis zum dritten Grad verwandter Personen verwertet werden darf und
4. die festgestellten DNA-Identifizierungsmuster nicht zur Identitätsfeststellung in künftigen Strafverfahren beim Bundeskriminalamt gespeichert werden.“

8. § 100a wird wie folgt geändert:

a) Dem Absatz 1 werden die folgenden 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 insbeson-

dere 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."

9. § 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 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 zwei-

ter 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.“

10. § 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 wird die Angabe „§ 100d Abs. 2“ durch die Angabe „§ 100e Absatz 3“ ersetzt.

d) Die Absätze 4 bis 7 werden aufgehoben.

11. 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 zweiter Halbsatz, 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 könnten, oder zur Ermittlung des Aufenthalts der einer solchen Straftat beschuldigten Person verwendet werden."

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

13. 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.

14. § 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.

15. § 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" ersetzt.

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.

16. § 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.

Seite 8 – 48 fehlen.