Entwurf:

Erläuterungen:

I. Allgemeiner Teil

Der vorliegende Antrag beinhaltet folgende Schwerpunkte:

1.) Überarbeitung und Ergänzung des 5. Abschnitts des 8. Hauptstückes der StPO („Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Lokalisierung einer technischen Einrichtung, Überwachung von Nachrichten, verschlüsselter Nachrichten und von Personen“) sowie des § 76a Abs. 1 StPO. Diese beruhen zu wesentlichen Teilen auf den Ergebnissen einer von Herrn Bundesminister Univ. Prof. Dr. Wolfgang Brandstetter u.a. zur Thematik der Überwachung internetbasierter Kommunikation eingesetzten Expertengruppe und Bedürfnissen der Strafverfolgungsbehörden und dienen auch einer teilweisen Umsetzung des Arbeitsprogramms der Bundesregierung 2017/2018. Dies betrifft insbesondere:

a) Angleichung der verfahrensrechtlichen Voraussetzungen der Auskunft über den PUK-Code an die Auskunft über Stammdaten;
b) Schaffung einer ausdrücklichen gesetzlichen Regelung für die seit Jahren eingesetzte Ermittlungsmaßnahme der Lokalisierung einer technischen Einrichtung ohne Mitwirkung eines Betreibers (sog. IMSI-Catcher);
c) Schaffung einer eigenständigen und aussagekräftigen Definition der Überwachung von Nachrichten unter weitgehender Lösung von Begrifflichkeiten des TKG;
d) Neuregelung der verfahrensrechtlichen Bestimmungen zur Beschlagnahme von Briefen unter Anpassung an jene der Überwachung der Telekommunikation;
e) Einführung einer neuen Ermittlungsmaßnahme zur Überwachung verschlüsselter Nachrichten unter Berücksichtigung der Beratungen einer Expertengruppe zur Überwachung internetbasierter Kommunikation;
f) Einführung einer neuen Ermittlungsmaßnahme der akustischen Überwachung von Personen in Fahrzeugen;

2.) Die Umsetzung der Richtlinie 2016/343/EU über die Stärkung bestimmter Aspekte der Unschuldsvermutung und des Rechts auf Anwesenheit in der Verhandlung im Strafverfahren, ABl. Nr. L 65 vom 11.03.2016 S 1 (im Folgenden: RL Unschuldsvermutung).

Ad 1.)

a) Um zu verhindern, dass den Anbietern von Kommunikationsdiensten bei der Erteilung des Auftrags zur Bekanntgabe der vom Anbieter vergebenen Nummer, die dem Teilnehmer die Überwindung der Sperre der persönliche Identifikationsnummer des Benutzers ermöglicht (PUK-Code) auch weiterhin die Verdachtslage offengelegt werden muss, obwohl bei den eingriffsintensiveren Ermittlungsmaßnahmen der Mitwirkung an der Überwachung von Nachrichten und der Erteilung von Auskünften über Daten einer Nachrichtenübermittlung eine Bezugnahme auf die gerichtliche Bewilligung der Maßnahme ausreichend ist (§ 138 Abs. 3 StPO), wird vorgeschlagen, die Ermittlung des PUK-Codes aus datenschutzrechtlichen und rechtssystematischen Erwägungen in § 76a Abs. 1 StPO aufzunehmen.

b) In Angleichung an die Regelungen im Sicherheitspolizeigesetz (SPG) wird vorgeschlagen, eine eigene Rechtsgrundlage für die seit Jahren erfolgreich eingesetzte und in der Praxis unumgängliche Lokalisierung einer technischen Einrichtung durch die Kriminalpolizei mittels des sog. IMSI-Catchers (IMSI=die zur internationalen Kennung des Benutzers dienende Nummer) vorzusehen.

c) und e) Die im Rahmen des Begutachtungsverfahrens zur Einführung der Ermittlungsmaßnahme der „Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden“ mit dem Ministerialentwurf betreffend ein Bundesgesetz, mit dem die Strafprozessordnung und das Staatsanwaltschaftsgesetz geändert werden (192/ME XXV. GP), geäußerten Bedenken und aufgeworfenen Fragestellungen machten eine weitere Auseinandersetzung mit der Thematik notwendig. Herr Bundesminister Univ. Prof. Dr. Wolfgang Brandstetter berief zu diesem Zweck eine hochrangige Expertengruppe ein, die sich unter anderem mit der Überwachung internetbasierter Kommunikation befasste und deren Ergebnisse dem vorliegenden Entwurf zugrunde gelegt wurden.

Im Zuge der Beratungen der Expertengruppe wurde anerkannt, dass die Technologieneutralität der Strafprozessordnung einen wesentlichen Vorteil darstellt und soweit tunlich durch die Schaffung eigenständiger Definitionen unter weitgehender Loslösung von Bezugnahmen auf das Telekommunikationsgesetz 2003 (TKG 2003) dauerhaft gewährleistet werden soll. Im Sinne der Diskussionen in der Expertengruppe soll daher die Definition der „Überwachung von Nachrichten“ in § 134 Z 3 StPO durch die Loslösung von § 92 Abs. 3 Z 7 TKG und die Schaffung einer eigenen Begriffsbestimmung klarer und transparenter formuliert und unmissverständlich klargestellt werden, dass von dieser Ermittlungsmaßnahme nicht nur zwischenmenschlicher Gedankenaustausch erfasst wird.

Mit der Einführung einer neuen Ermittlungsmaßnahme zur Überwachung verschlüsselter Nachrichten, die aufgrund der geltenden Rechtslage grundsätzlich nach den Bestimmungen der Überwachung von Nachrichten zulässig ist, aber aufgrund der Verschlüsselung ins Leere läuft, soll den Strafverfolgungsbehörden ein dringend notwendiges, effektives Instrument zur Aufklärung und Verfolgung von Straftaten zur Verfügung gestellt werden. Dadurch soll eine Lücke in der Strafverfolgung geschlossen werden, sodass es Beschuldigten künftig nicht mehr möglich sein soll, durch die Wahl verschlüsselter Telekommunikation (z. B. Skype und WhatsApp) jegliche Überwachung zu verhindern.

Mit der vorgeschlagenen Ermittlungsmaßnahme der Überwachung verschlüsselter Nachrichten soll ausdrücklich auf einen **Übertragungsvorgang** abgestellt werden, sodass sie systemkonform in die StPO eingebunden werden kann und sich zweifelsfrei von einer Online-Durchsuchung abgrenzt. Die vorgeschlagene Ermittlungsmaßnahme ist der herkömmlichen Überwachung von Nachrichten nach §§ 134 Z 3, 135 Abs. 3 StPO nachgebildet und unterscheidet sich von dieser nur dahingehend, dass bei der Überwachung von Nachrichten unverschlüsselte, mit der neuen Ermittlungsmaßnahme hingegen verschlüsselte Nachrichten überwacht werden sollen. Damit soll ausdrücklich klargestellt werden, dass Straftäter durch die Wahl des technischen Kommunikationsmittels keinen wie immer gearteten Vor- oder Nachteil erlangen und die Strafverfolgungsbehörden unabhängig von der Wahl des technischen Kommunikationsmittels technologieunabhängig und effizient reagieren können. Dieser Umstand erlangt umso mehr Bedeutung, als verschlüsselte Kommunikation herkömmliche Telefonie oder SMS zunehmend verdrängt und die Strafverfolgung aufgrund dieser technologischen Entwicklung zunehmend erschwert und behindert wird. Die Überwachung verschlüsselter Nachrichten soll durch (remote oder physikalische) Installation eines Programms in dem zu überwachenden Computersystem erfolgen, welches **ausschließlich gesendete, übermittelte, oder empfangene Nachrichten und Informationen entweder vor der Verschlüsselung oder nach Entschlüsselung** an die Strafverfolgungsbehörden ausleitet.

Da die Durchführung einer solchen Ermittlungsmaßnahme nach dem derzeitigen Stand der Technik quantitativ und qualitativ sehr ressourcenintensiv ist, wird einerseits vorgeschlagen, eine Legisvakanz bis 1. August 2019 vorzusehen, damit dem Bundesministerium für Inneres ausreichend Zeit zur Beschaffung der erforderlichen Software und Treffen der erforderlichen technischen und personellen Vorkehrungen zur Durchführung der vorgeschlagenen neuen Ermittlungsmaßnahme zur Verfügung steht. Andererseits soll die Ermittlungsmaßnahme vorerst an höhere Schranken als für die Überwachung von Nachrichten nach § 135 Abs. 3 StPO gebunden werden. Überdies soll die Ermittlungsmaßnahme vorerst nur für einen befristeten Zeitraum von fünf Jahren in Kraft gesetzt sowie rechtzeitig vor Ende der Befristung (auch im Hinblick auf einen voraussichtlich erfolgten technischen Fortschritt) einer Evaluierung unterzogen werden, wobei auch die Zulässigkeitsvoraussetzungen neu zu überdenken sein werden.

d) Durch den Entfall der Voraussetzung, dass sich der Beschuldigte wegen einer vorsätzlichen, mit mehr als einjähriger Freiheitsstrafe bedrohten Tat in Haft befindet oder eine Vorführung oder Festnahme deswegen angeordnet wurde, soll den Strafverfolgungsbehörden die den Zollorganen bereits zur Verfügung stehende rechtliche Handhabe zur Beschlagnahme von Briefen und Paketen unbekannter Täter oder auf freiem Fuß befindlicher Beschuldigter eingeräumt und damit insbesondere der zunehmende Versand von Briefen mit im sog. Darknet angebotenen Suchtmitteln effektiv bekämpft werden.

f) Da eine (bloß) akustische Überwachung in Fahrzeugen derzeit nur unter den restriktiven Zulässigkeitsvoraussetzungen für eine optische und akustische Überwachung von Personen nach § 136

Abs. 1 StPO zulässig ist, wird vorgeschlagen, für diese spezielle Konstellation einen eigenen Eingriffstatbestand zu schaffen und die Zulässigkeitsvoraussetzungen aufgrund der vergleichbaren Eingriffsintensität an jene der Überwachung von Nachrichten nach § 135 Abs. 3 StPO anzuknüpfen.

Ad. 2.) In Umsetzung der RL Unschuldsvermutung soll die bis zum 31.12.2007 in der StPO vorgesehene und in der Praxis nach wie vor erfolgende Belehrung eines Angeklagten über die Folgen des Nichterscheinens zur Hauptverhandlung ausdrücklich Eingang in den Gesetzestext finden.

II. Besonderer Teil

Aus Gründen der Übersichtlichkeit sollen vorerst die vorgeschlagenen Änderungen im 5. Abschnitt des 8. Hauptstückes der StPO – gegliedert nach den jeweiligen Ermittlungsmaßnahmen – und im Folgenden die weiteren Änderungen in der StPO dargestellt werden.

Vorbemerkung zu Z 1, 2, 4, 7 bis 35 und 38 (Inhaltsverzeichnis und Überschrift des 5. Abschnittes des 8. Hauptstückes der StPO, Überschrift von § 135 StPO, §§ 76a Abs. 1, 134 Z 2a, 3, 3a und 5, 135 Abs. 1, 2a und Abs. 3 Z 3, 135a, 136 Abs. 1 Z 3 und Abs. 1a, 137 Abs. 1, 2 und 3, 138 Abs. 1, 2, 3 und 5, 140 Abs. 1 Z 2 und 4, 144 Abs. 3, 145 Abs. 3 und 4, 147 Abs. 1 Z 2a, 3 und 5, Abs. 2 und 3a, 148 und § 381 Abs. 1 Z 5 StPO):

Mit den vorgeschlagenen Änderungen erfolgt eine Überarbeitung und Ergänzung des 5. Abschnitts des 8. Hauptstückes („Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Lokalisierung einer technischen Einrichtung, Überwachung von Nachrichten, verschlüsselter Nachrichten und von Personen“) sowie des § 76a Abs. 1 StPO. Diese beruhen zu wesentlichen Teilen auf den Ergebnissen einer von Herrn Bundesminister Univ.-Prof. Dr. Wolfgang Brandstetter u.a. zur Thematik der Überwachung internetbasierter Kommunikation eingesetzten Expertengruppe und Bedürfnissen der Strafverfolgungsbehörden und dienen auch einer teilweisen Umsetzung des Arbeitsprogramms der Bundesregierung 2017/2018.

Der Systematik der StPO folgend, sollen sämtliche im Entwurf erfassten Ermittlungsmaßnahmen (wie bisher) den Verdacht der Begehung einer Straftat erfordern, wobei die gesetzlichen Grundlagen je nach Ermittlungsmaßnahme zusätzliche Erfordernisse (dringender Tatverdacht, besondere Schwere der Tat) vorsehen. Das Verhältnismäßigkeitsprinzip ist im Einzelfall zu wahren. Darüber sollen die Rechtsschutzmöglichkeiten, Verwertungs- bzw. Verwendungsverbote und Löschungsverpflichtungen entsprechend angepasst bzw. erweitert werden.

Zu Z 1, 2, 7, 12, 38 (Inhaltsverzeichnis und Überschrift des 5. Abschnittes des 8. Hauptstückes der StPO, Überschrift von § 135 StPO und § 381 Abs. 1 Z 5 StPO):

Die vorgeschlagenen Änderungen umfassen Anpassungen an die Begriffe der neuen Ermittlungsmaßnahmen der Überwachung verschlüsselter Nachrichten und teilweise auch der Lokalisierung einer technischen Einrichtung (s. dazu unten) sowie den Entfall der Bezugnahme auf die Vorratsspeicherung von Daten, die mit Erkenntnis des VfGH vom 27. Juni 2014 (Kundmachung in BGBl. I Nr. 44/2014) aufgehoben worden ist. Bei dieser Gelegenheit wird auch die Regelung in § 381 Abs. 1 Z 5 StPO über den Kostenersatz einer Auskunft über Vorratsdaten bereinigt.

Auskunft über den PUK-Code:

Zu Z 4 (§ 76a Abs. 1 StPO):

Da der PUK-Code (das ist die vom Anbieter vergebene Nummer, die dem Teilnehmer die Überwindung der Sperre der persönliche Identifikationsnummer des Benutzers ermöglicht) definitionsgemäß weder in die Kategorie der Stamm-, Verkehrs-, Zugangs- oder Standortdaten fällt, wurde bisher vertreten, dass zu dessen Erlangung mit Sicherstellung gemäß § 110 StPO vorzugehen ist (*Reindl Krauskopf; Tipold/Zerbes* in *Fuchs/Ratz*, WK StPO § 134 StPO Rz 38). Dieses Vorgehen birgt allerdings erhebliche datenschutzrechtliche Nachteile, weil dem Anbieter von Kommunikationsdiensten mit der begründungspflichtigen Anordnung einer Sicherstellung (im Gegensatz zu den eingriffsintensiveren Ermittlungsmaßnahmen der Mitwirkung an der Überwachung von Nachrichten und der Erteilung von Auskünften über Daten einer Nachrichtenübermittlung, bei denen eine Bezugnahme auf die gerichtliche Bewilligung der Maßnahme ausreichend ist; vgl. § 138 Abs. 3 StPO) auch die gesamte Verdachts- und Beweislage zur Kenntnis gebracht werden muss.

Mit der vorgeschlagenen Änderung sollen Anbieter von Kommunikationsdiensten den PUK-Code („Personal Unlocking Key“, vgl. Definition und vorgesehener Kostenersatz in § 2 Z 7, § 10 ÜKVO) aufgrund der sachlichen Nähe und vergleichbaren Eingriffsintensität unter den Voraussetzungen der Auskunft über Stammdaten eines Teilnehmers (§ 76a Abs. 1 StPO) bekannt geben müssen. Vergleichbar mit Stammdaten braucht es auch bei der Ermittlung des PUK-Codes keines Rückgriffes auf (von § 76a

Abs. 2 StPO erfasste) Verkehrsdaten, d.h. es genügt zur Kenntnisnahme der Daten ein Blick in die Vertragsunterlagen (vgl. *Nimmervoll*, Das Strafverfahren, 228 mwN).

Lokalisierung einer technischen Einrichtung:

Zu Z 8, 11, 14 und 25 bis 28 (§§ 134 Z 2a und 5, 135 Abs. 2a, 140 Abs. 1 Z 2 und 4, 144 Abs. 3 und 145 Abs. 3 StPO):

Mit dieser Bestimmung soll eine klare und eigenständige Rechtsgrundlage für die Lokalisierung einer technischen Einrichtung durch Einsatz technischer Mittel zur Feststellung von geografischen Standorten und IMSI-Nummern (International Mobile Subscriber Identification, vgl. § 2 Z 5 ÜKVO) ohne Mitwirkung eines Anbieters (§ 92 Abs. 3 Z 1 TKG) oder sonstigen Diensteanbieters (§§ 13, 16 und 18 Abs. 2 des E – Commerce – Gesetzes, BGBl. I Nr. 152/2001) geschaffen werden, die den für die Strafverfolgungspraxis unabdingbaren Einsatz eines IMSI-Catchers, der eine präzise Ortung innerhalb einer Funkzelle erlaubt und keine Mitwirkung von Anbietern oder sonstigen Diensteanbietern erfordert, regelt (zur Funktionsweise des Funkzellennetzes siehe OGH vom 5.3.2015, 12 Os 93/13i, 12 Os 94/14m). Tatsächlich wird diese Ermittlungsmaßnahme seit Jahren erfolgreich eingesetzt und von der Rsp. als Auskunft über Daten einer Nachrichtenübermittlung nach §§ 134 Z 2, 135 Abs. 2 StPO (zuletzt OLG Wien vom 3.2.2017, 20 Bs 4/17k) qualifiziert.

Im Bereich des Sicherheitspolizeigesetzes (SPG) ist der Einsatz technischer Mittel zur Lokalisierung einer Endeinrichtung im Rahmen der Gefahrenabwehr bereits in § 53 Abs. 3b SPG eigenständig geregelt. Diese Maßnahme erfordert keine richterliche Bewilligung, sondern kann von den Sicherheitsbehörden zur Hilfeleistung oder Abwehr einer gegenwärtigen Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen vorgenommen werden.

Um die Technologieneutralität der StPO weiterhin zu gewährleisten und dem Rechtsanwender kompakt Klarheit über die Reichweite der Ermittlungsbefugnisse zu vermitteln sowie häufige Anpassungen an technische Entwicklungen oder Änderungen im TKG zu vermeiden, soll in Entsprechung dieser Regelung im Sicherheitspolizeigesetz (SPG) nunmehr eine ausdrückliche gesetzliche, von den Bestimmungen des TKG unabhängige (daher „Feststellung von geografischen Standorten“) Definition und Regelung in der StPO für die Lokalisierung einer technischen Einrichtung durch die Kriminalpolizei mittels des sog. IMSI-Catchers geschaffen werden.

Damit korrespondierend sollen auch entsprechende Schutzbestimmungen in **§ 140 Abs. 1 StPO** (Verwendungsverbote) vorgesehen werden. Demnach sollen Ergebnisse bei sonstiger Nichtigkeit nur als Beweismittel verwendet werden können, wenn die Ermittlungsanordnung auch rechtmäßig angeordnet und bewilligt wurde (§ 140 Abs. 1 **Z 2** StPO) und auch nur zum Nachweis einer vorsätzlich begangenen strafbaren Handlung, derentwegen die Ermittlungsmaßnahme angeordnet wurde oder hätte angeordnet werden können (§ 140 Abs. 1 **Z 4** StPO). Darüber hinaus ist diese Ermittlungsmaßnahme auch von **§§ 144 Abs. 3, 145 Abs. 3 StPO** umfasst.

Überwachung von Nachrichten:

Zu Z 9 (§ 134 Z 3 StPO):

Die Definition von „Überwachung von Nachrichten“ in § 134 Z 3 StPO soll von den Begrifflichkeiten des TKG (§ 92 Abs. 3 Z 7 TKG) gelöst und durch Schaffung einer eigenständigen Begriffsbestimmung in der StPO klarer und transparenter formuliert werden. Da die Stellungnahmen im Begutachtungsverfahren zum Ministerialentwurf betreffend ein Bundesgesetz, mit dem die Strafprozessordnung und das Staatsanwaltschaftsgesetz geändert werden (192/ME XXV. GP), bemerkenswerte Auffassungsunterschiede bezüglich der Bedeutung und Reichweite der Ermittlungsmaßnahme der Überwachung von Nachrichten gemäß §§ 134 Z 3, 135 Abs. 3 StPO aufgezeigt haben, sollen Auslegungsspielräume und folglich Auffassungsunterschiede in Bezug auf den Nachrichtenbegriff im Allgemeinen vermieden werden.

So wurden in den Stellungnahmen mitunter mit dem Begriff der Nachricht insbesondere unterschiedliche Bedeutungsinhalte assoziiert, die davon abhängen, ob ihm ein soziales oder technisches Verständnis zugrunde gelegt wird. Klarstellend ist auszuführen, dass Nachrichten iSd § 92 Abs. 3 Z 7 TKG bereits in der geltenden Fassung des § 135 Abs. 3 StPO weder einen menschlichen Denkvorgang voraussetzen, noch durch eine menschliche Tätigkeit übertragen werden müssen (*Zanger/Schöll*, Kommentar zum TKG 2003 (2004), § 92 Rz 32) und auch beim Senden und Empfangen von Datenstreams Nachrichten ausgetauscht werden (vgl. *Riesz/Schilchegger*, TKG (2016) § 107 Rz 36); außerdem fallen nach *Zanger/Schöll*, Kommentar zum TKG 2003 (2004), § 92 Rz 32, auch Messwerte, sowie Regelungs- Steuerungs- und Alarmimpulse darunter, z. B. Inhalte von Homepages, Beiträge in Newsgroups, Informationen über Bestellvorgänge Aufrufstatistiken von Webseiten, die es ermöglichen, ein Benutzerprofil zu erstellen (vgl. hingegen zum Terminus „Nachricht“ im StGB *Lewisch* in *Höpfel/Ratz*,

WK^2 StGB § 119 Rz 9a). Aufgrund der technologieneutralen Formulierung der StPO ist daher schon bislang nicht nur zwischenmenschlicher Gedankenaustausch, sondern ebenso eine Ausleitung des Internetdatenverkehrs zulässig. Auf diese Rechtsansicht hat bereits die interministerielle Arbeitsgruppe zur „Online-Durchsuchung“ in ihrem Schlussbericht aus 2008 Bezug genommen und ausgeführt, dass die Internetüberwachung nach geltendem Recht zulässig ist, unter § 135 StPO fällt und sich von der Online-Durchsuchung unterscheidet (vgl. Schlussbericht S 38, 46).

Argumente, wonach der Aufruf von Websites einen tieferen Eingriff in Grundrechte als die Überwachung zwischenmenschlichen Gedankenaustauschs (über Telefon, SMS oder E-Mail) darstelle, hat zuletzt das deutsche Bundesverfassungsgericht in seiner Entscheidung vom 6. Juli 2016, 2 BVR 1454/13, ausdrücklich verworfen. Das Bundesverfassungsgericht hielt explizit fest, dass das allenfalls damit verbundene quantitative Mehr an überwachter Kommunikation im Vergleich zur Telefonüberwachung regelmäßig dadurch aufgewogen wird, dass lediglich Einzelakte einer oft nur kurzen und oberflächlichen Telekommunikation zur Kenntnis genommen werden und bei der Internetnutzung Akte der höchstvertraulichen Kommunikation nur einen kleinen Teil darstellen, der bei der Überwachung miterfasst zu werden droht, der aber nicht – wie die Überwachung des Rückzugsbereichs der Wohnung – typusprägend ist, sodass die Internetüberwachung sogar weit weniger eingriffsintensiv als eine Hausdurchsuchung ist. Eine (u.a. vom BVerfG geforderte) strenge Prüfung der Verhältnismäßigkeit und Erforderlichkeit der Maßnahme im Einzelfall sowie Dokumentationspflichten und Verwertungsverbote sind in der StPO ohnedies vorgesehen (s. insbes. §§ 101 f., 138 ff.).

Basierend auf den einvernehmlichen Ergebnissen der von Herrn Bundesminister Univ.-Prof. Dr. Wolfgang Brandstetter eingesetzten Expertengruppe zur Überwachung internetbasierter Kommunikation (s. dazu bei § 135a StPO) soll daher ausdrücklich klargestellt werden, dass die vorgeschlagene Formulierung der „Überwachung von Nachrichten“ gemäß § 134 Z 3 StPO weiterhin ausdrücklich nicht nur menschliche Gedankeninhalte (herkömmliche Telefonie, SMS, MMS, Sprachnachrichten, Videonachrichten, E-Mails, etc.), sondern ebenso über ein Kommunikationsnetz (§ 3 Z 11 TKG) oder einen Dienst der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes) gesendete, übermittelte oder empfangene Informationen umfasst, d.h. auch Kommunikation im technischen Sinn, wie z. B. den Aufruf von Websites, Surfen im Internet und unverschlüsselte Übertragungsvorgänge in eine Cloud.

Durch Streichung des Verweises auf § 92 Abs. 3 Z 7 TKG sowie Aufnahme des Begriffes der „Informationen“ und sprachliche Anlehnung an die entsprechende Regelung im deutschen Recht soll dies für die Rechtsanwender klarer und transparenter formuliert und insbesondere ausdrücklich klargestellt werden, dass eine Überwachung von Nachrichten nicht die in § 92 Abs. 3 Z 7 TKG genannte endliche Zahl von Beteiligten voraussetzt. Vielmehr ist die Ermittlungsmaßnahme auch bei unbestimmter oder unbestimmbarer Zahl von Beteiligten (seien es Menschen oder Computersysteme) zulässig. Anstelle des Austausches oder Weiterleitens (vgl. § 92 Abs. 3 Z 7 TKG) soll auf Senden, Übermitteln oder Empfangen abgestellt und damit alle Übertragungsvorgänge abgedeckt werden (vgl. § 3 Z 22 deutsches TKG, wonach „Telekommunikation“ der technische Vorgang des Aussendens, Übermittelns und Empfangen von Signalen mittels Telekommunikationsanlagen ist).

Überwachung verschlüsselter Nachrichten:

Zu Z 10, 11, 16, 25 und 26 (§§ 134 Z 3a und 5, 135a, 140 Abs. 1 Z 2 und 4 StPO):

Der im Frühjahr 2016 zur allgemeinen Begutachtung versandte Ministerialentwurf betreffend ein Bundesgesetz, mit dem die Strafprozessordnung und das Staatsanwaltschaftsgesetz geändert werden (192/ME XXV. GP), der den Vorschlag zur Einführung einer neuen Ermittlungsmaßnahme in Form der Anordnung der Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, enthielt (192/ME XXV. GP), baute auf den rechtlichen Überlegungen einer im Jahr 2007 eingesetzten interdisziplinären Arbeitsgruppe unter der Leitung von o. Univ. Prof. Dr. Bernd-Christian Funk und deren Schlussbericht aus März 2008 auf, die zur Klärung der technischen Voraussetzungen und der Möglichkeiten der Steuerung des Einsatzes der sogenannten „Online-Durchsuchung“ unter Berücksichtigung der Erfahrungen mit solchen Ermittlungsmaßnahmen in anderen Staaten samt der Klärung der rechtlichen Fragen unter besonderer Berücksichtigung datenschutzrechtlicher, rechtsvergleichender und europarechtlicher Aspekte ins Leben gerufen wurde. Im Gegensatz zu den damaligen Überlegungen beschränkte sich der Ministerialentwurf allerdings auf eine Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden.

Das Begutachtungsverfahren hat im Wesentlichen zwei Stoßrichtungen aufgezeigt: Auf der einen Seite wurde v.a. von besorgten Datenschutzinstitutionen, (Nichtregierungs-)Organisationen sowie mehreren Privatpersonen kritisiert, dass durch den als zu weitgehend empfundenen Begriff „sonstige Daten“ (trotz des Verweises auf § 74 Abs. 2 StGB) im Zusammenhang mit den Erläuterungen, wonach auch der Zugriff

auf lokal gespeicherte Kontakt- und Adressverzeichnisse sowie Daten in einer Cloud möglich sein solle, eine Unterscheidung zwischen der geplanten Maßnahme und einer Online-Durchsuchung nicht mehr zu erkennen sei, weshalb der Entwurf in gewissen Bereichen einer Online-Durchsuchung gleichkomme. Außerdem wurden Zweifel an der technischen Umsetzbarkeit gemeldet. Zahlreiche der eingelangten Stellungnahmen haben allerdings auch gezeigt, dass die Notwendigkeit sowie die Sinn- und Zweckmäßigkeit der Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, aufgrund des geänderten Kommunikationsverhaltens und der praktischen Bedeutung von Kommunikationsprogrammen wie WhatsApp, Skype, Telegram, etc. in der heutigen Zeit nicht mehr geleugnet werden kann. Insbesondere der Oberste Gerichtshof, die Generalprokuratur und die staatsanwaltschaftliche Praxis problematisierten, dass aufgrund der vorgeschlagenen strengen Zulässigkeitsvoraussetzungen (orientiert an der optischen und akustischen Überwachung) und des Ausschlusses der remote Installation keine – dem Gewicht der neuen Kommunikationskanäle entsprechende – praktische Bedeutung der geplanten Ermittlungsmaßnahme zu erwarten sei. Die Zulässigkeitsvoraussetzungen wurden als zu streng empfunden und in diesem Zusammenhang – wie im Übrigen auch von Teilen der Lehre – insbesondere die thematische Nähe zur Überwachung von Nachrichten nach § 135 StPO hervorgehoben. Der Oberste Gerichtshof hat in seiner Stellungnahme im Übrigen ausdrücklich festgehalten, dass der Entwurf keine Systemwidrigkeiten oder unverhältnismäßigen Eingriffe in Grundrechte erkennen lässt, sodass gegen ihn grundsätzlich keine Einwände bestehen.

Zur Klärung der aufgeworfenen Fragenstellungen hat Herr Bundesminister für Justiz Univ.-Prof. Dr. Wolfgang Brandstetter eine hochrangige Expertengruppe eingesetzt und sie mit der Erarbeitung von Vorschlägen für die Überarbeitung des vorliegenden Entwurfs unter Einbeziehung rechtsvergleichender Aspekte beauftragt. Dieser Expertengruppe unter Vorsitz von SC Mag. Christian Pilnacek (Sektion Strafrecht des Bundesministeriums für Justiz) gehörten über Einladung des Bundesministers für Justiz Prof. Dr. Gerhard Dannecker (Universität Heidelberg), Univ.-Prof. DDr. Peter Lewisch, Univ.-Prof. Dr. Susanne Reindl-Krauskopf (beide Universität Wien), Univ.-Prof. Mag. Dr. Alois Birklbauer (Johannes Kepler Universität Linz), Prof. Dr. Ingeborg Zerbes (Universität Bremen), SC Mag. Dr. Mathias Vogl (Bundesministerium für Inneres) und LStAin Mag[a]. Carmen Prior (Abteilung Strafverfahrensrecht des Bundesministeriums für Justiz) an. Die Ermöglichung der Überwachung internetbasierter Kommunikation wurde schließlich auch Teil des Arbeitsprogramms der Bundesregierung für 2017/2018.

Im Rahmen von insgesamt fünf Sitzungen von August 2016 bis Februar 2017 erörterte die Expertengruppe zunächst grundsätzliche Fragenstellungen, wobei **Einigkeit über die Notwendigkeit der Ermittlungsmaßnahme** der Überwachung verschlüsselter Kommunikation (z. B. Skype, WhatsApp) herrschte. Übereinstimmend wurde die Ansicht vertreten, dass es für die Effektivität der Strafverfolgung möglich sein muss, eine Ermittlungsmaßnahme einsetzen zu können, mit der auch verschlüsselte Kommunikation überwacht werden kann. Es liege kein Wertungsunterschied beim Eingriff in die Privatsphäre dahingehend vor, ob eine Nachricht überwacht werden soll, die ein Beschuldigter als SMS oder per WhatsApp oder Telegram übermittelt. Wachsendes Bewusstsein für datenschutzrechtliche Belange und Sensibilität im Umgang mit neuer Technologie führen dazu, dass vermehrt Anbieter von Kommunikationsprogrammen wie z. B. WhatsApp oder Telegram standardisiert end-to-end-Verschlüsselungen vorsehen, wofür das Modell der StPO, das auf der Ausleitung lesbarer Datenströme unter Mitwirkung von Anbieter und sonstiger Dienstanbieter aufbaut, keine praktikable Handhabe bietet (mangels „Schlüssel“, vgl. *Reindl-Krauskopf; Tipold/Zerbes* in *Fuchs/Ratz*, WK StPO § 134 StPO Rz 58/1). Während die StPO zwar technologieneutral formuliert ist und daher grundsätzlich auch verschlüsselte Nachrichten unter „Überwachung von Nachrichten“ subsumierbar sind, liegt derzeit eine offenkundige und eine die Effektivität der Strafverfolgung hindernde Gesetzeslücke vor, weil verschlüsselte Kommunikation von den Strafverfolgungsbehörden nicht überwacht werden kann. Dieses Problem von end-to-end-verschlüsselter Kommunikation kann allerdings über Installation einer Software direkt im zu überwachenden Computersystem und Ausleitung der Datenströme bei einer Nachrichtenübermittlung noch vor Verschlüsselung oder bereits nach Entschlüsselung gelöst werden, sodass aufgrund der unterschiedlichen Art der Überwachungsmethode im Sinne der Rechtsklarheit eine spezielle Rechtsgrundlage geschaffen werden soll (vgl. die Diskussion in Deutschland zur Quellen-TKÜ).

Darüber hinaus bestand in der Expertengruppe breite Übereinstimmung, dass die neue Ermittlungsmaßnahme – **von der Eingriffsintensität betrachtet – mit der Überwachung von Nachrichten gem. §§ 134 Z 3, 135 Abs. 3 StPO** (Überwachung herkömmlicher Telefonie, SMS, E-Mail-Verkehr) **vergleichbar** ist und daher unter den gleichen rechtlichen Voraussetzungen zulässig sein sollte. Da die Durchführung einer solchen Ermittlungsmaßnahme nach dem derzeitigen Stand der Technik allerdings quantitativ und qualitativ sehr ressourcenintensiv ist, sollte die Zulässigkeit für den Zeitraum einer befristeten Geltung an höhere Schranken gebunden werden. Nach einer Evaluierungsphase (und

einem voraussichtlich erfolgten technischen Fortschritt) sollten auch die Einsatzvoraussetzungen überdacht werden.

Auch eine Fokussierung auf die Überwachung der verschlüsselten Kommunikation und eine **klare Abgrenzung zur Online-Durchsuchung** (d.h. keine Online-Durchsuchung des kompletten Computersystems und lokal abgespeicherter, nicht mit einem Übertragungsvorgang im Zusammenhang stehender Dateien) mit dem Ziel der Überwindung der Transportverschlüsselung (end-to-end-Verschlüsselung), nicht jedoch auch der Offline-Verschlüsselung (Verschlüsselung von Dokumenten unabhängig von einer Übermittlung) wurde für sinnvoll erachtet. In diesem Sinn soll gesetzlich klar definiert werden, welche Daten von der Überwachung erfasst werden sollen und dabei auf die über ein Kommunikationsnetz (§ 3 Z 11 TKG) oder einen Dienst der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes) verschlüsselt gesendeten, übermittelten oder empfangenen Nachrichten und Informationen sowie damit im Zusammenhang stehenden Daten im Sinn des § 76a und des § 92 Abs. 3 Z 4 und 4a TKG (somit im Ergebnis Stamm-, Zugangs- und Verkehrsdaten wie bei der klassischen Telefonüberwachung) durch Installation eines Programms in einem Computersystem (§ 74 Abs. 1 Z 8 StGB) ohne Kenntnis dessen Inhabers oder sonstiger Verfügungsberechtigter, um eine Verschlüsselung beim Senden, Übermitteln oder Empfangen der Nachrichten und Informationen zu überwinden, abgestellt werden. Eine remote Installation eines zum Zwecke der Überwachung zu installierenden Programms im Fall der Gewährleistung einer eindeutigen Zuordenbarkeit des mobilen Endgeräts und des überwachten Kommunikationsvorgangs zu einer bestimmten Zielperson wurde ausdrücklich befürwortet.

Da die Überwachung verschlüsselter Nachrichten technische Besonderheiten aufweist, benötigt diese Ermittlungsmaßnahme engmaschige flankierende Schutzmaßnahmen, die die Einhaltung von Grundrechten gewährleisten sollen. Neben lückenlosen Protokollierungspflichten, die den Vollzug der Maßnahme nachvollziehbar und überprüfbar machen, schlägt der Entwurf daher auch derartige Schutzmaßnahmen vor (gerichtliche Bewilligung im Einzelfall, umfassende begleitende und nachträgliche Kontrollrechte des Rechtsschutzbeauftragten, der dafür auch entsprechende (IT-)Sachverständige heranziehen kann sowie strenge Verwendungsverbote für unzulässig erhobene Daten bzw. Zufallsfunde). Ein auf Grundlage der bisherigen Diskussionen vom Bundesministerium für Justiz ausgearbeiteter Textentwurf zur Überwachung verschlüsselter Nachrichten fand in der Sitzung vom 2. Februar 2017 die im Wesentlichen einhellige Zustimmung der Expertengruppe und soll daher Grundlage der Neuregelung bilden.

Aus Anlass der Einsetzung der Expertengruppe wurde vom Bundesministerium für Justiz auch ein Rechtsvergleich zur Überwachung verschlüsselter Nachrichten in anderen Mitgliedstaaten der Europäischen Union durchgeführt. Insgesamt konnten Informationen über 21 Mitgliedstaaten und ein Fragebogen von Eurojust eingeholt werden. Die Ergebnisse der Recherche lassen sich dahingehend zusammenfassen, dass eine Überwachung von Nachrichten (durch remote Installation eines Programms auf einem Computersystems, z. B. eines Smartphones) ohne Kenntnis der betroffenen Person in Bulgarien, Tschechien, Estland, Spanien, Frankreich, Italien, Polen, Portugal, Rumänien, im Vereinigten Königreich und Kroatien sowie in einigen Bundesländern in Deutschland grundsätzlich (unter unterschiedlichen Voraussetzungen) bereits gesetzlich zulässig ist.

Die Mitglieder der Expertengruppe vertraten kurz zusammengefasst folgende Positionen:

Prof. **Dr. Gerhard Dannecker** vertrat mit Blick auf die Rechtsprechung des deutschen BVerfG die Ansicht, dass die Unterscheidung zwischen Quellen-TKÜ und Online-Durchsuchung maßgeblich davon abhänge, ob technisch sichergestellt werden könne, dass ausschließlich die Kommunikation vor der Verschlüsselung und nicht auch darüber hinausgehende Daten durch die Maßnahme abgegriffen werden. Die Verwendung des Begriffes der „Nachricht“ erscheine zunächst in Bezug auf die komplexe informationstechnische Materie mit ihren zahlreichen Fachbegriffen recht „untechnisch“, sei mit Blick auf die Verständlichkeit des Normtextes für den Normadressaten jedoch zu begrüßen. Gleiches gelte für die Anlehnung des Begriffs der „Computersysteme“ an den bisherigen Gebrauch im StGB. Der explizite Ausschluss anderer technischer Möglichkeiten als einer Überwachungssoftware werde im Hinblick darauf, dass hier eine Kernproblematik der Quellen-TKÜ thematisiert werde, explizit gutgeheißen. Auch die Sicherstellung, dass das Programm (unter Aufsicht bzw. Kontrolle des Rechtsschutzbeauftragten) nach Beendigung der Maßnahme endgültig und ohne Schädigung des Computersystems von diesem entfernt werde, werde als zwingend und begrüßenswert empfunden. Schließlich wies Prof. Dr. Gerhard Dannecker auch auf die Notwendigkeit durchgehender Protokoll- und Dokumentationspflichten und eines Richtervorbehalts hin.

Univ.-Prof. **Dr. Susanne Reindl-Krauskopf** zog bei der Frage, ob für eine notwendige Vorfeldauswertung zur Durchführung der Maßnahme eine eigene Rechtsgrundlage notwendig sei, den Vergleich zur Anordnung der Durchsuchung von Orten und führte aus, dass die Eruierung möglicher

Zutrittsmöglichkeiten dort ebenso keiner gesonderten gesetzlichen Grundlage bedürfe, weil es sich nur um die Umsetzung eines gerichtlich bewilligten Grundrechtseingriffs handle. Wesentlich sei vielmehr, die zeitliche Reihenfolge der Grundrechtseingriffe und die Intensität deren Zusammenhangs, ob diese gemeinsam oder separat betrachtet werden müssen. Das Wissen über das von dem jeweiligen Computerbetreiber verwendende Betriebssystem sei mit der Kommunikationsüberwachung zwingend verbunden, wobei darauf geachtet werden müsse, keine Überregulierung zu erzeugen.

Univ.-Prof. **Dr. Peter Lewisch** merkte an, dass es sachlich nicht einsichtig sei, dass gewisse Kommunikationsformen (verschlüsselte Kommunikation) grundsätzlich, weil schlicht technologiebedingt, außerhalb der strafprozessualen Überwachung stehen sollen. Wolle man internetbasierte bzw. verschlüsselte Kommunikation einer funktional gleichwertigen Überwachung unterwerfen, müsse die Maßnahme technisch möglich, praktikabel, zielgenau (nur auf die Erfassung von Kommunikationsäquivalenten bezogen) sein, Vorsorge gegen Streuschäden/Kollateralschäden treffen und eine wirksame Missbrauchskontrolle bieten.

Prof. Dr. Ingeborg **Zerbes** wies darauf hin, dass nach deutscher Rechtslage bei der Überwachung laufender Kommunikation, auch wenn diese durch eine am Endgerät installierte Überwachungssoftware bewerkstelligt wird, ausschließlich das Fernmeldegeheimnis maßgebend ist, welches das spezifische Ausgeliefertsein von Daten schützt, das während des Ablaufs der Übertragung entsteht. Sämtliche Daten eines Computersystems *außerhalb* laufender Kommunikation werden in Deutschland hingegen vom (von der österreichischen Rechtsprechung nicht eigenständig anerkannten) „IT-Grundrecht“ geschützt (vergleichbar mit Art. 8 EMRK). Für die Ermittlungsmaßnahme der Überwachung von Nachrichten habe der österreichische Gesetzgeber in § 135 Abs. 3 StPO die Voraussetzungen bereits festgelegt. Bei der Einführung einer Befugnis zur Überwachung verschlüsselter Nachrichten die gleichen Schwellen vorzusehen sei daher grundrechtskonform. Internetbasierte Kommunikation sei typischerweise durch eine sog. Transportverschlüsselung verschlüsselt, die noch am Endgerät und unmittelbar *vor* der eigentlichen Übergabe der Nachricht in ihren Transport erfolge und diesem diene, sodass sich der technische Vorgang einer derartigen Verschlüsselung durchaus als Teil der Übertragung betrachten lasse. Da die Entschlüsselung durch die Behörden bei der Übertragung erfolge – und damit laufende Kommunikation öffne – sei dieser Vorgang daher durchaus als eine Art Nachrichtenüberwachung zu werten, die sich von einer (umfassenden) Online-Überwachung abgrenzen lasse und deren gesetzliche Grundlage nur die Vorgaben des Fernmeldegeheimnisses, nicht aber die (qualifizierteren) Vorgaben des „IT-Grundrechts“ erfüllen müsse. Wichtig sei, dass eine Software eingesetzt werde, die ausschließlich Transportverschlüsselungen (erkenne und) decodiere. Die notwendige Manipulation am Endgerät und die Missbrauchsgefahr mache den Eingriff in internetbasierte Kommunikation in gewisser Weise heikler als herkömmliche Nachrichtenüberwachung, was durch eine höhere Einsatzvoraussetzung abgehoben werden könnte. Eine Möglichkeit, den Bedenken, dass die Überwachungstechnik über das Erlaubte hinaus für eine breitere Online-Durchsuchung oder Online-Überwachung ausgenutzt werde, zu begegnen, wäre eine Ergänzung im System der Verwendungsverbote (Ergänzung in § 140 StPO).

SC **Dr. Mathias Vogl** (BM.I) begrüßte ausdrücklich die vorgeschlagenen Änderungen und betonte, dass die Einführung der neuen Ermittlungsmaßnahme einen bedeutenden Mehrwert für die Arbeit der Kriminalpolizei darstellen werde. Eine Gleichstellung der Maßnahme mit jener der Überwachung von Nachrichten gemäß § 134 Z 3 StPO werde auf Grund der gleichen Intensität des Grundrechtseingriffs grundsätzlich befürwortet. Hingewiesen werde aber darauf, dass daher dementsprechend mit einem höheren Anfall zu rechnen und die technische Umsetzung äußert aufwendig seien. Da anzunehmen sei, dass für jeden Fall eine individuelle Software er- bzw. zusammengestellt werden müsse, bedürfe es einer ausreichenden Legisvakanz, um eine ordnungsgemäße technische Umsetzung zu gewährleisten.

Zu den vorgeschlagenen Regelungen im Detail:

Sowohl im Titel als auch in der Definition der neuen Ermittlungsmaßnahme der „Überwachung verschlüsselter Nachrichten“ in **§ 134 Z 3a StPO** soll bereits unmissverständlich zum Ausdruck kommen, dass die Unterscheidung zur Überwachung von Nachrichten nach § 134 Z 3 StPO lediglich in der Überwindung einer Verschlüsselung liegt und daher in Übereinstimmung mit den Ergebnissen der Expertengruppe im Sinne einer Gleichförmigkeit mit § 134 Z 3 StPO das Überwachen von Nachrichten und Informationen (worunter neben dem Austausch zwischenmenschlicher Gedankeninhalte auch Kommunikation im technischen Sinn zu verstehen ist), erfasst wird (siehe Erläuterungen zu Z 9, § 134 Z 3 StPO).

Den angemeldeten Bedenken im Rahmen des Begutachtungsverfahrens (192/ME XXV. GP), wonach aufgrund des Verweises auf § 74 Abs. 2 StGB letztlich doch eine Online-Durchsuchung möglich sein könnte, soll mit dem gegenständlichen Entwurf auf zwei Arten Rechnung getragen werden: Einerseits soll durch die gewählte Formulierung „damit im Zusammenhang stehender Daten“ klargestellt werden, dass

nur jene Daten ermitteln werden dürfen, die mit dem Übertragungsvorgang in unmittelbarem Zusammenhang stehen (bei Kommunikations-Apps die Telefonnummer des Senders bzw. Empfängers, die Skype-ID, etc.), andererseits der Begriff der „Daten“ durch Verweis auf § 76a StPO und § 92 Abs. 3 Z 4 und 4a TKG konkreter gefasst und dadurch klargestellt werden, dass es sich dabei – ebenso wie bei der Überwachung von Nachrichten iSd § 134 Z 3 StPO – um Stamm-, Zugangs- und Verkehrsdaten handelt. Ein Screenen von lokalen Adressbüchern oder Kontaktverzeichnissen soll hingegen nicht zulässig sein.

Wesentlich ist daher, dass nur Nachrichten und Informationen sowie damit im Zusammenhang stehende Daten überwacht werden dürfen, die über ein Kommunikationsnetz (§ 3 Z 11 TKG) oder einen Dienst der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes) verschlüsselt gesendet, übermittelt oder empfangen werden. Jedes Senden, Übermitteln und Empfangen von Nachrichten und Informationen über eine internetbasierte App, die Chat-Funktionen erfüllt und dabei eine end-to-end- bzw. Transportverschlüsselung verwendet (z. B. WhatsApp, Telegram), ist daher ebenso von der Bestimmung umfasst wie das Übermitteln eines Datenpakets an einen Cloud-Server über einen Cloud-Dienstanbieter und das Abspeichern von E-Mail-Entwürfen über ein Webmail-Programm mit Transportverschlüsselung, weil in beiden Fällen eine Übermittlung von Nachrichten und Informationen an einen anderen Server stattfindet. Nicht erfasst ist hingegen etwa das verschlüsselte Übermitteln von Daten von einer lokalen Festplatte auf einen USB-Stick, weil in diesem Fall zwar Kommunikation im technischen Sinne vorliegt, diese Information aber nicht über ein Kommunikationsnetz oder einen Dienst der Informationsgesellschaft übermittelt wird. Ebenso wenig ist eine Verschlüsselung, die der Betreiber zum Schutz der ihm zur Übermittlung anvertrauten Inhaltsdaten anbringt, angesprochen (vgl. Bereitstellungspflicht unverschlüsselter Daten durch den Betreiber nach § 4 Abs. 4 ÜVO).

Als weiteres Kriterium ist vorgesehen, dass die Installation eines Programm in einem Computersystems (§ 74 Abs. 1 Z 8 StGB) ohne Kenntnis dessen Inhabers oder sonstiger Verfügungsberechtigter nur zulässig ist, um dadurch eine Verschlüsselung beim Senden, Übermitteln oder Empfangen der Nachrichten und Informationen zu überwinden und somit Nachrichten und Informationen überwachen zu können, die nach geltendem Recht – würden sie in unverschlüsselter Form übertragen werden – im Rahmen des § 134 Z 3 StPO unter Mitwirkung des Betreibers überwacht werden könnten.

Der Begriff „Computersystem“ wird mit Verweis auf die Begriffsbildung im StGB definiert (vgl. die Definition von Computersystem in § 74 Abs. 1 Z 8 StGB sowie die Verwendung des Begriffes in §§ 118a und 119a StGB). Nach der Legaldefinition des § 74 Abs. 1 Z 8 StGB sind unter dem Begriff „Computersystem“ sowohl einzelne als auch verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen, und von der, über die oder an die daher Daten übermittelt werden können (vgl. *Reindl-Krauskopf* in WK^2 StGB § 119a Rz 5), zu verstehen. Das bedeutet, dass die neue Ermittlungsmaßnahme nicht nur den klassischen Computerbegriff (Desktop-PC, Notebook) erfasst, sondern auch andere Geräte, die eine Internetverbindung ermöglichen (z. B. Smartphones, Tablets, Spielekonsolen etc.). Durch die Wahl des Begriffes soll einerseits vermieden werden, dass für ähnliche Sachverhalte und Gegenstände neue Terminologien mit sich überschneidenden Inhalten geschaffen werden und andererseits deutlich gemacht werden, dass es sich bei diesem Eingriff grundsätzlich um einen strafrechtswidrigen Eingriff handelt, der aufgrund der geschaffenen Rechtsgrundlage legitimiert wird (Art. 10a StGG).

Die Definition in Z 3a stellt darüber hinaus eindeutig klar, dass zur Durchführung einer solchen Überwachung lediglich die Installation eines Programms in dem Computersystem zulässig sein soll. Andere technische Möglichkeiten, wie z. B. das Auffangen elektromagnetischer Strahlungen oder der Einbau von Hardware-Komponenten in das Computersystem (z. B. eines „Keyloggers“) sind nicht zulässig. Eine praktische Umsetzung der gesetzlichen Vorgaben (Programmierung einer Software, die nur die gesetzlich vorgesehenen Vorgänge des Sendens, Übermittelns und Empfangens überwacht) ist nach dem derzeitigen Stand der Technik möglich, wobei die konkrete Durchführung in die Zuständigkeit des Bundesministeriums für Inneres fällt. Bedenken zur technischen Umsetzbarkeit Rechnung tragend, ist vorgesehen, ein unabhängiges Audit der Programmarchitektur durchzuführen. Dieses soll sowohl die Beschränkung des Programms auf die gesetzlich vorgesehenen Funktionen und die Nachvollziehbarkeit der getroffenen Maßnahmen sicherstellen als auch die berechtigten Sicherheits- und Geheimhaltungsinteressen des Staates berücksichtigen. Die Architektur des Programms wird entsprechend den Bestimmungen des DSG 2000 bei der Datenschutzbehörde anzumelden sein.

Die vorgeschlagene Regelung steht freilich der Sicherstellung eines Computersystems nach §§ 109 Z 1, 110 Abs. 1 Z 1 StPO und der Auswertung der darin gespeicherten Daten nicht entgegen.

Aus Anlass der Einführung dieser neuen Ermittlungsmethode soll auch die Definition des Ergebnisses in **§ 134 Z 5 StPO** angepasst werden, um auch die Ergebnisse der Überwachung verschlüsselter Nachrichten erfassen zu können (siehe dazu auch die Erläuterungen zu Z 8, § 134 Z 2a).

§ 135a StPO regelt die Voraussetzungen, unter denen die vorgeschlagene neue Ermittlungsmaßnahme zulässig sein soll. Da die Überwachung verschlüsselter Nachrichten nach § 135a StPO bereits derzeit rechtlich unter § 135 Abs. 3 StPO subsumiert werden kann (vgl. *Nimmervoll*, Das Strafverfahren, 233, wonach auch per Internet versendete Nachrichten wie WhatsApp o.ä. von den Bestimmungen über die Überwachung von Nachrichten umfasst wären) und unter diesen Voraussetzungen zulässig ist, die praktische Durchführung jedoch (aufgrund der Verschlüsselung) an der mangelnden Lesbarkeit der von den Betreibern ausgeleiteten Daten scheitert, wären auch bei Schaffung einer eigenständigen Regelung grundsätzlich die gleichen Zulässigkeitsvoraussetzungen wie in § 135 Abs. 3 StPO vorzusehen. Da die Durchführung einer solchen Ermittlungsmaßnahme nach derzeitigem Stand der Technik aber quantitativ und qualitativ sehr ressourcenintensiv ist (im Vorfeld sind aufwendige Ermittlungen zur Beschaffenheit des zu überwachenden Computersystems, eine individuelle Programmierung der Software und das unbemerkte Einbringen der Software im Zielsystem notwendig), wird vorgeschlagen, die Zulässigkeitsvoraussetzungen für den Zeitraum der vorgeschlagenen befristeten Geltung an höhere Schranken zu binden und daher einerseits an die Zuständigkeit des Landesgerichts als Schöffen- oder Geschworenengericht anzuknüpfen sowie die Ermittlungsmaßnahme darüber hinaus auch bei Ermittlungen bei strafbaren Handlungen nach §§ 277, 278, 278a und 278b StGB sowie damit im Zusammenhang stehenden Taten zum Einsatz bringen zu können (§ 135a Abs. 1 Z 3 StPO). Rechtzeitig vor Ende der Befristung soll die Ermittlungsmaßnahme im Hinblick auf den technischen Fortschritt einer Evaluierung unterzogen werden, wobei auch die Zulässigkeitsvoraussetzungen neu zu überdenken sein werden.

Die Installation des Programms auf dem zu überwachenden Computersystem kann grundsätzlich auf verschiedene Arten erfolgen (physikalische oder remote Installation), wobei in jedem Fall der eindeutigen Zuordnung des Zielsystems zur Zielperson vor und während der Maßnahme besondere Bedeutung zukommt. Dem Grundsatz der Gesetz- und Verhältnismäßigkeit folgend (§ 5 StPO) soll daher eine remote-Installation der Überwachungssoftware nur erlaubt sein, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass das zu überwachende Computersystem einer Zielperson zugeordnet werden kann (beispielsweise durch entsprechende begleitende Ermittlungsmaßnahmen wie Observation oder eindeutige Identifikation durch Mac-Adresse oder allenfalls Seriennummer, Geräte-ID, IMEI-Nummer oder individuelle IP-Adresse). Das Vorgehen unterscheidet sich dabei im Grunde nicht von der herkömmlichen Überwachung von Nachrichten, bei der ebenso die Möglichkeit besteht, dass eine andere als die Zielperson das Telefon verwendet und dadurch Nachrichten überwacht werden, die nicht von der gerichtlichen Anordnung umfasst waren. In beiden Fällen ist bei Feststellung dieses Umstandes die Überwachung umgehend zu beenden. Damit korrespondierend sollen auch entsprechende Schutzbestimmungen in **§ 140 Abs. 1 StPO** (Verwendungsverbote) vorgesehen werden. Demnach sollen Ergebnisse bei sonstiger Nichtigkeit nur als Beweismittel verwendet werden können, wenn die Ermittlungsanordnung auch rechtmäßig angeordnet und bewilligt wurde (§ 140 Abs. 1 **Z 2** StPO) und auch nur zum Nachweis einer vorsätzlich begangenen strafbaren Handlung, derentwegen die Ermittlungsmaßnahme angeordnet wurde oder hätte angeordnet werden können (§ 140 Abs. 1 **Z 4** StPO).

Nach Beendigung der Ermittlungsmaßnahme muss sichergestellt sein, dass die Software dauerhaft funktionsunfähig oder ohne dauerhafte Beschädigung oder Beeinträchtigung des Computersystems und der in ihm gespeicherten Daten entfernt wird (**§ 135a Abs. 2 StPO**). Dies kann in der Praxis durch die Ausstattung des Programms mit einem sogenannten „Kill-Switch“ sichergestellt werden, der nach Ablauf der vorgegebenen Periode oder durch remote-Betätigung (z. B. wenn es notwendig ist, die Maßnahme vorzeitig zu beenden, etwa weil das Gerät weitergegeben wurde und von einer anderen als der Zielperson verwendet wird) die vollständige forensische und sichere Löschung der Überwachungssoftware gewährleistet. Schließlich dürfen auch an dritten Computersystemen keine Schädigungen oder dauerhaften Beeinträchtigungen bewirkt werden (zur Nachvollziehbarkeit der Eingriffe durch das Programm siehe oben die Ausführungen zum geplanten Audit).

Zur Gewährleistung der praktischen Durchführung der Ermittlungsmaßnahme wird in **§ 135a Abs. 3 StPO** überdies vorgeschlagen, nicht nur das Eindringen in vom Hausrecht geschützte Räume, sondern auch das Überwinden spezifischer Sicherheitsvorkehrungen zu ermöglichen, weil Computersysteme in der Regel mit einem Zugangsschutz (z. B. durch ein Passwort oder einen Fingerabdruck) vor dem Zugriff Dritter geschützt werden können. Schließlich wird es für die Kriminalpolizei für die Installation der Überwachungssoftware in manchen Fällen auch notwendig sein, Behältnisse (z. B. Aktentaschen, Schreibtischladen) zu öffnen oder das Gerät aus der Kleidung des Betroffenen zu entnehmen, um sich Zugriff auf das Computersystem verschaffen zu können; auch die Zulässigkeit eines solchen Eingriffs soll

ausdrücklich klargestellt werden. § 135a Abs. 3 letzter Satz StPO ist § 121 Abs. 3 zweiter Satz StPO nachgebildet und soll zum Ausdruck bringen, dass bei Zugriff auf das Computersystem die Eigentums- und Persönlichkeitsrechte sämtlicher Betroffener soweit wie möglich zu wahren sind.

Zu Z 18, 20, 21 und 24 (§§ 137 Abs. 1 und 3, 138 Abs. 1 und 5 StPO):

Es wird vorgeschlagen, die übrigen Bewilligungsvoraussetzungen für die Überwachung verschlüsselter Nachrichten ebenso anzugleichen: Das Eindringen in vom Hausrecht geschützte Räume soll im Einzelnen einer gerichtlichen Bewilligung unterliegen (**§ 137 Abs. 1 StPO**). Die vorgeschlagene neue Ermittlungsmaßnahmen soll nur für einen künftigen Zeitraum angeordnet werden dürfen, der überdies zur Erreichung ihres Zwecks voraussichtlich erforderlich sein muss (**§ 137 Abs. 3 StPO**), wodurch ebenfalls zum Ausdruck gebracht wird, dass dadurch nicht auf bereits vor dem Anordnungszeitraum bestandene Daten, die in keinem Zusammenhang mit einem Übertragungsvorgang stehen, zugegriffen werden darf (klare Abgrenzung zur Online-Durchsuchung).

Schließlich sollen auch Anpassungen des notwendigen Inhalts der Anordnung (**§ 138 Abs. 1 StPO**) vorgenommen werden, die zusätzlich zu den in § 102 Abs. 2 StPO genannten Bestandteilen in die Anordnung und die gerichtliche Bewilligung aufzunehmen sind. Während § 135a Abs. 1 StPO die Zulässigkeitsvoraussetzungen für die in § 134 Z 3a StPO definierte Ermittlungsmaßnahme der Überwachung verschlüsselter Nachrichten normiert, handelt es sich bei § 138 StPO (nur) um eine Durchführungsvorschrift, die lediglich in Ansehung der unmittelbar die Zulässigkeit der Ermittlungsmaßnahme betreffenden Angaben zwingend ist. Soweit die gemäß § 138 StPO in Anordnung und gerichtlicher Bewilligung anzuführenden Daten mit Blick auf § 135a Abs. 1 StPO daher nicht zwingender Natur sind, müssen sie lediglich soweit wie möglich bzw. als zur Durchführung erforderlich angegeben werden (vgl. OGH vom 5.3.2015, 12 Os 93/14i, 12 Os 94/14m). Das Computersystem, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll, ist in einer Anordnung und gerichtlichen Bewilligung einer Überwachung verschlüsselter Nachrichten soweit wie erforderlich und möglich zu bezeichnen; gleiches gilt für die Örtlichkeit. Die häufig gar nicht mögliche Individualisierung des Computersystems ist nicht in jedem Fall notwendig und wird durch die (Gattungs-)Bezeichnung des Computersystems, z. B. PC, Laptop, Smartphone des zu Überwachenden, zu bezeichnen sein. Knüpft diese Ermittlungsmaßnahme an einem bereits bekannten Identifizierungsmerkmal (z. B. Rufnummer eines Smartphones, Mac-Adresse, Seriennummer, Geräte-ID, IMEI-Nummer oder individuelle IP-Adresse) an, so wird dieses anzuführen sein.

In **§ 138 Abs. 1 Z 3 StPO** wird zur Vermeidung von Unklarheiten letztlich vorgeschlagen, die Bezugnahme auf das Endgerät zu streichen, weil dies in jüngster Vergangenheit zu Zweifeln über die Zulässigkeit der Auswertung von Funkzellen in der Praxis entstehen hat lassen (vgl. jedoch die eine an der Standortkennung (Cell-ID) anknüpfende Auskunft über Daten einer Nachrichtenübermittlung gemäß § 135 Abs. 2 StPO („Funkzellenabfrage“) grundsätzlich für zulässig erachtende Entscheidung OGH vom 5.3.2015, 12 Os 93/14i, 12 Os 94/14m).

§ 138 Abs. 5 StPO soll ebenfalls an die neue Ermittlungsmaßnahme angepasst werden. Die notwendigen Zustellungen sollen grundsätzlich unverzüglich nach Beendigung der Ermittlungsmaßnahme vorgenommen werden, soweit und solange nicht ein Aufschub der Zustellung geboten ist, weil durch die Zustellung der Zweck dieses oder eines anderen Verfahrens gefährdet wäre. In den Rechtsmittelbelehrungen ist auch ein Hinweis auf die Möglichkeit der Geltendmachung von Ersatzansprüchen nach § 148 StPO aufzunehmen.

Zu Z 27 bis 29 (§§ 144 Abs. 3, 145 Abs. 3 und 4 StPO):

Während §§ 144 Abs. 3, 145 Abs. 3 StPO nur um die neue Ermittlungsmaßnahme zu ergänzen wären, soll mit dem neuen § 145 Abs. 4 StPO die Authentizität und Verlässlichkeit der ermittelten Daten sichergestellt werden. Von besonderer Bedeutung ist dabei die lückenlose Nachvollziehbarkeit der Eingriffe durch den behördlichen Zugang und jede im Wege des Programms erfolgende Übertragung von Nachrichten und Informationen in und aus diesem Computersystem durch geeignete Protokollierung. Dabei muss technisch gewährleistet werden, dass es durch die Durchführung der Überwachung zu keiner über die Installation und die mit der Überwachung notwendig einhergehenden Eingriffe der Software hinausgehenden Veränderung der ursprünglich am Computersystem vorhandenen Daten kommt. Durch die Protokollierung soll sichergestellt werden, dass jeder Zugriff der Software auf das Computersystem (ebenso bereits die Installation der Software selbst) und alle durch die Software ausgeleiteten Daten protokolliert werden; ebenso soll dadurch gewährleistet werden, dass über die Installation des Programms und einen allfälligen „Kill-Switch“ hinaus keine Daten in das von der Installation betroffene Computersystem übertragen werden. Durch die Protokollierung soll ausschließlich die Authentizität und Integrität der gewonnenen Ergebnisse sichergestellt werden, sodass Anregungen im Begutachtungsverfahren folgend die Wendung, dass erforderliche Sicherungskopien herzustellen sind,

nicht mehr vorgesehen ist. Vielmehr soll gewährleistet werden, dass alle Prozessschritte definiert und jederzeit überprüfbar sind, wobei die Korrektheit der konkreten technischen und organisatorischen Abwicklung durch das Bundesministerium für Inneres der Kontrolle des Rechtschutzbeauftragten der Justiz (§ 47a StPO) unterliegt (siehe dazu im Folgenden).

Zu Z 30, 33 und 34 (§§ 147 Abs. 1 Z 2a, Abs. 2 und 3a StPO):

Dem Rechtsschutzbeauftragen der Justiz soll die umfassende Prüfung und Kontrolle der Anordnung, Genehmigung, Bewilligung und Durchführung der Überwachung verschlüsselter Nachrichten obliegen (§ 147 Abs. 1 Z 2a StPO). Da diese Ermittlungsmaßnahme zwar im Hinblick auf die Eingriffsintensität nach Ansicht der Expertengruppe mit jener einer Überwachung von Nachrichten vergleichbar ist, jedoch auch in eine bestimmte Wohnung oder andere durch das Hausrecht geschützte Räume eingedrungen werden darf, wenn dies zu deren Durchführung unumgänglich ist (§ 135a Abs. 3 StPO), soll auch ein besonderer Schutz von ausschließlich der Berufsausübung gewidmeten Räumen oder einer der in § 157 Abs. 1 Z 2 bis 4 StPO genannten Personen eröffnet werden. Auf Grund des Gewichts der mit der Maßnahme verbundenen Grundrechtseingriffe müssen daher besondere Gründe vorliegen, die die Verhältnismäßigkeit des Eingriffes begründen (§ 147 Abs. 2 StPO).

Mit § 147 Abs. 3a StPO sollen die Rechte des Rechtsschutzbeauftragten der Justiz weiter ausgebaut werden, um eine effektive Kontrolle nicht nur der Anordnung, sondern auch der Durchführung der Maßnahme zu ermöglichen. Dem Rechtsschutzbeauftragten der Justiz soll dazu Einsicht in alle Unterlagen und Protokolle (§ 145 Abs. 4 StPO) zustehen, überdies soll er zu diesem Zweck nach Maßgabe der §§ 126 und 127 StPO auch die Beiziehung eines Sachverständigen verlangen können. Der Sachverständige ist gemäß § 126 Abs. 3 StPO im Ermittlungsverfahren von der Staatsanwaltschaft zu bestellen.

Zu Z 35 (§ 148 StPO):

Diese Bestimmung soll die verschuldensunabhängige Haftung des Bundes für durch die Ermittlungsmaßnahme verursachte Schäden auch für Fälle der Überwachung verschlüsselter Nachrichten begründen.

Beschlagnahme von Briefen:

Zu Z 13 (§ 135 Abs. 1 StPO):

Der klassische Briefverkehr ist aufgrund der mit dem technischen Fortschritt zur Verfügung stehenden modernen Kommunikationsmittel in den letzten Jahren kontinuierlich zurückgegangen.

Demgegenüber ist es in den letzten Jahren – nicht zuletzt aufgrund der zunehmenden Beliebtheit des Online-Handels – zu einem starken Zuwachs an Paketsendungen gekommen. Kriminelle Netzwerke nutzen weidlich die Möglichkeiten, im sog. Darknet anonym Verkäufe von Suchtgift, Waffen, Falschgeld, gefälschte Ausweise abzuwickeln und mittels Paketsendungen an Empfänger zuzustellen, auf welche die im Vergleich zu Eingriffen in die Telekommunikation restriktiveren Regelungen über die Beschlagnahme von Briefen anwendbar sind. In der Praxis kommt es immer wieder vor, dass Ermittlungen im Rahmen von Telefonüberwachungen oder im Bereich des Darknets den Verdacht erhärten, dass z. B. Suchtmittel im Wege von Brief- oder Paketsendungen zugestellt werden. Im Gegensatz zu § 26 ZollR-DG, der den Zollorganen eine rechtliche Handhabe zur Verfügung stellt, besteht nach der StPO allerdings derzeit in diesen Fällen keine Möglichkeit zur Beschlagnahme dieser Sendungen, weil die insofern einschlägige Vorschrift des § 135 Abs. 1 StPO derzeit voraussetzt, dass sich der Beschuldigte wegen einer vorsätzlichen, mit mehr als einjähriger Freiheitsstrafe bedrohten Tat in Haft befindet oder eine Vorführung oder Festnahme deswegen angeordnet wurde. Auch § 21 SMG betreffend Sicherstellung und Beschlagnahme von Drogenausgangsstoffen schafft hier keine Abhilfe, weil ein Regelungsinhalt, der über die Bestimmungen der StPO hinausginge, für das gerichtliche Strafverfahren kaum auszumachen ist (*Litzka/Matzka/Zeder*, SMG[2] § 21 Rz 5). Die Bestimmungen über die Beschlagnahme von Briefen iSd § 134 Z 1 StPO weisen daher eine geringe praktische Relevanz auf; so wurde diese Ermittlungsmaßnahme in den Jahren 2014 und 2015 jeweils lediglich einmal bewilligt (8572/AB vom 13. Juni 2016 zu 8964/J-25. GP; 4046/AB vom 18. Mai 2015 zu 4209/J-25. GP). Auch die Zahl der Anträge bewegte sich in den letzten Jahren im einstelligen Bereich; sie lag 2016 bei 5 und 2015 bei 6 (10933/AB vom 17.3.2017 zu 11420/J-25. GP). Durch den Entfall der Wortfolge „und sich der Beschuldigte wegen einer solchen Tat in Haft befindet oder seine Vorführung oder Festnahme deswegen angeordnet wurde“ soll künftig auch die Beschlagnahme von Briefen unbekannter Täter oder auf freiem Fuß befindlicher Beschuldigter ermöglicht werden.

Die vorgeschlagene Änderung steht mit Art. 10 StGG im Einklang: §§ 134 Z 1 und 135 Abs. 1 StPO sind insofern weiter als Art. 10 StGG, als letzterer nur Briefe in dem engen Sinn schriftlicher und körperlich fixierter Gedankenerklärungen (vgl. *Wiederin* in *Korinek/Holoubek*, B-VG, Art. 10 StGG Rz 12f) erfasst,

während §§ 134 Z 1 und 135 Abs. 1 StPO den Zugriff auf die Beförderung sämtlicher körperlicher Gegenstände unabhängig davon regelt, ob sie Gedankenerklärungen enthalten oder bloß – grundrechtlich nicht so weitgehend geschützte – sonstige Gegenstände (*Tipold/Zerbes* in WK-StPO § 134 Rz 7). Ein Brief iSd Art. 10 StGG liegt allerdings nur dann nicht vor, wenn – wie etwa bei gekennzeichneten Warensendungen – schon von außen erkennbar ist, dass die Sendung keinerlei Kommunikation enthält (*Wiederin* in *Korinek/Holoubek*, B-VG, Art. 10 StGG Rz 12). Bei Zustellungen von Paketen mit illegalen Inhalten kann jedoch in der Regel bei rein äußerer Betrachtung nicht ausgeschlossen werden, dass (auch) Gedankenerklärungen im Sinn des Art. 10 StGG darin enthalten sind. Die Beschlagnahme von Briefen darf gemäß Art. 10 StGG außer dem Falle einer gesetzlichen Verhaftung oder Haussuchung, nur in Kriegsfällen oder auf Grund eines richterlichen Befehls in Gemäßheit bestehender Gesetze vorgenommen werden. Ein richterlicher Befehl iSd Art. 10 StGG verlangt zum einen, dass die Ermächtigung zum Eingriff von einem Organ herrührt, das über die richterlichen Garantien des Art. 87 B-VG verfügt, und zum anderen, dass sie dem Eingriff vorausgeht (*E. Wiederin*, Schutz der Privatsphäre in *Merten/Papier/Kucsko-Stadlmayer* (Hg.). HGR VII/1., 2. Aufl, § 10 RN 27). Beide Voraussetzungen sind hier gegeben: Gemäß § 137 Abs. 1 StPO sind Ermittlungsmaßnahmen nach den §§ 135 bis 136 (und somit auch die Beschlagnahme von Briefen nach § 135 Abs. 1 StPO) von der Staatsanwaltschaft auf Grund einer gerichtlichen Bewilligung anzuordnen. Die Beschlagnahme von Briefen darf nach § 137 Abs. 3 auch nur für einen solchen künftigen Zeitraum angeordnet werden, der zur Erreichung des Zwecks voraussichtlich erforderlich ist.

Zu Z 19 und 24 (§§ 137 Abs. 2, 138 Abs. 5 StPO):

Der mit der vorgeschlagenen Änderung des § 135 Abs. 1 StPO verbundene Nutzen für die Ermittlungsbehörden wäre zunichte gemacht, wenn die Staatsanwaltschaft wie bisher ihre Anordnung und deren gerichtliche Bewilligung den von der Durchführung der Beschlagnahme von Briefen Betroffenen unverzüglich zustellen müsste, weil weitergehende Ermittlungen zur Ausforschung der an kriminellen Handlungen beteiligten Personen nicht mehr möglich wären. Die Aufschiebung der Zustellung aus ermittlungstaktischen Gründen soll daher – wie sie schon bisher bei Eingriffen in die Telekommunikation iSd § 134 Z 2 und 3 StPO vorgesehen ist– künftig auch bei der Beschlagnahme von Briefen nach § 135 Abs. 1 StPO zulässig sein.

Der mit der Aufschiebung der Zustellung der Anordnung verbundene Zweck könnte jedoch nicht erreicht werden, wenn vor der Öffnung des Briefes oder Pakets – wie derzeit in § 137 Abs. 2 StPO vorgesehen – auch weiterhin iSd § 111 Abs. 4 und § 112 StPO vorgegangen werden müsste.

Zweck der Bestätigung iSd § 111 Abs. 4 StPO ist es, den Betroffenen von der Beschlagnahme und ihrem Ausmaß zu informieren (*Bertel/Venier*, StPO § 137 Rz 2). Dies ergibt sich jedoch bereits hinreichend aus der in jedem Fall schriftlich auszufertigenden und zu begründenden Anordnung auf Beschlagnahme von Briefen (vgl. die §§ 102, 138 Abs. 1 StPO). Das mit dem Budgetbegleitgesetz 2009, BGBl. I Nr. 52/2009, in § 111 Abs. 4 StPO eingefügte Erfordernis der Belehrung über das Recht des Betroffenen, eine gesonderte gerichtliche Entscheidung über die Aufhebung oder Fortsetzung der Sicherstellung iSd § 109 Z 1 und § 110 StPO verlangen zu können, soll ausgleichen, dass die Sicherstellung von Gegenständen (§ 109 Z 1 lit. a StPO) grundsätzlich ohne Beschlagnahme und damit ohne gerichtliche Kontrolle fortgesetzt wird – der Betroffene soll daher eine solche gemäß § 115 Abs. 2 StPO zumindest beantragen können (*Tipold/Zerbes* in *Fuchs/Ratz*, WK-StPO § 111 Rz 25). Der Beschlagnahme von Briefen geht aber ohnehin in jedem Fall eine gerichtliche Bewilligung der Anordnung der Staatsanwaltschaft voraus (§ 137 Abs. 1 StPO).

Gegen die Beschlagnahme von Briefen stehen die Rechtsmittel der Beschwerde gegen die gerichtliche Bewilligung und der Einspruch gegen die Anordnung und Durchführung der Beschlagnahme aufgrund der gerichtlichen Bewilligung zur Verfügung (vgl. *Reindl-Krauskopf*, WK-StPO § 138 Rz 8). Da § 111 Abs. 4 StPO weniger Rechtsmittelmöglichkeiten als die auf die Beschlagnahme von Briefen unmittelbar anwendbaren Bestimmungen (vgl. die §§ 86 Abs. 1, 102 Abs. 2 Z 4 StPO) erwähnt, erweist sich auch dieser Teil des Verweises als nicht erforderlich. Insgesamt ergibt sich somit, dass eine sinngemäße Anwendung des § 111 Abs. 4 StPO, der teilweise auf die Ermittlungsmaßnahme der Beschlagnahme von Briefen gar nicht zugeschnitten ist, zur Wahrung der Rechte der Betroffenen nicht erforderlich ist.

Zweck der Belehrung iSd § 112 StPO wiederum ist, dem Betroffenen die Erhebung eines Widerspruchs gegen die Beschlagnahme unter Berufung auf ein gesetzlich anerkanntes Recht zur Verschwiegenheit zu ermöglichen (*Fabrizy*, StPO[12] § 138 Rz 2). Auch diese Belehrung ist jedoch bei näherer Betrachtung nicht erforderlich, weil die Staatsanwaltschaft die Ergebnisse der Beschlagnahme, also den Inhalt der Briefe oder anderer Sendungen, zu prüfen und (nur) jene Teile zu den Akten zu nehmen hat, die für das Verfahren von Bedeutung sind und als Beweismittel verwendet werden dürfen. Die zusätzliche Formulierung in § 138 Abs. 4 StPO, dass die beweisrelevanten und verwendbaren Teile in Bild- oder

Schriftform zu übertragen sind, ist lediglich für die übrigen in §§ 135 und 136 StPO genannten Ermittlungsmaßnahmen relevant, hat aber für die Beschlagnahme von Briefen keine Bedeutung, weil diese Schriftstücke ohnehin in Originalform zum Akt genommen werden können.

Ob Ergebnisse einer Beschlagnahme von Briefen verwendet werden dürfen, richtet sich vor allem nach § 140 StPO und den Regeln über den Schutz der geistlichen Amtsverschwiegenheit und der besonderen sonstigen Berufsgeheimnisse (§§ 144, 157 Abs. 2 StPO). Stellt sich bei Prüfung der Ergebnisse z. B. heraus, dass Verteidigerpost beschlagnahmt wurde, würde die Verwendung solcher Sendungen in der Hauptverhandlung das Recht auf Verteidigung (Art. 6 Abs. 3 lit. b und c EMRK) unterlaufen und wäre überdies eine unzulässige Umgehung des Aussageverweigerungsrechtes des Parteienvertreters (§ 157 Abs. 1 Z 2 iVm § 157 Abs. 2 und § 144 Abs. 2 StPO). Die Briefe dürfen aus diesen Gründen bei sonstiger Nichtigkeit nicht als Beweismittel verwendet werden (§ 157 Abs. 2 StPO) und sind daher nicht zu den Akten zu nehmen (*Reindl-Krauskopf*, WK-StPO § 138 Rz 22), vielmehr sind die Ergebnisse der Ermittlungsmaßnahme gemäß § 139 Abs. 4 StPO auf Antrag des Beschuldigten, weiteren von der Ermittlungsmaßnahme Betroffenen oder von Amts wegen zu vernichten. Die zitierten Bestimmungen stellen daher die Wahrung der gesetzlich anerkannten Rechte zur Verschwiegenheit im Rahmen der Beschlagnahme von Briefen ausreichend sicher und eine adäquate Anpassung des Rechtsschutzes an den Bereich der Eingriffe in die Telekommunikation dar.

Akustische Überwachung von Personen:

Zu Z 17, 18, 27, 28 und 32 (§§ 136 Abs. 1a, 137 Abs. 1, 140 Abs. 1 Z 2, 144 Abs. 3, 145 Abs. 3, 147 Abs. 1 Z 5 StPO):

Da eine akustische Überwachung in Fahrzeugen derzeit nur unter den restriktiven Zulässigkeitsvoraussetzungen für eine optische und akustische Überwachung von Personen nach § 136 Abs. 1 StPO zulässig ist, eine solche jedoch einen schwerwiegenden Grundrechtseingriff darstellt, indem sie die optische **und** akustische Überwachung von Personen umfasst, wird in Umsetzung der Vorgaben des Arbeitsprogramms der Bundesregierung für 2017/2018 vorgeschlagen, für die spezielle Konstellation einer bloß akustischen Überwachung von Personen in Fahrzeugen (zu der bloß optischen Überwachung von Personen siehe § 136 Abs. 3 StPO) eine eigene Bestimmung zu schaffen und wegen vergleichbarer Eingriffsintensität an die Voraussetzungen der Überwachung von Nachrichten (§ 135 Abs. 3 StPO) anzuknüpfen.

Die akustische Überwachung in Fahrzeugen soll gemäß § 137 Abs. 1 StPO von der Staatsanwaltschaft auf Grund einer gerichtlichen Bewilligung anzuordnen sein. Anders als bei dem in § 136 Abs. 2 angesprochenen Eindringen in durch das Hausrecht geschützte Räume, handelt es sich bei einem Fahrzeug (in das zur Installation der Überwachungsinstrumente unter Umständen eingedrungen wurden muss) typischerweise nicht um einen vom Hausrecht geschützten Raum; Fremdes Hausrecht wird beim geheimen Eindringen in das Auto nicht verletzt (vgl. *Tipold/Zerbes* in WK-StPO § 117 Rz 9 – 14; . *Reindl/Krauskopf* in WK-StPO, § 136 Rz 19). Es ist daher auch keine gesonderte gerichtliche Bewilligung nach § 137 Abs. 1 letzter Halbsatz erforderlich.

Auch diese Maßnahme soll nur für einen zukünftigen Zeitraum angeordnet werden dürfen (§ 137 Abs. 3 StPO). Durch Ergänzung der neuen Maßnahme in § 140 Abs. 1 Z 2 StPO soll die neue Maßnahme an die Verwendungsverbote, die u.a. auch bei § 136 Abs. 3 StPO vorgesehen sind, angeglichen werden. Die Ergebnisse sollen überdies ebenso unter Verschluss aufbewahrt werden, solange die in Bild- und Schriftform übertragenen Ergebnisse nicht zum Akt genommen werden (§ 145 Abs. 3 StPO; Verschlusssachenverordnung).

Ist die Maßnahme gegen eine Person gerichtet, die gemäß § 157 Abs. 1 Z 2 bis 4 StPO berechtigt ist, die Aussage zu verweigern, soll sie (wie auch in den Fällen der § 135 Abs. 2 bis 3, 135a und 136 Abs. 1 Z 2 und 3 StPO) der Prüfung und Kontrolle der Anordnung, Genehmigung, Bewilligung und Durchführung durch den Rechtsschutzbeauftragten unterliegen (§ 144 Abs. 3 iVm § 147 Abs. 1 Z 5 StPO).

Sonstige Änderungen im 5. Abschnitt des 8. Hauptstückes:

Zu Z 15 und 31 (§ 135 Abs. 3 Z 3 und 136 Abs. 1 Z 3, 147 Abs. 1 Z 3)

Durch diese Änderungen sollen redaktionelle Versehen behoben werden.

Zu Z 22 und 23 (§ 138 Abs. 2 und 3 StPO):

Da es in der Vergangenheit zu Unklarheiten bei der Reichweite der Auskunfts- und Mitwirkungspflicht von Anbietern und sonstigen Diensteanbietern gekommen ist, wird vorgeschlagen, ausdrücklich klarzustellen, dass diesen Pflichten unverzüglich nachzukommen ist. In der Praxis ist es in der Vergangenheit wiederholt zu nicht tolerierbaren Verzögerungen bei der Aufklärung und Verfolgung von Strafverfahren gekommen, weil Anbieter und sonstige Diensteanbieter die Meinung vertreten haben, dass

zu ihrer rechtlichen Absicherung vorab eine Prüfung der rechtlichen Voraussetzungen der Anordnung erforderlich sei (idR durch Rechtsabteilungen, die aber nicht rund um die Uhr erreichbar sind bzw. waren). Zur weiteren rechtlichen Absicherung der Anbieter und sonstigen Diensteanbieter soll – trotz insofern eindeutiger Rechtslage – zusätzlich eine (§ 53 Abs. 3c SPG oder § 48b Abs. 8 BörseG vergleichbare) ausdrückliche gesetzliche Klarstellung erfolgen, dass die rechtliche Zulässigkeit der Auskunftserteilung und Mitwirkung auf der gerichtlichen Bewilligung der Anordnung gründet. Einer Erwähnung der neuen Ermittlungsmaßnahme der Überwachung verschlüsselter Nachrichten nach § 135a StPO bedarf es nicht, weil diese ohne Mitwirkung der Betreiber von den Strafverfolgungsbehörden durchgeführt wird.

Durch Ergänzung des „Betreibers“ in der Aufzählung des § 138 Abs. 3 StPO wird ein Redaktionsversehen behoben.

Sonstige Änderungen der StPO:

Zu Z 3 (§ 67 Abs. 7 StPO):

Gemäß § 67 Abs. 7 letzter Satz StPO gelten für die Beigebung und Bestellung eines Vertreters des Privatbeteiligten die Bestimmungen der §§ 61 Abs. 4, 62 Abs. 1, 2 und 4 StPO sinngemäß. Dagegen enthält § 67 StPO derzeit keinen Verweis auf § 63 Abs. 1 StPO, der die Unterbrechungswirkung des Verfahrenshilfeantrags hinsichtlich des Fristenlaufs beim Beschuldigten regelt. Praktisch kann aufgrund der notwendigen Schritte (Beigebung durch das Gericht, Bestellungsbescheid durch die Rechtsanwaltskammer) ohne Unterbrechungswirkung des Antrags jedoch in vielen Fällen die Frist zur Ausführung des Rechtsmittels oder einer sonstigen Prozesshandlung nicht gewahrt werden. Zwar hat der Verfassungsgerichtshof jüngst im Verfahren G 139/2016 den auf eine behauptete Verfassungswidrigkeit dieses Umstandes gerichteten Parteienantrag auf Normenkontrolle aus formalen Gründen zurückgewiesen, durch die Einfügung eines Verweises in § 67 Abs. 7 StPO auf § 63 Abs. 1 StPO soll aber künftig sichergestellt werden, dass auch dem Privatbeteiligten die Unterbrechungswirkung des Verfahrenshilfeantrags zugutekommt. Die Frist soll daher auch für den Privatbeteiligten erst mit dem Zeitpunkt neu beginnen, ab welchem entweder dem bestellten Vertreter Beigebungsbeschluss, Bestellungsbescheid und Aktenstück oder dem Privatbeteiligten der seinen Verfahrenshilfeantrag abweisende (rechtskräftige) Beschluss zugestellt werden/wird.

Zu Z 5 (§ 94 letzter Satz StPO):

§ 94 letzter Satz StPO wies bisher nur die Aufforderung, einen anderen **Verteidiger** zu bestellen, der gerichtlichen Kompetenz zu, während die Aufforderung an das Opfer oder einen sonst Beteiligten, einen anderen Vertreter zu wählen, nicht erwähnt wurde. Ungeachtet dieses Umstandes wurde in den Erläuterungen zur Regierungsvorlage des Strafprozessreformgesetzes ausgeführt: „Die dort genannten Ordnungsstrafen und Maßnahmen (Aufforderung, einen anderen **Vertreter** zu bestellen, gegebenenfalls Beigabe eines Vertreters von Amts wegen und vorübergehender Entzug der Vertretungsbefugnis) sollen jedoch weiterhin nur dem Gericht – allenfalls auf Antrag der Staatsanwaltschaft und Initiative der Kriminalpolizei – zukommen.“ (EBRV 25 BlgNR 22. GP 124). Im Hinblick darauf, dass bereits in den Gesetzesmaterialien davon ausgegangen wurde, dass sämtliche Vertreter in die Gerichtskompetenz fallen sollen, und eine Differenzierung zwischen Verteidigern und sonstigen Vertretern in diesem Zusammenhang auch nicht sachgerecht erscheint, soll diese Unterscheidung bei dieser Gelegenheit beseitigt werden.

Für die Verhängung von Ordnungsstrafen und die Aufforderung, einen anderen Vertreter zu bestellen, soll in Anlehnung an § 93 Abs. 4 letzter Satz StPO festgelegt werden, dass der Einzelrichter des Landesgerichts auf Antrag der Staatsanwaltschaft darüber zu entscheiden hat (§ 94 letzter Satz iVm § 31 Abs. 1 Z 2 und § 105 StPO). Über den Entzug der Vertretungsbefugnis für die Dauer von einem bis zu sechs Monaten soll hingegen wie bisher das Oberlandesgericht auf Antrag der Staatsanwaltschaft zu entscheiden haben (§ 94 dritter Satz iVm § 236 Abs. 3 StPO).

Zu Z 6 (§ 116 Abs. 6 zweiter Satz StPO):

Mit der vorgeschlagenen Änderung soll eine im Bereich des verwaltungsbehördlichen Finanzstrafverfahrens bereits durch das 2. Abgabenänderungsgesetz 2014, BGBl. I Nr. 105/2014, erfolgte und mit 30. Dezember 2014 in Kraft getretene Änderung (§ 99 Abs. 6 vierter Satz FinStrG) auch für den Bereich des gerichtlichen Strafverfahrens (und im Wege des § 195 Abs. 1 FinStrG) des Verfahrens wegen gerichtlich strafbarer Finanzvergehen nachvollzogen werden.

Durch die geltende Regelung des § 116 Abs. 6 zweiter Satz erfüllen Kreditinstitute ihre gesetzliche Verpflichtung zur Herausgabe der Daten „in einem allgemein gebräuchlichen Dateiformat“ auch durch Übermittlung von Dateien im PDF-Format. Die aus solchen PDF-Dateien nur ablesbaren – nicht aber strukturiert zu verarbeitenden – Informationen müssen sodann händisch in andere Dateiformate

(Tabellenkalkulations- oder Datenbankprogramme) übertragen werden, um eine elektronische Auswertung vornehmen zu können. Damit ist gerade in der Praxis des strafprozessualen Ermittlungsverfahrens ein beträchtlicher Zeit- und Ressourcenaufwand verbunden. Um diesen Aufwand und damit auch Kosten zu verringern, potentielle Fehlerquellen bei der händischen Übertragung der Daten auszuschließen und eine verfahrensrechtlich nicht gebotene Differenzierung zum verwaltungsbehördlichen Finanzstrafverfahren zu beseitigen, soll § 116 Abs. 6 zweiter Satz entsprechend § 99 Abs. 6 vierter Satz FinStrG geändert werden. Die Daten sollen künftig von Kredit- und Finanzinstituten auch im Bereich des gerichtlichen Strafverfahrens so zu übermitteln sein, dass diese auch elektronisch weiterverarbeitet werden können, beispielsweise in Form von Dateien gängiger Tabellenkalkulations- oder Datenbankprogramme (vgl. EBRV 360 BlgNr. 25. GP, 24).

Zu Z 36 (§ 209b Abs. 1 StPO)

Durch diese Änderung soll der Verweis in § 209b Abs. 1 StPO auf das Wettbewerbsgesetz an die Änderungen durch das Bundesgesetz, mit dem das Kartellgesetz 2005, das Wettbewerbsgesetz und das Bundesgesetz zur Verbesserung der Nahversorgung und der Wettbewerbsbedingungen geändert werden (Kartell- und Wettbewerbsrechts-Änderungsgesetz 2017 – KaWeRÄG 2017, BGBl. I Nr. 56/2017) angepasst werden.

Zu Z 37 (§ 221 Abs.1 StPO):

Artikel 8 Abs. 2 lit. a der Richtlinie 2016/343/EU über die Stärkung bestimmter Aspekte der Unschuldsvermutung und des Rechts auf Anwesenheit in der Verhandlung im Strafverfahren ABl. Nr. L 65 vom 11.03.2016 S 1 (RL Unschuldsvermutung) verlangt für eine Verhandlung und Urteilsfällung in Abwesenheit des Verdächtigen oder der beschuldigten Person eine rechtzeitige Unterrichtung über die Verhandlung und über die Folgen des Nichterscheinens.

Bis zum 31.12.2007 erforderte § 221 Abs. 1 dritter Satz StPO hinsichtlich des Angeklagten die Androhung, „daß er im Fall seines Ausbleibens zu gewärtigen habe, daß je nach Umständen entweder die Hauptverhandlung in seiner Abwesenheit vorgenommen oder er durch einen Vorführbefehl zur Verhandlung gestellt oder, falls dies nicht zeitgerecht ausführbar sei, die Hauptverhandlung auf seine Kosten vertagt und er zur Verhandlung vorgeführt werde“. Diese Belehrung wurde zwar nicht ausdrücklich ins neue Recht übernommen, jedoch ist in Schrifttum und Rechtsprechung nicht zweifelhaft, dass die Nichtigkeitsdrohung des § 427 StPO – neben den bereits zu § 221 Abs. 2 StPO verlangten Voraussetzungen einer wirksamen Ladung – auch den Hinweis auf die Möglichkeit eines Verfahrens in Abwesenheit erfasst (*Bauer/Jerabek* in WK-StPO § 427 Rz 9 ff; *Danek/Mann* in WK-StPO § 221 Rz 16; *Ratz* in WK-StPO § 281 Rz 243; 13 Os 107/08x, 108/08v, 109/08s). Auch wenn die Ladung des Angeklagten zur Hauptverhandlung seit dem 1.1.2008 nicht mehr zwingend die Androhung seiner Vorführung im Fall seines Nichterscheinens zu enthalten hat, wird im Schrifttum empfohlen, den genannten Passus in keiner Ladung fehlen zu lassen, um eine gegebenenfalls sonst notwendige neuerliche Ladung (anstelle der Vorführung) vermeiden zu können (*Danek/Mann* in WK-StPO § 221 Rz 16). Die Ladungsformulare des Bundesministeriums für Justiz enthalten daher nach wie vor die früher in § 221 Abs. 1 dritter Satz StPO gesetzlich normierten Belehrungen über die Säumnisfolgen. Um den Vorgaben der Richtlinie zu entsprechen sollen die bis 31.12.2007 in Geltung stehenden Belehrungen mit an die aktuelle Terminologie der StPO angepassten Formulierungen wieder in den Rechtsbestand aufgenommen werden.

Zu Z 39 (§ 514 Abs. 36 StPO):

Diese Regelung regelt das Inkrafttreten. Die Überwachung verschlüsselter Nachrichten soll vorerst nur für einen befristeten Zeitraum von fünf Jahren in Kraft treten, aussagekräftig evaluiert und mit gegebenenfalls erforderlichen Änderungen in den permanenten Rechtsbestand überführt werden.

Zu Z 40 (§ 516a Abs. 6 StPO):

Durch die genannte Änderung wird die RL Unschuldsvermutung im nationalen Recht umgesetzt.