Entwurf

Erläuterungen:

I. Allgemeiner Teil

Die vorliegende Regierungsvorlage beinhaltet folgende Schwerpunkte:

1.) Überarbeitung und Ergänzung des 5. Abschnitts des 8. Hauptstücks der StPO („Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Lokalisierung einer technischen Einrichtung, Anlassdatenspeicherung, Überwachung von Nachrichten, verschlüsselter Nachrichten und von Personen“) samt Bezug habender Änderungen im Staatsanwaltschaftsgesetz (im Folgenden „StAG“) und Telekommunikationsgesetz 2003 (im Folgenden „TKG“). Die vorgeschlagenen Änderungen sind zum Teil zur Umsetzung der Richtlinie (EU) 2017/541 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates, ABl. Nr. L 88 vom 15.03.2017 S. 6 (im Folgenden „RL Terrorismus“) erforderlich. Im Übrigen dienen sie der Umsetzung des Regierungsprogramms der Bundesregierung 2017 – 2022 „Zusammen. Für unser Österreich“ (S. 31). Inhaltlich beruhen die Vorschläge zu wesentlichen Teilen auf den Ergebnissen einer in der abgelaufenen Legislaturperiode im Bundesministerium für Justiz u.a. zur Thematik der Überwachung internetbasierter Kommunikation eingesetzten Expertengruppe und berücksichtigen auch im Lichte der Ergebnisse des Begutachtungsverfahrens zum Ministerialentwurf 325/ME 25. GP Bedürfnisse der Strafverfolgungsbehörden ebenso wie jene nach effektivem Rechtschutz. Die vorgeschlagenen Änderungen betreffen insbesondere:

a) Schaffung einer ausdrücklichen gesetzlichen Regelung für die seit Jahren eingesetzte Ermittlungsmaßnahme der Lokalisierung einer technischen Einrichtung ohne Mitwirkung eines Betreibers (sog. IMSI-Catcher);
b) Schaffung einer eigenständigen und aussagekräftigen Definition der Überwachung von Nachrichten;
c) Neuregelung der verfahrensrechtlichen Bestimmungen zur Beschlagnahme von Briefen unter Anpassung an jene der Überwachung der Telekommunikation und systemkonformem Ausbau des Rechtsschutzes der Korrespondenz mit Berufsgeheimnisträgern durch Kontroll- und Prüfungsbefugnisse des Rechtsschutzbeauftragten der Justiz;
d) Einführung einer neuen Ermittlungsmaßnahme zur Überwachung verschlüsselter Nachrichten unter Berücksichtigung der Beratungen einer Expertengruppe zur Überwachung internetbasierter Kommunikation sowie den Umsetzungserfordernissen aus der RL Terrorismus; Ergänzung des jährlichen Berichts über besondere Ermittlungsmaßnahmen, der vom Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz dem Nationalrat, dem Datenschutzrat und der Datenschutzbehörde vorzulegen ist, um die Ergebnisse der Anwendung dieser Ermittlungsmaßnahme;
e) Einführung einer neuen Ermittlungsmaßnahme der Anlassdatenspeicherung (sog. Quick-freeze);
f) Erweiterung der Möglichkeiten des Einsatzes der optischen und akustischen Überwachung von Personen um Straftaten nach §§ 278c bis 278e StGB in Umsetzung der RL Terrorismus.

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

Ad 1.)

a) Für die im Strafverfahren bereits 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) soll auch in der StPO eine exakte Rechtsgrundlage geschaffen werden. Diese gesetzliche Klarstellung erhöht die Rechtssicherheit (s. § 5 Abs. 1 StPO) und ordnet diese Ermittlungsmaßnahme in ein klares Rechtsschutzsystem ein (siehe im Detail II. Besonderer Teil).

b) und d) Zur Schließung entstandener Lücken in der Strafverfolgung aufgrund des technischen Fortschritts soll eine neue Ermittlungsmaßnahme zur Überwachung verschlüsselter Nachrichten mit einem der Grundrechtsintensität dieser zielgerichteten Maßnahme entsprechend umfassenden Rechtsschutzkonzept eingeführt werden. Dabei soll entgegen der in Stellungnahmen zum Ministerialentwurf, 325/ME 25. GP, vielfach geäußerten Besorgnis einer Massenüberwachung ausdrücklich klargestellt werden, dass die Ermittlungsmaßnahme nur in einem konkreten Strafverfahren wegen eines konkreten Verdachts von Straftaten und nicht zur Überwachung einer nicht bestimmten Anzahl von Personen angeordnet werden darf. Im Einzelnen ist stets eine begründete Anordnung der Staatsanwaltschaft erforderlich, die einer gerichtlichen Bewilligung bedarf. Unabhängige gerichtliche Kontrolle soll nicht nur gegen die Bewilligung der Anordnung, sondern auch gegenüber Rechtsverletzungen bei der Durchführung der Ermittlungsmaßnahme deren Recht- und Verhältnismäßigkeit sichern. Umfassende Verständigungs- und Einsichtsrechte für Beschuldigte und Betroffene sollen Transparenz und Kontrolle ermöglichen. Umgehungs- und Beweisverwendungsverbote dienen dem Schutz von Berufsgeheimnisträgern wie auch der genauen Einhaltung der Einsatzvoraussetzungen. Die engmaschige Einbindung des Rechtsschutzbeauftragten der Justiz gewährleistet nicht nur „kommissarischen“ Rechtsschutz, sondern auch die Kontrolle der Durchführung unter Beiziehung von Sachverständigen. Schließlich soll Transparenz und parlamentarische Kontrolle durch Aufnahme dieser Ermittlungsmaßnahme in den jährlichen Bericht des Bundesministers für Verfassung, Reformen, Deregulierung und Justiz über besondere Ermittlungsmaßnahmen an den Nationalrat, den Datenschutzrat und die Datenschutzbehörde ermöglicht werden. (siehe im Detail II. Besonderer Teil).

Die Vorschläge des Entwurfs können sich in weiten Bereichen auf die Ergebnisse einer im Sommer 2016 einberufen hochrangigen Expertengruppe stützen.

Im Zuge der Beratungen der Expertengruppe wurde die Technologieneutralität der Strafprozessordnung als wesentlicher Vorteil erkannt (siehe in diesem Sinn z. B. auch die Stellungnahme der Staatsanwaltschaft Eisenstadt zu 325/ME 25. GP), der durch die Schaffung eigenständiger Definitionen unter weitgehender Loslösung von Verweisen dauerhaft gewährleistet werden soll. In diesem Sinn 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 werden, wodurch auch unmissverständlich klargestellt werden kann, dass der Begriff der „Nachricht“ die autonome Kommunikation zwischen zwei Geräten („M2M“-Kommunikation) ohne menschliches Zutun nicht umfasst.

Die Überwachung von Nachrichten wäre aufgrund der geltenden Rechtslage grundsätzlich auch im Fall ihrer Verschlüsselung zulässig, läuft aber eben aufgrund dieser Verschlüsselung ins Leere. Mit der Einführung einer neuen Ermittlungsmaßnahme zur Überwachung verschlüsselter Nachrichten 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. So betont auch die RL Terrorismus, dass den für die Ermittlung oder strafrechtliche Verfolgung der dort bezeichneten Straftaten zuständigen Behörden wirksame Ermittlungsinstrumente, wie sie beispielsweise im Zusammenhang mit organisierter Kriminalität oder anderen schweren Straftaten verwendet werden, zur Verfügung stehen, wobei solche wirksamen Ermittlungsinstrumente auch die Überwachung des Kommunikationsverkehrs umfassen sollen (Art. 20 Abs. 1, Erw 21 der RL Terrorismus).

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 eindeutig 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 effizient reagieren können. Dieser Umstand erlangt umso mehr Bedeutung, als verschlüsselte Kommunikation herkömmliche Telefonie oder SMS bereits weitgehend verdrängt hat und die Strafverfolgung aufgrund dieser technologischen Entwicklung zunehmend erschwert und behindert wird.

Mangels anderer, insbesondere technischer Alternativen, sowie aufgrund des Umstandes, dass die Verschlüsselung der Kommunikation direkt auf dem Gerät erfolgt und daher auch nicht durch Mitwirkung des Betreibers umgangen werden kann, ist für die Überwachung verschlüsselter Nachrichten die (remote oder physikalische) Installation eines Programms in dem zu überwachenden Computersystem erforderlich, welches **ausschließlich von einer natürlichen Person 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 vorgeschlagen, eine Legisvakanz bis 1. April 2020 vorzusehen, um 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 zu ermöglichen. Aus Verhältnismäßigkeitserwägungen soll die Ermittlungsmaßnahme an höhere Zulässigkeitsvoraussetzungen als die Überwachung von Nachrichten nach § 135 Abs. 3 StPO gebunden werden. Schließlich soll sich die Ermittlungsmaßnahme bewähren müssen, weshalb sie vorerst nur für einen befristeten Zeitraum von fünf Jahren in Kraft gesetzt werden sowie rechtzeitig vor Ende der Befristung (auch im Hinblick auf einen voraussichtlich erfolgten technischen Fortschritt) einer Evaluierung unterzogen werden soll, wobei auch die Zulässigkeitsvoraussetzungen neu zu überdenken sein werden.

Das Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz hat dem Nationalrat, der Datenschutzbehörde und der Datenschutzkommission jährlich über den Einsatz besonderer Ermittlungsmaßnahmen (derzeit nach § 136 Abs. 1 Z 2 und 3 StPO oder nach § 141 Abs. 2 und Abs. 3 StPO) Bericht zu erstatten (vgl. Gesamtbericht über den Einsatz besonderer Ermittlungsmaßnahmen; § 10a Abs. 4 StAG). Aus den bisherigen Berichten ergibt sich in einer Gesamtschau, dass die Maßnahme der optischen und/oder akustischen Überwachung nach § 136 Abs. 1 Z 2 und 3 StPO in der Praxis maßvoll eingesetzt wird. Im Jahr 2014 kam es in sechs Verfahren zu einer optischen und akustischen Überwachung nach § 136 Abs. 1 Z 3 StPO („großer Späh- und Lauschangriff“), im Jahr 2015 in insgesamt fünf und im Jahr 2016 in insgesamt zwei Verfahren. Der sog. „kleine Späh- und Lauschangriff“ nach § 136 Abs. 1 Z 2 StPO gelangte im Jahr 2014 in sechs Verfahren, im Jahr 2015 in vier Verfahren und im Jahr 2016 in fünf Verfahren zur Anwendung. Anordnung und Durchführung der neuen Ermittlungsmaßnahme der Überwachung verschlüsselter Nachrichten soll in diesen Gesamtbericht integriert werden (siehe Artikel 2, Änderungen im Staatsanwaltschaftsgesetz), wodurch in größtmöglicher Transparenz parlamentarische und datenschutzrechtliche Kontrolle nach Art einer „Gesamtüberwachungsrechnung“ gewährleistet werden soll.

c) Die Ermittlungsmaßnahme der Beschlagnahme von Briefen soll 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, insbesondere eine effektive Bekämpfung und Verfolgung des zunehmenden Versandes von Briefen mit im sog. Darknet angebotenen Suchtmitteln ermöglichen. Eine Einschränkung des Rechtsschutzes ist damit nicht verbunden, weil die Beschlagnahme von Briefen weiterhin nur auf Anordnung der Staatsanwaltschaft nach gerichtlicher Bewilligung zulässig ist (vgl. § 137 Abs. 1 StPO), wogegen gerichtlicher Rechtsschutz besteht (Beschwerde gegen die gerichtliche Bewilligung und Einspruch wegen Rechtsverletzung, § 87 StPO und § 106 StPO, siehe im Detail II. Besonderer Teil). Im Hinblick auf schriftliche Korrespondenz von und mit Berufsgeheimnisträgern, die grundsätzlich dem – unter Nichtigkeitssanktion stehenden – Umgehungsverbot des § 157 Abs. 2 StPO unterliegt, soll der Rechtsschutz durch Kontroll- und Prüfungsbefugnisse des Rechtsschutzbeauftragten der Justiz systemkonform ausgebaut werden.

e) Das Regierungsprogramm der Bundesregierung 2017 – 2022 (s. S. 44) sieht die Einführung eines Quick-Freeze-Modells (Anlassdatenspeicherung) bei Vorliegen eines Anfangsverdachts bestimmter gerichtlich strafbarer Handlungen aufgrund einer staatsanwaltschaftlichen Anordnung und eine gerichtliche Bewilligung unter der Voraussetzung eines konkreten Tatverdachtes, um auf diese gespeicherten Daten zugreifen zu können, vor. Zur Umsetzung dieses Vorhabens sollen bei Vorliegen eines Anfangsverdachts bestimmter gerichtlich strafbarer Handlungen Telekommunikationsanbieter aufgrund staatsanwaltschaftlicher Anordnung verpflichtet werden, Telekommunikationsdaten (Verkehrsdaten, Zugangsdaten und Standortdaten) nach Ablauf der etwa für Verrechnungszwecke zulässigen Speicherung bis zu zwölf Monate weiter zu speichern (Anlassdatenspeicherung, sog. Quick-freeze). Im Falle, dass sich der Anfangsverdacht verdichtet, kann die Staatsanwaltschaft wie schon bisher

nach § 135 Abs. 2 oder § 76a Abs. 2 StPO auf diese gespeicherten Daten zugreifen. Sollte sich der Anfangsverdacht nicht erhärten, so soll die staatsanwaltschaftliche Anordnung außer Kraft treten und der Verdächtige über den Vorgang zu informieren sein. In Artikel 3 sollen die notwendigen Folgeanpassungen im TKG vorgenommen werden. Damit sollen aber auch die grundrechtlichen Anforderungen im Lichte der jüngsten Judikatur des EuGHs (vgl. Urteil des EuGH vom 21.12.2016, verbundene Rechtssachen C-203/15 und C-698/15 Tele2 Sverige AB gegen Post- och telestyrelsen und Secretary of State of the Home Department gegen Tom Watson u.a., im Folgenden: Tele2 Sverige) umgesetzt werden.

f) Zur Umsetzung des Art. 20 der RL Terrorismus betreffend den Einsatz wirksamer Ermittlungsinstrumente (s. Erw 21) soll die optische und akustische Überwachung von Personen (§ 136 Abs. 1 Z 3 StPO) auch zur Aufklärung terroristischer Straftaten (§ 278c StGB) und weiterer besonders schwerwiegender Straftaten im Zusammenhang mit terroristischen Aktivitäten, nämlich Terrorismusfinanzierung (§ 278d StGB) und Ausbildung für terroristische Zwecke (§ 278e StGB) zulässig sein. Hinsichtlich des geltenden Zulässigkeitskriteriums der Aufklärung oder Verhinderung von im Rahmen einer kriminellen Organisation oder einer terroristischen Vereinigung (§ 278a und § 278b StGB) begangenen oder geplanten Straftaten, soll klargestellt werden, dass es sich bei solchen Straftaten um Verbrechen (§ 17 Abs. 1 StGB) handeln muss.

Ad. 2.) Zur 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 und klargestellt werden, dass im Verfahren zur Unterbringung in einer Anstalt für geistig abnorme Rechtsbrecher nach § 21 Abs. 1 StGB Betroffene jedenfalls über die Verhandlung zu unterrichten sind.

Kompetenzgrundlage:

Die Zuständigkeit des Bundes zur Erlassung dieses Bundesgesetzes ergibt sich aus Art. 10 Abs. 1 Z 6 B-VG (Strafrechtswesen).

II. Besonderer Teil

Zu Artikel I (Änderungen der StPO)

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.

Allgemeines zu den Änderungen im 5. Abschnitt des 8. Hauptstücks der StPO:

Zu Z 2, 3, 4, 9 bis 37 und 40 (Inhaltsverzeichnis, Überschrift des 5. Abschnitts des 8. Hauptstücks der StPO, § 134 Z 2a und 2b, 3, 3a und 5, Überschrift von § 135 StPO, § 135 Abs. 1, 2a, 2b und Abs. 3 Z 3, § 135a, § 136 Abs. 1 Z 3, Abs. 4, § 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 soll eine Überarbeitung und Ergänzung des 5. Abschnitts des 8. Hauptstücks („Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Lokalisierung einer technischen Einrichtung, Anlassdatenspeicherung, Überwachung von Nachrichten, verschlüsselter Nachrichten und von Personen“) erfolgen. Die Änderungen sind zum Teil zur Umsetzung der RL Terrorismus erforderlich. Im Übrigen dienen sie der Umsetzung des Regierungsprogramms der Bundesregierung 2017 – 2022 (S. 31 und 44) und berücksichtigen Bedürfnisse der Strafverfolgungsbehörden ebenso wie jene nach effektivem Rechtsschutz.

Sämtliche Änderungen orientieren sich an den zur Wahrung der Grundrechte notwendigen Anforderungen eines effektiven Rechtsschutzes. Eine Optimierung des Strafverfahrens soll eben nur unter größtmöglichem Schutz der Rechte des Einzelnen erzielt werden. Der Systematik der StPO folgend, sollen daher 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. Der Verhältnismäßigkeitsgrundsatz (§ 5 StPO) ist im Einzelfall zu wahren. Darüber hinaus sollen die Rechtsschutzmöglichkeiten, Verwertungs- bzw. Verwendungsverbote und Löschungsverpflichtungen entsprechend angepasst bzw. erweitert werden.

Zur Umsetzung der RL Terrorismus notwendige Änderungen im 5. Abschnitt des 8. Hauptstücks der StPO:

Zu Z 2 bis 4, 11, 12, 17 bis 20, 22, 23, 26, 28 bis 37 (Inhaltsverzeichnis, Überschrift des 5. Abschnitts des 8. Hauptstücks der StPO, § 134 Z 3a und 5, § 135a, § 136 Abs. 1 Z 3, Abs. 4, § 137 Abs. 1 und 3, § 138 Abs. 1 und 5, § 140 Abs. 1 Z 2 und 4, § 144 Abs. 3, § 145 Abs. 3 und 4, § 147 Abs. 1 Z 2, 3 und 5, Abs. 2 und 3a und § 148 StPO):

Nach Art. 20 Abs. 1 der RL Terrorismus treffen die Mitgliedstaaten die erforderlichen Maßnahmen, um sicherzustellen, dass den für die Ermittlung oder strafrechtliche Verfolgung der Straftaten nach den Art. 3 bis 12 zuständigen Personen, Stellen oder Diensten wirksame Ermittlungsinstrumente, wie sie beispielsweise im Zusammenhang mit organisierter Kriminalität oder anderen schweren Straftaten verwendet werden, zur Verfügung stehen. Erw 21 der RL Terrorismus präzisiert diese Bestimmung dahingehend, dass der Einsatz dieser Instrumente im Einklang mit dem nationalen Recht gezielt erfolgen sollte und dem Grundsatz der Verhältnismäßigkeit sowie der Art und Schwere der untersuchten Straftaten Rechnung tragen. Weiters sei auch auf den Schutz personenbezogener Daten zu achten. Falls angezeigt, sollten diese Instrumente beispielsweise die Durchsuchung jeglichen persönlichen Eigentums, die Überwachung des Kommunikationsverkehrs, die verdeckte Überwachung einschließlich elektronischer Überwachung, die Aufnahme und Aufbewahrung von Tonaufnahmen in privaten und öffentlichen Fahrzeugen oder an privaten oder öffentlichen Orten sowie Aufnahmen von Bildmaterial von Personen in öffentlichen Fahrzeugen und an öffentlichen Orten sowie Finanzermittlungen umfassen.

Der Großteil der in Erw 21 der RL Terrorismus genannten Ermittlungsinstrumente für die Ermittlung und Verfolgung der in Art. 3 bis 12 der RL Terrorismus genannten Straftaten steht nach der StPO bereits zur Verfügung. So wird die „Durchsuchung jeglichen persönlichen Eigentums“ durch die Dursuchung von Orten und Gegenständen sowie von Personen nach §§ 119ff StPO ermöglicht, die „Überwachung des Kommunikationsverkehrs“ durch die Überwachung von Nachrichten nach § 134 Z 3, § 135 Abs. 3 StPO (faktisch derzeit jedoch lediglich im Bereich der nicht verschlüsselten Kommunikation), die „verdeckte Überwachung einschließlich elektronischer Überwachung“ durch die verdeckte Ermittlung nach § 129 Z 2, § 131, § 133 StPO und die Observation (allenfalls unter Einsatz technischer Mittel) nach § 129 Z 1, § 130, § 133 StPO, die „Aufnahmen von Bildmaterial von Personen in öffentlichen Fahrzeugen und an öffentlichen Orten“ durch die optische Überwachung von Personen nach § 134 Z 4, § 136 Abs. 3 StPO sowie „Finanzermittlungen“ durch die Auskunft aus dem Kontenregister und Auskunft über Bankkonten und Bankgeschäfte nach § 109 Z 3 und 4, § 116 StPO. Die Zulässigkeitsvoraussetzungen dieser Ermittlungsmaßnahmen erlauben bereits nach geltendem Recht deren Einsatz im Bereich der in Art. 3 bis 12 der RL Terrorismus genannten Straftaten.

Ein gewisser Umsetzungsbedarf ergibt sich jedoch im Bereich der genannten „Aufnahme und Aufbewahrung von Tonaufnahmen in privaten oder öffentlichen Fahrzeugen oder an privaten oder öffentlichen Orten“. Mit den vorgeschlagenen Änderungen sollen daher die Möglichkeiten der optischen und akustischen Überwachung von Personen auf terroristische Straftaten und besonders schwerwiegende Straftaten im Zusammenhang mit terroristischen Aktivitäten erweitert werden. Auch die neue Ermittlungsmaßnahme der Überwachung verschlüsselter Nachrichten (§ 135a StPO) soll, wenngleich die Zulässigkeitserfordernisse gegenüber dem ME eines Strafprozessrechtsänderungsgesetzes 2017, 325/ME 25. GP, angehoben werden sollen, den Vorgaben der RL Terrorismus entsprechend bei Straftaten nach §§ 278a bis 278e StGB zur Anwendung gelangen können.

Zu Z 2, 3, 13,40 (Inhaltsverzeichnis und Überschrift des 5. Abschnitts des 8. Hauptstücks 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, Anlassdatenspeicherung 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.

Lokalisierung einer technischen Einrichtung:

Zu Z 9, 12, 15 und 27 bis 30, 34 bis 35 (§ 134 Z 2a und 5, § 135 Abs. 2a, § 140 Abs. 1 Z 2 und 4, § 144 Abs. 3, § 145 Abs. 3, § 147 Abs. 1 Z 5 und Abs. 2 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 Überwachungskostenverordnung – ÜKVO, BGBl. II Nr. 322/2004) ohne Mitwirkung eines Anbieters

(§ 92 Abs. 3 Z 1 TKG) oder sonstigen Diensteanbieters (§ 13, § 16 und § 18 Abs. 2 des E–Commerce–Gesetzes – ECG, 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 bereits seit Jahren erfolgreich auf der Rechtsgrundlage der § 134 Z 2, § 135 Abs. 2 StPO eingesetzt.

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 nunmehr für die Lokalisierung einer technischen Einrichtung durch die Kriminalpolizei mittels des sog. IMSI-Catchers eine ausdrückliche gesetzliche, von den Bestimmungen des TKG unabhängige (daher „Feststellung von geografischen Standorten“) Definition und Regelung in der StPO geschaffen werden.

Entgegen mitunter anzutreffender Kritik zu 325/ME 25. GP handelt es sich nicht um eine „nachträgliche Legalisierung“, weil nach der geltenden Rechtslage der Einsatz eines IMSI-Catchers im Strafverfahren unter die Bestimmungen der Auskunft über Daten einer Nachrichtenübermittlung eingeordnet wurde (vgl. in diesem Sinne auch die Rechtsprechung, zuletzt OLG Wien vom 3.2.2017, 20 Bs 4/17k, und etwa den Erlass des Bundesministeriums für Justiz vom 4. April 2008 GZ BMJ-L430.001/002-II 3/2008). Die Einführung der Definition in § 134 Z 2a StPO samt Anschlussänderungen dienen lediglich der Klarstellung und Abgrenzung des Einsatzes dieser auch bereits derzeit rechtlich zulässigen Ermittlungsmaßnahme und damit insgesamt der Erhöhung der Rechtssicherheit.

Zur unmissverständlichen Klarstellung, dass der Einsatz eines IMSI-Catchers keiner Gesprächsüberwachung dienen darf, soll in § 135 Abs. 2a StPO ausdrücklich angeordnet werden, dass die Ermittlungsmaßnahme nur in den Fällen des § 135 Abs. 2 Z 1, 3 und 4 StPO und ausschließlich zur Feststellung der in § 134 Z 2a StPO genannten Daten, also ausschließlich zur Feststellung von geographischen Standorten und der IMSI-Nummer, zulässig ist.

Im Bereich des Sicherheitspolizeigesetzes – SPG, BGBl. Nr. 566/1991, ist der Einsatz technischer Mittel zur Lokalisierung einer Endeinrichtung im Rahmen der Gefahrenabwehr bereits in § 53 Abs. 3b SPG eigenständig geregelt und kann von den Sicherheitsbehörden zur Hilfeleistung oder Abwehr einer gegenwärtigen Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen vorgenommen werden. Mit der Stellungnahme der Generalprokuratur zu 325/ME 25. GP ist die sachliche Nähe und vergleichbare Eingriffsintensität zur Abfrage von Stammdaten (§ 76a Abs. 1 StPO) bzw. Observation unter Einsatz technischer Mittel (§ 130 Abs. 3 StPO zu betonen, weil die Lokalisierung einer technischen Einrichtung durch Einsatz technischer Mittel nur zur Feststellung von geografischen Standorten und IMSI-Nummern ohne Mitwirkung eines Anbieters (Einsatz des IMSI-Catchers) unter begleitender Observation einer Zielperson eingesetzt werden und bloß dazu dienen darf, das von dieser Person eingesetzte Computersystem (Endgerät, Smartphone) zu identifizieren. Aus diesem Grund sollen auch die Eingriffsvoraussetzungen an diesen Ermittlungsmethoden orientiert werden, die gleichfalls eine begründete staatsanwaltschaftliche Anordnung genügen lassen.

Das Erfordernis einer Anordnung der Staatsanwaltschaft gewährleistet unabhängigen gerichtlichen Rechtschutz in Gestalt des Einspruchs wegen Rechtsverletzung (§ 106 StPO), dem die Staatsanwaltschaft entweder zu entsprechen oder diesen an das Gericht weiterzuleiten hat (vgl. § 106 Abs. 4 und 5 StPO). Gegen die daraufhin ergehende Entscheidung des Gerichts steht wiederum Beschwerde (§ 87 StPO) zu. Entsprechend den allgemeinen Grundsätzen des Strafverfahrens ist der Verhältnismäßigkeitsgrundsatz (§ 5 StPO) auch bei der Anordnung der Lokalisierung einer technischen Einrichtung in vollem Umfang zu wahren. In weiterer Verfolgung des Gedankens effektiven Rechtsschutzes sollen in **§ 140 Abs. 1 StPO** flankierende Schutzbestimmungen (Verwendungsverbote) vorgesehen werden. Demnach sollen Ergebnisse bei sonstiger Nichtigkeit nur als Beweismittel verwendet werden können, wenn die Ermittlungsmaßnahme 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 unterliegt die Ermittlungsmaßnahme dem Umgehungsverbot und erfordert in bestimmten Fällen die Ermächtigung des Rechtsschutzbeauftragten der Justiz insbesondere zum Schutz von Berufsgeheimnisträgern (vgl. Z 33, § 144 Abs. 3 StPO). Korrespondierend dazu obliegt dem Rechtsschutzbeauftragten der Justiz die Prüfung und Kontrolle der Anordnung und Durchführung dieser Maßnahme (vgl. Z 38 und 39, § 147 Abs. 1 Z 5 und Abs. 2 StPO).

Anlassdatenspeicherung:

Zu Z 9, 15, 20, 22 bis 24, 26 und 27 (§ 134 Z 2b, § 135 Abs. 2b, 137 Abs. 1 und 3, § 138 Abs. 1, 2 und 5, § 140 Abs. 1 Z 2 StPO):

Das Regierungsprogramm 2017-2022 der Bundesregierung (S. 44) sieht die Einführung eines „*Quick-freeze"*-Modells (Anlassdatenspeicherung) bei Vorliegen eines Anfangsverdachts (§ 1 Abs. 3 StPO) bestimmter gerichtlich strafbarer Handlungen aufgrund staatsanwaltschaftlicher Anordnung vor. Der Zugriff auf die gespeicherten Daten soll eines konkreten Tatverdachts und einer gerichtlichen Bewilligung bedürfen.

Zur Umsetzung dieses Vorhabens sollen Anbieter und sonstige Diensteanbieter aufgrund einer staatsanwaltschaftlicher Anordnung (§ 137 Abs. 1 StPO) bei Vorliegen eines Anfangsverdachts (§ 1 Abs. 3 StPO) verpflichtet werden (§ 138 Abs. 2 StPO), zur Sicherstellung einer Anordnung nach § 135 Abs. 2 Z 2 bis 4 StPO oder einer Anordnung nach § 76a Abs. 2 StPO von der Löschung der in § 134 Z 2 StPO genannten Daten abzusehen und diese nach Ende der ansonsten (etwa für Verrechnungszwecke) zulässigen Speicherung bis zu 12 Monate weiter zu speichern (§ 134 Z 2b StPO und § 135 Abs. 2a StPO). Die Kategorien von zu speichernden Daten werden – wie vom EuGH gefordert – durch die Bezugnahme auf § 134 Z 2 StPO auf das absolut Notwendige beschränkt. Das Erfordernis eines Anfangsverdachts (§ 1 Abs. 3 StPO) gewährleistet den notwendigen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel und Personenkreis (vgl. EuGH Tele2 Sverige zum notwendigen Zusammenhang zwischen Speicherung und Zweck der Bekämpfung schwerer Straftaten). Die Speicherfrist ist individuell in der Anordnung zu bestimmen und mit höchstens zwölf Monaten begrenzt (Verhältnismäßigkeitsgrundsatz § 5 StPO). Gegen diese Anordnung steht jeder Person, die behauptet, im Ermittlungsverfahren durch die Staatsanwaltschaft in einem subjektiven Recht verletzt zu sein, der Einspruch an das Gericht zu (§ 106 StPO). Wesentlich ist, dass weiterhin keine Form von anlassloser Massenspeicherung von Kommunikationsdaten für zulässig erklärt wird, sondern nur im konkreten Einzelfall auf Anordnung der Staatsanwaltschaft bestimmte Kategorien von Daten für einen bestimmten Zeitraum nicht gelöscht werden dürfen. Korrespondierend dazu soll in § 99 Abs. 2 TKG, der jene Fälle normiert, in denen Anbieter Daten nicht zu löschen haben, um eine entsprechende Bestimmung (in § 99 Abs. 2 Z 4 TKG) ergänzt werden (siehe dazu Artikel 3).

Im Falle, dass sich der Anfangsverdacht verdichtet, kann die Staatsanwaltschaft wie bereits derzeit nach § 135 Abs. 2 StPO oder § 76a Abs. 2 StPO auf solcherart nicht gelöschte Daten zugreifen, weil es keinen Unterschied macht, ob – wie bisher – auf übliche historische Verrechnungsdaten oder – die inhaltlich selben „Quick-Freeze"-Daten zugegriffen wird. Schließlich ist bereits in § 137 Abs. 3 StPO normiert, dass in den Fällen des § 135 Abs. 2 StPO die Ermittlungsmaßnahme auch für einen vergangenen Zeitraum angeordnet werden kann. Sollte sich der Anfangsverdacht hingegen nicht erhärten, so tritt die staatsanwaltschaftliche Anordnung außer Kraft und der Verdächtige ist über den Vorgang zu informieren (vgl. Änderung in § 138 Abs. 5 StPO, wonach nach Beendigung der Ermittlungsmaßnahme die Anordnung und gegebenenfalls die gerichtliche Bewilligung dem Beschuldigten und den von der Durchführung Betroffenen unverzüglich zuzustellen ist).

Zur Gewährleistung einer ihrer Sensibilität entsprechenden sorgfältigen Verarbeitung der Daten soll in § 138 Abs. 1 StPO normiert werden, dass Anbieter und sonstige Diensteanbieter Anordnungen zur Anlassdatenspeicherung (§ 135 Abs. 2b StPO) unverzüglich zu entsprechen und die von der Löschungsverpflichtung ausgenommenen Daten (§ 99 Abs. 2 Z 4 TKG) nach Ablauf der angeordneten Dauer oder auf Grund einer Anordnung der Staatsanwaltschaft zu löschen haben. Gleiches gilt, wenn die Staatsanwaltschaft die Anlassdatenspeicherung vor dem angeordneten Zeitraum beendet. Andernfalls sollen empfindliche Verwaltungsstrafen drohen (vgl. Artikel 3, § 109 Abs. 3 Z 23 TKG).

Da der Zugriff auf die gespeicherten Daten im Rahmen der Ermittlungsmaßnahme der Auskunft über Daten einer Nachrichtenübermittlung nach § 134 Z 3, § 135 Abs. 2 StPO der gerichtlichen Bewilligung bedarf (gegen die wiederum Beschwerde an das Oberlandesgericht möglich ist, vgl. § 87 StPO), ist die Regelung auch in dieser Hinsicht im Einklang mit der Rechtsprechung des EuGH. Die Speicherfrist ist individuell in der Anordnung zu bestimmen und mit höchstens zwölf Monaten begrenzt (Verhältnismäßigkeitsgrundsatz § 5 StPO).

Die weiteren Änderungen sind notwendige Folgeanpassungen, die dem Charakter des Grundrechtseingriffs entsprechend anwendbar sein sollen (§ 138 Abs. 1, § 140 Abs. 1 Z 2 StPO). Da bei der Anlassdatenspeicherung keine „Ergebnisse" iSd § 134 Z 5 StPO entstehen, weil nur bereits vorhandene Daten (für die angeordnete Frist, maximal jedoch für zwölf Monate) nicht gelöscht, nicht hingegen erst Daten neu gespeichert werden, hat eine Ergänzung in den Begleitbestimmungen (§ 140, § 144, § 145 StPO) zu unterbleiben; ein allfälliger Zugriff auf die solcherart nicht gelöschten Daten bedarf ohnedies einer gesonderten Anordnung nach § 135 Abs. 2 StPO oder § 76a Abs. 2 StPO sowie im

Fall einer Anordnung nach § 135 Abs. 2 StPO auch einer gerichtlichen Bewilligung bedarf (vgl. § 137 Abs. 1 StPO).

Überwachung von Nachrichten:

Zu Z 10 (§ 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, wodurch Auslegungsspielräume und folglich Auffassungsunterschiede in Bezug auf den Nachrichtenbegriff im Allgemeinen vermieden werden sollen.

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 die Überwachung eines zwischenmenschlichen Gedankenaustausches, 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). Dagegen soll die autonome (Maschinen-) Kommunikation zwischen zwei Geräten („M2M"-Kommunikation, „Internet der Dinge") ohne menschliches Zutun ausdrücklich vom Regelungsumfang ausgenommen werden. Von der Ermittlungsmaßnahme sollen daher schon definitionsgemäß nur Nachrichten und Informationen erfasst werden, die von einer natürlichen Person über ein Kommunikationsnetz (§ 3 Z 11 TKG) oder einen Dienst der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes) gesendet, übermittelt oder empfangen werden. Zumindest eine natürliche Person muss somit am Kommunikationsvorgang beteiligt sein. Da § 134 Z 3a StPO auf § 134 Z 3 StPO verweist, ist klargestellt, dass auch bei der Überwachung verschlüsselter Kommunikation M2M-Kommunikation nicht umfasst wird, sondern erforderlich ist, dass eine natürliche Person Nachrichten oder Informationen sendet, übermittelt oder empfängt.

Argumente, wonach der Aufruf von Websites einen tieferen Eingriff in Grundrechte als die Überwachung zwischenmenschlichen Gedankenaustausches (über Telefon, SMS oder E-Mail) darstelle, hat das deutsche Bundesverfassungsgericht in seiner Entscheidung vom 6. Juli 2016, 2 BVR 1454/13, verworfen. Das Bundesverfassungsgericht hielt ausdrücklich 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 einvernehmlich erzielten Ergebnissen der vom Sommer 2016 bis Februar 2017 im Bundesministerium für Justiz tätigen Expertengruppe soll daher ausdrücklich klargestellt werden, dass die vorgeschlagene Formulierung der „Überwachung von Nachrichten" gemäß § 134 Z 3 StPO weiterhin nicht nur menschliche Gedankeninhalte (herkömmliche Telefonie, SMS, MMS, Sprachnachrichten, Videonachrichten, E-Mails, etc.), sondern ebenso von einer natürlichen Person 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 damit auch 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, sofern die Nachricht oder Information von zumindest einer natürlichen Person gesendet, übermittelt oder empfangen wird) zulässig. Anstelle des Austausches oder Weiterleitens (vgl. § 92 Abs. 3 Z 7 TKG) soll auf Senden, Übermitteln oder Empfangen abgestellt, wodurch alle Übertragungsvorgänge erfasst werden sollen (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 11, 12, 17, 27 und 28 (§ 134 Z 3a und 5, § 135a, § 140 Abs. 1 Z 2 und 4 StPO):

Ein im Frühjahr 2016 zur allgemeinen Begutachtung versandter Ministerialentwurf betreffend ein Bundesgesetz, mit dem die Strafprozessordnung und das Staatsanwaltschaftsgesetz geändert werden, 192/ME 25. 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, 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 zu 192/ME 25. GP allerdings auf eine Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden.

Das Begutachtungsverfahren zu 192/ME 25. GP 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 wurde die technische Umsetzbarkeit bezweifelt. 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 wurde im Sommer 2016 vom Bundesministerium für Justiz eine hochrangige Expertengruppe eingesetzt und 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 Verfassung, Reformen, Deregulierung und Justiz) gehörten 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 Verfassung, Reformen, Deregulierung und 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 auch verschlüsselte Nachrichten unter „Überwachung von Nachrichten“ subsumierbar sind und deren Überwachung daher rechtlich bereits zulässig wäre, liegt jedoch derzeit eine offenkundige und die Effektivität der Strafverfolgung hindernde Gesetzeslücke vor, weil verschlüsselte Kommunikation von den Strafverfolgungsbehörden technisch 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. In Deutschland wurden ebenfalls lange Zeit vergleichbare Diskussionen zur Quellen-TKÜ geführt, die zwischenzeitig zu deutlich weitergehenden Änderungen führten. So ist seit 24. August 2017 eine Novelle der deutschen StPO in Kraft, nach der nunmehr sowohl die – der vorgeschlagenen Ermittlungsmaßnahme des § 135a vergleichbare – Online-Überwachung (allerdings im Gegensatz zur vorliegenden Regierungsvorlage unter denselben Voraussetzungen wie bei der herkömmlichen Telefonüberwachung) als auch – jedoch unter strengeren Voraussetzungen – eine Online-Durchsuchung zulässig ist. Solange eine Software für die Online-Überwachung (noch) nicht zur Verfügung steht, ist diese Maßnahme nach deutschem Recht zwar unzulässig, allerdings wurde ausdrücklich klargestellt, dass in diesen Fällen eine Online-Durchsuchung in Betracht kommt, wenn deren Voraussetzungen vorliegen.

In der Expertengruppe bestand überdies breite Übereinstimmung, dass die neue Ermittlungsmaßnahme – **von der Eingriffsintensität betrachtet – mit der Überwachung von Nachrichten gemäß § 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 von einer natürlichen Person 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 StPO 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. Neben dem Inhalt der Nachricht soll daher – wie bei der herkömmlichen Telefonüberwachung, bei der in der Praxis zur Gewährleistung verwertbarer und aussagekräftiger Ermittlungsergebnisse eine Auskunft über Daten einer Nachrichtenübermittlung nach § 135 Abs. 2 StPO und eine Überwachung von Nachrichten nach § 135 Abs. 3 StPO gemeinsam angeordnet, bewilligt und durchgeführt werden – z. B. ebenfalls nachvollzogen werden können, wann und zwischen welchen Personen eine Kommunikation erfolgt. 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 Justiz, der dafür auch entsprechende (IT-)Sachverständige heranziehen kann, Protokollierungspflichten 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 Computersystem, z. B. eines Smartphones) ohne Kenntnis der betroffenen Person in Bulgarien, Tschechien, Estland, Spanien, Frankreich, Italien, Polen, Portugal, Rumänien, im Vereinigten Königreich, Kroatien und 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 der Justiz) 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 äußerst 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 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 erfasst wird (siehe Erläuterungen zu Z 12, § 134 Z 3 StPO).

Der deutlichen Abgrenzung der hier vorgeschlagenen Ermittlungsmaßnahme zu jener der Online-Durchsuchung soll 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 überdies, dass nur Nachrichten und Informationen sowie damit im Zusammenhang stehende Daten im Sinn des § 76a StPO und § 92 Abs. 3 Z 4 und 4a TKG überwacht werden dürfen, die über ein Kommunikationsnetz (§ 3 Z 11 TKG) oder einen Dienst der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes) von einer natürlichen Person 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). Ebenfalls nicht enthalten ist die autonome Kommunikation ausschließlich zwischen Endgeräten ohne menschliches Zutun (M2M Kommunikation).

Als weiteres Kriterium ist vorgesehen, dass die Installation eines Programms in einem Computersystem (§ 74 Abs. 1 Z 8 StGB) ohne Kenntnis dessen Inhabers oder sonstiger Verfügungsberechtigter nur zulässig sein soll, um dadurch eine Verschlüsselung beim Senden, Übermitteln oder Empfangen der Nachrichten und Informationen zu überwinden und somit Nachrichten und Informationen (sowie damit im Zusammenhang stehende Daten im Sinn des § 76a StPO und des § 92 Abs. 3 Z 4 und 4a TKG, siehe oben) 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“ soll mit Verweis auf die Begriffsbildung im StGB definiert werden (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 Staatsgrundgesetz über die allgemeinen Rechte der Staatsbürger – StGG, RGBl. Nr. 142/1867).

Die Definition in Z 3a soll darüber hinaus eindeutig klarstellen, 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 (s. § 5 Abs. 1 StPO). 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 der Ermittlungsmaßnahme 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. Beim geplanten Inkrafttreten des § 135a StPO mit 1. April 2020 wird das Bundesministerium für Inneres, das die vorgeschlagene Ermittlungsmaßnahme operativ durchführen und die ermittelten Daten verarbeiten wird, als datenschutzrechtlich Verantwortlicher (vgl. § 36 Abs. 2 Z 8 iVm §§ 46ff DSG idF BGBl. I Nr. 120/2017) für das Überwachungsprogramm ein Verzeichnis von Verarbeitungstätigkeiten führen (vgl. § 4 DSG idF BGBl. I Nr. 120/2017 sowie § 49 DSG idF BGBl. I Nr. 120/2017), mit der Datenschutzbehörde zusammenarbeiten (§ 51 DSG idF BGBl. I Nr. 120/2017) und diese vorher konsultieren (§ 53 DSG idF BGBl. I Nr. 120/2017). Entsprechend der Verpflichtung in § 50 DSG idF BGBl. I Nr. 120/2017 ist jeder Verarbeitungsvorgang in geeigneter Weise so zu protokollieren, dass die Zulässigkeit der Verarbeitung nachvollzogen und überprüft werden kann. Selbstverständlich wird vom Bundesministerium für Inneres als Verantwortlicher auch eine Datenschutz-Folgenabschätzung (§ 52 DSG idF BGBl. I Nr. 120/2017) durchgeführt werden. 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 14, § 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 an höhere Schranken zu binden. Anregungen im Begutachtungsverfahren zu 325/ME 25. GP folgend, sollen (im Bereich des Abs. 1 Z 3) die Zulässigkeitserfordernisse insofern erhöht werden, als nicht mehr an die Zuständigkeit des Landesgerichts als Schöffen- oder Geschworenengericht, sondern vielmehr daran angeknüpft werden soll, dass die Ermittlungsmaßnahme in den Fällen des § 136 Abs. 1 Z 3 StPO (d.h. wenn die Aufklärung eines mit mehr als zehn Jahren Freiheitsstrafe bedrohten Verbrechens, einer Straftat nach §§ 278a bis 278e StGB oder die Aufklärung oder Verhinderung von im Rahmen einer kriminellen Organisation oder einer terroristischen Vereinigung (§ 278a und § 278b StGB) begangenen oder geplanten Verbrechens (§ 17 Abs. 1 StGB) oder die Ermittlung des Aufenthalts des wegen einer der davor genannten Straftaten Beschuldigten ansonsten aussichtslos oder wesentlich erschwert wäre) sowie zur Aufklärung eines mit mehr als fünfjähriger Freiheitsstrafe bedrohten Verbrechens gegen Leib und Leben oder die sexuelle Integrität und Selbstbestimmung ansonsten aussichtslos oder wesentlich erschwert wäre. Zusätzlich muss der Inhaber oder Verfügungsberechtigte des Computersystems, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll, einer solchen Straftat dringend verdächtig sein (§ 135a Abs. 1 Z 3 lit. a StPO) oder es muss auf Grund bestimmter Tatsachen anzunehmen sein, dass eine einer solchen Tat dringend verdächtige Person das Computersystem, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll, benützen oder mit ihm eine Verbindung herstellen werde (§ 135a Abs. 1 Z 3 lit. b StPO). Die Ermittlungsmaßnahme soll daher zur Umsetzung des Art. 20 Abs. 1 iVm Erw 21 der RL Terrorismus (siehe oben) auch der Aufklärung von Straftaten nach §§ 278c bis 278e StGB dienen können.

Rechtzeitig vor Ende der Befristung, also innerhalb von drei Jahren ab ihrem Inkrafttreten soll die Ermittlungsmaßnahme im Hinblick auf den technischen Fortschritt einer Evaluierung unterzogen werden, wobei auch die Zulässigkeitsvoraussetzungen neu zu überdenken sein werden. Zahlreiche Stellungnahmen im Begutachtungsverfahren zu 325/ME 25. GP wiesen nämlich darauf hin, dass die vorgeschlagenen Zulässigkeitsvoraussetzungen zu hoch seien und stattdessen an jene der Überwachung von Nachrichten (vgl. § 135 Abs. 2 StPO) angepasst werden sollten (vgl. etwa die Stellungnahmen der Oberstaatsanwaltschaft Linz, des Amts der Wiener Landesregierung, der Generalprokuratur, des Landesgerichts für Strafsachen Graz und des Bundesministeriums für Finanzen).

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, IMSI- oder 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 ist 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. Ebenso kann in die Software eine laufende Datumsprüfung eingebaut werden, sodass sich die Software bei Erreichen eines bestimmten Datums löscht, auch wenn keine Verbindung mit dem Internet besteht oder durch ein Back-up das Programm auf das Computersystem wiederaufgespielt wird. 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 20, 22, 23 und 26 (§ 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 Ermittlungsmaßnahme soll nur für einen künftigen Zeitraum angeordnet werden dürfen, der überdies zur Erreichung ihres Zwecks voraussichtlich erforderlich ist (**§ 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. Über die bislang vorgesehenen Bestandteile hinaus wird (der bestehenden Praxis folgend) nunmehr über Anregung des Verfassungsdienstes auch ausdrücklich klargestellt, dass Anordnung und gerichtliche Bewilligung aller in §§ 135 bis 136 StPO genannter Ermittlungsmaßnahmen auch eine Information über die Rechte des von der Anordnung oder Bewilligung Betroffenen zu enthalten hat. 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, IMSI- oder 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 Zweifeln an der 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 29 bis 31 (§ 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 im Wege des Programms und jede auf diesem Weg 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 zu 192 ME/ 25. GP 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 34 und 38). Selbstverständlich gelten auch die besonderen Durchführungsbestimmungen des § 145 StPO für die neue Ermittlungsmaßnahme (vgl. die dort normierten Löschungs- und Aufbewahrungspflichten).

Zu Z 32, 34 bis 36 (§ 147 Abs. 1 Z 2a und 5, 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 Computersystemen 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).

Anregungen im Begutachtungsverfahren folgend, soll der Rechtsschutz von Berufsgeheimnisträgern systemkonform erweitert werden: Für die Anordnung und Durchführung einer Ermittlungsmaßnahme nach § 135a StPO, die gegen eine Person gerichtet ist, die gemäß § 157 Abs. 1 Z 2 bis 4 StPO berechtigt ist, die Aussage zu verweigern, soll eine Ermächtigung des Rechtsschutzbeauftragten der Justiz erforderlich sein (§ 144 Abs. 3 StPO). Des Weiteren soll er eine Ermächtigung zu einem Antrag auf Bewilligung der Anordnung einer Überwachung nach § 135a StPO von ausschließlich der Berufsausübung gewidmeten Computersystemen einer der in § 157 Abs. 1 Z 2 bis 4 StPO erwähnten Personen nur erteilen dürfen, wenn – neben den Voraussetzungen des § 144 Abs. 3 StPO – besonders schwerwiegende Gründe vorliegen, die diesen Eingriff verhältnismäßig erscheinen lassen. Auf Grund des Gewichts der mit der Maßnahme verbundenen Grundrechtseingriffe müssen Gründe vorliegen, die die Verhältnismäßigkeit des Eingriffes begründen.

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. Anregungen im Begutachtungsverfahren Rechnung tragend, soll der Rechtsschutzbeauftragte der Justiz im Fall des § 135a StPO die Bestellung eines Sachverständigen durch das Gericht im Rahmen gerichtlicher Beweisaufnahme (§ 104 StPO) und nicht dessen Bestellung durch die Staatsanwaltschaft verlangen können. Da gemäß § 138 Abs. 5 StPO die Zustellung der Anordnung der betreffenden Ermittlungsmaßnahme samt deren gerichtlicher Bewilligung an den Beschuldigten erst nach Beendigung der Maßnahme erfolgt, muss dies auch für die Zustellung der Ausfertigung der Sachverständigenbestellung an den Beschuldigten gelten. Dies entspricht der

grundsätzlichen Funktion und Rolle des Rechtsschutzbeauftragten der Justiz, zu einem Zeitpunkt, in dem die Ermittlungsmaßnahmen für die davon Betroffenen noch geheim sind, bereits auf die Wahrung ihrer Rechte zu achten, indem er die Anordnung der jeweiligen Ermittlungsmethode prüft und die Durchführung begleitend kontrolliert (vgl. *Reindl-Krauskopf* in *Fuchs/Ratz*, WK-StPO § 47a Rz 1 mwN).

Zu Z 37 (§ 148 StPO):

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

Optische und akustische Überwachung von Personen

Zu Z 18, 19, 20, 23 und 35 (§ 136 Abs. 1 Z 3, Abs. 4, § 137 Abs. 1, § 138 Abs. 1 und § 147 Abs. 2 StPO):

In Umsetzung der Vorgaben der RL Terrorismus zur Sicherstellung der Verfügbarkeit wirksamer Ermittlungsinstrumente (Art. 20 und Erw 21 der RL Terrorismus) soll die optische und akustische Überwachung von Personen (§ 136 Abs. 1 Z 3 StPO) nicht nur weiterhin zur Aufklärung eines mit mehr als zehn Jahren Freiheitsstrafe bedrohten Verbrechens oder des Verbrechens der kriminellen Organisation oder der terroristischen Vereinigung (§§ 278a und 278b StGB) sowie zur Ermittlung des Aufenthalts des wegen einer solchen Straftat Beschuldigten zulässig sein, sondern auch **zur Aufklärung** terroristischer Straftaten (§ 278c StGB) und weiterer schwerwiegender Straftaten im Zusammenhang mit terroristischen Aktivitäten, nämlich Terrorismusfinanzierung (§ 278d StGB) und Ausbildung für terroristische Zwecke (§ 278e StGB). Dem Grundsatz der Verhältnismäßigkeit sowie der Art und Schwere der untersuchten Straftaten Rechnung tragend (vgl. Erw 21 der RL Terrorismus) soll die optische und akustische Überwachung nur auf diese mit besonders hoher Strafe bedrohten Straftaten, nicht jedoch für jene Straftaten, die einer geringeren Strafdrohung unterliegen (§ 278f, § 282a StGB), ausgeweitet werden. Damit die Ermittlungsmaßnahme der optischen und akustischen Überwachung von Personen (§ 136 Abs. 1 Z 3 StPO) auch zur Aufklärung dieser Straftaten zur Verfügung steht, werden Verweise auf die §§ 278c bis 278e StGB in § 136 Abs. 1 Z 3 StPO sowie in dessen lit. a aufgenommen.

Im Einklang mit der in der Lehre vertretenen Ansicht soll nunmehr eindeutig klargestellt werden, dass § 136 Abs. 1 Z 3 StPO keine Überwachung zur Verhinderung oder Aufklärung jedweder Straftat ermöglicht, denn die Verhinderung oder Aufklärung bloßer Vergehen vermag den Einsatz dieser Maßnahme nicht zu rechtfertigen (vgl. *Reindl-Krauskopf* in WK-StPO § 136 Rz 20, 22f). Dementsprechend ist auch schon bisher in § 140 Abs. 1 Z 3 StPO vorgesehen, dass Ergebnisse von Ermittlungsmaßnahmen nach § 136 Abs. 1 Z 2 und 3 StPO bei sonstiger Nichtigkeit nur als Beweismittel zum Nachweis eines Verbrechens (§ 17 Abs. 1 StGB) verwendet werden dürfen. Sofern die Ermittlungsmaßnahme der Aufklärung oder Verhinderung von ihm Rahmen einer kriminellen Organisation oder einer terroristischen Vereinigung (§ 278a und § 278b StGB) begangenen oder geplanten Taten dient, soll ausdrücklich angeordnet werden, dass es sich dabei um Verbrechen (§ 17 Abs. 1 StGB) handeln muss. § 136 Abs. 4 zweiter Satz StPO ist konsequenterweise insofern anzupassen, als eine Überwachung nach § 136 Abs. 1 Z 3 StPO zur Verhinderung von im Rahmen einer terroristischen Vereinigung oder einer kriminellen Organisation (§§ 278a und 278b StGB) begangenen oder geplanten Verbrechen (§ 17 Abs. 1 StGB) nur dann zulässig sein soll, wenn bestimmte Tatsachen auf eine schwere Gefahr für die öffentliche Sicherheit schließen lassen.

Diese Ermittlungsmaßnahme ist wegen ihrer Grundrechtsintensität mit dem weitreichendsten Rechtsschutz ausgestattet. Selbstverständlich gelten auch weiterhin die strengen Zulässigkeits- und Begründungsvoraussetzungen (Erfordernis eines entsprechenden dringenden Tatverdachts, vgl. § 136 Abs. 3 Z 1 lit. a oder b StPO). Die Durchführung bedarf einer begründeten Anordnung der Staatsanwaltschaft nach gerichtlicher Bewilligung im Einzelfall (vgl. § 137 Abs. 1 StPO, zu den notwendigen Angaben siehe § 138 Abs. 1 StPO). Damit Beschuldigte und Betroffene umfassend von ihren Rechtsschutzmöglichkeiten Gebrauch machen können, sind ihnen Anordnung und gerichtliche Bewilligung in der Regel unverzüglich nach Beendigung der Maßnahme zuzustellen (vgl. § 138 Abs. 5 StPO) und Einsicht in die Ergebnisse zu gewähren (vgl. § 139 StPO). Diese Regelungen werden flankiert von umfassenden Beweisverwendungsverboten (vgl. § 140 Abs. 1 Z 2 und 3 StPO) und Umgehungsverboten (vgl. § 144 Abs. 3 StPO). Gegen die gerichtliche Bewilligung der Ermittlungsmaßnahme steht das Rechtsmittel der Beschwerde an das Oberlandesgericht zu (vgl. § 87 StPO). Darüber hinaus kann jede Person, die behauptet, im Ermittlungsverfahren durch die Staatsanwaltschaft in einem subjektiven Recht verletzt zu sein, Einspruch wegen Rechtsverletzung an das Gericht erheben (vgl. § 106 StPO). Des Weiteren obliegt dem Rechtsschutzbeauftragen der Justiz die Prüfung und Kontrolle der Anordnung, Genehmigung, Bewilligung und Durchführung dieser Ermittlungsmaßnahme (§ 147 Abs. 1 Z 3 StPO); diese Tätigkeit ist Teil seines jährlich zu erstattenden

Berichtes (vgl. § 47a Abs. 7 StPO). Schließlich haben die Staatsanwaltschaften den Oberstaatsanwaltschaften über derartige Anordnungen jährlich gesonderte Berichte zu erstatten, die die Basis des Gesamtberichts über den Einsatz besonderer Ermittlungsmaßnahmen bilden, der jährlich vom Bundesminister für Verfassung, Reformen, Deregulierung und Justiz dem Nationalrat, dem Datenschutzrat und der Datenschutzbehörde vorgelegt wird (vgl. § 10a StAG). Aus den bisherigen Berichten ergibt sich im Übrigen, dass die Maßnahme der optischen und akustischen Überwachung nach § 136 Abs. 1 Z 3 StPO in der Praxis ohnedies nur äußerst maßvoll eingesetzt wird. Im Jahr 2014 kam es in sechs Verfahren zu einer optischen und akustischen Überwachung nach § 136 Abs. 1 Z 3 StPO („großer Späh- und Lauschangriff"), im Jahr 2015 in insgesamt fünf und im Jahr 2016 in insgesamt zwei Verfahren.

Beschlagnahme von Briefen:

Zu Z 14 (§ 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 (vgl. diesbezügliche Stellungnahmen im Begutachtungsverfahren, etwa die Stellungnahme der Staatsanwaltschaft Eisenstadt zu über das Internet bestellten verbotenen Substanzen nach dem SMG und dem Anti-Doping-Bundesgesetz 2007, die Stellungnahme der Oberstaatsanwaltschaft Wien zu dem immer stärker auftretenden Phänomen des Verkaufs verbotener Gegenstände wie Waffen, Suchtgift oder gefälschter Dokumente über das Internet – insbesondere über das Darknet – und der Lieferung dieser Gegenstände an den Besteller im Postweg, sowie die Stellungnahmen der Oberstaatsanwaltschaft Linz, der Staatsanwaltschaft Wien und des Bundes der österreichischen Frauenvereine). Während § 26 Zollrechts-Durchführungsgesetz – ZollR-DG, BGBl. I Nr. 659/1994, den Zollorganen eine rechtliche Handhabe zur Verfügung stellt, besteht nach der StPO 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 Änderungen haben keine Einschränkung des Rechtsschutzes zur Folge, weil die Beschlagnahme von Briefen auch weiterhin nur auf Anordnung der Staatsanwaltschaft mit gerichtlicher Bewilligung zulässig ist (vgl. § 137 Abs. 1 StPO). Gegen die Beschlagnahme von Briefen stehen die Rechtsmittel der Beschwerde gegen die gerichtliche Bewilligung (§ 87 StPO) und der Einspruch gegen die Anordnung und Durchführung der Beschlagnahme aufgrund der gerichtlichen Bewilligung (§ 106 StPO) zur Verfügung (vgl. *Reindl-Krauskopf*, WK-StPO § 138 Rz 8).

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 – mit Ausnahme der Lokalisierung einer technischen Einrichtung nach § 135 Abs. 2a und der Anlassdatenspeicherung nach § 135 Abs. 2b – nach den §§ 135 bis 136 StPO (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 StPO auch nur für einen solchen künftigen Zeitraum angeordnet werden, der zur Erreichung des Zwecks voraussichtlich erforderlich ist.

Zu Z 21, 26, 29 und 34 (§ 137 Abs. 2, § 138 Abs. 5, § 144 Abs. 3, § 147 Abs. 1 Z 5 StPO):

Wie bereits derzeit bei Eingriffen in das Grundrecht in das Fernmeldegeheimnis (Art. 10a StGG) in Fällen von Ermittlungsmaßnahmen nach § 134 Z 2 und 3 iVm § 135 Abs. 2 und 3 StPO möglich, soll die Aufschiebung der Zustellung aus ermittlungstaktischen Gründen künftig auch bei der Beschlagnahme von Briefen nach § 135 Abs. 1 StPO zulässig sein (§ 138 Abs. 5 StPO). Schließlich wäre der mit der vorgeschlagenen Änderung des § 135 Abs. 1 StPO verbundene Nutzen für die Ermittlungsbehörden 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.

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). Durch die Ergänzung der Verständigungspflichten in § 138 Abs. 5 StPO um die Beschlagnahme von Briefen führt die Streichung des Verweises auf § 111 Abs. 4 StPO auch nicht zu einem Informations- oder Rechtsschutzdefizit (wie dies in einigen Stellungnahmen im Begutachtungsverfahren 325/ME 25. GP befürchtet wurde).

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. Schließlich war der Verweis auf die sinngemäße Anwendung des § 112 StPO wenig passend, weil die Regelung keine Sicherstellung zum Gegenstand hat und der Beschlagnahme von Briefen ohnehin in jedem Fall eine gerichtliche Bewilligung der Anordnung der Staatsanwaltschaft vorausgeht (§ 137 Abs. 1 StPO).

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. Anderes gilt – wie allgemein bei Sicherstellungen und Beschlagnahmen – wenn Briefe nicht Korrespondenz mit dem Berufsgeheimnisträger, sondern andere, bereits bestehende Urkunden oder Schriftstücke enthalten. Solche Unterlagen können nicht bloß durch ihre Übermittlung an einen Berufsgeheimnisträger immunisiert werden (vgl. OGH vom 13 Os 71/13k; EBRV 1058 BlgNR 25. GP, S. 10). Bereits die zitierten Bestimmungen stellen die Wahrung der gesetzlich anerkannten Rechte zur Verschwiegenheit im Rahmen der Beschlagnahme von Briefen ausreichend sicher. Darüber hinaus wird der Rechtschutz für Berufsgeheimnisträger durch Aufnahme auch der Beschlagnahme von Briefen nach § 135 Abs. 1 StPO in § 147 Abs. 1 Z 5 StPO weiter und für den Bereich der Ermittlungsmaßnahmen des 5. Abschnitts des 8. Hauptstücks der StPO systemkonform ausgebaut, indem dem Rechtsschutzbeauftragten der Justiz die Prüfung und Kontrolle der Anordnung, Genehmigung, Bewilligung und Durchführung auch der Ermittlungsmaßnahme nach § 135 Abs. 1 StPO obliegen soll, die gegen eine Person gerichtet ist, die gemäß § 157 Abs. 1 Z 2 bis 4 StPO berechtigt ist, die Aussage zu verweigern (§ 144 Abs. 3 StPO). Des Weiteren soll der Rechtsschutzbeauftragte der Justiz eine Ermächtigung zu einem Antrag auf Bewilligung der Anordnung der Beschlagnahme von Briefen nach § 135 Abs. 1 StPO einer der in § 157 Abs. 1 Z 2 bis 4 StPO erwähnten Personen nur erteilen dürfen, wenn – neben den Voraussetzungen des § 144 Abs. 3 StPO – besonders schwerwiegende Gründe vorliegen, die diesen Eingriff verhältnismäßig erscheinen lassen.

Sonstige Änderungen im 5. Abschnitt des 8. Hauptstücks:

Zu Z 16 und 33 (§ 135 Abs. 3 Z 3 und § 147 Abs. 1 Z 3)

Durch diese Änderungen sollen redaktionelle Versehen behoben werden.

Zu Z 24 und 25 (§ 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 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 ihnen nicht zukommende, weil ausschließlich den Gerichten obliegende, 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 § 153 Abs. 8 BörseG 2018 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. Der Ansicht einiger Betreiber im Begutachtungsverfahren zu 325/ME 25. GP, wonach die Einrichtung von Bereitschaftsdiensten extra zu honorieren wäre, ist zu entgegnen, dass dieser Forderung bereits mit Erlassung der ÜKVO im Jahr 2004 entsprochen wurde, die in § 5 vorsieht, dass für Leistungen an Samstagen, Sonntagen und gesetzlichen Feiertagen sowie an Werktagen zwischen 22.00 und 6.00 Uhr dem Anbieter ein Zuschlag von 100% für die in den Tarifen des 2. Abschnitts enthaltenen Personalkosten

gebührt, es sei denn, dass die Leistungen ohne Nachteil für die Überwachung auch zu einem anderen Zeitpunkt hätten erbracht werden können.

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

Zu Z 34 und 35 (§ 147 Abs. 1 Z 5 und Abs. 2)

Anregungen im Begutachtungsverfahren zu 325/ME 25. GP folgend, soll der Rechtsschutz von Berufsgeheimnisträgern systemkonform erweitert werden: Dem Rechtsschutzbeauftragten der Justiz soll die Prüfung und Kontrolle der Anordnung, Genehmigung, Bewilligung und Durchführung einer Ermittlungsmaßnahme nach § 135 Abs. 1, 2, 2a und 3 StPO sowie einer optischen und akustischen Überwachung von Personen nach § 136 Abs. 1 Z 2 StPO obliegen, die gegen eine Person gerichtet ist, die gemäß § 157 Abs. 1 Z 2 bis 4 StPO berechtigt ist, die Aussage zu verweigern (§ 144 Abs. 3 StPO)

Des Weiteren soll der Rechtsschutzbeauftragte der Justiz eine Ermächtigung zu einem Antrag auf Bewilligung der Anordnung einer Überwachung nach § 135 StPO oder nach § 135a StPO von ausschließlich der Berufsausübung gewidmeten Computersystemen oder nach § 136 Abs. 1 Z 3 StPO in den ausschließlich der Berufsausübung gewidmeten Räumen einer der in § 157 Abs. 1 Z 2 bis 4 StPO erwähnten Personen nur erteilen dürfen, wenn – neben den Voraussetzungen des § 144 Abs. 3 StPO – besonders schwerwiegende Gründe vorliegen, die diesen Eingriff verhältnismäßig erscheinen lassen.

Sonstige Änderungen der StPO:

Zu Z 5 (§ 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 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 der Bestellungsbescheid und das fristauslösende Aktenstück oder dem Privatbeteiligten der seinen Verfahrenshilfeantrag abweisende (rechtskräftige) Beschluss zugestellt werden/wird.

Zu Z 6 (§ 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 7 (§ 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 sechster 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 StPO 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 StPO entsprechend § 99 Abs. 6 sechster 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 38 und 42 (§ 209b Abs. 1, § 514 Abs. 37 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. Entsprechend den mit dem Strafprozessrechtsänderungsgesetz II 2016, BGBl. I Nr. 121/2016, geänderten Bestimmungen zur Kronzeugenregelung soll – wie dort für § 209a und § 209b StPO generell angeordnet – diese Bestimmung mit Ablauf des 31. Dezember 2021 wieder außer Kraft treten.

Zu Z 39 (§ 221 Abs. 1 StPO):

Artikel 8 Abs. 2 lit. a der 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 Verfassung, Reformen, Deregulierung und 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 41 (§ 430 Abs. 5 StPO):

Nach Artikel 8 Abs. 1 lit. b der RL Unschuldsvermutung können die Mitgliedstaaten vorsehen, dass eine Verhandlung, die zu einer Entscheidung über die Schuld oder Unschuld eines Verdächtigen oder einer beschuldigten Person führen kann, in seiner bzw. ihrer Abwesenheit durchgeführt werden kann, sofern der Verdächtige oder die beschuldigte Person, nachdem er bzw. sie über die Verhandlung unterrichtet wurde, von einem bevollmächtigten Rechtsanwalt vertreten wird, der entweder von dem Verdächtigen oder der beschuldigten Person oder vom Staat bestellt wurde. Im Verfahren zur Unterbringung in einer Anstalt für geistig abnorme Rechtsbrecher nach § 21 Abs. 1 StGB (vgl. §§ 429ff StPO) kann die Hauptverhandlung in Abwesenheit des Betroffenen durchgeführt werden, soweit der Zustand des

Betroffenen eine Beteiligung an der Hauptverhandlung innerhalb angemessener Frist nicht gestattet oder von einer solchen Beteiligung eine erhebliche Gefährdung seiner Gesundheit zu besorgen wäre (§ 430 Abs. 5 StPO). Da im gesamten Verfahren zur Unterbringung in einer Anstalt für geistig abnorme Rechtsbrecher nach § 21 StGB notwendige Verteidigung besteht (vgl. § 61 Abs. 1 Z 2 StPO), der Betroffene also durch einen Verteidiger vertreten sein muss, wobei ihm bei finanzieller Bedürftigkeit ein Verfahrenshilfeverteidiger beizugeben ist (vgl. § 61 Abs. 2 und 3 StPO), ist das von Art. 8 Abs. 1 lit. b der RL Unschuldsvermutung normierte Kriterium der Vertretung durch einen Rechtsanwalt jedenfalls erfüllt. Im Hinblick auf das Erfordernis „nachdem er bzw. sie über die Verhandlung unterrichtet wurde“ sieht § 430 Abs. 5 vierter Satz StPO vor, dass ein Beschluss, die Hauptverhandlung zur Gänze in Abwesenheit des Betroffenen durchzuführen, nur gefasst werden darf, nachdem sich der Vorsitzende vom Zustand des Betroffenen überzeugt und mit ihm gesprochen hat. Es ist davon auszugehen, dass dieses Gespräch des Vorsitzenden mit dem Betroffenen eine „Unterrichtung über die Verhandlung“ des Betroffenen miteinschließt. Dennoch soll zur Klarstellung, dass der Betroffene jedenfalls im Sinne des Artikel 8 Abs. 1 lit. b der RL Unschuldsvermutung über die Verhandlung zu unterrichten ist, in § 430 Abs. 5 StPO nach dem Wort „nachdem“ die Wendung „der Betroffene vom Termin der Hauptverhandlung verständigt wurde und“ eingefügt werden.

Zu Z 42 (§ 514 Abs. 37 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 43 (§ 516a Abs. 7 und 8 StPO):

Durch die genannte Änderung werden die RL Terrorismus und die RL Unschuldsvermutung im nationalen Recht umgesetzt.

Zu Artikel 2 (Änderung des Staatsanwaltschaftsgesetzes):

Z 1 bis 3 (§ 10a Abs. 1 und 2, § 42 StAG)

Zunächst sollen im Bereich des staatsanwaltschaftlichen Berichtswesens bei der Überwachung verschlüsselter Nachrichten dieselben Vorkehrungen wie im Fall einer optischen und akustischen Überwachung von Personen nach § 136 Abs. 1 Z 2 und 3 StPO getroffen werden. Die Staatsanwaltschaften sollen daher den Oberstaatsanwaltschaften bereits über die beabsichtigte Anordnung dieser Maßnahme berichten (Abs. 1).

Darüber hinaus wird die Aufnahme der Ermittlungsmaßnahme der Überwachung verschlüsselter Nachrichten (§ 135a StPO) in den vom Bundesministerium für Verfassung, Reformen, Deregulierung und Justiz auf Grundlage der Berichte der Staatsanwaltschaften und des Berichtes des Rechtsschutzbeauftragten der Justiz alljährlich dem Nationalrat, dem Datenschutzrat und der Datenschutzbehörde erstatteten Gesamtbericht über den Einsatz besonderer Ermittlungsmaßnahmen vorgeschlagen. Im Begutachtungsverfahren geäußerten Forderungen nach einer „Gesamtüberwachungsrechnung“ ist daher mit Hinweis auf den jährlichen Gesamtbericht über den Einsatz besonderer Ermittlungsmaßnahmen sowie auf die jährlichen Sicherheitsberichte der Bundesregierung über die Tätigkeit der Strafjustiz zu entgegnen. Diese Berichte sollen insbesondere auch als Grundlage für die angekündigte Evaluierung der Ermittlungsmaßnahme der Überwachung verschlüsselter Nachrichten vor Ablauf ihrer Befristung herangezogen werden.

Die Änderungen im StAG sollen zum gleichen Zeitpunkt wie die korrespondierenden Regelungen der StPO in Kraft (1. April 2020) und außer Kraft (mit Ablauf des 31. März 2025) treten.

Zu Artikel 3 (Änderung des Telekommunikationsgesetzes 2003):

Z 1 bis 5 (§ 99 Abs. 2, § 102c, § 109 Abs. 3 und § 137 Abs. 9 TKG)

Da in § 99 Abs. 2 TKG jene Fälle normiert sind, in denen Verkehrsdaten nicht zu löschen sind (vgl. § 99 Abs. 2 Z 1 bis 3 TKG, z. B. Einspruch gegen die Abrechnung, Nichtbegleichung der Rechnung, Einleitung eines Verfahrens über die Höhe der Entgelte), soll diese Bestimmung um einen Verweis auf die Anordnung der Staatsanwaltschaft nach § 135 Abs. 2b StPO in Form der neu einzufügenden Z 4 erweitert werden. Die näheren Voraussetzungen dieser Ermittlungsmaßnahme sollen systemkonform nicht im TKG festgelegt werden, sondern dem Materiengesetz, konkret der StPO, vorbehalten werden. Dabei soll besonderes Augenmerkt auf die Judikatur des EuGH, insbesondere die Entscheidung Tele2 Sverige gelegt werden, wie dies in § 135 Abs. 2b StPO und den Begleitbestimmungen (siehe oben zu Artikel 1) vorgesehen ist.

Ein allfälliger späterer Zugriff auf solcherart gemäß § 99 Abs. 2 Z 4 TKG nicht gelöschte Daten bedarf keiner eigenen Rechtsgrundlage im TKG, weil der Zugriff bereits durch die bereits derzeit zulässige Verarbeitung nach § 99 Abs. 5 Z 1 und 2 TKG geregelt ist.

Besondere Protokollierungs- und Auskunftspflichten sind nicht erforderlich, weil es sich bei der Anlassdatenspeicherung nach § 135 Abs. 2b StPO gerade nicht um eine neue Form der Vorratsdatenspeicherung, sondern vielmehr um eine Anordnung der Staatsanwaltschaft in einem konkreten Einzelfall bei begründetem Anfangsverdacht (§ 1 Abs. 3 StPO) zum Absehen von der Löschung bereits vorhandener (und somit ohnedies bereits gespeicherter) Daten handelt. Statistischen Anforderungen kann zweckmäßigerweise mit Einführung von Schrittcodes in der Verfahrensautomation Justiz entsprochen werden. Darüber hinaus sind entsprechende Löschungsverpflichtungen in der StPO vorgesehen (siehe oben Artikel 1), auf die ohnehin verwiesen wird.

Da § 102c TKG die Speicherung der Vorratsdaten zum Gegenstand hat, obwohl die Regelungen über die Vorratsdatenspeicherung bereits mit Erkenntnis des VfGH vom 27. Juni 2014 (Kundmachung in BGBl. I Nr. 44/2014) aufgehoben worden sind, soll diese Bestimmung nunmehr aufgehoben werden.

Die vorgeschlagenen Verwaltungsübertretungen sollen in § 109 Abs. 3 TKG (Geldstrafen bis zu EUR 37.000,-) geregelt werden, um eine entsprechende Werterelation zu gewährleisten, weil ein Verstoß gegen § 99 Abs. 5 TKG (unzulässige Auskunft oder Verarbeitung von Verkehrsdaten) ebenfalls bis zu EUR 37.000,- geahndet werden kann (§ 109 Abs. 3 Z 21 TKG). Wegen der besonderen Bedeutung und Vertraulichkeit der übermittelten Daten soll eine Übermittlung in nicht verschlüsselter Form verwaltungsstrafrechtlich geahndet werden können. Die Verpflichtung, Verkehrsdaten, Standortdaten und Stammdaten, welche die Verarbeitung von Verkehrsdaten erfordern, nach den Bestimmungen der StPO, des SPG sowie des PStSG (Polizeiliches Staatsschutzgesetz, BGBl. I Nr. 5/2016) in verschlüsselter Form zu übermitteln, ist bereits in § 94 Abs. 4 TKG normiert. Weiters soll auch eine neue Verwaltungsstrafbestimmung eingeführt werden und mit einer Geldstrafe bis zu EUR 37.000,- zu bestrafen sein, wer entgegen § 99 Abs. 2 Z 4 TKG die in einer Anordnung einer Staatsanwaltschaft nach § 135 Abs. 2b StPO bezeichneten Daten nicht löscht oder nach Beendigung der Verpflichtung zum Absehen von der Löschungsverpflichtung nicht löscht.