Entwurf

Erläuterungen

I. Allgemeiner Teil

Der vorliegende Entwurf schlägt vor, die Anordnung der Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, als neue Ermittlungsmaßnahme für den Bereich schwerster Kriminalität (organisierte Kriminalität und Terrorismus) in die StPO einzuführen.

Mit gemeinsamem Vortrag an den Ministerrat vom 17. Oktober 2007 zum Thema „Erweiterung des Instrumentariums zur Bekämpfung schwerer, organisierter und terroristischer Kriminalitätsformen („Online-Durchsuchung“)“ kündigten die damalige Bundesministerin für Justiz Dr. Maria Berger und der damalige Bundesminister für Inneres Günther Platter die Einsetzung einer Arbeitsgruppe mit dem Ziel der 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 an.

Gegenstand des Ministerratsvortrages war die Durchführung einer „Online-Durchsuchung“. Darunter wurde der Einsatz von Programmen verstanden, die unbemerkt auf einem Computer installiert werden und es ermöglichen, den Inhalt gespeicherter Daten auszulesen, den E-Mail-Verkehr zu überwachen oder das Aufsuchen bestimmter Internetseiten zu ermitteln, ohne dass es der Inhaber merkt.

Dieser interdisziplinären Arbeitsgruppe unter Leitung von o. Univ. Prof. Dr. Bernd-Christian Funk gehörten Vertreterinnen und Vertreter des Bundesministeriums für Justiz, des Bundesministeriums für Inneres, des Bundesministeriums für Landesverteidigung, des Bundesministeriums für Verkehr, Innovation und Technologie, des Bundeskanzleramt-Verfassungsdienstes, der Bundesrechenzentrum GmbH, der ISPA Internet Service Providers Austria, der Höchstgerichte, der Rechtswissenschaft sowie Standesvertreter der Richter und Staatsanwälte und der Chief Information Officer – CIO des Bundes an.

Nach intensiver viermonatiger Tätigkeit legte die Arbeitsgruppe im März 2008 einen umfassenden Schlussbericht vor, in dem sie zum Ergebnis kam, dass eine derartige Ermittlungsmaßnahme nach geltendem Recht nicht zulässig ist. Gleichzeitig wurden Überlegungen vorgezeichnet, wie die gesetzliche Grundlage für eine solche Maßnahme und die Sicherungs- und Rechtsschutzmaßnahmen ausgestaltet sein sollten.

Der nunmehr vorgelegte Entwurf baut auf den rechtlichen Überlegungen auf, beschränkt sich im Gegensatz dazu allerdings auf eine Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden. Da er somit einen weitaus geringeren Anwendungsbereich umfasst, ist nicht die Gesamtheit der für eine Online-Durchsuchung als notwendig angedachten Sicherungsmaßnahmen erforderlich.

Seit Abschluss der Arbeitsgruppe ist es aufgrund des technischen Fortschrittes zu einer breiten Verwendung neuer Kommunikationsmittel und generell zu einer Änderung des Kommunikationsverhaltens gekommen. Vermehrt werden anstelle herkömmlicher Telefonie und Kurznachrichten internetbasierte Kommunikationsmöglichkeiten verwendet, die auch eine Verschlüsselung der übertragenen Daten ermöglichen (WhatsApp, Skype). Der Umstand, dass sich Täter zunehmend bewusst dieser Kommunikationsmöglichkeiten bedienen, macht es notwendig, die Strafverfolgungsbehörden mit adäquaten Möglichkeiten auszustatten, um mit diesen technischen Entwicklungen zumindest annähernd Schritt zu halten. Eine Anpassung der Ermittlungsmethoden an die

technischen Entwicklungen und das geänderte Kommunikationsverhalten erscheint auch deshalb indiziert, weil den verfügbaren Informationen zufolge die Kommunikation der Attentäter von Paris im November 2015 nicht auf dem Wege der Kommunikation über Kurznachrichten oder Sprachtelefonie, sondern vielmehr internetbasiert über Spielekonsolen erfolgte.

Zur Ermöglichung einer wirksamen Strafverfolgung unter größtmöglicher Wahrung der Grundrechte und der Verhältnismäßigkeit ist daher die Einführung einer neuen Ermittlungsmaßnahme zur Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, notwendig. Sie soll jedoch auf den Bereich schwerster Kriminalität (organisierte Kriminalität und Terrorismus) beschränkt bleiben.

Es wird daher nunmehr vorgeschlagen, die bereits vorhandenen Ermittlungsmaßnahmen um die Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, zu ergänzen und damit auch neue Formen der Kommunikation unter Verwendung von Verschlüsselungssoftware zu erfassen. Im Einzelfall sollen durch diese Maßnahme Kommunikationsinhalte auf dem von der Maßnahme betroffenen Gerät noch vor einer eventuellen Verschlüsselung bzw. nach einer allfälligen Entschlüsselung überwacht und die Kommunikationspartner der Person, gegen die sich die Überwachung richtet, und somit gegebenenfalls auch Mittäter identifiziert werden können. Die Ermittlung von sonst auf dem Computersystem gespeicherten Daten ist – im Gegensetz zu dem von der oben erwähnten Arbeitsgruppe verfassten Schlussbericht – ausdrücklich nicht erfasst.

Der Entwurf nimmt auch Bezug auf die Kritik des VfGH in seinem Erkenntnis (27.6.2014, G 47/2012, G 59/2012, G 62/2012, G 70/2012, G 71/2012) über die Aufhebung der Regelungen über die Vorratsdatenspeicherung in TKG, SPG und StPO, wonach bei jenen Bestimmungen nicht sichergestellt worden sei, dass die Auskunft über Vorratsdaten nur im Fall eines Verdachts der Begehung schwerer Straftaten angewendet werden könne. Der Vorschlag sieht daher vor, dass die Regelungen über die Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, nur bei Vorliegen eines dringenden Verdachts der Begehung schwerster Straftaten zur Anwendung gelangen (siehe im Folgenden). Aufgrund der Eingriffsintensität orientiert sich der Entwurf an den Voraussetzungen und Regelungen der optischen und akustischen Überwachung von Personen (sogenannter „Lauschangriff“). Vorgeschlagen werden folgende Voraussetzungen:

- Gleicher Anwendungsbereich wie bei der optischen und akustischen Überwachung von Personen unter Verwendung technischer Mittel gemäß § 136 Abs. 1 Z 3 StPO, d.h.: Notwendigkeit 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) oder zur Aufklärung oder Verhinderung von im Rahmen einer solchen Organisation oder Vereinigung begangener oder geplanter strafbarer Handlungen oder zur ansonsten aussichtslosen oder wesentlich erschwerten Ermittlung des Aufenthalts des wegen einer solchen Straftat Beschuldigten. Zusätzlich muss die Person, gegen die sich die Überwachung richtet, des mit mehr als zehn Jahren Freiheitsstrafe bedrohten Verbrechens nach § 278a oder § 278b StGB dringend verdächtig sein oder auf Grund bestimmter Tatsachen anzunehmen sein, dass ein Kontakt einer solcherart dringend verdächtigen Person mit der Person hergestellt werde, gegen die sich die Überwachung richtet;
- Anordnung der Staatsanwaltschaft, die vor ihrer Durchführung durch das Gericht zu genehmigen ist und der Kontrolle des Rechtsschutzbeauftragten unterliegt;
- besondere Anordnung der Staatsanwaltschaft für den Fall, dass ein Eindringen in eine Wohnung erforderlich ist, die im Einzelnen einer Genehmigung durch das Gericht bedarf;
- strenge Beachtung des Verhältnismäßigkeitsgrundsatzes;
- Kontrolle der Durchführung durch Rechtsschutzbeauftragten der Justiz;
- Verständigung sämtlicher Personen, deren Daten ermittelt wurden und umfängliche Beschwerdemöglichkeiten;
- strenge Vernichtungsregelungen von unzulässig ermittelten oder für die Untersuchung nicht bedeutsamen Daten sowie Beschränkung der Verwertbarkeit von Zufallsfunden;
- eine verschuldensunabhängige Haftung des Bundes für Schäden, die durch eine Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, verursacht wurde (§ 148 StPO);
- Aufnahme in den jährlichen Bericht über besondere Ermittlungsmaßnahmen, der Nationalrat, Datenschutzrat und Datenschutzbehörde vorzulegen ist.

Das Bundesministerium für Justiz berichtet dem Parlament jährlich über den Einsatz dieser Ermittlungsmaßnahme (vgl. Gesamtbericht über den Einsatz besonderer Ermittlungsmaßnahmen). 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 2012 kam es in zwei Verfahren zu einer optischen und akustischen Überwachung nach § 136 Abs. 1 Z 3 StPO („großer Späh- und Lauschangriff"), im Jahr 2013 in insgesamt drei Verfahren. Der sog. „kleine Späh- und Lauschangriff" nach § 136 Abs. 1 Z 2 StPO gelangte im Jahr 2012 in drei Verfahren, im Jahr 2013 in einem Verfahren und im Jahr 2014 in 6 Verfahren zur Anwendung. Es ist daher zu erwarten, dass auch die Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, ebenso maßvoll angewendet werden wird.

Allgemeines zum Vorschlag:

Die Überwachung von Nachrichten wird in §§ 134 Z 3, 135 Abs. 2 StPO geregelt. Sie umfasst das Ermitteln von Nachrichten, die über ein Kommunikationsnetz (§ 3 TKG) oder einen Dienst der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes) übermittelt werden und erfasst grundsätzlich auch internetbasierte Telekommunikation. Tatsächlich lässt sich eine Veränderung des Kommunikationsverhaltens erkennen, sodass sich laufend mehr Personen internetbasierter Dienste wie WhatsApp oder Skype anstelle der „klassischen" Telefonie und des Short Messaging Service (SMS) bedienen, die (v.a. im Fall der Nutzung von WLAN) eine kostengünstige Alternative darstellen. Darüber hinaus werden Daten oftmals über Cloud-Speicher wie z. B. iCloud oder Dropbox ausgetauscht, ohne dass es zu einer „klassischen" Nachrichtenübertragung kommt.

Bei vielen internetbasierten Diensten besteht die Möglichkeit, die zu übertragenden Daten zu verschlüsseln. Im Fall der Verschlüsselung ist es anderen Personen nicht möglich, vom Inhalt der Kommunikation Kenntnis zu erlangen; dies hat insbesondere den Nachteil, dass auch Strafverfolgungsbehörden mit den bestehenden gesetzlichen Möglichkeiten eine Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, nicht möglich ist.

Auch eine Mitwirkung des Betreibers würde eine Überwachung nicht möglich machen, weil die Verschlüsselung unmittelbar zwischen den an der Kommunikation beteiligten Computersystemen erfolgt und in der Regel auch der jeweilige Betreiber nicht über den für eine Entschlüsselung erforderlichen Schlüssel verfügt. Der Umstand der lückenhaften Überwachungsmöglichkeiten wird daher zunehmend von Beschuldigten genützt, um gezielt einer Überwachung zu entgehen, wenn diese die Befürchtung haben, Subjekt einer Überwachung zu werden. Eine Überwachung dieser Kommunikationsformen ist derzeit lediglich möglich, wenn eine optische und akustische Überwachung im Rahmen der strengen Voraussetzungen der §§ 136 ff StPO angeordnet werden kann, was jedoch einen weitaus schwereren Grundrechtseingriff für den Überwachten mit sich brächte, weil davon nicht nur die im Wege des betreffenden Computersystems übermittelten Nachrichten überwacht werden.

Internetbasierte Kommunikation wird oft zum Nachrichtenaustausch mit Personen im Ausland genutzt, was insbesondere in Ermittlungsverfahren wegen der (versuchten) Beteiligung an einer terroristischen Vereinigung nach § 278b Abs. 2 StGB und wegen Ausbildung für terroristische Zwecke nach § 278e StGB von großer ermittlungstechnischer Bedeutung ist, befinden sich doch die „Terrorcamps" in den Kampfgebieten selbst (Syrien, Afghanistan, …) oder deren Nachbarstaaten. Die Sammlung von stichhaltigem Beweismaterial, das eine (geplante) Reise ins Ausland zur Beteiligung an einer terroristischen Vereinigung („foreign fighters") und terroristischen Ausbildungen belegt, kann von den Strafverfolgungsbehörden derzeit nur schwer bewerkstelligt werden, weil die Durchführungen von Ermittlungen im Wege von Rechtshilfeersuchen, z. B. nach Syrien, nahezu unmöglich ist. Wie bei den jüngsten Anschlägen offenkundig wurde, werden diese Kommunikationswege aber auch zur Vorbereitung terroristischer Straftaten im europäischen Raum und zur Koordinierung von Tätergruppierungen verwendet.

Die Bedrohung durch terroristische Straftaten (§§ 278b bis 278f StGB) in Österreich spiegelt sich auch sehr deutlich in der Zahl der von der Staatsanwaltschaft eingeleiteten Ermittlungsverfahren wieder: während die Anzahl der Verfahren zuvor noch 75 (2012) bzw. 62 (2013) betrug, erhöhte sie sich im Jahr 2014 beinahe um das Doppelte im Vergleich zum Vorjahr und lag bei 115. Im Jahr 2015 sind bei den Staatsanwaltschaften 200 Verfahren wegen Beteiligung an einer terroristischen Vereinigung nach § 278b StGB angefallen, 49 Anklagen wegen § 278b StGB wurden eingebracht. Bis März 2016 sind bereits 30 Verfahren angefallen, 8 Anklagen wurden eingebracht; es ist daher auch in diesem Jahr mit einem massiven Anstieg der Verfahren wegen terroristischer Straftaten zu rechnen.

Im Vergleich zum vorliegenden nationalen Vorschlag sei darauf hingewiesen, dass das Bundesverfassungsgericht in Deutschland sogar eine – hier gar nicht geplante – Online-Durchsuchung selbst für präventive Zwecke nicht für ausgeschlossen hält (BVerfG 27.02.2008 1 BvR 370/07, 1 BvR 595/07). Auch die Bestimmung des § 20k des deutschen BKA-G („Verdeckter Eingriff in informationstechnische Systeme") regelt einen verwandten Eingriff bereits im Bereich der

sicherheitspolizeilichen Befugnisse, wonach das Bundeskriminalamt ohne Wissen des Betroffenen mit technischen Mitteln in vom Betroffenen genutzte informationstechnische Systeme eingreifen und aus ihnen Daten erheben darf, wenn bestimmte Tatsachen die Annahme rechtfertigen, dass eine Gefahr vorliegt für

Leib, Leben oder Freiheit einer Person oder

solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.

Eine Maßnahme nach Satz 1 ist danach auch zulässig, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass ohne Durchführung der Maßnahme in näherer Zukunft ein Schaden eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für eines der in Satz 1 genannten Rechtsgüter hinweisen. Die Maßnahme darf nur durchgeführt werden, wenn sie für die Aufgabenerfüllung nach § 4a erforderlich ist und diese ansonsten aussichtslos oder wesentlich erschwert wäre.

II. Besonderer Teil

Zu Artikel I (Änderungen der StPO)

Zu Z 1 bis 3 (Inhaltsverzeichnis und Überschrift des 5. Abschnittes des 8. Hauptstückes der StPO):

Diese Änderungen umfassen Anpassungen an den Begriff der neuen Ermittlungsmaßnahme.

Zu Z 4 und 5 (§ 134 Z 4a und 5 StPO):

Der Begriff „Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden“ umfasst ausschließlich die Ermittlung von Nachrichten und sonstigen Daten (§ 74 Abs. 2 StGB), die im Wege eines Computersystems (§ 74 Abs. 1 Z 8 StGB) übermittelt und empfangen werden, durch direkte Installation eines Überwachungsprogramms im Computersystem. Der Begriff „Nachricht“ bezeichnet den Gedankeninhalt der Mitteilung, also die Inhaltsdaten der Kommunikation (*Lewisch* in WK^2 StGB § 119 Rz 9a). Umfasst sind darüber hinaus auch sonstige Daten (§ 74 Abs. 2 StGB), somit personenbezogene und nicht personenbezogene Daten und Programme, die an ein anderes Computersystem übertragen oder von einem solchen empfangen werden, wobei es auf einen gedanklichen Inhalt nicht ankommt. Daten sind somit auch der Gedankeninhalt eines E-Mails ebenso wie die bloße Zahlenabfolge, die einen PIN-Code, ein Passwort oder die Kreditkartennummer beschreibt (*Reindl-Krauskopf* in WK^2 StGB § 119a Rz 8). Die Übermittlung kann in unterschiedlicher Form erfolgen, z. B. als Sprache („Voice over IP“), als Text- oder Video-Chat, als E-Mail Korrespondenzen oder durch Hoch- und Herunterladen von Dokumenten in eine bzw. aus einer Cloud.

Da die meisten dieser Übertragungsmöglichkeiten durch Verschlüsselung gesichert werden können, ermöglicht auch eine Einbindung der Betreiber der jeweiligen Dienste, wie sie bei der Überwachung von Nachrichten in § 138 Abs. 2 StPO vorgesehen ist, keinen Zugriff auf die unverschlüsselten Daten, weil diese in der Regel keinen Zugriff auf den zur Entschlüsselung erforderlichen geheimen Schlüssel haben. Zur Überwachung dieser Kommunikationsformen ist es daher notwendig, ein Überwachungsprogramm direkt auf dem Computersystem zu installieren, mit dem ein Zugriff auf die zu übertragenden Daten vor und die empfangenen Daten nach der Verschlüsselung möglich ist.

Der Begriff „Computersystem“ wird in enger Anlehnung an die Begriffsbildung des StGB definiert (vgl. § 74 Abs. 1 Z 8, Abs. 2, §§ 118a und 119a StGB). 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 (straf)rechtswidrigen Eingriff handelt. 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.).

Die Definition in Z 4a stellt darüber hinaus eindeutig klar, dass im Hinblick auf die unterschiedlichen Techniken zur Durchführung einer solchen Überwachung lediglich die Verwendung einer Überwachungssoftware zulässig sein soll. Andere technische Möglichkeiten, wie z. B. das Auffangen elektromagnetischer Strahlungen, der Einbau von Hardware-Komponenten in das Computersystem (z. B. eines „Keyloggers“) sind nicht zulässig. Die Regelung steht freilich nicht der Sicherstellung eines

Computersystems nach §§ 109 Z 1, 110 Abs. 1 Z 1 StPO und der Auswertung der darin gespeicherten Daten entgegen.

Durch die Einführung dieser neuen Ermittlungsmethode wird weiters vorgeschlagen, auch die Definition des Ergebnisses in § 134 Z 5 StPO anzupassen, um auch die Ergebnisse der Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, zu erfassen.

Zu Z 6 (§ 136a StPO):

Mit dieser Bestimmung sollen die Zulässigkeitsvoraussetzungen der vorgeschlagenen Ermittlungsmaßnahme festgelegt werden, die sich zunächst an den Voraussetzungen der optischen und akustischen Überwachung orientieren. Zwar ist die Maßnahme von ihrer Natur her eher mit der Überwachung von Nachrichten (§§ 134 Z 3, 135 Abs. 2 StPO) zu vergleichen, die geringere Zulässigkeitsschranken vorsieht, doch wird für die Durchführung der hier vorgeschlagenen Überwachung oft ein Eindringen in vom Hausrecht geschützte Räumlichkeiten (Abs. 2) erforderlich sein, sodass eine erhöhte Eingriffsintensität vorliegt, weshalb die Voraussetzungen zur Anordnung und Durchführung einer optischen und akustischen Überwachung vorliegen müssen. Es wird darüber hinaus vorgeschlagen (Abs. 2), 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) 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 geregelt werden.

Die Installation der Überwachungssoftware kann grundsätzlich durch zwei, sich im Installationsablauf unterscheidende Verfahren durchgeführt werden, wobei der eindeutigen Zuordnung des Zielsystems zur Zielperson vor und während der Maßnahme besondere Bedeutung zukommt, weshalb ausschließlich eine Installation durch physischen Zugriff auf das Computersystem, nicht jedoch eine remote-Installation der Überwachungssoftware zulässig sein soll.

Zur Sicherstellung der Verhältnismäßigkeit der Maßnahme sieht Abs. 3 weitere einschränkende Zulässigkeitsvoraussetzungen vor, die über die optische und akustische Überwachung hinaus gehen: Das von den Ermittlungsbehörden zum Einsatz gelangende Überwachungsprogramm muss gewährleisten, dass ausschließlich Daten ermittelt werden, die im Wege des Computersystems empfangen oder übermittelt werden, sowie mit dieser Übertragung in unmittelbarem Zusammenhang stehende Daten. Dies umfasst sowohl die übertragene Nachricht, Protokolldateien der für diese Übertragung verwendeten Programme (z. B. Chat-Logs) als auch die Möglichkeit der Identifizierung der Kommunikationspartner jener Person, gegen die sich die Überwachung richtet. Account-Namen oder –Bezeichnungen lassen oftmals keinen Rückschluss auf deren Benutzer zu, allerdings sind die Daten, die Rückschlüsse auf dessen Namen oder andere Identifizierungsmerkmale ermöglichen, in vielen Fällen in Adressbüchern und Kontaktverzeichnissen der jeweiligen Anwendung gespeichert; durch einen Zugriff auf diese Adressbücher und Kontaktverzeichnisse (Skype, WhatsApp usw.) soll eine Identifizierung des Benutzers ermöglicht werden. Unter einem solchen Zugriff ist allerdings keinesfalls eine Durchsuchung des Computersystems nach weiteren Daten zur Identifizierung einer Person oder sonstiger im Computersystem gespeicherter oder verarbeiteter Daten im Sinne einer „Online-Durchsuchung“ zu verstehen.

Darüber hinaus muss nach Beendigung der Ermittlungsmaßnahme sichergestellt sein, dass die Überwachungssoftware dauerhaft funktionsunfähig oder ohne dauerhafte Beschädigung oder Beeinträchtigung des Computersystems und der in ihm gespeicherten Daten entfernt wird (vgl. im Folgenden die Erläuterungen zu §§ 145, 147 StPO). Schließlich dürfen auch an dritten Computersystemen keine Schädigungen oder dauerhaften Beeinträchtigungen bewirkt werden.

Zu Z 7 bis 10 (§§ 137 Abs. 1 und 3, 138 Abs. 1 und 5 StPO):

Es wird vorgeschlagen, die übrigen Bewilligungsvoraussetzungen ebenso anzugleichen: Das Eindringen in vom Hausrecht geschützte Räume soll im Einzelnen einer gerichtlichen Bewilligung unterliegen (§ 137 Abs. 1 StPO); überdies soll die Maßnahme nur für einen künftigen oder vergangenen Zeitraum angeordnet werden dürfen, der zur Erreichung des Zweckes voraussichtlich erforderlich ist (§ 137 Abs. 3 StPO). Es versteht sich von selbst, dass die Anordnung der Überwachung für einen vergangenen Zeitraum eine rechtmäßige Bewilligung voraussetzt, die nachträgliche Legitimierung eines ohne Anordnung und Bewilligung vorgenommenen Einsatzes wird dadurch nicht ermöglicht. 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 (§ 138 Abs. 5 StPO). Klarzustellen ist, dass in den

Rechtsmittelbelehrungen auch ein Hinweis auf die Möglichkeit der Geltendmachung von Ersatzansprüchen nach § 148 StPO aufzunehmen ist.

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 Anordnung und gerichtliche Bewilligung aufzunehmen sind. Während § 136a Abs. 1 StPO die Zulässigkeitsvoraussetzungen für die in § 134 Z 4a StPO definierte Ermittlungsmaßnahme der Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, 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 § 136a Abs. 1 StPO daher nicht zwingender Natur sind, müssen sie lediglich soweit wie möglich bzw. als zur Durchführung erforderlich angegeben werden (vgl. OGH 5.3.2015, 12 Os 93/14i (12 Os 94/14m)).

Das Computersystem, das überwacht werden soll, ist in einer Anordnung und gerichtlichen Bewilligung einer Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, 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) an, so wird dieses anzuführen sein.

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

Zu Z 11 (§ 140 Abs. 1 Z 4 StPO):

Die Zulässigkeit der Verwertung von Zufallsfunden soll sich an den strengen Zulässigkeitserfordernissen für die Anordnung bzw. Bewilligung dieser Ermittlungsmaßnahme orientieren.

Zu Z 12 bis 16 (§§ 144 Abs. 3, 145 Abs. 3 und 4, 147 Abs. 1 bis 3a StPO):

Während § 145 Abs. 3 StPO nur um die neue Ermittlungsmaßnahme zu ergänzen wäre, soll mit dem neuen Abs. 4 die Authentizität und Verlässlichkeit der ermittelten Daten – ein wesentlicher Aspekt im Falle einer Anklageerhebung – sichergestellt werden. Von besonderer Bedeutung ist dabei die Nachvollziehbarkeit der Eingriffe durch den behördlichen Zugang und jede nachträgliche Veränderung an der installierten Software durch geeignete Protokollierung. Dabei muss technisch gewährleistet werden, dass es durch die Durchführung der Überwachung zu keiner über die Installation der Überwachungssoftware hinausgehenden Veränderung der ursprünglich am Computersystem vorhandenen Daten gekommen ist. Zu diesem Zweck sollen Installations-, Übermittlungs-, Änderungs- und Deinstallationsprotokolle zu führen sein. Bei der Übertragung der Daten sind Prüfsummen zu bilden, um zu gewährleisten, dass Datenpakete im Quell- und Zielsystem ident sind. Mit diesen Maßnahmen soll sichergestellt werden, dass alle Prozessschritte definiert und jederzeit überprüfbar sind, wobei die konkrete Ausgestaltung der technischen und organisatorischen Abwicklung in die Zuständigkeit des Bundesministeriums für Inneres fällt.

Darüber hinaus muss nach Abschluss der Maßnahme sichergestellt werden, dass die Vorrichtungen zur Überwachung oder Durchsuchung wieder entfernt oder diese funktionsunfähig werden. Technisch ist dafür nach Beendigung der Maßnahme eine Löschung des Überwachungsprogramms am Gerät selbst, somit ein neuerlicher direkter Zugriff auf das Computersystem wie bereits bei der Installation, erforderlich. Um sicherzustellen, dass das Überwachungsprogramm nicht durch ein eventuell zwischenzeitig erfolgtes BackUp des Geräts nach einer Datenwiederherstellung aus diesem BackUp wieder aktiviert wird, wird zur Sicherstellung der Löschungsverpflichtung auch die Möglichkeit vorgeschlagen, das Überwachungsprogramm mit einem Funktionszeitraum zu versehen, der mit der Dauer der gerichtlich bewilligten Anordnung übereinstimmt, sodass das Programm nach deren Ablauf ohne weiteren Eingriff funktionsunfähig wird. Dabei ist auch die Möglichkeit vorzusehen, dass der Funktionszeitraum für den Fall der vorzeitigen Beendigung oder der Verlängerung der Maßnahme ohne neuen direkten Zugriff auf das Computersystem angepasst werden kann.

Die Durchführung der neuen Ermittlungsmaßnahme soll nach § 147 StPO der Prüfung und Kontrolle des Rechtsschutzbeauftragten der Justiz (§ 47a) unterliegen (Abs. 1 Z 3a). Auf Grund des Gewichts der mit der Maßnahme verbundenen Grundrechtseingriffe müssen besondere Gründe vorliegen, die die

Verhältnismäßigkeit des Eingriffes begründen (Abs. 2). Mit Abs. 3a sollen die Rechte des Rechtsschutzbeauftragten weiter ausgebaut werden, um eine effektive Kontrolle nicht nur der Anordnung, sondern auch der Durchführung der Maßnahme zu ermöglichen. Dem Rechtsschutzbeauftragten soll dazu Einsicht in alle Unterlagen und Protokolle (§ 145 Abs. 4 StPO) zustehen, überdies soll er zu diesem Zweck nach Maßgabe der §§ 126 und 127 StPO auch die Beiziehung eines Sachverständigen verlangen können. Der Sachverständige ist gemäß § 126 Abs. 3 StPO im Ermittlungsverfahren von der Staatsanwaltschaft zu bestellen.

Zu Z 17 (§ 148 StPO):

Diese Bestimmung soll die Haftung des Bundes für durch die Maßnahme verursachte Schäden auch für Fälle der Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, begründen.

Zu Z 18 (§ 514 Abs. 35 StPO):

Diese Bestimmungen regelt das Inkrafttreten.

Zu Artikel 2 (Änderung des Staatsanwaltschaftsgesetzes):

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

Zunächst wird im Bereich des staatsanwaltschaftlichen Berichtswesens vorgeschlagen, bei der Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden, dieselben Vorkehrungen zu treffen, wie dies auch im Fall einer optischen und akustischen Überwachung von Personen nach § 136 Abs. 1 Z 2 und 3 StPO der Fall ist. Die Staatsanwaltschaften sollen daher den Oberstaatsanwaltschaften bereits über die beabsichtigte Anordnung dieser Maßnahme zu berichten haben (Abs. 1).

Darüber hinaus wird die Aufnahme der Ermittlungsmaßnahme der Überwachung von Nachrichten, die im Wege eines Computersystems übermittelt werden (§ 136a StPO), in den vom Bundesministerium für Justiz auf Grundlage der Berichte der Staatsanwaltschaften und des Berichtes des Rechtsschutzbeauftragten alljährlich dem Nationalrat, dem Datenschutzrat und der Datenschutzbehörde erstatteten Gesamtbericht über den Einsatz besonderer Ermittlungsmaßnahmen vorgeschlagen.

Die Änderungen im StAG sollen zum gleichen Zeitpunkt (1. Jänner 2017) wie die korrespondierenden Regelungen der StPO in Kraft treten.