Bundesministerium für Justiz
Museumstraße 7
1070 Wien

Ihr Zeichen	Unser Zeichen	Bearbeiter/in	Tel	Fax	Datum
BMJ-S578.031/0008-IV 3/2017	AR-GStBAK/Ht	David Koxeder	501 65 DW 16434	501 65 DW 12471	18.08.2017

Bundesgesetz, mit dem die Strafprozessordnung1975 geändert wird (Strafprozessrechtsänderungsgesetz 2017)

Die Bundesarbeitskammer dankt für die Übermittlung des Entwurfs und nimmt dazu wie folgt Stellung:

Allgemeines:

Der vorliegende Gesetzesentwurf verfolgt gemäß den Erläuterungen im Wesentlichen den Ausbau von Überwachungsmaßnahmen durch die Strafverfolgungsbehörden.

Eingangs wird ausdrücklich festgehalten, dass die Bundesarbeitskammer in Zeiten der steigenden Terrorgefahr in Europa Maßnahmen, die dem Zweck der Aufrechterhaltung der nationalen oder öffentlichen Sicherheit sowie der Gewährleistung der öffentlichen Ruhe und Ordnung, für erforderlich erachtet und begrüßt. Die Schnelllebigkeit der Technik, vor allem der Kommunikationsmittel, verlangt auch die Anpassung der (technischen) Ermittlungsmaßnahmen der Sicherheitsbehörden, damit die (Schwerst-)Kriminalität gezielt und effizient bekämpft werden kann.

Das stetig größer werdende Sicherheitsbedürfnis in der Bevölkerung findet offenkundig seine Ursache in den Terrorattacken der jüngsten Vergangenheit. Infolgedessen ist nachvollziehbar, dass sich die Menschen Schutzmaßnahmen erwarten, die die Unversehrtheit des Einzelnen garantieren. Die Erwartungshaltungen der Bevölkerung sind daher hoch. Fraglich ist in diesem Zusammenhang, ob die nun vorgeschlagenen Ermittlungsmaßnahmen, die dem gegenständlichen Gesetzesentwurf zu Grunde liegen, mit den verfassungsgesetzlich gewährleisteten Grundrechten in Einklang gebracht werden können.

Die vergangenen Terroranschläge in Europa haben verdeutlicht, dass diese trotz bereits bestehender weitreichender Überwachungsvorkehrungen nicht verhindert werden konnten. Oftmals waren es der Polizei und Staatsanwaltschaft bereits bekannte Einzeltäter, die auch zuvor vonseiten des Bundesamts für Verfassungsschutz und Terrorismusbekämpfung unter (ständiger) Beobachtung standen.

Überwachungsmaßnahmen sowie die Ausweitung von Ermittlungsschritten mit dem Zweck die öffentliche Sicherheit zu gewährleisten, stehen bekanntlich in einem Spannungsverhältnis mit verfassungsgesetzlich gewährleisteten Grundrechten. Im vorliegenden Fall ist der Gesetzesentwurf insbesondere im Lichte des Grundrechts auf Achtung des Privat- und Familienlebens gemäß Art 8 EMRK sowie des Grundrechts auf Datenschutz iSd § 1 Datenschutzgesetz (DSG) zu beurteilen.

In Anbetracht des medialen Echos und der Tatsache, dass bis dato eine Vielzahl von kritischen Stellungnahmen einzelner Personen zum vorliegenden Gesetzesentwurf eingebracht wurden, bedarf es jedenfalls einer gesellschaftspolitischen Diskussion bzw Auseinandersetzung mit dieser Strafprozessnovelle.

Der gegenständliche Gesetzesentwurf sieht überaus umfangreiche Maßnahmen zur Überwachung vor, wobei es sich bei einigen dieser vorgeschlagenen Vorkehrungen um weitreichende Eingriffe in die verfassungsmäßig gewährleisteten Grundrechte der Betroffenen handelt, sodass die Verhältnismäßigkeit und Notwendigkeit der Grundrechtseingriffe zumindest zu hinterfragen sind.

Aus Sicht der Bundesarbeitskammer wird aus obgenannten Gründen eine grundlegende Überarbeitung des vorliegenden Gesetzesentwurfs – im Sinne der Verfassungskonformität – ausdrücklich empfohlen.

Zu den Bestimmungen im Detail:

Änderung der Strafprozessordnung 1975

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

Auskunft über den PUK-Code:

Zu Z 4 (§ 76a Abs 1 StPO):
Mit der vorgeschlagenen Fassung des § 76a Abs 1 StPO sollen zur Aufklärung des konkreten Verdachts einer Straftat einer bestimmten Person Anbieter von Kommunikationsdiensten den PUK-Code („Personal Unlocking Key“) aufgrund der sachlichen Nähe unter den Voraussetzungen der Auskunft über Stammdaten eines Teilnehmers (vgl § 76a Abs 1 StPO) den kriminalpolizeilichen Behörden, Staatsanwaltschaften und Gerichten bekanntgeben müssen.

Die beabsichtigte Maßnahme ist vor allem aus grund- bzw verfassungsrechtlicher Sicht bedenklich, jedenfalls aber in diesem Zusammenhang zu hinterfragen, zumal staatliche Eingriffe in die Telekommunikation nicht nur an den einfachgesetzlichen Bestimmungen zu messen sind, sondern auch der verfassungsrechtliche Rahmen zu berücksichtigen ist. Die gegenständliche Anordnung steht vor allem mit dem Grundrecht auf Achtung des Privat- und Familienlebens nach Art 8 EMRK und dem Grundrecht auf Datenschutz iSd § 1 DSG in einem Spannungsverhältnis.

Das Grundrecht auf Achtung des Privat- und Familienlebens gemäß Art 8 EMRK gewährleistet unter dem Aspekt der Achtung des Privatlebens Schutz vor staatlichen Eingriffen. In Hinblick auf staatliche Eingriffe im Rahmen der Telekommunikation ergibt sich daraus ein umfassender Schutz, wonach die Inhaltsüberwachung (vgl EGMR 16.02.2000, 27798/95, Amann/Schweiz), als auch die Erhebung von Vermittlungsdaten des Kommunikationsvorgangs (vgl EGMR 25.09.2001, 44787/98, P.G. und J.H./UK), wie auch die Ermittlung von Standortdaten des Mobiltelefons an Art 8 EMRK zu messen sind. Dies hat zur Folge, dass eine beabsichtigte Maßnahme nicht nur gesetzlich vorgesehen sein muss, sondern auch verhältnismäßig und notwendig (vgl Reindl-Krauskopf; Tipold/Zerbes in Fuchs/Ratz, WK StPO § 134 Rz 22).

Fraglich ist, ob die vorgeschlagene Maßnahme iSd § 76a Abs 1 StPO, wonach Telekommunikationsanbieter zur Bekanntgabe des PUK-Codes verpflichtet werden, – in Anbetracht der Schwere des Eingriffs – mit dem Verhältnismäßigkeitsgrundsatz iSd Art 8 EMRK im Einklang steht. Dies vor allem vor dem Hintergrund, dass mit der Bekanntgabe des Codes den Strafverfolgungsbehörden ein uneingeschränkter – und somit ein unter Umständen ausufernder, jeder Kontrolle entzogener – Zugriff auf das jeweilige Kommunikationsmittel (Mobiltelefon, Tablet etc), insbesondere auf die gespeicherten Inhalte übertragener Nachrichten (zB SMS) sowie auf lokal gespeicherte Kontakt- und Adressverzeichnisse, ermöglicht wird. Anders ausgedrückt: Die Einschreiter könnten unter anderem auch auf Daten zugreifen, die mit der Verdachtslage bzw dem vorgeworfenen Faktum überhaupt nicht im Zusammenhang stehen.

Dabei ist auch ausdrücklich auf § 5 StPO zu verweisen, wonach jede Rechtsgutbeeinträchtigung verhältnismäßig und erforderlich sein muss; das bedeutet, die Strafverfolgungsbehörden müssen jenes Mittel auswählen, das mit den am wenigsten negativen Auswirkungen für den Betroffenen verbunden ist (vgl Wiederin in Fuchs/Ratz, WK StPO § 5 Rz 89).

Fest steht, dass durch die geplante Maßnahme in das Grundrecht auf Achtung des Privat- und Familienlebens gemäß Art 8 EMRK eingegriffen wird (vgl EGMR 23.11.1993, 14.838/89, A/Frankreich). Dass der Verhältnismäßigkeitsgrundsatz iSd Grundrechts durch die erwähnte Eingriffsintensität in Form einer generell verpflichtenden Bekanntgabe des PUK-Codes gewahrt bleibt, ist aufgrund der obgenannten Bedenken mehr als kritisch zu hinterfragen.

Das Grundrecht auf Datenschutz erfasst alle personenbezogenen Daten, sofern ein schutzwürdiges Geheimhaltungsinteresse an diesen besteht. Neben den Inhaltsdaten (Inhalte übertragener Nachrichten, vgl § 92 Abs 3 Z 5 iVm Z 7 TKG 2003) und Vermittlungsdaten

werden auch Stammdaten (zB Name und die Postanschrift, vgl § 92 Abs 3 Z 3 TKG 2003) sowie Standortdaten (vgl § 92 Abs 3 Z 6 TKG 2003) geschützt. Insofern wird durch die geplante Gesetzesänderung jedenfalls in das Grundrecht auf Datenschutz eingegriffen. Nachdem die Verfassungsbestimmung des § 1 DSG auf das Grundrecht auf Achtung des Familienlebens gemäß Art 8 EMRK verweist, ist im Hinblick auf die Verfassungskonformität (insbesondere iZm mit der Verhältnismäßigkeit des Grundrechtseingriffs, vgl dazu auch Berka, Die Grundrechte, Rz 266 ff) der strafprozessualen Überwachung der Telekommunikation – um Wiederholungen zu vermeiden – auf die zuvor erwähnten Ausführungen zum Grundrecht auf Achtung des Privat- und Familienlebens gemäß Art 8 EMRK hinzuweisen.

Zu Z 8, 11, 14 und 25 bis 28 (§§ 134 Z 2a und 5, 135 Abs 2a, 140 Abs 1 Z 2 und 4, 144 Abs 3 und 145 Abs 3 StPO):
Diese Bestimmungen beinhalten Legaldefinitionen und Rechtsgrundlagen zur Lokalisierung von technischen Einrichtungen durch den Einsatz technischer Mittel (zB IMSI-Catchers) zur Feststellung von geografischen Standorten und IMSI-Nummern ohne die Mitwirkung eines Telekommunikationsanbieters oder eines sonstigen Dienstanbieters.

Diese Ermittlungsmaßnahme wird ohnehin schon seit Jahren eingesetzt und von der Rechtsprechung als Auskunft über Daten einer Nachrichtenübermittlung nach §§ 134 Z 2, 135 Abs 2 StPO qualifiziert. Auch im Bereich des Sicherheitspolizeigesetzes (SPG) wird der Einsatz von (derartigen) technischen Mitteln zur Lokalisierung einer Endeinrichtung im Rahmen der Gefahrenabwehr in § 53 Abs 3b SPG eigenständig geregelt. Es ist somit bedenklich, ob eine weitere – die StPO noch zusätzlich verkomplizierende – Regelung tatsächlich dem Rechtsanwender (eine ohnehin aufgrund der derzeitigen Gesetzeslage schon bestehende) Klarheit über die Reichweite der Ermittlungsbefugnisse vermitteln wird.

Überwachung von Nachrichten:

Zu Z 9 (§ 134 Z 3 StPO):
Fest steht, dass die Überwachung von Nachrichten einen weitreichenden Grundrechtseingriff darstellt, weshalb es einer besonders strengen Prüfung der Verhältnismäßigkeit und Erforderlichkeit der Maßnahme im Einzelfall sowie der Dokumentationspflicht und der Berücksichtigung der jeweiligen Verwertungsverbote bedarf.

Mit der vorgeschlagenen Formulierung der „Überwachung von Nachrichten“ iSd § 134 Z 3 StPO wird unmissverständlich klargestellt, dass dies zu einer Ausweitung der Überwachung internetbasierter Kommunikation führen soll und zwar dahingehend, dass damit (auch) über ein Kommunikationsnetz oder einen Dienst der Informationsgesellschaft gesendete, übermittelte oder empfangene Informationen umfasst werden (zB Aufruf von Websites, Surfen im Internet und unverschlüsselte Übertragungsvorgänge in eine Cloud). Anders ausgedrückt: Durch das Abstellen auf die Tatbestandsmerkmale Senden, Übermitteln oder Empfangen soll im Zusammenhang mit der Überwachung von Nachrichten auf alle Übertragungsmerkmale abgestellt bzw sollen damit alle Übertragungsvorgänge abgedeckt werden.

Aufgrund der beabsichtigten Ausweitung der Überwachungsmaßnahmen stellt sich auch hier die Frage, ob diese – zweifellos gegebenen Grundrechtseingriffe – mit Art 8 EMRK und dem Grundrecht auf Datenschutz, insbesondere unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes, in Einklang gebracht werden können. Bei der Verhältnismäßigkeitsprüfung ist auf die Zahl der aufgrund der Streuwirkung von der geplanten Überwachungsmaßnahme betroffenen Personen Bedacht zu nehmen, die womöglich an der aufzuklärenden Straftat nicht beteiligt waren und dennoch durch den nun geplanten staatlichen Grundrechtseingriff beeinträchtigt werden (vgl dazu auch auf einfachgesetzlicher Ebene ausdrücklich § 5 StPO sowie Reindl-Krauskopf; Tipold/Zerbes in Fuchs/Ratz, WK StPO § 134 Rz 25).

Überwachung verschlüsselter Nachrichten:

Zu Z 10, 11 16, 25 und 26 (§§ 134 Z 3a und 5, 135a, 140 Abs 1 Z 2 und 4 StPO):
Die vorliegende Änderung der Strafprozessordnung ist offenkundig Folge der steigenden Terrorgefahr in Europa. Aus diesem Grund wird auch mit der Notwendigkeit sowie Sinn- und Zweckmäßigkeit der Überwachung von verschlüsselten Nachrichten, die – nun aufgrund des geänderten Kommunikationsverhaltens – im Wege von Kommunikationsprogrammen wie WhatsApp, Skype, Telegramm etc übermittelt werden, argumentiert. Gleichzeitig wird die Ansicht vertreten, dass kein Wertungsunterschied beim Eingriff in das Grundrecht auf Achtung des Privat- und Familienlebens gemäß Art 8 EMRK dahingehend vorliegt, ob eine Nachricht überwacht werden soll, die der Beschuldigte via SMS oder per WhatsApp oder mittels Telegramm versendet.

Wie bereits oben erwähnt, muss bei jeder Überwachungsmaßnahme die Einhaltung der Grundrechte (insbesondere die Verhältnismäßigkeit des jeweiligen Grundrechtseingriffs) gewährleistet werden, und sie darf zu keinen Systemwidrigkeiten führen.

Mit dem vorliegenden Entwurf sollen die bei WhatsApp- und Telegrammnachrichten standardisiert vorgesehenen end-to-end-Verschlüsselungen – die eine Überwachung der Kommunikation durch die Strafverfolgungsbehörden unmöglich machen – über die Installation einer Software direkt im zu überwachenden Computersystem (zB Desktop-PC, Notebook) oder mobilen Endgerät (zB Smartphone) entsperrt und somit die Lesbarkeit der Nachrichten bzw die Überwachung derselben ermöglicht werden.

Problematisch ist die geplante Maßnahme im Zusammenhang mit der sogenannten „Online-Durchsuchung“ zu sehen. Dies deshalb, weil die Installation einer derartigen Software die Gefahr in sich birgt, dass eine Durchsuchung des gesamten Computersystems oder Endgerätes, insbesondere lokal abgespeicherter, nicht mit dem Übertragungsvorgang im Zusammenhang stehender Daten, ermöglicht wird. Zwar wird in den gegenständlichen Erläuterungen festgehalten, dass mit dem Gesetzesentwurf eine derartige Online-Durchsuchung nicht stattfinden soll; dennoch bestünde durch eine derartige Softwareinstallation die Möglichkeit zum Missbrauch von Daten (zB aufgrund unzulässig erhobener Daten bzw Zufallsfunde). Vor allem lässt sich aus dem Gesetzesentwurf bzw der geplanten Ermittlungsmaßnahme nicht ableiten, ob technisch sichergestellt werden kann,

dass ausschließlich die Kommunikation und nicht auch darüberhinausgehende Daten durch die Maßnahme (mit)überwacht werden. Daran ändert auch die Anmerkung in den Erläuterungen, dass die Software bzw das Programm auf die gesetzlich vorgesehenen Funktionen und die Nachvollziehbarkeit der getroffenen Maßnahmen beschränkt werden soll, nichts. Der Hinweis, wonach ein Screenen von lokalen Adressbüchern oder Kontaktverzeichnissen nicht zulässig sein soll, ist zu begrüßen, jedoch nicht ausreichend, um einen dementsprechenden Missbrauch auszuschließen. Im Übrigen ist an dieser Stelle darauf hinzuweisen, dass die verfahrensgegenständliche „Überwachungssoftware“ noch nicht vorliegt, sondern erst beschafft werden muss (weshalb auch empfohlen wird, eine Legisvakanz bis 01.08.2019 vorzusehen). Die Einrichtung einer Missbrauchskontrolle wäre aus obgenannten Gründen jedenfalls erforderlich (zB Schutz vor Manipulation am Endgerät oder Computersystem). Fraglich ist auch, wie lange die von den Strafverfolgungsbehörden überwachten und gesammelten Daten aufbewahrt werden bzw wann diese zu löschen sind. Eine diesbezügliche Bestimmung findet sich im Gesetzesentwurf nicht.

Die geplante Maßnahme ist aber nicht nur in grund- bzw verfassungsrechtlicher Hinsicht kritisch zu hinterfragen. Zu klären ist in diesem Zusammenhang auch, inwieweit durch die Installation einer derartigen Software die Gefahr von Softwareschäden (Stichwort: Viren) besteht. Ob ein sogenannter „Kill-Switch“ tatsächlich ausreichenden Schutz vor Beschädigung bzw Beeinträchtigung des Computersystems oder Endgerätes gewährleisten kann, bleibt zu hinterfragen. Inwiefern Vorsorge gegen Streuschäden bzw Verhinderung oder Eingrenzung von Kollateralschäden (siehe dazu die Ausführungen zu Z 9 [§ 134 Z 3 StPO]) getroffen wurde, ist ebenfalls den Erläuterungen nicht zu entnehmen. Vor diesem Hintergrund und mit Blick auf das gesamte beabsichtigte Regelungsregime bestehen Bedenken, ob die gegenständlichen gesetzlichen Eingriffe aus grund- und verfassungsrechtlicher Sicht die gebotene Präzision erreichen (vgl dazu auch OLG Linz 26.04.2013, 9 Bs 108/13s und 06.05.2013, 9Bs 128/13g der Beschwerde des Rechtsschutzbeauftragten folgend; Reindl-Krauskopf, 18. ÖJT I/2, 149-151; Salimi, JBl 2013, 698 [706]).

Diesbezüglich sprechen die Erläuterungen davon, dass „auch an dritten Computersystemen keine Schädigungen oder dauerhafte Beeinträchtigungen bewirkt werden dürfen“. Aus dieser Formulierung ist abzuleiten, dass die gegenständliche Software ebenso in dritten Computersystemen – somit auch bei all jenen, mit denen der Verdächtigte bzw Beschuldigte in Kontakt getreten ist bzw treten könnte – installiert werden darf. Eine derartige überschießende Maßnahme würde jedenfalls dem Verhältnismäßigkeitsprinzip widersprechen und somit einen grundrechtswidrigen (weil die Eigentums- und Persönlichkeitsrechte nicht wahrenden) Eingriff darstellen. Auch auf einfachgesetzlicher Ebene würde diese Maßnahme gegen § 5 StPO (Gesetz- und Verhältnismäßigkeit) verstoßen. Dies deshalb, weil auch Personen überwacht würden, die (möglicherweise) nicht an der aufzuklärenden Straftat beteiligt waren.

Im Übrigen wird angeregt in der vorgeschlagenen Fassung des § 135a Abs 1 lit b StPO die wiederholte Wortfolge „(…), werden soll,“ zu löschen.

Unabhängig von den bisher angestellten Überlegungen stellt sich die Frage, ob der Infiltration einer Kommunikationsquelle (hier: Computersystem, Smartphone etc) mit einem Spionagetool (hier: Überwachungssoftware) nach Art und Bedeutung des (Grund-)Rechtseingriffs – parallel zur eigentlichen Überwachung – ein gesondertes Gewicht zukommt, und die Konstellation folglich mit einem Eingriff in das Hausrecht im Rahmen des Lauschangriffs vergleichbar ist. In diesem Fall könnte die beabsichtigte Infiltration nämlich nicht als von den geplanten gesetzlichen Bestimmungen zur Überwachung verschlüsselter Nachrichten gedeckt sein, und wäre mangels gesetzlicher Grundlage nicht zuletzt wegen § 5 StPO rechtswidrig. Zwar stellt das Eindringen in ein Computersystem oder mobiles Endgerät selbstverständlich als solches keine Verletzung des Hausrechts iSd Art 9 StGG dar. Jedoch wird – unabhängig von der tatsächlichen Überwachung – in die Privatsphäre des Nutzers eingegriffen. Überdies greift die beabsichtigte Infiltration in dessen Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme (vgl zu diesem Grundrecht ua BVerGE 120, 274) ein (vgl ebenso Buermeyer/Bäcker, HRRS 2009, 433 [439]). Aufgrund der Funktion, die eine Kommunikationsquelle für den Nutzer darstellt, ist dieser Eingriff in hohem Maße sensibel und stellt in gewisser Weise eine Verletzung des „digitalen Hausrechts“ an der jeweiligen Kommunikationsquelle dar, sodass auch aus diesem Grund die vorgeschlagene Überwachungsmaßnahme kritisch zu hinterfragen ist (vgl Reindl-Krauskopf; Tipold/Zerbes in Fuchs/Ratz, WK StPO § 134 Rz 58/3).

Ungeachtet dessen ist zu hinterfragen, ob die Überwachungssoftware nicht zu potentiellen Sicherheitslücken am Computersystem bzw Endgerät führt. Sicherheitslücken, die zugunsten der Strafrechtsverfolgung nicht unmittelbar geschlossen werden (können), sind auch ein Einfallstor für Anwender von Hacking-Tools für kriminelle Zwecke. Informationen über noch ungeschlossene Sicherheitslücken werden nämlich in kriminellen Kreisen (Schwarzmarkt bzw im Darknet) zu enormen Preisen verkauft. Es sind somit Maßnahmen zu setzen, die eine leichte Angreifbarkeit der Kommunikationsinfrastruktur der Betreiber schützt. Derartige Schutzmaßnahmen finden sich jedoch in den vorliegenden Erläuterungen nicht.

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

In den Erläuterungen wird die Abgrenzung zur Online-Durchsuchung damit begründet, dass die vorgeschlagenen neuen Ermittlungsmaßnahmen nur für einen künftigen Zeitraum angeordnet werden dürfen und dadurch nicht auf bereits vor dem Anordnungszeitraum bestandene Daten, die in keinem Zusammenhang mit einem Übertragungsvorgang stehen, zugegriffen werden darf. Damit wird jedoch verkannt, dass es bei der Online-Durchsuchung nicht unbedingt auf den Zeitraum ankommt, sondern vielmehr auf die Intensität bzw Umfang der Durchsuchung. Somit besteht auch im Falle der Anordnung der Ermittlungsmaßnahmen für einen künftigen Zeitraum die Gefahr, dass durch die Installation der Überwachungssoftware auf lokal abgespeicherte, nicht mit dem Übertragungsvorgang im Zusammenhang stehender Daten zugegriffen werden könnte, was faktisch einer Online-Durchsuchung gleichkäme. Diesbezüglich wird – um Wiederholungen zu vermeiden – auf das zur Online-Durchsuchung bereits Gesagte verwiesen.

Zu Z 27 bis 29 (§§ 144 Abs 3, 145 Abs 3 und 4 StPO):
In den Erläuterungen wird zwar festgehalten, dass es im Rahmen der Durchführung der Überwachung zu keiner über die Installation und die mit der Überwachung einhergehenden Eingriffe der Software hinausgehenden Veränderung der ursprünglich am Computersystem vorhandenen Daten kommen darf. Jedoch ist an dieser Stelle nochmals ausdrücklich anzumerken, dass die gegenständliche Überwachungssoftware noch nicht entwickelt wurde, sodass derzeit nicht feststellbar ist, ob ein derartiger Schutz vor Veränderungen der Daten am Computersystem durch den Eingriff der Software überhaupt gewährleistet werden kann.

Zu Z 30, 33 und 34 (§§ 147 Abs 1 Z 2a, Abs 2 und 3a StPO):
Es werden keine Einwände erhoben.

Zu Z 35 (§ 148 StPO):
Es werden keine Einwände erhoben.

Beschlagnahme von Briefen:

Zu Z 13 (§ 135 Abs 1 StPO):
Mit der vorgeschlagenen Änderung soll es zum Entfall der Wortfolge „und sich der Beschuldigte wegen einer solchen Tat in Haft befindet oder seine Vorführung oder Festnahme deswegen angeordnet wurde“ kommen, wodurch künftig auch die Beschlagnahme von Briefen unbekannter Täter oder auf freiem Fuß befindlicher Beschuldigter ermöglicht werden soll.

Fraglich ist, ob die geplante Änderung mit dem verfassungsgesetzlich gewährleisteten Schutz des Briefgeheimnisses gemäß Art 10 Staatsgrundgesetz (StGG) im Einklang steht. Die verfassungsrechtliche Norm des Art 10 StGG steht unter Gesetzesvorbehalt: Ein Eingriff ist grundsätzlich nur erlaubt, sofern eine gesetzliche Grundlage dafür besteht und ein richterlicher Befehl vorliegt. Daher ist ein richterlicher Befehl auch bei Gefahr im Verzug zwingend, und so räumt § 138 Abs 2 StPO verfassungskonform (vgl dazu Wiederin in Korinek/Holoubek, B-VG, Art 10 StGG Rz 23) der Staatsanwaltschaft bloß ein Anhalterecht ein (vgl. Reindl-Krauskopf; Tipold/Zerbes in Fuchs/Ratz, WK StPO § 135 Rz 10). Gemäß § 137 Abs 1 StPO sind Ermittlungsmaßnahmen nach den §§ 135 bis 137 StPO (und somit auch die Beschlagnahme von Briefen nach § 135 Abs 1 StPO) von der Staatsanwaltschaft aufgrund einer gerichtlichen Bewilligung anzuordnen. Ob allerdings mit einer richterlichen Bewilligung iSd § 137 Abs 1 StPO den Anforderungen eines richterlichen Befehls Genüge getan wird, ist zweifelhaft (vgl Reindl-Krauskopf; Tipold/Zerbes in Fuchs/Ratz, WK StPO § 134 Rz 9). Dies vor allem deshalb, weil – im Unterschied zu einer gerichtlichen Bewilligung – ein richterlicher Befehl einen exklusiv von der Justiz ausgehenden Willensakt darstellt. Die vorliegenden Erläuterungen erkennen zwar das gegenständliche Problem, indem sie sich mit der Verfassungsbestimmung des Art 10 StGG auseinandersetzen, argumentieren jedoch ambivalent, indem sie sich einerseits auf Verfassungskonformität mit Art 10 StGG berufen, andererseits durch eine Art „Auslegung“, die sich jedoch jeder rationalen Überprüfung entzieht, den „Befehl“ durch die „Bewilligung“ ersetzen wollen (vgl dazu auch Hauenschild, Rz 2000, 194; Walter/Zeleny, ÖJZ 2001, 878 f). Derartige „Umdeutungen“ des eindeutigen Textes des StGG sind – zumal auch

der historische Hintergrund der Normierung klar ist – als inakzeptabel zu werten (vgl Walter/Mayer, Bundesverfassungsrecht Rz 1423 bzw 1424).

Zu Z 19 und 24 (§§ 137 Abs 2, 138 Abs 5 StPO):
Die geplante Änderung sieht den Entfall des § 137 Abs 2 StPO vor. Das ist grundsätzlich nachvollziehbar und auch zweckmäßig. Nicht nachvollziehbar ist jedoch, warum auch § 112 StPO entfallen soll. Zweck der Belehrung iSd § 112 StPO ist bekanntlich, dem Betroffenen die Erhebung eines Widerspruchs gegen die Beschlagnahme unter Berufung auf ein gesetzlich anerkanntes Recht zur Verschwiegenheit zu ermöglichen (vgl Fabrizy, StPO12 § 138 Abs 2 Rz 2). Auch wenn 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, besteht kein Rechtsgrund von der Belehrung iSd § 112 StPO abzusehen. Zu berücksichtigen ist diesbezüglich, dass die Beschlagnahme von Briefen mit dem Berufsgeheimnis (zB ärztliches und anwaltliches Berufsgeheimnis, vgl dazu auch die Aussageverweigerung nach § 157 Abs 1 Z 2 – 4 StPO) in einem Spannungsverhältnis steht und die Folge des Widerspruchs gegen die Beschlagnahme die Sicherung (Versiegelung) der Unterlagen gegen unbefugte Einsichtnahme oder Veränderung sowie Hinterlegung bei Gericht ist. Der Entfall der Belehrung führt zu einer unzulässigen Benachteiligung des Betroffenen und folglich zu einem Verstoß gegen den Grundsatz der Waffengleichheit sowie Art 6 EMRK (Recht auf ein faires Verfahren).

Akustische Überwachung von Personen:

Zu Z 17, 18, 27, 28 und 32 (§§ 136 Abs 1a, 137 Abs 1, 140 Abs 1 Z 2, 144 Abs 3, 145 Abs 3, 147 Abs 1 Z 5 StPO):
Eine akustische Überwachung von Personen greift wie jede andere staatliche (Zwangs-) Maßnahme auch in die Grundrechte der von der Maßnahme betroffenen Personen ein. Zunächst ist bei der (geheimen) Überwachung an einen Eingriff in das Grundrecht auf Achtung des Privat- und Familienlebens nach Art 8 EMRK zu denken. Auch bei der akustischen Überwachung von Personen stellt sich die Frage, ob der Eingriff unter den Voraussetzungen des Art 8 Abs 2 EMRK zulässig ist, das heißt, notwendig und verhältnismäßig (vgl Reindl-Krauskopf; Tipold/Zerbes in Fuchs/Ratz, WK StPO § 134 Rz 102). Letztlich geht es auch bei der akustischen Überwachung darum, einen Ausgleich zwischen der Ausübung des durch Art 8 Abs 1 EMRK garantierten Rechts des Einzelnen und der Notwendigkeit, geheime Überwachungsmaßnahmen zum Schutz der demokratischen Gesellschaft in ihrer Gesamtheit einzusetzen (vgl EGMR 06.09.1978, 5029/71, Klaas/Deutschland § 59; Reindl-Krauskopf; Tipold/Zerbes in Fuchs/Ratz, WK StPO § 134 Rz 25), zu erzielen. Bei der Verhältnismäßigkeitsprüfung ist insbesondere auch auf die mit der Überwachungsmaßnahme stattfindende Streuwirkung Bedacht zu nehmen. Das heißt, auf Personen, die – wie bereits oben erwähnt – überwacht werden, jedoch mit der aufzuklärenden Straftat nicht im Zusammenhang stehen (vgl dazu auch die obige Ausführung zu Z 9).

Nachdem geheime Überwachungsmaßnahmen stets auf Datensammlung ausgerichtet sind, ist auch ein Eingriff in das Grundrecht auf Datenschutz gemäß § 1 DSG wahrscheinlich.

Betreffend die Verhältnismäßigkeit und Notwendigkeit des Eingriffs wird – um Wiederholungen zu vermeiden – auf das Obgesagte verwiesen.

Richtig ist, dass es sich bei einem Fahrzeug – in das zur Installation der Überwachungsinstrumente unter Umständen eingedrungen werden muss – typischerweise nicht um einen vom Hausrecht iSd Art 9 EMRK geschützten Raum handelt und daher auch keine gesonderte gerichtliche Bewilligung nach § 137 Abs 1 letzter Halbsatz erforderlich ist. Nur der Vollständigkeit halber wird diesbezüglich festgehalten, dass sich die Rechtslage bei zum Wohnen verwendeter Fahrzeuge, wie etwa Wohnmobile und Hausboote, anders darstellt (vgl Wiederin in Korinek/Holoubek B-VG StGG Art 9 Rz 24). Hierbei handelt es sich sehr wohl um zum Hauswesen gehörende Räume, die dem Schutzziel des Hausrechts unterliegen (vgl. Birklbauer/Tipold/Zerbes in Fuchs/Ratz, WK StPO § 117 Rz 9 f), sodass wiederum eine gesonderte gerichtliche Bewilligung nach § 137 Abs 1 letzter Halbsatz erforderlich wäre.

Sonstige Änderungen im 5. Abschnitt des 8. Hauptstückes:

Zu Z 15 und 31 (§ 135 Abs 3 Z 3 und 136 Abs 1 Z 3, 147 Abs 1 Z 3):
Es werden keine Einwände erhoben.

Zu Z 22 und 23 (§ 138 Abs 2 und 3 StPO):
Es werden keine Einwände erhoben.

Sonstige Änderungen der StPO:

Zu Z 3 (§ 67 Abs 7 StPO):
Es werden keine Einwände erhoben.

Zu Z 5 (§ 94 letzter Satz StPO):
Es werden keine Einwände erhoben.

Zu Z 6 (§ 116 Abs 6 zweiter Satz StPO):
Die geplante Gesetzesänderung sieht vor, dass in Hinkunft im Bereich des gerichtlichen Strafverfahrens die Daten von den Kredit- und Finanzinstituten den Strafverfolgungsbehörden so übermittelt werden müssen, dass sie auch elektronisch weiterverarbeitet werden können. Diese Änderung ist unter anderem aus verfahrensökonomischer Sicht (derzeit ist mit der händischen Übertragung in andere Dateiformate ein erheblicher Zeit- und Ressourcenaufwand und infolgedessen Fehleranfälligkeit verbunden) nachvollziehbar. Dem Kreditinstitut sind auch die Kosten für Personal- und Sachaufwendungen zu ersetzen, wenn sie durch einen konkreten gerichtlichen Auftrag entstanden sind und das ortsübliche Maß nicht überschritten wird (vgl Lendl in Fuchs/Ratz, WK StPO § 381 Rz 30).

Nicht ausdrücklich geregelt ist, bei wem das Kredit- und Finanzinstitut den Kostenersatz zu beantragen hat.

Zwar wird von der herrschenden Lehre vertreten, dass dies beim Gericht, das auch die gerichtliche Bewilligung erlassen hat, vorzunehmen ist (vgl Flora in Fuchs/Ratz, WK StPO § 116 Rz 121). Dennoch wird angeregt, diesbezüglich eine gesetzliche Regelung zu treffen.

Zu Z 36 (§ 209b Abs 1 StPO):
Es werden keine Einwände erhoben.

Zu Z 37 (§ 221 Abs 1 StPO):
Es werden keine Einwände erhoben.

Zu Z 39 (§ 514 Abs 36 StPO):
Es werden keine Einwände erhoben.

Zu Z 40 (§ 516a Abs 6 StPO):
Der Richtigkeit halber wird festgehalten, dass – entgegen den Erläuterungen – die Richtlinie 2016/343/EU über die Stärkung bestimmter Aspekte der Unschuldsvermutung und des Rechts auf Anwesenheit in der Verhandlung in Strafverfahren, ABl. Nr. L 65 vom 11.03.2016 S 1 (Richtlinie Unschuldsvermutung) nicht in § 516a Abs 6 StPO, sondern in § 516a Abs 7 StPO in das nationale Recht umgesetzt werden soll.

Rudi Kaske
Präsident
F.d.R.d.A.

Hans Trenner
iV des Direktors
F.d.R.d.A.