Parlamentsdirektion
Dr. Karl Renner-Ring 3
1017 Wien

Ihr Zeichen	Unser Zeichen	Bearbeiter/in	Tel **501 65**	Fax **501 65**	Datum
13280.0050/1-L1.3/2018	AR-GStBAK/Gm	Alexander Krendl	DW 12773	DW 12471	23.03.2018

Bundesgesetz, mit dem die Strafprozeßordnung 1975, das Staatsanwaltschaftsgesetz und das Telekommunikationsgesetz 2003 geändert werden (Strafprozessrechtsänderungsgesetz 2018)

Die Bundesarbeitskammer bedankt sich für die Übermittlung des Entwurfs und erlaubt sich zu den nachfolgenden Gesetzesvorschlägen wie folgt Stellung zu nehmen:

Allgemeines:

Gemäß den Erläuterungen verfolgt der vorliegende Gesetzesentwurf, wie bereits der Entwurf des Strafprozessrechtsänderungsgesetzes 2017 (325/ME XXV. GP) im Wesentlichen den Ausbau der den Strafverfolgungsbehörden zur Verfügung stehenden Überwachungsmaßnahmen.

Die Bundesarbeitskammer hat bereits zum Entwurf des Strafprozessrechtsänderungsgesetzes 2017 umfassend Stellung genommen, weshalb – um Wiederholungen zu vermeiden – auf diese Stellungnahme verwiesen wird, soweit die vorliegende Regierungsvorlage Bestimmungen des Ministerialentwurfes übernimmt.

Grundsätzlich werden Maßnahmen, die dem Zweck der Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit dienen, von der Bundesarbeitskammer begrüßt. Durch den technischen Fortschritt und die Weiterentwicklung diverser Kommunikationsmittel sind Maßnahmen erforderlich, die auch zukünftig eine effektive und umfassende, aber gezielte Verfolgung und Aufklärung von Straftaten sicherstellen.

Solch grundrechtsinvasive Maßnahmen müssen jedoch immer einer strengen Prüfung der Verhältnismäßigkeit unterzogen werden sowie gerichtliche Kontrollmöglichkeiten und Rechtsschutzmöglichkeiten vorsehen.

Der vorliegende Gesetzesentwurf sieht, wie bereits der Ministerialentwurf des Strafprozessrechtsänderungsgesetzes 2017, überaus weitreichende und flächendeckende Überwachungsmaßnahmen vor. Bei den vorgeschlagenen Maßnahmen handelt es sich um massive Eingriffe in die verfassungsmäßig gesicherten Grundrechte des Einzelnen, deren Verhältnismäßigkeit und damit Zweckmäßigkeit sowie Notwendigkeit an dieser Stelle bezweifelt wird.

Die geplanten Maßnahmen sind – trotz teilweiser Überarbeitung in Reaktion der weitestgehend kritischen Stellungnahmen im Begutachtungsverfahren zum Ministerialentwurf 325/ME XXV. GP – überschießend und zum Teil zu wenig genau determiniert. Auch dem Erfordernis verfassungskonformer Rechtsschutzgarantien wurde bei grundrechtsinvasiven Überwachungsmaßnahmen, wie der geplanten Anlassdatenspeicherung („Quick-freeze“) oder der Nutzung von IMSI-Catchern, nicht Rechnung getragen.

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

Zu den Bestimmungen im Detail:

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):

Gemäß den Erläuterungen soll bei Vorliegen eines Anfangsverdachts die Möglichkeit geschaffen werden, die nach der derzeitigen Rechtslage geltende Verpflichtung von Telekommunikationsanbietern, Verkehrsdaten unverzüglich nach Beendigung der Verbindung bzw. sobald der Bezahlvorgang durchgeführt wurde und innerhalb einer Frist von drei Monaten, sofern die Entgelte nicht schriftlich beeinsprucht wurden, durch Anordnung der Staatsanwaltschaft zu unterbrechen. Sohin können Telekommunikationsanbieter in Folge dazu verpflichtet werden, die gespeicherten Daten bis zu 12 Monate zu speichern.

Erst der Zugriff auf diese Daten soll einer gerichtlichen Bewilligung bedürfen.

Bezüglich der im Entwurf vorausgesetzten Strafandrohung (in gewissen Fällen ab sechs Monaten Freiheitsstrafe) ist auf die Judikatur des EuGH (EuGH 8.4.2014, C-293/12, Digital Rights Ireland, Rz. 60; EuGH 21.12.2016, C-203/15 Tele2 Sverige, Rz. 102) zu verweisen. Eine Speicherung von Verkehrs- und Standortdaten ist laut EuGH nur zur Bekämpfung schwerer Straftaten zulässig. Da der im Gesetzesentwurf vorgesehene Strafrahmen (in gewissen Fällen ab einer Freiheitsstrafe von sechs Monaten) am unteren Ende des Strafgesetzbuches angesiedelt ist, ist davon auszugehen, dass diese Schwelle hinsichtlich der Rechtsprechung des EuGH zu niedrig angesetzt ist.

Auch ist fraglich, ob die mögliche Speicherdauer von bis zu 12 Monaten der vom EuGH verlangten Beschränkung der Datenspeicherung auf das absolut Notwendigste genügt. Dies auch deshalb, da der Gesetzgeber in der vom VfGH aufgehobenen Regelung zur Vorratsdatenspeicherung eine Speicherdauer von nicht mehr als 6 Monaten für notwendig hielt.

Es wird weiters darauf hingewiesen, dass entsprechend dem vorliegenden Entwurf keine Prüfungs- und Kontrollmöglichkeit des Rechtsschutzbeauftragten vorgesehen ist. Sowohl im Entwurf, als auch in der Gegenüberstellung des Gesetzestextes fehlt in § 147 Abs 1 Z 5 StPO Regierungsvorlage ein Verweis auf die geplante Ermittlungsmaßnahme des § 135 Abs 2b StPO Regierungsvorlage. Auch in den Erläuterungen findet sich keine Erklärung, warum die Maßnahme der Anlassdatenspeicherung von der Prüfungs- und Kontrollkompetenz des Rechtsschutzbeauftragten ausgenommen sein soll.

Festzuhalten ist, dass schon die Speicherung von Daten einen Eingriff in das Recht auf Achtung des Privatlebens iSd Art 8 EMRK darstellt, der nur unter den Voraussetzungen des Art 8 Abs 2 EMRK gerechtfertigt sein kann. Das bedeutet, dass schon bei der Speicherung „auf Vorrat“ entsprechende Rechtsschutzgarantien, auch in Hinblick auf die bereits genannte Rechtsprechung des EuGH, erforderlich sind, was der vorliegende Entwurf aus Sicht der Bundesarbeitskammer jedoch übersieht.

Es ist zu befürchten, dass es – mangels Notwendigkeit einer gerichtlichen Bewilligung der staatsanwaltschaftlichen Anordnung für die Speicherung von Daten sowie fehlender Prüfungs- und Kontrollmöglichkeit des Rechtsschutzbeauftragten – zu einem überbordenden Einsatz dieser Möglichkeiten durch die Staatsanwaltschaft kommen könnte.

Aus Sicht der Bundesarbeitskammer sollte daher bereits die staatsanwaltschaftliche Anordnung zur Unterbrechung der Löschungsverpflichtung nur nach gerichtlicher Bewilligung erfolgen dürfen und sollte diese zwingend der Prüfungs- und Kontrollmöglichkeit des Rechtsschutzbeauftragten unterliegen.

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 diesen Bestimmungen soll eine eigenständige Rechtsgrundlage für die Lokalisierung einer technischen Einrichtung durch den Einsatz technischer Mittel (den Erläuterungen zufolge soll ein sogenannter IMSI-Catcher zum Einsatz gelangen) zur Feststellung von geografischen Standorten und IMSI-Nummern (International Mobile Subscriber Identification) ohne die Mitwirkung eines Telekommunikationsanbieters oder eines sonstigen Dienstanbieters geschaffen werden.

Den Erläuterungen folgend soll eine eigenständige Definition und Regelung der vorgenannten Ermittlungsmethode die Technologieneutralität der StPO weiterhin gewährleisten und dem Rechtsanwender Klarheit über die Reichweite der Ermittlungsbefugnisse vermitteln.

Bereits jetzt wird im Bereich des Sicherheitspolizeigesetzes (SPG) (eingeführt durch die Novelle des SPG 2008) der Einsatz von technischen Mitteln zur Lokalisierung einer Endeinrichtung im Rahmen der Gefahrenabwehr in § 53 Abs 3b SPG eigenständig geregelt. Es stellt sich somit die Frage, ob eine weitere Regelung tatsächlich dem Rechtsanwender (eine ohnehin aufgrund der derzeitigen Gesetzeslage schon bestehende) Klarheit über die Reichweite der Ermittlungsbefugnisse vermitteln wird.

Gem § 53 Abs 3 SPG beschränkt sich die Zulässigkeit dieser Maßnahme auf Hilfeleistung oder Abwehr einer gegenwärtigen Gefahr für das Leben, die Sicherheit oder die Freiheit eines Menschen. In der vorliegenden Bestimmung der StPO soll diese Maßnahme bereits bei minderschweren Straftaten mit Strafandrohung von mehr als einem Jahr zulässig sein. Die Eingriffsintensität des Einsatzes eines IMSI-Catchers steht hierbei nicht im Verhältnis zur Schwere der Straftat.

Überdies soll dem Entwurf zufolge für den Einsatz eines IMSI-Catchers eine staatsanwaltliche Anordnung ohne gerichtliche Bewilligung genügen. Da durch den Einsatz eines IMSI-Catchers jedoch eine präzise geographische Ortung einer Person innerhalb einer Funkzelle und somit auch die Erstellung eines exakten Bewegungsprofils der überwachten Person möglich ist, ist diese Ermittlungsmethode wertungsgemäß einer Standortbestimmung iSd § 134 Z 2 und § 135 Abs 2 StPO zumindest gleichzuhalten. Für eine solche Standortbestimmung ist jedoch eine gerichtliche Bewilligung vorgesehen.

Warum trotz vergleichbarer Eingriffsintensität der Einsatz eines IMSI-Catchers dem Erfordernis der gerichtlichen Bewilligung entzogen sein soll, ist nicht nachvollziehbar und findet auch in den Erläuterungen keine Erklärung.

Die Bundesarbeitskammer regt aufgrund der zuvor beschriebenen Eingriffsintensität dringend an, die vorgeschlagene Bestimmung dahingehend zu überarbeiten, dass der Einsatz einer Ermittlungsmaßnahme zur Lokalisierung einer technischen Einrichtung nur aufgrund einer gerichtlich bewilligten Anordnung passieren darf.

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):

Mit dem vorliegenden Entwurf soll die Überwachung verschlüsselter Nachrichten ermöglicht werden.

Die geplante Ermittlungsmaßnahme soll – anders noch als im Ministerialentwurf aus dem Jahr 2017 – nicht mehr bei allen Straftaten, die in die Zuständigkeit des Schöffengerichts fallen, zur Überwachung herangezogen werden dürfen, sondern nur bei mit mehr als fünfjähriger Freiheitsstrafe bedrohten Verbrechen gegen Leib und Leben oder die sexuelle Selbstbestimmung. In Hinblick auf die Grundrechtsintensität des Eingriffs ist es jedoch noch immer bedenklich, ob hier die gebotene Verhältnismäßigkeit zwischen dem Grundrechtseingriff und der aufzuklärenden strafbaren Handlung angenommen werden kann.

Aus dem Gesetzesentwurf lässt sich nicht ableiten, ob und wie technisch sichergestellt werden kann, dass nicht auch über die Kommunikationsdaten hinausgehende 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 beschränkt werden soll, nichts. Vielmehr stellt sich die Frage, wie die Überwachung übermittelter Nachrichten logisch von der Durchsuchung lokal gespeicherter Dateien am Zielsystem getrennt werden kann, wenn die Überwachungssoftware verwertbare Ermittlungsergebnisse liefern soll. Da Dateien vor der Übermittlung durch Kommunikationssoftware verschlüsselt werden können, müsste die Überwachungssoftware einen Überblick über sämtliche Dateien des überwachten Systems haben, um einen Nutzen zu haben. Würde dies jedoch zugelassen, so käme dies einem unverhältnismäßigen Grundrechtseingriff gleich. Auch im Falle der Anordnung der Ermittlungsmaßnahmen für einen künftigen Zeitraum besteht entgegen den Erläuterungen die Gefahr, dass durch die Installation der Überwachungssoftware auf lokal abgespeicherte, nicht mit dem Übertragungsvorgang im Zusammenhang stehende Daten zugegriffen werden könnte, was faktisch einer Online- Durchsuchung gleichkäme.

In § 135a Abs 2 Z 1 StPO des vorliegenden Entwurfs ist vorgesehen, dass die auf dem Zielsystem installierte Überwachungssoftware nach Beendigung der Ermittlungsmaßnahme „funktionsunfähig ist oder ohne dauerhafte Schädigung oder Beeinträchtigung des Computersystems, in dem es installiert wurde,…“ entfernt werden kann. Aus technischer Sicht kann nicht sichergestellt werden, ob die Überwachungssoftware funktionsunfähig wird, da ein Programm seine eigene Deinstallation nicht überprüfen kann. Weiters könnte die Formulierung „…oder ohne dauerhafte Schädigung…“ dahingehend interpretiert werden, dass eine dauerhafte Schädigung oder Beeinträchtigung des Computersystems in Kauf zu nehmen wäre, wenn das Programm funktionsunfähig wird, aber aus dem betroffenen Computersystem nicht entfernt wird und (schädigend) in diesem verbleibt.

Dass Streuschäden und Kollateralschäden vermieden werden sollen, wird in den Erläuterungen zwar neuerlich angesprochen, doch wie eine solche Vermeidung technisch sichergestellt werden soll, ist den Erläuterungen nicht zu entnehmen.

Um die geplante Ermittlungsmaßnahme vollziehen und unbemerkt eine Software auf dem Computersystem einer Zielperson installieren zu können, ist es notwendig, Sicherheitslücken gängiger Betriebssysteme zu kennen. Zur Beschaffung dieser Informationen muss der Staat Informationen über diese Sicherheitslücken entweder direkt oder indirekt (über den Hersteller der staatlichen Spionagesoftware) am Schwarzmarkt zukaufen. Dadurch wird ein Interesse daran entwickelt, dass bestehende Sicherheitslücken geheim bleiben und damit offengehalten werden, was insgesamt zu einer Verringerung der Sicherheit von Nutzern von Computersystemen und einer denkbaren Gefährdung der gesamten kritischen Infrastruktur des Staates führt, da Hersteller mangels der Meldung von Sicherheitslücken nicht für deren Schließung sorgen können.

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.

In § 145 Abs 4 letzter Satz StPO des Entwurfs sollte die Wendung „…entfernt, oder dieses funktionsunfähig wird“ lauten, da sich das Wort „dieses“ wohl auf das für die Überwachung genutzte Programm bezieht.

Rudi Kaske
Präsident
F.d.R.d.A.

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