

Bundesministerium für Inneres  
Herrengasse 7  
1010 Wien

Ihr Zeichen	Unser Zeichen	Bearbeiter/in	Tel 501 65	Fax 501 65	Datum
BMI-LR1340/ 0019-III/1/2017	AR-GStBAK/Ap	Christos Kariotis	DW 2864	DW 2471	18.08.2017

Bundesgesetz, mit dem das Sicherheitspolizeigesetz, das Bundesstraßen-Mautgesetz 2002, die Straßenverkehrsordnung 1960 und das Telekommunikationsgesetz 2003 geändert werden

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

**Allgemeines:**

Gemäß den Erläuterungen verfolgt der vorliegende Gesetzesentwurf im Wesentlichen den Ausbau der technischen Ermittlungsmöglichkeiten durch die Sicherheitsbehörden.

Zunächst wird festgehalten, dass die Bundesarbeitskammer Maßnahmen, die dem Zweck der Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit dienen, grundsätzlich begrüßt. Der ständige Wandel des technischen Fortschrittes kann es vereinzelt notwendig machen, auch die Möglichkeiten der technischen Ermittlungsmaßnahmen der Sicherheitsbehörden anzupassen, um (insb organisierte) schwere Straftaten effizient, schnell und gezielt verhindern bzw vorbeugen zu können.

Das Bedürfnis nach Sicherheit in der Bevölkerung (insb aufgrund von Terroranschlägen in jüngerer Vergangenheit) steigt. Die Erwartungshaltung der Bevölkerung, dass der Staat Maßnahmen setzen soll, um die Unversehrtheit des Einzelnen zu schützen, ist durchaus nachzuvollziehen. Es stellt sich jedoch die Frage, ob die Maßnahmen, die dem vorliegenden Gesetzesentwurf zu Grunde liegen, in einem angemessenen Verhältnis zu den verfassungsrechtlich gewährleisteten Grundrechten des Einzelnen stehen und zweckmäßig sind.

Im Hinblick auf die terroristischen Anschläge im Vereinigten Königreich in jüngerer Vergangenheit ist anzumerken, dass diese trotz weitreichender technischer Überwachungsmöglichkeiten (insbesondere auch durch die britischen Geheimdienste) schlussendlich nicht verhindert werden konnten. Die Täter waren zumeist polizeibekannt und wurden auch zuvor überwacht.

Maßnahmen der Überwachung bzw der Ausbau der Ermittlungsmöglichkeiten mit dem Ziel die öffentliche Sicherheit zu gewährleisten, stehen regelmäßig in einem Spannungsverhältnis mit verfassungsrechtlich gesicherten Grundrechten, weshalb die vorgeschlagenen Änderungen insbesondere im Lichte des Datenschutzes und der Achtung des Privat- und Familienlebens (Artikel 8 der EMRK) zu beurteilen sind.

In Anbetracht dessen, dass lange vor Ablauf der Begutachtungsfrist bereits tausende kritische Stellungnahmen einzelner Personen zum vorliegenden Gesetzesentwurf eingegangen sind, wird auf die Notwendigkeit einer gesellschaftspolitischen Diskussion in Teilbereichen des Sicherheitspakets hingewiesen.

Der vorliegende Gesetzesentwurf sieht überaus weitreichende und flächendeckende Überwachungsmaßnahmen vor. Bei einigen 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. Einige der geplanten Maßnahmen sind überschießend und zu wenig genau determiniert.

Aus den genannten Gründen wird aus Sicht der Bundesarbeitskammer eine grundlegende Überarbeitung des vorgeschlagenen Gesetzesentwurfs - im Sinne einer genaueren Determinierung der betreffenden Bestimmungen - ausdrücklich empfohlen.

### **Zu den Bestimmungen im Detail:**

#### **Artikel 1 (Änderung des SPG)**

##### **§ 25 iVm § 56 Abs 1 SPG (sicherheitspolizeiliche Beratungen) „Sicherheitsforen“:**

Mit Ergänzung der betreffenden Regelung sollen Sicherheitsbehörden zur Vorbeugung gefährlicher Angriffe gegen Leben, Gesundheit und Vermögen, befugt sein, Plattformen („Sicherheitsforen“) unter Einbeziehung von Menschen, die an der Erfüllung von Aufgaben im öffentlichen Interesse mitwirken, zu bilden. Im Rahmen dieser Sicherheitsforen sollen auf regionaler Ebene erforderliche Maßnahmen erarbeitet und koordiniert werden.

Ein Informationsaustausch innerhalb dieser Foren soll insoweit zulässig sein, als dass es sich um Informationen handelt, die den Teilnehmern dem Grunde nach bekannt sind oder deren Weitergabe im wesentlichen Interesse Betroffener ist.

Den vorliegenden Erläuterungen nach sollen diese Sicherheitsforen etwa privaten Vereinen, NGO's oder sonstigen freiwilligen Privatpersonen ermöglichen, gemeinsam mit den Sicherheitsbehörden Problemlösungen in Sicherheitsfragen zu erarbeiten.

Aus Sicht der Bundesarbeitskammer kann eine Zusammenarbeit zwischen Sicherheitsbehörden und privaten Personen **im konkreten Einzelfall** sinnvoll sein, um einen effizienten und praxistauglichen Lösungsansatz zur Vorbeugung bzw Verhinderung von Straftaten zu schaffen. Genauer zu normieren wäre jedoch wie diese Zusammenarbeit gestaltet sein soll und welche Aufgaben Privatpersonen in diesem Zusammenhang erfüllen können/dürfen/sollen.

Die Grenzen des Informationsaustausches innerhalb dieses Sicherheitsforums sind im vorliegenden Gesetzesentwurf weitestgehend unscharf formuliert.

Die Formulierungen, welche Informationen „... dem Grunde nach bekannt sind...“ und „... im wesentlichen Interesse Betroffener ist...“ und daher ausgetauscht werden dürfen, lässt einen äußerst weitreichenden Interpretationsspielraum offen. Eine Konkretisierung schafft auch die vorgesehene Einschränkung des Informationsaustausches, wonach „...nicht besondere Gründe vorliegen (dürfen), die dennoch für eine Geheimhaltung sprechen...“ nicht, da hier ebenso nicht konkretisiert wird, ab wann solche besonderen Gründe, die eine Geheimhaltung rechtfertigen, vorliegen.

Aufgrund des überaus weiten Interpretationsspielraumes dieser Formulierungen besteht die Gefahr, dass es zu Datenschutzverletzungen kommt, da gänzlich im Dunkeln bleibt, welche Informationen konkret ausgetauscht werden dürfen. Eine klare und einschränkende Formulierung wie, wann und warum Sicherheitsbehörden Informationen an private Personen weitergeben dürfen, ist aus Sicht der Bundesarbeitskammer unerlässlich.

Problematisch in diesem Zusammenhang erscheint darüber hinaus die Frage, in welchem Ausmaß Privatpersonen überhaupt geeignet sind, Problemlösungen in Sicherheitsfragen zu „erarbeiten“, um Kriminalität vorzubeugen. Vielmehr fällt es in die Kompetenz der zuständigen Sicherheitsbehörden Beratungs- und Präventionsarbeit bei den betroffenen Bürgern zu leisten. Es wird an dieser Stelle festgehalten, dass die Kompetenz zur Verfolgung von Straftaten ausschließlich den Sicherheitsbehörden zukommt, weshalb eine Mitwirkung durch Privatpersonen im betreffenden Bereich aus Sicht der Bundesarbeitskammer äußerst kritisch gesehen wird. Die Weitergabe von (schutzwürdigen) personenbezogenen Daten Dritter an Privatpersonen birgt zudem jedenfalls die Gefahr von Vorverurteilungen unbescholtener Dritter.

Das vorgeschlagene Konzept von „Sicherheitsforen“ sollte nicht dazu dienen, Bürgerwehren oder gar die Schaffung von „Ersatzpolizisten“ zu fördern, weshalb es aus Sicht der Bundesarbeitskammer jedenfalls notwendig ist, den Kreis der teilnahmeberechtigten „Sicherheitspartner“ an solchen Foren einzuschränken bzw auch Voraussetzungen zu schaffen, unter denen jemand überhaupt an solchen Foren teilnehmen darf.

Im Hinblick auf die Einrichtung solcher Sicherheitsforen wäre darüber hinaus zu bedenken, dass bei einer etwaigen Verwirklichung eines solchen Konzepts, den Sicherheitsbehörden ausreichend Personalressourcen zur Verfügung zu stellen wären, um eine Überlastung der Beschäftigten der Sicherheitsbehörden zu vermeiden.

**§ 53 Abs 5, § 84 Abs 1 Z 7, § 91c Abs 3 sowie § 93 a („Videoüberwachung“ und „Echtzeitstreaming“):**

§ 53 Abs 5 SPG normiert eine massive Ausweitung der Videoüberwachung, wonach Sicherheitsbehörden für die Zwecke der Vorbeugung wahrscheinlicher oder Abwehr gefährlicher Angriffe, Zugriff auf aufgezeichnete Bilddaten von Behörden und Unternehmen mit öffentlichen Versorgungsauftrag erhalten sollen bzw ihnen ein Zugriff auf (etwaig vorhandene) Echtzeitstreamings einzuräumen ist. Laut Gesetzesvorschlag handelt es sich hierbei um eine Verpflichtung der betreffenden Rechtsträger, eben diese Daten auf Verlangen der Sicherheitsbehörden zur Verfügung zu stellen. Ab Kenntnis eines solchen Verlangens darf der verpflichtete Rechtsträger die verlangten Bilddaten nicht löschen.

Weiters sollen die Sicherheitsbehörden im Einzelfall berechtigt sein, für sämtliche in § 53 Abs 1 SPG genannte Zwecke personenbezogene Bild- **und Tondaten** zu verwenden, die ihnen freiwillig von privaten oder öffentlichen Rechtsträgern übergeben worden sind.

Die weitgehende Unbestimmtheit der angeführten Zwecke („...Vorbeugung wahrscheinlicher oder Abwehr gefährlicher Angriffe...“) zur Verwendung von Daten Dritter gibt Anlass zur Sorge, dass Zugriffe auf Bild- oder Tondaten in unverhältnismäßiger Weise erfolgen könnten. Darüber hinaus ist aufgrund des großen Umfangs der Datenquellen, auf die ein Zugriff möglich sein soll (Videomaterial der Asfinag, ÖBB, Wiener Linien etc.), mit zahlreichen Eingriffen in die Privatsphäre Unbeteiligter zu rechnen.

Der normierte Verweis, wonach „...*besonders darauf zu achten... (ist)...*, dass *Eingriffe in die Privatsphäre der Betroffenen die Verhältnismäßigkeit (§29) zum Anlass wahren...*“, erscheint dahingehend unzureichend, zumal unklar bleibt, wer die Verhältnismäßigkeit überprüft. Aus Sicht der Bundesarbeitskammer wird für die Zulässigkeit der Verarbeitung von Bilddaten eine restriktive und abschließende Aufzählung der Zwecke sowie eine Einschränkung auf bestimmte schwere Straftaten als unerlässlich angesehen.

Das Zugriffsrecht auf Videoüberwachungsanlagen erfordert entgegen den Vereinbarungen im Arbeitsprogramm der Regierung 2017/2018 keine staatsanwaltliche Anordnung, sondern ist vielmehr lediglich auf Verlangen der Sicherheitsbehörden zu ermöglichen. Eine solche Befugnisenerweiterung der Sicherheitsbehörden wird auch in den Erläuterungen nicht begründet und kann daher nicht nachvollzogen werden.

Auch lässt der in § 53 Abs 5 SPG verwendete Begriff der „...*Rechtsträger des privaten Bereiches, sofern...(ihnen)...ein öffentlicher Versorgungsauftrag zukommt...*“ weitreichenden Interpretationsspielraum offen, der dazu führt, dass beispielsweise Supermärkte, Banken, Ärztezentren oder Restaurants in kleinen Orten betroffen sein könnten. Eine Klarstellung im

Sinne der Erläuterungen, wonach etwa ÖBB, ASFINAG, Post etc gemeint sind, sollte definiert werden.

Die Einschränkung des § 91c Abs 3 SPG, wonach die Fortsetzung einer Maßnahme gemäß § 53 Abs 5 SPG über die Dauer von drei Tagen die ausdrückliche Zustimmung des Rechtsschutzbeauftragten erfordert, ist zwar zu begrüßen, erscheint jedoch im Hinblick auf die Schwere des Eingriffs in Datenschutzrechte und den Schutz der Privatsphäre Unbeteiligter als nicht angemessene Rechtsschutzgarantie.

Hingewiesen wird darauf, dass die in § 93a SPG vorgeschlagene Verpflichtung, wonach der Betrieb von Videoüberwachungsanlagen den Sicherheitsbehörden zu melden ist, im Hinblick auf die bereits bestehende Meldepflicht im Datenverarbeitungsregister doppelgleisig wäre.

In § 93a 2. Satz SPG ist weiter geregelt, dass die Sicherheitsbehörden, sofern es im Einzelfall aus Gründen der Aufrechterhaltung der öffentlichen Sicherheit oder der Strafverfolgung erforderlich ist, mittels Bescheid eine zweiwöchige Aufbewahrungsverpflichtung der Bildaufnahmen festlegen können.

Zu bedenken gilt hier, dass bei den meisten bestehenden Videoüberwachungsanlagen eine Speicherdauer von bis zu zwei Wochen aus datenschutzrechtlichen Gründen nicht vorgesehen ist und daher mit Umrüstkosten (zB Erweiterung der Speicherkapazität) zu rechnen ist.

**Zu Z 4: § 53a Abs 6 – „Datenanwendungen der Sicherheitsbehörden“:**

Mit vorgeschlagener Änderung soll die Speicherfrist für Daten von Verdächtigen bei Ermittlungen im Zusammenhang mit vorsätzlich begangenen strafbaren Handlungen, die mit einer Freiheitsstrafe von mindestens drei Jahren bedroht sind, von drei auf fünf Jahre verlängert werden. Dies soll gemäß den vorliegenden Erläuterungen aufgrund der langen Ermittlungsdauer im Bereich der organisierten Kriminalität notwendig sein.

Die Notwendigkeit der Verlängerung der Frist erscheint nachvollziehbar, weshalb aus Sicht der Bundesarbeitskammer kein Einwand zu betreffender Änderung besteht.

**§§ 54 Abs 4b, 57 Abs 2a SPG, 19 a Abs 1a Bundesstraßen Mautgesetz und § 98a Abs 2 StVO – Kennzeichenerfassungssysteme, Herausgabepflicht von Verkehrsdaten:**

Mit betreffender Regelung soll zum Zwecke der Fahndung und zur Abwehr und Aufklärung gefährlicher Angriffe die Identifizierung von Fahrzeugen ausgeweitet werden. In diesem Zusammenhang sollen über das Kennzeichen hinausgehende Informationen, nämlich „...insbesondere...“ Fahrzeugmarke, Fahrzeugtype, Fahrzeugfarbe sowie Fahrzeuglenker von Sicherheitsbehörden verarbeitet werden dürfen. Die zu erfassenden Daten sollen längstens nach 48 Stunden, wenn sie nicht zur weiteren Verfolgung aufgrund eines Verdachts strafbarer Handlungen erforderlich sind, wieder zu löschen sein.

Das bedeutet, dass die betreffenden Informationen künftig für eine Zeitspanne von zumindest 48 Stunden gespeichert werden sollen, auch ohne dass ein konkreter Verdacht einer strafbaren Handlung vorliegt.

Die Argumentation in den Erläuterungen für die zeitlich befristete Speichernotwendigkeit der Informationen ist, dass die derzeitige Regelung insofern mangelhaft ist, da bei Fahrzeugdiebstählen nur dann ein Treffer in der Fahndungsevidenz angezeigt werden kann, wenn im Zeitpunkt der Erfassung des Kennzeichens das Fahrzeug bereits zur Fahndung ausgeschrieben wurde (was bei Fahrzeugdiebstählen in den Nachtstunden, die oft erst am nächsten Tag erkannt und zur Anzeige gebracht werden, regelmäßig nicht der Fall ist). Dies kann aus Sicht der Bundesarbeitskammer grundsätzlich nachvollzogen werden.

Bedenklich erscheint in diesem Zusammenhang jedoch, ob solch ein Mittel der Massenüberwachung und damit einhergehender Vorratsdatenspeicherung für die genannten Zwecke ohne ein konkretes Verdachtsmoment verhältnismäßig ist. Die pauschale Speicherung von schutzwürdigen Daten von Personen, die nicht unter Verdacht stehen eine Straftat begangen zu haben, erscheint mangels Verhältnismäßigkeit des Eingriffs verfassungsrechtlich bedenklich und mit dem Grundrecht auf Privatsphäre nicht vereinbar.

Die vorgeschlagene Erweiterung der speicherbaren Merkmale wird durch die demonstrative Aufzählung („insbesondere“) nicht abschließend determiniert, weshalb auch die uneingeschränkte Verarbeitung anderer Informationen möglich wäre. Eine taxative Aufzählung zur Klarstellung wird in diesem Zusammenhang ausdrücklich empfohlen, da ansonsten nicht klar ist, welche Informationen verarbeitet werden dürfen und eine überschießende Datensammlung vermieden werden kann.

Darüber hinaus lässt die Erweiterung der Datenverarbeitungsmöglichkeit um den Zweck der Abwehr und Aufklärung gefährlicher Angriffe einen sehr weiten Interpretationsspielraum zu. Eine Einschränkung auf bestimmte strafrechtliche Delikte wird an dieser Stelle empfohlen.

Zu bedenken gilt hier zudem, dass eine effiziente Fahndung über Kennzeichenerfassungssysteme eine möglichst flächendeckende Infrastruktur von bildverarbeitenden technischen Einrichtungen im gesamten Bundesgebiet erfordern würde. Zudem müssten sämtliche Videokameras mit einer eigenen (Kennzeichen-)Erkennungssoftware ausgestattet werden. Die finanziellen Auswirkungen auf den Bund, insbesondere in Anbetracht des Kosten-Nutzen-Verhältnisses, sollten aus diesen Gründen vorab eruiert werden.

#### **§ 92a Abs 1a SPG (Kostenersatz für Einschreiten der Sicherheitsbehörden)**

Mit vorgeschlagener Änderung soll künftig derjenige die Kosten für ein Einschreiten der Organe öffentlicher Sicherheitsbehörden ersetzen, der „...*vorsätzlich eine falsche Notmeldung abgibt...*“ oder der „...*sich grob fahrlässig (§ 6 Abs 3 StGB) einer Gefahr für Leben oder Gesundheit ausgesetzt hat...*“.

Die Intention des Gesetzgebers kann hinsichtlich der vorgeschlagenen Änderungen dem Grunde nach durchaus nachvollzogen werden.

Aus Sicht der Bundesarbeitskammer gilt es jedoch zu bedenken, dass es in der Praxis für den Normalbürger oft schwierig ist einzuschätzen, ob eine konkrete Gefahrensituation, die eine Notmeldung notwendig macht, vorliegt oder nicht. Zu denken wäre hier beispielsweise an Fälle häuslicher Gewalt, bei denen die Lage bei Eintreffen der Polizei ruhig erscheint oder eine Gefahrensituation fälschlicherweise angenommen wurde. Die Regelung birgt die Gefahr (insbesondere bei zu extensiver Exekution dieser Norm), dass die Normadressaten aus Angst, als „Falschmelder“ abgestempelt zu werden und daher die Kosten für das Einschreiten der Sicherheitsbehörden tragen zu müssen, die Polizei gar nicht oder seltener alarmieren, obwohl dies, notwendig gewesen wäre.

Im Hinblick auf den, mit diesem Gesetzesentwurf verfolgten Zweck der effizienten Kriminalitätsbekämpfung, erscheint diese Regelung inkonsequent. Einerseits sollen sich Privatpersonen im Bereich der Kriminalitätsbekämpfung mehr einbringen (siehe „Sicherheitsforen“) und gemäß den vorliegenden Erläuterungen im Bereich der Prävention auf sicherheitspolizeilichen Gebiet in einem höheren Ausmaß mitwirken. Andererseits wird mit dieser Bestimmung, eine Mitwirkung von Privatpersonen, die eine falsche Notmeldung billig in Kauf genommen haben (im Sinne eines bedingten Vorsatzes gemäß § 5 Abs. 1 StGB), mit dem Ersatz der Kosten für das Einschreiten der Sicherheitsbehörden bestraft.

#### **Artikel 4 (Änderung des Telekommunikationsgesetzes 2003)**

##### **§ 17 Abs 1a TKG:**

Mit vorgeschlagener Änderung soll es Anbietern von Internetzugangsdiensten künftig erlaubt werden, Verkehrsmanagementmaßnahmen im Sinn des Art. 3 der Verordnung (EU) 2015/2120 zur Vermeidung von strafrechtlich relevanten Handlungen anzubieten. Internetprovider können demnach auf Inhalte zugreifen und bei strafrechtlicher Relevanz der Inhalte dieselben einschränken oder gar gänzlich blockieren.

Klargestellt sei an dieser Stelle, dass die Bundesarbeitskammer Maßnahmen, die die Verbreitung von gewaltverherrlichenden oder pornografischen Darstellungen im Sinn der Jugendschutzgesetze an Minderjährige im Internet verhindern sollen, durchaus begrüßt und gesellschaftspolitisch als überaus wichtig erachtet.

Unabhängig davon bedeutet der vorliegende Vorschlag eine deutliche Einschränkung des europarechtlichen Grundsatzes der Netzneutralität bzw scheint mit diesem nicht im Einklang zu stehen. Verkehrsmanagementmaßnahmen sind gemäß Art 3 der betreffenden EU-VO 2015/2120 nur in engen Grenzen bzw unter bestimmten Voraussetzungen erlaubt und müssen angemessen sein. Laut betreffender EU-Verordnung sind solche Maßnahmen nur möglich, sofern sie der Sicherstellung der Netzintegrität, der Verhinderung einer drohenden Netzüberlastung oder der Umsetzung von Gesetzgebungsakten der Union oder mit dem Unionsrecht im Einklang stehenden nationalen Rechtsvorschriften dienen.

Der vorliegende Entwurf lässt jedoch die genaueren Umstände solcher Verkehrsmanagementmaßnahmen gänzlich offen.

Die Entscheidung, ob Inhalte eine strafrechtliche Relevanz haben und welche konkreten Methoden gegebenenfalls eingesetzt werden, sollte keinesfalls ein privater Internetprovider treffen können. Die vorgeschlagene Fassung sieht auch in keiner Weise ein rechtsförmiges Verfahren oder gar etwaige Verfahrensgarantien vor.

Aus den genannten Gründen wird diese Bestimmung aus Sicht der Bundesarbeitskammer äußerst kritisch gesehen.

**§ 92 Abs 3 Z 3 lit g; § 97 Abs 1 a; (Abschaffung der anonymen SIM-Karten)**

Die betreffenden Bestimmungen sehen vor, dass die Stammdaten von Wertkartenhandybenutzer künftig registriert werden sollen, um die Identität der Wertkarteninhaber im Anlassfall festzustellen. Dies sei gemäß den Erläuterungen aufgrund sicherheits- und kriminalpolizeilicher Zwecke erforderlich. Damit wird die bisher in Österreich bestehende Möglichkeit eine SIM-Karte anonym zu erwerben und zu verwenden abgeschafft.

Einerseits bedeutet diese Änderung einen großen Erhebungs- und Personalaufwand für die (vor allem kleinere) Betreiber, der wiederum mit noch nicht abschätzbaren Kosten verbunden ist. Andererseits bedeutet dies für Konsumenten einen größeren Aufwand beim Erwerb einer SIM-Karte. Es ist zudem damit zu rechnen, dass die Mehrkosten auf den Konsumenten abgewälzt werden.

Zu bedenken gilt zudem, dass die Nutzung von ausländischen SIM-Karten oder anderen anonymen Messaging-Diensten (und damit ein Ausweichen in die Anonymität) nicht verhindert werden kann. Aus Sicht der Bundesarbeitskammer kann eine effiziente Terrorismusbekämpfung im Bereich der Telekommunikation nur auf gesamteuropäischer bzw. internationaler Ebene erfolgreich sein. Die Tatsache, dass die Anschaffung von ausländischen SIM-Karten (in Ländern wie zB Tschechien, Slowenien oder Kroatien) ohne Registrierung möglich ist, unterläuft die verfolgten Zwecke gänzlich.

Vor diesem Hintergrund ist die geplante Maßnahme überaus nachteilig für Millionen betroffene Handynutzer, ohne dass gleichzeitig ein nachweisbarer Nutzen für die Bekämpfung von schwerer Kriminalität nachvollzogen werden kann.

Aus Sicht der Bundesarbeitskammer ist daher die vorgeschlagene Maßnahme abzulehnen.

**§ 99 Abs 1a bis 1f („Quick-Freeze-Modell“)**

Mit vorgeschlagener Änderung soll eine Speicherung von Telekommunikationsdaten (Verkehrs-, Standort- und Zugangsdaten) durch eine Anordnung der Staatsanwaltschaft bis zu zwölf Monaten möglich sein (im Sinne einer Vorratsdatenspeicherung).



Gemäß den Erläuterungen soll bei „Vorliegen eines Anfangsverdachts“ die Möglichkeit bestehen, dass Telekommunikationsanbieter durch staatsanwaltliche Anordnung verpflichtet werden, betreffende Daten zunächst zu speichern. Eine richterliche Bewilligung ist erst bei Beauskunftung dieser Daten erforderlich.

In diesem Zusammenhang ist zu befürchten, dass es - mangels Notwendigkeit einer gerichtlichen Anordnung für die Speicherung von Daten - zu einem überbordenden Einsatz dieser Möglichkeiten durch die Staatsanwaltschaft kommen könnte. 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 erforderlich sind, was der vorliegende Entwurf aus Sicht der Bundesarbeitskammer jedoch übersieht.

Rudi Kaske  
Präsident  
F.d.R.d.A.

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