BM.I REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES
SEKTION III-RECHT

GZ.: BMI-LR1429/0054-III/1/2009 Wien, am 11. Jänner 2010

An das
Bundesministerium für Verkehr, Innovation und Technologie

Abteilung III/PT2 (Recht)

Radetzkystraße 2
1030 Wien
Zu Zl: BMVIT-630.333/0001-III/PT2/2009

Mag. Verena Weiss
BMI - III/1 (Abteilung III/1)
Herrengasse 7, 1014 Wien
Tel.: +43 (01) 531262377
Pers. E-Mail: Verena.Weiss@bmi.gv.at
Org.-E-Mail: BMI-III-1@bmi.gv.at
WWW.BMI.GV.AT
DVR: 0000051
Antwortschreiben bitte unter Anführung der GZ an die Org.-E-Mail-Adresse.

Betreff: Legistik und Recht; Fremdlegistik; BG-BMVIT
Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 – TKG 2003 geändert wird

Aus Sicht des Bundesministeriums für Inneres ergeben sich zu dem im Betreff genannten Entwurf folgende Bemerkungen:

I. Allgemeines:

Die hohe Sensibilität der „lückenlosen“ Speicherung von Kommunikationsdaten durch die Betreiber und die im allgemeinen Teil der Erläuterungen (insb. in FN 1) angesprochene Möglichkeit, aus der Zusammenschau bloßer Verkehrsdaten, etwa einem Anruf bei der Aidshilfe, oder dem Emailkontakt zu einem bestimmten Versandhaus, Rückschlüsse auf Kommunikationsinhalte oder auf das Kaufverhalten eines Kommunikationsteilnehmers zu schließen, wird nicht verkannt. Zur Vermeidung des „gläsernen Menschen“ ist es daher absolut erforderlich, die Zwecke und Voraussetzungen für den Zugriff und damit die Auswertbarkeit der bei den Betreibern anfallenden Kommunikationsdaten gesetzlich detailliert und restriktiv zu regeln.
Das geltende Sicherheitspolizeigesetz beinhaltet mit § 53 Abs 3a eine solche restriktive Regelung, die Inhaltsüberwachung oder die Frage an einen Betreiber danach, welche Internetseiten ein bestimmter Teilnehmer auf- oder welche Telefonnummern er angerufen hat, nicht zulässt. Nicht die Überwachung des passiven Internetkonsums steht zur Diskussion. Vielmehr muss ein Kommunikationsteilnehmer seine durch Artikel 8 EMRK geschützte Privatsphäre durch einen eine Aufgabe der Sicherheitsbehörden auslösenden und „nach außen gerichteten“ Kommunikationsvorgang (etwa eine anonyme Drohmail an einen Dritten oder einen Hilferuf oder die Ankündigung einer Straftat in einem Blog)

verlassen haben. Damit ist aber die Aufrechterhaltung der Anonymität nicht mehr mit dem Schutz der Kommunikation rechtfertigbar. Nur die Rückführbarkeit dieses einzelnen Kommunikationsvorgangs auf einen bestimmten Anschluss ist Zweck der sicherheitspolizeilichen Regelung.

1. Grundsätzliches zur Richtlinienumsetzung:

Der vorliegende Entwurf bezweckt die Umsetzung der auf Art 95 EGV gestützten Richtlinie 2006/24/EG über die Vorratsdatenspeicherung, die im Hinblick auf das Funktionieren des Binnenmarktes die Harmonisierung der Pflichten für Diensteanbieter bzw. Netzbetreiber im Zusammenhang mit der Speicherung bestimmter Daten zum Ziel hat. Die vorgeschlagenen Regelungen haben sich daher auf die zur Speicherung verpflichteten Betreiber, den Umfang (Datenarten) der Speicherverpflichtung von „Vorratsdaten“ durch diese, die durch die Richtlinie vorgegebenen Datensicherheitsmaßnahmen sowie die Festlegung der Speicherdauer zu beschränken.

Hinsichtlich der Zweckbindung gemäß der RL 2006/24/EG („Ermittlung, Feststellung und Verfolgung schwerer Straftaten“) und der Möglichkeit, in eingeschränktem Maße auch zu anderen Zwecken auf Kommunikationsdaten (insb. IP-Adressen) zuzugreifen, hat der OGH, der sich mehrfach im Zusammenhang mit Verletzungen des Urheberrechtsgesetzes umfassend mit dieser Frage beschäftigt hat, Folgendes vertreten:

Die Herausgabe von Daten bei Delikten, die über das Internet begangen werden (z.B. Urheberrechtsverletzungen) unterliegt nicht unbedingt der strengen Zweckbindung (Bekämpfung schwerer Straftaten). Er begründet dies damit, dass Art 6 Abs 1 der RL 2002/58/EG vorbehaltlich des Art 15 dieser RL gilt. Der EuGH hat dazu in der Entscheidung C-275/06 (Promusicae) - entgegen den Ausführungen der Generalanwältin Kokott (Rz 99 ff) - ausgeführt, dass die letztgenannte Bestimmung wegen des darin enthaltenen Verweises auf Art 13 Abs 1 der RL 95/46/EG auch Regelungen zum Schutz von Urheberinteressen gestatte. Damit steht es den Mitgliedstaaten aus gemeinschaftsrechtlicher Sicht grundsätzlich frei, die Speicherung und Verarbeitung von Verkehrsdaten auch für die Erteilung von Auskünften über nähere Umstände von Urheberrechtsverletzungen zu erlauben. Dies gilt grundsätzlich unabhängig von den Regelungen der RL 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden. Denn diese Richtlinie ist zwar nach dem durch sie eingefügten Art 15 Abs 1a der RL 2002/58/EG lex specialis gegenüber der allgemeinen Ausnahmeklausel des Art 15 Abs 1 der RL 2002/58/EG, das Weiterbestehen der allgemeinen Ausnahmeklausel zeigt aber, dass der Gemeinschaftsgesetzgeber die Vorratsspeicherung nicht auf Fälle der RL 2006/24/EG beschränken wollte.

2. Grundsätzliches zur Frage des Fernmeldegeheimnisses:

Die (gesamte) Bundesregierung hat – ebenso wie ein Teil der Lehre (Nachweise bei Wiederin in Korinek/Holoubek [Hrsg], Bundesverfassungsrecht III Grundrechte Art 10a StGG Rz 12, insb FN 56) – in ihrer Stellungnahme in den Verfahren G 147, 148/08-2 und G 29/08, G 30/08, G 31/08 und G 35/08 vor dem Verfassungsgerichtshof vertreten, dass der Schutzbereich des Art. 10a StGG auf (geheime) Inhaltsdaten beschränkt ist und die Beauskunftung von Telekommunikationsdaten nach dem Sicherheitspolizeigesetz das Fernmeldegeheimnis nicht berührt.

In seinem zurückweisenden Erkenntnis G 147/08 vom 1.7.2009 hat der Verfassungsgerichtshof dazu Folgendes ausgeführt:

„ …Die hier angegriffenen Bestimmungen des SPG gestatten hingegen nicht - wie von den Antragstellern befürchtet - die "geheime Überwachung des Fernmeldeverkehrs". § 53 Abs3a SPG ermächtigt die Sicherheitsbehörden vielmehr bloß, bei Vorliegen gesetzlich bestimmter Voraussetzungen von Betreibern öffentlicher Telekommunikationsdienste und von sonstigen Diensteanbietern bestimmte Auskünfte zu verlangen. Auch § 53 Abs 3b SPG bietet keine Grundlage für die Ermittlung von Inhaltsdaten von Mobiltelefongesprächen (vgl. VfGH 1.7.2009, G31/08). Die gegen Bestimmungen des SPG gerichteten Anträge sind daher schon deshalb unzulässig.

Im Übrigen wird auch noch auf Folgendes hingewiesen:

Personen, die den konkreten Verdacht hegen, dass ihre Daten aufgrund der angegriffenen Bestimmungen des SPG ermittelt wurden, stehen das Auskunftsrecht gemäß §26 DSG 2000, das Löschungsrecht gemäß §27 DSG 2000 (etwa wegen Wegfalls des gesetzlichen Zwecks der Datenerhebung), das Beschwerderecht gemäß §31 DSG 2000 iVm §90 SPG, aber auch die Eingabe an die Datenschutzkommission gemäß §30 Abs1 DSG 2000, die im Fall eines begründeten Verdachtes zu einer Systemprüfung gemäß §30 Abs2 DSG 2000 führen kann, zur Verfügung.

Schließlich wird auch auf den kommissarischen Rechtsschutz durch den Rechtsschutzbeauftragten (vgl. §§ 91a bis 91d SPG) hingewiesen. …“

Mit Urteil vom 14.7.2009, 4 Ob 41/09xn hat sich der OGH ebenfalls mit der Frage des Richtervorbehalts auseinandergesetzt und im Hinblick auf die ergangene Vorabentscheidung C-557/07 (LSG/Tele2) des EUGH betont, dass *aus dem Gemeinschaftsrecht die Notwendigkeit eines Richtervorbehalts nicht mehr abgeleitet werden könne*. Gegen die *nationale* verfassungsrechtliche Notwendigkeit eines Richtervorbehalts (dazu zuletzt etwa Edthaler/Schmid, Auskunft über IP-Adressen im Strafverfahren, MR 2008, 220 [222 ff] mwN) im konkreten Fall spricht laut OGH, *dass die Verarbeitung der sensiblen Verkehrsdaten intern erfolgt und nach außen nur Stammdaten bekanntgegeben werden.* Der Verletzte will nicht

Verkehrsdaten erfahren (welche Internetseiten hat ein bestimmter Nutzer wann besucht), sondern (umgekehrt) zu einer bereits bekannten Nutzung eines bestimmten Internetangebots Name und Anschrift des Nutzers erfahren.
Auf dieser - auch der Entscheidung 11 Os 57/05z zugrunde liegende und im österreichischen Schrifttum mehrfach betonten (Daum, Glosse zu 11 Os 57/05z, MR 2005, 354; Edthaler/Schmid, MR 2008, 223; Stomper, MR 2005, 120 f; Walter, MR 2007, 442 f) - Differenzierung basiert auch die einstweilige Anordnung des deutschen Bundesverfassungsgerichts zur Umsetzung der RL 2006/24/EG, in der das BVerfG das (vorläufige) Verbot einer Bestandsdatenauskunft unter Verwendung gespeicherter Verkehrsdaten ablehnte, dies jedoch mit dem Hinweis auf eine im Hauptverfahren dennoch erforderliche Prüfung (1 BvR 256/08 vom 28. 10. 2008 = MMR 2009, 29 [Bär], Rz 88).)

Verfassungsbestimmungen sind daher weder in § 99 Abs 5 Z 2 noch in § 98 TKG erforderlich, statt § 99 Abs. 5 Z 2 sollte das TKG lediglich einen Verweis auf die Bestimmungen des Sicherheitspolizeigesetzes enthalten, wie unten noch im Detail ausgeführt wird.

II. Zu den einzelnen Bestimmungen:

- **In § 1 Abs. 4 TKG** ist eine Aufzählung der dem Telekommunikationsgesetz zugrundeliegenden Gemeinschaftsrechtsakte enthalten, in die auch die RL 2006/24/EG aufzunehmen wäre.

- **Zu §§ 90 Abs 6 und 7 und 99 TKG**

Im vorliegenden Entwurf wird (in Entsprechung der höchstgerichtlichen Judikatur) davon ausgegangen, dass es sich bei einer Anfrage hinsichtlich des Namens und der Adresse eines Teilnehmers anhand einer (der anfragenden Behörde) bekannten IP-Adresse nicht um eine Stammdatenauskunft handelt, wenn die IP-Adresse dynamisch vergeben wurde, weil beim Betreiber dazu Logfiles (Verkehrsdaten) ausgewertet werden müssen. Hingegen handelt es sich bei einer Anfrage zu einer statisch vergebenen IP-Adresse laut Erläuterungen dann, wenn die konkrete IP-Adresse dem Kunden vertraglich zugesichert wurde, um eine Stammdatenauskunft nach § 90 Abs 6 und 7 TKG. Diese Differenzierung, die ausschließlich von im Ermessen der Betreiber liegenden technischen Rahmenbedingungen bzw. von Vereinbarungen mit dem Kunden abhängt, ist im Hinblick auf die daran anknüpfenden Konsequenzen aus Sicht des BMI **sachlich keinesfalls gerechtfertigt:** Bei einer vertraglich zugesicherten, statisch vergebenen IP-Adresse ist die Identität des Teilnehmers, etwa bei Vorliegen einer sicherheitspolizeilichen Aufgabenstellung, ohne weiteres zu beauskunften (bzw. im öffentlichen WHOIS Register zu

eruieren), hingegen ist dieselbe Auskunft unter anderen technischen bzw. mit dem Kunden vertraglich vereinbarten Bedingungen nicht mehr oder nur mehr unter den Voraussetzungen für eine Vorratsdatenbeauskunftung (schwere Straftat, richterliche Anordnung, verschlüsselte Übertragung) zulässig. Mit der vorgeschlagenen Novelle zum TKG ist die Identifizierung eines bestimmten Rechners durch entsprechende Betreiberauskunft und damit die Ausforschung eines Kommunikationsteilnehmers nach einem „anonymen“ Hilferuf z.B. in einem Forum bei dynamisch vergebener IP-Adresse (mit Flatrate) in vielen Fällen nicht mehr möglich.

Die Anfrage beim Betreiber, die notwendig ist, um herauszufinden, ob eine IP-Adresse dynamisch oder statisch vergeben wurde und die für die Zulässigkeit der weiteren Beauskunftung gemäß §§ 90, 99 oder 102b TKG entscheidend ist, **ist gesetzlich überdies gar nicht vorgesehen**.

- **Zu § 92 TKG:**

In § 92 Abs 3 Z 3 wurde die Nennung der lit d) bis e) vergessen, was wohl ein Versehen darstellt, da Zitate an anderer Stelle – etwa in § 90 Abs 7 – vom Vorhandensein der lit a) bis e) in § 92 Abs 3 Z 3 ausgehen.

Aus Sicht des BMI bedarf es darüber hinaus einer Klarstellung, was unter dem Terminus „**sonstige Kontaktinformation für die Nachricht**“ in § 92 Abs 3 Z 3 lit d) zu verstehen ist. So fallen nach den EB der Regierungsvorlage zum TKG 2003 (128 BlgNR, 22 GP) auch eine vom Betreiber bereitgestellte E-Mail-Adresse oder sonstige ähnlich individuelle dauerhafte Rufzeichen oder Kennungen. In den Erläuterungen zu § 90 Abs 7 wird die IMSI Nummer mit der Begründung, dass es für die Zuordnung einer IMSI zu einem bestimmten Kommunikationsvorgang der Auswertung Verkehrsdaten bedarf, nicht als Stammdatum gewertet. Dieser Ansicht kann nicht gefolgt werden. Die IMSI einer SIM Karte ist wie die öffentliche (nicht dynamische) IP – Adresse einem bestimmten Nutzer auf die Dauer des Vertrags zu ausschließlichen Nutzung zugewiesen und die Verbindung von IMSI- Nummer mit dem Teilnehmer besteht - genau wie bei einer statischen IP-Adresse - unabhängig vom konkreten Kommunikationsvorgang. Die IMSI ist mit einer SIM-Karte ebenso dauerhaft zugeordnet wie die jeweilige Rufnummer und entsteht nicht erst beim Kommunikationsvorgang. Wenn also zu einer bestimmten Rufnummer die IMSI angefragt wird, handelt es sich um eine Stammdatenauskunft im Sinne des § 92 Abs 3 Z 3 lit d), die sowohl im Dienste der Strafverfolgung als auch gemäß § 53 Abs 3b formlos zu erteilen ist.

- **Zu § 94 Abs 4 TKG:**

In § 94 Abs 3 TKG ist vorgesehen, dass die näheren Bestimmungen für die Gestaltung der technischen Einrichtungen zur Überwachung durch eine gesonderte Verordnung des BMVIT zu erfolgen haben. Damit ist sicher gestellt, dass mit der (leichter zu adaptierenden) VO der jeweils aktuelle Stand der Technik (und damit der bestmögliche Sicherheitsstandard) gewahrt ist.
Vor diesem Hintergrund erscheint es nicht ratsam, sich in Abs 4 auf eine bestimmte Übertragungstechnik (Email) und ein bestimmtes Datenformat (CSV) festzulegen.

- **Zu § 98 Abs 2:**

Die ausdrückliche Normierung der Zulässigkeit von Standortfeststellung anhand von „historischen" Standortdaten (=Vorratsdaten) in Notfällen auf Grundlage des TKG ist zu begrüßen. Aus den bereits unter Punkt I. dargelegten Gründen ist auch hier eine Ausgestaltung als Verfassungsbestimmung nicht notwendig. Auch die verpflichtende Information des Betroffenen erscheint aufgrund der Einschränkung auf Fälle der ersten allgemeinen Hilfeleistung entbehrlich.

Es wird angeregt, darüber hinaus in einem neu zu schaffenden **§ 98a** die Mitwirkung der in den §§ 112 f TKG geregelten Fernmeldebehörden bzw. deren Organen bei der Ortung von Mobiltelefonen in Hilfeleistungsfällen zu regeln. Grundvoraussetzung für die Durchführung einer derartigen Handypeilung ist, dass sich das gesuchte Mobiltelefon noch in betriebsfähigem Zustand und im Versorgungsgebiet des Mobilfunknetzes befindet, womit diese Möglichkeit bei Vorliegen der Voraussetzungen eine sinnvolle Ergänzung zum Einsatz des IMSI-Catchers darstellt.
Unter Berücksichtigung der bereits derzeit in § 98 TKG normierten Regelung in Zusammenhang mit Notfallbefugnissen von Betreibern von Notrufdiensten wird daher folgende Formulierung vorgeschlagen:

„§ 98a. Die Organe der Fernmeldebüros haben bei der Ortung von Telekommunikationsendgeräten durch Betreiber von Notrufdiensten (§ 98) über deren Ersuchen mitzuwirken. Voraussetzung dafür ist ein Notfall, der nur durch die Peilung abgewehrt werden kann."

- **Zu § 99 Abs 5 Z 2 TKG:**

Diese Regelung normiert keine (zusätzliche) Speicherverpflichtung, sondern nur eine Zugriffsregelung für sicherheitspolizeiliche Zwecke. § 99 Abs. 5 Z 2 des vorliegenden Entwurfs regelt jene Ermächtigungen der Sicherheitsbehörden neu, die derzeit in § 53 Abs. 3a und 53

Abs. 3b SPG geregelt sind. Diesen Bestimmungen würde durch eine inhaltlich abweichende und materiell - rechtlich sicherheitspolizeiliche Regelung im TKG aufgrund der lex-posterior-Regel wohl derogiert. Dem kann seitens des BMI keinesfalls zugestimmt werden, weshalb die Regelung ersatzlos zu streichen ist.

Darüber hinaus werden massive Bedenken gegen die inhaltliche Ausgestaltung der Bestimmung geäußert:

Zur Verschlechterung aufgrund der Einschränkung der zu schützenden Rechtsgüter:
Der vorliegende Entwurf lässt in § 99 Abs 5 eine Beauskunftung von dynamischen IP-Adressen nur dann zu, wenn die Auskunft zur Abwehr einer konkreten Gefahr für *das Leben oder die Gesundheit* eines Menschen notwendig ist. Diese Einschränkung der schützenswerten Rechtsgüter stellt gegenüber der jetzigen Rechtslage in § 53 Abs 3a SPG eine massive Verschlechterung dar und ist **sachlich auch nicht gerechtfertigt**. Internetbetrügereien oder auch eine Gefahr für Eigentum in großem Ausmaß könnten wegen der Einschränkung des Schutzes auf Leben oder die Gesundheit eines Menschen sicherheitspolizeilich nicht mehr abgewehrt werden. Aber auch dann, wenn ein Benutzer mit dynamischer IP-Adresse im Internet androht, der Umwelt durch das Verseuchen eines Gewässers zu schaden, könnte er zur sicherheitspolizeilichen Abwehr der Gefahr nicht ausgeforscht werden. Elementare Rechtsgüter wie die sexuelle Integrität oder die Freiheit sind dem Vorschlag zufolge ebenfalls ausgenommen. Die Wertung, dass die Rechtsgüter Leben oder Gesundheit als höherwertig anzusehen sind und nur diesfalls der Benutzer einer dynamischen IP-Adresse zur Gefahrenabwehr ausgeforscht werken kann, ist aufgrund der Strafrechtsakzessorietät des SPG systemwidrig.

Hinsichtlich der (im Hinblick auf § 53 Abs. 3b SPG entbehrlichen) Regelung zur Beauskunftung von Standortdaten gemäß § 99 Abs. 5 Z 2 TGK ist anzumerken, dass im Unterschied zum SPG die für die Ortung erforderliche Beauskunftung der IMSI-Nummer ebenso wenig vorgesehen ist wie die Ermächtigung zur Lokalisierung einer Endeinrichtung mit technischen Hilfsmitteln.

Zur Verschlechterung aufgrund mangelnder Speicherverpflichtung:
Aus den Erläuterungen zu § 99 Abs 5 Z 1 geht hervor, dass ein Zugriff auf Vorratsdaten auf die Verfolgung „schwere Straftaten“ limitiert ist, aber „*die meisten Anbieter* „(auch bei flat-Tarifen) die sogenannten Zugangsdaten *bis zu 96 Stunden* aus Betriebsnotwendigkeit aufbewahren. Garantie für das Vorhandensein der Daten gibt es keine, insbesondere **keine gesetzliche Verpflichtung** des Betreibers, die Daten für einen bestimmten Zeitraum zur

Verfügung zu stellen, sodass Gefahrenabwehr und erste allgemeine Hilfeleistung nach dem Sicherheitspolizeigesetz, aber auch Strafverfolgung im niederschwelligen Bereich (unter dem, was hinkünftig unter einer schweren Straftat zu verstehen sein wird), wenn dafür die Identifikation eines Internetbenutzers erforderlich ist, letztlich von unterschiedlichen, nicht nachprüfbaren und ausschließlich der Ingerenz der Betreiber unterliegenden Rahmenbedingungen abhängen. Es handelt sich dabei um die Art der Vergabe von IP-Adressen (statisch oder dynamisch) und um die im Einzelfall vertraglich vereinbarten Verrechnungsmodalitäten (Flatrate bzw. Einspruchsmöglichkeit nach Rechnungslegung durch den Kunden).

Bei der Strafverfolgung „im niederschwelligen Bereich“ ist davon auszugehen, dass mangels Aufzeichnungen beim Betreiber (abgesehen von für diese Fälle nicht zur Verfügung stehenden Vorratsdaten) die Beauskunftung von Namen und Anschrift etwa eines Stalkers, der via Internet „anonym“ sein Opfer terrorisiert oder eines Internetbetrügers mit dynamischer IP-Adresse in vielen Fällen nicht mehr erfolgt. Dasselbe gilt bei einer Reihe von mit einer geringen Strafandrohung bedrohten Delikten, bei denen die Ausforschung des Internetnutzer anhand der Zugangsdaten unbedingt erforderlich ist (etwa §118a Abs 1 StGB, §119 StGB, §119a StGB, §126a StGB). **Deshalb ist eine gesetzliche Speicherverpflichtung sowohl für sicherheitspolizeiliche Zwecke als auch im Hinblick auf effiziente Strafverfolgung unterhalb der Grenze der schweren Straftat notwendig.** Schon aus Verhältnismäßigkeitserwägungen wird die Speicherdauer dabei unter der für die Verfolgung schwerer Straftaten vorgesehenen Speicherdauer von sechs Monaten liegen.

<u>Zur verpflichtenden Information des Betroffenen:</u>

In § 98 Abs 2 und in 99 Abs 5 Z 2 ist eine verpflichtende Information des Betroffenen vorgesehen. Wie bereits dargelegt, wird der Rechtsschutz durch den Rechtsschutzbeauftragten (§§ 91a bis d SPG) wirkungsvoll wahrgenommen, dem unter anderen alle Auskunftsverlangen gem. § 53 Abs 3a und 3b verpflichtend zu melden sind. Der Rechtsschutzbeauftragte selbst ist zur Information der betroffenen Person bzw. zur Erhebung einer Beschwerde an die Datenschutzkommission befugt. Darüber hinaus erstattet der Rechtsschutzbeauftragte der Bundesministerin für Inneres gemäß § 91d Abs. 4 jährlich einen Bericht über seine Tätigkeit und Wahrnehmungen im Rahmen seiner Aufgabenerfüllung. Dieser Bericht ist auch dem ständigen Unterausschuss des Innenausschusses zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit vorzulegen. Der diesjährige Bericht des Rechtsschutzbeauftragten wird eine statistische Auswertung sämtlicher Meldungen an den Rechtsschutzbeauftragen enthalten.

Der so sichergestellte hohe Standard wurde auch vom VfGH als wirksamer Rechtsschutz anerkannt (G 147/08 vom 1.7.2009).

Aufgrund dieser Überlegungen ist aus Sicht des BMI die Bestimmung des § 99 Abs 5 Z 2 ersatzlos zu streichen und durch eine Speicherverpflichtung für die in § 53 Abs 3a und 3b aufgezählten Datenarten, verbunden mit einem Verweis auf die sicherheitspolizeilichen Regelungen, zu ersetzen. Eine konkrete Anpassung des Sicherheitspolizeigesetzes kann erst erfolgen, wenn über die grundsätzliche Frage der Speicherverpflichtung zur Erfüllung der gesetzlichen Auskunftsansprüche (sicherheitspolizeilich, im „niederschwelligen" Bereich der Strafverfolgung und allenfalls im Urheberrecht) entschieden wurde.

- **Zu § 102a und 102b TKG:**

Nach § 102a und 102b des Entwurfes darf eine Speicherung und Beauskunftung von Vorratsdaten nur zur Verfolgung „schwerer Straftaten" erfolgen. Was darunter zu verstehen ist, bleibt allerdings offen. Nach Ansicht des BMI sollte dabei bei Vorsatztaten angeknüpft werden, die mit einer Strafdrohung von mehr als einem Jahr bedroht sind und nicht darüber. Dies wäre insofern „überschießend" und systemwidrig, als die Verwendungsvoraussetzungen bei den unter die Vorratsdatenhaltung fallenden „äußeren Gesprächsdaten" strenger wären, als die Vorraussetzungen für Inhaltsüberwachung (= Gesprächen od. E-Mailverkehr gemäß §§ 134 f StPO bei Vorsatztaten von mehr als einem Jahr).

- **Zu § 109 Abs 3:**

Wie bereits bei § 99 Abs. 5 Z 2 ausgeführt, ist aufgrund des ausreichenden Rechtsschutzes durch den Rechtsschutzbeauftragten eine zusätzliche Informationspflicht des Betroffenen – und damit auch die Strafbestimmung – nicht erforderlich und ersatzlos zu streichen.

Für die Bundesministerin:

Mag. Peter Andre

elektronisch gefertigt