PROKSCH & FRITZSCHE | RECHTSANWÄLTE
Dr. Wolfram Proksch
Dr. Thomas Fritzsche
Mag. Christian Frank

An den
Verfassungsgerichtshof
Judenplatz 11
1010 Wien
EINSCHREIBEN

Wien, am 03.03.2008
RingMa/SPG/WP/ro/
G:\ADVOKAT\DATEN\WINWORD\RingMa\SPG\1.doc

Antragstellerin: Mag.a Marie Ringler, Landtagsabgeordnete,
[redacted]

vertreten durch:

RECHTSANWALT
DR. WOLFRAM PROKSCH
A-1010 WIEN, NIBELUNGENGASSE 11/4
Tel.: (01) 877 04 54, Fax: (01) 877 04 56
R145682, ✉ proksch@pfr.at

Vollmacht gem. § 8 RAO erteilt

Antragsgegnerin: Republik Österreich (Bund)

INDIVIDUALANTRAG gem Art 140 Abs 1 B-VG

3-fach/1 HS / Beilagen

I. Darstellung der Rechtslage

Der Nationalrat hat aufgrund der Regierungsvorlage 272 der Beilagen XXIII GP unter anderem eine Änderung des § 53 Abs 3a und Abs 3b des Sicherheitspolizeigesetzes (SPG) beschlossen. Die nun geltende Rechtslage stellt sich wie folgt dar:

(3a) Die Sicherheitsbehörden sind berechtigt, von Betreibern öffentlicher Telekommunikationsdienste (§ 92 Abs. 3 Z 1 Telekommunikationsgesetz 2003 - TKG 2003, BGBl. I Nr. 70) und sonstigen Diensteanbietern (§ 3 Z 2 E-Commerce-Gesetz - ECG, BGBl. I Nr. 152/2001) Auskunft zu verlangen über

1. Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses,
2. Internetprotokolladresse (IP-Adresse) zu einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung sowie
3. Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war,

wenn bestimmte Tatsachen die Annahme einer konkreten Gefahrensituation rechtfertigen und sie diese Daten als wesentliche Voraussetzung für die Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben benötigen. Die Bezeichnung eines Anschlusses nach Z 1 kann für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder die Abwehr gefährlicher Angriffe auch durch Bezugnahme auf ein von diesem Anschluss geführtes Gespräch durch Bezeichnung eines möglichst genauen Zeitraumes und der passiven Teilnehmernummer erfolgen. Die ersuchte Stelle ist verpflichtet, die Auskunft unverzüglich und kostenlos zu erteilen.

(3b) Ist auf Grund bestimmter Tatsachen anzunehmen, dass eine gegenwärtige Gefahr für das Leben oder die Gesundheit eines Menschen besteht, sind die Sicherheitsbehörden zur Hilfeleistung oder Abwehr dieser Gefahr berechtigt, von Betreibern öffentlicher Telekommunikationsdienste Auskunft über Standortdaten und die internationale Mobilteilnehmerkennung (IMSI) der von dem gefährdeten Menschen mitgeführten Endeinrichtung zu verlangen sowie technische Mittel zu ihrer Lokalisierung zum Einsatz zu bringen. Die Sicherheitsbehörde trifft die Verantwortung für die rechtliche Zulässigkeit des Auskunftsbegehrens, dessen Dokumentation dem Betreiber unverzüglich, spätestens innerhalb von 24 Stunden nachzureichen ist. Die ersuchte Stelle ist verpflichtet, die Auskünfte unverzüglich und gegen Ersatz der Kosten nach § 7 Z 4 der Überwachungskostenverordnung - ÜKVO, BGBl. II Nr. 322/2004, zu erteilen.

Die bis dahin gültigen Bestimmungen lauteten wie folgt:

(3a) Die Sicherheitsbehörden sind berechtigt, von den Betreibern öffentlicher Telekommunikationsdienste Auskunft über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses zu verlangen, wenn sie diese Daten als wesentliche Voraussetzung für die Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben benötigen. Die Bezeichnung dieses Anschlusses kann für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder die Abwehr gefährlicher Angriffe auch durch Bezugnahme auf ein von diesem Anschluß geführtes Gespräch durch Bezeichnung des Zeitpunktes und der passiven Teilnehmernummer erfolgen. Die ersuchte Stelle ist verpflichtet, die Auskunft unverzüglich und kostenlos zu erteilen.

Die Regierungsvorlage wurde nicht im Ausschuss beraten, sondern mittels sogenannter „Fristsetzung“ ins Plenum gebracht. Dort wurde in zweiter Lesung ein Abänderungsantrag gestellt, welcher die Grundlage für den späteren Beschluss des Nationalrates zur Änderung des SPG in den vorgenannten Bestimmungen war.

Beweis: beiliegender Abänderungsantrag
beiliegender Beschluss des Nationalrates

Das Begutachtungsverfahren (4.9. bis 2.10.2007) hatte dementsprechend nur die ursprüngliche Fassung des Ministerialentwurfs bzw der Regierungsvorlage zum Gegenstand. Zu den Änderungen, welche im Abänderungsantrag enthalten sind, gab es insofern weder ein entsprechendes Begutachtungsverfahren noch Ausschussberatungen.

Die vom Nationalrat beschlossenen Änderungen des SPG verpflichten jedenfalls (wie bisher) die Betreiber öffentlicher Telekommunikationsdienste iSd § 92 Abs 3 Z 1 TKG 2003 sowie (nun zusätzlich) auch sonstige Diensteanbieter iSd § 3 Z 2 E-Commerce-Gesetzes, den Sicherheitsbehörden über Anfrage bestimmte Auskünfte zu erteilen.

„Betreiber“ iSd TKG 2003 ist ein Unternehmen, das ein öffentliches Kommunikationsnetz oder eine zugehörige Einrichtung bereitstellt, oder zur Bereitstellung hiervon befugt ist (vgl § 3 Z 1 TKG 2003). „Kommunikationsnetz" sind Übertragungssysteme und gegebenenfalls Vermittlungs- und Leitwegeinrichtungen sowie anderweitige Ressourcen, die die elektronische Übertragung von Signalen über Kabel, Funk, optische oder andere elektromagnetische Einrichtungen ermöglichen, einschließlich Satellitennetze, feste (leitungs- und paketvermittelte, einschließlich Internet) und mobile terrestrische Netze, Stromleitungssysteme, soweit sie zur Signalübertragung genutzt werden, Netze für Hörfunk und Fernsehen sowie Kabelrundfunknetze (Rundfunknetze), unabhängig von der Art der übertragenen Informationen (vgl § 3 Z 11 TKG 2003).

Nach der Legaldefinition des ECG ist Diensteanbieter jede natürliche oder juristische Person oder sonstige rechtsfähige Einrichtung, die einen Dienst der Informationsgesellschaft bereitstellt; Dienst der Informationsgesellschaft ist ein in der Regel gegen Entgelt elektronisch im Fernabsatz auf individuellen Abruf des Empfängers bereitgestellter Dienst (§ 1 Abs 1 Z 2 Notifikationsgesetz 1999), insbesondere der Online-Vertrieb von Waren und

Dienstleistungen, Online-Informationsangebote, die Online-Werbung, elektronische Suchmaschinen und Datenabfragemöglichkeiten sowie Dienste, die Informationen über ein elektronisches Netz übermitteln, die den Zugang zu einem solchen vermitteln oder die Informationen eines Nutzers speichern.

Die Auskunftspflichten der Betreiber und Anbieter sind nicht an das Vorliegen eines richterlichen Befehls geknüpft; eine Auskunftserteilung gem § 53 Abs 3a SPG hat unverzüglich und kostenlos zu erfolgen; für eine Auskunftserteilung gem § 53 Abs 3b SPG steht eine Kostenersatz gem ÜKVO zu.

II. Prüfungsgegenstand

Die Antragstellerin bekämpft die Bestimmungen des § 53 Abs 3a sowie 3b SPG, BGBl I Nr 114/2007, in Kraft getreten am 1. Jänner 2008, gem Art 140 Abs 1 B-VG wegen Verfassungswidrigkeit.

III. Antragslegitimation

Voraussetzung für die Antragslegitimation nach Art 140 Abs 1 B-VG ist nach hRsp, dass der Antragsteller behauptet, unmittelbar durch das angefochtene Gesetz oder die angefochtene Verordnung – im Hinblick auf die Rechtswidrigkeit der Norm – in seinen Rechten verletzt zu sein, sowie, dass die Norm für den Antragsteller tatsächlich, und zwar ohne Fällung einer gerichtlichen Entscheidung oder ohne Erlassung eines Bescheides wirksam geworden ist. Das Gesetz oder die Verordnung muss unmittelbar in die Rechtssphäre des Antragstellers nachteilig eingreifen und diese - im Falle der Rechtswidrigkeit – verletzen. Ein derartiger Eingriff ist nur dann anzunehmen, wenn dieser nach Art und Ausmaß der Norm selbst eindeutig bestimmt ist und wenn er die rechtlichen Interessen des Antragstellers nicht bloß potenziell, sondern aktuell beeinträchtigt und wenn dem Antragsteller kein anderer zumutbarer Weg zur Abwehr zur Verfügung steht [vgl VfSlg 16808].

Zum Nachweis ihrer Antragslegitimation verweist die Antragstellerin darauf, dass sie selbst Internetnutzerin und auch Inhaberin eines Mobiltelefons ist. Weiters betreibt die Antragstellerin unter der Domain http://www.marieringler.at/ eine Informations-Webseite und ist als Diensteanbieterin iSd § 3 Z 2 E-Commerce-Gesetzes (ECG) BGBl I Nr. 152/2001 zu

qualifizieren. Darüber hinaus ist die Antragstellerin Mitglied des Kommunikationsnetzwerks http://www.funkfeuer.at/ und betreibt in ihrem Haushalt in der [redacted] basierend auf der Wireless LAN-Technologie einen eigenen Netzwerkknoten. Sie ist daher auch Anbieterin eines Kommunikationsdienstes bzw (Mit-)Betreiberin eines Kommunikationsnetzes iSd § 3 Z 1 u 11 TKG 2003 (vgl http://www.funkfeuer.at/).

Durch die angefochtene Bestimmung des § 53 Abs 3a SPG wird der Antragstellerin als Diensteanbieterin iSd des ECG und als Mit-Betreiberin eines Kommunikationsnetzes bzw als damit als Telekommunikationsdienstbetreiberin iSd § 92 Abs 1 TKG 2003 eine Rechtspflicht auferlegt, die in ihre Rechtssphäre unmittelbar und aktuell eingreift, ohne dass es hierfür einer behördlichen Entscheidung bedürfte: Sie hat die zur Bearbeitung von Auskunftsverlangen erforderlichen Daten zu erheben und zu speichern oder zumindest derart zu verarbeiten, dass im Falle eines Auskunftverlangens tatsächlich Auskunft erteilt werden kann, wenn sie über die gewünschten Daten verfügt. Für den Fall eines Zuwiderhandelns gegen die Bestimmung des § 53 Abs 3a SPG muss die Antragstellerin mit der Verhängung einer Verwaltungsstrafe oder mit unmittelbarer behördlicher Befehls- oder Zwangsgewalt rechnen, was ihr nicht zumutbar ist. Es steht der Antragstellerin auch kein anderer zumutbarer Weg zur Verfügung, um sich gegen das verfassungswidrige Gesetz zur Wehr zu setzen. Insbesondere kann von der Antragstellerin wohl nicht verlangt werden, eine Überwachung ihres Telekommunikationsverhaltens, insbesondere der von ihr versendeten oder an sie gerichteten Nachrichten, oder des Kommunikationsverhaltens anderer Mitglieder oder Nutzer im Netzwerk www.funkfeuer.at zu provozieren.

Durch die angefochtene Bestimmung des § 53 Abs 3b SPG werden die Sicherheitsbehörden im Wesentlichen ermächtigt, sog IMSI-Catcher (das sind Geräte, mit welchen die auf einer Mobilfunk-Karte eines Mobiltelefons gespeicherte *International Mobile Subscriber Identity* ausgelesen werden kann) einzusetzen und damit den Standort von Mobiltelefonen respektive jenen der Inhaber zu bestimmen. Da Art und Ausmaß des Eingriffs durch die angefochtene Norm eindeutig bestimmt sind, der Einsatz sog IMSI-Catcher auch Mobiltelefone „Unbeteiligter" miterfasst und es der Antragstellerin nicht zumutbar ist, die Notwendigkeit der Standort-Bestimmung ihres Mobiltelefons oder eines solchen in ihrer Umgebung zu simulieren, um sich dann gegen einen derartigen Eingriff in ihre Privatsphäre zur Wehr zu setzen, greift auch diese Bestimmung akut und unmittelbar in die Rechtssphäre der Antragstellerin ein. Die Antragslegitimation ist somit gegeben.

IV. Darlegung der Bedenken

Die angefochtenen Bestimmungen des § 53 Abs 3a und 3b SPG greifen in verfassungsgesetzlich gewährleistete subjektive Rechte der Antragstellerin, nämlich das Recht auf Wahrung des Fernmeldegeheimnisses gem Art 10a StGG, das Recht auf Achtung des Privat- und Familienlebens gem § 8 Abs 1 EMRK, das Grundrecht auf Datenschutz gem Art 1 § 1 Datenschutzgesetz 2000, sowie das Recht auf Gleichheit aller Staatsbürger vor dem Gesetz gem Art 7 B-VG, ein.

1. Zu den Bedenken gegen § 53 Abs 3a SPG

1.1. Verletzung des Fernmeldegeheimnisses

Der mit BGBl 1974/8 in das StGG vom 21.12.1876 über die allgemeinen Rechte der Staatsbürger für die im Reichsrathe vertretenen Königreiche und Länder, RGBl 1867/142 (StGG) eingefügte Artikel 10a bestimmt, dass „das Fernmeldegeheimnis ... nicht verletzt werden" darf und erklärt Ausnahmen nur aufgrund eines richterlichen Befehls in Gemäßheit bestehender Gesetze für zulässig.

Einfachgesetzlich wurde das Fernmeldegeheimnis in § 93 TKG 2003 (idF BGBl I Nr. 133/2005) neu geregelt. Demnach unterliegen die Inhaltsdaten, die Verkehrsdaten und die Standortdaten dem so genannten „Kommunikationsgeheimnis", welches sich auch auf die Daten erfolgloser Verbindungsversuche erstreckt.

Nach den Begriffsdefinitionen des TKG 2003 sind „Inhaltsdaten" die Inhalte übertragener Nachrichten (§ 92 Abs 3 Z 5 TKG 2003), „Standortdaten" Daten, die in einem Kommunikationsnetz verarbeitet werden und die den geografischen Standort der Telekommunikationseinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben (Abs 3 Z 6 *leg cit*), sowie „Verkehrsdaten" Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung des Vorgangs verarbeitet werden; auch sogenannte „Zugangsdaten" werden als Verkehrsdaten qualifiziert (Abs 3 Z 4 und Z 4a *leg cit*). Darunter verstehen sich jene Daten, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz beim Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten

Netzwerkadressierungen zum Teilnehmer notwendig sind. Unter „Nachricht" versteht das TKG 2003 schließlich jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet wird. Dies schließt nicht Informationen ein, die als Teil eines Rundfunkdienstes über ein Kommunikationsnetz an die Öffentlichkeit weitergeleitet werden, soweit die Informationen nicht mit dem identifizierbaren Teilnehmer oder Nutzer, der sie erhält, in Verbindung gebracht werden können (Abs 3 Z 7).

Was das Fernmeldegeheimnis iSd Art 10a StGG angeht, wird teils vertreten, dass lediglich Inhaltsdaten demselben unterliegen würden [ua *Wessely*, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht?, ÖJZ 1999, 491; *Stomper*, Auskunftsansprüche gegen Internet-Provider nach österreichischem Recht, MR-Int 2005, 99]. Dies wird va mit der Gesetzesgeschichte bzw der Orientierung des Art 10a StGG am Briefgeheimnis gem Art 10 StGG argumentiert.

Dem wird nach Ansicht der Antragstellerin zu Recht entgegengehalten, dass auch die zur Vermittlung verwendeten Daten zunehmend „informationell angereichert" werden: Da sich der Schutz des Fernmeldegeheimnisses, auch auf die Kommunikationsbeziehung bezieht, ist eine Einbeziehung auch der Verkehrsdaten bzw nach früherer Diktion der Vermittlungsdaten geboten [*Wiebe*, Auskunftsverpflichtung der Access Provider, MR 2005 H 4 Beilage 1; *Mayer/Pilz*, Gutachten ENFOPOL, 1999 (unveröffentlicht); VfGH 27.2.2003, G37/02; V42/02 ua].

Nach herrschender strafrechtlicher Judikatur und Literatur unterliegen auch Verkehrsdaten jedenfalls dem Fernmeldegeheimnis iSd Art 10a StGG [ua OGH 26.7.2005, 11 Os 57/05Z = JBL 2006, 130; OGH 6.12.1995, 13 Os 161/95 = JBl 1997, 260; *Reindl*, WK-StPO vor 149a – c; RZ 9; *Burgstaller*, Anm zu OGH 18.1.2001; 12 Os 152/00; JBL 2001, 536]. Der hohe Verfassungsgerichtshof war – soweit ersichtlich – noch nicht mit der Frage des Schutzumfanges des Fernmeldegeheimnisses gem Art 10a StGG bzw des Rechtes auf Privat- und Familienleben gem Art 8 EMRK im Hinblick auf Verbindungs-, Vermittlungs-, Verkehrs- oder Standortdaten befasst.

Die angefochtenen Bestimmungen berechtigen die Sicherheitsbehörden nach Meinung der Antragstellerin, von Betreibern öffentlicher Telekommunikationsdienste und von sonstigen

Diensteanbietern iSd ECG sowohl Auskunft über „Stammdaten" als auch über „Verkehrsdaten" und „Inhaltsdaten" zu verlangen, ohne dass für die beiden letztgenannten Datenkategorien ein richterlicher Befehl notwendig wäre. Die in § 53 Abs 3a SPG geregelte Verpflichtung, Sicherheitsbehörden über Anfrage Internetprotokolladressen (IP-Adressen) zu einer bestimmten Nachricht und den Zeitpunkt der Übermittlung mitzuteilen und auch Auskunft über Name und Anschrift eines bestimmten Benutzers zu erteilen, dem die IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet war, geht aus folgenden Überlegungen weit über eine reine Stammdatenabfrage und sogar über eine Verkehrsdatenabfrage hinaus:

- Die in § 53 Abs 3a Z 3 SPG genannten Name und Anschrift eines Benutzers sind jedenfalls keine „Stammdaten" gem § 92 Abs 3 TKG 2003. Letztgenannte betreffen ja nur jene personenbezogenen Daten, die für die *Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind*, und beziehen sich – vereinfacht ausgedrückt – immer nur auf Kunden- bzw Vertragspartner eines „Anbieters" iSd § 92 Abs 3 Z 1 TKG 2003. Die genannten Bestimmungen der SPG sind aber nicht auf Kunden bzw Vertragspartner von Betreibern öffentlicher Kommunikationsdienste oder Diensteanbieter iSd ECG beschränkt, sondern beziehen sich ganz offensichtlich auf jeden Benutzer eines Telekommunikationsdienstes, jeden Benutzer bzw jede Benutzerin eines Dienstes der Informationsgesellschaft iSd ECG, und auch jeden Verfasser einer Nachricht an derartige Betreiber oder Anbieter.

- In den genannten Bestimmungen des SPG wird auch nicht zwischen vom Telekommunikationsdienstbetreiber oder Diensteanbieter *selbst versandten* Nachrichten und von Dritten *empfangenen* Nachrichten differenziert. Dem Wortlaut der angefochtenen Bestimmung entsprechend ist nunmehr jeder Kommunikationsdienstbetreiber iSd TKG 2003 und Diensteanbieter iSd ECG verpflichtet, auch Auskunft über die IP-Adresse und den Zeitpunkt empfangener Nachrichten zu geben sowie auch Name und Anschrift des Benutzers zu nennen. Ebenfalls dem Wortlaut der angefochtenen Bestimmung folgend, würde dies plakativ ausgedrückt bedeuten, dass auch jeder Diensteanbieter iSd ECG und jeder Telekommunikationsdienstebetreiber seit 1.1.2008 auf Anfrage der Sicherheitsbehörde unverzüglich und kostenlos und ohne richterlichen Beschluss Auskunft darüber zu

erteilen hat, von welcher IP-Adresse bzw auch von wem (Name & Anschrift) ihm wann zB eMails oder sonstige Nachrichten geschickt wurden.

- „Inhaltsdaten" iSd TKG 2003 sind (wie oben ausgeführt) alle Inhalte übertragener Nachrichten. „Nachricht" meint dabei jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet wird. Das bedeutet, dass nicht nur eMails oder SMS bzw MMS „Nachrichten" darstellen, sondern wohl auch alle anderen erdenklichen Arten der Online-Kommunikation – wie etwa Chat, Newsforen, Voice-over-IP-Telefonie, Skype, das Ausfüllen eines Webformulars oder die Nutzung einer Website oder sonstiger Online-Umgebungen (zB 2nd Life, etc).

- Grob gesprochen bedeutet dies, dass bereits jeder Besuch einer Website Nachrichten und Inhaltsdaten iSd TKG 2003 betreffen kann: So etwa das (vom Betreiber der Website uU mitprotokollierte) Anklicken einer Banner-Werbung oder der Befehl zum Download einer bestimmten Datei oder eines Programms durch Anklicken eines bestimmten Feldes auf der Website. Der ohne weiters daraus ableitbare „Inhalt" solcher „Nachrichten" wäre dann etwa „mich interessiert diese Werbung / dieser Artikel" oder „ich möchte diese Datei auf meinen Rechner herunter laden".

- Diese Nachrichten bzw Informationen sind in aller Regel „geheim" bzw gerade nicht an die Öffentlichkeit gerichtet. Sie sind höchstens für den Inhaber der besuchten Website oder gar nicht für Dritte bestimmt (bei der Qualifikation als Geheimnisses iSd Art 10a StGG oder auch des Art 10 StGG kommt es dabei immer auf die „Intention" des Absenders oder Verfassers der Nachricht an).

- Es handelt sich dabei auch keineswegs um Daten, die nur zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung des Vorgangs verarbeitet werden ("Verkehrsdaten").

Setzt man die Kenntnis einer bestimmten „Nachricht" an sich voraus und werden dazu IP-Adresse und Übermittlungszeit oder auch Name und Anschrift des Benutzers bekannt gegeben, lässt sich in aller Regel auch auf den Inhalt der Nachricht schließen, wenn man etwa wiederum den Inhalt der aufgerufenen Website oder der Newsforen-Einträge kennt.

Da die Inhalte einer Website, von Gästebucheinträgen, Newsforen, Blogs etc zu einem bestimmten Zeitpunkt aber wesentlich leichter nachvollziehbar sind (vgl etwa Web-Archive wie http://www.archive.org/) als die Inhalte eines mündlich geführten Telefongesprächs, sind auch derartige Daten keineswegs mit jenen „Verkehrsdaten" vergleichbar, die bei der Führung eines Ferngesprächs anfallen. Die Grenze zwischen „Verkehrsdaten" und „Inhaltsdaten" verschwimmt dabei – es geht in Wahrheit nicht (nur) um die Frage, ob bzw wann jemand kommuniziert hat, sondern was mit wem kommuniziert wurde (zB welche Inhalte von wem wann heruntergeladen wurden, wer wann welcher Website besucht hat, wer welchen Eintrag in einem Forum veröffentlicht hat etc). Dies führt zu folgendem Ergebnis:

- Unter der Annahme, dass die in § 53 Abs 3a Z 2 u 3 SPG festgelegten Verpflichtungen der Telekommunikationsdienstbetreiber und Diensteanbieter auch Inhaltsdaten betreffen, stellen die genannten Bestimmungen jedenfalls eine Verletzung des Fernmeldegeheimnisses iSd Art 10a StGG dar, da die Auskunftsberechtigung der Sicherheitsbehörden nicht an einen richterlichen Befehl geknüpft wurde. Dies wäre aber nach der gesamten, zuvor zitierten Rsp und Literatur erforderlich gewesen.

- Auch unter der Annahme, dass die in § 53 Abs 3a Z 2 u 3 SPG festgelegten Verpflichtungen der Telekommunikationsdienstbetreiber und Diensteanbieter „nur" Verkehrsdaten betreffen, stellen die genannten Bestimmungen eine Verletzung des Art 10a StGG dar, wenn der Schutzumfang des Fernmeldegeheimnisses (wie von der dargestellten Literatur und Rsp vertreten) zumindest auch derartige Verkehrsdaten umfasst.

1.2. Verletzung des Rechtes auf Achtung des Privat- und Familienlebens

Parallel zum Fernmeldegeheimnis gem Art 10a StGG regelt Art 8 Abs 1 EMRK das Recht auf Achtung des Privat- und Familienlebens, der Wohnung und des Briefverkehrs. In der genannten Grundrechtsbestimmung fehlt zwar eine explizite Nennung des Fernmeldeverkehrs. Seit dem Fall *Klass/Bundesrepublik Deutschland* [EGMR 6.9.1978; EuGZR 1979, 278ff] wird aber auch der Fernmeldeverkehr dem Privatleben bzw dem Briefverkehr zugeordnet.

Im Fall *Malone/Vereinigtes Königreich* [EGMR 2.8.1984; EuGZR 1985, 23f] hielt der EGMR ausdrücklich fest, dass abgesehen von Inhaltsdaten auch sog äußere Gesprächsdaten dem Schutzbereich des Art 8 Abs 1 EMRK zuzurechnen sind. Zu diesen äußeren Gesprächsdaten zählen nach Ansicht des EGMR auch die Nummern beteiligter Anschlüsse sowie Zeitpunkt und Dauer des Gesprächs. Die staatliche Ermittlung äußerer Gesprächsdaten stellt nach der genannten Entscheidung auch dann einen Eingriff in das Grundrecht des Art 8 Abs 1 EMRK dar (der nur nach Maßgabe des Abs 2 zulässig ist), wenn die Registrierung des Fernmeldeverkehrs des Betroffenen nicht von staatlicher Stelle veranlasst wurde, sondern staatliche Stellen lediglich auf bereits vorhandene Datenbestände zurückgreifen und diese Daten (zB vom Fernmeldeunternehmen) legitimerweise ermittelt und verarbeitet wurden.

Der EGMR hat bereits mehrfach ausgesprochen, dass schon das bloße Bestehen eines Gesetzes, das eine geheime Überwachung der Telekommunikation erlaubt, als solches für alle Personen, auf die es Anwendung finden kann, die Gefahr einer Überwachung mit sich bringt. Diese Gefahr greife notwendigerweise in die Freiheit der Kommunikation zwischen Benützern von Telekommunikationseinrichtungen ein und stelle daher unabhängig von irgendwelchen tatsächlich gegen sie ergriffenen Maßnahmen einen Eingriff in die durch Art 8 EMRK geschützten Rechte dar [*Weber, Saravia/Deutschland*; EGMR 29.6.2006; Bsw 54934/00].

Ein Eingriff in die in Art 8 Abs 1 EMRK statuierten Rechte durch eine öffentliche Behörde darf gem Art 8 Abs 2 EMRK nur stattfinden, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist.

Nach der angefochtenen Bestimmung des § 53 Abs 3a SPG sind die Sicherheitsbehörden berechtigt, Auskunft zu verlangen, *wenn bestimmte Tatsachen die Annahme einer konkreten Gefahrensituation rechtfertigen und sie diese Daten als wesentliche Voraussetzung für die Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben benötigen*. Bezüglich Z 1 leg cit wird zusätzlich auf die *erste allgemeine Hilfeleistungspflicht* und *die Abwehr gefährlicher Angriffe* verwiesen.

Den Sicherheitsbehörden obliegt gem § 2 SPG die sog Sicherheitsverwaltung, welche aus der Sicherheitspolizei, dem Pass- und Meldewesen, der Fremdenpolizei, der Grenzüberwachung, dem Waffen-, Munitions-, Schieß- und Sprengmittelwesen sowie aus dem Pressewesen und den Vereins- und Versammlungsangelegenheiten besteht.

Durch die angefochtene Bestimmung des § 53 Abs 3a SPG wurde nun zweifelsohne eine gesetzliche Grundlagen iSd Art 8 Abs 2 EMRK für bestimmte Eingriffe geschaffen, welche Zwecken der Sicherheitsverwaltung bzw Sicherheitspolizei dienen soll. Es ist aber in keiner Weise ersichtlich, weshalb es in einer demokratischen Gesellschaft erforderlich bzw *notwendig* iSd Art 8 Abs 2 EMRK wäre, Sicherheitsbehörden zu berechtigen, von allen Betreibern öffentlicher Telekommunikationsdienste und allen Diensteanbietern iSd des ECG Auskunft über

- Name, Anschrift und Teilnehmernummer eines bestimmten Anschlusses,
- IP-Adresse zu einer bestimmten Nachricht und den Zeitpunkt der Übermittlung sowie
- Name und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war,

verlangen zu können.

- Bemängelt wird, dass schon die Formulierung in § 53 Abs 3a SPG „*wenn bestimmte Tatsachen die Annahme einer konkreten Gefahrensituation rechtfertigen*“ viel zu vage ist, um daraus ableiten zu können, wann ein Eingriff gerechtfertigt sein soll bzw wann nicht. Im SPG ist weder definiert, was „bestimmte Tatsachen“ sind, noch ist geregelt, wann eine „konkrete Gefahrensituation“ vorliegt. Letztere ist insb nicht mit der in § 16 Abs 1 u 2 SPG genannten „Allgemeinen Gefahr“ oder einem "gefährlichen Angriff“ gleichzusetzen, sonst hätte der Gesetzgeber wohl auf § 16 SPG Bezug genommen.

- Bemängelt wird weiters, dass auch unklar bleibt, wann „*diese Daten als wesentliche Voraussetzung für die Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben*“ benötigt werden. Auch diese Formulierung ist zu unbestimmt, erscheint formelhaft und lässt einen nahezu unbegrenzten Ermessensspielraum der handelnden Organe der Sicherheitsbehörden offen. Was sind denn „wesentliche Voraussetzungen“ für die Erfüllung der bundesgesetzlich übertragenen Aufgaben?

- Die Auskunftsverpflichtung ist weder nach dem Gesetzeswortlaut noch nach den Erläuterungen etwa nur auf eMails beschränkt. Wie ebenfalls bereits ausgeführt definiert das TKG 2003 „Nachrichten" wie folgt: *Jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet wird.* Das bedeutet, dass die Telekommunikationsdienstebetreiber und Diensteanbieter die genannten Daten also auch für alle erdenklichen Nachrichten bzw Informationen im Zuge einer Kommunikation wie Internet-Relay-Chat (IRC), Einträge in Newsforen oder Gästebüchern, SMS, MMS, Skypenachrichten und sogar Website-Aufrufe (denn auch diese können eben „Informationen" beinhalten) durch Benutzer an die Sicherheitsbehörden im Falle eines Auskunftsbegehrens weiterleiten müssten.

- Die angefochtene Bestimmung des § 53 Abs 3a SPG wirft damit auch die Frage auf, ob jeder Telekommunikationsdienstbetreiber iSd TKG und jeder Diensteanbieter iSd § 3 Z 2 ECG ab sofort (und unbefristet?) etwa jedes an ihn gerichtete und natürlich auch jedes von ihm (bzw seinem Unternehmen) gesendete eMail samt zugehöriger IP-Adresse und Zeitpunkt der Übermittlung speichern, zusätzlich von jedem Verfasser einer an ihn adressierten Nachricht Namen und Anschrift erheben, oder gar jeden Aufruf seiner Website sowie die Daten des dazugehörigen Benutzers verarbeiten muss, um seiner Auskunftsverpflichtung nachkommen zu können? Dies stünde auch – wie noch zu zeigen sein wird – jedenfalls im Widerspruch zu den Bestimmungen der §§ 96 Abs 1 u 99 Abs 1 TKG 2003.

- Selbst wenn man wohl davon ausgehen darf, dass eine Verpflichtung zur unverzüglichen und kostenlosen Auskunftserteilung seitens der Betreiber und Diensteanbieter nur besteht, wenn diese selbst (noch) über die genannten Daten verfügen, erscheint die genannte Berechtigung der Sicherheitsbehörden wohl viel zu weit gefasst. Sie stellt eine immense Erweiterung zur alten Regelung des § 53 Abs 3a SPG dar, welche einerseits nur die Betreiber öffentlicher Telekommunikationsdienste verpflichtete und andererseits nur Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses (als tatsächlich reine Stammdaten) betraf.

Die angefochtene Bestimmung des § 53 Abs 3a SPG (neu) verstößt aus den genannten Gründen auch gegen den Verhältnismäßigkeitsgrundsatz. Die Wahrnehmung der Sicherheitspolizei bzw der Sicherheitsverwaltung im Allgemeinen bildet zwar zweifelsohne eine im öffentlichen Interesse gelegene staatliche Aufgabe. Die damit verbundene Überwachung des Fernmeldeverkehrs bzw eine gesetzlich verankerte Mitwirkungs- und Auskunftspflicht von privaten Betreibern muss aber sachlich rechtfertigbar sein [vgl VfSlg 16808, VfgH 27.2.2003, G37/02 ua, V42/02 ua], was gegenständlich nicht der Fall ist.

Der EGMR hat auch schon in mehreren Entscheidungen betont, dass die Telefonüberwachung einer Person bzw der Einsatz anderer technischer Überwachungsgeräte einen typischen Eingriff in die Privatsphäre darstellt, wobei es keine Rolle spielt, ob es sich um private oder geschäftliche Anrufe handelt [vgl ua *Halford/Vereinigtes Königreich*]. Aus dem bereits zitierten Urteil *Klass/Bundesrepublik Deutschland* lässt sich jedenfalls ableiten, dass eine gesetzliche Grundlage, die eine Überwachung vorsieht, im weiteren der nationalen Sicherheit (insbesondere etwa der Aufrechterhaltung der Verfassungsordnung bzw zur Verbrechensbekämpfung) zu dienen hat.

Die Verhältnismäßigkeit ist nach dieser EGMR-Entscheidung dann gewahrt, wenn

- tatsächliche Anhaltspunkte für den Verdacht einer Straftat bestehen
- die Maßnahme nur die verdächtigten Personen erfasst
- dasselbe Ziel nicht mit anderen (gelinderen) Maßnahmen erreicht werden kann
- ein besonderes Verfahren für die Überwachung besteht
- die Überwachung zeitlich beschränkt ist
- eine möglichst richterliche Kontrolle der Überwachung erfolgt
- die überwachte Person nachträglich jedenfalls von der Maßnahme informiert wird, wenn der ursprüngliche Zweck der Überwachung dadurch nicht vereitelt wird

Die angefochten Bestimmung des § 53 Abs 3a SPG stellt im Gegensatz dazu überhaupt nicht auf Straftaten sondern lediglich auf „*konkrete Gefahrensituationen*“ ab. Eine nachträgliche Information der betroffenen Personen (also etwa der Verfasser der Nachrichten, bzgl welcher die Auskunft verlangt werden kann) ist im SPG ebenso wenig vorgesehen, wie eine Löschung der Daten oder – wie zur Verletzung des Fernmeldegeheimnisses bereits ausgeführt - eine richterliche Kontrolle.

Die Abweisung der Beschwerde *Weber, Saravia/Deutschland*, EGMR 29.6.2006, welche auch eine Verletzung des (wenn auch nicht gänzlich vergleichbaren) deutschen Fernmeldegeheimnisses betraf, wurde vom EGMR ua damit begründet, dass die umstrittene Regelung zahlreiche Schutzvorkehrungen enthielt, um den Eingriff in das Fernmeldegeheimnis in den Grenzen des (zum Erreichen der verfolgten legitimen Ziele) Notwendigen zu halten, insbesondere durch eine vernünftige Eingrenzung der Straftaten, in Bezug auf welche eine Übermittlung der Daten (an andere Behörden) zulässig war, als auch durch Kontrollmechanismen gegen Missbrauch.

Die Berechtigung der Sicherheitsbehörden gem Art 53 Abs 3a SPG, Auskunft zu verlangen, ist weder auf bestimmte Straftaten eingeschränkt, noch sind wirksame Kontrollmechanismen gegen den Missbrauch vorgesehen. Die Verpflichtung der Sicherheitsbehörden, den Rechtsschutzbeauftragten gem § 91c Abs 1 SPG (neu) über Auskunftsverlangen gem § 53 Abs 3a SPG zu informieren, stellt jedenfalls keine hinreichende Schutzvorkehrung dar. Die (zumindest in den Medien) kolportierten Auskunftsformulare lassen vielmehr befürchten, dass ein Missbrauch nur allzu leicht möglich wäre.

Beweis: beiliegendes Auskunftsformular

Die angefochtenen Bestimmung des Art 53 Abs 3a SPG widerspricht somit auch den Vorgaben des Art 8 EMRK.

1.3. Verletzung des Grundrechts auf Datenschutz

Die Verfassungsbestimmung des Art 1 § 1 des Datenschutzgesetzes 2000 normiert das sog Grundrecht auf Datenschutz. Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Die Einschränkung dieses Grundrechtes ist nur im lebenswichtigen Interesse des Betroffenen selbst bzw zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig. Eingriffe durch staatliche Behörden dürfen nur auf Grund von Gesetzen erfolgen, die aus den in Art 8 Abs 2 EMRK genannten Gründen notwendig sind.

Da die angefochtene Bestimmung Art 53 Abs 3a SPG wie bereits dargestellt die Art 8 EMRK normierten Vorgaben nicht erfüllt, ist auch das Grundrecht auf Datenschutz nach Ansicht der Antragstellerin jedenfalls verletzt. Um Wiederholungen zu vermeiden wird auf die Ausführungen unter Punkt IV.1.2. des Individualantrages verwiesen.

Es kann gerade nicht ausgeschlossen werden, dass im Hinblick auf die mittelbare Abfrage von „Inhaltsdaten" im Wege des § 53 Abs 3a SPG auch sensible Daten – wie etwa politische Meinung, ethnische Herkunft, religiöse oder weltanschauliche Überzeugung etc – anfallen. Selbst wenn man wiederum davon ausginge, dass (lediglich) „Verkehrsdaten" betroffen wären, welche als nicht-sensible Daten iSd DSG 2000 eingestuft werden könnten, müsste eine Interessensabwägung zwischen den schutzwürdigen Geheimhaltungsinteressen der Betroffenen und allenfalls überwiegenden (öffentlichen) Interessen vorgenommen werden. Es ist nicht ersichtlich, inwiefern selbst das legitime öffentliche Interesse an der staatlichen Wahrnehmung der Sicherheitspolizei bzw der Sicherheitsverwaltung den durch § 53 Abs 3a SPG ermöglichten gravierenden Eingriff in das Grundrecht auf Datenschutz der Betroffenen zu überwiegen vermag.

Für die Erfüllung von Auskunftsbegehren der Sicherheitsbehörden gem § 53 Abs 3a Z 2 u 3 SPG, betreffend IP-Adressen, Zeitpunkte der Übermittlung von Nachrichten, sowie Namen und Anschriften von Benutzern, denen eine IP-Adresse zugewiesen war, müssten wohl zunächst die gespeicherten IP-Adressen ausgewertet werden, um dazugehörige Personendaten festzustellen. Dabei werden jedenfalls wieder zumindest sog „Verkehrsdaten" ermittelt. Nach der Bestimmung des § 96 Abs 1 TKG 2003 dürfen Stammdaten, Verkehrsdaten, Standortdaten und Inhaltsdaten aber nur für Zwecke der Besorgung eines Kommunikationsdienstes ermittelt und verarbeitet werden. Dieser Bestimmung liegt Art 6 der Kommunikations-Datenschutz-RL zugrunde, welche die Verarbeitung von Verkehrsdaten auf Handlungen beschränkt, die zur Gebührenabrechnung, Verkehrsentwicklung, Kundenanfragen, Betrugsermittlung, Vermarktung elektronischer Kommunikationsdienste oder für die Bereitstellung von Diensten mit Zusatznutzen erforderlich sind. Die angefochtenen Bestimmungen § 53 Abs 3a Z 2 u 3 SPG fallen unter keine der Zulässigkeitsvoraussetzungen.

Überdies sind (zumindest solange die Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten in Österreich nicht umgesetzt ist) Verkehrsdaten gem § 99 Abs 1 TKG 2003

grundsätzlich nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren, soweit sie nicht zur Entgeltverrechnung benötigt werden (dann müssen sie gespeichert werden). Zu prüfen wäre letztlich wohl auch, inwieweit IP-Adressen zu den für die Entgeltverrechnung notwendigen Daten gehören, was bei flatrate-Tarifen wohl zu Recht bezweifelt werden muss [vgl dazu auch bereits *Wiebe*, Auskunftsverpflichtung der Access Provider, MR 2005 H 4 Beilage 1].

Die Bearbeitung eines Auskunftverlangens der Sicherheitsbehörden gem § 53 Abs 3a Z 2 u 3 SPG durch Telekommunikationsdienstebetreiber iSd TKG 2003 bzw Diensteanbieter iSd ECG widerspräche damit nach Ansicht der Antragstellerin auch den bereichsspezifisch datenschutzrechtlichen Regelung der §§ 96 Abs 1 u 99 Abs 1 TKG 2003.

1.4. Verletzung des Rechtes auf Gleichheit aller Staatsbürger vor dem Gesetz

Bemängelt wird schließlich auch, dass die Telekommunikationsdienstebetreiber iSd TKG 2003 bzw Diensteanbieter iSd ECG gem § 53 Abs 3a SPG verpflichtet sind, die verlangten Auskünfte unverzüglich und kostenlos zu erteilen.

Alleine die Auswertung von gespeicherten IP-Adressen, Nachrichten oder Übermittlungszeitpunkten sowie die Zuordnung zu bestimmten Personendaten (Name und Adresse der Benutzer, welchen die IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war) ist wohl mit erheblichem Aufwand verbunden. Unabhängig von der Frage, ob die Verpflichtung zur Bereitstellung der Daten verfassungskonform ist, bleibt unerfindlich, weshalb den Telekommunikationsdienstebetreibern und Diensteanbietern die bei jedem Auskunftsverlangen von Sicherheitsbehörden immer wieder anfallenden Kosten in unlimitierter Höhe auferlegt werden. Es wäre zumindest ein Kostenersatz vorzusehen gewesen. Selbst wenn das allgemeine (öffentliche) Interesse an der Wahrnehmung der Sicherheitsverwaltung und der Sicherheitspolizei die oben dargelegten Bedenken im Hinblick auf das Fernmeldegeheimnis, Art 8 EMRK oder das Grundrecht auf Datenschutz überwiegen würden, wäre es unbillig und sachlich nicht gerechtfertigt, den Betreibern und Dienstanbieter für die Verpflichtung zur Mitwirkung bei der Erfüllung staatlicher Aufgaben auch noch erhebliche finanzielle Lasten aufzubürden. Es ist letztlich auch nicht ersichtlich, weshalb die Bearbeitung von Auskunftsverlangen nach § 53 Abs 3a SPG weniger aufwendig bzw mit geringeren Kosten verbunden wäre, als die Erfüllung der Verpflichtungen gem

§ 53 Abs 3b SPG bzgl der Auskunftserteilung zu Standortdaten und internationalen Mobilteilnehmerkennungen.

Die angefochtene Bestimmung des § 53 Abs 3a SPG verletzt die Antragstellerin als Betreiberin eines Online-Informationsportals bzw als Diensteanbieterin iSd ECG daher auch in ihrem Recht auf Gleichheit aller Staatsbürger vor dem Gesetz gem Art 7 B-VG.

2. Zu den Bedenken gegen § 53 Abs 3b SPG

Nach der angefochtenen Bestimmung des § 53 Abs 3b SPG sind die Sicherheitsbehörden weiters berechtigt, von Betreibern öffentlicher Telekommunikationsdienste Auskunft über Standortdaten und die internationale Mobilteilnehmerkennung (IMSI) der von dem gefährdeten Menschen mitgeführten Endeinrichtung zu verlangen sowie technische Mittel zu ihrer Lokalisierung zum Einsatz zu bringen, *wenn auf Grund bestimmter Tatsachen anzunehmen, dass eine gegenwärtige Gefahr für das Leben oder die Gesundheit eines Menschen besteht.* Die Sicherheitsbehörde trifft nach dem Gesetzeswortlaut die *Verantwortung für die rechtliche Zulässigkeit des Auskunftsbegehrens, dessen Dokumentation dem Betreiber unverzüglich, spätestens innerhalb von 24 Stunden nachzureichen ist.*

In den Erläuterungen wird wie folgt argumentiert: *Nur Inhaltsdaten seien dem Fernmeldegeheimnis iSd Art 10a StGG zuzurechnen, ihre Erhebung sei unter Gesetzes- und Richtervorbehalt zu stellen [...]. Solange Standortdaten nicht auf dem Übertragungsweg abgefangen werden würden, sondern durch Erhebung beim Diensteanbieter gewonnen würden, liege kein Eingriff in das Fernmeldegeheimnis des Art 10a StGG vor.*

Diese Argumentation ist nach Ansicht der Antragstellerin verfehlt, da die angefochtene Bestimmung eben nicht (nur) die „Gewinnung" der Standortdaten durch Erhebung beim Diensteanbieter erlaubt, sondern auch Auskunftsverlangen bzgl der sog internationalen Mobilteilnehmerkennungen (IMSI). Letztere ermöglichen die direkte Lokalisierung von Endgeräten bzw ihren Inhabern durch die Sicherheitsbehörden mit Hilfe von technischen Geräten wie insb sog IMSI-Catchern. Den Sicherheitsbehörden wird mit der angefochtenen Bestimmung auch ausdrücklich der Einsatz solcher technischen Mittel zur Standortbestimmung erlaubt. Entgegen den Ausführungen werden die Standortdaten der

betroffenen Personen damit gerade auf dem Übertragungsweg an die Diensteanbieter bzw Telekommunikationsdienstebetreiber abgefangen.

Ein Eingriff in das Fernmeldegeheimnis iSd Art 10a StGG liegt daher sehr wohl vor. Die angefochtene Bestimmung des § 53 Abs 3b SPG ist schon in Ermangelung der Erfüllung des Richtervorbehalts grundrechtswidrig. Ungeachtet dessen ist die Antragstellerin der Meinung, dass die angefochtene Bestimmung § 53 Abs 3b SPG auch die in Art 8 EMRK und in Art 1 § 1 DSG 2000 normierten Grundrechte auf Achtung des Privat- und Familienlebens bzw auf Datenschutz verletzt. Um Wiederholungen zu vermeiden wird dazu zunächst auf die obigen Ausführungen zum Schutzumfang dieser Grundrechte unter IV.1. des Individualantrages verwiesen. Ergänzend wird aber vorgebracht wie folgt:

- Es wird nicht bestritten, dass eine rasche und effiziente Hilfeleistung durch die Sicherheitsbehörden in Notfällen bzw bei gegenwärtiger Gefahr für das Leben oder die Gesundheit von Menschen im allgemeinen (öffentlichen) Interesse liegt. Nach Ansicht der Antragstellerin öffnet die angefochtene Bestimmung bzw die darin enthaltene Ermächtigung der Sicherheitsbehörden, sog IMSI-Catcher einzusetzen, einem möglichen Missbrauch derartiger Geräte Tür und Tor:

- Das Gerät arbeitet gegenüber dem Mobiltelefon wie eine Funkzelle (Basisstation) und gegenüber dem Netzwerk wie ein Mobiltelefon. Der IMSI-Catcher simuliert also ein Mobilfunknetzwerk. Mobiltelefone in einem gewissen Umkreis buchen sich bei dieser Funkzelle mit dem stärksten Signal, also dem IMSI-Catcher, ein. Damit wird auch die Erstellung von Bewegungsprofilen und sogar das Mithören bzw Mitspeichern von Handy-Telefonaten möglich. Ein erfolgter Einsatz von IMSI-Catchern wird von den Betroffenen nicht bemerkt und ist idR nicht oder nur schwer nachzuweisen. Überdies werden auch Daten Unbeteiligter im Funknetzbereich des IMSI-Catchers erfasst. Schlussendlich besteht auch die Gefahr, dass der IMSI-Catcher unter Umständen den gesamten Mobilfunkverkehr der betroffenen Mobiltelefone lahmlegen, so dass auch Notrufe nicht möglich sind. Das Eingriffspotenzial ist im Vergleich zum allfälligen allgemeinen Interesse an der Gefahrenabwehr unverhältnismäßig hoch.

Beweis: beiliegende Ausdrucke aus Wikipedia,
Erläuterungen zu IMSI und IMSI-Catchern

- Die angefochtene Bestimmung des § 53 Abs 3b SPG sieht jedenfalls keinerlei Schutzvorkehrungen gegen Missbrauch vor. Die Verpflichtung zur nachträglichen Übergabe einer Dokumentation an den Betreiber stellt auch keinen wirksamen Kontrollmechanismus dar; abgesehen davon, dass dies gar nicht Aufgabe der Betreiber ist, können Betreiber auch anhand einer übergebenen Dokumentation schwerlich abschätzen, ob die erfolgte Standort-Ermittlung oder Überwachung rechtmäßig war. Das SPG sieht schließlich keinerlei Löschungsverpflichtung bzgl der verarbeiteten Daten vor und auch keine (zumindest) nachträgliche Information der betroffenen Personen – wenn sich etwa herausstellen sollte, dass diese gar nicht in Gefahr waren bzw dass keine Notwendigkeit zur Auslesung ihrer IMSI bzw Ermittlung ihres Standortes gegeben war.

Die in den Erläuterungen zur Regierungsvorlage enthaltene Argumentation bzw die angeführten Beispiele (am Abend nicht heimkehrende Tourengeher, etc) sind schließlich auch im Hinblick auf die bereits bestehenden Möglichkeiten der Standortdatenauskunft an Betreiber von Notrufdiensten nach § 98 Abs 2TKG 2003 nicht stichhältig.

Die Formulierung in der angefochtenen Bestimmung, dass *die Sicherheitsbehörde die Verantwortung für die rechtliche Zulässigkeit des Auskunftsbegehrens treffe*, erscheint formelhaft und ist nicht geeignet, die dargestellten Bedenken auch im Hinblick auf die Unverhältnismäßigkeit des Eingriffspotenzials zu lindern.

V. Aufhebungsbegehren

Die Antragstellerin stellt daher den umseitigen

A N T R A G ,

der hohe Verfassungsgerichtshof möge bezüglich der angefochtenen Bestimmungen ein Gesetzesprüfungsverfahren iSd §§ 62ff VerfGG einleiten, eine mündliche Verhandlung durchführen und die Bestimmungen des § 53 Abs 3a u 3b SPG idgF als verfassungswidrig aufheben. Weiters wird beantragt, dem Bund den Prozesskostenersatz aufzuerlegen, wobei iS des § 27 VerfGG der Zuspruch für alle regelmäßigen Kosten zuzüglich USt begehrt wird.

Mag.a Marie Ringler