

# FREIMÜLLER / NOLL / OBEREDER / PILZ

RECHTSANWÄLTE & PARTNER RECHTSANWÄLTE GmbH

A-1080 Wien, Alser Straße 21 • T: +43/1/406 05 51 • F: +43/1/406 96 01 • kanzlei@jus.at • <http://www.jus.at>

An den  
Fachverband IT-Unternehmen der  
Wirtschaftskammer Österreich  
**z.H. Herrn Mag. René Tritscher**  
Wiedner Hauptstraße 63  
1045 Wien

Dr. Georg Freimüller

Univ.-Doz. Dr. Alfred J. Noll

Dr. Alois Obereder

Mag. Michael Pilz

Dr. Erwin Senoner

Dr. Michael Celar

In ständiger Kooperation mit der  
selbständigen Rechtsanwältin

Dr. Simone Schweinhammer LL.M.

Wien, 28. Februar 2008  
07/FacRec/3 - 2/mp - 413399.doc  
Sekretariat: Frau Pokorny, DW 28

## Rechtsberatung

Sehr geehrte Damen und Herren!  
Sehr geehrter Herr Mag. Tritscher!

Sie haben mich ersucht, die mit 01.01.2008 in Kraft getretenen Änderungen des Sicherheitspolizeigesetzes, insbesondere die Neuformulierung der Bestimmungen des § 53 Abs. 3a und Abs. 3b dahingehend zu überprüfen, ob diese Bestimmungen mit den verfassungsgesetzlich geschützten Grundwerten übereinstimmen. Ziel der rechtlichen Beurteilung sollte es sein, zu klären, ob wegen tatsächlicher oder zu vermutender Grundrechtswidrigkeit dieser Bestimmungen eine Höchstgerichtsbeschwerde mit hinreichenden Erfolgsaussichten eingebracht werden könnte. Der Fachverband der IT-Unternehmen bzw. vor allem dessen Mitglieder seien durch die Novellierung des Sicherheitspolizeigesetzes unmittelbar betroffen, da nunmehr einerseits eine bei weitem größere Zahl von Mitglieder zur Auskunft verpflichtet werden kann und andererseits der Umfang der von den Mitgliedern zu erteilenden Auskünfte signifikant erweitert worden sei. Der Fachverband sei deshalb daran interessiert, zu klären, ob die vom Gesetzgeber seinen Mitgliedern auferlegten Verpflichtungen tatsächlich mit grundrechtlichen Vorgaben in Übereinstimmung zu bringen seien.

Zu den von Ihnen gestellten Fragen darf ich nach ausführlicher Prüfung gerne festhalten:

1. Gegenstand der Novelle des SPG:

Mit dem *"Bundesgesetz, mit dem das Sicherheitspolizeigesetz, das Grenzkontrollgesetz und das Polizeikooperationsgesetz geändert werden"*, BGBl. 2007/114, wurden wichtige Bestimmungen des Sicherheitspolizeigesetzes geändert. Insbesondere die Regelungen über Datenanwendungen der Sicherheitsbehörden wurden einer Neuordnung unterzogen. Im Zuge der Novelle wurde auch § 53 Abs. 3a SPG, der die Sicherheitsbehörden berechtigt, bestimmte Auskünfte von Telekommunikationsdienstleistern zu verlangen, völlig neu formuliert. Zugleich wurde ein neuer § 53 Abs. 3b eingeführt, der neben der in Abs. 3a geregelten Auskunftserteilung über bestimmte Verbindungsdaten nun auch die Auskunftserteilung über Standortdaten und die internationale Mobilteilnehmerkennung (IMSI) regelt. Im Vergleich zu der vorangehenden Fassung führt die Novelle des SPG zu einer dramatischen Ausweitung der Auskunftsverpflichtungen.

2. Inhalt der Auskunftspflicht:

Gemäß § 53 Abs. 3a des SPG sind – anders als in der Fassung vor dem 01.01.2008 – sowohl Betreiber öffentlicher Telekommunikationsdienste (§ 92 Abs. 3 Zif. 1 TKG 2003) als auch sonstige Diensteanbieter gemäß § 3 Zif. 2 E-commerce-Gesetz (ECG) zur Auskunftserteilung an Sicherheitsbehörden verpflichtet. Erstmals werden daher nicht nur kommerzielle Anbieter von öffentlichen Telekommunikationsdiensten sondern auch alle sonstigen *"natürlichen oder juristischen Personen oder sonstige rechtsfähige Einrichtungen, die einen Dienst der Informationsgesellschaft bereitstellen"* (§ 3 Zif. 2 ECG) von der Auskunftspflicht erfasst. Ein Dienst der Informationsgesellschaft ist ein *"in der Regel gegen Entgelt elektronisch im Fernabsatz auf individuellen Abruf des Empfängers bereit gestellter Dienst"* (§ 1 Abs. 1 Zif 2 Notifikationsgesetz 1999), insbesondere über das Internet bereitgestellte kommerzielle elektronische Dienste. Unter kommerziell sind alle Dienste zu verstehen, die in Ertragsabsicht erbracht werden (RV zum ECG, 26). So ist *"auch eine von einem Sponsor finanzierte, vom Nutzer unentgeltlich abrufbare Website oder der Betrieb einer mit Werbung unterlegten elektronischen"*

*Suchmaschine oder die Werbung selbst ein Dienst der Informationsgesellschaft... ein Content-Angebot, das zwar ohne Werbeeinschaltungen, aber als Eigenwerbung in einem Kommunikationsnetz bereitgestellt wird, ist ebenfalls ein Dienst der Informationsgesellschaft... letztlich gehören auch unentgeltlich bereitgestellte Angebote, die im Endeffekt den Unternehmenswert steigern sollen, zu den Diensten der Informationsgesellschaft"* (RV zum ECG, 26f). Diese weite Definition führt dazu, dass praktisch jeder Webseiten-Anbieter, der auf seiner Seite Informationen bereithält und dieses Anbot nicht gänzlich von seiner sonstigen kommerziellen Tätigkeit zu trennen ist, der Auskunftspflicht des § 53 Abs. 3a SPG unterliegt.

Inhaltlich können neben der bisher bereits geregelten Verpflichtung zur Bekanntgabe von Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses auch die IP-Adresse zu einer bestimmten Nachricht und der Zeitpunkt ihrer Übermittlung sowie Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, von den Sicherheitsbehörden verlangt werden. Die Ausweitung auf IP-Adressen in der nunmehr ausdrücklichen gesetzlichen Regelung beendet damit eine Streitfrage über die entsprechende Auskunftspflicht. Schon gemäß § 53 Abs. 3a SPG (alt) war strittig, ob IP-Adressen der Auskunftspflicht unterliegen. Da in der Neuformulierung *ausdrücklich* von „IP-Adressen, die zu einem bestimmten Zeitpunkt zugewiesen waren“, die Rede ist, wird klargestellt, dass nicht nur statische, sondern auch so genannte dynamische IP-Adressen, die also etwa nur am Beginn einer Internet-"Sitzung" einem bestimmten User zugeordnet werden, von der Auskunftspflicht mit umfasst sind.

Einer der Hintergründe der Erweiterung des SPG war nämlich der *Bescheid der Datenschutzkommission vom 03.10.2007 zur Zahl K121.279/0017-DSK/2007*, in welchem die Datenschutzkommission aufgrund der Beschwerde eines Internet-Users feststellte, dass die Übermittlung einer dynamischen IP-Adresse von der gesetzlichen Grundlage des § 53 Abs. 3a SPG (alt) nicht gedeckt sei. Die IP-Adresse stelle unzweifelhaft ein Verkehrsdatum dar, der Beschwerde gegen die Sicherheitsdirektion wurde stattgegeben, die Beschwerde gegen den Diensteanbieter, der die Auskunft erteilt hatte, allerdings zurückgewiesen. Die Qualifikation dynamischer IP-Adressen als Verkehrsdaten hat die Datenschutzkommission bereits in ihrer *Entscheidung vom 11.10.2006 zur Zahl K213.000/0005-DSK/2006* festgelegt, in dieser Entscheidung konstatierte sie auch,

dass statische IP-Adressen sowohl Verkehrsdaten als auch Stammdaten darstellten. Eine Speicherung dieser Daten durch Telekommunikationsdienstbetreiber sei nur zulässig, soweit dies für Verrechnungszwecke notwendig sei oder die ausdrückliche Einwilligung des Betroffenen vorliege.

Unklar bleibt in der Neufassung des § 53 Abs. 3a SPG die Bedeutung des Begriffes „*Nachricht*“ in Zif. 2 leg.cit. . Eine IP-Adresse soll hier dann den Sicherheitsbehörden beauskunftet werden, wenn sie zu einer bestimmten Nachricht gehört. Ob es sich bei einer Nachricht um eine E-Mail, eine über IRC übersandte Mitteilung, eine SMS oder auch nur um einen besuch auf einer Web-Site (was ja auch mit Informationstransport verbunden ist) oder gar nur um ein Ping handelt, wird vom Gesetzgeber nicht definiert. Da hier ein Eingriff in das grundrechtlich geschützte Telekommunikationsgeheimnis vorgesehen wird, ist der Begriff restriktiv zu interpretieren und im Zweifel ausschließlich eine E-Mail und/oder eine über Internet versandte SMS zu verstehen.

Mit § 53 Abs. 3b SPG (*neu*) wird auch zusätzlich eine Auskunftsberechtigung der Sicherheitsbehörden gegenüber Betreibern öffentlicher Telekommunikationsdienste über die Auskunft über Standortdaten und IMSI (Internationale Mobilteilnehmerkennung) Daten verankert, wenn aufgrund bestimmter Tatsachen anzunehmen ist, dass eine gegenwärtige Gefahr für Leben oder Gesundheit eines Menschen bestehe. Standortdaten und IMSI-Daten sind aber gegen Ersatz der Kosten nach § 7 Zif. 4 der Überwachungskostenverordnung – ÜKVO zu erteilen. Eine Auskunft gemäß § 53 Abs. 3a hat kostenlos zu erfolgen.

### 3. Überprüfung der Auskunftspflicht in Hinblick auf Art. 10 Staatsgrundgesetz (Fernmeldegeheimnis) iVm Art 8 MRK (Achtung des Privat- und Familienlebens):

Überprüft wird nunmehr, ob die Verpflichtung zur Auskunftserteilung über IP-Adressen in das verfassungsrechtlich geschützte Recht auf Wahrung des Fernmeldegeheimnisses (Telekommunikationsgeheimnis, Art. 10a StGG 1867) eingreift. Nach der genannten Gesetzesbestimmung ist ein Eingriff in das Fernmeldegeheimnis nur *aufgrund eines richterlichen Befehls in Gemäßheit bestehender Gesetze* zulässig. Vom Schutzbereich des Grundrechts erfasst sind nicht nur Telefongespräche über Festnetz und Handy, Telefax und Telegramme, sondern

auch alle sonstigen Arten der Telekommunikation (vergleiche *Wiederin* in *Korinek/Holoubeck* Kommentar, RZ 5 f zu Art. 10 a StGG). Strittig ist aber, ob nur die Ermittlung von Gesprächsinhalten oder auch die Feststellung reiner Vermittlungsdaten erfasst ist (dagegen *Wiederin* in *Korinek/Holoubeck*, Kommentar, RZ 12 ff zu Art. 10 a StGG, anders für Art. 8 MRK *Grabenwarter*, Menschenrechtskonvention 192).

Auch *Berka*, Lehrbuch Verfassungsrecht, RZ 1428, meint, dass Stamm-, Verkehrs- und Standortdaten nicht vom richterlichen Eingriffsvorbehalt des Art. 10 a Staatsgrundgesetz erfasst sind, allerdings schützt nach herrschender Lehre auch Art. 8 MRK den Fernmeldeverkehr, der inhaltlich aufgrund des materiellen Gesetzesvorbehaltes weit über Art. 10 a StGG hinausgeht. Nach der Judikatur des EGMR bedürfen Maßnahme zur geheimen Überwachung von Bürgern besonderer begleitender Bestimmungen des Rechtsschutzes und sind nur in außergewöhnlichen Situationen zulässig (EGMR, *Klass*, EuGRZ 1979, 278). Der Eingriff ist dem zufolge nur zulässig, wenn er gesetzlich vorgesehen ist, ein ausdrücklich genanntes legitimes Ziel verfolgt und in einer demokratischen Gesellschaft notwendig, d.h. verhältnismäßig ist. Die (bloße) Einrichtung eines nicht weisungsfreien Rechtsschutzbeauftragten, wie dies im SPG (*neu*) vorgesehen ist, wurde beim Anlassfall Observation und militärische Aufklärungsarbeit vom VfGH bereits unter Berufung auf Art. 13 MRK als unzureichend festgestellt, da den Betroffenen ein faktisch effizienter Rechtsschutz zur Verfügung stehen müsse.

Das Erfordernis einer klaren gesetzlichen Grundlage (Art. 8 Abs. 2 MRK) ist durch die indifferente Formulierung ("*bestimmte Tatsachen, die Annahme einer konkreten Gefahrensituation rechtfertigen*") in § 53 Abs. 3a SPG mE nicht ausreichend erfüllt. Der Verfassungsgerichtshof hat in seiner Judikatur die Pflicht zur besonders deutlichen Formulierung von Eingriffstatbeständen nämlich stets betont (vergleiche VfSlg 10.737, 11.455, 13.785). Auch die Unbestimmtheit der gewählten Formulierungen, etwa des Wortes „Nachricht“ (siehe oben unter 2.), lässt die klare Gesetzliche Grundlage vermissen.

Nach Art. 8 Abs. 2 MRK ist auch der Grundsatz der Verhältnismäßigkeit des Eingriffs zu beachten. Die Verhältnismäßigkeit ist im Gesetz selbst zu verankern, wobei die im SPG gewählte Formulierung hinsichtlich der Schwere der konkreten

Gefahrensituation aber keine Einschränkungen vornimmt. Nach dem Sicherheitspolizeigesetz ist neben der „*konkreten Gefahrensituation*“ lediglich die Benötigung der Daten als wesentliche Voraussetzung für die den Sicherheitsbehörden übertragenen Aufgaben genannt. Ob die Gefahrensituation hinsichtlich der überwachten Teilnehmeranschlüsse, unbeteiligter Dritter oder gar nur abstrakt bestehen muss, wird vom Gesetzgeber ebenso nicht näher definiert. Das Erfordernis der Verhältnismäßigkeit des Eingriffs wird durch den Gesetzgeber daher nicht nachvollziehbar definiert.

Die mangelnde Beachtung des Grundsatzes der Verhältnismäßigkeit wird auch bei einem Vergleich der Bestimmungen der Absätze 3a und 3b deutlich: In § 53 Abs. 3b SPG wird von einer „*gegenwärtigen Gefahr für das Leben oder die Gesundheit eines Menschen*“ gesprochen, in der die Sicherheitsbehörden „zur Abwehr dieser Gefahr“ Standortdaten von den Betreibern verlangen können. Hier wird die Gefahrensituation und der Zweck des Grundrechtseingriffes klar abgegrenzt und nachvollziehbarer. In Abs. 3a hingegen wird indifferent von einer „*konkreten Gefahrensituation*“ gesprochen, in der die Daten „zur Erfüllung der Aufgaben“ der Sicherheitsbehörden benötigt werden. Die Gefahr muss dabei nicht unmittelbar mit der Aufgabenerfüllung in Verbindung stehen, sie kann auch als Gefahr für reine Sachwerte und nur in geringem Umfang bestehen. Da die in Abs. 3a vorgesehenen Grundrechtseingriffe aber mindestens so weit reichen, wie die in Abs. 3b genannte Bekanntgabe von Standortdaten, kann die Verhältnismäßigkeit hier nicht nachvollzogen werden.

Hinzuweisen ist auch darauf, dass eine gesetzlich vorgesehene Verpflichtung der Behörde, die rechtliche Verantwortung für das Auskunftsbegehren zu übernehmen, nur in Abs. 3b festgeschrieben ist, weshalb – im Umkehrschluss – die Verantwortung für die Zulässigkeit der Datenweitergabe im Rahmen des Abs. 3a weiterhin (auch) beim Dienstbetreiber bzw. –anbieter liegt.

Zusammengefasst ist eine Übereinstimmung des Art. 53 Abs. 3a SPG mit dem Grundrecht auf Schutz des Fernmeldegeheimnisses und Wahrung des Schutzes des Privatlebens daher fragwürdig; neben der Frage, ob für die Herausgabe von Verkehrsdaten nicht gemäß § 10a StGG das Vorliegen eines richterlichen Befehls erforderlich wäre, ist insbesondere der Gesetzesvorbehalt des Art. 8 Abs. 2 MRK,

wonach der Eingriff gesetzlich ausreichend determiniert sein muss und in einer demokratischen Gesellschaft notwendig sein muss, durch die Formulierung des Gesetzgebers wahrscheinlich nicht gegeben.

#### 4. Eingriff in die Freiheit der Erwerbstätigkeit:

Die Bekanntgabe und Auskunftserteilung an die Sicherheitsbehörden gemäß § 53 Abs. 3a SPG hat unentgeltlich zu erfolgen. Wie ich mittlerweile durch Rücksprache mit zahlreichen Betreibern von Diensten feststellen konnte, ist die Erteilung der Auskunft im Einzelfall oft mit erheblichen personellen und logistischen Kosten verbunden. Zu prüfen ist, ob der Umstand, dass einerseits die Herausgabe von Standortdaten und IMSI-Daten nach der Überwachungskostenverordnung nur gegen Kostenersatz stattzufinden hat und andererseits auch Überwachung des Telekommunikationsverkehrs nach dem TKG Kostenersatzpflichten vorsieht, im Vergleich mit der Pflicht zur unentgeltlichen Auskunftserteilung nach § 53 Abs. 3a SPG eine sachliche ungleiche Behandlung und könnte einen unzulässigen Eingriff in das Eigentumsrecht darstellen.

Der VfGH hatte zu G37/02 u.a. vom 27.02.2003 bereits einmal die Rechtmäßigkeit unentgeltlicher Mitwirkung an der Überwachung des Fernmeldeverkehrs zu prüfen. Dabei ging es um die damalige Bestimmung des § 89 Abs. 1, letzter Satz, TKG 1997, mit welchem die Betreiber von Telekommunikationsdiensten verpflichtet worden waren, Einrichtungen zur Überwachung des Fernmeldeverkehrs unentgeltlich zur Verfügung zu stellen. Der VfGH führte damals aus, dass die wirtschaftliche Belastung von Telekommunikationsbetreibern nur bei Vorliegen besonderer Umstände und nach Maßgabe einer Interessenabwägung gerechtfertigt sei. Es sei eine Abwägung der Höhe der den Privaten erwachsenen Kosten einerseits und konkreter Kriterien, die eine besondere rechtliche und wirtschaftliche Beziehung begründen, andererseits vorzunehmen. *"Zu diesen Kriterien gehören unter anderem die Eingrenzbarkeit und damit konkrete Kalkulierbarkeit der von Privaten zu erbringenden Leistungen, die wirtschaftliche Zumutbarkeit des Aufwandes für den einzelnen Unternehmer, ein allfälliges Interesse, dass nicht bloß die Allgemeinheit, sondern auch die betroffenen Unternehmer selbst an den im Rahmen der Mitwirkung zu erbringenden Leistungen haben, und eine allfällige zusätzliche Gefährdung, die gerade vom Betrieb des Unternehmens ausgeht und der durch die vom*

*Unternehmen verlangte Mitwirkung entgegengewirkt werden soll"* (VfGH, G37/02 u.a. vom 27.02.2003). Im konkreten Fall war der VfGH der Auffassung, dass bei der Regelung der Kostenfragen der Verhältnismäßigkeitsgrundsatz nicht ausreichend beachtet wurde, sondern eine Belastungsgrenze völlig fehlte, weshalb die Bestimmung verfassungswidrig sei.

Die genannte Argumentation lässt sich zwanglos auf die nunmehrige Bestimmung des § 53 Abs. 3a SPG (neu) übertragen: Nach der Neufassung sind nicht nur die Betreiber öffentlicher Telekommunikationsdienste sondern auch sonstige Diensteanbieter zur Auskunftserteilung verpflichtet. Eine betragsmäßige Begrenzung oder sonstige sachliche Eingrenzung der vom Diensteanbieter zu erbringenden Leistungen fehlt, insbesondere ist auch aus dem Gesetz nicht ersichtlich, ob zur potenziellen Auskunftserteilung auch eine entsprechende Datenspeicherung notwendig ist (der sonstige Diensteanbieter nach dem ECG ist kein Betreiber eines öffentlichen Telekommunikationsdienstes und unterliegt daher nicht den strengen Vorschriften über Datenlöschung nach dem TKG). Wenn es sich beim Diensteanbieter um ein Unternehmen ohne eigene Server handelt, ist zur Auskunftserteilung jeweils die entsprechende Dienstleistung eines Dritten Unternehmens heranzuziehen, sodass neben den Selbstkosten auch echte Fremdkosten entstehen. Hinweise auf Verhältnismäßigkeit ergeben sich aus dem Gesetz keine, da weder das Ausmaß der Gefahrensituation noch die Höhe der zumutbaren Kosten beschrieben sind. Eine besondere Nähe der Betreiber von Diensten der Informationsgesellschaft zu den möglichen Gefahren ist nicht gegeben oder wird vom Gesetz nicht verlangt.

Auch hier sprechen daher die besseren Argumente dafür, dass der völlige Verzicht auf jegliche Kostenersatzregelung einen unzumutbaren Eingriff in Erwerbs- und Eigentumsfreiheit der Betroffenen darstellt.

#### 5. Ergänzende Bemerkungen zum Formblatt der Sicherheitsbehörden:

Seit Mitte Februar 2008 hat das Bundesministerium für Inneres ein Formblatt mittels Erlass herausgegeben, dass in der Kommunikation mit den Betreibern und Anbietern bei Auskunftsverlangen nach § 53 SPG Verwendung finden soll. Ein Muster dieses Formblattes ist diesem Gutachten angeschlossen.

In diesem Formblatt wird behauptet, die Sicherheitsbehörde könne bestätigen, dass sie die „Verantwortung für die rechtliche Zulässigkeit des [...] Auskunftsbegehrens trifft“. Schon diese Ausführungen sind falsch, da im Verhältnis zum betroffenen Kunden/User jedenfalls im Rahmen der Auskunftserteilung nach § 53 Abs 3a SPG eine Haftungsbefreiung beim Dienstbetreiber oder –anbieter nicht stattfindet und durch dieses Formblatt auch nicht vorgesehen werden kann (inwiefern die Formulierung Regressansprüche gegen den Staat zulässt, wird im Rahmen des Gutachtens nicht näher untersucht, ist aber vermutlich zu bejahen).

Hinsichtlich einer Auskunft nach § 53 Abs 3a SPG verzichtet das Formblatt auch darauf, eine Gefahrensituation (und damit das Vorliegen der gesetzlichen Voraussetzungen) auch nur zu behaupten. Bei einer Auskunft nach § 53 Abs. 3b soll nur die konkrete sicherheitspolizeiliche Aufgabe, zu deren Erfüllung die Daten benötigt werden, genannt werden. Für den Dienstbetreiber ist die Überprüfung der Berechtigung des Auskunftsbegehrens gemäß diesem Formblatt völlig unmöglich, das Auskunftsverlangen kann auch willkürlich sein. Wird ein derartiges Auskunftsbegehren erfüllt, trifft den Betreiber daher im Verhältnis zum Kunden das volle Risiko einer Rechtswidrigkeit seines Handelns.

Auch soll es seit Inkrafttreten der neuen Regelung zu einem sprunghaften Ansteigen der Auskunftsbegehren gekommen sein, was nur mit der faktischen Durchlöcherung des Fernmeldegeheimnisses und nicht mit einem Anstieg der Notwendigkeiten erklärbar wäre.

#### 6. Zulässigkeit der Erhebung einer Beschwerde beim VfGH:

Ausgehend von den bisherigen Überlegungen ist noch zu prüfen, ob die rechtliche Möglichkeit besteht, die vorerst behaupteten Verfassungswidrigkeiten direkt beim Verfassungsgerichtshof zu rügen. Gemäß Art. 140 Abs. 1 B-VG erkennt der Verfassungsgerichtshof über die Verfassungswidrigkeit von Gesetzen auf Antrag einer Person, die unmittelbar durch diese Verfassungswidrigkeit in ihren Rechten verletzt zu sein behauptet, sofern die betreffende Norm ohne Fällung einer gerichtlichen Entscheidung oder ohne Erlassung eines Bescheides für diese Person wirksam geworden ist.

Voraussetzung ist sohin, dass der Antragsteller behauptet, unmittelbar durch das angefochtene Gesetz im Hinblick auf die Rechtswidrigkeit der betreffenden Norm an seinen Rechten verletzt worden zu sein wobei die Norm für den Antragsteller tatsächlich und zwar ohne Fällung einer gerichtlichen Entscheidung oder ohne Erlassung eines Bescheides wirksam geworden ist. Notwendig ist es daher, dass das Gesetz in die Rechte des Antragstellers nachteilig eingreift und diese – im Falle der Rechtswidrigkeit – verletzt. Der Eingriff ist nur dann anzunehmen, wenn dieser nach Art und Ausmaß durch die Norm selbst eindeutig bestimmt ist, wenn er die Interessen des Antragstellers nicht bloß potenziell beeinträchtigt und dem Antragsteller kein anderer zumutbarer Weg zur Abwehr des Eingriffs zur Verfügung steht.

Antragsteller könnte daher einerseits eine von einem Auskunftsbegehren unmittelbar betroffene Person sein, deren Daten von einem Dienstebetreiber oder -anbieter den Sicherheitsbehörden weitergegeben werden mussten. Aber auch die Betreiber könnten eine Beschwerde erheben, wenn einerseits vorgebracht wird, dass Betreiber öffentlicher Telekommunikationsdienste und sonstige Diensteanbieter durch die im SPG verankerte Auskunftspflicht bereits jetzt aktuell zu entsprechenden Maßnahmen verpflichtet sind (Vorhaltekosten) oder bereits Adressaten konkreter Auskunftsverlangen geworden sind. Zu argumentieren wäre, dass die Norm ohne Fällung von gerichtlichen Entscheidungen und ohne Erlassung eines Bescheides für die Betroffenen Wirksam geworden ist und durch die mit den Auskunftsbegehren notwendigerweise verbundenen Haftungen gegenüber den eigenen Kunden ein unzumutbar großes Risiko besteht, in zivilrechtliche Haftungen oder Unterlassungsklagen zu geraten. Der Gutachter geht davon aus, dass es möglich sein sollte, derartige Betreiber von öffentlichen Telekommunikationsdiensten und/oder Diensten der Informationsgesellschaft oder auch Betroffene der Auskunftsbegehren zu identifizieren, denen eine Antragslegitimation gemäß Art. 140 BVG zukommt.

## 7. Zusammenfassung:

Zusammenfassend ist daher festzuhalten:

Die Novelle des § 53 Abs. 3a und Abs. 3b SPG bringt eine deutlich erweiterte Befugnis der Sicherheitsbehörden, Auskünfte von Betreibern öffentlicher Telekommunikationsdienste und – neu – von Diensteanbietern nach dem E-Commerce-Gesetz zu verlangen. Durch die Hinzunahme von IP-Adressen und Standortdaten werden erstmals auch neben Stammdaten echte Verkehrsdaten der Auskunftspflicht ohne vorherige richterliche Anordnung unterworfen. **Die im SPG damit verankerte Auskunftspflicht verstößt möglicherweise gegen Art. 10a Staatsgrundgesetz (Fernmeldegeheimnis), vermutlich aber mangels klarer gesetzlicher transparenter Anordnung und Beachtung des Verhältnismäßigkeitsgrundsatzes gegen die Bestimmung des Art. 8 MRK (Wahrung des Privat- und Familienlebens).** Durch die lediglich bei der Bekanntgabe von Standortdaten und IMSI-Daten vorgesehene Regelung des Kostenersatzes nach der Überwachungskostenverordnung wird gleichartiger Sachverhalt ungleich behandelt und kann argumentiert werden, dass die **kostenersatzfreie Beauskunftung nach § 53 Abs. 3a SPG in das Recht der Diensteanbieter auf Schutz Ihres Eigentums und der freien Erwerbsausübung** eingreifen kann.

Das **Formblatt der Sicherheitsbehörden** über die Auskunftsbegehren stellt die gesetzlichen Voraussetzungen der Auskunft nicht dar, so dass **der Dienstebetreiber bzw. -anbieter nicht in die Lage versetzt wird, die Berechtigung des Auskunftersuchens zu überprüfen.** Eine Übernahme der Verantwortung durch die Sicherheitsbehörde, wie das Formblatt es suggeriert, ist jedenfalls im Bereich des § 53 Abs. 3a SPG im Gesetz nicht vorgesehen, so dass diesbezüglich die Entscheidung des Dienstebetreibers auf eigenes Risiko erfolgt. Die **Kunden und User haben bei unberechtigter Auskunftserteilung Schadenersatz- und Unterlassungsansprüche** gegen den Betreiber des Dienstes.

**Antragslegitimiert** beim Verfassungsgerichtshof wären Adressaten von Auskunftsbegehren und alle sonstigen in § 53 Abs. 3a genannten Diensteanbieter, sofern sie zur Erfüllung der ihnen gesetzlich auferlegten Verpflichtungen bereits jetzt unmittelbar entsprechende Vorhaltemaßnahmen zu ergreifen haben, sowie die Betroffenen von Auskunftsbegehren, also jene Personen, deren Daten auf Grund einer sicherheitsbehördlichen Anfrage nach § 53 SPG beauskunftet worden sind.

Für weitere Auskünfte stehe ich Ihnen gerne zur Verfügung und verbleibe

mit freundlichen Grüßen



Mag. Michael Pilz

Anlage: Formblatt

- **Briefkopf der Dienststelle** -

Betreff: **Auskunftsverlangen gemäß § 53 Abs. 3a u. 3b SPG bzw. § 98 TKG**

GZ:

**per FAX – Nr.:**

- Anfrage betreffend:
- Daten gemäß § 53 Abs. 3a Z 1 SPG (Auskunft erfolgt kostenlos)
  - Daten gemäß § 53 Abs. 3a Z 2 SPG (Auskunft erfolgt kostenlos)
  - Daten gemäß § 53 Abs. 3a Z 3 SPG (Auskunft erfolgt kostenlos)
  - Daten gemäß § 53 Abs. 3a 2. Satz SPG (Auskunft erfolgt kostenlos)
  
  - Daten gemäß § 53 Abs. 3b SPG (Auskunft ist kostenpflichtig)
  - Daten gemäß § 98 TKG (Auskunft erfolgt kostenlos)

Die oben angeführte Behörde/Dienststelle ersucht um unverzügliche Übermittlung der unter Anfrage angeführten Daten.

Die anfragende Behörde/Dienststelle bestätigt ausdrücklich, dass sie im Sinne des § 7 Abs. 2 Z. 2 DSG 2000 zur Durchführung der zugrunde liegenden Amtshandlung gesetzlich zuständig ist, wobei die Sicherheitsbehörde die Verantwortung für die rechtliche Zulässigkeit des obigen Auskunftsbegehrens trifft.

Die Verwendung der Daten durch die anfragende Behörde/Dienststelle ist wesentliche Voraussetzung für die Wahrnehmung der sicherheitspolizeilichen Aufgabe nach der jeweiligen unter Anfrage angeführten Bestimmung.

Es wird ersucht, die Auskunft wie folgt zu erteilen:

- per Fax unter
- per E-Mail unter
- fernmündlich unter

Beilage: Liste

<b>Bei der Sicherheitsexekutive bekannte Anfragekriterien</b>	
Name	
Anschrift	
Teilnehmernummer	
Zeitraum und passive Teilnehmernummer eines geführten Telefongesprächs	
Bekannte Informationen zu einer bestimmten Nachricht im Internet	
IP-Adresse und bestimmter Zeitpunkt (inklusive Zeitzone) ihrer Übermittlung	
Dokumentation bei Auskunftsverlangen gem. § 53 Abs. 3b SPG und § 98 TKG: Anführung der SPG-Aufgabe (z. B. erste allgem. Hilfeleistungspflicht)	

<b>Umfang des Auskunftsbegehrens und Auskunft des Betreibers/Diensteanbieters</b>		
Sicherheitsexekutive kreuzt in der mittleren Spalte die begehrte Auskunft an Betreiber/Diensteanbieter beauskunftet die begehrten Daten in der rechten Spalte		
Name		
Anschrift		
Teilnehmernummer		
IP-Adresse zur bei der Sicherheitsexekutive vorliegenden Nachricht und Zeitpunkt (inklusive Zeitzone) der Übermittlung		
Standortdaten		
Internationale Mobilteilnehmerkennung (IMSI)		