Gericht

Verfassungsgerichtshof

Entscheidungsdatum

01.07.2009

Geschäftszahl

G147/08 ua

Sammlungsnummer

18831

Leitsatz

Zurückweisung des Individualantrags eines Mobilfunkbetreibers auf Aufhebung der durch die Novelle 2007 zum Sicherheitspolizeigesetz eingeführten Bestimmungen über die Auskunftspflicht von Telekombetreibern über bestimmte Handy- und Internetdaten; kein unmittelbarer Eingriff in rechtlich geschützte Interessen der antragstellenden Gesellschaft mangels zusätzlich auferlegter Speicherverpflichtungen; zumutbarer Weg zur Bekämpfung der Auskunftspflicht durch Beschwerde an den Unabhängigen Verwaltungssenat gegeben; zahlreiche Rechte von Privatpersonen nach dem Datenschutzgesetz im Fall unzulässiger Datenermittlung

Spruch

Die Anträge werden zurückgewiesen.

Begründung

Begründung:

I. 27 Antragsteller begehren mit ihren auf Art140 Abs1 B-VG

gestützten Anträgen die Aufhebung folgender gesetzlicher Bestimmungen "wegen Verletzung verfassungsgesetzlich gewährleisteter Rechte":

1. Aufhebung des §53 Abs1 des Bundesgesetzes über die Organisation und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz - SPG), BGBl. 566/1991 idF BGBl. I 4/2008 zur Gänze sowie in Abs2 der Wortfolgen "Die Sicherheitsbehörden dürfen Daten, die sie in Vollziehung von Bundes- oder Landesgesetzes[n] verarbeitet haben, für die Zwecke und unter den Voraussetzungen nach Abs1 ermitteln und weiterverarbeiten;" und "ihnen jedoch"

1.1. In eventu wird der unter 12. wiedergegebene Antrag gestellt.

2. Aufhebung des §53 Abs3a SPG zur Gänze

2.1. In eventu wird der Antrag gestellt, in §53 Abs3a SPG die Wortfolgen "und sie diese Daten als wesentliche Voraussetzung für die Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben benötigen. Die Bezeichnung eines Anschlusses nach Z1 kann" und "oder die Abwehr gefährlicher Angriffe" und des Wortes "erfolgen" aufzuheben sowie in §53 Abs3a zweiter Satz SPG die Wortfolge "durch Bezeichnung eines möglichst genauen Zeitraumes" mit der Maßgabe aufzuheben, dass die Wortfolge "durch die Bezeichnung des Zeitpunktes" in der vor der SPG-Novelle BGBl. I 114/2007 gültigen Fassung des §53 Abs3a zweiter Satz SPG, BGBl. 566/1991 idF BGBl. I 146/1999, wieder in Kraft tritt.

2.2. Ebenfalls in eventu wird der unter 12. wiedergegebene Antrag gestellt.

3. Aufhebung des §53 Abs3b SPG zur Gänze

3.1. In eventu wird der Antrag gestellt, in §53 Abs3b SPG die Wortfolge "und die Internationale Mobilteilnehmerkennung (IMSI)" sowie die Wortfolge "sowie technische Mittel zu ihrer Lokalisierung zum Einsatz zu bringen" aufzuheben.

3.2. Ebenfalls in eventu wird der unter 12. wiedergegebene Antrag gestellt.

4. Aufhebung der Wortfolge "aus allen anderen verfügbaren Quellen durch Einsatz geeigneter Mittel, insbesondere" im §53 Abs4
SPG

4.1. In eventu wird der Antrag gestellt, im §53 Abs4 SPG die Wortfolge "aus allen anderen verfügbaren Quellen" aufzuheben.

4.2. Ebenfalls in eventu wird der unter 12. wiedergegebene Antrag gestellt.

5. Aufhebung der Wortfolge "sowie Verwaltungsdaten" im §53a Abs1 SPG

5.1. In eventu wird der unter 12. wiedergegebene Antrag gestellt.

6. Aufhebung des §53a Abs2 SPG zur Gänze

6.1. In eventu wird der Antrag gestellt, im Einleitungssatz des §53a Abs2 SPG im die Wortfolge "oder gefährlicher Angriffe sowie zur Vorbeugung gefährlicher Angriffe, wenn nach der Art des Angriffs eine wiederholte Begehung wahrscheinlich ist, mittels operativer oder strategischer Analyse" sowie die Z2 bis 5 des §53a Abs2 SPG aufzuheben.

6.2. Ebenfalls in eventu wird der Antrag gestellt, im Einleitungsteil des §53a Abs2 SPG die Wortfolge "oder gefährlicher Angriffe sowie zur Vorbeugung gefährlicher Angriffe, wenn nach der Art des Angriffs eine wiederholte Begehung wahrscheinlich ist, mittels operativer oder strategischer Analyse", in §53a Abs2 litk SPG das Wort "/Lebensverhältnisse" und in §53a Abs2 litn SPG die Wortfolge "Kommunikations- und Verkehrsmittel sowie" und im Schlussteil des §53a Abs2 SPG die Wortfolge "und Verwaltungsdaten" aufzuheben.

6.3. Ebenfalls in eventu wird der unter 12. wiedergegebene Antrag gestellt.

7. Aufhebung der Wortfolge "gefährlicher Angriffe oder" in §54 Abs2 Z3 SPG

7.1. In eventu wird der unter 12. wiedergegebene Antrag gestellt.

8. Aufhebung der Wortfolge "gefährlicher Angriffe oder" in §54 Abs3 SPG

8.1. In eventu wird der unter 12. wiedergegebene Antrag gestellt.

9. Aufhebung der Wortfolge "gefährlicher Angriffe oder" in §54 Abs4 SPG

9.1. In eventu wird der unter 12. wiedergegebene Antrag gestellt.

10. Aufhebung des §54 Abs4b SPG

10.1. In eventu wird der unter 12. wiedergegebene Antrag gestellt.

11. Aufhebung des letzten Satzes des §56 Abs2 SPG

11.1. In eventu wird der unter 12. wiedergegebene Antrag gestellt.

12. Aufhebung der Wortfolge "aus Anlaß der Ermittlung von Daten" in §24 Abs1 des Bundesgesetzes über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000), BGBl. I 165/1999 idF BGBl. I 2/2008, des §24 Abs3 Z l DSG 2000 zur Gänze und der Wortfolge "und 3" in §24 Abs4 DSG 2000.

II. Zur Rechtslage:

1. Die angefochtenen Bestimmungen des Bundesgesetzes über die Organisation und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz - SPG), BGBl. 566/1991 idF BGBl. I 4/2008 haben folgenden Wortlaut:

"Zulässigkeit der Verarbeitung

§53. (1) Die Sicherheitsbehörden dürfen personenbezogene Daten ermitteln und weiterverarbeiten

1. für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht (§19);

2. für die Abwehr krimineller Verbindungen (§§16 Abs1 Z2 und 21);

2a. für die erweiterte Gefahrenerforschung (§21 Abs3) unter den Voraussetzungen des §91c Abs3;

3. für die Abwehr gefährlicher Angriffe (§§16 Abs2 und 3 sowie 21 Abs2); einschließlich der im Rahmen der Gefahrenabwehr notwendigen Gefahrenerforschung (§16 Abs4 und §28a);

4. für die Vorbeugung wahrscheinlicher gefährlicher Angriffe gegen Leben, Gesundheit, Sittlichkeit, Freiheit, Vermögen oder Umwelt (§22 Abs2 und 3) oder für die Vorbeugung gefährlicher Angriffe mittels Kriminalitätsanalyse, wenn nach der Art des Angriffes eine wiederholte Begehung wahrscheinlich ist;

5. für Zwecke der Fahndung (§24);

6. um bei einem bestimmten Ereignis die öffentliche Ordnung aufrechterhalten zu können.

(2) Die Sicherheitsbehörden dürfen Daten, die sie in Vollziehung von Bundes- oder Landesgesetzen verarbeitet haben, für die Zwecke und unter den Voraussetzungen nach Abs1 ermitteln und weiterverarbeiten; ein automationsunterstützter Datenabgleich im Sinne des §141 StPO ist ihnen jedoch untersagt. Bestehende Übermittlungsverbote bleiben unberührt.

...

(3a) Die Sicherheitsbehörden sind berechtigt, von Betreibern öffentlicher Telekommunikationsdienste (§92 Abs3 Z1 Telekommunikationsgesetz 2003 - TKG 2003, BGBl. I Nr. 70) und sonstigen Diensteanbietern (§3 Z2 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 Z1 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 Z4 der Überwachungskostenverordnung - ÜKVO, BGBl. II Nr. 322/2004, zu erteilen.

...

(4) Abgesehen von den Fällen der Abs2 bis 3b sind die Sicherheitsbehörden für Zwecke des Abs1 berechtigt, personenbezogene Daten aus allen anderen verfügbaren Quellen durch Einsatz geeigneter Mittel, insbesondere durch Zugriff auf allgemein zugängliche Daten, zu ermitteln und weiterzuverarbeiten.

Datenanwendungen der Sicherheitsbehörden

§53a. (1) Die Sicherheitsbehörden dürfen für die Leitung, Administration und Koordination von Einsätzen, insbesondere von sicherheitspolizeilichen Schwerpunktaktionen, Fahndungen oder ordnungsdienstlichen Anlässen sowie für den Personen- und Objektschutz und die Erfüllung der ersten allgemeinen Hilfeleistungspflicht Daten über natürliche und juristische Personen sowie Sachen und Gebäude verarbeiten. Es dürfen zu Personen, die von einer Amtshandlung betroffen sind, zu Einbringern von Anträgen, Anzeigen oder sonstigen Mitteilungen, zu gefährdeten Personen oder Institutionen und zu Zeugen und anderen Personen, die im Zuge einer Amtshandlung zu verständigen sind, die erforderlichen Identifikations- und Erreichbarkeitsdaten verarbeitet werden sowie zu gefahndeten Personen auch Lichtbild und eine allenfalls vorhandene Beschreibung des Aussehens und ihrer Kleidung. Darüber hinaus dürfen die erforderlichen Sachdaten einschließlich KFZ-Kennzeichen, Angaben zu Zeit, Ort, Grund und Art des Einschreitens sowie Verwaltungsdaten verarbeitet werden.

(2) Die Sicherheitsbehörden dürfen für die Abwehr krimineller Verbindungen oder gefährlicher Angriffe sowie zur Vorbeugung gefährlicher Angriffe, wenn nach der Art des Angriffs eine wiederholte Begehung wahrscheinlich ist, mittels operativer oder strategischer Analyse

1. zu Verdächtigen

a) Namen,
b) frühere Namen,
c) Aliasdaten,
d) Namen der Eltern,
e) Geschlecht,
f) Geburtsdatum und Ort,
g) Staatsangehörigkeit,
h) Wohnanschrift/Aufenthalt,
i) sonstige zur Personenbeschreibung erforderliche Daten,
j) Dokumentendaten,
k) Beruf und Qualifikation/Beschäftigung/Lebensverhältnisse,
l) erkennungsdienstliche Daten,
m) Informationen über wirtschaftliche und finanzielle Verhältnisse einschließlich damit im Zusammenhang stehender Daten juristischer Personen und
n) sachbezogene Daten zu Kommunikations- und Verkehrsmittel sowie Waffen einschließlich Registrierungsnummer/Kennzeichen,

2. zu Opfern oder Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie Opfer einer mit beträchtlicher Strafe bedrohten Handlung werden können, die Datenarten 1. a) bis k) sowie Gründe für die Viktimisierung und eingetretener Schaden,

3. zu Zeugen die Datenarten 1. a) bis j) und zeugenschutzrelevante Daten,

4. zu Kontakt- oder Begleitpersonen, die nicht nur zufällig mit Verdächtigen in Verbindung stehen und bei denen ausreichende Gründe für die Annahme bestehen, dass über sie Informationen zu

Verdächtigen beschafft werden können, die Datenarten 1. a) bis n) bis zur möglichst rasch vorzunehmenden Klärung der Beziehung zum Verdächtigen, sowie

5. zu Informanten und sonstigen Auskunftspersonen die Datenarten 1. a) bis j),

sowie tat- und fallbezogene Informationen und Verwaltungsdaten verarbeiten, auch wenn es sich um besonders schutzwürdige Daten im Sinne des §4 Z2 DSG 2000 handelt.

...

Besondere Bestimmungen für die Ermittlung

§54. ...

(2) Die Ermittlung personenbezogener Daten durch Beobachten (Observation) ist zulässig

1. zur erweiterten Gefahrenerforschung (§21 Abs3);

2. um eine von einem bestimmten Menschen geplante strafbare Handlung gegen Leben, Gesundheit, Sittlichkeit, Freiheit, Vermögen oder Umwelt noch während ihrer Vorbereitung (§16 Abs3) verhindern zu können;

3. wenn sonst die Abwehr gefährlicher Angriffe oder krimineller Verbindungen gefährdet oder erheblich erschwert wäre.

(3) Das Einholen von Auskünften ohne Hinweis gemäß Abs1 (verdeckte Ermittlung) ist zulässig, wenn sonst die Abwehr gefährlicher Angriffe oder krimineller Verbindungen gefährdet oder erheblich erschwert, oder die erweiterte Gefahrenerforschung durch Einsatz anderer Ermittlungsmaßnahmen aussichtslos wäre.

(4) Die Ermittlung personenbezogener Daten mit Bild- und Tonaufzeichnungsgeräten ist nur für die Abwehr gefährlicher Angriffe oder krimineller Verbindungen und zur erweiterten Gefahrenerforschung (§21 Abs3) zulässig; sie darf unter den Voraussetzungen des Abs3 auch verdeckt erfolgen. Das Fernmeldegeheimnis bleibt unberührt. Unzulässig ist die Ermittlung personenbezogener Daten jedoch

1. mit Tonaufzeichnungsgeräten, um nichtöffentliche und nicht in Anwesenheit eines Ermittelnden erfolgende Äußerungen aufzuzeichnen;

2. mit Bildaufzeichnungsgeräten, um nichtöffentliches und nicht im Wahrnehmungsbereich eines Ermittelnden erfolgendes Verhalten aufzuzeichnen.

...

(4b) Die Sicherheitsbehörden sind ermächtigt, verdeckt mittels Einsatz von Kennzeichenerkennungsgeräten personenbezogene Daten für Zwecke der Fahndung (§24 SPG) zu verarbeiten. Der Einsatz ist auf maximal einen Monat zu beschränken. Die Daten sind zu löschen, sobald sie für Zwecke der konkreten Fahndung nicht mehr benötigt werden.

...

Zulässigkeit der Übermittlung

§56. ...

(2) Die Übermittlung personenbezogener Daten ist aktenkundig zu machen. Übermittlungen aus einer automationsunterstützt geführten Evidenz können statt dessen protokolliert werden; die Protokollaufzeichnungen können nach drei Jahren gelöscht werden. Von der Protokollierung ausgenommen sind automatisierte Abfragen gemäß §54 Abs4b, es sei denn, es handelt sich um einen Trefferfall."

2. Die weiteren hier maßgeblichen Bestimmungen des SPG lauten:

"Beschwerden wegen Verletzung der Bestimmungen über den Datenschutz

§90. Die Datenschutzkommission entscheidet gemäß §31 des Datenschutzgesetzes 2000 über Beschwerden wegen Verletzung von Rechten durch Verwenden personenbezogener Daten in Angelegenheiten der Sicherheitsverwaltung entgegen den Bestimmungen des Datenschutzgesetzes. Davon ausgenommen ist die Beurteilung der Rechtmäßigkeit der Ermittlung von Daten durch die Ausübung verwaltungsbehördlicher Befehls- und Zwangsgewalt.

...

Rechtsschutzbeauftragter

§91a. (1) Zur Wahrnehmung des besonderen Rechtsschutzes im Ermittlungsdienst der Sicherheitsbehörden ist beim Bundesminister für Inneres ein Rechtsschutzbeauftragter mit zwei Stellvertretern eingerichtet, die bei der Besorgung der ihnen nach dem Sicherheitspolizeigesetz zukommenden Aufgaben unabhängig und weisungsfrei sind und der Amtsverschwiegenheit unterliegen.

(2) Der Rechtsschutzbeauftragte und seine Stellvertreter haben gleiche Rechte und Pflichten. Sie werden vom Bundespräsidenten auf Vorschlag der Bundesregierung nach Anhörung der Präsidenten des Nationalrates sowie der Präsidenten des Verfassungsgerichtshofes und des Verwaltungsgerichtshofes auf die Dauer von fünf Jahren bestellt. Wiederbestellungen sind zulässig.

(3) (Verfassungsbestimmung) Eine Einschränkung seiner Befugnisse nach §91c sowie seiner Rechte und Pflichten nach §91d kann vom Nationalrat nur in Anwesenheit von mindestens der Hälfte der Mitglieder mit einer Mehrheit von zwei Dritteln der abgegebenen Stimmen beschlossen werden.

Organisation

§91b. (1) Der Rechtsschutzbeauftragte und seine Stellvertreter müssen besondere Kenntnisse und Erfahrungen auf dem Gebiet der Grund- und Freiheitsrechte aufweisen und mindestens fünf Jahre in einem Beruf tätig gewesen sein, in dem der Abschluss des Studiums der Rechtswissenschaften Berufsvoraussetzung ist. Richter und Staatsanwälte des Dienststandes, Rechtsanwälte, die in die Liste der Rechtsanwälte eingetragen sind, und andere Personen, die vom Amt eines Geschworenen oder Schöffen ausgeschlossen oder zu diesem nicht zu berufen sind (§§2 und 3 des Geschworenen- und Schöffengesetzes 1990) dürfen nicht bestellt werden.

(2) Die Bestellung des Rechtsschutzbeauftragten und seiner Stellvertreter erlischt bei Verzicht, im Todesfall oder mit Wirksamkeit der Neu- oder Wiederbestellung. Wenn ein Grund besteht, die volle Unbefangenheit des Rechtsschutzbeauftragten oder eines Stellvertreters in Zweifel zu ziehen, hat sich dieser des Einschreitens in der Sache zu enthalten.

(3) Der Bundesminister für Inneres stellt dem Rechtsschutzbeauftragten die zur Bewältigung der administrativen Tätigkeit notwendigen Personal- und Sacherfordernisse zur Verfügung. Dem Rechtsschutzbeauftragten und seinen Stellvertretern gebührt für die Erfüllung ihrer Aufgaben eine Entschädigung. Der Bundesminister für Inneres ist ermächtigt, mit Verordnung Pauschalsätze für die Bemessung dieser Entschädigung festzusetzen.

Befassung des Rechtsschutzbeauftragten

§91c. (1) Die Sicherheitsbehörden sind verpflichtet, den Rechtsschutzbeauftragten von jeder Ermittlung personenbezogener Daten durch verdeckte Ermittlung (§54 Abs3), durch den verdeckten Einsatz von Bild- oder Tonaufzeichnungsgeräten (§54 Abs4), durch Verarbeiten von Daten, die andere mittels Einsatz von Bild- und Tonaufzeichnungsgeräten er- und übermittelt haben (§53 Abs5) unter Angabe der für die Ermittlung wesentlichen Gründe in Kenntnis zu setzen. Für derartige Maßnahmen im Rahmen der erweiterten Gefahrenerforschung gilt Abs3. Darüber hinaus ist der Rechtsschutzbeauftragte über Auskunftsverlangen (§53 Abs3a Z2 und 3, Abs3a zweiter Satz und 3b) sowie über den Einsatz von Kennzeichenerkennungsgeräten (§54 Abs4b) zu informieren.

(2) Sicherheitsbehörden, die die Überwachung öffentlicher Orte mit Bild- und Tonaufzeichnungsgeräten im Sinne des §54 Abs6 und 7 oder die Führung einer Datenanwendung gemäß §53a Abs2 und 6 beabsichtigen,

haben unverzüglich den Bundesminister für Inneres zu verständigen. Dieser hat dem Rechtsschutzbeauftragten Gelegenheit zur Äußerung binnen drei Tagen zu geben. Der tatsächliche Einsatz der Bild- und Tonaufzeichnungsgeräte oder die Aufnahme der Datenanwendung darf erst nach Ablauf dieser Frist oder Vorliegen einer entsprechenden Äußerung des Rechtsschutzbeauftragten erfolgen.

(3) Sicherheitsbehörden, denen sich eine Aufgabe gemäß §21 Abs3 stellt, haben vor der Durchführung der Aufgabe die Ermächtigung des Rechtsschutzbeauftragten im Wege des Bundesministers für Inneres einzuholen. Dasselbe gilt, wenn beabsichtigt ist, im Rahmen der erweiterten Gefahrenerforschung (§21 Abs3) besondere Ermittlungsmaßnahmen nach §54 Abs3 und 4 zu setzen oder gemäß §53 Abs5 ermittelte Daten weiterzuverarbeiten.

Rechte und Pflichten des Rechtsschutzbeauftragten

§91d. (1) Die Sicherheitsbehörden haben dem Rechtsschutzbeauftragten bei der Wahrnehmung seiner Aufgaben jederzeit Einblick in alle erforderlichen Unterlagen und Aufzeichnungen zu gewähren, ihm auf Verlangen Abschriften (Ablichtungen) einzelner Aktenstücke unentgeltlich auszufolgen und alle erforderlichen Auskünfte zu erteilen; insofern kann ihm gegenüber Amtsverschwiegenheit nicht geltend gemacht werden. Dies gilt jedoch nicht für Auskünfte und Unterlagen über die Identität von Personen oder über Quellen, deren Bekannt werden die nationale Sicherheit oder die Sicherheit von Menschen gefährden würde, und für Abschriften (Ablichtungen), wenn das Bekannt werden der Information die nationale Sicherheit oder die Sicherheit von Menschen gefährden würde.

(2) Dem Rechtsschutzbeauftragten ist jederzeit Gelegenheit zu geben, die Durchführung der in §91c genannten Maßnahmen zu überwachen und alle Räume zu betreten, in denen Aufnahmen oder sonstige Überwachungsergebnisse aufbewahrt werden. Darüber hinaus hat er im Rahmen seiner Aufgabenstellungen die Einhaltung der Pflicht zur Richtigstellung oder Löschung nach §63 oder den besonderen Löschungsbestimmungen zu überwachen.

(3) Nimmt der Rechtsschutzbeauftragte wahr, dass durch Verwenden personenbezogener Daten Rechte von Betroffenen verletzt worden sind, die von dieser Datenverwendung keine Kenntnis haben, so ist er zu deren Information oder, sofern eine solche aus den Gründen des §26 Abs2 des DSG 2000 nicht erfolgen kann, zur Erhebung einer Beschwerde an die Datenschutzkommission nach §90 befugt.

(4) Der Rechtsschutzbeauftragte erstattet dem Bundesminister für Inneres jährlich bis spätestens 31. März einen Bericht über seine Tätigkeit und Wahrnehmungen im Rahmen seiner Aufgabenerfüllung. Diesen Bericht hat der Bundesminister für Inneres dem ständigen Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit auf dessen Verlangen im Rahmen des Auskunfts- und Einsichtsrechtes nach Art52a Abs2 B-VG zugänglich zu machen."

3. §24 des Bundesgesetzes über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000), BGBl. I 165/1999 (teilweise zur Aufhebung beantragt) lautet:

"Informationspflicht des Auftraggebers

§24. (1) Der Auftraggeber einer Datenanwendung hat aus Anlaß der Ermittlung von Daten die Betroffenen in geeigneter Weise

1. über den Zweck der Datenanwendung, für die die Daten ermittelt werden, und

2. über Namen und Adresse des Auftraggebers,

zu informieren, sofern diese Informationen dem Betroffenen nach den Umständen des Falles nicht bereits vorliegen.

(2) Über Abs1 hinausgehende Informationen sind in geeigneter Weise zu geben, wenn dies für eine Verarbeitung nach Treu und Glauben erforderlich ist; dies gilt insbesondere dann, wenn

1. gegen eine beabsichtigte Verarbeitung oder Übermittlung von Daten ein Widerspruchsrecht des Betroffenen gemäß §28 besteht oder

2. es für den Betroffenen nach den Umständen des Falles nicht klar erkennbar ist, ob er zur Beantwortung der an ihn gestellten Fragen rechtlich verpflichtet ist, oder

3. Daten in einem Informationsverbundsystem verarbeitet werden sollen, ohne daß dies gesetzlich vorgesehen ist.

(3) Werden Daten nicht durch Befragung des Betroffenen, sondern durch Übermittlung von Daten aus anderen Aufgabengebieten desselben Auftraggebers oder aus Anwendungen anderer Auftraggeber ermittelt, darf die Information gemäß Abs1 entfallen, wenn

1. die Datenverwendung durch Gesetz oder Verordnung vorgesehen ist oder

2. die Information im Hinblick auf die mangelnde Erreichbarkeit von Betroffenen unmöglich ist oder

3. wenn sie angesichts der Unwahrscheinlichkeit einer Beeinträchtigung der Betroffenenrechte einerseits und der Kosten der Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordert. Dies liegt insbesondere dann vor, wenn Daten für Zwecke der wissenschaftlichen Forschung oder Statistik gemäß §46 oder Adreßdaten im Rahmen des §47 ermittelt werden und die Information des Betroffenen in diesen Bestimmungen nicht ausdrücklich vorgeschrieben ist. Der Bundeskanzler kann durch Verordnung weitere Fälle festlegen, in welchen die Pflicht zur Information entfällt.

(4) Keine Informationspflicht besteht bei jenen Datenanwendungen, die gemäß §17 Abs2 und 3 nicht meldepflichtig sind."

4. Die weiteren hier maßgeblichen Bestimmungen des DSG 2000 lauten:

"5. Abschnitt

Die Rechte des Betroffenen

Auskunftsrecht

§26. (1) Der Auftraggeber hat dem Betroffenen Auskunft über die zu seiner Person verarbeiteten Daten zu geben, wenn der Betroffene dies schriftlich verlangt und seine Identität in geeigneter Form nachweist. Mit Zustimmung des Auftraggebers kann das Auskunftsbegehren auch mündlich gestellt werden. Die Auskunft hat die verarbeiteten Daten, die verfügbaren Informationen über ihre Herkunft, allfällige Empfänger oder Empfängerkreise von Übermittlungen, den Zweck der Datenverwendung sowie die Rechtsgrundlagen hiefür in allgemein verständlicher Form anzuführen. Auf Verlangen des Betroffenen sind auch Namen und Adresse von Dienstleistern bekanntzugeben, falls sie mit der Verarbeitung seiner Daten beauftragt sind. Mit Zustimmung des Betroffenen kann anstelle der schriftlichen Auskunft auch eine mündliche Auskunft mit der Möglichkeit der Einsichtnahme und der Abschrift oder Ablichtung gegeben werden.

(2) Die Auskunft ist nicht zu erteilen, soweit dies zum Schutz des Betroffenen aus besonderen Gründen notwendig ist oder soweit überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten, insbesondere auch überwiegende öffentliche Interessen, der Auskunftserteilung entgegenstehen. Überwiegende öffentliche Interessen können sich hiebei aus der Notwendigkeit

1. des Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich oder

2. der Sicherung der Einsatzbereitschaft des Bundesheeres oder

3. der Sicherung der Interessen der umfassenden Landesverteidigung oder

4. des Schutzes wichtiger außenpolitischer, wirtschaftlicher oder finanzieller Interessen der Republik Österreich oder der Europäischen Union oder

5. der Vorbeugung, Verhinderung oder Verfolgung von Straftaten ergeben. Die Zulässigkeit der Auskunftsverweigerung aus den Gründen der Z1 bis 5 unterliegt der Kontrolle durch die Datenschutzkommission nach §30 Abs3 und dem besonderen Beschwerdeverfahren vor der Datenschutzkommission gemäß §31 Abs4.

(3) Der Betroffene hat am Auskunftsverfahren über Befragung in dem ihm zumutbaren Ausmaß mitzuwirken, um ungerechtfertigten und unverhältnismäßigen Aufwand beim Auftraggeber zu vermeiden.

(4) Innerhalb von acht Wochen nach Einlangen des Begehrens ist die Auskunft zu erteilen oder schriftlich zu begründen, warum sie nicht oder nicht vollständig erteilt wird. Von der Erteilung der Auskunft kann auch deshalb abgesehen werden, weil der Betroffene am Verfahren nicht gemäß Abs3 mitgewirkt oder weil er den Kostenersatz nicht geleistet hat.

(5) In jenen Bereichen der Vollziehung, die mit der Wahrnehmung der in Abs2 Z1 bis 5 bezeichneten Aufgaben betraut sind, ist, soweit dies zum Schutz jener öffentlichen Interessen notwendig ist, die eine Auskunftsverweigerung erfordert, folgendermaßen vorzugehen:

Es ist in allen Fällen, in welchen keine Auskunft erteilt wird - also auch weil tatsächlich keine Daten verwendet werden -, anstelle einer inhaltlichen Begründung der Hinweis zu geben, daß keine der Auskunftspflicht unterliegenden Daten über den Betroffenen verwendet werden. Die Zulässigkeit dieser Vorgangsweise unterliegt der Kontrolle durch die Datenschutzkommission nach §30 Abs3 und dem besonderen Beschwerdeverfahren vor der Datenschutzkommission nach §31 Abs4.

(6) Die Auskunft ist unentgeltlich zu erteilen, wenn sie den aktuellen Datenbestand einer Datenanwendung betrifft und wenn der Betroffene im laufenden Jahr noch kein Auskunftsersuchen an den Auftraggeber zum selben Aufgabengebiet gestellt hat. In allen anderen Fällen kann ein pauschalierter Kostenersatz von 18,89 Euro verlangt werden, von dem wegen tatsächlich erwachsender höherer Kosten abgewichen werden darf. Ein etwa geleisteter Kostenersatz ist ungeachtet allfälliger Schadenersatzansprüche zurückzuerstatten, wenn Daten rechtswidrig verwendet wurden oder wenn die Auskunft sonst zu einer Richtigstellung geführt hat.

(7) Ab dem Zeitpunkt der Kenntnis von einem Auskunftsverlangen darf der Auftraggeber Daten über den Betroffenen innerhalb eines Zeitraums von vier Monaten und im Falle der Erhebung einer Beschwerde gemäß §31 an die Datenschutzkommission bis zum rechtskräftigen Abschluß des Verfahrens nicht vernichten.

(8) Soweit Datenanwendungen von Gesetzes wegen öffentlich einsehbar sind, hat der Betroffene ein Recht auf Auskunft in dem Umfang, in dem ein Einsichtsrecht besteht. Für das Verfahren der Einsichtnahme gelten die näheren Regelungen der das öffentliche Buch oder Register einrichtenden Gesetze.

(9) Für Auskünfte aus dem Strafregister gelten die besonderen Bestimmungen des Strafregistergesetzes 1968 über Strafregisterbescheinigungen.

(10) Im Falle der auf Grund von Rechtsvorschriften, Standesregeln oder Verhaltensregeln gemäß §6 Abs4 eigenverantwortlichen Entscheidung über die Durchführung einer Datenanwendung durch einen Auftragnehmer gemäß §4 Z4, dritter Satz, kann der Betroffene sein Auskunftsbegehren zunächst auch an denjenigen richten, der die Herstellung des Werkes aufgetragen hat. Dieser hat dem Betroffenen, soweit dies nicht ohnehin bekannt ist, binnen zwei Wochen unentgeltlich Namen und Adresse des eigenverantwortlichen Auftragnehmers mitzuteilen, damit der Betroffene sein Auskunftsrecht gemäß Abs1 gegen diesen geltend machen kann.

Recht auf Richtigstellung oder Löschung

27. (1) Jeder Auftraggeber hat unrichtige oder entgegen den Bestimmungen dieses Bundesgesetzes verarbeitete Daten richtigzustellen oder zu löschen, und zwar

1. aus eigenem, sobald ihm die Unrichtigkeit von Daten oder die Unzulässigkeit ihrer Verarbeitung bekannt geworden ist, oder

2. auf begründeten Antrag des Betroffenen.

Der Pflicht zur Richtigstellung nach Z1 unterliegen nur solche Daten, deren Richtigkeit für den Zweck der Datenanwendung von Bedeutung ist. Die Unvollständigkeit verwendeter Daten bewirkt nur dann einen Berichtigungsanspruch, wenn sich aus der Unvollständigkeit im Hinblick auf den Zweck der Datenanwendung die Unrichtigkeit der Gesamtinformation ergibt. Sobald Daten für den Zweck der Datenanwendung nicht mehr benötigt werden, gelten sie als unzulässig verarbeitete Daten und sind zu löschen, es sei denn, daß ihre Archivierung rechtlich zulässig ist und daß der Zugang zu diesen Daten besonders geschützt ist. Die Weiterverwendung von Daten für einen anderen Zweck ist nur zulässig, wenn eine Übermittlung der Daten für diesen Zweck zulässig ist; die Zulässigkeit der Weiterverwendung für wissenschaftliche oder statistische Zwecke ergibt sich aus den §§46 und 47.

(2) Der Beweis der Richtigkeit der Daten obliegt - sofern gesetzlich nicht ausdrücklich anderes angeordnet ist - dem Auftraggeber, soweit die Daten nicht ausschließlich auf Grund von Angaben des Betroffenen ermittelt wurden.

(3) Eine Richtigstellung oder Löschung von Daten ist ausgeschlossen, soweit der Dokumentationszweck einer Datenanwendung nachträgliche Änderungen nicht zuläßt. Die erforderlichen Richtigstellungen sind diesfalls durch entsprechende zusätzliche Anmerkungen zu bewirken.

(4) Innerhalb von acht Wochen nach Einlangen eines Antrags auf Richtigstellung oder Löschung ist dem Antrag zu entsprechen und dem Betroffenen davon Mitteilung zu machen oder schriftlich zu begründen, warum die verlangte Löschung oder Richtigstellung nicht vorgenommen wird.

(5) In jenen Bereichen der Vollziehung, die mit der Wahrnehmung der in §26 Abs2 Z1 bis 5 bezeichneten Aufgaben betraut sind, ist, soweit dies zum Schutz jener öffentlichen Interessen notwendig ist, die eine Geheimhaltung erfordern, mit einem Richtigstellungs- oder Löschungsantrag folgendermaßen zu verfahren:

Die Richtigstellung oder Löschung ist vorzunehmen, wenn das Begehren des Betroffenen nach Auffassung des Auftraggebers berechtigt ist. Die gemäß Abs4 erforderliche Mitteilung an den Betroffenen hat in allen Fällen dahingehend zu lauten, daß die Überprüfung der Datenbestände des Auftraggebers im Hinblick auf das Richtigstellungs- oder Löschungsbegehren durchgeführt wurde. Die Zulässigkeit dieser Vorgangsweise unterliegt der Kontrolle durch die Datenschutzkommission nach §30 Abs3 und dem besonderen Beschwerdeverfahren vor der Datenschutzkommission nach §31 Abs4.

(6) Wenn die Löschung oder Richtigstellung von Daten auf ausschließlich automationsunterstützt lesbaren Datenträgern aus Gründen der Wirtschaftlichkeit nur zu bestimmten Zeitpunkten vorgenommen werden kann, sind bis dahin die zu löschenden Daten für den Zugriff zu sperren und die zu berichtigenden Daten mit einer berichtigenden Anmerkung zu versehen.

(7) Werden Daten verwendet, deren Richtigkeit der Betroffene bestreitet, und läßt sich weder ihre Richtigkeit noch ihre Unrichtigkeit feststellen, so ist auf Verlangen des Betroffenen ein Vermerk über die Bestreitung beizufügen. Der Bestreitungsvermerk darf nur mit Zustimmung des Betroffenen oder auf Grund einer Entscheidung des zuständigen Gerichtes oder der Datenschutzkommission gelöscht werden.

(8) Wurden im Sinne des Abs1 richtiggestellte oder gelöschte Daten vor der Richtigstellung oder Löschung übermittelt, so hat der Auftraggeber die Empfänger dieser Daten hievon in geeigneter Weise zu verständigen, sofern dies keinen unverhältnismäßigen Aufwand, insbesondere im Hinblick auf das Vorhandensein eines berechtigten Interesses an der Verständigung, bedeutet und die Empfänger noch feststellbar sind.

(9) Die Regelungen der Abs1 bis 8 gelten für das gemäß Strafregistergesetz 1968 geführte Strafregister sowie für öffentliche Bücher und Register, die von Auftraggebern des öffentlichen Bereichs geführt werden, nur insoweit als für

1. die Verpflichtung zur Richtigstellung und Löschung von Amts wegen oder
2. das Verfahren der Durchsetzung und die Zuständigkeit zur Entscheidung über Berichtigungs- und Löschungsanträge von Betroffenen

durch Bundesgesetz nicht anderes bestimmt ist.

...

6. Abschnitt
Rechtsschutz
Kontrollbefugnisse der Datenschutzkommission

§30. (1) Jedermann kann sich wegen einer behaupteten Verletzung seiner Rechte oder ihn betreffender Pflichten eines Auftraggebers oder Dienstleisters nach diesem Bundesgesetz mit einer Eingabe an die Datenschutzkommission wenden.

(2) Die Datenschutzkommission kann im Fall eines begründeten Verdachtes auf Verletzung der im Abs1 genannten Rechte und Pflichten Datenanwendungen überprüfen. Hiebei kann sie vom Auftraggeber oder Dienstleister der überprüften Datenanwendung insbesondere alle notwendigen Aufklärungen verlangen und Einschau in Datenanwendungen und diesbezügliche Unterlagen begehren.

(3) Datenanwendungen, die der Vorabkontrolle gemäß §18 Abs2 unterliegen, dürfen auch ohne Vorliegen eines Verdachts auf rechtswidrige Datenverwendung überprüft werden. Dies gilt auch für jene Bereiche der Vollziehung, in welchen ein Auftraggeber des öffentlichen Bereichs die grundsätzliche Anwendbarkeit der §§26 Abs5 und 27 Abs5 in Anspruch nimmt.

(4) Zum Zweck der Einschau ist die Datenschutzkommission nach Verständigung des Inhabers der Räumlichkeiten und des Auftraggebers (Dienstleisters) berechtigt, Räume, in welchen Datenanwendungen vorgenommen werden, zu betreten, Datenverarbeitungsanlagen in Betrieb zu setzen, die zu überprüfenden Verarbeitungen durchzuführen sowie Kopien von Datenträgern in dem für die Ausübung der Kontrollbefugnisse unbedingt erforderlichen Ausmaß herzustellen. Der Auftraggeber (Dienstleister) hat die für die Einschau notwendige Unterstützung zu leisten. Die Kontrolltätigkeit ist unter möglichster Schonung der Rechte des Auftraggebers (Dienstleisters) und Dritter auszuüben.

(5) Informationen, die der Datenschutzkommission oder ihren Beauftragten bei der Kontrolltätigkeit zukommen, dürfen ausschließlich für die Kontrolle im Rahmen der Vollziehung datenschutzrechtlicher Vorschriften verwendet werden. Die Pflicht zur Verschwiegenheit besteht auch gegenüber Gerichten und Verwaltungsbehörden, insbesondere Abgabenbehörden; dies allerdings mit der Maßgabe, daß dann, wenn die Einschau den Verdacht einer strafbaren Handlung nach den §§51 oder 52 dieses Bundesgesetzes oder eines Verbrechens nach §278a StGB (kriminelle Organisation) oder eines Verbrechens mit einer Freiheitsstrafe, deren Höchstmaß fünf Jahre übersteigt, ergibt, Anzeige zu erstatten ist und hinsichtlich solcher Verbrechen und Vergehen auch dem Ersuchen der Strafgerichte nach §26 StPO zu entsprechen ist.

(6) Zur Herstellung des rechtmäßigen Zustandes kann die Datenschutzkommission Empfehlungen aussprechen, für deren Befolgung erforderlichenfalls eine angemessene Frist zu setzen ist. Wird einer solchen Empfehlung innerhalb der gesetzten Frist nicht entsprochen, so kann die Datenschutzkommission je nach der Art des Verstoßes von Amts wegen insbesondere

1. ein Verfahren zur Überprüfung der Registrierung gemäß §22 Abs4 einleiten, oder

2. Strafanzeige nach §§51 oder 52 erstatten, oder

3. bei schwerwiegenden Verstößen durch Auftraggeber des privaten Bereichs Klage vor dem zuständigen Gericht gemäß §32 Abs5 erheben, oder

4. bei Verstößen von Auftraggebern, die Organe einer Gebietskörperschaft sind, das zuständige oberste Organ befassen. Dieses Organ hat innerhalb einer angemessenen, jedoch zwölf Wochen nicht überschreitenden Frist entweder dafür Sorge zu tragen, daß der Empfehlung der Datenschutzkommission entsprochen wird, oder der Datenschutzkommission mitzuteilen, warum der Empfehlung nicht entsprochen wurde. Die Begründung darf von der Datenschutzkommission der Öffentlichkeit in geeigneter Weise zur Kenntnis gebracht werden, soweit dem nicht die Amtsverschwiegenheit entgegensteht.

(7) Der Einschreiter ist darüber zu informieren, wie mit seiner Eingabe verfahren wurde.

Beschwerde an die Datenschutzkommission

§31. (1) Die Datenschutzkommission erkennt auf Antrag des Betroffenen über behauptete Verletzungen des Rechtes auf Auskunft gemäß §26 durch den Auftraggeber einer Datenanwendung, soweit sich das Auskunftsbegehren nicht auf die Verwendung von Daten für Akte der Gesetzgebung oder der Gerichtsbarkeit bezieht.

(2) Zur Entscheidung über behauptete Verletzungen der Rechte eines Betroffenen auf Geheimhaltung, auf Richtigstellung oder auf Löschung nach diesem Bundesgesetz ist die Datenschutzkommission dann zuständig, wenn der Betroffene seine Beschwerde gegen einen Auftraggeber des öffentlichen Bereichs richtet, der nicht als Organ der Gesetzgebung oder der Gerichtsbarkeit tätig ist.

(3) Bei Gefahr im Verzug kann die Datenschutzkommission im Zuge der Behandlung einer Beschwerde nach Abs2 die weitere Verwendung von Daten zur Gänze oder teilweise untersagen oder auch - bei Streitigkeiten über die Richtigkeit von Daten - dem Auftraggeber die Anbringung eines Bestreitungsvermerks auftragen.

(4) Beruft sich ein Auftraggeber des öffentlichen Bereichs bei einer Beschwerde wegen Verletzung des Auskunfts-, Richtigstellungs- oder Löschungsrechts gegenüber der Datenschutzkommission auf die §§26 Abs5 oder 27 Abs5, so hat diese nach Überprüfung der Notwendigkeit der Geheimhaltung die geschützten öffentlichen Interessen in ihrem Verfahren zu wahren. Kommt sie zur Auffassung, daß die Geheimhaltung von verarbeiteten Daten gegenüber dem Betroffenen nicht gerechtfertigt war, ist die Offenlegung der Daten mit Bescheid aufzutragen. Gegen diese Entscheidung der Datenschutzkommission kann die belangte Behörde Beschwerde an den Verwaltungsgerichtshof erheben. Wurde keine derartige Beschwerde eingebracht und wird dem Bescheid der Datenschutzkommission binnen acht Wochen nicht entsprochen, so hat die Datenschutzkommission die Offenlegung der Daten gegenüber dem Betroffenen selbst vorzunehmen und ihm die verlangte Auskunft zu erteilen oder ihm mitzuteilen, welche Daten bereits berichtigt oder gelöscht wurden."

III. Antragsvorbringen betreffend die Frage der Zulässigkeit:

1. Im Antrag seien im Hinblick auf das Zulässigkeitskriterium der Betroffenheit - und in der Folge auch im Hinblick auf die Eingriffsfrage und die Grundrechtswidrigkeit der angefochtenen gesetzlichen Regelungen - zwei unterschiedliche Argumentationsstränge zu unterscheiden:

* wonach das durch die Ausnahmen von der Informationspflicht des §24 DSG 2000 bedingte Fehlen eines effizienten, gesetzlich eingerichteten Rechtsschutzes gegen die Ausübung der angefochtenen Befugnisse der Sicherheitsbehörden eine aktuelle und unmittelbare Betroffenheit der Antragsteller im Hinblick auf das prozessuale Recht auf eine wirksame Beschwerde gemäß Art13 EMRK iVm §1 DSG, Art8 und 10 EMRK sowie Art7 B-VG, aber auch "in" die materiellen Rechte auf Datenschutz gemäß §1 DSG 2000, auf Achtung des Privatlebens und des Briefverkehrs gemäß Art8 EMRK, auf Meinungs- und Informationsfreiheit des Art10 EMRK sowie auf Gleichheit vor dem Gesetz gemäß Art7 B-VG auslöse;

* wonach eben wegen des Fehlens eines wirksamen

Rechtsschutzes die angefochtenen, im SPG geregelten Befugnisse der Sicherheitsbehörden ebenso in materiellrechtlicher Hinsicht eine aktuelle und unmittelbare Betroffenheit der Antragsteller im Hinblick auf deren Rechte auf Datenschutz gemäß §1 DSG 2000, auf Achtung des Privatlebens und des Briefverkehrs gemäß Art8 EMRK, auf Meinungs- und Informationsfreiheit des Art10 EMRK sowie auf Gleichheit vor dem Gesetz gemäß Art7 B-VG auslösten.

Betroffen könnten nach ständiger Rechtsprechung des Verfassungsgerichtshofs nur solche Rechtsträger sein, an oder gegen die sich das Gesetz richtet. Die angefochtenen SPG-Normen würden die Organe der Sicherheitsbehörden nun zur Verwendung personenbezogener Daten ermächtigen. Die Antragsteller verfügten alle über einen Wohnsitz/Unternehmenssitz in Österreich und einen mobilen und/oder festen Telefonanschluss sowie einen EDV/Internetanschluss mit IP-Adresse. Gegen sie - so wie gegen alle anderen Menschen in Österreich, auf die diese Eigenschaften zutreffen - würden sich somit die angefochtenen Bestimmungen des SPG richten, die den Sicherheitsbehörden rechtsstaatlich unkontrollierte Datenverwendungen einräumten. Den von den Antragstellern geltend gemachten verfassungsgesetzlich gewährleisteten Rechten werde auch durch §24 iVm §17 DSG 2000 aufgrund fehlender Informationsverpflichtungen nicht wirksam Rechnung getragen, weswegen sie ebenso durch die angefochtenen Teile des §24 DSG 2000 rechtlich betroffen seien.

Es stelle sich aber die grundsätzliche Frage, ob ein Rechtsträger durch ein Gesetz, das die Behörden zur Vornahme von Vollzugsakten ermächtige, überhaupt "aktuell" und "unmittelbar" iSd Rechtsprechung des Verfassungsgerichtshofs zu Art140 B-VG betroffen sein kann. Eine "Betroffenheit" bzw. ein "Eingriff" im Sinne dieser Rechtsprechung scheine erst durch ein konkretes Organhandeln möglich zu sein, im vorliegenden Fall also durch eine konkrete Datenverwendung im Einzelfall.

Da die Antragsteller alleine bedingt durch die Gesetzeslage ohne Dazwischentreten einer individuellen Entscheidung über allfällige sicherheitsbehördliche Datenverwendungen der Sicherheitsbehörden nicht informiert würden, verträten sie die Auffassung, dass die angefochtenen gesetzlichen Bestimmungen eine "aktuelle" und "unmittelbare" rechtliche Betroffenheit der Antragsteller auslösten. Nur für den Fall, dass "der VfGH dieser Argumentation nicht zu folgen vermag", also in eventu, würden die Antragsteller auf die Judikatur des deutschen Bundesverfassungsgerichts (BVerfG) hinweisen, wonach für die Annahme einer aktuellen und gegenwärtigen Betroffenheit ausreiche, wenn der Beschwerdeführer darlegt, dass er "mit einiger Wahrscheinlichkeit" durch die auf den angegriffenen Rechtsnormen beruhenden Maßnahmen in seinen Grundrechten berührt wird. Der geforderte Grad der Wahrscheinlichkeit werde davon beeinflusst, welche

Möglichkeit der Beschwerdeführer habe, seine Betroffenheit darzulegen. So sei bedeutsam, ob die Maßnahme auf einen tatbestandlich eng umgrenzten Personenkreis zielt oder ob sie eine große Streubreite hat und Dritte auch zufällig erfassen kann. Darlegungen, durch die sich der Beschwerdeführer selbst einer Straftat bezichtigen müsste, dürften zum Beleg der eigenen gegenwärtigen Betroffenheit nicht verlangt werden.

Wie "das BVerfG ausführt", genügten im Hinblick auf die Frage der unmittelbaren und gegenwärtigen Betroffenheit die Darlegungen der Antragsteller zum Nachweis ihrer persönlichen und gegenwärtigen Betroffenheit. Betroffener einer Überwachung sei dieser Judikaturlinie zufolge jeder, in dessen Persönlichkeitsrechte durch die Maßnahme eingegriffen wird, auch wenn er nicht Zielperson der Anordnung ist. Die Möglichkeit, Objekt einer Maßnahme der Telekommunikationsüberwachung aufgrund der angegriffenen Regelungen zu werden, bestehe zwar praktisch für jede Person. Sie betreffe aber nicht nur mögliche Straftäter selbst oder deren Kontakt- und Begleitpersonen, sondern auch Personen, die mit den Adressaten der Maßnahme über Telekommunikationseinrichtungen auch nur zufällig in Verbindung stehen.

Wenngleich alle Antragsteller (und letztlich alle in Österreich lebenden Menschen, die über ein Mobiltelefon, einen Internetanschluss und ein Fahrzeug verfügen) durch die angefochtenen Normen unmittelbar und aktuell betroffen seien, solle für ausgewählte Antragsteller deren besondere berufliche Situation herausgestrichen werden, die für die Beantwortung der Frage nach deren wahrscheinlicher Betroffenheit von erheblicher Relevanz sei. Die Antragsteller seien unterschiedlichen Berufsgruppen zuzuordnen. Die meisten von ihnen würden Tätigkeiten ausüben, bei denen mit Hilfe moderner Technologie sensible Inhalte, oft auch auf vertraulicher Basis, kommuniziert würden, an deren Kenntnis Sicherheitsbehörden in Verdachtsfällen im Sinne der angefochtenen Bestimmungen des SPG ein Interesse hätten. Die Wahrscheinlichkeit, dass die Antragsteller von entsprechenden "Auskunftsverlangen an Datenverwendungen" der Sicherheitsbehörden betroffen sein könnten, sei daher sehr hoch.

Die meisten Antragsteller würden nämlich Berufsgruppen angehören, deren berufliche Kommunikation über Telefon und Internet - in unterschiedlichem Umfang - auch mit Personen erfolge, an denen Sicherheitsbehörden im Sinne der Wahrnehmung der ihnen nach den angefochtenen Bestimmungen des SPG übertragenen Aufgaben ein Interesse haben könnten. Dadurch sei im Sinne der Rechtsprechung des BVerfG "mit einiger Wahrscheinlichkeit" davon auszugehen, dass die Antragsteller durch die angefochtenen Bestimmungen betroffen und in den geltend gemachten Grundrechten berührt sind.

2. Die Antragsteller vertreten die Auffassung, dass die angefochtenen Bestimmungen ohne Dazwischentreten eines individuellen Vollzugsaktes in ihre verfassungsgesetzlich gewährleisteten Rechte auf Datenschutz gemäß §1 DSG 2000, auf Achtung des Privatlebens und des Briefverkehrs gemäß Art8 EMRK, auf Meinungs- und Informationsfreiheit des Art10 EMRK sowie auf Gleichheit vor dem Gesetz gemäß Art7 B-VG eingriffen.

3.1. Die Ausübung der angefochtenen Befugnisse erfolge nicht durch einen den Antragstellern zur Kenntnis zu bringenden Verwaltungsakt, etwa einen Bescheid. Vielmehr dürften diese Maßnahmen als so genanntes "schlichtes Verwaltungshandeln" zu qualifizieren sein.

Mangels entsprechender Regelungen sei davon auszugehen, dass Betroffene tatsächlich über Datenverwendungen iSd angefochtenen Befugnisse [nicht] informiert werden würden. Daher seien die Antragsteller - wie alle anderen Kommunikationsteilnehmer in Österreich auch - "stets gleichermaßen aktuell wie potentiell" in ihrer Rechtssphäre betroffen. Diese Frage verschmelze auch untrennbar mit jener nach einem zumutbaren Rechtsweg. Denn um herauszufinden, ob "ein Auskunftsersuchen nach §26 Abs1 DSG 2000 der angefochtenen Befugnisse ausgeübt wurde", müssten die Antragsteller praktisch täglich eine entsprechende Beschwerde gegen eine unbekannte Sicherheitsbehörde oder alle Sicherheitsbehörden an die Datenschutzkommission erheben oder eine Anfrage nach dem Auskunftspflichtgesetz an jede zur Vollziehung der angefochtenen Bestimmungen des SPG befugte Sicherheitsbehörde als Auftraggeber iSd DSG 2000 wegen einer bloß vermuteten, aber jederzeit möglichen Datenverwendung stellen. So eine Vorgehensweise sei weder effektiv noch den Antragstellern zumutbar. Noch weniger zumutbar sei den Antragstellern, die Sicherheitsbehörden zu einer Datenverwendung zu provozieren, etwa indem sie sich selbst in eine Gefahrensituation begeben oder den Verdacht eines gefährlichen Angriffs erwecken.

3.2. Ein möglicher Rechtsschutz über den Zivilrechtsweg scheide schon deshalb als zumutbarer "Umweg" aus, weil bei gegebenenfalls rechtswidrigen Verhaltensweisen der Diensteanbieter und Provider die hier bekämpften Normen gar nicht präjudiziell wären.

Es sei den Antragstellern im Sinne der Rechtsprechung des Verfassungsgerichtshofs zur "Umwegs(un)zumutbarkeit" gemäß Art140 Abs1 B-VG keinesfalls zumutbar, bei vollem Kostenrisiko

irgendeinen privaten Anbieter zivilgerichtlich wegen einer mutmaßlichen Handlung (der Herausgabe personenbezogener Daten) zu klagen, dessen Passivlegitimation sie mangels Information nicht einmal substantiiert behaupten könnten. Daher könne eine Klage gegen Betreiber vor den Zivilgerichten keinesfalls eine zumutbare Rechtsschutzalternative sein.

3.3. Der Antrag nach Art140 Abs1 B-VG bleibe das letzte und einzige zumutbare Rechtsmittel, er sei hier die "ultima ratio" des Grundrechtsschutzes. Weil Art13 EMRK den Antragstellern ein Recht auf eine wirksame Beschwerde vor einer nationalen Instanz einräume, wenn die Möglichkeit der Verletzung eines materiellen Konventionsrechtes besteht, würden die Antragsteller wegen des Fehlens zumutbarer Rechtsschutzwege von der Zulässigkeit des vorliegenden Individualantrags ausgehen.

Die zur Wahrung der Rechtsschutzinteressen durchaus als conditio sine qua non zu bezeichnenden Informationen über zumindest den Zweck und somit den Umstand der Datenverwendung sowie über die Identität des Auftraggebers kämen den Betroffenen nicht zu. Die dieser Praxis zugrunde liegende Rechtsauffassung des Bundesministers für Inneres sei zumindest vom Wortlaut der (einfach)gesetzlichen Bestimmungen des DSG 2000 sowie des SPG gedeckt. Ohne entsprechende Information hätten die Betroffenen aber keine Möglichkeiten, Datenverwendungen auf deren Rechtmäßigkeit zu überprüfen und im Falle einer rechtswidrigen Vorgangsweise der Behörden sich gegen diese zur Wehr zu setzen. Auch die anderen Kontroll- und Beschwerdeinstrumente erwiesen sich angesichts des Rechtsschutzbedürfnisses der Antragsteller gegen die angefochtenen Befugnisse der Sicherheitsbehörden als ungeeignet oder ungenügend, da sie keine "wirksame Beschwerdemöglichkeit" iSd Art13 EMRK in Verbindung mit den geltend gemachten materiellen Grundrechten eröffneten.

IV. Die Bundesregierung erstattete eine Äußerung, in der sie die Zulässigkeit des Individualantrages mit folgenden Argumenten bestreitet:

1. Zur Zulässigkeit der Anträge im Allgemeinen führt die Bundesregierung aus:

Die Antragsteller würden zu ihrer aktuellen und unmittelbaren Betroffenheit argumentieren, sie "verfügen alle über einen Wohnsitz/Unternehmenssitz in Österreich und einen mobilen und/oder festen Telefonanschluss sowie einen EDV-Internetanschluss mit IP-Adresse. Gegen sie - so wie gegen alle anderen Menschen in Österreich, auf die diese Eigenschaft[en] zutreffen - würden sich somit die angefochtenen Bestimmungen des SPG richten, die den Sicherheitsbehörden rechtsstaatlich unkontrollierte Datenverwendungen einräumen ...".

Zu diesem Vorbringen sei zunächst anzumerken, dass ihm der entsprechende Nachweis bezogen auf die jeweiligen Antragsteller fehle. Das Vorbringen werde auch pauschal zu allen der angefochtenen Bestimmungen vorgebracht und unterlasse eine nähere Substantiierung und Auseinandersetzung mit den jeweiligen - immerhin zu zwölf Antragsgegenständen gruppierten - Bestimmungen. Vermissen lasse das Vorbringen zum einen auch die Darlegung der jeweiligen konkreten Betroffenheit der siebenundzwanzig Antragsteller. Zum anderen lege es auch nicht dar, inwieweit die Antragsteller im Einzelnen, etwa von der angefochtenen ermächtigenden Bestimmung des Einsatzes von Kennzeichenerkennungsgeräten (§54 Abs4b SPG), in ihren Rechten konkret betroffen sein könnten. Das Erfordernis der Darlegung der aktuellen und unmittelbaren rechtlichen Betroffenheit der Antragsteller erfordere nach Ansicht der Bundesregierung substantiiertere Darlegungen als das - zusammengefasste - Vorbringen, dass sich die angefochtenen Bestimmungen gegen die Antragsteller ebenso wie gegen alle anderen Menschen in Österreich richten.

Die Antragsteller argumentierten in eventu - und bei näherer Betrachtung liege hier das Schwergewicht der Argumentation der Betroffenheit - darüber hinaus unter Abstellen auf die Judikatur des deutschen Bundesverfassungsgerichts, dass es für die Annahme einer aktuellen und gegenwärtigen Betroffenheit ausreiche, wenn von den Antragstellern dargelegt werde, dass sie "mit einiger Wahrscheinlichkeit" durch die auf den angegriffenen Rechtsnormen beruhenden Maßnahmen in ihren Rechten berührt werden. Die Ausführungen des Antrages zu den vom deutschen Bundesverfassungsgericht aufgestellten Kriterien für die Beurteilung der aktuellen und gegenwärtigen Betroffenheit bedürften nach Ansicht der Bundesregierung keiner Auseinandersetzung, da die Antragsteller nicht dargetan hätten, inwieweit diese Rechtsprechung geeignet ist, den vom (österreichischen) Verfassungsgerichtshof in ständiger Rechtsprechung festgelegten Prüf- und Beurteilungsmaßstab der aktuellen und unmittelbaren Betroffenheit zu modifizieren.

2. Zur Zulässigkeit des Antrages auf Aufhebung von Bestimmungen des DSG 2000 führt die Bundesregierung aus:

Der Antrag enthalte keine Darlegungen über die unmittelbare Betroffenheit der Antragsteller in ihrer Rechtssphäre durch die angefochtene Wortfolge in §24 Abs1 DSG 2000, wonach die Information "aus Anlaß der Ermittlung von Daten" zu erfolgen hat. Im Antrag würden wohl verfassungsrechtliche Bedenken gegen diese

Wortfolge im Hinblick auf näher bezeichnete Grundrechte vorgebracht. Weder dabei noch sonst werde jedoch ausgeführt, inwieweit eine Rechtssphäre des Antragstellers bestünde, in welche durch diese Norm eingegriffen würde bzw. inwieweit die Antragsteller durch diese Norm unmittelbar betroffen wären. Fehlt eine solche Darlegung, führe dies zur Unzulässigkeit des Individualantrages.

Auch im Übrigen vermöge der Antrag die Voraussetzungen für die Zulässigkeit nicht zu erfüllen. Die Antragsteller begründeten ihre Legitimation allgemein damit, dass das "durch die Ausnahmen von der Informationspflicht des §24 DSG 2000 bedingte Fehlen eines effizienten, gesetzlich eingerichteten Rechtsschutzes gegen die Ausübung der angefochtenen Befugnisse der Sicherheitsbehörden ... eine aktuelle und unmittelbare Betroffenheit im Hinblick auf das prozessuale Recht auf eine wirksame Beschwerde gemäß Art13 EMRK iVm §1 DSG, Art8 und 10 EMRK sowie Art7 B-VG, aber auch 'in' die materiellen Rechte auf Datenschutz gemäß §1 DSG 2000, auf Achtung des Privatlebens und des Briefverkehrs gemäß Art8 EMRK, auf Meinungs- und Informationsfreiheit des Art10 EMRK sowie auf Gleichheit vor dem Gesetz gemäß [Art.] 7 B-VG auslöst". Diesen Rechten werde "auch durch §24 iVm §17 DSG 2000 aufgrund fehlender Informationsverpflichtungen nicht wirksam Rechnung getragen, weswegen [die Antragsteller] ... durch die angefochtenen Teile des §24 DSG 2000 rechtlich betroffen sind". Dadurch vermöge ein Eingriff in eine Rechtssphäre der Antragsteller nicht dargetan zu werden. Die Antragsteller vermöchten auch nicht darzulegen, dass sie Normadressaten der angefochtenen Wortfolgen in §24 DSG 2000 seien und es zu einem unmittelbaren Eingriff in ihre (behauptete) Rechtssphäre komme. Der Antrag begründe die rechtliche Betroffenheit der Antragsteller allgemein damit, dass an sich alle in Österreich lebenden Menschen, die über einen Telefon- oder Internetanschluss verfügen, durch die angefochtenen Bestimmungen aktuell und unmittelbar in ihrer Rechtssphäre berührt seien. Die Antragsteller würden aber nicht darlegen, dass gerade ihre (behauptete) Rechtssphäre berührt würde. Es würden auch keine besonderen Umstände geltend gemacht, die es erlauben würden, einen solchen Eingriff bei ihnen anzunehmen. Der Antrag behaupte zwar eine "sehr hohe Wahrscheinlichkeit", dass die Antragsteller "von entsprechenden Auskunftsverlangen an Datenverwendungen der Sicherheitsbehörden betroffen sein können" und führe dies hinsichtlich der einzelnen Antragsteller näher aus. Diese Ausführungen bezögen sich allerdings im Detail lediglich auf die angefochtenen Ermittlungsbefugnisse des §53 Abs3a und 3b SPG, nicht aber auf die angefochtenen Wortfolgen in §24 DSG 2000.

3. Zur Zulässigkeit der Anträge auf Aufhebung von Bestimmungen des SPG führt die Bundesregierung aus:

Dem Antragsvorbringen sei zu entnehmen, dass keine der angefochtenen Bestimmungen für einen oder mehrere Antragsteller direkte Wirkung dadurch entfalte, dass aus konkretem Anlass eine Ermittlung (und Verarbeitung) personenbezogener Daten eines der Antragsteller stattgefunden hat. Insbesondere werde nicht behauptet, dass ein konkretes Auskunftsverlangen gemäß §§53 Abs3a oder 3b SPG an Betreiber oder Diensteanbieter gestellt worden sei, im Zuge dessen Auskünfte über Daten eines der Antragsteller an die Sicherheitsbehörden erteilt worden seien. Es werde vielmehr ausdrücklich darauf verwiesen, dass auf Basis der vorgebrachten Argumente "letztlich alle in Österreich lebenden Menschen, die über ein Mobiltelefon, einen Internetanschluss und ein Fahrzeug verfügen, durch die angefochtenen Normen unmittelbar und aktuell betroffen seien". Das Vorbringen beziehe sich jedoch - wie die Antragsteller selbst einräumten - nicht auf eine konkrete Datenverwendung (insbesondere Ermittlung und Verarbeitung) durch die Exekutive, von der einer oder mehrere Antragsteller betroffen seien, was aber Voraussetzung für die Antragslegitimation sei.

Lediglich hinsichtlich der Antragsgegenstände §53 Abs3a und 3b SPG würden die Antragsteller ihre Ausführungen zur Antragslegitimation vertiefen, insbesondere auch zum Fehlen zumutbarer Rechtsschutzwege. Die Antragsteller vermöchten dabei aber nicht darzulegen, dass sie Normadressaten der Bestimmungen des §53 Abs3a und 3b SPG seien und diese auch für sie selbst direkte und aktuelle Wirksamkeit entfalteten. Die darin statuierten Verpflichtungen zur Erteilung bestimmter Auskünfte würden sich an Betreiber von Telekommunikationsdiensten und sonstige Diensteanbieter richten und seien erst dann für die Antragsteller wirksam, wenn es zu einem die Daten eines Antragstellers betreffenden Auskunftsverlangen der Sicherheitsbehörden kommt. Dies sei nicht behauptet worden. §53 Abs3b SPG statuiere eine Pflicht zur Auskunftserteilung, konkret zur Erteilung der Auskunft über Standortdaten und die internationale Mobilteilnehmerkennung der von einem in Gefahr befindlichen Menschen mitgeführten Endeinrichtung. Standortdaten seien regelmäßig bei Betreibern öffentlicher Telekommunikationsdienste vorhanden; über sie sei schon auf Grund der bestehenden Rechtslage etwa bei Notrufen gemäß §98 TKG 2003 Auskunft zu erteilen; wären die Antragsteller Betreiber öffentlicher Telekommunikationsdienste, so träfe sie bereits aufgrund der zuletzt genannten Bestimmung eine Verpflichtung einem Auskunftsverlangen zu entsprechen. Dass über Standortdaten eines der Antragsteller Auskunft erteilt wurde, werde ebenfalls nicht behauptet.

Darüber hinaus sei dem Vorbringen entgegenzuhalten, dass der aktuell von einer Datenermittlung auf Grundlage der §§53 Abs3a und 3b SPG Betroffene regelmäßig von der Ermittlung seiner Daten erfahre, da diese nicht von der Aufgabenstellung losgelöst zu sehen sei. Es handle sich bei jeder Dateneingriffsermächtigung um eine Befugnis, die nur unter den im Gesetz normierten Voraussetzungen und unter Beachtung der

Verhältnismäßigkeit zulässig sei. Konkret sei der Bezug zu einer gesetzlich vorgesehenen Aufgabe erforderlich. Die Datenverwendung durch die Sicherheitsbehörde gemäß §53 Abs3a und 3b SPG sei nur zur Erfüllung der ihr gesetzlich übertragenen Aufgaben, insbesondere zur Gefahrenabwehr (§21 SPG) und zur ersten allgemeinen Hilfeleistung (§19 SPG) zulässig. Daher werde der Datenermittlung regelmäßig ein "außenwirksames" Einschreiten folgen, etwa das Ausforschen eines Verdächtigen zur Beendigung eines gefährlichen Angriffs oder die Rettung eines Verirrten, und damit gehe für den Betroffenen die Möglichkeit einher, wegen einer behaupteten Verletzung seines Rechts auf Geheimhaltung Rechtsmittel (insb. gemäß §§90 und 88 SPG) zu ergreifen. Dasselbe gelte im Übrigen beim Einsatz besonderer Ermittlungsmaßnahmen nach §54 Abs2 Z3 sowie Abs3 und 4 SPG zur Abwehr gefährlicher Angriffe, weil aufgrund der vorauszusetzenden Aktualität der Rechtsgutbedrohung der verdeckten Maßnahme im Regelfall ein außenwirksames Einschreiten folgen werde. Insoweit gehe daher die Argumentation zum fehlenden Rechtsschutz ins Leere.

Abgesehen von den spezifischen Ausführungen zu den Antragsgegenständen §53 Abs3a und 3b SPG würden nähere Ausführungen zur Antragslegitimation gänzlich fehlen, insbesondere zur zentralen Frage der aktuellen Betroffenheit. Auch die Ausführungen zur Grundrechtswidrigkeit, auf die im Vorbringen zur Antragslegitimation verwiesen werde, würden keine weiteren Anhaltspunkte für eine aktuelle und unmittelbare rechtliche Betroffenheit eines der Antragsteller hinsichtlich der einzelnen Antragsgegenstände geben, weshalb sich diese Anträge jedenfalls als unzulässig erweisen würden.

Keiner der Antragsteller habe eine konkrete und aktuelle Betroffenheit durch Verwendung ihn betreffender personenbezogener Daten in einer Anwendung auch nur behauptet, obwohl dies im Wege der Rechte Betroffener insbesondere auf Auskunft (§26 DSG 2000) feststellbar gewesen wäre. Vom Fehlen zumutbarer Rechtsschutzwege könne insofern nicht gesprochen werden.

Unabhängig von den Beschwerdemöglichkeiten durch den Betroffenen selbst werde an dieser Stelle auf den Rechtsschutz durch den im Sicherheitspolizeigesetz verankerten Rechtsschutzbeauftragten (§§91a ff) hingewiesen, dessen Aufgabe es gerade sei, effektiven Rechtsschutz in allen Fällen von Ermittlung ohne Wissen der Betroffenen zu gewährleisten.

V. Der Verfassungsgerichtshof hat über die Zulässigkeit der Anträge erwogen:

1. Voraussetzung der Antragslegitimation ist einerseits, dass der Antragsteller behauptet, unmittelbar durch das angefochtene Gesetz - im Hinblick auf dessen Verfassungswidrigkeit - in seinen Rechten verletzt worden zu sein, dann aber auch, dass das Gesetz für den Antragsteller tatsächlich, und zwar ohne Fällung einer gerichtlichen Entscheidung oder ohne Erlassung eines Bescheides wirksam geworden ist. Grundlegende Voraussetzung der Antragslegitimation ist, dass das Gesetz in die Rechtssphäre des Antragstellers nachteilig eingreift und diese - im Falle seiner Verfassungswidrigkeit - verletzt. Hiebei hat der Verfassungsgerichtshof vom Antragsvorbringen auszugehen und lediglich zu prüfen, ob die vom Antragsteller ins Treffen geführten Wirkungen solche sind, wie sie Art140 Abs1 letzter Satz B-VG als Voraussetzung für die Antragslegitimation fordert (vgl. zB VfSlg. 11.730/1988, 15.863/2000, 16.088/2001, 16.120/2001).

Nicht jedem Normadressaten aber kommt die Anfechtungsbefugnis zu. Es ist darüber hinaus erforderlich, dass das Gesetz selbst tatsächlich in die Rechtssphäre des Antragstellers unmittelbar eingreift. Ein derartiger Eingriff ist jedenfalls nur dann anzunehmen, wenn dieser nach Art und Ausmaß durch das Gesetz selbst eindeutig bestimmt ist, wenn er die (rechtlich geschützten) Interessen des Antragstellers nicht bloß potentiell, sondern aktuell beeinträchtigt und wenn dem Antragsteller kein anderer zumutbarer Weg zur Abwehr des - behaupteterweise - rechtswidrigen Eingriffes zur Verfügung steht (VfSlg. 11.868/1988, 15.632/1999, 16.616/2002, 16.891/2003).

2. Die Antragsteller behaupten nicht, dass aufgrund der in den bekämpften Bestimmungen des SPG vorgesehenen Ermächtigungen unmittelbar und aktuell in ihre Rechtsposition eingegriffen werde. Sie bringen im Wesentlichen lediglich vor, dass sie mit einiger Wahrscheinlichkeit von Maßnahmen der Sicherheitsbehörden betroffen sein könnten, zu denen die bekämpften Bestimmungen des SPG ermächtigen. Damit stützen sie ihre Antragslegitimation bloß auf die Existenz einer die Sicherheitsbehörden ermächtigenden Norm, die erst im Falle der Inanspruchnahme dieser Ermächtigung unter Umständen zu einer Beeinträchtigung der Rechtssphäre der Antragsteller führen könnte. Der bloße Verweis auf die rechtliche Existenz von die Sicherheitsbehörden zu Auskunftsverlangen gegenüber Dritten ermächtigenden Bestimmungen sowie auf die Tatsache, dass die Antragsteller österreichische Staatsbürger sind, bestimmte Berufe ausüben, Internetnutzer sind und über ein Mobiltelefon und ein KFZ verfügen, vermag aber eine unmittelbare und aktuelle Betroffenheit der Antragsteller durch die von ihnen bekämpften Bestimmungen des SPG nicht darzutun.

Soweit die Antragsteller jedoch ihre Legitimation aus Entscheidungen des EGMR abzuleiten versuchen (insb. EGMR 6.9.1978, Fall Klass ua. gg. Deutschland, EuGRZ 1979, 278, und zuletzt EGMR 29.6.2006, Fall Weber und Saravia gg. Deutschland, Appl. 54.934/00), ist ihnen zu entgegnen: Der EGMR hat zwar ausgesprochen, dass

"die bloße Existenz von Gesetzen, die eine geheime Überwachung des Fernmeldeverkehrs gestatten [Anm.: in diesen Fällen ging es um die Befugnisse des dt. Bundesnachrichtendienstes zur Abhörung des Fernmeldeverkehrs im Zuge der sog. 'strategischen Überwachung'], für alle möglicherweise von dem Gesetz Betroffenen ein Überwachungsrisiko beinhaltet. Dieses Risiko betrifft notwendigerweise die Kommunikationsfreiheit zwischen den Nutzern der Telekommunikationsdienste und stellt daher an sich schon einen Eingriff in die Rechte der Beschwerdeführer nach Artikel 8 dar, unabhängig davon, ob gegen sie tatsächlich Maßnahmen ergriffen wurden." (EGMR, Fall Weber und Saravia gegen Deutschland, Rz 78)

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 Abs3b 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. Gemäß §91c Abs1 SPG sind die Sicherheitsbehörden verpflichtet, den Rechtsschutzbeauftragten u.a. von jeder Ermittlung personenbezogener Daten durch verdeckte Ermittlung (§54 Abs3 SPG) und durch den verdeckten Einsatz von Bild- oder Tonaufzeichnungsgeräten (§54 Abs4 SPG) unter Angabe der für die Ermittlung wesentlichen Gründe in Kenntnis zu setzen. Darüber hinaus ist der Rechtsschutzbeauftragte über Auskunftsverlangen (§53 Abs3a Z2 und 3, Abs3a zweiter Satz und 3b SPG) sowie über den Einsatz von Kennzeichenerkennungsgeräten (§54 Abs4b SPG) zu informieren. Gemäß §91c Abs3 SPG haben Sicherheitsbehörden, wenn beabsichtigt ist, im Rahmen der erweiterten Gefahrenerforschung (§21 Abs3 SPG) besondere Ermittlungsmaßnahmen nach §54 Abs3 und 4 SPG zu setzen, die Ermächtigung des Rechtsschutzbeauftragten im Wege des Bundesministers für Inneres einzuholen. Gemäß §91c Abs2 SPG haben Sicherheitsbehörden, die die Führung einer Datenanwendung gemäß §53a Abs2 SPG beabsichtigen, unverzüglich den Bundesminister für Inneres zu verständigen. Dieser hat dem Rechtsschutzbeauftragten Gelegenheit zur Äußerung binnen drei Tagen zu geben. Nimmt der Rechtsschutzbeauftragte wahr, dass durch Verwenden personenbezogener Daten Rechte von Betroffenen verletzt worden sind, die von dieser Datenverwendung keine Kenntnis haben, so ist er - in (pflichtgemäßer) Erfüllung seiner Aufgabe zur Wahrnehmung des besonderen Rechtsschutzes im Ermittlungsdienst der Sicherheitsbehörden (vgl. §91a Abs1 SPG) - gemäß §91d Abs3 SPG zu deren Information oder, sofern eine solche aus den Gründen des §26 Abs2 des DSG 2000 nicht erfolgen kann, zur Erhebung einer Beschwerde an die Datenschutzkommission nach §90 SPG befugt.

3. Zur Zulässigkeit des Antrags auf Aufhebung von Teilen des §24 DSG 2000:

Der Antrag enthält weder nähere Ausführungen über die Rechtssphäre der Antragsteller, in die §24 DSG 2000 eingreifen solle, noch über die Unmittelbarkeit dieses Eingriffs. Eingriffe werden stets im Zusammenhang mit den angefochtenen Bestimmungen des SPG geltend gemacht. Zum allgemein gehaltenen Vorbringen, die Ausnahmen von der Informationspflicht des §24 DSG 2000 und das Fehlen eines ausreichenden Rechtsschutzes gegen die Ausübung der Befugnisse der Sicherheitsbehörden lösten eine aktuelle und unmittelbare Betroffenheit im Hinblick auf die Verfassungsgarantien der Art8, 10 und 13 EMRK, des §1 DSG 2000 und des Art7 B-VG aus, wird auf die Ausführungen unter Punkt 2. verwiesen.

4. Die Anträge sind daher insgesamt unzulässig und waren daher zurückzuweisen.

Dieser Beschluss konnte gemäß §19 Abs3 Z2 lite VfGG in nichtöffentlicher Sitzung gefasst werden.