Gericht

Verfassungsgerichtshof

Entscheidungsdatum

01.07.2009

Geschäftszahl

G31/08

Sammlungsnummer

18830

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. 1. Die antragstellende Gesellschaft verfügt nach ihren

Angaben über eine Konzession zur Erbringung eines reservierten Fernmeldedienstes im digitalen, zellularen Mobilfunkbereich (GSM und UMTS).

Sie beantragt als Betreiberin öffentlicher Telekommunikationsdienste iSd §92 Abs3 Z1 Telekommunikationsgesetz 2003 - TKG 2003, BGBl. I 70/2003, mit ihrem ersten Hauptantrag die Aufhebung des gesamten Art1 Punkt 4. des Bundesgesetzes, mit dem das Sicherheitspolizeigesetz, das Grenzkontrollgesetz und das Polizeikooperationsgesetz geändert werden, BGBl. I 114/2007, wegen Verfassungswidrigkeit.

In eventu beantragt sie die Aufhebung des gesamten §53 Abs3a des Bundesgesetzes über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz - SPG), BGBl. 566/1991 idF BGBl. I 114/2007 unter Wiederinkrafttreten der davor geltenden Textfassung des §53 Abs3a SPG BGBl. I 158/2005 wegen Verfassungswidrigkeit.

Weiters beantragt sie die Aufhebung des gesamten §53 Abs3b SPG idF BGBl. I 114/2007 (zweiter Hauptantrag) sowie die Aufhebung der Wortfolge "Kommunikations- und" in §53a Abs2 Z1 litn SPG idF BGBl. I 114/2007 (dritter Hauptantrag) wegen Verfassungswidrigkeit.

2.1. Art1 Z4 bis 8 des Bundesgesetzes, mit dem das Sicherheitspolizeigesetz, das Grenzkontrollgesetz und das Polizeikooperationsgesetz geändert werden, BGBl. I 114/2007 lautet:

"4. §53 Abs3a lautet:

'(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.'

5. Der bisherige §53 Abs3b erhält die Absatzbezeichnung '(3c)'.

6. Nach §53 Abs3a wird folgender Abs3b (neu) eingefügt:

'(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.'

7. Der bisherige §53a samt Paragraphenüberschrift wird zu
§53b.

8. §53a (neu) samt Überschrift lautet:

'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.

(3) Zur Evidenthaltung von Wegweisungen, Betretungsverboten und einstweiligen Verfügungen zum Schutz vor Gewalt in der Familie sind die Sicherheitsbehörden ermächtigt, zu Personen, gegen die eine derartige Maßnahme verfügt wurde, Namen, Geburtsdatum und Ort, Geschlecht, Verhältnis zur gefährdeten Person, Staatsangehörigkeit, Wohnanschrift, zu gefährdeten Personen Namen, Geburtsdatum und Ort, Geschlecht, Staatsangehörigkeit, Beziehung zum Gefährder, Wohnanschrift und Erreichbarkeitsdaten sowie Art der Maßnahme, frühere Maßnahmen, Bereich (Anschrift, nähere Beschreibung), auf den sich die Maßnahme bezieht, bestimmte Tatsachen, auf die sich die Maßnahme stützt (insbesondere vorangegangener gefährlicher Angriff), Geltungsdauer der Maßnahme, Verstöße gegen verfügte Maßnahmen, Abgabestelle für Zwecke der Zustellung der Aufhebung des Betretungsverbotes oder einer einstweiligen Verfügung nach §382b EO, und Verwaltungsdaten zu verarbeiten. Die Daten von Opfern sind längstens nach einem Jahr zu löschen. Bei mehreren Speicherungen bestimmt sich die Löschung nach dem Zeitpunkt der letzten Speicherung.

(4) Zur Evidenthaltung von Wegweisungen und Betretungsverboten in Schutzzonen sind die Sicherheitsbehörden ermächtigt, zu Personen, gegen die eine derartige Maßnahme verfügt wurde, Namen, Geburtsdatum und Ort, Geschlecht, Staatsangehörigkeit, Wohnanschrift, sowie Art der Maßnahme, Bereich (Anschrift, nähere Beschreibung), auf den sich die Maßnahme bezieht, bestimmte Tatsachen, auf die sich die Maßnahme stützt (insbesondere vorangegangener gefährlicher Angriff), Geltungsdauer der Maßnahme und Verwaltungsdaten zu verarbeiten.

(5) Soweit wegen eines sprengelübergreifenden Einsatzes eine gemeinsame Verarbeitung durch mehrere Sicherheitsbehörden erforderlich ist, dürfen Datenanwendungen gemäß Abs1 im Informationsverbundsystem geführt werden. Die Daten sind nach Beendigung und Evaluierung des Einsatzes, längstens jedoch nach einem Jahr zu löschen. Übermittlungen der gemäß Abs1 verarbeiteten Daten sind nur zulässig, wenn hierfür eine ausdrückliche gesetzliche Ermächtigung besteht.

(6) Soweit eine gemeinsame Verarbeitung durch mehrere Sicherheitsbehörden erforderlich ist, dürfen Datenanwendungen gemäß Abs2 im Informationsverbundsystem geführt werden. Daten gemäß Abs2 Z1 sind längstens nach drei Jahren, Daten nach Abs2 Z2 und 3 längstens nach einem Jahr, Daten gemäß Abs2 Z4 bei Wegfall der ausreichenden Gründe für die Annahme nach dieser Ziffer, längstens aber nach drei Jahren und

Daten gemäß Abs2 Z5 längstens nach drei Jahren zu löschen. Bei mehreren Speicherungen nach derselben Ziffer bestimmt sich die Löschung nach dem Zeitpunkt der letzten Speicherung. Übermittlungen sind an Sicherheitsbehörden, Staatsanwaltschaften und Gerichte für Zwecke der Strafrechtspflege und im Übrigen nur zulässig, wenn hierfür eine ausdrückliche gesetzliche Ermächtigung besteht.'"

2.2. Für die Beurteilung der Zulässigkeit der Anträge sind noch folgende Bestimmungen des SPG und des Telekommunikationsgesetzes 2003 - TKG 2003, BGBl. I 70, von Bedeutung:

2.2.1. §88 SPG:

"Beschwerden wegen Verletzung subjektiver Rechte

§88. (1) Die unabhängigen Verwaltungssenate erkennen über Beschwerden von Menschen, die behaupten, durch die Ausübung unmittelbarer sicherheitsbehördlicher Befehls- und Zwangsgewalt in ihren Rechten verletzt worden zu sein (Art129a Abs1 Z2 B-VG).

(2) Außerdem erkennen die unabhängigen Verwaltungssenate über Beschwerden von Menschen, die behaupten, auf andere Weise durch die Besorgung der Sicherheitsverwaltung in ihren Rechten verletzt worden zu sein, sofern dies nicht in Form eines Bescheides erfolgt ist.

(3) Beschwerden gemäß Abs1, die sich gegen einen auf dieses Bundesgesetz gestützten Entzug der persönlichen Freiheit richten, können während der Anhaltung bei der Sicherheitsbehörde eingebracht werden, die sie unverzüglich dem unabhängigen Verwaltungssenat zuzuleiten hat.

(4) Über Beschwerden gemäß Abs1 oder 2 entscheidet der unabhängige Verwaltungssenat durch eines seiner Mitglieder. Im übrigen gelten die §§67c bis 67g und 79a AVG."

2.2.2. §50 SPG:

"Unmittelbare Zwangsgewalt

§50. (1) Die Organe des öffentlichen Sicherheitsdienstes sind, sofern nicht anderes bestimmt ist, ermächtigt, die ihnen von diesem Bundesgesetz oder von einer auf Grund dieses Bundesgesetzes erlassenen Verordnung eingeräumten Befugnisse mit unmittelbarer Zwangsgewalt durchzusetzen.

(2) Die Organe des öffentlichen Sicherheitsdienstes haben anwesenden Betroffenen die Ausübung von unmittelbarer Zwangsgewalt anzudrohen und anzukündigen. Hievon kann in den Fällen der Notwehr oder der Beendigung gefährlicher Angriffe (§33) soweit abgesehen werden, als dies für die Verteidigung des angegriffenen Rechtsgutes unerläßlich erscheint.

(3) Für die Anwendung von unmittelbarer Zwangsgewalt gegen Menschen gelten die Bestimmungen des Waffengebrauchsgesetzes 1969.

(4) Die Organe des öffentlichen Sicherheitsdienstes dürfen physische Gewalt gegen Sachen anwenden, wenn dies für die Ausübung einer Befugnis unerläßlich ist. Hiebei haben sie alles daranzusetzen, daß eine Gefährdung von Menschen unterbleibt."

2.2.3. §18 SPG:

"Rechte und Pflichten juristischer Personen

§18. Soweit in diesem Bundesgesetz von Rechten und Pflichten von Menschen die Rede ist, sind darunter auch Rechte und Pflichten juristischer Personen zu verstehen."

2.2.4. §§92 und 93 TKG 2003:

"Allgemeines

§92. (1) Soweit dieses Bundesgesetz nicht anderes bestimmt, sind auf die in diesem Bundesgesetz geregelten Sachverhalte die Bestimmungen des Datenschutzgesetzes 2000, BGBl. I Nr. 165/1999, anzuwenden.

(2) Die Bestimmungen der Strafprozessordnung (StPO), BGBl. Nr. 631/1975, bleiben durch die Bestimmungen dieses Abschnittes unberührt.

(3) In diesem Abschnitt bezeichnet unbeschadet des §3 der Begriff

1. 'Anbieter' Betreiber von öffentlichen Kommunikationsdiensten;

2. 'Benutzer' eine natürliche Person, die einen öffentlichen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst zwangsläufig abonniert zu haben;

3. 'Stammdaten' alle personenbezogenen Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind; dies sind:

   a) Familienname und Vorname,
   b) akademischer Grad,
   c) Wohnadresse,
   d) Teilnehmernummer und sonstige Kontaktinformation für die Nachricht,
   e) Information über Art und Inhalt des Vertragsverhältnisses,
   f) Bonität;

4. 'Verkehrsdaten' Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden;

4a. 'Zugangsdaten' jene Verkehrsdaten, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz beim Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierungen zum Teilnehmer notwendig sind;

5. 'Inhaltsdaten' die Inhalte übertragener Nachrichten (Z7);

6. 'Standortdaten' Daten, die in einem Kommunikationsnetz verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben;

7. 'Nachricht' jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet wird. Dies schließt nicht Informationen ein, die als Teil eines Rundfunkdienstes über ein Kommunikationsnetz an die Öffentlichkeit weitergeleitet werden, soweit die Informationen nicht mit dem identifizierbaren Teilnehmer oder Nutzer, der sie erhält, in Verbindung gebracht werden können;

8. 'Anruf' eine über einen öffentlich zugänglichen Telefondienst aufgebaute Verbindung, die eine zweiseitige Echtzeit-Kommunikation ermöglicht;

9. 'Dienst mit Zusatznutzen' jeden Dienst, der die Bearbeitung von Verkehrsdaten oder anderen Standortdaten als Verkehrsdaten in einem Maße erfordert, das über das für die Übermittlung einer Nachricht oder die Fakturierung dieses Vorgangs erforderliche Maß hinausgeht;

10. 'elektronische Post' jede über ein öffentliches Kommunikationsnetz verschickte Text-, Sprach-, Ton- oder Bildnachricht, die im Netz oder im Endgerät des Empfängers gespeichert werden kann, bis sie von diesem abgerufen wird.

Kommunikationsgeheimnis

§93. (1) Dem Kommunikationsgeheimnis unterliegen die Inhaltsdaten, die Verkehrsdaten und die Standortdaten. Das Kommunikationsgeheimnis erstreckt sich auch auf die Daten erfolgloser Verbindungsversuche.

(2) Zur Wahrung des Kommunikationsgeheimnisses ist jeder Betreiber und alle Personen, die an der Tätigkeit des Betreibers mitwirken, verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(3) Das Mithören, Abhören, Aufzeichnen, Abfangen oder sonstige Überwachen von Nachrichten und der damit verbundenen Verkehrs- und Standortdaten sowie die Weitergabe von Informationen darüber durch andere Personen als einen Benutzer ohne Einwilligung aller beteiligten Benutzer ist unzulässig. Dies gilt nicht für die Aufzeichnung und Rückverfolgung von Telefongesprächen im Rahmen der Entgegennahme von Notrufen und die Fälle der Fangschaltung sowie für eine technische Speicherung, die für die Weiterleitung einer Nachricht erforderlich ist.

(4) Werden mittels einer Funkanlage, einer Telekommunikationsendeinrichtung oder mittels einer sonstigen technischen Einrichtung Nachrichten unbeabsichtigt empfangen, die für diese Funkanlage, diese Telekommunikationsendeinrichtung oder den Anwender der sonstigen Einrichtung nicht bestimmt sind, so dürfen der Inhalt der Nachrichten sowie die Tatsache ihres Empfanges weder aufgezeichnet noch Unbefugten mitgeteilt oder für irgendwelche Zwecke verwertet werden. Aufgezeichnete Nachrichten sind zu löschen oder auf andere Art zu vernichten."

2.2.5. §§97 - 99 TKG 2003:

"Stammdaten

§97. (1) Stammdaten dürfen unbeschadet der §§90 Abs6 und 96 Abs2 von Betreibern nur für folgende Zwecke ermittelt und verarbeitet werden:

1. Abschluss, Durchführung, Änderung oder Beendigung des Vertrages mit dem Teilnehmer;

2. Verrechnung der Entgelte;

3. Erstellung von Teilnehmerverzeichnissen, auch gemäß §18 und

4. Erteilung von Auskünften an Notrufträger.

(2) Stammdaten sind spätestens nach Beendigung der vertraglichen Beziehungen mit dem Teilnehmer vom Betreiber zu löschen. Ausnahmen sind nur soweit zulässig, als diese Daten noch benötigt werden, um Entgelte zu verrechnen oder einzubringen, Beschwerden zu bearbeiten oder sonstige gesetzliche Verpflichtungen zu erfüllen.

Auskünfte an Betreiber von Notrufdiensten

§98. Betreiber haben Betreibern von Notrufdiensten [Anm:
derzeit sind das die einheitliche europäische Notrufnummer 112, Feuerwehr 122, Notrufnummer bei Gasgebrechen 128, Polizei 133, Bergrettung 140, Ärztenotdienst 141, Telefonseelsorge 142, Rettungsdienst 144 und Notrufdienst für Kinder und Jugendliche 147 - vgl. §17 der Kommunikationsparameter-, Entgelt- und Mehrwertdiensteverordnung (KEM V) der RTR-GmbH] auf deren Verlangen Auskünfte über Stammdaten im Sinne von §92 Abs3 Z3 lita bis d sowie über Standortdaten im Sinne des §92 Abs3 Z6 zu erteilen. In beiden Fällen ist Voraussetzung für die Zulässigkeit der Übermittlung ein Notfall, der nur durch Bekanntgabe dieser Informationen abgewehrt werden kann. Die Notwendigkeit der Informationsübermittlung ist vom Betreiber des Notrufdienstes zu dokumentieren und dem Betreiber unverzüglich, spätestens jedoch innerhalb von 24 Stunden nachzureichen. Der Betreiber darf die Übermittlung nicht von der vorherigen Darlegung der Notwendigkeit abhängig machen. Den Betreiber des Notrufdienstes trifft die Verantwortung für die rechtliche Zulässigkeit des Auskunftsbegehrens.

Verkehrsdaten

§99. (1) Verkehrsdaten dürfen außer in den gesetzlich geregelten Fällen nicht gespeichert werden und sind vom Betreiber nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren.

(2) Sofern dies für Zwecke der Verrechnung von Entgelten, einschließlich der Entgelte für Zusammenschaltungen, erforderlich ist, hat der Betreiber Verkehrsdaten bis zum Ablauf jener Frist zu speichern, innerhalb derer die Rechnung rechtlich angefochten werden oder der Anspruch auf Zahlung geltend gemacht

werden kann. Diese Daten sind im Streitfall der entscheidenden Einrichtung sowie der Schlichtungsstelle unverkürzt zur Verfügung zu stellen. Wird ein Verfahren über die Höhe der Entgelte eingeleitet, dürfen die Daten bis zur endgültigen Entscheidung über die Höhe der Entgelte nicht gelöscht werden. Der Umfang der gespeicherten Verkehrsdaten ist auf das unbedingt notwendige Minimum zu beschränken.

(3) Die Verarbeitung von Verkehrsdaten darf nur durch solche Personen erfolgen, die für die Entgeltverrechnung oder Verkehrsabwicklung, Behebung von Störungen, Kundenanfragen, Betrugsermittlung oder Vermarktung der Kommunikationsdienste oder für die Bereitstellung von Diensten mit Zusatznutzen zuständig sind oder die von diesen Personen beauftragt wurden. Der Umfang der verwendeten Verkehrsdaten ist auf das unbedingt notwendige Minimum zu beschränken.

(4) Dem Betreiber ist es außer in den gesetzlich besonders geregelten Fällen untersagt, einen Teilnehmeranschluss über die Zwecke der Verrechnung hinaus nach den von diesem Anschluss aus angerufenen Teilnehmernummern auszuwerten. Mit Zustimmung des Teilnehmers darf der Betreiber die Daten zur Vermarktung für Zwecke der eigenen Telekommunikationsdienste oder für die Bereitstellung von Diensten mit Zusatznutzen verwenden."

2.2.6. §102 TKG 2003:

"§102. (1) Andere Standortdaten als Verkehrsdaten dürfen unbeschadet des §98 nur verarbeitet werden, wenn sie

1. anonymisiert werden oder

2. die Benutzer oder Teilnehmer eine jederzeit widerrufbare Einwilligung gegeben haben.

(2) Selbst im Falle einer Einwilligung zur Verarbeitung von Daten gemäß Abs1 müssen die Benutzer oder Teilnehmer die Möglichkeit haben, diese Verarbeitung von Daten für jede Übertragung einfach und kostenlos zeitweise zu untersagen.

(3) Die Verarbeitung anderer Standortdaten als Verkehrsdaten gemäß Abs1 und 2 muss auf das für die Bereitstellung des Dienstes mit Zusatznutzen erforderliche Maß sowie auf Personen beschränkt werden, die im Auftrag des Betreibers oder des Dritten, der den Dienst mit Zusatznutzen anbietet, handeln."

2.3. §7 Z4 der Überwachungskostenverordnung - ÜKVO, BGBl. II 322/2004 lautet:

"§7. Die Kosten einer Standortbestimmung betragen

...

4. für eine Ermittlung aktueller Standortdaten

```
a) Einrichtung pro Rufnummer ..................... Euro 37,00
b) Auswertung und Versand pro Abfrage ohne
   Plandarstellung/Landkarte ..................... Euro 16,00
c) Plandarstellung/Landkarte pro Abfrage ........ Euro 16,00"
```

3. Zur Antragslegitimation führt die antragstellende Gesellschaft aus:

Sie sei Diensteanbieterin im Sinne des §92 Abs3 Z1 TKG 2003. Sie sei daher gemäß §53 Abs3a SPG verpflichtet, Behörden die Internetprotokolladresse (IP-Adresse) einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung sowie Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, wenn bestimmte Tatsachen die Annahme einer konkreten Gefahrensituation rechtfertigen, mitzuteilen. Um dieser Mitteilungspflicht nachkommen zu können, müsste die antragstellende Gesellschaft die IP-Adressen zunächst überhaupt erst einmal speichern. Bislang speichere die antragstellende Gesellschaft die IP-Adressen allerdings noch nicht, weil sie diese zur Erbringung ihrer Dienstleistungen nicht benötige und für eine Speicherung keine Rechtsgrundlage existiere, sondern diese gegen das Kommunikationsgeheimnis des §93 TKG 2003 sowie das Fernmeldegeheimnis des Art10a StGG verstoßen würde. §53 Abs3a Z2 SPG enthalte somit eine implizite Speicherpflicht. Dies sei ein offensichtlicher Vorgriff auf die in Österreich noch umzusetzende Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher

Kommunikationsnetze erzeugt oder verarbeitet werden, ABl. 2006 L 105, S. 54. Da §53 Abs3a Z2 SPG nicht unterscheide, ob eine bestimmte Nachricht von einem Kunden des Netzbetreibers gesendet oder empfangen wurde, müssten sämtliche IP-Pakete (Nachricht plus IP-Adresse), die in einem bestimmten Zeitraum anfallen, - egal ob gesendet oder empfangen - gespeichert werden, ergänzt um einen Zeitstempel. Auf einen Zeitraum von 6 Monaten hochgerechnet würde das dabei anfallende Datenvolumen mindestens 685 Terabyte betragen.

Weiters sei die antragstellende Gesellschaft gemäß §53 Abs3b SPG verpflichtet, über Standortdaten Auskunft zu erteilen, was "im Falle nicht geführter Gespräche" nur durch Verarbeitung gesonderter Verbindungsdaten, die durch Zuhilfenahme der Verbindungswege nach Beauftragung durch den Betreiber individuell herzustellen seien, erfolgen könne. Dies stehe gemäß §§134 ff StPO unter Vorbehalt der Anordnung durch die Staatsanwaltschaft nach richterlicher Bewilligung. Überdies sehe diese Bestimmung den Einsatz eines IMSI-Catchers vor, der es der antragstellenden Gesellschaft unmöglich mache, die ihr nach §93 Abs2 TKG 2003 gesetzlich obliegende Pflicht zur Wahrung des Kommunikationsgeheimnisses sowie die gemäß §20 TKG 2003 bestehende Verpflichtung zur Herstellung der Verbindung zu Notrufnummern zu erfüllen und der sie daran hindere, die in ihrer Mobilfunkkonzession vorgeschriebene Netzverfügbarkeit zu garantieren.

Zwar enthalte ein Formblatt, das für die konkreten Anfragen zu §53 Abs3a und 3b SPG von den Sicherheitsbehörden entworfen worden sei, den Hinweis, dass die Sicherheitsbehörden "die Verantwortung für die rechtliche Zulässigkeit des Auskunftsbegehrens trifft". Tatsächlich führe dies aber zu keiner Haftungsbefreiung der antragstellenden Gesellschaft gegenüber ihren Kunden für unzulässige Auskünfte nach §53 Abs3a und 3b SPG. "Willkürliche" Auskunftsbegehren, die die Sicherheitsbehörden unter vermeintlicher Übernahme der Haftung stellen, könnten die antragstellende Gesellschaft somit direkt in eine Haftung gegenüber ihren Kunden bringen (Schadenersatzforderungen, Unterlassungsklagen), womit die antragstellende Gesellschaft durch §53 Abs3a und 3b SPG in ihrer Rechtssphäre (Eigentumsfreiheit, Erwerbsfreiheit) unmittelbar betroffen sei.

Die angefochtenen Bestimmungen würden unmittelbar und aktuell - also ohne Fällung eines gerichtlichen Urteils oder Erlassung eines Bescheids - in die (Verfassungs-)Rechtssphäre der antragstellenden Gesellschaft eingreifen, nämlich in das Grundrecht auf Freiheit des Eigentums und der Erwerbsfreiheit, den Gleichheitsgrundsatz, das Datengeheimnis, Art8 Abs2 EMRK, das Fernmeldegeheimnis und das Kommunikationsgeheimnis. Die antragstellende Gesellschaft erhalte seit dem In-Kraft-Treten der bekämpften Bestimmungen am 1. Jänner 2008 laufend Anfragen von Polizeidienststellen.

Da der antragstellenden Gesellschaft kein anderer zumutbarer Weg zur Verfügung stehe, sich gegen die angefochtenen Bestimmungen zur Wehr zu setzen, sei sie antragslegitimiert.

4. Die Bundesregierung bestreitet die Legitimation der antragstellenden Gesellschaft mit folgenden Argumenten:

Der erste Hauptantrag sei auf die Aufhebung der Novellierungsanordnung des ArtI Z4 des Bundesgesetzes BGBl. I 114/2007 gerichtet. Die Anfechtung einer bloßen Novellierungsanordnung - an Stelle der novellierten Gesetzesstelle in der Fassung der Novelle - sei nur dann zulässig, wenn eine Bestimmung durch eine Novelle aufgehoben worden ist und sich das Bedenken (etwa auf Grund des Fehlens von Ausnahmen oder Übergangsbestimmungen) gegen diese Aufhebung richtet, sodass die behauptete Verfassungswidrigkeit anders nicht beseitigt werden könnte (VfSlg. 16.588/2002, 16.764/2002). Vor diesem Hintergrund erweise sich der erste Hauptantrag als unzulässig.

Die Bundesregierung bestreitet auch die Legitimation zur Anfechtung des gesamten §53 Abs3a SPG idF BGBl. I 114/2007 (Eventualantrag) mit folgender Argumentation:

Bereits aus dem Antragsvorbringen sei erschließbar, dass die angefochtenen Bestimmungen selbst keine direkte Wirksamkeit entfalten. Die in den angefochtenen Bestimmungen statuierten Verpflichtungen zur Erteilung bestimmter Auskünfte über dort näher normierte Daten seien nicht bereits mit In-Kraft-Treten der Novelle BGBl. I 114/2007 für die antragstellende Gesellschaft direkt wirksam; vielmehr bedürfe es für die Aktualisierung der konkreten Verpflichtung zur Erteilung der normierten Auskünfte des Dazwischentretens eines diesem unmittelbar vorangehenden und konkretisierenden Auskunftsverlangens der Sicherheitsbehörden. In ihrem Vorbringen beziehe sich die antragstellende Gesellschaft selbst auf solche Auskunftsverlangen.

Die antragstellende Gesellschaft moniere, sie sei auf Grund des §53 Abs3a SPG verpflichtet, die dort genannten Daten zu speichern, um bei entsprechendem Verlangen solche Auskünfte erteilen zu können. Dem sei entgegenzuhalten, dass diese Bestimmung die Sicherheitsbehörden ermächtige, ein Auskunftsverlangen zu bestimmten taxativ aufgezählten Daten, die von der antragstellenden Gesellschaft als Betreiberin öffentlicher

Telekommunikationsdienste verarbeitet wurden, zu stellen. Eine Verpflichtung zur Speicherung von Daten, sei es der Name, die Anschrift oder die Teilnehmernummer eines bestimmten Teilnehmers (Z1) oder die IP-Adresse zu einer bestimmten Nachricht (Z2) oder Name und Anschrift eines Benutzers (Z3), ergebe sich hingegen nicht daraus.

Die Erteilung der Auskunft sei auf diejenigen Daten beschränkt, die die antragstellende Gesellschaft auf der Grundlage anderer (gesetzlicher) Verpflichtungen verarbeitet hat, wie zB zu Verrechnungszwecken nach §97 TKG 2003. Der Auskunftsverpflichtung könne nur in dem Maße nachgekommen werden, als die angefragten Daten auch tatsächlich zur Verfügung stünden. Insofern würden den Betreibern öffentlicher Telekommunikationsdienste oder sonstigen Diensteanbietern keine zusätzlichen Speicherverpflichtungen aufgrund von §53 Abs3a SPG auferlegt, die nicht auch schon vor dessen In-Kraft-Treten bestanden.

Auch hinsichtlich des §53 Abs3b SPG (zweiter Hauptantrag) sei nicht ersichtlich, inwieweit dieser die Rechtssphäre der antragstellenden Gesellschaft aktuell beeinträchtigt. Dabei handle es sich um eine Pflicht zur Auskunftserteilung, konkret zur Auskunft über Standortdaten und die internationale Mobilteilnehmerkennung der von einem in Gefahr befindlichen Menschen mitgeführten Endeinrichtung. Die Standortdaten seien regelmäßig bei Betreibern öffentlicher Telekommunikationsdienste vorhanden und schon auf Grund der bestehenden Rechtslage etwa bei Notrufen gemäß §98 TKG 2003 zu beauskunften; es entstehe durch diese Bestimmung des SPG keine wie immer geartete Verpflichtung, Daten gesondert zu speichern.

Die antragstellende Gesellschaft begründe ihre rechtliche Betroffenheit durch §53 Abs3a und 3b SPG auch mit allfälligen Haftungen gegenüber ihren Kunden. Hinsichtlich Abs3b leg.cit. werde zunächst angemerkt, dass die Sicherheitsbehörden ebenso wie die Notrufdienste nach §98 TKG 2003 die Verantwortung für die rechtliche Zulässigkeit des Auskunftsbegehrens treffe. Für den Fall einer unrechtmäßigen Anfrage treffe die Sicherheitsbehörde bis zu allfälligen Amtshaftungsansprüchen die Verantwortung. Abgesehen davon könnten die monierten zivilrechtlichen Haftungen der antragstellenden Gesellschaft gegenüber ihren Kunden lediglich einen potentiellen Eingriff in die rechtlich geschützten Interessen der antragstellenden Gesellschaft dartun, nicht jedoch die von Art140 B-VG geforderte aktuelle Beeinträchtigung.

Schließlich moniere die antragstellende Gesellschaft, ihr stünde kein anderer zumutbarer Weg offen, sich gegen "die

Novellierung der genannten Bestimmungen ... zur Wehr zu setzen". Dem

hält die Bundesregierung entgegen, dass §88 SPG einen Rechtsschutzweg eröffne. Der antragstellenden Gesellschaft wäre es möglich und auch zumutbar, dort die vermeintliche Rechtswidrigkeit des Auskunftsverlangens und in weiterer Folge die Bedenken, die nach ihrer Ansicht gegen die Verfassungsmäßigkeit der angefochtenen Normen sprechen, vorzubringen und geltend zu machen.

Im Übrigen weist die Bundesregierung darauf hin, dass die antragstellende Gesellschaft nicht dartut, inwieweit durch die mit Drittantrag angefochtene Wortfolge "Kommunikations- und" in §53a Abs2 Z1 litn SPG in ihre Rechtssphäre unmittelbar und aktuell eingegriffen wird. Da der Antrag keine Ausführungen zur Legitimation zum dritten Hauptantrag enthalte, sei er zurückzuweisen.

Schließlich bringt die Bundesregierung vor, dass der Antrag dem Erfordernis der Darlegung der gegen die Verfassungsmäßigkeit des Gesetzes sprechenden Bedenken im Einzelnen an mehreren Stellen nicht entspreche.

5. Der Verfassungsgerichtshof richtete an den Bundesminister für Inneres folgende Fragen, die dieser wie im Folgenden kursiv wiedergegeben beantwortete:

"Frage 1: Welche technischen Mittel werden zur Lokalisierung von Endeinrichtungen iSd §53 Abs3b SPG eingesetzt?

Zur Lokalisierung von Mobilfunkendeinrichtungen iSd §53 Abs3b SPG wird von der Sicherheitsbehörde das unter der Bezeichnung 'IMSI-Catcher' bekannte technische Einsatzmittel im Zusammenwirken mit geeigneten Peilempfängern/-antennen eingesetzt.

Frage 2: Kann mit den zu diesem Zweck eingesetzten technischen Mitteln tatsächlich nur der Standort der 'Endeinrichtung' oder können auch Inhalte von Gesprächen und anderen Datenübermittlungen mit diesen Endeinrichtungen ermittelt werden?

Aufgrund der technischen Beschaffenheit des der Sondereinheit für Observation (SEO) für diesen Zweck zur Verfügung stehenden Einsatzmittels ist ein 'Ermitteln' von Gesprächsinhalten oder anderen Datenübermittlungen nicht möglich.

Frage 3: Gibt es Vorkehrungen, um sicherzustellen, dass in Fällen, in denen von der Berechtigung gemäß §53 Abs3b SPG Gebrauch gemacht wird, tatsächlich nur der Standort der Endeinrichtung des gefährdeten Menschen und nicht auch von unbeteiligten Dritten ermittelt wird?

Durch den Einsatz spezieller Software des IMSI-Catchers wird sichergestellt, dass dem Bediener des technischen Einsatzmittels bei Messungen ausschließlich die gerätespezifische Nummer der zu lokalisierenden Mobilfunkendeinrichtung eines gefährdeten Menschen angezeigt wird.

Frage 4: Kann es im Zusammenhang mit dem Einsatz dieser technischen Mittel zu Beeinträchtigungen des Betriebes von Mobilfunknetzen kommen? Sind bisher solche Beeinträchtigungen aufgetreten?

Bei einer Verwendung des technischen Einsatzmittels durch geschultes und qualifiziertes Fachpersonal der SEO, das über ausgezeichnete Kenntnisse in Bezug auf den Aufbau und die Funktionsweise der Mobilfunknetzstruktur sowie über entsprechende Erfahrungen im Umgang und der Arbeitsweise des eingesetzten technischen Mittels verfügt, ist eine Beeinträchtigung des Mobilfunknetzes auszuschließen. Die SEO kann auf eine zehnjährige Erfahrung beim Einsatz des IMSI-Catchers zurückblicken. Innerhalb dieses Zeitraumes sind bis dato keine Beeinträchtigungen evident."

II. Der Verfassungsgerichtshof hat zur Zulässigkeit des Antrags 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. Mit dem ersten Hauptantrag begehrt die antragstellende Gesellschaft, Art1 Z4 des Bundesgesetzes BGBl. I 114/2007 als verfassungswidrig aufzuheben. Mit dieser Novellierungsanordnung wurde §53 Abs3a SPG neu gefasst. Eine solche Novellierungsanordnung greift selbst nicht unmittelbar in die Rechtssphäre eines Normadressaten ein; ein Eingriff könnte sich nur aus der Gesetzesstelle selbst in ihrer novellierten Fassung ergeben (vgl. VfSlg. 17.363/2004, 18.285/2007 und VfGH 24.9.2008, G44/07 ua.). Insoweit ist der Antrag schon aus diesem Grund unzulässig.

Mit ihrem Eventualantrag bekämpft die antragstellende Gesellschaft §53 Abs3a SPG idF BGBl. I 114/2007. Die antragstellende Gesellschaft bringt zunächst vor, sie müsse, um der Auskunftspflicht gemäß §53 Abs3a SPG bezüglich der Internetprotokolladressen nachkommen zu können, die IP-Adressen zunächst überhaupt erst einmal speichern. Bislang speichere die antragstellende Gesellschaft die IP-Adressen noch nicht, weil sie diese zur Erbringung ihrer Dienstleistung nicht benötige und weil für eine derartige Speicherung keine Rechtsgrundlage existiere.

Die Bundesregierung hält dieser Argumentation entgegen, dass sich aus §53 Abs3a Z2 SPG keine Verpflichtung ergebe, die Internetprotokolladressen zu speichern; mit der Neuregelung des §53 Abs3a Z2 und Z3 SPG habe der Gesetzgeber lediglich auf die Entscheidung der Datenschutzkommission vom 3. Oktober 2007, K121.279/0017-DSK/2007 reagiert, in der diese die Ansicht vertrat, dass "für die Übermittlung der (dynamischen) IP-Adresse, die unzweifelhaft ein Verkehrsdatum darstellt, auf Basis eines 'nickname'

... §53 Abs3a SPG [idF vor der Novelle BGBl. I 117/2008] keine geeignete Grundlage bieten" könne.

Der Verfassungsgerichtshof vertritt dazu die folgende Auffassung: Mit der Novellierung des §53 Abs3a SPG wurde zwar eine gesetzliche Grundlage für die Übermittlung der IP-Adresse an die Sicherheitsbehörden, aber keine neue Verpflichtung zur Speicherung von IP-Adressen geschaffen: Gemäß der - durch die genannte SPG-Novelle unberührt gebliebenen - Regelung des §99 Abs1 TKG 2003 dürfen nämlich Verkehrsdaten außer in den gesetzlich geregelten Fällen nicht gespeichert werden und sind diese Daten vom Betreiber nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren. Gemäß §99 Abs2 TKG 2003 dürfen Verkehrsdaten für Zwecke der Verrechnung von Entgelten bis zum Ablauf jener Frist gespeichert werden, innerhalb derer die Rechnung rechtlich angefochten werden oder der Anspruch auf Zahlung geltend gemacht werden kann. Gemäß §99 Abs3 TKG 2003 dürfen Verkehrsdaten nur durch solche Personen verarbeitet werden, die für die Entgeltverrechnung oder Verkehrsabwicklung, Behebung von Störungen, Kundenanfragen, Betrugsermittlung oder Vermarktung der Kommunikationsdienste oder für die Bereitstellung von Diensten mit Zusatznutzen zuständig sind oder die von diesen Personen beauftragt wurden. Der Umfang der verwendeten Verkehrsdaten ist auf das unbedingt notwendige Minimum zu beschränken. Nach diesen Bestimmungen kann es zu einer Speicherung der IP-Adresse beispielsweise zum Zwecke der Verrechnung von Entgelten oder zur Behebung von Störungen (Lösung von Internet-Verbindungsproblemen) kommen. Das SPG idF der Novelle BGBl. I 114/2007 enthält hingegen keine Ermächtigung zur Speicherung von Verkehrsdaten. Somit ist davon auszugehen, dass durch die SPG-Novelle den Betreibern von Telekommunikationsdiensten keine weiter reichenden Speicherverpflichtungen auferlegt wurden, als sie schon bisher bestanden haben. Die hier bekämpften Bestimmungen schaffen Auskunftsverpflichtungen; aus solchen Auskunftsverpflichtungen können jedoch keine zusätzlichen Speicherverpflichtungen abgeleitet werden, sodass diese Auskunftsverpflichtungen nur solche Daten betreffen können, hinsichtlich derer bereits aufgrund der genannten - durch die SPG-Novelle unverändert gebliebenen - Bestimmungen des TKG 2003 die Ermächtigung der Betreiber von Telekommunikationsdiensten zur Speicherung besteht.

Da §53 Abs3a SPG somit keine Verpflichtung zur Speicherung der IP-Adresse vorsieht, liegen die von der antragstellenden Gesellschaft behaupteten Eingriffe in ihre rechtlich geschützten Interessen infolge der Verpflichtung zur zusätzlichen Speicherung von Daten im Ausmaß von 685 Terabyte nicht vor.

Hingegen greifen die Auskunftsverpflichtungen der antragstellenden Gesellschaft gemäß §53 Abs3a SPG in ihre rechtlich geschützten Interessen aktuell ein.

Die Bundesregierung bringt vor, dass §88 SPG einen Rechtsschutzweg eröffne. Der antragstellenden Gesellschaft wäre es möglich und auch zumutbar, dort die vermeintliche "Rechtswidrigkeit des Auskunftsverlangens" und in weiterer Folge die Bedenken, die nach ihrer Ansicht gegen die Verfassungsmäßigkeit der angefochtenen Normen sprechen, vorzubringen und geltend zu machen.

Gemäß §88 Abs1 SPG erkennen die unabhängigen Verwaltungssenate über Beschwerden von Menschen (wobei darunter gemäß §18 SPG auch juristische Personen zu verstehen sind), die behaupten, durch die Ausübung unmittelbarer sicherheitsbehördlicher Befehls- und Zwangsgewalt in ihren Rechten verletzt worden zu sein (Art129a Abs1 Z2 B-VG). Gemäß §88 Abs2 SPG erkennen die unabhängigen Verwaltungssenate über Beschwerden von Menschen, die behaupten, auf andere Weise durch die Besorgung der Sicherheitsverwaltung in ihren Rechten verletzt worden zu sein, sofern dies nicht in Form eines Bescheides erfolgt ist. Soweit ein Auskunftsverlangen als Akt der Ausübung unmittelbarer sicherheitsbehördlicher Befehls- und Zwangsgewalt zu qualifizieren wäre, ist es gemäß §88 Abs1 SPG bekämpfbar; erfolgt es in anderer Weise, kann der zur Auskunft Verpflichtete eine Beschwerde gemäß §88 Abs2 SPG erheben.

Da somit der antragstellenden Gesellschaft, wenn von ihr als Betreiberin eines öffentlichen Telekommunikationsdienstes tatsächlich eine Auskunft iSd §53 Abs3a SPG verlangt wird, über eine Beschwerde gemäß §88 Abs1 bzw. 2 SPG und über eine Beschwerde gemäß Art144 B-VG gegen die Entscheidung des UVS ein anderer zumutbarer Weg zur Verfügung steht, die Frage der Verfassungsmäßigkeit des §53 Abs3a SPG an den Verfassungsgerichtshof heranzutragen, erweist sich auch der - in eventu gestellte - Individualantrag auf Aufhebung dieser Bestimmung als unzulässig. Er war daher zurückzuweisen.

3. Betreffend den zweiten Hauptantrag behauptet die antragstellende Gesellschaft, sie sei nach §53 Abs3b SPG verpflichtet, Auskunft über Standortdaten zu erteilen, was "im Falle nicht geführter Gespräche" nur durch Verarbeitung gesonderter Verbindungsdaten, die durch Zuhilfenahme der Verbindungswege nach Beauftragung durch den Betreiber individuell herzustellen seien, erfolgen könne. Dies stehe gemäß §134 ff StPO unter Vorbehalt der Anordnung durch die Staatsanwaltschaft nach richterlicher Bewilligung. Überdies sehe diese Bestimmung den Einsatz eines IMSI (International Mobile Subscriber Identity)-Catchers vor, der es der

antragstellenden Gesellschaft unmöglich mache, die ihr nach §93 Abs2 TKG 2003 gesetzlich obliegende Pflicht zur Wahrung des Kommunikationsgeheimnisses sowie die gemäß §20 TKG 2003 bestehende Verpflichtung zur Herstellung der Verbindung zu Notrufnummern zu erfüllen und der sie daran hindere, die in ihrer Mobilfunkkonzession vorgeschriebene Netzverfügbarkeit zu garantieren.

Dazu vertritt der Verfassungsgerichtshof folgende Auffassung:

§53 Abs3b SPG verpflichtet zunächst Betreiber öffentlicher Telekommunikationsdienste, Auskunft über Standortdaten und die internationale Mobilteilnehmerkennung (IMSI) der von dem gefährdeten Menschen mitgeführten Endeinrichtung (Mobiltelefon) zu erteilen.

Standortdaten sind gemäß §92 Abs2 Z6 TKG 2003 Daten, die in einem Kommunikationsnetz verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben. Gemäß §96 Abs1 TKG 2003 dürfen Standortdaten nur für Zwecke der Besorgung eines Kommunikationsdienstes ermittelt oder verarbeitet werden. Standortdaten unterliegen gemäß §93 Abs1 TKG 2003 dem Kommunikationsgeheimnis. §98 TKG 2003 verpflichtet Betreiber öffentlicher Kommunikationsdienste, Betreibern von Notrufdiensten auf deren Verlangen Auskünfte über Standortdaten zu erteilen. Für den Verfassungsgerichtshof ist daher nicht erkennbar, dass §53 Abs3b SPG die antragstellende Gesellschaft zur Speicherung zusätzlicher Daten verpflichtet.

Gemäß §53 Abs3b letzter Satz SPG sind die Auskünfte gegen Ersatz der Kosten zu erteilen.

Soweit die antragstellende Gesellschaft behauptet, die Kostenersatzregelung entspreche "weder dem Legalitätsprinzip des Art18 Abs1 B-VG noch dem allgemeinen Sachlichkeitsgebot", ist darauf hinzuweisen, dass die Frage der Verfassungsmäßigkeit der Kostenersatzregelung über einen Antrag auf Kostenbestimmung durch Bescheid, dagegen gerichtete Rechtsmittel und schließlich über eine Beschwerde gemäß Art144 Abs1 B-VG an den Verfassungsgerichtshof herangetragen werden kann. Überdies steht der antragstellenden Gesellschaft über eine Beschwerde gemäß §88 Abs1 bzw. 2 SPG und über eine Beschwerde gemäß Art144 B-VG gegen die Entscheidung des UVS ein anderer zumutbarer Weg zur Verfügung, die Frage der Verfassungsmäßigkeit auch des §53 Abs3b SPG an den Verfassungsgerichtshof heranzutragen, was die dort enthaltene Verpflichtung zur Auskunftserteilung betrifft (vgl. oben Pkt. 2.).

§53 Abs3b SPG ermächtigt außerdem die Sicherheitsbehörden, technische Mittel zur Lokalisierung der Endeinrichtung zum Einsatz zu bringen. Auf die Klärung der Frage, welche "technischen Mittel" der Gesetzgeber hier anspricht, zielten die oben in Punkt I.5. wiedergegebenen Fragen an den Bundesminister für Inneres ab. Aus den - den übrigen mitbeteiligten Parteien zur Kenntnisnahme übermittelten und unwidersprochen gebliebenen - Antworten des Bundesministers für Inneres geht hervor, dass hier sog. "IMSI-Catcher" und "Peilempfänger/-antennen" zum Einsatz kommen, die nicht zur Ermittlung von Gesprächsinhalten geeignet sind, sondern nur zur Standortermittlung von Mobilfunkendeinrichtungen, wobei nur die zu lokalisierende Mobilfunkendeinrichtung und nicht auch solche unbeteiligter Dritter angezeigt werden; überdies würden diese "technischen Mittel" bei fachgerechter Bedienung den Betrieb von Mobilfunknetzen nicht stören. Der Verfassungsgerichtshof geht davon aus, dass §53 Abs3b SPG - verfassungskonform interpretiert - auch nur den Einsatz solcher Einrichtungen zulässt, deren Funktionen auf die Ermittlung des Standorts der gesuchten Mobilfunkendeinrichtung beschränkt sind, weil sie das gelindeste Mittel zur Erreichung des vom Gesetz verfolgten Zwecks darstellen.

Wenn die antragstellende Gesellschaft behauptet, der durch §53 Abs3b SPG erlaubte Einsatz technischer Mittel zur Lokalisierung von Telekommunikationsendeinrichtungen (Mobiltelefonen) führe einerseits dazu, dass sie daran gehindert werde, die in ihrer Mobilfunkkonzession vorgeschriebene Netzverfügbarkeit zu garantieren, und andererseits dazu, dass es ihr unmöglich gemacht werde, das Kommunikationsgeheimnis zu wahren (gemeint offenbar: da die Sicherheitsbehörden über solche technische Einrichtungen auch den Inhalt von Telefongesprächen ermitteln könnten), so ist ihr Folgendes entgegenzuhalten:

Die bekämpfte Norm richtet sich nicht an die Betreiber von Telekommunikationsdiensten, sondern an die Sicherheitsbehörden. Die Ermächtigung der Sicherheitsbehörden, technische Mittel zur Lokalisierung der Endeinrichtung zum Einsatz zu bringen, bewirkt daher keinen Eingriff in die rechtlich geschützten Interessen der antragstellenden Gesellschaft, zumal §53 Abs3b SPG keine Grundlage für die Ermittlung von Inhaltsdaten von Mobiltelefongesprächen bietet und insofern die Rechtssphäre des Telekommunikationsdienstebetreibers, der zur Wahrung des Kommunikationsgeheimnisses verpflichtet ist, nicht berührt. Eine allfällige Beeinträchtigung der Verpflichtungen der antragstellenden Gesellschaft aus ihrer Mobilfunkkonzession, die Netzverfügbarkeit zu garantieren, ist aber kein Eingriff in eine Rechtsposition; vielmehr wäre eine allfällige Störung des

Mobilfunkbetriebs durch den Einsatz eines IMSI-Catchers bloß eine faktische Reflexwirkung (vgl. VfSlg. 16.364/2001) der bekämpften Bestimmungen des SPG.

Was schließlich die Behauptung einer allfälligen Haftung der antragstellenden Gesellschaft gegenüber ihren Kunden betrifft, ist darauf hinzuweisen, dass allfällige zivilrechtliche Haftungen der antragstellenden Gesellschaft gegenüber ihren Kunden keine aktuelle Beeinträchtigung ihrer rechtlich geschützten Interessen, sondern bloß eine potentielle Beeinträchtigung dieser Interessen darstellt (vgl. VfSlg. 17.093/2003). Es ist derzeit nämlich ungewiss, ob gegenüber der antragstellenden Gesellschaft jemals Haftungsansprüche geltend gemacht werden. Wie der Verfassungsgerichtshof in ständiger Judikatur ausgesprochen hat, reicht die bloß potentielle Beeinträchtigung von rechtlich geschützten Interessen nicht aus, um die Antragslegitimation nach Art140 B-VG zu begründen.

Selbst wenn aber eine solche Klage gegen die antragstellende Gesellschaft eingebracht werden sollte, würde ihr dann der Weg offen stehen, ihre Bedenken gegen die angefochtenen Bestimmungen dem ordentlichen Gericht vorzutragen, und es könnten die Rechtsmittelgerichte einen Gesetzesprüfungsantrag beim Verfassungsgerichtshof stellen. Ein solcher Weg ist den Antragstellern auch zumutbar: Der Verfassungsgerichtshof hat zwar wiederholt ausgesprochen, dass einem Normunterworfenen nicht zumutbar sei, eine Klage und ein in der Folge eingeleitetes zivilgerichtliches Verfahren dadurch zu provozieren, dass er sich rechtswidrig verhält (VfSlg. 13.659/1993, 15.030/1997, 16.042/2000, 16.920/2003, 17.093/2003). Die antragstellende Gesellschaft müsste sich jedoch gerade nicht rechtswidrig, sondern dem §53 Abs3a bzw. 3b SPG entsprechend verhalten, um in einem allfälligen Haftungsprozess Bedenken gegen diese Bestimmungen vorzutragen.

Aus diesen Gründen ist auch der Individualantrag auf Aufhebung des §53 Abs3b SPG (zweiter Hauptantrag) unzulässig und war daher zurückzuweisen.

4. Zum dritten Hauptbegehren auf Aufhebung der Wortfolge "Kommunikations- und" in §53a Abs2 Z1 litn SPG enthält der Antrag keine Ausführungen, inwieweit diese Bestimmungen in die rechtlich geschützten Interessen der antragstellenden Gesellschaft aktuell eingreifen. Der Antrag war insoweit daher schon aus diesem Grunde zurückzuweisen.

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