

TE Vwgh Erkenntnis 2009/5/27 2007/05/0280

JUSLINE Entscheidung

© Veröffentlicht am 27.05.2009

Index

001 Verwaltungsrecht allgemein;
10/10 Grundrechte;
19/05 Menschenrechte;
20/06 Konsumentenschutz;
41/01 Sicherheitsrecht;
91/01 Fernmeldewesen;
95/08 Sonstige Angelegenheiten der Technik;

Norm

ECG 2001 §13;
ECG 2001 §16 Abs1;
ECG 2001 §16;
ECG 2001 §3 Z1;
MRK Art8;
NotifG 1999 §1 Abs1 Z2;
SPG 1991 §53 Abs3a;
StGG Art10a;
TKG 2003 §3 Z1;
TKG 2003 §3 Z21;
TKG 2003 §3 Z9;
TKG 2003 §92 Abs3 Z3;
TKG 2003 §92 Abs3 Z4;

VwRallg;

1. NotifG 1999 § 1 heute
2. NotifG 1999 § 1 gültig ab 20.08.1999

1. StGG Art. 10a heute
2. StGG Art. 10a gültig ab 01.01.1975 zuletzt geändert durch BGBl. Nr. 8/1974

1. TKG 2003 § 3 gültig von 01.12.2018 bis 31.10.2021 aufgehoben durch BGBl. I Nr. 190/2021
2. TKG 2003 § 3 gültig von 27.11.2015 bis 30.11.2018 zuletzt geändert durch BGBl. I Nr. 134/2015
3. TKG 2003 § 3 gültig von 22.11.2011 bis 26.11.2015 zuletzt geändert durch BGBl. I Nr. 102/2011
4. TKG 2003 § 3 gültig von 20.08.2003 bis 21.11.2011

1. TKG 2003 § 3 gültig von 01.12.2018 bis 31.10.2021 aufgehoben durch BGBl. I Nr. 190/2021
2. TKG 2003 § 3 gültig von 27.11.2015 bis 30.11.2018 zuletzt geändert durch BGBl. I Nr. 134/2015
3. TKG 2003 § 3 gültig von 22.11.2011 bis 26.11.2015 zuletzt geändert durch BGBl. I Nr. 102/2011
4. TKG 2003 § 3 gültig von 20.08.2003 bis 21.11.2011

1. TKG 2003 § 3 gültig von 01.12.2018 bis 31.10.2021 aufgehoben durch BGBl. I Nr. 190/2021
2. TKG 2003 § 3 gültig von 27.11.2015 bis 30.11.2018 zuletzt geändert durch BGBl. I Nr. 134/2015
3. TKG 2003 § 3 gültig von 22.11.2011 bis 26.11.2015 zuletzt geändert durch BGBl. I Nr. 102/2011
4. TKG 2003 § 3 gültig von 20.08.2003 bis 21.11.2011

1. TKG 2003 § 92 gültig von 01.01.2019 bis 31.10.2021 aufgehoben durch BGBl. I Nr. 190/2021
2. TKG 2003 § 92 gültig von 01.01.2019 bis 30.11.2018 zuletzt geändert durch BGBl. I Nr. 29/2018
3. TKG 2003 § 92 gültig von 01.12.2018 bis 31.12.2018 zuletzt geändert durch BGBl. I Nr. 78/2018
4. TKG 2003 § 92 gültig von 01.07.2014 bis 30.11.2018 zuletzt geändert durch BGBl. I Nr. 44/2014
5. TKG 2003 § 92 gültig von 22.11.2011 bis 30.06.2014 zuletzt geändert durch BGBl. I Nr. 102/2011
6. TKG 2003 § 92 gültig von 19.05.2011 bis 21.11.2011 zuletzt geändert durch BGBl. I Nr. 27/2011
7. TKG 2003 § 92 gültig von 20.08.2003 bis 18.05.2011

1. TKG 2003 § 92 gültig von 01.01.2019 bis 31.10.2021 aufgehoben durch BGBl. I Nr. 190/2021
2. TKG 2003 § 92 gültig von 01.01.2019 bis 30.11.2018 zuletzt geändert durch BGBl. I Nr. 29/2018
3. TKG 2003 § 92 gültig von 01.12.2018 bis 31.12.2018 zuletzt geändert durch BGBl. I Nr. 78/2018
4. TKG 2003 § 92 gültig von 01.07.2014 bis 30.11.2018 zuletzt geändert durch BGBl. I Nr. 44/2014
5. TKG 2003 § 92 gültig von 22.11.2011 bis 30.06.2014 zuletzt geändert durch BGBl. I Nr. 102/2011
6. TKG 2003 § 92 gültig von 19.05.2011 bis 21.11.2011 zuletzt geändert durch BGBl. I Nr. 27/2011
7. TKG 2003 § 92 gültig von 20.08.2003 bis 18.05.2011

Betreff

Der Verwaltungsgerichtshof hat durch die Vorsitzende Senatspräsidentin Dr. Giendl und die Hofräte Dr. Pallitsch, Dr. Handstanger, Dr. Hinterwirth und Dr. Moritz als Richter, im Beisein des Schriftführers Mag. Crnja, über die Beschwerde des Bundesministers für Inneres in 1014 Wien, Herrengasse 7, gegen den Bescheid der Datenschutzkommission vom 3. Oktober 2007, Zl. K121.279/0017-DSK/2007, betreffend Amtsbeschwerde in einer Datenschutzangelegenheit (mitbeteiligte Partei: JG, vertreten durch Dr. Helmut Graupner, Rechtsanwalt in 1130 Wien, Maxingstraße 22-24), zu Recht erkannt:

Spruch

Die Beschwerde wird als unbegründet abgewiesen.

Der Bund hat der mitbeteiligten Partei Aufwendungen in der Höhe von EUR 1.106,40 binnen zwei Wochen bei sonstiger Exekution zu ersetzen.

Begründung

In seiner nicht ausdrücklich auf § 31 DSG 2000 gestützten Beschwerde an die Datenschutzkommission brachte der Mitbeteiligte vor, durch die Ausforschung seiner IP-Adresse sowie seines Namens und seiner Adresse im Recht auf Geheimhaltung verletzt worden zu sein. Er habe sich im Oktober 2006 im "Chatforum" von "www.s.at" mit einem für die Benutzung nicht registrierten Pseudonym ("nickname") als Frau ausgegeben und mit einem zufälligen "Chatpartner" in einem Privatfenster einen sexualbezogenen Phantasiechat geführt. Im Zuge dieser Unterhaltung habe er dem "Chatpartner" seine minderjährige Tochter zum sexuellen Missbrauch angeboten und beim "Chatpartner" die Befürchtung geweckt, dass er selbst die Tochter bereits sexuell missbraucht habe und weiterer Missbrauch drohe. Der "Chatpartner" habe daraufhin bei der Polizeiinspektion Trofaiach Anzeige erstattet. Anhand des "nicknames" habe das Landeskriminalamt des Landespolizeikommandos Steiermark beim "Chatroom-Betreiber" die IP-Adresse des Mitbeteiligten telefonisch erfragt und sodann anhand des öffentlichen Verzeichnisses der RIPE ("reseaux IP europeens") den "Internet-Accessprovider" (U) ausfindig gemacht, der diese IP-Adresse vergeben hatte. Der "Internet-Accessprovider" habe schließlich den Mitbeteiligten als Nutzer dieser IP-Adresse identifiziert. Für die Ermittlung und Verarbeitung seiner Daten ohne eine richterliche Ermächtigung gäbe es keine taugliche Rechtsgrundlage; die vom Landespolizeikommando Steiermark gewählte Vorgangsweise sei sohin rechtswidrig gewesen. In seiner nicht

ausdrücklich auf Paragraph 31, DSG 2000 gestützten Beschwerde an die Datenschutzkommission brachte der Mitbeteiligte vor, durch die Ausforschung seiner IP-Adresse sowie seines Namens und seiner Adresse im Recht auf Geheimhaltung verletzt worden zu sein. Er habe sich im Oktober 2006 im "Chatforum" von "www.s.at" mit einem für die Benutzung nicht registrierten Pseudonym ("nickname") als Frau ausgegeben und mit einem zufälligen "Chatpartner" in einem Privatfenster einen sexualbezogenen Phantasiechat geführt. Im Zuge dieser Unterhaltung habe er dem "Chatpartner" seine minderjährige Tochter zum sexuellen Missbrauch angeboten und beim "Chatpartner" die Befürchtung geweckt, dass er selbst die Tochter bereits sexuell missbraucht habe und weiterer Missbrauch drohe. Der "Chatpartner" habe daraufhin bei der Polizeiinspektion Trofaiach Anzeige erstattet. Anhand des "nicknames" habe das Landeskriminalamt des Landespolizeikommandos Steiermark beim "Chatroom-Betreiber" die IP-Adresse des Mitbeteiligten telefonisch erfragt und sodann anhand des öffentlichen Verzeichnisses der RIPE ("reseaux IP europeens") den "Internet-Accessprovider" (U) ausfindig gemacht, der diese IP-Adresse vergeben hatte. Der "Internet-Accessprovider" habe schließlich den Mitbeteiligten als Nutzer dieser IP-Adresse identifiziert. Für die Ermittlung und Verarbeitung seiner Daten ohne eine richterliche Ermächtigung gäbe es keine taugliche Rechtsgrundlage; die vom Landespolizeikommando Steiermark gewählte Vorgangsweise sei sohin rechtswidrig gewesen.

Die Sicherheitsdirektion für das Bundesland Steiermark bestätigte das Vorbringen des Mitbeteiligten im Verfahren vor der belangten Behörde und führte aus, die Rechtsgrundlage für das Vorgehen des Landeskriminalamtes des Landespolizeikommando Steiermark sei § 53 Abs. 3a SPG idF BGBl. I Nr. 158/2005; eine richterliche Ermächtigung sei nicht notwendig gewesen. Die Sicherheitsdirektion für das Bundesland Steiermark bestätigte das Vorbringen des Mitbeteiligten im Verfahren vor der belangten Behörde und führte aus, die Rechtsgrundlage für das Vorgehen des Landeskriminalamtes des Landespolizeikommando Steiermark sei Paragraph 53, Absatz 3 a, SPG in der Fassung Bundesgesetzblatt Teil eins, Nr. 158 aus 2005;; eine richterliche Ermächtigung sei nicht notwendig gewesen.

Mit dem nunmehr angefochtenen Bescheid der Datenschutzkommission wurde der Beschwerde des Mitbeteiligten stattgegeben.

Begründet wurde diese Entscheidung damit, dass § 53 Abs. 3a SPG idF BGBl. I Nr. 158/2005 allein keine ausreichende Grundlage für die Ermittlung von Verkehrsdaten darstellen könne, sondern hiefür der Umfang besonderer Eingriffsbefugnisse maßgeblich sei, die den Sicherheitsbehörden nach dem Sicherheitspolizeigesetz oder einem anderen Gesetz eingeräumt seien. In der Literatur werde der Betrieb eines "Chatrooms" regelmäßig als ein solcher Dienst der Informationsgesellschaft angesehen, der nur dem E-Commerce-Gesetz (ECG) und nicht auch dem Telekommunikationsgesetz (TKG) unterliege; dieser sei somit kein "Telekommunikationsdienst" im Sinne des § 3 Z 14 bzw. § 3 Z 9 TKG. Das Betreiben eines "Chatrooms" sei ein Fall des "Hostings", wobei der Speichervorgang der wesentliche Unterschied zwischen einem "Hosting" und einem Access-Provider sei. Der Dienst "www.s.at" biete inhaltliche Leistungen an. Der Umstand, dass der "Chat" in einem Privatfenster regelmäßig nicht gespeichert würde, habe nichts mit der technischen Natur des Dienstes zu tun, sondern stelle nur ein spezielles Angebot dar. Selbst wenn man jedoch davon ausginge, dass es sich im gegenständlichen Fall um einen Telekommunikationsdienst im Sinn des § 53 Abs. 3a SPG (alt) handle, wäre die Ermittlung der IP-Adresse aus nachstehenden Gründen nicht durch diese Bestimmung gedeckt: Begründet wurde diese Entscheidung damit, dass Paragraph 53, Absatz 3 a, SPG in der Fassung Bundesgesetzblatt Teil eins, Nr. 158 aus 2005, allein keine ausreichende Grundlage für die Ermittlung von Verkehrsdaten darstellen könne, sondern hiefür der Umfang besonderer Eingriffsbefugnisse maßgeblich sei, die den Sicherheitsbehörden nach dem Sicherheitspolizeigesetz oder einem anderen Gesetz eingeräumt seien. In der Literatur werde der Betrieb eines "Chatrooms" regelmäßig als ein solcher Dienst der Informationsgesellschaft angesehen, der nur dem E-Commerce-Gesetz (ECG) und nicht auch dem Telekommunikationsgesetz (TKG) unterliege; dieser sei somit kein "Telekommunikationsdienst" im Sinne des Paragraph 3, Ziffer 14, bzw. Paragraph 3, Ziffer 9, TKG. Das Betreiben eines "Chatrooms" sei ein Fall des "Hostings", wobei der Speichervorgang der wesentliche Unterschied zwischen einem "Hosting" und einem Access-Provider sei. Der Dienst "www.s.at" biete inhaltliche Leistungen an. Der Umstand, dass der "Chat" in einem Privatfenster regelmäßig nicht gespeichert würde, habe nichts mit der technischen Natur des Dienstes zu tun, sondern stelle nur ein spezielles Angebot dar. Selbst wenn man jedoch davon ausginge, dass es sich im gegenständlichen Fall um einen Telekommunikationsdienst im Sinn des Paragraph 53, Absatz 3 a, SPG (alt) handle, wäre die Ermittlung der IP-Adresse aus nachstehenden Gründen nicht durch diese Bestimmung gedeckt:

§ 53 Abs. 3a SPG (alt) umfasse mehrere unterschiedliche Fälle. Neben der Bekanntgabe einer Telefonnummer eines namentlich bezeichneten Teilnehmers betreffe diese Bestimmung auch die Auskunft über die Identität des

Teilnehmers eines mit Hilfe der Telefonnummer bezeichneten Anschlusses. Darüber hinaus bestimme der zweite Satz des § 53 Abs. 3a SPG (alt) aber, dass der Betreiber auch Auskunft über die Identität des Inhabers eines nicht bekannten Anschlusses zu geben habe. Die letztere Auskunftspflicht habe eine andere Dimension als die sonstigen Fälle, weil sie die Auswertung von Verkehrsdaten notwendig mache. Derselbe Vorgang werde in der StPO mit "Feststellung des Ursprungs einer Telekommunikation" bezeichnet und an das Vorliegen eines richterlichen Überwachungsbeschlusses geknüpft. Soweit also Sicherheitsbehörden im Rahmen der ihnen nach dem SPG übertragenen Aufgaben der Gefahrenabwehr in einem gewissen Umfang eine - aus datenschutzrechtlicher Sicht doch eingriffsintensive - Befugnis zur Rufdatenrück Erfassung zustünde, sei nach Auffassung der Datenschutzkommission nur eine restriktive und am Wortlaut der Bestimmung orientierte Auslegung angemessen. Am ehesten komme im beschwerdegegenständlichen Fall der 2. Satz der genannten Bestimmung in Betracht, jedoch würde diese Bestimmung ausdrücklich auf ein "von einem Anschluss aus geführtes Gespräch" abstellen und sei daher auf die Sprachtelefonie zugeschnitten und auf diese begrenzt. Zusätzlich sei auch nicht aufgrund einer passiven Teilnehmernummer erhoben worden, sondern sei der Betreiber des "Chatrooms" vielmehr um Aushebung des vom anzeigenden "Chatpartners" angegebenen und vom Mitbeteiligten verwendeten "nickname" ersucht worden, der dann die diesem "nickname" zugeordnete IP-Adresse mitgeteilt habe. Für die Ermittlung der dynamischen IP-Adresse, welche ein Verkehrsdatum darstelle, stelle Paragraph 53, Absatz 3 a, SPG (alt) umfasse mehrere unterschiedliche Fälle. Neben der Bekanntgabe einer Telefonnummer eines namentlich bezeichneten Teilnehmers betreffe diese Bestimmung auch die Auskunft über die Identität des Teilnehmers eines mit Hilfe der Telefonnummer bezeichneten Anschlusses. Darüber hinaus bestimme der zweite Satz des Paragraph 53, Absatz 3 a, SPG (alt) aber, dass der Betreiber auch Auskunft über die Identität des Inhabers eines nicht bekannten Anschlusses zu geben habe. Die letztere Auskunftspflicht habe eine andere Dimension als die sonstigen Fälle, weil sie die Auswertung von Verkehrsdaten notwendig mache. Derselbe Vorgang werde in der StPO mit "Feststellung des Ursprungs einer Telekommunikation" bezeichnet und an das Vorliegen eines richterlichen Überwachungsbeschlusses geknüpft. Soweit also Sicherheitsbehörden im Rahmen der ihnen nach dem SPG übertragenen Aufgaben der Gefahrenabwehr in einem gewissen Umfang eine - aus datenschutzrechtlicher Sicht doch eingriffsintensive - Befugnis zur Rufdatenrück Erfassung zustünde, sei nach Auffassung der Datenschutzkommission nur eine restriktive und am Wortlaut der Bestimmung orientierte Auslegung angemessen. Am ehesten komme im beschwerdegegenständlichen Fall der 2. Satz der genannten Bestimmung in Betracht, jedoch würde diese Bestimmung ausdrücklich auf ein "von einem Anschluss aus geführtes Gespräch" abstellen und sei daher auf die Sprachtelefonie zugeschnitten und auf diese begrenzt. Zusätzlich sei auch nicht aufgrund einer passiven Teilnehmernummer erhoben worden, sondern sei der Betreiber des "Chatrooms" vielmehr um Aushebung des vom anzeigenden "Chatpartners" angegebenen und vom Mitbeteiligten verwendeten "nickname" ersucht worden, der dann die diesem "nickname" zugeordnete IP-Adresse mitgeteilt habe. Für die Ermittlung der dynamischen IP-Adresse, welche ein Verkehrsdatum darstelle, stelle

§ 53 Abs. 3a SPG (alt) keine taugliche Basis dar, selbst wenn sich angesichts der Sachverhaltsumstände das Verständnis für ein Verhalten wie jenes des Mitbeteiligten in Grenzen hielte. Es sei bedenklich, den Anwendungsbereich des § 53 Abs. 3a SPG (alt) auch auf ausdrücklich nicht erfasste Sachverhalte im Wege der Analogie zu erweitern. Paragraph 53, Absatz 3 a, SPG (alt) keine taugliche Basis dar, selbst wenn sich angesichts der Sachverhaltsumstände das Verständnis für ein Verhalten wie jenes des Mitbeteiligten in Grenzen hielte. Es sei bedenklich, den Anwendungsbereich des Paragraph 53, Absatz 3 a, SPG (alt) auch auf ausdrücklich nicht erfasste Sachverhalte im Wege der Analogie zu erweitern.

Es bleibe daher aufgrund der erfolgten Zuordnung von "Chatforen" zu den sogenannten "Host Providern" nach § 16 ECG zu prüfen, ob allenfalls § 18 ECG als Grundlage für ein Auskunftsverlangen von Sicherheitsbehörden wie im vorliegenden Fall in Frage kommen könnte. Gemäß § 18 Abs. 3 ECG müssten "Hostingprovider" aufgrund der Anordnung einer Verwaltungsbehörde Auskunft über "Namen" und "Adresse" der Nutzer ihrer Dienste geben. "Name und Adresse" seien jedoch "Stammdaten" und sei "Adresse" im Sinn von "Anschrift" zu verstehen, eine IP-Adresse sei hievon nicht umfasst. Die IP-Adresse allerdings sei ein "Verkehrsdatum" und unterliege daher der Vertraulichkeit gem. Art. 5 der RL 2002/58/EG bzw. dem Kommunikationsgeheimnis gemäß § 93 Abs. 1 TKG und besonderen Verwendungsbeschränkungen gem. Art. 6 der genannten RL und § 99 TKG. Dies bedeute vor allem, dass derartige Daten nur zu Verrechnungszwecken gespeichert werden dürften oder eine ausdrückliche Einwilligung des Betroffenen vorliegen müsse. Es sei daher insgesamt davon auszugehen, dass das Vorgehen weder im SPG noch im ECG eine gesetzliche Deckung finden könne. Es bleibe daher aufgrund der erfolgten Zuordnung von "Chatforen" zu den

sogenannten "Host Providern" nach Paragraph 16, ECG zu prüfen, ob allenfalls Paragraph 18, ECG als Grundlage für ein Auskunftsverlangen von Sicherheitsbehörden wie im vorliegenden Fall in Frage kommen könnte. Gemäß Paragraph 18, Absatz 3, ECG müssten "Hostingprovider" aufgrund der Anordnung einer Verwaltungsbehörde Auskunft über "Namen" und "Adresse" der Nutzer ihrer Dienste geben. "Name und Adresse" seien jedoch "Stammdaten" und sei "Adresse" im Sinn von "Anschrift" zu verstehen, eine IP-Adresse sei hievon nicht umfasst. Die IP-Adresse allerdings sei ein "Verkehrsdatum" und unterliege daher der Vertraulichkeit gem. Artikel 5, der RL 2002/58/EG bzw. dem Kommunikationsgeheimnis gemäß Paragraph 93, Absatz eins, TKG und besonderen Verwendungsbeschränkungen gem. Artikel 6, der genannten RL und Paragraph 99, TKG. Dies bedeute vor allem, dass derartige Daten nur zu Verrechnungszwecken gespeichert werden dürften oder eine ausdrückliche Einwilligung des Betroffenen vorliegen müsse. Es sei daher insgesamt davon auszugehen, dass das Vorgehen weder im SPG noch im ECG eine gesetzliche Deckung finden könne.

Dagegen richtet sich die vorliegende Amtsbeschwerde gemäß § 91 Abs. 1 Z. 2 SPG wegen Rechtswidrigkeit des Inhaltes und Rechtswidrigkeit infolge Verletzung von Verfahrensvorschriften. Dagegen richtet sich die vorliegende Amtsbeschwerde gemäß Paragraph 91, Absatz eins, Ziffer 2, SPG wegen Rechtswidrigkeit des Inhaltes und Rechtswidrigkeit infolge Verletzung von Verfahrensvorschriften.

Begründend wird darin ausgeführt, dass es sich gerade bei der Bereitstellung eines "vertraulichen Chats", bei dem keine Inhalte gespeichert würden, um einen Kommunikationsdienst iSd § 3 Z 9 iVm Z 17 TKG handle, auch wenn von dem Anbieter andere Dienste angeboten würden. Selbst der Mitbeteiligte sei davon ausgegangen, dass das "gewerbliche Betreiben eines Internetchats einen Telekommunikationsdienst" darstelle und daher § 53 Abs. 3a SPG (alt) grundsätzlich anzuwenden gewesen sei. Die Datenschutzkommission habe sich im gegenständlichen Verfahren überhaupt nicht mit der Frage auseinander gesetzt, wie der Begriff "Betreiber eines öffentlichen Telekommunikationsdienstes" im Sinne des § 53 Abs. 3a SPG auszulegen sei, sondern sich lediglich mit den Definitionen des TKG und ECG sowie der rechtlichen Einordnung des "Chatroombetreibers" unter eine dieser Materien beschäftigt. Die Subsumption des gegenständlichen Sachverhaltes unter § 53 Abs. 3a SPG (alt) sei ohne weitere Begründung verneint worden und dies würde einen Verfahrensmangel iSd § 42 Abs. 2 Z 3 VwGG darstellen. Als ausdrückliche Ermächtigung zu informellen Eingriffen im Rahmen der Gefahrenabwehr stehe § 53 Abs. 3a erster Satz SPG zur Verfügung. Mit dieser Regelung sollen die Sicherheitsbehörden in die Lage versetzt werden, im Zusammenhang mit der Benützung öffentlicher Telekommunikationsnetze Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses (auch Internetzuganges) in Erfahrung zu bringen. Es handle sich dabei um jene Daten, die zur Identifizierung eines bestimmten Teilnehmers an einer öffentlichen Kommunikation notwendig seien. Darauf habe sich auch das Auskunftsbegehren des Landespolizeikommandos Steiermark bezogen, als "um Aushebung des gegenüber dem Chatpartner angegebenen 'nicknames'" ersucht worden sei. Der "nickname" sei ein Attribut des Gesamtdatensatzes, der für alle "Chatter" nach außen sichtbar sei. Hätte sich ein Teilnehmer unter seinem Namen und seiner Anschrift registriert, wäre bei der Aushebung ein Name und eine Adresse ermittelt worden. Da allerdings im vorliegenden Fall für die Registrierung nur ein geringes Maß an Daten notwendig gewesen sei und nur die IP-Adresse als Teilnehmernummer habe ausgeforscht werden können, handle es sich bei diesem Datum um die zulässigerweise erfragte "Teilnehmernummer" im Sinne des § 53 Abs. 3a erster Satz SPG. Ob eine IP-Adresse statisch oder dynamisch sei, hänge nicht vom "Chatroom-Betreiber" ab, sondern bestimme sich nach den technischen Gegebenheiten des "Access-Providers". Erst durch eine weitere Auskunft beim "Access-Provider" könne eine IP-Adresse einem bestimmten Menschen zugeordnet werden. Bei dieser Ermittlung handle es sich erneut um eine solche nach dem 1. Satz des § 53 Abs. 3a SPG, weil nunmehr anhand einer bestimmten IP-Adresse nach Name und Anschrift des registrierten Benutzers gefragt werden könne. Der Beschwerdeführer verweist auf das Urteil des Obersten Gerichtshofes (OGH) vom 26. Juli 2005, 11 Os 57/05z, in dem dieser Gerichtshof die IP-Adresse als Identifikationsmerkmal eines Teilnehmers im Sinne des § 103 Abs. 4 TKG über die Teilnehmerverzeichnisse und deren zulässige Beauskunftung an ein Gericht nach dieser Norm annahm und die Anwendbarkeit der Strafprozessordnung für diesen Fall der Beauskunftung verneinte. Darüber, dass der OGH entschieden habe, die Erhebungen des Namens und der Wohnadresse eines Internetnutzers, dem eine statische oder dynamische Internetadresse zugewiesen worden sei, wären unter keinen der Eingriffstatbestände des § 149a Abs. 1 Z 1 StPO zu subsumieren, weil "selbst bei dynamischen IP-Adressen die Übermittlung der zugehörigen Stammdaten keine Feststellung erfordert, welche Teilnehmeranschlüsse Ursprung einer Telekommunikation waren", würde sich die Datenschutzkommission einfach hinwegsetzen. Dass weder in § 53 Abs. 3a SPG noch in § 103 Abs. 4 TKG die Datenkategorie (IP-Adresse) als Kriterium für die das Auskunft-Geben

ausdrücklich angeführt würde, sondern der Überbegriff "Teilnehmernummer" verwendet würde, ändere nichts an der Zulässigkeit des Erteilens der Auskunft als einzig zulässiges Identifikationskriterium. Es würde dem Zweck der Norm gänzlich zuwider laufen, wenn man die Zulässigkeit der Ermittlung der "Identifikationsdaten" durch die Sicherheitsbehörde auf Grundlage von § 53 Abs. 3a erster Satz SPG von den Registrierungsmodalitäten abhängig macht. Es wäre im Ergebnis völlig ungerechtfertigt, diesen Fall des Erteilens der Auskunft im Hinblick auf die rechtliche Zulässigkeit der Rufdatenrück Erfassung im Sinne des § 53 Abs. 3a zweiter Satz SPG zu qualifizieren und somit strenger zu behandeln als den vom OGH ausjudizierten Fall der "formlosen", auf § 103 TKG gestützten "Beauskunftung" des Namens anhand einer bekannten IP-Adresse. Wenn nämlich die IP-Adresse anhand des "nicknames" als einziges rückführbares Identifikationskriterium nicht ermittelt werden dürfte, würde sich die Frage der weiteren "Beauskunftung" zur Ermittlung des tatsächlichen Benutzers gar nicht stellen. Die Rechtsansicht der Datenschutzkommission, diesen Akt der Auskunftserlangung als ein Ganzes zu betrachten und unter die Ermächtigung des § 53 Abs. 3a zweiter Satz SPG zu subsumieren, sei daher verfehlt. Begründend wird darin ausgeführt, dass es sich gerade bei der Bereitstellung eines "vertraulichen Chats", bei dem keine Inhalte gespeichert würden, um einen Kommunikationsdienst iSd Paragraph 3, Ziffer 9, in Verbindung mit Ziffer 17, TKG handle, auch wenn von dem Anbieter andere Dienste angeboten würden. Selbst der Mitbeteiligte sei davon ausgegangen, dass das "gewerbliche Betreiben eines Internetchats einen Telekommunikationsdienst" darstelle und daher Paragraph 53, Absatz 3 a, SPG (alt) grundsätzlich anzuwenden gewesen sei. Die Datenschutzkommission habe sich im gegenständlichen Verfahren überhaupt nicht mit der Frage auseinander gesetzt, wie der Begriff "Betreiber eines öffentlichen Telekommunikationsdienstes" im Sinne des Paragraph 53, Absatz 3 a, SPG auszulegen sei, sondern sich lediglich mit den Definitionen des TKG und ECG sowie der rechtlichen Einordnung des "Chatroombetreibers" unter eine dieser Materien beschäftigt. Die Subsumption des gegenständlichen Sachverhaltes unter Paragraph 53, Absatz 3 a, SPG (alt) sei ohne weitere Begründung verneint worden und dies würde einen Verfahrensmangel iSd Paragraph 42, Absatz 2, Ziffer 3, VwGG darstellen. Als ausdrückliche Ermächtigung zu informellen Eingriffen im Rahmen der Gefahrenabwehr stehe Paragraph 53, Absatz 3 a, erster Satz SPG zur Verfügung. Mit dieser Regelung sollen die Sicherheitsbehörden in die Lage versetzt werden, im Zusammenhang mit der Benützung öffentlicher Telekommunikationsnetze Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses (auch Internetzuganges) in Erfahrung zu bringen. Es handle sich dabei um jene Daten, die zur Identifizierung eines bestimmten Teilnehmers an einer öffentlichen Kommunikation notwendig seien. Darauf habe sich auch das Auskunftsbegehren des Landespolizeikommandos Steiermark bezogen, als "um Aushebung des gegenüber dem Chatpartner angegebenen 'nicknames'" ersucht worden sei. Der "nickname" sei ein Attribut des Gesamtdatensatzes, der für alle "Chatter" nach außen sichtbar sei. Hätte sich ein Teilnehmer unter seinem Namen und seiner Anschrift registriert, wäre bei der Aushebung ein Name und eine Adresse ermittelt worden. Da allerdings im vorliegenden Fall für die Registrierung nur ein geringes Maß an Daten notwendig gewesen sei und nur die IP-Adresse als Teilnehmernummer habe ausgeforscht werden können, handle es sich bei diesem Datum um die zulässigerweise erfragte "Teilnehmernummer" im Sinne des Paragraph 53, Absatz 3 a, erster Satz SPG. Ob eine IP-Adresse statisch oder dynamisch sei, hänge nicht vom "Chatroom-Betreiber" ab, sondern bestimme sich nach den technischen Gegebenheiten des "Access-Providers". Erst durch eine weitere Auskunft beim "Access-Provider" könne eine IP-Adresse einem bestimmten Menschen zugeordnet werden. Bei dieser Ermittlung handle es sich erneut um eine solche nach dem 1. Satz des Paragraph 53, Absatz 3 a, SPG, weil nunmehr anhand einer bestimmten IP-Adresse nach Name und Anschrift des registrierten Benutzers gefragt werden könne. Der Beschwerdeführer verweist auf das Urteil des Obersten Gerichtshofes (OGH) vom 26. Juli 2005, 11 Os 57/05z, in dem dieser Gerichtshof die IP-Adresse als Identifikationsmerkmal eines Teilnehmers im Sinne des Paragraph 103, Absatz 4, TKG über die Teilnehmerverzeichnisse und deren zulässige Beauskunftung an ein Gericht nach dieser Norm annahm und die Anwendbarkeit der Strafprozessordnung für diesen Fall der Beauskunftung verneinte. Darüber, dass der OGH entschieden habe, die Erhebungen des Namens und der Wohnadresse eines Internetnutzers, dem eine statische oder dynamische Internetadresse zugewiesen worden sei, wären unter keinen der Eingriffstatbestände des Paragraph 149 a, Absatz eins, Ziffer eins, StPO zu subsumieren, weil "selbst bei dynamischen IP-Adressen die Übermittlung der zugehörigen Stammdaten keine Feststellung erfordert, welche Teilnehmeranschlüsse Ursprung einer Telekommunikation waren", würde sich die Datenschutzkommission einfach hinwegsetzen. Dass weder in Paragraph 53, Absatz 3 a, SPG noch in Paragraph 103, Absatz 4, TKG die Datenkategorie (IP-Adresse) als Kriterium für die Auskunft-Geben ausdrücklich angeführt würde, sondern der Überbegriff "Teilnehmernummer" verwendet würde, ändere nichts an der Zulässigkeit des Erteilens der Auskunft als einzig zulässiges Identifikationskriterium. Es würde

dem Zweck der Norm gänzlich zuwider laufen, wenn man die Zulässigkeit der Ermittlung der "Identifikationsdaten" durch die Sicherheitsbehörde auf Grundlage von Paragraph 53, Absatz 3 a, erster Satz SPG von den Registrierungsmodalitäten abhängig macht. Es wäre im Ergebnis völlig ungerechtfertigt, diesen Fall des Erteilens der Auskunft im Hinblick auf die rechtliche Zulässigkeit der Rufdatenrück Erfassung im Sinne des Paragraph 53, Absatz 3 a, zweiter Satz SPG zu qualifizieren und somit strenger zu behandeln als den vom OGH ausjudizierten Fall der "formlosen", auf Paragraph 103, TKG gestützten "Beauskunftung" des Namens anhand einer bekannten IP-Adresse. Wenn nämlich die IP-Adresse anhand des "nicknames" als einziges rückführbares Identifikationskriterium nicht ermittelt werden dürfte, würde sich die Frage der weiteren "Beauskunftung" zur Ermittlung des tatsächlichen Benutzers gar nicht stellen. Die Rechtsansicht der Datenschutzkommission, diesen Akt der Auskunftserlangung als ein Ganzes zu betrachten und unter die Ermächtigung des Paragraph 53, Absatz 3 a, zweiter Satz SPG zu subsumieren, sei daher verfehlt.

Der Mitbeteiligte erstattete eine Gegenschrift, in der er ausführte, die Ansicht des Beschwerdeführers, dass die Auskunft bereits aufgrund von Satz 1 des § 53 Abs. 3a SPG habe erteilt werden können, da die IP-Adresse die "Teilnehmernummer" eines "Internetchats" im Sinne der genannten Bestimmung sei, sei verfehlt. Es sei unbestritten, dass der Verdacht einer strafbaren Handlung vorgelegen sei, dem die Sicherheitsbehörden nachgehen haben müssen. Auch sei es richtig, dass die Sicherheitsbehörden dabei berechtigt gewesen seien, die IP-Adresse und in der Folge deren Inhaber ausfindig zu machen. Strittig sei lediglich, ob der von der Sicherheitsbehörde verfolgte Weg der direkten Anfrage ohne Gerichtsbeschluss (noch dazu unter Berufung auf eine gesetzliche Auskunftsverpflichtung des "Chatbetreibers") auf Grundlage des § 53 Abs. 3a SPG (alt) der richtige gewesen sei. Gemäß dem ersten Satz der Bestimmung dürfe die Sicherheitsbehörde Name, Anschrift und Teilnehmernummer eines bestimmten Anschlusses ermitteln. Die IP-Adresse eines "Chatteilnehmers" sei jedoch keine Teilnehmernummer des "Chatbetreibers" bzw. des von ihm betriebenen Telekommunikationsdienstes, sondern nur eine Teilnehmernummer der Firma U. Zusätzlich sei der in der Bestimmung genannte Anschluss des 1. und 2. Satzes in § 53 Abs. 3a SPG ident und würde auf ein von diesem Anschluss geführtes Gespräch abstellen, es sei sohin die Bestimmung lediglich auf Sprachtelefonie zugeschnitten und nur diese würde erfasst. Es sei weder ein "nickname" ein bestimmter Anschluss eines "Chats", noch sei eine von der Firma U vergebene IP-Adresse eine Teilnehmernummer eines solchen "nicknames". Aus diesen Gründen sei § 53 Abs. 3a SPG keine taugliche Rechtsgrundlage für das inkriminierende Vorgehen der einschreitenden Behörde. Die einzig taugliche gesetzliche Grundlage wäre § 18 Abs. 2 ECG gewesen. Die Sicherheitsbehörde hätte also eine gerichtliche Anordnung an den "Chatbetreiber" anregen können; diese wäre sicher erteilt worden. Dadurch wäre das Gesetz und insbesondere das grundrechtlich verbürgte Fernmeldegeheimnis (Art. 10a StGG) gewahrt worden. Die IP-Adresse sei für den "Chatbetreiber" jedenfalls ein Verkehrsdatum. Daten darüber, wann mit welcher IP-Adresse mit welchem "nickname" auf welchem der beiden "Chatserver" in welchen Räumen kommuniziert worden sei, seien unzweifelhaft Verkehrsdaten im Sinne des § 92 Abs. 3 Z 4 TKG. Die IP-Adresse selbst sei auch für den "Chatbetreiber" ein Verkehrsdatum und kein Stammdatum, da sie nicht in einem Verzeichnis mit Identitätsdaten eines Teilnehmers verbunden werde. Um festzustellen, mit welcher IP-Adresse zu einem bestimmten Zeitpunkt mit einem bestimmten "nickname" in den "Chat" eingestiegen und in diesem kommuniziert worden sei, oder gar in welchen Räumen, müsse ein "Chatroombetreiber" seine "Logfiles" durchsuchen. Dieses Durchsuchen bedinge beim Betreiber unzweifelhaft eine Verarbeitung von Daten, die er zum Zweck der Weiterleitung einer Nachricht an ein Kommunikationsnetz verarbeite; es handle sich also um Verkehrsdaten, die keine der Eigenschaften von Stammdatens aufwiesen. Der Mitbeteiligte erstattete eine Gegenschrift, in der er ausführte, die Ansicht des Beschwerdeführers, dass die Auskunft bereits aufgrund von Satz 1 des Paragraph 53, Absatz 3 a, SPG habe erteilt werden können, da die IP-Adresse die "Teilnehmernummer" eines "Internetchats" im Sinne der genannten Bestimmung sei, sei verfehlt. Es sei unbestritten, dass der Verdacht einer strafbaren Handlung vorgelegen sei, dem die Sicherheitsbehörden nachgehen haben müssen. Auch sei es richtig, dass die Sicherheitsbehörden dabei berechtigt gewesen seien, die IP-Adresse und in der Folge deren Inhaber ausfindig zu machen. Strittig sei lediglich, ob der von der Sicherheitsbehörde verfolgte Weg der direkten Anfrage ohne Gerichtsbeschluss (noch dazu unter Berufung auf eine gesetzliche Auskunftsverpflichtung des "Chatbetreibers") auf Grundlage des Paragraph 53, Absatz 3 a, SPG (alt) der richtige gewesen sei. Gemäß dem ersten Satz der Bestimmung dürfe die Sicherheitsbehörde Name, Anschrift und Teilnehmernummer eines bestimmten Anschlusses ermitteln. Die IP-Adresse eines "Chatteilnehmers" sei jedoch keine Teilnehmernummer des "Chatbetreibers" bzw. des von ihm betriebenen Telekommunikationsdienstes, sondern nur eine Teilnehmernummer der Firma U. Zusätzlich sei der in der Bestimmung genannte Anschluss des 1. und 2. Satzes in Paragraph 53, Absatz 3

a, SPG ident und würde auf ein von diesem Anschluss geführtes Gespräch abstellen, es sei sohin die Bestimmung lediglich auf Sprachtelefonie zugeschnitten und nur diese würde erfasst. Es sei weder ein "nickname" ein bestimmter Anschluss eines "Chats", noch sei eine von der Firma U vergebene IP-Adresse eine Teilnehmernummer eines solchen "nicknames". Aus diesen Gründen sei Paragraph 53, Absatz 3 a, SPG keine taugliche Rechtsgrundlage für das inkriminierende Vorgehen der einschreitenden Behörde. Die einzig taugliche gesetzliche Grundlage wäre Paragraph 18, Absatz 2, ECG gewesen. Die Sicherheitsbehörde hätte also eine gerichtliche Anordnung an den "Chatbetreiber" anregen können; diese wäre sicher erteilt worden. Dadurch wäre das Gesetz und insbesondere das grundrechtlich verbürgte Fernmeldegeheimnis (Artikel 10 a, StGG) gewahrt worden. Die IP-Adresse sei für den "Chatbetreiber" jedenfalls ein Verkehrsdatum. Daten darüber, wann mit welcher IP-Adresse mit welchem "nickname" auf welchem der beiden "Chatserver" in welchen Räumen kommuniziert worden sei, seien unzweifelhaft Verkehrsdaten im Sinne des Paragraph 92, Absatz 3, Ziffer 4, TKG. Die IP-Adresse selbst sei auch für den "Chatbetreiber" ein Verkehrsdatum und kein Stammdatum, da sie nicht in einem Verzeichnis mit Identitätsdaten eines Teilnehmers verbunden werde. Um festzustellen, mit welcher IP-Adresse zu einem bestimmten Zeitpunkt mit einem bestimmten "nickname" in den "Chat" eingestiegen und in diesem kommuniziert worden sei, oder gar in welchen Räumen, müsse ein "Chatroombetreiber" seine "Logfiles" durchsuchen. Dieses Durchsuchen bedinge beim Betreiber unzweifelhaft eine Verarbeitung von Daten, die er zum Zweck der Weiterleitung einer Nachricht an ein Kommunikationsnetz verarbeite; es handle sich also um Verkehrsdaten, die keine der Eigenschaften von Stammdatens aufwiesen.

Die belangte Behörde legte die Verwaltungsakten vor und erstattete eine Gegenschrift, in der sie ausführte, dass "Betreiber eines öffentlichen Telekommunikationsdienstes" gemäß § 53 Abs. 3a SPG (alt) im Sinne des TKG zu verstehen sei. § 53 Abs. 3a SPG sei mit der Novelle BGBl I Nr. 146/1999 eingeführt worden. Der Begriff "Betreiber eines öffentlichen Telekommunikationsdienstes" werde darin ohne nähere Definition verwendet. Das zu diesem Zeitpunkt geltende TKG habe eine gesetzliche Definition dieses Begriffes enthalten und es sei daher angesichts der Einheit der Rechtsordnung davon auszugehen, dass, sofern es für einen im TKG bestimmten Begriff eine abweichende Bedeutung in einem anderen Gesetz geben sollte, dies ausdrücklich festgelegt worden wäre. Die Datenschutzkommission sei im Einklang mit der Literatur davon ausgegangen, dass ein "Chatroom-Betreiber" kein Betreiber eines öffentlichen Telekommunikationsdienstes iSd TKG sei, sondern zu jenen Anbietern von Diensten der Informationsgesellschaft iSd § 3 Z 1 ECG gehöre, die als "Host-Betreiber" nur dem ECG (§§ 16 ff ECG) unterlägen. Dem Argument, beim "Chatten" im Privatfenster sei es nicht zu einer Speicherung der Inhaltsdaten gekommen, sei entgegenzuhalten, dass die Qualifikation als Betreiber nach dem TKG oder nur nach dem ECG auf Grund des grundsätzlichen Charakters der angebotenen Leistung erfolge. Dies sei eindeutig der Legaldefinition von "Kommunikationsdienst" iSd § 3 Z 9 TKG 2003 zu entnehmen. Damit ein "Chatroom" als Telekommunikationsdienst einzustufen wäre, dürfte der angebotene Dienst "ganz oder überwiegend" keine inhaltsbezogenen Leistungen erbringen, was allerdings für einen "Chatroom" völlig atypisch wäre. Es fehle ein sachlicher Hinweis, dass der Begriff "Telekommunikationsdienst" im § 53 Abs. 3a SPG (alt) von einer anderen Bedeutung als der Legaldefinition des § Z 9 TKG 2003 ausgehe. Weiters fehle jeglicher sachlicher Hinweis darauf, dass im Begriff des Telekommunikationsdienstes jemals auch Inhaltsdienste miteingeschlossen gewesen wären, da diese doch eine neuere Entwicklung im Portfolio der Dienstleistungen der Informationsgesellschaft seien. Eine ausdehnende Interpretation von Eingriffsnormen nach dem Utilitätsprinzip, wie vom Beschwerdeführer nunmehr verlangt, mache die Schutzfunktion des Gesetzesvorbehaltes bei Grundrechtseingriffen zunichte. Dass der Gesetzgeber die "Content-Provider" in der beschwerdegegenständlichen Fassung des § 53 Abs. 3a SPG nicht miteingeschlossen habe, werde dadurch bewiesen, dass er die von der Datenschutzkommission aufgezeigte Lücke umgehend durch eine Novellierung des § 53 Abs. 3a SPG mit BGBl. I Nr. 114/2007 geschlossen habe, ohne den Ausgang des gegenständlichen Verfahrens abzuwarten. Nunmehr könnten Sicherheitsbehörden ausdrücklich Auskünfte von Betreibern öffentlicher Telekommunikationsdienste (§ 92 Abs. 3 Z 1 TKG 2003) und sonstigen Diensteanbietern (§ 3 Z 2 ECG) verlangen. Bezüglich der zitierten OGH-Entscheidung sei festzuhalten, dass diese auf den vorliegenden Fall nicht übertragbar sei, da in jenem Fall die IP-Adresse bekannt gewesen sei und nur noch die dazugehörigen Identitätsdaten des Teilnehmers erfragt worden seien. Im gegenständlichen Fall sei jedoch die IP-Adresse eben nicht bekannt gewesen. Hätte sich das beschwerdegegenständliche Problem im strafprozessualen Verfahren gestellt, wäre dies als Fall des § 149a Abs. 1 Z 1 lit. a StPO qualifiziert worden, da neben dem unbekannten Täter auch der unbekannte Teilnehmeranschluss ermittelt habe werden müssen, der Ursprung der Telekommunikation gewesen sei. Ein- und dieselbe Ermittlungshandlung sei nämlich im strafgerichtlichen Verfahren an das Erfordernis einer richterlichen Anordnung geknüpft und dadurch besonders geschützt, wohingegen an dieselbe

Handlung im Bereich des sicherheitspolizeilichen Verfahrens keine vergleichbaren Schutzanforderungen gestellt würden. Die Datenschutzkommission sei daher davon ausgegangen, dass das Betreiben eines "Chatrooms" nicht als "Telekommunikationsdienst" im Sinne des § 53 Abs. 3a SPG (alte Fassung) anzusehen sei, was nunmehr durch die neue Rechtslage bestätigt werde. Da auch die §§ 16 und 18 ECG keine ausreichenden Grundlagen für die beschwerdegegenständlichen Ermittlungen geliefert hätten, sei auszusprechen gewesen, dass die Ermittlungshandlung gegenüber dem Betreiber von "www.s.at" keine ausreichende Rechtsgrundlage gehabt habe. Die belangte Behörde legte die Verwaltungsakten vor und erstattete eine Gegenschrift, in der sie ausführte, dass "Betreiber eines öffentlichen Telekommunikationsdienstes" gemäß Paragraph 53, Absatz 3 a, SPG (alt) im Sinne des TKG zu verstehen sei. Paragraph 53, Absatz 3 a, SPG sei mit der Novelle Bundesgesetzblatt Teil eins, Nr. 146 aus 1999, eingeführt worden. Der Begriff "Betreiber eines öffentlichen Telekommunikationsdienstes" werde darin ohne nähere Definition verwendet. Das zu diesem Zeitpunkt geltende TKG habe eine gesetzliche Definition dieses Begriffes enthalten und es sei daher angesichts der Einheit der Rechtsordnung davon auszugehen, dass, sofern es für einen im TKG bestimmten Begriff eine abweichende Bedeutung in einem anderen Gesetz geben sollte, dies ausdrücklich festgelegt worden wäre. Die Datenschutzkommission sei im Einklang mit der Literatur davon ausgegangen, dass ein "Chatroom-Betreiber" kein Betreiber eines öffentlichen Telekommunikationsdienstes iSd TKG sei, sondern zu jenen Anbietern von Diensten der Informationsgesellschaft iSd Paragraph 3, Ziffer eins, ECG gehöre, die als "Host-Betreiber" nur dem ECG (Paragraphen 16, ff ECG) unterlägen. Dem Argument, beim "Chatten" im Privatfenster sei es nicht zu einer Speicherung der Inhaltsdaten gekommen, sei entgegenzuhalten, dass die Qualifikation als Betreiber nach dem TKG oder nur nach dem ECG auf Grund des grundsätzlichen Charakters der angebotenen Leistung erfolge. Dies sei eindeutig der Legaldefinition von "Kommunikationsdienst" iSd Paragraph 3, Ziffer 9, TKG 2003 zu entnehmen. Damit ein "Chatroom" als Telekommunikationsdienst einzustufen wäre, dürfte der angebotene Dienst "ganz oder überwiegend" keine inhaltsbezogenen Leistungen erbringen, was allerdings für einen "Chatroom" völlig atypisch wäre. Es fehle ein sachlicher Hinweis, dass der Begriff "Telekommunikationsdienst" im Paragraph 53, Absatz 3 a, SPG (alt) von einer anderen Bedeutung als der Legaldefinition des Paragraph Ziffer 9, TKG 2003 ausgehe. Weiters fehle jeglicher sachlicher Hinweis darauf, dass im Begriff des Telekommunikationsdienstes jemals auch Inhaltsdienste miteingeschlossen gewesen wären, da diese doch eine neuere Entwicklung im Portfolio der Dienstleistungen der Informationsgesellschaft seien. Eine ausdehnende Interpretation von Eingriffsnormen nach dem Utilitätsprinzip, wie vom Beschwerdeführer nunmehr verlangt, mache die Schutzfunktion des Gesetzesvorbehaltes bei Grundrechtseingriffen zunichte. Dass der Gesetzgeber die "Content-Provider" in der beschwerdegegenständlichen Fassung des Paragraph 53, Absatz 3 a, SPG nicht miteingeschlossen habe, werde dadurch bewiesen, dass er die von der Datenschutzkommission aufgezeigte Lücke umgehend durch eine Novellierung des Paragraph 53, Absatz 3 a, SPG mit Bundesgesetzblatt Teil eins, Nr. 114 aus 2007, geschlossen habe, ohne den Ausgang des gegenständlichen Verfahrens abzuwarten. Nunmehr könnten Sicherheitsbehörden ausdrücklich Auskünfte von Betreibern öffentlicher Telekommunikationsdienste (Paragraph 92, Absatz 3, Ziffer eins, TKG 2003) und sonstigen Diensteanbietern (Paragraph 3, Ziffer 2, ECG) verlangen. Bezüglich der zitierten OGH-Entscheidung sei festzuhalten, dass diese auf den vorliegenden Fall nicht übertragbar sei, da in jenem Fall die IP-Adresse bekannt gewesen sei und nur noch die dazugehörigen Identitätsdaten des Teilnehmers erfragt worden seien. Im gegenständlichen Fall sei jedoch die IP-Adresse eben nicht bekannt gewesen. Hätte sich das beschwerdegegenständliche Problem im strafprozessualen Verfahren gestellt, wäre dies als Fall des Paragraph 149 a, Absatz eins, Ziffer eins, Litera a, StPO qualifiziert worden, da neben dem unbekannten Täter auch der unbekannte Teilnehmeranschluss ermittelt habe werden müssen, der Ursprung der Telekommunikation gewesen sei. Ein- und dieselbe Ermittlungshandlung sei nämlich im strafgerichtlichen Verfahren an das Erfordernis einer richterlichen Anordnung geknüpft und dadurch besonders geschützt, wohingegen an dieselbe Handlung im Bereich des sicherheitspolizeilichen Verfahrens keine vergleichbaren Schutzanforderungen gestellt würden. Die Datenschutzkommission sei daher davon ausgegangen, dass das Betreiben eines "Chatrooms" nicht als "Telekommunikationsdienst" im Sinne des Paragraph 53, Absatz 3 a, SPG (alte Fassung) anzusehen sei, was nunmehr durch die neue Rechtslage bestätigt werde. Da auch die Paragraphen 16, und 18 ECG keine ausreichenden Grundlagen für die beschwerdegegenständlichen Ermittlungen geliefert hätten, sei auszusprechen gewesen, dass die Ermittlungshandlung gegenüber dem Betreiber von "www.s.at" keine ausreichende Rechtsgrundlage gehabt habe.

Die belangte Behörde und der Mitbeteiligte beantragten, die Beschwerde als unbegründet abzuweisen.

Der Verwaltungsgerichtshof hat erwogen:

Die vorliegende Amtsbeschwerde stützt sich auf § 91 Abs. 1 Z 2 Sicherheitspolizeigesetz (SPG). Nach dieser Bestimmung kann der Bundesminister für Inneres gegen Entscheidungen der Datenschutzkommission über Beschwerden gemäß § 90 SPG sowohl zugunsten als auch zum Nachteil des Betroffenen Beschwerde wegen Rechtswidrigkeit an den Verwaltungsgerichtshof erheben. Die vorliegende Amtsbeschwerde stützt sich auf Paragraph 91, Absatz eins, Ziffer 2, Sicherheitspolizeigesetz (SPG). Nach dieser Bestimmung kann der Bundesminister für Inneres gegen Entscheidungen der Datenschutzkommission über Beschwerden gemäß Paragraph 90, SPG sowohl zugunsten als auch zum Nachteil des Betroffenen Beschwerde wegen Rechtswidrigkeit an den Verwaltungsgerichtshof erheben.

Nach § 90 SPG entscheidet die Datenschutzkommission gemäß § 31 Datenschutzgesetz 2000 (DSG 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. Nach Paragraph 90, SPG entscheidet die Datenschutzkommission gemäß Paragraph 31, Datenschutzgesetz 2000 (DSG 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.

Gemäß § 31 Abs. 1 DSG 2000 erkennt die Datenschutzkommission 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. Gemäß Paragraph 31, Absatz eins, DSG 2000 erkennt die Datenschutzkommission auf Antrag des Betroffenen über behauptete Verletzungen des Rechtes auf Auskunft gemäß Paragraph 26, durch den Auftraggeber einer Datenanwendung, soweit sich das Auskunftsbegehren nicht auf die Verwendung von Daten für Akte der Gesetzgebung oder der Gerichtsbarkeit bezieht.

Die belangte Behörde hat der Beschwerde des Mitbeteiligten stattgegeben, weil dieser durch die Ermittlungstätigkeit der Sicherheitsbehörde ohne richterlichen Befehl in seinem Recht auf Geheimhaltung nach § 1 Abs. 1 DSG 2000 verletzt wurde. Die belangte Behörde hat der Beschwerde des Mitbeteiligten stattgegeben, weil dieser durch die Ermittlungstätigkeit der Sicherheitsbehörde ohne richterlichen Befehl in seinem Recht auf Geheimhaltung nach Paragraph eins, Absatz eins, DSG 2000 verletzt wurde.

Der angefochtene Bescheid erweist sich auf Grund folgender Erwägungen als frei von Rechtsirrtum:

§ 1 Abs. 1 DSG 2000, BGBl. I Nr. 165/1999, bestimmt, dass "jedermann (...), insbesondere im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten" hat, "soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind". Paragraph eins, Absatz eins, DSG 2000, Bundesgesetzblatt Teil eins, Nr. 165 aus 1999,, bestimmt, dass "jedermann (...), insbesondere im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten" hat, "soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind".

Gemäß Abs. 2 dieser Bestimmung sind Beschränkungen des Anspruches auf Geheimhaltung grundsätzlich nur zur Wahrung überwiegend berechtigter Interessen eines anderen zulässig, und zwar bei Eingriff einer staatlichen Behörde nur auf Grund von Gesetzen und aus den in Art. 8 Abs. 2 EMRK genannten Gründen. Derartige Gesetze dürfen die Verwendung von Daten, die besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jedenfalls nur in der gelindesten, zum Ziel führenden Art vorgenommen werden. Gemäß Absatz 2, dieser Bestimmung sind Beschränkungen des Anspruches auf Geheimhaltung grundsätzlich nur zur Wahrung überwiegend berechtigter Interessen eines anderen zulässig, und zwar bei Eingriff einer staatlichen Behörde nur auf Grund von Gesetzen und aus den in Artikel 8, Absatz 2, EMRK genannten Gründen. Derartige Gesetze dürfen die Verwendung von Daten, die

besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jedenfalls nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.

Die Sicherheitsbehörde ging - insoweit zutreffend - vom Vorliegen eines "gefährlichen Angriffs auf die Sitte" (§ 16 Abs. 2 iVm § 22 Abs. 2 SPG) aus und stützte ihr Auskunftersuchen an den "Chatroom-Betreiber" auf § 53 Abs. 3a SPG (in der hier (noch) anzuwendenden Fassung BGBl. I Nr. 158/2005). Die Sicherheitsbehörde ging - insoweit zutreffend - vom Vorliegen eines "gefährlichen Angriffs auf die Sitte" (Paragraph 16, Absatz 2, in Verbindung mit Paragraph 22, Absatz 2, SPG) aus und stützte ihr Auskunftersuchen an den "Chatroom-Betreiber" auf Paragraph 53, Absatz 3 a, SPG (in der hier (noch) anzuwendenden Fassung Bundesgesetzblatt Teil eins, Nr. 158 aus 2005,).

Die belangte Behörde ging in ihrer Entscheidung davon aus, dass der Eingriff der Sicherheitsbehörde nicht auf Grund des Gesetzes erfolgte.

§ 53 SPG in der im Beschwerdefall maßgeblichen Fassung BGBl. I Nr. 158/2005 hatte folgenden Wortlaut (auszugsweise): Paragraph 53, SPG in der im Beschwerdefall maßgeblichen Fassung Bundesgesetzblatt Teil eins, Nr. 158 aus 2005, hatte folgenden Wortlaut (auszugsweise):

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

...

3. für die Abwehr gefährlicher Angriffe (§§ 16 Abs. 2 und 3 sowie 21 Abs. 2); einschließlich der im Rahmen der Gefahrenabwehr notwendigen Gefahrenforschung (§ 16 Abs. 4 und § 28a); 3. für die Abwehr gefährlicher Angriffe (Paragraphen 16, Absatz 2, und 3 sowie 21 Absatz 2,); einschließlich der im Rahmen der Gefahrenabwehr notwendigen Gefahrenforschung (Paragraph 16, Absatz 4 und Paragraph 28 a,);

...

1. (3a) Absatz 3 a, Die Sicherheitsbehörden sind berechtigt, von den Betreibern öffentlicher Telekommunikationsdienste Auskunft über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses zu verlangen, wenn sie diese Daten als wesentliche Voraussetzung für die Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben benötigen. Die Bezeichnung dieses Anschlusses kann für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder die Abwehr gefährlicher Angriffe auch durch Bezugnahme auf ein von diesem Anschluß geführtes Gespräch durch Bezeichnung des Zeitpunktes und der passiven Teilnehmernummer erfolgen. Die ersuchte Stelle ist verpflichtet, die Auskunft unverzüglich und kostenlos zu erteilen.

..."

Gemäß § 53 Abs. 1 Z 3 SPG dürfen die Sicherheitsbehörden personenbezogene Daten "für die Abwehr gefährlicher Angriffe (iSd § 16 Abs. 2 und 3 sowie § 21 Abs. 2 SPG)" ermitteln und verarbeiten. Gemäß Paragraph 53, Absatz eins, Ziffer 3, SPG dürfen die Sicherheitsbehörden personenbezogene Daten "für die Abwehr gefährlicher Angriffe (iSd Paragraph 16, Absatz 2, und 3 sowie Paragraph 21, Absatz 2, SPG)" ermitteln und verarbeiten.

§ 53 Abs. 3a SPG in der hier anzuwendenden Fassung BGBl. I Nr. 158/2005 berechtigt die Sicherheitsbehörden "von den Betreibern öffentlicher Telekommunikationsdienste Auskunft über Name, Anschrift und Teilnehmernummer eines bestimmten Anschlusses zu verlangen, wenn sie diese Daten als wesentliche Voraussetzung für die Erfüllung der ihnen übertragenen Aufgaben benötigen. Die Bezeichnung dieses Anschlusses kann für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder die Abwehr gefährlicher Angriffe auch durch Bezugnahme auf ein von diesem Anschluss geführtes Gespräch durch Bezeichnung des Zeitpunktes und der passiven Teilnehmernummer erfolgen. Die ersuchte Stelle ist verpflichtet, die Auskunft unverzüglich und kostenlos zu erteilen". (Hervorhebungen durch den Verwaltungsgerichtshof.) Paragraph 53, Absatz 3 a, SPG in der hier anzuwendenden Fassung Bundesgesetzblatt Teil eins, Nr. 158 aus 2005, berechtigt die Sicherheitsbehörden "von den Betreibern öffentlicher Telekommunikationsdienste Auskunft über Name, Anschrift und Teilnehmernummer eines bestimmten Anschlusses zu verlangen, wenn sie diese Daten als wesentliche Voraussetzung für die Erfüllung der ihnen übertragenen Aufgaben benötigen. Die Bezeichnung dieses Anschlusses kann für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder die Abwehr gefährlicher Angriffe auch durch Bezugnahme auf ein von diesem Anschluss geführtes Gespräch

durch Bezeichnung des Zeitpunktes und der passiven Teilnehmernummer erfolgen. Die ersuchte Stelle ist verpflichtet, die Auskunft unverzüglich und kostenlos zu erteilen". (Hervorhebungen durch den Verwaltungsgerichtshof.)

In den Erläuternden Bemerkungen (EB) BlgNR 1479 20. GP zu dieser Bestimmung wird hiezu ausgeführt: In den Erläuternden Bemerkungen (EB) BlgNR 1479 20. Gesetzgebungsperiode zu dieser Bestimmung wird hiezu ausgeführt:

"Bis zur Privatisierung der PTV konnten die Sicherheitsbehörden unter Berufung auf Amtshilfe iSd B-VG Auskünfte etwa über Telefonnummern und Anschlüsse (Stammdaten § 87 Abs. 3 Z 4 TKG) erhalten. ...§ 53 Abs. 3a soll nunmehr jene Stellen, die über Stamm- oder Vermittlungsdaten iSd TKG verfügen, dazu verpflichten, den Sicherheitsbehörden Auskunft über Namen und Adresse und/oder Teilnehmernummer zu erteilen; eine Verpflichtung zur Datenübermittlung darüber hinaus auf Grund dieser Bestimmung ist ausgeschlossen. Der Zugriff auf diese Daten stellt keinen Eingriff in das Fernmeldegeheimnis gemäß Art10a StGG über die allgemeinen Rechte der Staatsbürger dar". "Bis zur Privatisierung der PTV konnten die Sicherheitsbehörden unter Berufung auf Amtshilfe iSd B-VG Auskünfte etwa über Telefonnummern und Anschlüsse (Stammdaten Paragraph 87, Absatz 3, Ziffer 4, TKG) erhalten. ...Paragraph 53, Absatz 3 a, soll nunmehr jene Stellen, die über Stamm- oder Vermittlungsdaten iSd TKG verfügen, dazu verpflichten, den Sicherheitsbehörden Auskunft über Namen und Adresse und/oder Teilnehmernummer zu erteilen; eine Verpflichtung zur Datenübermittlung darüber hinaus auf Grund dieser Bestimmung ist ausgeschlossen. Der Zugriff auf diese Daten stellt keinen Eingriff in das Fernmeldegeheimnis gemäß Art10a StGG über die allgemeinen Rechte der Staatsbürger dar".

Wesentlich ist daher die Frage, wer "Betreiber eines öffentlichen Telekommunikationsdienstes" im Sinne des § 53 Abs. 3a SPG ist. Im SPG wird der Begriff "Betreiber" und "Telekommunikationsdienst" nicht erläutert. Diesbezüglich ist auf die Begriffsbestimmungen des Telekommunikationsgesetzes 2003 (TKG 2003), BGBl. I 2003/70 zurückzugreifen (vgl. hiezu auch Pürstl-Zirnsack, SPG (2005), § 53 Anm 33 und 34, sowie Hauer/Keplinger, Sicherheitspolizeigesetz, 3. Auflage (2005), Seite 601). Wesentlich ist daher die Frage, wer "Betreiber eines öffentlichen Telekommunikationsdienstes" im Sinne des Paragraph 53, Absatz 3 a, SPG ist. Im SPG wird der Begriff "Betreiber" und "Telekommunikationsdienst" nicht erläutert. Diesbezüglich ist auf die Begriffsbestimmungen des Telekommunikationsgesetzes 2003 (TKG 2003), BGBl. römisch eins 2003/70 zurückzugreifen vergleiche , hiezu auch Pürstl-Zirnsack, SPG (2005), Paragraph 53, Anmerkung 33, und 34, sowie Hauer/Keplinger, Sicherheitspolizeigesetz, 3. Auflage (2005), Seite 601).

Nach den Begriffsbestimmungen des § 3 Telekommunikationsgesetz 2003 (TKG) ist Nach den Begriffsbestimmungen des Paragraph 3, Telekommunikationsgesetz 2003 (TKG) ist

1. "Betreiber" ein Unternehmen, das ein öffentliches Kommunikationsnetz oder eine zugehörige Einrichtung bereitstellt, oder zur Bereitstellung hiervon befugt ist;

9. "Kommunikationsdienst" eine gewerbliche Dienstleistung, die ganz oder überwiegend in der Übertragung von Signalen über Kommunikationsnetze besteht, einschließlich Telekommunikations- und Übertragungsdienste in Rundfunknetzen, jedoch ausgenommen Dienste, die Inhalte über Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben. Ausgenommen davon sind Dienste der Informationsgesellschaft im Sinne von § 1 Abs. 1 Z 2 des Notifikationsgesetzes, BGBl. I Nr. 183/1999, die nicht ganz oder überwiegend in der Übertragung von Signalen über Kommunikationsnetze bestehen; 9. "Kommunikationsdienst" eine gewerbliche Dienstleistung, die ganz oder überwiegend in der Übertragung von Signalen über Kommunikationsnetze besteht, einschließlich Telekommunikations- und Übertragungsdienste in Rundfunknetzen, jedoch ausgenommen Dienste, die Inhalte über Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben. Ausgenommen davon sind Dienste der Informationsgesellschaft im Sinne von Paragraph eins, Absatz eins, Ziffer 2, des Notifikationsgesetzes, Bundesgesetzblatt Teil eins, Nr. 183 aus 1999,, die nicht ganz oder überwiegend in der Übertragung von Signalen über Kommunikationsnetze bestehen;

21. "Telekommunikationsdienst" ein Kommunikationsdienst mit Ausnahme von Rundfunk.

Gemäß § 1 Abs. 1 Z 2 Notifikationsgesetz 1999 bedeutet "'Dienst' eine Dienstleistung der Informationsgesellschaft, das ist jede in der Regel gegen Entgelt elektronisch in Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung. Gemäß Paragraph eins, Absatz eins, Ziffer 2, Notifikationsgesetz 1999 bedeutet "'Dienst' eine Dienstleistung der Informationsgesellschaft, das ist jede in der Regel gegen Entgelt elektronisch in Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung,

..." .

§ 3 Z 1 E-Commerce-Gesetz (ECG) definiert Paragraph 3, Ziffer eins, E-Commerce-Gesetz (ECG) definiert

"Dienst der Informationsgesellschaft": ein in der Regel gegen Entgelt elektronisch im Fernabsatz auf individuellen Abruf des Empfängers bereitgestellter Dienst (§ 1 Abs. 1 Z 2 Notifikationsgesetz 1999), insbesondere der Online-Vertrieb von Waren und Dienstleistungen, Online-Informationsangeboten, die Online-Werbung, elektronische Suchmaschinen und Datenabfragemöglichkeiten sowie Dienste, die Informationen über ein elektronisches Netz übermitteln, die den Zugang zu einem solchen vermitteln oder die Informationen eines Nutzers speichern. "Dienst der Informationsgesellschaft": ein in der Regel gegen Entgelt elektronisch im Fernabsatz auf individuellen Abruf des Empfängers bereitgestellter Dienst (Paragraph eins, Absatz eins, Ziffer 2, Notifikationsgesetz 1999), insbesondere der Online-Vertrieb von Waren und Dienstleistungen, Online-Informationsangeboten, die Online-Werbung, elektronische Suchmaschinen und Datenabfragemöglichkeiten sowie Dienste, die Informationen über ein elektronisches Netz übermitteln, die den Zugang zu einem solchen vermitteln oder die Informationen eines Nutzers speichern.

In den Erläuternden Bemerkungen (BlgNR 817 21. GP) zu dieser Bestimmung wird darauf verwiesen, dass die Dienste der Informationsgesellschaft nicht mit Telekommunikationsdiensten verwechselt werden sollten, die in der Übertragung oder Weiterleitung von Signalen auf Telekommunikationsnetzen bestehen. Die Abgrenzung könne freilich in der Praxis auf Grund des Zusammenwachsens verschiedener Technologien schwierig sein. Auch könnten die Anbieter von Diensten der Informationsgesellschaft dem vorgeschlagenen E-Commerce-Gesetz und zugleich dem Telekommunikationsgesetz unterliegen (etwa die Vermittlung des Zugangs durch einen "Access-Provider"). In den Erläuternden Bemerkungen (BlgNR 817 21. Gesetzgebungsperiode zu dieser Bestimmung wird darauf verwiesen, dass die Dienste der Informationsgesellschaft nicht mit Telekommunikationsdiensten verwechselt werden sollten, die in der Übertragung oder Weiterleitung von Signalen auf Telekommunikationsnetzen bestehen. Die Abgrenzung könne freilich in der Praxis auf Grund des Zusammenwachsens verschiedener Technologien schwierig sein. Auch könnten die Anbieter von Diensten der Informationsgesellschaft dem vorgeschlagenen E-Commerce-Gesetz und zugleich dem Telekommunikationsgesetz unterliegen (etwa die Vermittlung des Zugangs durch einen "Access-Provider").

Der Betreiber eines "Chat-Forums" ist als "Host-Provider" im Sinne des § 16 ECG ("Ein Diensteanbieter, der von einem Nutzer eingegebene Informationen speichert") anzusehen. Der "Host-Provider" speichert fremde Daten. Er stellt die Infrastruktur für die Verarbeitung der Informationen zur Verfügung, ohne damit in einem sachlichen Zusammenhang zu stehen oder inhaltlich darauf Einfluss zu nehmen (vgl. OLG Wien vom 03. August 2006, 3 R 10/06x, mit Hinweis auf Zankl, E-Commerce-Gesetz, Rz 222 und 229, sowie die bei Brenn (Hrsg), ECG, Seite 279, wiedergegebenen ErlRV). Der Betreiber eines "Chat-Forums" ist als "Host-Provider" im Sinne des Paragraph 16, ECG ("Ein Diensteanbieter, der von einem Nutzer eingegebene Informationen speichert") anzusehen. Der "Host-Provider" speichert fremde Daten. Er stellt die Infrastruktur für die Verarbeitung der Informationen zur Verfügung, ohne damit in einem sachlichen Zusammenhang zu stehen oder inhaltlich darauf Einfluss zu nehmen vergleiche , OLG Wien vom 03. August 2006, 3 R 10/06x, mit Hinweis auf Zankl, E-Commerce-Gesetz, Rz 222 und 229, sowie die bei Brenn (Hrsg), ECG, Seite 279, wiedergegebenen ErlRV).

Ein "Chatroom" oder "Chat-Forum" ist als ein Dienst der Informationsgesellschaft anzusehen; der Anbieter eines solchen Dienstes ist ein sogenannter "Host-Provider". Dieser bietet den Besuchern seiner Homepage Speichermöglichkeiten an bzw. räumt ihnen die Möglichkeit ein, sich zu den dort wiedergegebenen (eigenen oder fremden) Inhalten zu äußern, häufig in Form von "Postings" - elektronischen Leserbriefen - in Online-Ausgaben von Tageszeitungen (vgl. Zankl, E-Commerce-Gesetz, S.173, Rz 222). In § 16 Abs. 1 ECG wird ein "Host"-Betreiber als "Diensteanbieter, der von einem Nutzer eingegebene Informationen speichert", definiert. Ob die eingegebene Information dauerhaft (wie vor allem bei einer Homepage) oder nur vorübergehend gespeichert wird, ist ohne Bedeutung (vgl. Zankl, a.a.O, S.177, Rz 227). Im Gegensatz dazu vermittelt ein "Access-Provider" lediglich den Zugang zum Internet. Ein "Chatroom" oder "Chat-Forum" ist als ein Dienst der Informationsgesellschaft anzusehen; der Anbieter eines solchen Dienstes ist ein sogenannter "Host-Provider". Dieser bietet den Besuchern seiner Homepage Speichermöglichkeiten an bzw. räumt ihnen die Möglichkeit ein, sich zu den dort wiedergegebenen (eigenen oder fremden) Inhalten zu äußern, häufig in Form von "Postings" - elektronischen Leserbriefen - in Online-Ausgaben von Tageszeitungen vergleiche , Zankl, E-Commerce-Gesetz, S.173, Rz 222). In Paragraph 16, Absatz eins, ECG wird ein "Host"-Betreiber als "Diensteanbieter, der von einem Nutzer eingegebene Informationen speichert", definiert. Ob die

eingeegebene Information dauerhaft (wie vor allem bei einer Homepage) oder nur vorübergehend gespeichert wird, ist ohne Bedeutung vergleiche , Zankl, a.a.O, S.177, Rz 227). Im Gegensatz dazu vermittelt ein "Access-Provider" lediglich den Zugang zum Internet.

Nach den dem Beschwerdefall zu Grunde liegenden Feststellungen bestand die Leistung des "Chatforum-Betreibers" in der Ermöglichung der "Chateilnahme", also in der Zurverfügungstellung einer Software-Plattform, über die ein Austausch von Nachrichten zwischen den "Chateilnehmern" ermöglicht wurde. Nicht oder jedenfalls nicht überwiegend war Gegenstand des Dienstes die Übertragung von Signalen über Kommunikationsnetze. Dafür waren die "Chateilnehmer" auf die Leistungen ihrer jeweiligen Internet-Zugangsanbieter angewiesen. Beim "Chatforum-Betreiber" handelte es sich daher im gegenständlichen Fall nicht um den Betreiber eines (öffentlichen) Telekommunikationsdienstes im Sinne des § 3 Z. 9 und 21 TKG 2003 bzw. des § 53 Abs. 3a SPG idF BGBl I Nr. 158/2005. Nach den dem Beschwerdefall zu Grunde liegenden Feststellungen bestand die Leistung des "Chatforum-Betreibers" in der Ermöglichung der "Chateilnahme", also in der Zurverfügungstellung einer Software-Plattform, über die ein Austausch von Nachrichten zwischen den "Chateilnehmern" ermöglicht wurde. Nicht oder jedenfalls nicht überwiegend war Gegenstand des Dienstes die Übertragung von Signalen über Kommunikationsnetze. Dafür waren die "Chateilnehmer" auf die Leistungen ihrer jeweiligen Internet-Zugangsanbieter angewiesen. Beim "Chatforum-Betreiber" handelte es sich daher im gegenständlichen Fall nicht um den Betreiber eines (öffentlichen) Telekommunikationsdienstes im Sinne des Paragraph 3, Ziffer 9, und 21 TKG 2003 bzw. des Paragraph 53, Absatz 3 a, SPG in der Fassung Bundesgesetzblatt Teil eins, Nr. 158 aus 2005,.

Die Sicherheitsbehörden konnten sich daher im Beschwerdefall für die vom Mitbeteiligten in Beschwerde nach dem DSG 2000 gezogene Abfrage zulässigerweise nicht auf § 53 Abs. 3a SPG in der genannten Fassung stützen. Die Sicherheitsbehörden konnten sich daher im Beschwerdefall für die vom Mitbeteiligten in Beschwerde nach dem DSG 2000 gezogene Abfrage zulässigerweise nicht auf Paragraph 53, Absatz 3 a, SPG in der genannten Fassung stützen.

Der OGH hat sich in seinem Urteil vom 26. Juli 2005, 11 Os 57/05z, mit der hier entscheidungswesentlichen Frage, ob der Anbieter eines "Chatrooms" ein Betreiber eines öffentlichen Telekommunikationsdienstes im Sinne des § 53 Abs. 3a SPG ist, nicht auseinandergesetzt. Auf dieses (vom Beschwerdeführer ins Treffen geführte) Urteil war daher nicht näher einzugehen. Der OGH hat sich in seinem Urteil vom 26. Juli 2005, 11 Os 57/05z, mit der hier entscheidungswesentlichen Frage, ob der Anbieter eines "Chatrooms" ein Betreiber eines öffentlichen Telekommunikationsdienstes im Sinne des Paragraph 53, Absatz 3 a, SPG ist, nicht auseinandergesetzt. Auf dieses (vom Beschwerdeführer ins Treffen geführte) Urteil war daher nicht näher einzugehen.

Ergänzend ist darauf hinzuweisen, dass es sich bei einer dynamischen IP-Adresse wie im Beschwerdefall nicht um ein "Stammdatum" wie den Namen oder die Adresse, sondern um ein sogenanntes "Verkehrsdatum" im Sinne des § 92 Abs. 3 Z 4 TKG handelt, das zum Zweck der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zweck der Fakturierung dieses Vorgangs verarbeitet wird. Verkehrsdaten unterliegen dem Fernmeldegeheimnis des Art 10a StGG und Art 8 EMRK und daher dem Richtervorbehalt (vgl. den Vorabentscheidungsbeschluss des OGH vom 13. November 2007, 4 Ob 141/07z, sowie den hiezu ergangenen Beschluss des EuGH vom 19. Februar 2009, C-557/07). Ergänzend ist darauf hinzuweisen, dass es sich bei einer dynamischen IP-Adresse wie im Beschwerdefall nicht um ein "Stammdatum" wie den Namen oder die Adresse, sondern um ein sogenanntes "Verkehrsdatum" im Sinne des Paragraph 92, Absatz 3, Ziffer 4, TKG handelt, das zum Zweck der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zweck der Fakturierung dieses Vorgangs verarbeitet wird. Verkehrsdaten unterliegen dem Fernmeldegeheimnis des Artikel 10 a, StGG und Artikel 8, EMRK und daher dem Richtervorbehalt vergleiche , den Vorabentscheidungsbeschluss des OGH vom 13. November 2007, 4 Ob 141/07z, sowie den hiezu ergangenen Beschluss des EuGH vom 19. Februar 2009, C-557/07).

Aus diesen Gründen war daher die Beschwerde gemäß § 42 Abs. 1 VwGG abzuweisen. Aus diesen Gründen war daher die Beschwerde gemäß Paragraph 42, Absatz eins, VwGG abzuweisen.

Der Ausspruch über den Kostenersatz gründet sich auf die §§ 47 ff in Verbindung mit der Verordnung BGBl. II Nr. 455/2008. Die belangte Behörde hat keinen Aufwandsatz angesprochen. Der Ausspruch über den Kostenersatz gründet sich auf die Paragraphen 47, ff in Verbindung mit der Verordnung Bundesgesetzblatt Teil 2, Nr. 455 aus 2008,. Die belangte Behörde hat keinen Aufwandsatz angesprochen.

Wien, am 27. Mai 2009

Schlagworte

Definition von Begriffen mit allgemeiner Bedeutung VwRallg7

European Case Law Identifier (ECLI)

ECLI:AT:VWGH:2009:2007050280.X00

Im RIS seit

01.07.2009

Zuletzt aktualisiert am

31.07.2009

Quelle: Verwaltungsgerichtshof VwGH, <http://www.vwgh.gv.at>

© 2026 JUSLINE

JUSLINE® ist eine Marke der ADVOKAT Unternehmensberatung Greiter & Greiter GmbH.

www.jusline.at