-DOKNR-
DSKTE/20071003/K121279/0017-DSK/2007/00
-KINFO-
TE Datenschutzkommission Bescheid Beschwerde 2007/07/20
K121.279/0017-DSK/2007
-TYP-
Bescheid Beschwerde
-DATUM-
2007/07/20
-GZ-
K121.279/0017-DSK/2007
-NORM-
DSG 2000 §1 Abs1;
DSG 2000 §1 Abs2;
DSG 2000 §1 Abs5;
DSG 2000 §31 Abs1;
DSG 2000 §31 Abs2;
SPG §16 Abs2;
SPG §22 Abs1;
SPG §22 Abs2;
SPG §22 Abs3;
SPG §28a;
SPG §52;
SPG §53 Abs1;
SPG §53 Abs3a;
StGB §212 Abs1;
StGB §213;
ECG §16;
ECG §18 Abs1;
ECG §18 Abs2;
ECG §18 Abs3;
TKG 1997 §3 Z14;
TKG 2003 §3 Z9;
-TEXT-
[Anmerkung Bearbeiter: Namen (Firmen), (Internet-)Adressen, Aktenzahlen (und dergleichen), Rechtsformen und Produktbezeichnungen etc. sowie deren Initialen und Abkürzungen können aus Anonymisierungsgründen abgekürzt und/oder verändert sein.]

B E S C H E I D

Die Datenschutzkommission hat unter dem Vorsitz von Dr. KURAS und in Anwesenheit der Mitglieder Mag. MAITZ-STRASSNIG, Dr. KOTSCHY, Mag. HEILEGGER, Dr. HEISSENBERGER und Dr. BLAHA sowie des Schriftführers Dr. KÖNIG in ihrer Sitzung vom 3. Oktober 2007 folgenden Beschluss gefasst:

S p r u c h

Über die Beschwerde des Isidor H*** (Beschwerdeführer), vertreten durch ***, vom 19. Februar 2007

- gegen die Sicherheitsdirektion für das Bundesland Steiermark (Erst-Beschwerdegegnerin) wegen der Verletzung im Recht auf Geheimhaltung schutzwürdiger personenbezogener Daten durch unzulässige Datenermittlung und Verarbeitung,
- gegen Norbert Q*** (Zweit- Beschwerdegegner) wegen Verletzung seiner Pflichten als Auftraggeber der Datenanwendung www.***.at durch Verletzung im Recht auf Geheimhaltung schutzwürdiger personenbezogener Daten durch unzulässige Datenübermittlung sowie
- gegen die T*** AG, Deutschland (Dritt- Beschwerdegegnerin) wegen Verletzung ihrer Pflichten als Auftraggeber oder Dienstleister der Datenanwendung www.***.at durch Verletzung im Recht auf Geheimhaltung schutzwürdiger personenbezogener Daten durch unzulässige Datenübermittlung

wird gemäß den §§ 1 Abs. 1, 2 und 5, 4 Z.10, und 31 Abs. 2 Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999 idF BGBl. I Nr.13/2005, iVm §§ 16 und 18 Abs. 2 und 3 des E-Commerce-Gesetzes (ECG), BGBl I Nr. 152/2001 und §§ 16 Abs. 2, 21 Abs. 2, 22 Abs. 2, 28a Abs. 3, 52 und § 53 Abs. 1 und 3a des Sicherheitspolizeigesetzes (SPG), BGBl Nr. 566/1991 idF BGBl I Nr. 158/2005, sowie § 3 Telekommunikationsgesetz (TKG), BGBl. I Nr. 100/1997, und § 3 Telekommunikationsgesetz 2003 (TKG 2003), BGBl. I Nr. 70/2003, wie folgt entschieden:

1. Die gegen den Zweit- und Dritt-Beschwerdegegner gerichtete Beschwerde wird z u r ü c k g e w i e s e n.

2. Im Übrigen wird der Beschwerde s t a t t g e g e b e n.

<u>A) Vorbringen der Beteiligten</u>

In seiner nicht ausdrücklich auf § 31 DSG 2000 gestützten Beschwerde bringt der Beschwerdeführer vor, dass er sich durch den folgenden Vorgang im Recht auf Geheimhaltung verletzt erachtet: Er habe sich im Oktober 2006 im Chatroom von www.***.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. Aufgrund einer Anzeige dieses zufälligen Chatpartners - der die Äußerungen beim Chat für real gehalten hatte - bei der Polizeiinspektion Trofaiach habe das Landeskriminalamt des Landespolizeikommandos Steiermark beim Zweit-Beschwerdegegner die IP-Adresse anhand des ‚nickname' telefonisch erfragt und anhand des öffentlichen Verzeichnisses der RIPE (réseaux IP européens) den Internetaccessprovider ausfindig gemacht, der diese IP-Adresse vergeben hatte. Dieser habe den Beschwerdeführer als Nutzer dieser IP-Adresse identifiziert. Für die Ermittlung und Verarbeitung seiner IP-Adresse durch den Erst-Beschwerdegegner sowie die Beauskunftung derselben durch den Zweit- und Dritt-

Beschwerdegegner (ohne Gerichtsbeschluss) gebe es keine taugliche Rechtsgrundlage. Die Datenermittlung durch die drei Beschwerdegegner sei daher rechtswidrig gewesen.

Die Erst-Beschwerdegegnerin bestätigte die in der Beschwerde angegebene Sachverhaltsdarstellung und ergänzte diese mit der Angabe, dass der Beschwerdeführer (der sich als Frau ausgegeben hatte) am 31. Oktober 2006 um ca. 22h50 dem zufälligen Chatpartner im Chatverkehr seine 9-jährige Tochter für sexuelle Handlungen angeboten und sinngemäß angegeben habe, seine Tochter auch schon selbst missbraucht zu haben.

Die Identität des Beschwerdeführers sei durch Anfrage beim Betreiber der Website www.***.at und der T*** AG und letztlich beim Accessprovider *** ermittelt worden, wobei Rechtsgrundlage hiefür § 53 Abs 3a SPG gewesen sei.

Der Zweit-Beschwerdegegner bestätigte diese Sachverhaltsdarstellung und ergänzte sie mit der Angabe, dass der Dritt-Beschwerdegegner sein Dienstleister beim Betreiben des Chatrooms sei.

<u>B) Beschwerdegegenstand</u>

Aus dem Beschwerdevorbringen ergibt sich, dass Beschwerdegegenstand die Frage ist, ob der Beschwerdeführer bei der Ermittlung seiner Identität im Wege der Ausforschung einer ihm zu einem bestimmten Zeitpunkt zugeordneten IP-Adresse - dies insbesondere ohne Vorliegen eines richterlichen Überwachungsbeschlusses nach § 149b StPO - in seinem Recht auf Geheimhaltung nach § 1 Abs. 1 DSG 2000 verletzt wurde.

<u>C) Sachverhaltsfeststellung samt Beweiswürdigung</u>

Für die Datenschutzkommission steht folgender Sachverhalt fest:

Der Beschwerdeführer hat im Oktober 2006 in einem Privatfenster des unter der Adresse www.***.at im Internet zur Verfügung gestellten Chatrooms mit einem Unbekannten kommuniziert, wobei er ein Pseudonym (‚nickname') verwendet hat. Aus der Eingangswebseite des Dienstes www.***.at wird deutlich, dass hier mehr als bloße Nachrichtenübertragung angeboten wird, nämlich Spiele, Blinddate, Tagebuch, Diskussionsforum, Friendslist u.v.m.

Für die Benutzung des Chatrooms ist es nicht erforderlich, eine Identität registrieren zu lassen, doch hat der Nutzer beim Einloggen (irgend)eine Bezeichnung für sich selbst einzutragen - im vorliegenden Fall war dies der bereits zitierte ‚nickname'. Der Inhalt der Kommunikation hat beim Kommunikationspartner den Eindruck erweckt, dass strafbare

sexuelle Handlungen bereits begangen worden waren und dass die Gefahr weiterer solcher Handlungen an einer Minderjährigen bestehe. Er hat daher Anzeige bei der örtlichen Polizeiinspektion erstattet, die zu Ermittlungen des Landeskriminalamts des Landespolizeikommandos Steiermark geführt hat. Das Landeskriminalamt (Organ des Erst-Beschwerdegegners) hat beim Zweit-Beschwerdegegner, dem Chatroom-Betreiber, telefonisch um „die Aushebung des gegenüber dem Chatpartner angegebenen ‚nickname' ersucht" (siehe Äußerung des Erst-Beschwerdegegners im Ermittlungsverfahren).

In Beantwortung dieses Ersuchens hat der Zweit-Beschwerdegegner eine IP-Adresse bekannt gegeben, die dem Benutzer des ‚nickname' im Zeitpunkt der inkriminierten Kommunikation zugeordnet war. Mit Hilfe dieser IP-Adresse wurden beim zuständigen Internetaccessprovider schließlich Name und Adresse des Benutzers dieser IP-Adresse ausfindig gemacht.

Der Zweit-Beschwerdegegner bedient sich des Dritt-Beschwerdegegners, eines in Deutschland ansässigen Unternehmens, um www.***.at im Internet anzubieten.

<u>Beweiswürdigung:</u> Diese Feststellungen stützen sich auf die übereinstimmenden und unstrittigen Vorbringen der Parteien dieses Verfahrens bzw. auf die Einsicht der Behörde im Internet in die Website des in Rede stehenden Chatrooms.

<u>D) Rechtliche Beurteilung</u>

<u>1. Anzuwendende Rechtsvorschriften:</u>

Die Verfassungsbestimmungen des § 1 Abs. 1, 2 und 5 des Datenschutzgesetz 2000 (DSG 2000) lauten unter der Überschrift „Grundrecht auf Datenschutz":
„§ 1. (1) Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungs¬anspruch nicht zugänglich sind.
(2) Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutze

der Menschenrechte und Grundfreiheiten (EMRK), BGBl. Nr. 210/1958, genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach 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 jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.
[…]
(5) Gegen Rechtsträger, die in Formen des Privatrechts eingerichtet sind, ist, soweit sie nicht in Vollziehung der Gesetze tätig werden, das Grundrecht auf Datenschutz mit Ausnahme des Rechtes auf Auskunft auf dem Zivilrechtsweg geltend zu machen. In allen übrigen Fällen ist die Datenschutzkommission zur Entscheidung zuständig, es sei denn, daß Akte der Gesetzgebung oder der Gerichtsbarkeit betroffen sind."

§ 31 Abs. 1 und 2 DSG 2000 lauten unter der Überschrift „Beschwerde an die Datenschutzkommission":
„§ 31. (1) Die Datenschutzkommission erkennt auf Antrag des Betroffenen über behauptete Verletzungen des Rechtes auf Auskunft gemäß § 26 durch den Auftraggeber einer Datenanwendung, soweit sich das Auskunftsbegehren nicht auf die Verwendung von Daten für Akte der Gesetzgebung oder der Gerichtsbarkeit bezieht.
(2) Zur Entscheidung über behauptete Verletzungen der Rechte eines Betroffenen auf Geheimhaltung, auf Richtigstellung oder auf Löschung nach diesem Bundesgesetz ist die Datenschutzkommission dann zuständig, wenn der Betroffene seine Beschwerde gegen einen Auftraggeber des öffentlichen Bereichs richtet, der nicht als Organ der Gesetzgebung oder der Gerichtsbarkeit tätig ist."

§ 16 Abs. 2 des Sicherheitspolizeigesetzes (SPG) lautet unter der Überschrift „Begriffsbestimmungen, Allgemeine Gefahr; gefährlicher Angriff; Gefahrenerforschung":
„(2) Ein gefährlicher Angriff ist die Bedrohung eines Rechtsgutes durch die rechtswidrige Verwirklichung des Tatbestandes einer gerichtlich strafbaren Handlung, die vorsätzlich begangen und nicht bloß auf Begehren eines Beteiligten verfolgt wird, sofern es sich um einen Straftatbestand
1. nach dem Strafgesetzbuch (StGB), BGBl. Nr. 60/1974, ausgenommen die Tatbestände nach den §§ 278, 278a und 278b StGB, oder
2. nach dem Verbotsgesetz, StGBl. Nr. 13/1945, oder
3. nach dem Fremdenpolizeigesetz 2005 (FPG), BGBl. I Nr. 100, oder
4. nach dem Suchtmittelgesetz (SMG), BGBl. I Nr. 112/1997,

handelt, es sei denn um den Erwerb oder Besitz eines Suchtmittels zum eigenen Gebrauch."

§ 22 Abs. 1, 2 und 3 SPG lautet unter der Überschrift „Vorbeugender Schutz von Rechtsgütern":
„§ 22. (1) Den Sicherheitsbehörden obliegt der besondere Schutz
1. von Menschen, die tatsächlich hilflos sind und sich deshalb nicht selbst ausreichend vor gefährlichen Angriffen zu schützen vermögen;
[...]
(2) Die Sicherheitsbehörden haben gefährlichen Angriffen auf Leben, Gesundheit, Freiheit, Sittlichkeit, Vermögen oder Umwelt vorzubeugen, sofern solche Angriffe wahrscheinlich sind.
(3) Nach einem gefährlichen Angriff haben die Sicherheitsbehörden, unbeschadet ihrer Aufgaben nach der Strafprozeßordnung 1975 (StPO), BGBl. Nr. 631/1975, die maßgebenden Umstände, einschließlich der Identität des dafür Verantwortlichen, zu klären, soweit dies zur Vorbeugung weiterer gefährlicher Angriffe erforderlich ist. Sobald ein bestimmter Mensch der strafbaren Handlung verdächtig ist, gelten ausschließlich die Bestimmungen der StPO; die §§ 57 und 58 sowie die Bestimmungen über den Erkennungsdienst bleiben jedoch unberührt."

§ 28a SPG lautet unter der Überschrift „Sicherheitspolizeiliche Aufgabenerfüllung":
„§ 28a. (1) Wenn bestimmte Tatsachen die Annahme einer Gefahrensituation rechtfertigen, obliegt den Sicherheitsbehörden, soweit ihnen die Abwehr solcher Gefahren aufgetragen ist, die Gefahrenerforschung.
(2) Die Sicherheitsbehörden und die Organe des öffentlichen Sicherheitsdienstes dürfen zur Erfüllung der ihnen in diesem Bundesgesetz übertragenen Aufgaben alle rechtlich zulässigen Mittel einsetzen, die nicht in die Rechte eines Menschen eingreifen.
(3) In die Rechte eines Menschen dürfen sie bei der Erfüllung dieser Aufgaben nur dann eingreifen, wenn eine solche Befugnis in diesem Bundesgesetz vorgesehen ist und wenn entweder andere Mittel zur Erfüllung dieser Aufgaben nicht ausreichen oder wenn der Einsatz anderer Mittel außer Verhältnis zum sonst gebotenen Eingriff steht."

§ 52 SPG lautet unter der Überschrift „2. Hauptstück: Ermittlungsdienst: - Aufgabenbezogenheit":
„ § 52. Personenbezogene Daten dürfen von den Sicherheitsbehörden gemäß diesem Hauptstück nur verwendet werden, soweit dies zur Erfüllung der ihnen übertragenen Aufgaben erforderlich ist. Ermächtigungen nach anderen Bundesgesetzen bleiben unberührt."

§ 53 Abs. 1 sowie Abs. 3a des SPG lautet unter der Überschrift „Zulässigkeit der Verarbeitung":
„§ 53. (1) Die Sicherheitsbehörden dürfen personenbezogene Daten ermitteln und weiterverarbeiten

1. für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht (§ 19);
2. für die Abwehr krimineller Verbindungen (§§ 16 Abs. 1 Z 2 und 21);
2a. für die erweiterte Gefahrenerforschung (§ 21 Abs. 3) unter den Voraussetzungen des § 91c Abs. 3;
3. für die Abwehr gefährlicher Angriffe (§§ 16 Abs. 2 und 3 sowie 21 Abs. 2); einschließlich der im Rahmen der Gefahrenabwehr notwendigen Gefahrenerforschung (§ 16 Abs. 4 und § 28a);
4. für die Vorbeugung wahrscheinlicher gefährlicher Angriffe gegen Leben, Gesundheit, Sittlichkeit, Freiheit, Vermögen oder Umwelt (§ 22 Abs. 2 und 3) oder für die Vorbeugung gefährlicher Angriffe mittels Kriminalitätsanalyse, wenn nach der Art des Angriffes eine wiederholte Begehung wahrscheinlich ist;

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

§ 212 Abs. 1 des Strafgesetzbuches (StGB) lautet unter der Überschrift „Mißbrauch eines Autoritätsverhältnisses":
„§ 212. (1) Wer

1. mit einer mit ihm in absteigender Linie verwandten minderjährigen Person, seinem minderjährigen Wahlkind, Stiefkind oder Mündel oder
2. mit einer minderjährigen Person, die seiner Erziehung, Ausbildung oder Aufsicht untersteht, unter Ausnützung seiner Stellung gegenüber dieser Person

eine geschlechtliche Handlung vornimmt oder von einer solchen Person an sich vornehmen lässt oder, um sich oder einen Dritten geschlechtlich zu erregen oder zu befriedigen, dazu verleitet, eine geschlechtliche Handlung an sich selbst vorzunehmen, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen."

§ 213 des Strafgesetzbuches (StGB) lautet unter der Überschrift Kuppelei:
„§ 213. (1) Wer eine Person, zu der er in einem der im § 212 bezeichneten Verhältnisse steht, unter den dort genannten Voraussetzungen zu einer geschlechtlichen Handlung mit einer anderen Person verleitet oder die persönliche Annäherung der beiden Personen zur Vornahme einer geschlechtlichen Handlung herbeiführt, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.
(2) Handelt der Täter, um sich oder einem anderen einen Vermögensvorteil zu verschaffen, so ist er mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen."

§ 16 des E-Commercegesetz (ECG) lautet unter der Überschrift „Ausschluss der Verantwortlichkeit bei Speicherung fremder Inhalte (Hosting)"
„§ 16. (1) Ein Diensteanbieter, der von einem Nutzer eingegebene Informationen speichert, ist für die im Auftrag eines Nutzers gespeicherten Informationen nicht verantwortlich, sofern er
1. von einer rechtswidrigen Tätigkeit oder Information keine tatsächliche Kenntnis hat und sich in Bezug auf Schadenersatzansprüche auch keiner Tatsachen oder Umstände bewusst ist, aus denen eine rechtswidrige Tätigkeit oder Information offensichtlich wird, oder,
2. sobald er diese Kenntnis oder dieses Bewusstsein erhalten hat, unverzüglich tätig wird, um die Information zu entfernen oder den Zugang zu ihr zu sperren.
(2) Abs. 1 ist nicht anzuwenden, wenn der Nutzer dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird."

§ 18 Abs 1, 2 und 3 des ECG lautet unter der Überschrift „Umfang der Pflichten der Diensteanbieter":
„§ 18. (1) Die in den §§ 13 bis 17 genannten Diensteanbieter sind nicht verpflichtet, die von ihnen gespeicherten, übermittelten oder zugänglich gemachten Informationen allgemein zu überwachen oder von sich aus nach Umständen zu forschen, die auf rechtswidrige Tätigkeiten hinweisen.
(2) Die in den §§ 13 und 16 genannten Diensteanbieter haben auf Grund der Anordnung eines dazu gesetzlich befugten inländischen Gerichtes diesem alle Informationen zu übermitteln, an Hand deren die Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Übermittlung oder Speicherung von Informationen abgeschlossen haben, zur Verhütung, Ermittlung, Aufklärung oder Verfolgung gerichtlich strafbarer Handlungen ermittelt werden können.
(3) Die in § 16 genannten Diensteanbieter haben auf Grund der Anordnung einer Verwaltungsbehörde dieser den Namen und die Adresse der Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Speicherung von Informationen abgeschlossen haben, zu übermitteln, sofern die Kenntnis

dieser Informationen eine wesentliche Voraussetzung der Wahrnehmung der der Behörde übertragenen Aufgaben bildet."

§ 3 Z 14 des Telekommunikationsgesetzes (TKG), BGBl. Nr. 100/1997 lautet:
„14. „Telekommunikationsdienst": eine gewerbliche Dienstleistung, die in der Übertragung und/oder Weiterleitung von Signalen auf Telekommunikationsnetzen besteht, einschließlich des Angebots von Mietleitungen; nicht darunter fällt insbesondere der bloße Wiederverkauf (Handel mit) von Telekommunikationsleistungen sowie die Übertragung von Rundfunk und Fernsehrundfunk durch Inhaber von Gemeinschaftsantennenanlagen (Kabelnetzbetreiber);"

§ 3 Z 9 des Telekommunikationsgesetzes 2003 (TKG 2003) lautet:
"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;"

<u>2. Anwendung auf den Beschwerdefall:</u>

Zum Spruchpunkt 1: Zuständigkeit der Datenschutzkommission

Gemäß § 1 Abs 5 und § 31 Abs 2 DSG 2000 ist die Datenschutzkommission für Beschwerden zuständig, die sich gegen Auftraggeber des öffentlichen Bereichs richten. Das Grundrecht auf Datenschutz ist gegen Rechtsträger, die in Formen des Privatrechts eingerichtet sind, auf dem Zivilrechtsweg geltend zu machen. Die Beschwerde gegen die Internetserviceprovider (Zweit- und Dritt-Beschwerdegegner) war daher wegen Unzuständigkeit der Datenschutzkommission zurückzuweisen.

Die Frage der örtlichen Zuständigkeit der Datenschutzkommission für die beschwerdegegenständlichen Handlungen des in Deutschland ansässigen Dritt-Beschwerdegegners konnte daher im vorliegenden Verfahren außer Betracht bleiben.

Zum Spruchpunkt 2: Zulässigkeit der Datenverarbeitung durch die Sicherheitsdirektion für das Bundesland Steiermark (Erst-Beschwerdegegnerin)

Der Beschwerdeführer sieht die Verletzung im Recht auf Geheimhaltung dadurch bewirkt, dass die Erst-Beschwerdegegnerin ihn als Urheber einer bestimmten Kommunikation in einem Chatroom im Internet ohne Vorliegen eines diesbezüglichen richterlichen Befehls ausgeforscht hat.

Die Erst-Beschwerdegegnerin hat demgegenüber ins Treffen geführt, dass ein solcher richterlicher Beschluss nicht erforderlich gewesen sei, da sie gemäß § 16 Abs. 2 und 3 und § 21 Abs. 2 SPG zur Abwehr bzw. Beendigung eines gefährlichen Angriffs und weiters gemäß § 22 Abs. 2 und 3 SPG zum Zweck der Aufklärung einer strafbaren Handlung zu den beschwerdegegenständlichen Ermittlungshandlungen verpflichtet war. Überdies stelle „der Zugriff auf diese Daten keinen Eingriff in das Fernmeldegeheimnis dar - siehe dazu: RV 1497 XX.GP (zu § 53 Abs. 3a)."

Zu Letzterem ist allerdings auf folgende Ausführungen im Ausschussbericht zur SPG-Novelle 1999 (2023 der Beil. XX. GP) zu § 53 Abs. 3a hinzuweisen:
„Die Weitergabe nicht nur von Stamm-, sondern vor allem von Vermittlungsdaten ist jedoch ein Eingriff in das verfassungsrechtlich geschützte Fernmeldegeheimnis (Art. 10a Staatsgrundgesetz). Außerdem würden die Auskünfte über Vermittlungsdaten nicht nur Namen und Anschrift eines Anschlusses erfassen, sondern - im Falle befürchteter „gefährlicher Angriffe" - auch Auskünfte über „äußere Rufdaten" (Wer hat von welchen Anschluss wann und mit welchen Anschlüssen Telefongespräche geführt?). Das allerdings wäre ein gravierender Eingriff in das Privatleben (Art. 8 MRK) und das Grundrecht auf Datenschutz (§ Abs. 1 DSG), da man dadurch den Aufenthaltsort von Gesprächspartnern (auch „Bewegungsbild") ableiten könnte. Nach § 87 Abs. 3 Z 5 TKG können durch „Vermittlungsdaten" auch umfassende Informationen über das Privatleben der Betroffenen weitergegeben werden (Interpretation Datenschutzrat), was der EMRK widerspräche."

Der Auffassung, dass die Ermittlung jenes Anschlusses und seines Inhabers, der Ursprung einer Telekommunikation war (- oft auch als „Rufdatenrückerfassung" bezeichnet -), kein grundrechtsnaher Sachverhalt wäre, kann sich die Datenschutzkommission jedenfalls nicht anschließen; ob Art. 10a StGG auch „äußere Gesprächsdaten", d.h. die „Verbindungs-„ oder „Verkehrsdaten" schützt, ist zwar strittig, doch ist festzuhalten, dass die grundsätzliche Vertraulichkeit von Kommunikationen zwischen bestimmten Personen gegenüber Dritten sich anerkanntermaßen nicht nur auf den Inhalt, sondern auch auf die Verkehrsdaten erstreckt (vgl. Art. 5 der RL 58/2002 und das Kommunikationsgeheimnis nach § 93 TKG, das zwar nicht selbst in Verfassungsrang steht, aber jedenfalls als Ausfluss des Art. 8 EMRK und des Grundrechts auf Datenschutz im

Telekommunikationsbereich zu sehen ist). Die Ermittlung solcher Daten greift daher iSd § 28a Abs. 3 SPG in Rechte von Betroffenen ein und ist daher ohne besondere Befugnis der Sicherheitsbehörden nicht zulässig.

Daraus folgt, dass § 53 Abs. 1 SPG allein keine ausreichende Rechtsgrundlage für die Ermittlung von Verkehrsdaten darstellen kann, sondern hiefür der Umfang besonderer Eingriffsbefugnisse maßgeblich ist, die den Sicherheitsbehörden nach dem Sicherheitspolizeigesetz oder anderen Gesetzen eingeräumt sind. Die Erst-Beschwerdegegnerin hat dazu Folgendes ausgeführt:
„Die Ermittlung und Verarbeitung der IP-Adresse erfolgte gemäß § 53 Abs. 1 mit dem Ziel der Abwehr bzw. Beendigung eines gefährlichen Angriffs (Abs. 1 Z 3 leg.cit). Die Datenabfrage selbst erfolgte gemäß § 53 Abs. 3a SPG, da diese für die Abwehr des gefährlichen Angriffs notwendig (unerlässlich) war."

§ 53 Abs. 3a SPG ermächtigt die Sicherheitsbehörden, Auskünfte über „Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses" von Betreibern öffentlicher Telekommunikationsdienste zu verlangen - ein Telekommunikationsdienst ist eine gewerbliche Dienstleistung, die in der Übertragung und/oder Weiterleitung von Signalen auf Telekommunikationsnetzen besteht (§ 3 Z 14 TKG; im Wesentlichen gleichlautend § 3 Z 9 und 21 TKG 2003).

Bezogen auf den Beschwerdegegenstand ist somit zunächst die Frage zu beantworten, ob der Betreiber eines Chatrooms „Betreiber eines öffentlichen Telekommunikationsdienstes" ist: In der Literatur wird der Betrieb eines Chatrooms regelmäßig als ein solcher Dienst der Informationsgesellschaft angesehen, der nur dem ECG - und nicht auch dem TKG - unterliegt, der also kein „(Tele)Kommunikationsdienst" im Sinne des § 3 Z 14 TKG bzw. § 3 Z 9 TKG 2003 ist. So z.B. Zankl, Kommentar zum E-Commerce-Gesetz, der in RZ 222 (zu § 16 E-Commerce-Gesetz - ECG, BGBl. I Nr. 152/2001), der das Betreiben eines Chatforums ausdrücklich als Fall des „Hosting" bezeichnet: „Entscheidend ist jedenfalls der Speichervorgang, durch den sich der Host- vom Access-Provider unterscheidet. Wird z.B. ein SMS-Dienst mit der Möglichkeit angeboten, die gesendeten und/oder empfangenen Nachrichten zu speichern - wie dies beim Mobilfunkdienst gewöhnlich der Fall ist -, so liegt Hostproviding vor und es gilt § 16." Auch Laga/Sehrschön/ Ciresa, E-Commerce Gesetz, § 3 ECG, S 18, nennen Forenbetreiber als Beispiel für Diensteanbieter nach ECG - im Gegensatz zu jenen „Diensten der Informationsgesellschaft", die auch dem TKG unterliegen.

Die Sachverhaltsermittlungen haben ergeben, dass der Dienst „www.***.at" inhaltliche Leistungen anbietet (so die

Darstellung der angebotenen Leistungen auf der Einstiegswebsite des Chatrooms). Der Umstand, dass das Chatten im Privatfenster regelmäßig nicht gespeichert wird, hat nichts mit der technischen Natur des Dienstes zu tun, sondern stellt nur eine Ausnahme, eine spezielles Angebot dar, wonach auch vollkommen „vertraulich" gechattet werden kann.

Aber auch wenn man davon ausginge, dass es sich im gegenständlichen Fall um einen Telekommunikationsdienst im Sinne des § 53 Abs 3a SPG handelte, wäre die Ermittlung der IP-Adresse - wie im vorliegenden Sachverhalt erfolgt - nicht durch diese Bestimmung gedeckt:

§ 53 Abs. 3a SPG umfasst mehrere unterschiedliche Fälle. Neben der Bekanntgabe z.B. einer Telefonnummer eines namentlich bezeichneten Teilnehmers betrifft diese Bestimmung auch die Auskunft über die Identität des Teilnehmers eines mit Hilfe der Teilnehmernummer bezeichneten Anschlusses. Darüber hinaus bestimmt der zweite Satz des § 53 Abs. 3a SPG aber, dass der Betreiber auch Auskunft über die Identität des Inhabers eines nicht bekannten Anschlusses zu geben hat, wenn ihm zur Bestimmung des noch unbekannten Anschlusses die Teilnehmernummer des anderen Kommunikationspartners (also die passive Teilnehmernummer) zur Verfügung gestellt wird (samt dem Gesprächszeitpunkt). Diese letztere Auskunftsverpflichtung hat insofern eine andere Dimension als die sonstigen Fälle des § 53 Abs. 3a SPG, als sie die Auswertung von Verkehrsdaten notwendig macht. Derselbe Vorgang wird in der StPO mit „Feststellung des Ursprungs einer Telekommunikation" bezeichnet und es wird seine Zulässigkeit in der StPO 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 Rufdatenrückerfassung zusteht, ist nach Auffassung der Datenschutzkommission nur eine restriktive und am Wortlaut der Bestimmung orientierte Auslegung angemessen.

Nach dem allenfalls am ehesten als Grundlage der beschwerdegegenständlichen Auskunft in Frage kommenden Satz 2 des § 53 Abs 3a SPG kann eine solche - wie oben ausgeführt - gegenüber dem Betreiber nach dem Wortlaut der Bestimmung dann verlangt werden, wenn die Sicherheitsbehörde dem Betreiber des öffentlichen Telekommunikationsdienstes den (ungefähren) Zeitpunkt des Gespräches und die passive Teilnehmernummer einer Verbindung bekannt gibt, um dann die entsprechende aktive Teilnehmernummer und den Inhaber dieses Anschlusses zu erfahren. Die Bestimmung stellt ausdrücklich auf ein von einem Anschluss aus geführtes „Gespräch" ab. Abgesehen davon, dass die Bestimmung dadurch offenbar lediglich auf Sprachtelefonie zugeschnitten ist, sind auch die sonstigen Voraussetzungen für

die Zulässigkeit der Rufdatenrückerfassung im vorliegenden Fall nicht vorgelegen. Die Erhebung ist keinesfalls auf Basis einer passiven Teilnehmernummer erfolgt. Der Betreiber des Chatforums wurde vielmehr nach den Ausführungen der Erst-Beschwerdegegnerin um „Aushebung" des vom anzeigenden Chatpartner angegebenen und vom Beschwerdeführer verwendeten ‚nickname' ersucht, der dann auch die diesem ‚nickname' zugeordnete IP-Adresse mitgeteilt hat. Für die Übermittlung der (dynamischen) IP-Adresse, die unzweifelhaft ein Verkehrsdatum darstellt, auf Basis eines ‚nickname' kann § 53 Abs 3a SPG keine geeignete Grundlage bieten. Aus datenschutzrechtlicher Sicht schiene es - auch wenn sich angesichts der gegenständlichen Umstände des Sachverhaltes das Verständnis für ein Verhalten wie jenes des Beschwerdeführers in Grenzen halten wird - vielmehr außerordentlich bedenklich, den Anwendungsbereich des § 53 Abs. 31 SPG im Wege der Analogie auch auf nicht ausdrücklich erfasste Sachverhalte zu erweitern.

Als Folge der oben dargestellten Zuordnung von Chatforen zu den Hostprovidern nach § 16 ECG bleibt - auch wenn sich die Erst-Beschwerdegegnerin selbst nicht auf diese denkbare Grundlage gestützt hat - zu prüfen, ob allenfalls § 18 ECG als Grundlage für ein Auskunftsverlangen von Sicherheitsbehörden wie im vorliegenden Sachverhalt in Frage kommen könnte:

§ 18 ECG regelt an sich die Pflichten aller Anbieter von Diensten der Informationsgesellschaft, also sowohl jene der nur dem ECG unterliegenden sog. „Content-Provider" als auch jene der (Tele)Kommunikationsdienstebetreiber, deren Tätigkeit vornehmlich vom TKG (2003) geregelt werden. Hinsichtlich der Auskunftsverpflichtungen enthält § 18 die folgenden Regelungen:

Gemäß §18 Abs. 2 haben sowohl Content-Provider als auch (Tele)Kommunikationsdienstebetreiber auf Grund der Anordnung „eines dazu gesetzlich befugten inländischen Gerichtes diesem alle zur Verhütung, Ermittlung, Aufklärung oder Verfolgung gerichtlich strafbarer Handlungen" zweckdienlichen Informationen über die Nutzer der Dienste (soweit der Betreiber mit ihnen bestimmte Vereinbarungen geschlossen hat) zu übermitteln. Der Beschwerdeführer hat daraus geschlossen, dass Sicherheitsbehörden ohne Vorliegen einer gerichtlichen Anordnung nicht ermitteln dürfen.

Nun hat die Erst-Beschwerdegegnerin als Grund ihrer Ermittlungen nicht allein die Aufklärung und Verfolgung einer strafbaren Handlung genannt, sondern vor allem auch die Abwehr und Beendigung eines gefährlichen Angriffes, also die Verhütung einer strafbaren Handlung. Ob § 18 Abs. 2 ECG hinsichtlich der Aufklärung und Verfolgung von strafbaren Handlungen einer Anwendung des § 53 Abs. 3a SPG im Wege steht,

kann dahin gestellt bleiben - es gibt jedoch jedenfalls kein österreichisches Gericht, das für die „Verhütung strafbarer Handlungen" zuständig wäre. Die Datenschutzkommission geht davon aus, dass § 18 ECG hinsichtlich des Rekurses auf „gesetzlich befugte inländische Gerichte" die aufgrund des Sicherheitspolizeigesetzes und der Strafprozessordnung bestehende - wenn auch im Einzelfall nicht wirklich klar abgegrenzte - Aufgabenteilung zwischen Sicherheitsbehörden und Gerichten nicht ändern wollte , sodass Abs. 2 nur so weit anwendbar ist, als gerichtliche Zuständigkeiten bereits nach anderen Rechtsvorschriften als dem ECG bestehen. Jedenfalls für den Bereich rein sicherheitspolizeilicher Agenden kann daher § 18 Abs. 2 nicht zur Anwendung kommen, sondern nur allenfalls Abs. 3, der Auskunftsverpflichtungen an Verwaltungsbehörden statuiert.

Gemäß § 18 Abs. 3 ECG müssen Hosting-Betreiber auf Grund der Anordnung einer Verwaltungsbehörde Auskunft über „Namen und Adresse" der Nutzer ihres Dienstes geben, mit denen sie Vereinbarungen über die Speicherung von Informationen abgeschlossen haben, sofern die Kenntnis dieser Informationen eine wesentliche Voraussetzung der Wahrnehmung der der Behörde übertragenen Aufgaben bildet. Diese Verpflichtung betrifft ausdrücklich nur Hosting-Betreiber, während Telekommunikationsbetreiber für sicherheitspolizeiliche Zwecke gemäß § 53 Abs. 3a SPG Auskunft geben müssen - die Weitergeltung von Auskunftsverpflichtungen für Betreiber nach anderen Gesetzen als dem ECG wird durch § 18 Abs. 5 ECG ausdrücklich bestätigt.

Der Beschwerdeführer behauptet nun, dass auch bei Anwendung des § 18 Abs. 3 ECG die Ermittlung der IP-Adresse durch Befragung des Chatroom-Betreibers gesetzlich nicht gedeckt war, da § 18 Abs. 3 die Betreiber nur zur Bekanntgabe der Stammdaten „Name" und „Adresse" im Sinne von „Anschrift" ermächtige, nicht aber zur Bekanntgabe einer IP-Adresse - diese sei ein Verkehrsdatum und daher ein alterum gegenüber der „Anschrift". Auch sei die Auskunft auf Nutzer beschränkt, mit welchen eine Vereinbarung über die Speicherung geschlossen worden ist; er habe aber keine Vereinbarung über die Speicherung von Informationen mit dem Betreiber geschlossen - er sei vielmehr davon ausgegangen, dass die Inhalte seiner Chatroom-Beiträge sofort nach Übermittlung an die Chatpartner gelöscht werden.

Dem letzteren Einwand ist entgegen zu halten, dass dem § 18 Abs. 3 ECG naturgemäß eine sehr generalisierende Betrachtung der denkmöglichen Dienste gemäß § 16 zugrunde liegt, für die - wie oben ausgeführt - das Speichern von Information grundsätzlich als Definitionskriterium gilt; auch beim Chatroom ist regelmäßig die Speicherung der Kommunikationen als Teil des Dienstes angeboten, insbesondere auch um den

Verlauf der Diskussion für die Diskutanten nachvollziehbar zu machen. Auch aus der Eingangswebseite des Dienstes www.***.at wird deutlich, dass hier mehr als bloße Nachrichtenübertragung angeboten wird, nämlich Spiele, Blinddate, Tagebuch, Diskussionsforum, Friendslist u.v.m. Der Umstand, dass speziell für das Chatten im Privatfenster keine Aufzeichnung erfolgt, ändert nichts am grundsätzlichen Charakter des Dienstes als Hostproviding.

Weiters: Selbst wenn dies in concreto dem Nutzer nicht zu Bewusstsein gekommen sein sollte, lag auch eine „Vereinbarung" vor, die in den Benützungsbedingungen zu sehen ist, die der Nutzer akzeptiert, wenn er sich im Chatroom einloggt.

Darüber hinaus kommt dem Vorbringen des Beschwerdeführers allerdings Berechtigung zu: Durch die letztlich auf den Justizausschuss zurückgehende Änderung des § 18 Abs. 3 ECG sollte zwar eine von den jeweiligen Materiengesetzen unabhängige Rechtsgrundlage für die Auskunftsverpflichtung von Betreibern an Verwaltungsbehörden über Name und Adresse ihrer Nutzer geschaffen werden. Die im Justizausschussbericht festgehaltene Begründung macht allerdings deutlich, dass man dabei aber nicht sicherheits- oder kriminalpolizeiliche Ermittlungen, sondern primär andere verwaltungs(straf)rechtliche Ermittlungen vor Augen hatte, heißt es doch dort: „Die Verwaltungsbehörde (also etwa die Gewerbebehörden, die Finanzmarktaufsicht, aber auch andere, zur Aufsicht über einen Anbieter berufenen Stellen) soll vielmehr unmittelbar auf der Grundlage des E-Commerce-Gesetzes den Namen und die Adresse des Nutzers eines Host Providers erfragen können, sofern sie diese Informationen zur Wahrnehmung der ihr übertragenen Aufgaben (etwa zur Gewerbe- oder Finanzmarktaufsicht) benötigt" (853 der Beil. XXI GP). Dieses Verständnis dürfte wohl auch der Praxis der Sicherheitsbehörden entsprechen, die offenbar ebenfalls nicht von § 18 Abs 3 ECG als tauglicher Rechtsgrundlage für Ermittlungen wie jene im gegenständlichen Fall ausgehen. Abgesehen davon kann sich die Bestimmung des § 18 Abs 3 ECG auch nur auf Stammdaten und nicht auf Verkehrsdaten - die eine dynamische IP-Adresse unzweifelhaft ist - beziehen (vgl. Haidinger, Auskunfts- und Mitwirkungspflichten von ISP zur Täterausforschung, Seite 35, nachzulesen z.B. unter www.rechtsprobleme.at/doks/auskunfts-mitwirkungspflichten-isp-haidinger-pdf).

Die Verwendung von Verkehrsdaten unterliegt der Vertraulichkeit gem. Art 5 der RL 2002/58/EG bzw. dem Kommunikationsgeheimnis gem. § 93 Abs 1 TKG 2003 und besonderen Verwendungsbeschränkungen gem. Art 6 und Art 15 Abs 1 dieser RL bzw. § 92 Abs 2 und § 99 TKG 2003. Diese Verwendungsbeschränkungen bewirken vor allem, dass Verkehrsdaten bei Telekommunikationsbetreibern über die

Herstellung und Aufrechterhaltung der Verbindung im Netz hinaus nur gespeichert bleiben dürfen, soweit dies für Verrechnungszwecke notwendig ist oder soweit die ausdrückliche Einwilligung des Betroffenen vorliegt (Art. 6 der RL 2002/58/EG bzw. § 99 TKG 2003). Auch wenn im Gesetzestext nicht das Wort „Anschrift" verwendet wird - wie etwa in § 53 Abs. 3a SPG - kann darin keine gewollte Bedeutungsdifferenzierung zwischen „Anschrift" und „Adresse" gesehen werden. Dem Gesetzgeber kann nicht unterstellt werden, dass er durch die Verwendung des Wortes „Adresse" in der Formel „Name und Adresse" auch IP-Adressen erfassen wollte, die infolge ihres Charakters als Verkehrsdatum besonderen Verwendungsbeschränkungen unterliegen. Es soll nur ergänzend darauf hingewiesen werden, dass der Begriff „ Adresse" auch in zahlreichen anderen Rechtsvorschriften durchaus gebräuchlich im Sinne von „Wohnadresse" Verwendung findet (z. B § 136 EO, § 3 ÜberwachungsVO, § 580 ZPO, § 18a VersVG). Nachdem es sich bei einer IP-Adresse, die einem bestimmten Anschluss zugeordnet ist, im Vergleich zur „Adresse" im herkömmlichen Sinn von „Wohnadresse" um ein doch völliges aliud handelt, kann nicht davon ausgegangen werden, dass der Gesetzgeber ohne ausdrückliche Bezugnahme darauf auch dies mit dem Begriff „Adresse" erfasst wissen wollte.

Auch wenn sich das Verständnis für ein Verhalten wie jenes des Beschwerdeführers im gegenständlichen Fall in Grenzen halten muß, ist davon auszugehen, dass das Vorgehen der Sicherheitsbehörden weder im SPG noch im ECG eine gesetzliche Deckung finden kann. Die Datenschutzkommission kommt allerdings auch nicht um die Anmerkung umhin, dass die bestehende Rechtslage im Hinblick auf die Befugnisse der Sicherheitsbehörden nicht wirklich klar ist und daher im Interesse des Datenschutzes und der Rechtssicherheit sowohl aus der Sicht der Behörden, wie auch aus jener der betroffenen Bürger und der Auskunftspflichtigen durchaus verbesserungswürdig erscheint.

Im Ergebnis unerörtert bleiben kann die Frage, inwieweit nicht in besonders gelagerten Einzelfällen, in welchen die ganz konkrete Gefährdung von Menschen droht, auch deren verfassungsrechtlich gewährleistete Grundrechte und die daraus allenfalls für den Staat ableitbare "Garantenstellung" zu einer anderen, insofern verfassungskonformen Interpretation des § 53 Abs 3 a SPG verpflichten könnten und infolge dessen einen Eingriff in die Datentschutzrechte des betroffenen Kommunikationspartners rechtfertigen würden (vgl im Zusammenhang etwa Grabenwarter, Europäische Menschrechtskonvention2, 120 mwN, Preiss, Der politische Charakter der Menschenrechte, EuGRZ 2004, 611). Freilich könnte dies unter Beachtung der aus § 1 DSG ableitbaren Grundrechtspositionen immer nur eine "ultima ratio" sein, wenn nicht andere Wege zur Verfügung stünden. Davon kann aber hier

schon im Hinblick auf die ja gleichzeitig bestehenden strafgerichtlichen Verfolgungs- und Ausforschungsmöglichkeiten nicht ausgegangen werden.
-END-