UNIVERSITÄTSLEHRGANG
FÜR INFORMATIONSRECHT UND RECHTSINFORMATION
AN DER RECHTSWISSENSCHAFTLICHEN FAKULTÄT DER UNIVERSITÄT WIEN

Gesetzliche Auskunfts- und Mitwirkungspflichten von Internet Service Providern gegenüber Behörden und Privaten

Master Thesis

zur Erlangung des akademischen Grades

MASTER OF LAWS (LL.M.)

[INFORMATIONSRECHT UND RECHTSINFORMATION]

(Universitätslehrgang für Informationsrecht und Rechtsinformation der Universität Wien)

vorgelegt von

Mag Victoria Haidinger

begutachtet von

RA Dr Karin Wessely

Im September 2003

Hinweise

Dieses Layout basiert auf der Typoskriptvorlage der Österreichischen Rechtswissenschaftlichen Studien (ÖRSt). Die Verwendung, Bearbeitung und allfällige Veröffentlichung der Bearbeitung erfolgt mit freundlicher Bewilligung des Manz-Verlages. Ansonsten wird auf das UrhG verwiesen.

Paragraphenangaben, denen keine Gesetzesbezeichnung beigefügt ist, beziehen sich auf das im jeweiligen Kapitel in der Hauptsache behandelte Gesetz.

Vorliegende Arbeit orientiert sich im Wesentlichen an *Friedl* (Hrsg), Abkürzungs- und Zitierregeln der österreichischen Rechtssprache und europarechtlicher Rechtsquellen[5] (2000). Zeitschriftenartikel werden mit der Anfangsseitenzahl zitiert, um eine leichtere Auffindbarkeit in der RDB zu ermöglichen.

Die URLs wurden zuletzt am 1.9.2003 überprüft.

Inhaltsverzeichnis

I. Einleitung 1

A. Einordnung von Auskunftspflichten 2

B. Einteilung der Internet Service Provider (ISP) 4
1. Access- und Cashing Provider 5
2. Host-Provider 5
3. Content-Provider 6
4. Backbone- und Network-Provider 6

C. Protokollierte Daten 6

D. Verfassungsrechtliche Dimension 8
1. Begriffsbestimmungen 8
2. Das Fernmeldegeheimnis 13
3. Recht auf Datenschutz 17
4. *Nemo-Tenetur*-Grundsatz 21
5. Eigentum und Verbot der Zwangs- und Pflichtarbeit 21

II. Ausgangsfälle 23
1. *RiAA* vs *Verizon*: Auskunft Access-Provider an einen Privaten 23
2. Variante *RiAA* vs *Verizon*: Beteiligung eines Strafgerichts 23
3. Überwachung des Fernmeldeverkehrs auf Anordnung eines Gerichtes 23
4. Auskünfte an Verwaltungsbehörden 24
5. Mobilfunkbetreiber als Access-Provider 24

III. Das E-Commerce-Gesetz 25

A. Anwendungsbereich 25
1. Sachlicher Anwendungsbereich 25
2. Persönlicher Anwendungsbereich 29
3. Räumlicher Anwendungsbereich 30
4. Ausnahmen vom Anwendungsbereich 31
5. Zusammenfassung 31

B. Auskunftspflichten 31
1. Auskunftspflichten gegenüber Gerichten (§ 18 Abs 2) 32
2. Auskunftspflichten gegenüber Verwaltungsbehörden (§ 18 Abs 3) 33
3. Auskunftspflichten gegenüber Privaten (§ 18 Abs 4) 35
4. Abstellungsaufträge / Sperrverfügungen 37
5. Durchsetzung, Sanktionen und Rechtsfolgen 39

IV. Urheberrechtsgesetz 44

A. Die InfoSoc-RL 44

B. Die österreichische Umsetzung 44
Exkurs: Zum Begriff des Vermittlers 45
1. Unterlassungs- und Beseitigungsanspruch (§ 81 Abs 1a, § 82) 46
2. Auskunftspflichten (§ 87 Abs 3) und das Verhältnis zum ECG 46
3. Durchsetzung, Sanktionen und Rechtsfolgen 46

C. Ausblick: Richtlinienvorschlag über die Maßnahmen und Verfahren zum Schutz der Rechte an geistigem Eigentum 47
1. Beweismittel (Art 7 RL-Entw) 48
2. Beweissicherungsverfahren (Art 8 RL-Entw) 48
3. Recht auf Auskunft (Art 9 RL-Entw) 48
4. Einstweilige Maßnahmen zum Schutz geistigen Eigentums (Art 10 RL-Entw) 49

V. Strafprozessordnung und Telekommunikationsgesetz 51

A. Allgemeines 51

B. Mitwirkungspflichten bei der Datenerhebung 51
1. Beschlagnahme 51
2. Hausdurchsuchung 55
3. Überwachung des Fernmeldeverkehrs 56

C. Weitere Auskunftspflichten nach dem TKG 2003 62

D. Durchsetzung, Sanktionen und Rechtsfolgen 63

E. Ausblick 64
1. Strafreformprozessgesetz 64
2. Convention on Cyber-Crime 64

VI. Sicherheitspolizeigesetz 66

A. Allgemeines 66
1. Anwendungsbereich und Aufgaben 66
2. Sicherheitsbehörden 68

B. Besondere Befugnisse 68
1. Informationssammlung 69
2. Durchsuchung von Menschen und Objekten 73
3. Zugriffsbefugnisse auf Sachen 74

VII. Finanzstrafgesetz & Militärbefugnisgesetz 76

A. Finanzstrafgesetz 77
1. Auskunftspflichtig 77
2. Auskunftsberechtigt 77
3. Voraussetzungen 77
4. Inhalt 77

B. Militärbefugnisgesetz 78
1. Auskunftspflichtig 78
2. Auskunftsberechtigt 78

3. Voraussetzungen 78
4. Inhalt 79

VIII. Datenschutzgesetz 80
1. Auskunftspflichtig 81
2. Auskunftsberechtigt 81
3. Voraussetzungen 82
4. Inhalt 82
5. Sonstiges 83
6. Sanktion und Durchsetzung 84

IX. Beurteilung der Ausgangsfälle 85
1. Der Fall *RIAA* vs *Verizon*: Auskunft Access-Provider an Privaten . 85
2. Variante *RIAA* vs *Verizon*: Beteiligung eines Strafgerichts 85
3. Überwachung des Fernmeldeverkehrs auf Anordnung eines Gerichtes 86
4. Auskünfte an Verwaltungsbehörden 86
5. Mobilfunkbetreiber als Access-Provider 87

X. Übersicht über die wichtigsten Auskunftspflichten 89

Abkürzungsverzeichnis i

Literaturverzeichnis vi

Sonstige Quellen und online Datenbanken (annotiert) viii

GOD, GRANT ME THE SERENITY TO ACCEPT
THE THINGS I CANNOT CHANGE,
COURAGE TO CHANGE THE THINGS I CAN,
AND THE WISDOM TO KNOW THE DIFFERENCE
Dr Reinhold Nebuhr[1] , The Serenity Prayer

I. Einleitung

Die vorliegende Arbeit soll auf übersichtliche Art die verschiedenen Auskunfts- und Mitwirkungspflichten, welche Internet Service Provider treffen, darstellen. Dies insbesondere im Hinblick auf die Identitätsfeststellung von Rechtsverletzern, da gerade diese Pflichten in der Praxis am relevantesten sind.

„Kriminelle Geister" machen auch vor den neuen Medien nicht Halt. So werden einerseits konventionelle Delikte unter Nutzung von Telekommunikation und Internet begangen, wodurch insbes rechtswidrige Inhalte eine wesentlich schnellere Verbreitung erfahren. Andererseits hat der Gesetzgeber aber auch internet- bzw computerspezifische Delikte normiert.[2] „Stopline"[3], die Meldestelle der ISPA, verzeichnete im Jahr 2001 rund 400 zutreffende Meldungen, der Großteil hiervon bezog sich auf kinderpornographische Inhalte im Internet. Im Jahr 2000 erreichten die Meldestelle rund 380 zutreffende Meldungen.[4] Auf die Verfolgung solcher und anderer rechtswidriger Taten zielen die Auskunftspflichten des ECG, des UrhG, des SPG, des FinStrG, des MBG und der StPO ab.

Kürzlich erfolgte die Umsetzung der InfoSoc-RL[5], mit der eine weitere Auskunftspflicht der Provider eingeführt wurde. Sie betrifft Verstöße gegen das Urheberrecht durch Nutzer. Hier hat sich wohl das massive Lobbying der Rechteinhaber bezahlt gemacht, und so wurden spezielle Auskunftspflichten zum Schutz von Urheberrechten nach Vorbild der USA normiert. Zusätzlich stellte die EU-Kommission im Jänner 2003 einen Vorschlag betreffend einer Richtlinie zur Durchsetzung des Schutzes der Rechte am geistigen Eigentum vor.[6]

---

[1] Dieses Zitat wird fälschlicherweise häufig dem Hl Franz von Assisi zugeschrieben.

[2] Für das Strafrecht: Siehe *Venier/Ebensperger,* Internet und Strafrecht, in: *Brenn,* ECG 118.

[3] http://www.stopline.at . Die Daten sind dem Jahresbericht 2000 und 2001 entnommen, wo auch Details zur Geschichte der Meldestelle nachzulesen sind.

[4] Vgl zB: Internet spielt bei Kinderpornografie entscheidende Rolle, Heise Online, http://www.heise.de/newsticker/data/anw-23.05.03-005/ ; GEMA will Provider gegen Musikpiraterie in die Pflicht nehmen, Heise Online, http://www.heise.de/newsticker/data/tol-14.08.03-000/ .

[5] Richtlinie 2001/29/EG vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, ABl L 167 v 22.6.2001, 10, berichtigt durch ABl L 6 v 10.1.2002, 71.

[6] Siehe dazu unten im Kapitel Urheberrechtsgesetz, S 47.

Ferner lassen sich Informationsflüsse heute schwieriger kontrollieren als früher, und diese sind häufig für den Betroffenen nicht nachvollziehbar. Um dem Betroffenen eine Möglichkeit zu geben, herauszufinden, wer wie zu seinen Daten gelangt ist und was mit diesen geschieht, sind im DSG und im TKG Auskunfts- und aktive Informationspflichten der Datenverwender normiert.

Es stellt sich nun als nächstes die Frage, warum sich diese Arbeit mit Internet Service Providern beschäftigt. Einerseits, weil sie als „Träger des Internets" primär betroffen sind. Wie gezeigt werden wird, sind aber immer noch viele Bestimmungen auf Sprachtelephonie zugeschnitten. Daher geht es andererseits um die Anwendbarkeit dieser Auskunfts- und Mitwirkungspflichten, die ehemals nur auf POTS[7] ausgerichtet waren, auf das Internet bzw auf Internet Service Provider.

Rudimentär wird sich vorliegende Arbeit auch mit den Sanktionen bei Nichterfüllung von Auskunfts- und Mitwirkungspflichten beschäftigen. Zum einen mit den gesetzlich vorgesehenen straf- und verwaltungsstrafrechtlichen Rechtsfolgen, zum anderen aber auch mit allfälligen Schadenersatzansprüchen nach allgemeinem Zivilrecht. Häufig nehmen Auskunftsempfänger erteilte Auskünfte als Grundlage für Dispositionen, sodass unrichtige Auskünfte *„Schaden stiften"* [8] können. Dies gilt nicht minder für die Verweigerung von Auskünften.

A. Einordnung von Auskunftspflichten

Auskunftspflichten zielen auf die Herausgabe von Daten bzw Information ab. Eine allgemeine Auskunftspflicht existiert in Österreich nicht, vielmehr sind einzelne Auskunftspflichten aus dem materiellen oder formellen Recht herauszulesen. Es mangelt an einem geschlossenen System, weshalb auch die vorhandenen Auskunftspflichten über die ganze Rechtsordnung verstreut sind.[9] Hiervon ist das Auskunftsrecht des Datenverwenders nach dem DSG zu unterscheiden, welches als Datenweitergabe geregelt wird. Präziser gesagt, handelt es sich hier um eine Ermächtigung für den Datenverwender, bestimmte Daten herauszugeben.[10] Dies verleiht aber demjenigen, der die Daten verlangt, kein Recht auf Herausgabe.

Daten sind keine körperlichen Gegenstände und daher schwer in die vorhandenen Beweismittelkataloge einzuordnen.[11] Auf „neue" Beweismittel

---

[7] POTS = *Plain Old Telephony Service*. Mit diesem Begriff wird das alte, analoge, Telephonsystem bezeichnet (in Österreich das WS 48) und häufig als Gegensatz zu ISDN bzw zur digitalen Datenkommunikation überhaupt, verwendet.

[8] *Welser,* Die Haftung für Rat, Auskunft und Gutachten – Zugleich ein Beitrag zur Bankauskunft (1983) 1.

[9] Vgl *Bienert-Nießl,* Materiellrechtliche Auskunftspflichten im Zivilprozeß – Zugleich eine Untersuchung der prozessualen Mitwirkungspflichten der Parteien (2003) 27, die sich insbes mit Aufklärungs- und Auskunftspflichten *inter partes* beschäftigt.

[10] Vgl hierzu unten S 18.

[11] Vgl auch *Muskatelz,* Der Datenzugriff im Strafverfahren (2000) 47 ff. Den Grundsatz der Unbeschränktheit der Beweismittel kennen alle österreichischen Prozessgesetze: *Seiler,* Strafprozessrecht[6] Rz 437; *Rechberger/Simotta,*

sind im Zweifel die Regeln über das nächstverwandte sinngemäß anzuwenden.[12] So kann ein Datenträger in Augenschein genommen werden oder, wenn Daten ausgedruckt vorliegen, den Regeln über den Urkundebeweis unterliegen.[13] Auskunfts- und Mitwirkungspflichten wird man im Rahmen eines formellen Verfahrens in Form des Zeugenbeweises nachkommen müssen. Die ZPO definiert Zeugen als eine Personen, die über Wahrnehmungen von *„vergangenen Tatsachen oder Zuständen aussagen“* (§ 350 ZPO). Es wird also davon ausgegangen, dass der Zeuge einen Vorgang selbst beobachtet hat, und nicht, dass er die Informationen erst selbständig erheben muss, wie dies häufig bei Unternehmen der Fall ist. Von einem Zeugen kann Auskunft über bestimmte Fakten verlangt werden, seine Funktion geht allerdings darüber hinaus: so unterliegt der Zeuge selbst der freien Beweiswürdigung, die auch sein Verhalten mit einschließt, um zu beurteilen, ob dieser die Wahrheit sagt. Zu einem gewissen Maß an Mitwirkung in Form von Vorlagepflichten udgl kann ein Zeuge ebenfalls gezwungen werden, die materiellen Auskunftspflichten gehen allerdings weiter.[14]

Werden Auskunftspflichten normiert, so geschieht dies auch, um die Möglichkeit zu erlangen, große Datenmengen zu akquirieren, die im weiteren Verlauf des Verfahrens ausgewertet werden, und die in weiterer Folge im Hauptverfahren einem Augenschein unterzogen werden sollen.

Häufig sollen Daten zu Beweiszwecken aber nicht erst in einer kontradiktorischen Verhandlung mündlich durch den Richter aufgenommen werden. So ist es insbes im Strafverfahren oftmals notwendig, dass Auskünfte unmittelbar durch die Sicherheitsbehörden eingeholt werden, um weitere Ermittlungen zur Täterausforschung anstellen zu können. Darüber hinaus dienen die Auskunftspflichten idR nicht der unmittelbaren, also mündlichen, Beweisaufnahme, sondern werden vielmehr in einem schriftlichen Verfahren eingefordert (vgl die Bestimmungen der StPO und des ECG).[15] Schriftliche Zeugenaussagen sind den Prozessrechten grundsätzlich fremd.[16]

Zivilprozeßrecht[6] (2003) Rz 617; *Walter/Mayer,* Verwaltungsverfahrensrecht[7] (1999) Rz 335.

[12] *Rechberger/Simotta*, Zivilprozeßrecht[6] aaO.

[13] Vgl *Rechberger/Simotta*, Zivilprozeßrecht[6] aaO.

[14] Zum Zivilprozess: *Kodek,* Die Verwertung rechtswidriger Tonbandaufnahmen und Abhörergebnisse im Zivilverfahren, ÖJZ 2001, 287. Die ZPO selbst nimmt in § 304, §§ 318, 369 iVm § 304 auf materielle Informationspflichten Bezug (vgl hierzu *Bienert-Nießl,* Materiellrechtliche Auskunftspflichten im Zivilprozeß 249).

Zum Strafprozess im Zusammenhang mit dem *nemo tenetur*-Grundsatz: *Schmoller,* Erzwungene selbstbelastende Aussagen im Strafprozeß - zugleich ein Beitrag zu den Beweisverwertungsverboten, JBl 1992, 69.

[15] Dies mag prima vista einen Nachteil bedeuten. Es sei allerdings darauf hingewiesen, dass insbes im Alltag der Strafgerichte ein schriftliches Verfahren oft schneller abläuft, als die mündliche Vernehmung eines Zeugen, die eine ordnungsgemäß zugestellte Ladung voraussetzt. Gerade bei größeren Unternehmen bereitet die Entsendung der "informierten Vertreter" zur Zeugenvernehmung immer wieder Schwierigkeiten. Man bedenke auch, dass ein solcher Vertreter wohl kaum mit Festplatten vor Gericht erscheinen wird.

[16] Vgl *Rechberger/Simotta,* Zivilprozessrecht[6] Rz 627.

Für Private kann es gleichfalls bedeutend sein, außerhalb von gerichtlichen Verfahren (zB § 26 DSG, § 18 Abs 4 ECG, § 87b UrhG) diverse Informationen einzuholen, um überhaupt einen Anspruchsgegner benennen zu können. Nochmals erwähnt werden soll, dass die in vorliegender Arbeit behandelten Auskunftspflichten im Wesentlichen der Identitätsfeststellung eines Verantwortlichen dienen.[17]

B. Einteilung der Internet Service Provider (ISP)

Der Begriff „Internet Service Provider" fasst eine Fülle von Unternehmen zusammen, die sich allesamt mit internetrelevanter Telekommunikation und den damit zusammenhängenden Diensten befassen. Je nach konkreter Tätigkeit werden sie üblicherweise eingeteilt in: Access-Provider, Host-Provider und Content-Provider. Gelegentlich stößt man auch auf Backbone-Provider, Network-Provider und Cashing-Provider.[18] Schon vor Verabschiedung der E-Commerce-Richtlinie[19] war dies eine übliche Einteilung.[20] Diese RL übernahm (betreffend Access- und Host-Providern) diese traditionelle Terminologie nach Vorbild des § 5 des deutschen Teledienstegesetzes und des Titels II des US-Digital Millennium Copyright Act.[21] In Umsetzung der E-Commerce-Richtlinie erging das E-Commerce-Gesetz (ECG)[22], welches den Richtlinien-Text zum Großteil wörtlich übernahm.

Gleichzeitig ist der Begriff des „Internet Service Providers" reichlich undeutlich und missverständlich.[23] So verstehen manche darunter alle oben aufgezählten Provider, andere lediglich die Access-Provider[24], dritte wiederum nur jene Diensteanbieter, die im ECG genannt sind[25].[26] Letztendlich ist die Unterscheidung von untergeordneter Bedeutung, da die einschlägigen Gesetze

---

[17] Mit Auskunftspflichten zu anderen Zwecken beschäftigt sich *Bienert-Nießl,* Materiellrechtliche Auskunftspflichten im Zivilprozeß 27. Zur gerichtlichen Geltendmachung vgl *dies,* aaO 219 ff.

[18] Vgl *Ebensperger,* Die Verbreitung von NS-Gedankengut im Internet und ihre strafrechtlichen Auswirkungen unter besonderer Berücksichtigung des E-Commerce-Gesetzes, ÖJZ 2002, 132.

[19] Richtlinie 2000/31/EG über den elektronischen Rechtsverkehr, ABl L 178 v 17.7.2001, 1. Die Richtlinie nennt die von ihr behandelten Provider „Vermittler",

[20] Vgl zur Herausbildung dieser Begriffe in den USA: *Brandl/Mayer-Schönberger*, Die Haftung von Online-Diensten für übermittelte Inhalte, ecolex 1996, 129; *Fischer,* Die Haftung der Internet-Provider, (Diss Salzburg 2001), http://www.privatrecht.sbg.ac.at/forum/fischer.pdf .

[21] *Brenn* (Hrsg)*,* E-Commerce-Gesetz (2002) 261.

[22] BG, mit dem bestimmte rechtliche Aspekte des elektronischen Rechtsverkehrs geregelt werden (E-Commerce-Gesetz – ECG) vom 21.12.2001, BGBl I 152/2001 ((NR: GP XXI RV 817 AB 853 S 83. BR: AB 6499 S 682) [CELEX-Nr.: 300L0031].

[23] Vgl die Kritik bei *Fischer,* aaO.

[24] So *Blume/Hammerl,* E-Commerce-Gesetz Kommentar (2002) 116.

[25] So *Brenn,* ECG 173.

[26] Vgl auch *Parschalk/Otto/Zuser*, TKR 153f; *Brandl*, Datenschutz im Internet, in: *Studiengesellschaft für Wirtschaft und Recht* (Hrsg), Internet und Recht – Rechtsfragen von E-Commerce und E-Government 124.

ausschließlich auf die tatsächlich ausgeübte Tätigkeit abstellen. Dies gilt insbesonders für das ECG, welches an funktionalen Kriterien anknüpft.[27]

Im Folgenden werden diese Begriffe erklärt, und zwar unabhängig davon, ob das ECG - das Regelungen für manche dieser Provider enthält - anwendbar ist oder nicht. Näheres zum ECG siehe im Kapitel E-Commerce-Gesetz, S 25.

1. Access- und Cashing Provider

Die Tätigkeit der Access-Provider besteht in der Übertragung von Signalen und/oder Weiterleitung auf einem Kommunikationsnetz, nämlich den Datenleitungen bis zum nächsten Knoten des Internets.[28] Sie bieten daher iaR den Zugang zu fremden Inhalten oder zu einem Kommunikationsnetz an bzw übermitteln sie Informationen in einem solchen. Wenn im Folgenden von Access-Provider ieS gesprochen wird, so sind damit jene Provider gemeint, die mit Nutzern einen Vertrag über die Internetanbindung abgeschlossen haben.

Dem Access-Provider steht der Cashing-Provider nahe, der im § 15 ECG seine gesetzliche Normierung erfahren hat. Seine Tätigkeit besteht im Zurverfügungstellen von sog Proxy-Servern. Auf diesen werden fremde Inhalte, idR Websites, zwecks Beschleunigung der Informationsübertragung und damit zur Verbesserung des Kommunikationsnetzes, gespeichert.[29] Da seine Dienstleistung daher primär auf die Vermittlung und weniger auf die Speicherung abzielt - die EB[30] zum ECG sprechen von Tätigkeiten *„rein technischer, automatischer und passiver Art“* - steht er dem Access-Provider näher, als dem Host-Provider, und ist mit ihm vergleichbar. Er unterliegt damit auch einem ähnlichen Haftungsregime. Eine gesonderte Behandlung erscheint somit überflüssig.

2. Host-Provider

Der Host-Provider speichert fremde Inhalte (so auch § 16 ECG). Darunter fallen Anbieter von Webspaces, Gästebüchern, Foren[31], und Online-Tageszeitungen, die Postings zu Artikeln ermöglichen[32]. Wie man sieht, umfasst dieser Begriff eine Vielzahl unterschiedlicher Dienste, die auf den ersten Blick nicht viel gemeinsam haben. So kann von den einschlägigen Normen des ECG der Private, der ein Gästebuch auf seiner Homepage betreibt ebenso betroffen sein, wie das Telekommunikationsunternehmen, das Website-Hosting anbietet.

---

[27] Vgl *Zankl,* E-Commerce-Gesetz Kommentar und Handbuch (2002) Rz 184*; Blume/Hammerl*, ECG-Kommentar 114.

[28] Vgl *Parschalk/Zuser/Otto,* TKR 154. Vgl mwN *Otto/Parschalk*, Anzeige- und Konzessionspflicht von Internet Service Providern nach dem TKG, MR 2001, 420.

[29] Vgl die EB zum ECG, abgedruckt in: *Brenn,* ECG 275.

[30] aaO.

[31] Wie zB: „Gimix“ von http://www.gmx.de .

[32] Vgl http://www.diepresse.at, http://derstandard.at .

3. Content-Provider

Ein Content-Provider bietet eigene Inhalte im Internet an.

4. Backbone- und Network-Provider

Die Tätigkeit der Backbone- und Network-Provider (auch *Carrier* genannt) besteht im Zurverfügungstellen von Infrastruktur. Sie bieten also ein Netzwerk und Vermittlungsdienste an.[33] Während jedoch der Backbone-Provider das sog „Backbone-Netz", also die zentralen Übertragungswege, betreibt[34], bietet der Network-Provider die Leitungen zwischen Konsument und Access-Provider an.[35]

Ob diese Providerarten rechtlich mit Access-Providern gleichgestellt werden können, wird von einigen Stimmen in der Literatur mit der Begründung abgelehnt, dass sie nur die Bedingungen für den Zugang zum Kommunikationsnetz schaffen, aber sich nicht im elektronischen Bereich bewegen. Siehe hierzu im Kapitel E-Commerce-Gesetz, S 29.

C. Protokollierte Daten

Jeder Rechner - und damit in weiterer Folge auch der Nutzer - ist im Internet durch eine IP-Adresse (*Internet-Protocol*) bestimmbar. Je nach Art der Internetanbindung wird dem Rechner eine statische oder dynamische IP-Adresse zugewiesen. Letztere wird bei jedem Einwahlvorgang (zB per Modem) vom Access-Provider neu vergeben. Statische IP-Adressen werden als weiteres Datum bei den Stammdaten des Kunden gespeichert, und sind insbes bei Breitbandverbindungen üblich. Außerdem wird jede Ressource im Web durch eine URL (*Uniform Resource Locator*) eindeutig bezeichnet. Bei einer Kommunikation werden diese als Kopfzeile vorangestellt, und an jedem Netzknoten, den ein Datenpaket durchläuft, gelesen und temporär festgehalten. Diese Daten können als Web-Logs[36] theoretisch von allen am Kommunikationsvorgang Beteiligten gespeichert werden. Auf diese Weise erfährt der Diensteanbieter beim Aufbau der Verbindung folgende Details über seinen Nutzer:

- Aktuelle IP-Adresse des Rechners
- Verwendetes Betriebssystem
- Typ und Version des Browsers
- Protokolle, die verwendet werden
- URL der Dokumentenseite, von welcher der Nutzer gekommen ist
- Wahl der Sprache

---

[33] So *Blume/Hammerl,* ECG-Kommentar 114 f.

[34] Siehe *Otto/Parschalk* aaO.

[35] *Ebensperger*, aaO

[36] Auch logfiles genannt. Siehe *Brandl,* Datenschutz im Internet, in: *Studiengesellschaft für Wirtschaft und Recht* (Hrsg), Internet und Recht – Rechtsfragen von E-Commerce und E-Government 128.

- Gegebenenfalls bereits gespeicherte Cookies[37]

Zugriffe und Aktionen können anhand von Protokollen registriert werden. Mit Analyseprogrammen ist es möglich diese Daten detailliert auszuwerten, und Nutzungsstatistiken mit angebotsbezogenen Aussagen (wie häufig wurde eine Seite aufgerufen, zu welcher Tageszeit und an welchen Wochentagen sind Zugriffshäufungen) oder solche mit nutzerbezogenen Aussagen (welcher Browsertyp wird bevorzugt, regionale Zuordnung der Rechner) zu erstellen. Mit individualisierten Auswertungen ließen sich auch die Interessen der einzelnen Nutzerinnen und Nutzer ermitteln (sog Nutzerprofile).

Protokolldateien von Access-Providern lassen sich nach den erklärten Zwecken in Protokolle zur Abrechnung gegenüber ihren Kunden und in Protokolle zur Gewährleistung der Datensicherheit unterscheiden. Die Protokolle enthalten vielfach personenbezogene Daten (IP-Adresse, URL der Zieladresse, Datum und Uhrzeit des Zugriffs, Verweildauer und übertragene Datenmengen). Damit ist grundsätzlich nachvollziehbar, wer wann was gelesen oder veranlasst hat, die Speicherung dieser Daten ist allerdings idR unzulässig.[38]

Angaben über die Identität eines Nutzers lassen sich auch als Privater relativ leicht herausfinden, denn der Durchschnitts-Nutzer hinterlässt Spuren im Internet. Man sehe in das Protokoll seiner Firewall – vorausgesetzt man hat eine, was zu empfehlen ist – und lese dort eine IP-Adresse heraus, zB verzeichnete meine Firewall die IP-Adresse 62.116.19.122. Man gehe in eine Unix Shell[39], gebe dort „nslookup 62.116.19.122“ in die Befehlszeile ein, und erhält folgendes Ergebnis:

```
Server:     ns4.univie.ac.at
Address:    131.130.1.12
Name:       austria1.adverserve.net
Address:    62.116.19.122
```

Um festzustellen, wem dieser Server gehört, mache man eine „Whois-Abfrage“ mit dem Kommando „whois ADVERSERVE.NET“:

```
Domain Name: ADVERSERVE.NET
Registrar: NETWORK SOLUTIONS, INC.
Whois Server: whois.networksolutions.com
Referral URL: http://www.networksolutions.com
Name Server: NAMED.YUMYUM.NET
Name Server: NAMED2.YUMYUM.NET
Name Server: NS2.SIL.AT
```

[37] Vgl hierzu auch *Jahnel,* Datenschutz im Internet - Rechtsgrundlagen, Cookies und Web-Logs, ecolex 2001, 84.

[38] Vgl zB Punkt 4.1 der AGB der Eunet AG, http://www.eunet-ag.at/cms/produkte/15264720.htm? . Siehe dazu unten S 20.

[39] Hat man kein Unix, so kann man auch die „Dos-Box“ von Windows verwenden. Die Befehle sind dann allerdings nicht ident. Umfangreiche und benutzerfreundlichere Suchmöglichkeiten bietet auch die Site http://www.dnsstuff.com .

```
Status: ACTIVE
Updated Date: 02-jul-2002
Creation Date: 12-oct-2001
Expiration Date: 12-oct-2003
```

Diese Abfrage ergibt also den Verantwortlichen für diese IP-Adresse bzw denjenigen, dem diese Nummer, respektive der ganze Nummernblock, zu dem diese Nummer gehört, zugeteilt wurde.[40] Zusätzlich kann ein Nutzer natürlich anhand einer E-Mail Adresse oder eines Pseudonyms identifiziert werden. Dies betrifft dann aber vorwiegend Host-Provider.

D. Verfassungsrechtliche Dimension

In letzter Zeit wurden zunehmend Sonderbestimmungen für Telekommunikationsunternehmen eingeführt, die diese zu Auskünften und Mitwirkung verpflichten. Diese einschlägigen Sonderbestimmungen erklären sich insbes aus den verfassungsrechtlichen Vorgaben: Dem Fernmelde- bzw Telekommunikationsgeheimnis (Art 10a StGG und Art 8 EMRK), und dem Grundrecht auf Datenschutz (§ 1 DSG). Ferner sind Mitwirkungspflichten beschränkt durch den *nemo-tenetur* Grundsatz, das Eigentumsrecht und das Verbot der Zwangs- und Pflichtarbeit. Bis zur Privatisierung der Post- und Telegraphenverwaltung (PTV) wurde eine Vielzahl von Auskunfts- und Mitwirkungspflichten auf Art 22 B-VG (Amtshilfe) gestützt. Nach der Liberalisierung im Jahre 1998 bestand daher ein Bedürfnis, diese Pflichten einfachgesetzlich zu regeln.

1. Begriffsbestimmungen

a) Alte Rechtslage: TKG 1997

Das TKG 1997 enthält in seinen §§ 87 ff Bestimmungen zur näheren Ausgestaltung des „sektorspezifischen" Datenschutzrechts[41] und des Fernmeldegeheimnisses. § 87 TKG 1997 definiert die Begriffe Stammdaten, Vermittlungsdaten und Inhaltsdaten. Diese stellen die übliche Terminologie dar, um verschiedene Daten dem Fernmeldegeheimnis bzw dem Grundrecht auf Datenschutz zuzuordnen.

[40] Vgl auch die FAQ der Denic, http://www.denic.de/doc/faq/sonstiges.html#s0002 .

[41] Diese Vorschriften gehen zurück auf die ISDN-RL (Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, ABl L 24 v 30.1.1998, 1), die jedoch durch die Datenschutz-RL des neuen Rechtsrahmens ersetzt worden ist. Siehe dazu unten, S 10.

aa) Stammdaten (§ 87 Abs 3 Z 4 TKG 1997)

Unter Stammdaten versteht man alle personenbezogenen Daten, die für die Begründung, Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter von Telekommunikationsdiensten oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind. Taxativ zählt § 87 Abs 3 Z 4 zu den Stammdaten: Familienname und Vorname, akademischer Grad, Adresse, Teilnehmernummer und Bonität.

Stammdaten unterliegen zwar § 88 Abs 1 TKG 1997 *e-contrario* nicht dem Vertraulichkeitsschutz des TKG, aber dem des DSG.[42]

Exkurs: IP-Adressen als „Teilnehmernummern" und E-Mail Adressen als „Adressen"

Es stellt sich die Frage, ob IP-Adressen als Teilnehmernummern idS zu qualifizieren sind.[43] Im Bereich der Sprachtelephonie erfolgt die Zuordnung eines Anschlusses anhand der Telephonnummer, im Internet geschieht dies über die IP-Adresse. Nicht selten werden diese beiden Adressierungselemente verglichen, um das TCP/IP Protokoll zu erklären[44]. Die Frage ist jedoch, ob dies auch für die normative Bedeutung des Begriffes Teilnehmernummer gilt. § 2 Abs 1 Z 3 NVO[45] definiert die Teilnehmernummer als *„jene Ziffernfolge, die einem Teilnehmer innerhalb einer Region oder eines anderen Bereiches zugeordnet ist;"*. Teilnehmer ist gem § 87 Abs 3 Z 2 TKG 1997 *„eine natürliche oder juristische Person, die mit einem Anbieter eines öffentlichen Telekommunikationsdienstes einen Vertrag über die Inanspruchnahme dieser Dienste geschlossen hat."*. § 52 Z 3 TKG 1997 versteht unter Nummer *„Ziffernfolgen, die in Telekommunikationsnetzen Zwecken der Adressierung dienen;"*. IP-Adressen sind jedenfalls Adressen iSd § 52 Z 3 TKG 1997. Ferner können sie mE auch als Teilnehmernummern qualifiziert werden.[46]

Wenn aber IP-Adressen als Teilnehmernummern zu werten sind, könnte man auch auf die Idee kommen, diese Analogie gleichfalls bei E-Mail Adressen anzuwenden und damit die E-Mail Adresse mit Adresse iSd § 87 Abs 3 Z 4 gleichzusetzen. Dies ist jedoch aus folgenden Erwägungen abzulehnen: Wie bereits festgestellt, wird der Nutzer im Internet anhand seiner IP-Adresse identifiziert. Diese entspricht der Telephonnummer in der Sprachtelephonie. Bei der E-Mail Adresse verhält dies sich anders, denn auch der Internet-Nutzer besitzt

---

[42] Siehe hierzu unten, S 17.

[43] Diese Qualifikation ist insbes von Relevanz für die Auskunftspflichten nach dem SPG, dem FinStrG und dem MBG.

[44] Vgl *Müllschitzky,* Namensrechtliche Probleme von Domainnamen (Master Thesis 2000), http://members.aon.at/mamue/dokumente/pdf/domain_names.pdf, 12.

[45] Verordnung des Bundesministers für Wissenschaft und Verkehr über die Nummerierung (Nummerierungsverordnung – NVO), BGBl II 416/1997.

[46] So auch *Parschalk/Zuser/Otto,* Telekommunikationsrecht (2002) 157. Offenbar auch dieser Ansicht, allerdings von IP-Adressen als passive Teilnehmernummern sprechend: *Jahnel,* Datenschutz im Internet - Rechtsgrundlagen, Cookies und Web-Logs, ecolex 2001, 84.

eine Wohnadresse. Zu diesem Ergebnis gelangen auch die EB zum TKG 2003 (dazu gleich). E-Mail Adressen sind daher nach TKG 1997 kein Stammdatum.[47]

bb) Vermittlungsdaten (§ 87 Abs 3 Z 5 TKG 1997)

Vermittlungsdaten sind alle personenbezogenen Daten, die sich auf Teilnehmer und Benutzer beziehen, und für den Aufbau einer Verbindung oder für die Verrechnung von Entgelten erforderlich sind. Dies sind abschließend: aktive und passive Teilnehmernummern, Anschrift des Teilnehmers, Art des Endgerätes, Gebührencode, Gesamtzahl der für den Abrechnungszeitraum zu berechnenden Einheiten, Art, Datum, Zeitpunkt und Dauer der Verbindung, übermittelte Datenmenge, und andere Zahlungsinformationen, wie Vorauszahlung, Ratenzahlung, Sperren des Anschlusses oder Mahnungen.

Teilnehmernummern, und damit IP-Adressen, können daher sowohl Stamm- als auch Vermittlungsdaten sein. Mit Anschrift ist jedenfalls nur die Wohnadresse gemeint, und keine E-Mail Adresse.

cc) Inhaltsdaten (§ 87 Abs 3 Z 6 TKG 1997)

Hierunter sind grundsätzlich alle Inhalte übertragener Nachrichten zu verstehen.

b) Neue Rechtslage: TKG 2003

Mit 20.08.2003 trat das TKG 2003 in Kraft[48], mit dem der neue EU-Rechtsrahmen für elektronische Kommunikationsnetze und -dienste mit knapp einmonatiger Verspätung umgesetzt wurde. Über manche Themen, wie die Mobilnummernportierung und den Kostenersatz für die technischen Einrichtungen für die Überwachung des Fernmeldeverkehrs konnte mit den Diensteanbietern keine Einigung erzielt werden. Sie wurden daher dem Verordnungsgeber bzw einer kleinen Novelle des neuen Gesetzes vorbehalten.[49]

Dieser neue Rechtsrahmen besteht aus folgenden fünf Richtlinien:

---

[47] Dies gilt allerdings nicht unbedingt auch für andere Gesetze, und ist in concreto zu prüfen. Bei E-Mail Adressen sind grundsätzlich zwei unterschiedliche Fragestellungen zu unterscheiden: Die Beauskunftung der E-Mail Adresse selbst und die Identifikation anhand einer E-Mail Adresse, maW wer hinter der E-Mail Adresse steht.

[48] Bundesgesetz: Erlassung eines Telekommunikationsgesetzes und Änderung des Bundesgesetzes über die Verkehrs-Arbeitsinspektion und des KommAustria-Gesetzes, BGBl I 70/2003 (NR: GP XXII RV 128 AB 184 S. 29.BR: 6800 AB 6804 S. 700.) [CELEX-Nr.: 32002L0019, 32002L0020, 32002L0021, 32002L0022, 32002L0058].

[49] Zur Geschichte dieses Gesetzes, welches ebenso wie die UrhG-Novelle dem vorzeitigen Ende der XXI. Legislaturperiode zum Opfer fiel: Das Ende der "Holzhammerregulierung", orf futurezone, http://futurezone.orf.at/futurezone.orf?read=detail&id=179429 . Von dort gelangt man mittels Links auch zu den älteren Artikeln.

- Richtlinie 2002/19/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung (Zugangsrichtlinie), ABl L 108 vom 24.4.2002, 7;
- Richtlinie 2002/20/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über die Genehmigung elektronischer Kommunikationsnetze und -dienste (Genehmigungsrichtlinie), ABl L 108 vom 24.4.2002, 21;
- Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie), ABl L 108 vom 24.4.2002, 33;
- Richtlinie 2002/22/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten (Universaldienstrichtlinie), ABl L 108 vom 24.4.2002, 51;
- Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl L 201 vom 31.7.2002, 37.

Eine kompakte Darstellung der Neuerungen (außer der Datenschutz-RL) findet sich bei *Parschalk/Zuser/Otto,* TKR 2 ff und bei *Brandl,* Telekommunikationsrecht, in: *Jahnel/Schramm/Staudegger* (Hrsg), Informatikrecht[2] 276.

Im Rahmen dieser Arbeit wird jeweils bei den einzelnen Bestimmungen sowohl auf die alte, als auch auf die neue Rechtslage eingegangen.[50]

Die oben genannten Begriffsbestimmungen werden jetzt in § 92 TKG 2003 geregelt. Die EB[51] zu § 93 merken hierzu an, dass sich diese Begriffe an der bereits erwähnten Datenschutz-RL für elektronische Kommunikation orientieren.

aa) Stammdaten (§ 92 Abs 3 Z 3 TKG 2003)

Gem § 92 Abs 3 Z 3 TKG 2003 sind Stammdaten alle personenbezogenen Daten, die für die Begründung, Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind. Es handelt sich um: Familienname und Vorname, akademischer Grad, **Wohn**adresse, Teilnehmernummer **und sonstige Kontaktinformation für die Nachricht**, **Information über Art und Inhalt des Vertragsverhältnisses**, und Bonität.

Die EB[52] führen hierzu aus, dass nun klargestellt ist, dass mit Adresse nur die Wohnadresse gemeint sei, nicht aber eine E-Mail-, Netzwerk- oder IP-Adresse. Diese Informationen seien mit dem Begriff der *„Teilnehmernummer*

[50] Im Text werden diese Änderungen gegebenenfalls fett hervorgehoben.

[51] Regierungsvorlage zum TKG 2003, 128 BlgNR XXII. GP 18, http://www.parlinkom.gv.at/pd/pm/XXII/I/texte/001/I00128__4832.pdf .

[52] 128 BlgNR XXII. GP 17 f.

und sonstigen Kontaktinformation" und bei den Verkehrsdaten angesprochen. Neben der reinen Teilnehmernummer im Bereich der Sprachtelephonie, seien auch alle sonstigen benötigten Kontaktadressen des Teilnehmers für die Nachrichtenübermittlung an diesen konkreten Teilnehmer umfasst. Als Beispiele werden eine vom Betreiber bereitgestellte E-Mail-Adresse oder sonstige ähnlich individuelle dauerhafte Rufzeichen oder Kennungen, etwa die individuelle Kennung bei Selektivrufen im Funkbereich, genannt. In Abweichung von der alten Rechtslage gehören daher E-Mail Adressen nunmehr zu den Stammdaten.[53] Fraglich ist, ob die Erweiterung dieser Definition gegen die oben geäußerte Ansicht spricht, IP-Adressen wären als Teilnehmernummern ieS zu qualifizieren. Nicht eindeutig ist nämlich, ob der Gesetzgeber nur eine Klarstellung oder eine echte Änderung wollte. ME ist von ersterem auszugehen.

bb) Verkehrsdaten (§ 92 Abs 3 Z 4 TKG 2003)

Gem § 92 Abs 3 Z 4 TKG 2003 sind unter Verkehrsdaten solche Daten zu verstehen, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden. Dieser Begriff entspricht im Wesentlichen den Vermittlungsdaten der alten Rechtslage, enthält aber keine nähere Aufzählung mehr. Auffällig ist, dass die Daten nicht mehr personenbezogen sein müssen, um als Verkehrsdaten qualifiziert werden zu können (vgl noch § 87 Abs 3 Z 5 TKG 1997). Die EB[54] verweisen zur näheren Konkretisierung auf den 15. ErwGr der Datenschutz-RL, welcher demonstrativ folgendende Daten aufzählt: Aktive und passive Teilnehmernummer, die Art des Endgeräts, den Tarifcode, die Gesamtzahl der für den Abrechnungszeitraum zu berechnenden Einheiten, die Art, das Datum, den Zeitpunkt und die Dauer der Verbindung **oder sonstige Nutzung**, die übermittelte Datenmenge, **die Leitwege, das verwendete Protokoll, das Netz, von dem die Nachricht ausgeht oder an das sie gesendet wird, das Format der Nachricht,** sowie andere Zahlungsinformationen, wie Vorauszahlung, Ratenzahlung, Sperren des Anschlusses oder Mahnungen.

Außerdem enthält das TKG 2003 jetzt eine eigene Begriffsdefinition der Standortdaten - die bislang iaR als Vermittlungsdaten qualifiziert wurden - und zwar als Unterfall der Verkehrsdaten (siehe auch im Kapitel Strafprozessordnung und Telekommunikationsgesetz, S 56, und die EB zu § 93). Insbes die Normierung von *Location Based Services* machte eine solche Definition aber notwendig. Gem § 92 Z 6 sind Standortdaten *„Daten, die in einem Kommunikationsnetz verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben;"*.

---

[53] Wobei allerdings zweifelhaft ist, ob eine E-Mail Adresse immer zur Begründung, Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich ist.

[54] aaO.

Aufgrund des Abänderungsantrages des Verkehrsausschusses[55] wurde eine weitere Definition in das Gesetz aufgenommen. Einen Unterfall der Verkehrsdaten stellen gem § 92 Abs 3 Z 4a die Zugangsdaten dar. Dies sind *„jene Verkehrsdaten, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz beim Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierungen zum Teilnehmer notwendig sind.“* Zur Begründung wird im Abänderungsantrag angeführt, dass damit alle Daten gemeint sein sollen, die zur Identifikation eines Teilnehmers an einer Internetkommunikation notwendig sind. Das TKG 2003 enthält jedoch keine gesonderten Regelungen für Zugangsdaten. Es ist wohl zu vermuten, dass diese Definition zu Verweiszwecken aus anderen Gesetzen eingeführt worden ist oder sich im Rahmen einer Novelle als brauchbar erweisen kann.

cc) Inhaltsdaten (§ 92 Abs 3 Z 5 TKG 2003)

Die Definition der Inhaltsdaten ist gleich geblieben. Gem § 92 Z 7 ist eine Nachricht "*jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet wird“*, wobei ausgeschlossen wird, dass damit auch Rundfunkdienste gemeint sein sollen. Der Gesetzgeber definiert auch die *„elektronische Post“*, worunter gem Z 10 leg cit *„jede über ein öffentliches Kommunikationsnetz verschickte Text-, Sprach-, Ton- oder Bildnachricht, die im Netz oder im Endgerät des Empfängers gespeichert werden kann, bis sie von diesem abgerufen wird.“* zu verstehen ist. In diesem Zusammenhang bemerken die EB[56], dass für *„die Zwecke der Definition der elektronischen Post insbesondere auch Computer als ‚Endgeräte' zu werten“* sind.[57]

2. Das Fernmeldegeheimnis

a) Art 10a StGG

Art 10a StGG bezweckt - ebenso wie Art 10 StGG (Briefgeheimnis) – den Vertraulichkeitsschutz von im Wege der Telekommunikation übermittelter Information vor staatlichen Eingriffen.[58] Diese Bestimmung schützt daher ausschließlich Inhaltsdaten - nicht aber auch Vermittlungsdaten[59] - vor Kenntnisnahme durch die öffentliche Gewalt.

---

[55] Bericht des Verkehrsausschusses, 184 BlgNr XXII. GP, http://www.parlinkom.gv.at/pd/pm/XXII/I/texte/001/I00184__5449.pdf .

[56] aaO.

[57] Siehe dazu Näheres im Kapitel Strafprozessordnung und Telekommunikationsgesetz, S 56.

[58] Vgl *Wiederin* in: *Korinek/Holoubek* (Hrsg), Österreichisches Bundesverfassungsrecht III StGG Art 10a Rz 3.

[59] Dies ist allerdings strittig: Gegen einen Schutz von Vermittlungsdaten durch Art 10a StGG: *W Wessely,* Das Fernmeldegeheimnis - ein unbekanntes Grundrecht?, ÖJZ 1999, 491, und *Wiederin* in: *Korinek/Holoubek*, StGG Art 10a Rz 12, jeweils mit Hinweisen zur Gegenansicht.

Eingriffe in Art 10a StGG bedürfen ausnahmslos eines richterlichen Befehls.[60]

b) Art 8 EMRK

Art 8 EMRK gewährt einen fast umfassenden Persönlichkeitsschutz zur Absicherung des privaten Bereichs eines Individuums vor staatlichen Eingriffen. Auskunfts- und Meldepflichten, auch wenn sie juristischen Personen obliegen, können in dieses Recht eingreifen.[61] Der Schutzbereich des Art 8 EMRK umfasst auch die Überwachung des Fernmeldeverkehrs.[62] Neben Inhaltsdaten (die aber bereits durch Art 10a StGG geschützt werden; diese Bestimmung ist wohl iSd Art 53 EMRK durch das formelle Erfordernis des richterlichen Befehls ausnahmsweise das günstigere Grundrecht), unterliegen dem Schutzbereich dieser Bestimmung auch Vermittlungsdaten.[63] Nach der Jud des EGMR muss nicht notwendigerweise der Staat selbst - durch seine Organe - geschützte Daten ermitteln oder die Datenerhebung veranlassen, um in den Schutzbereich des Art 8 EMRK einzugreifen. Es genügt, wenn staatliche Stellen lediglich auf bereits vorhandene Datenbestände zurückgreifen.[64]

Im Unterschied zu Art 10a StGG, steht Art 8 EMRK unter einem materiellen Gesetzesvorbehalt. Für einen Eingriff bedarf es – wie bereits erwähnt - im Gegensatz zu Art 10a StGG aber nur einer gesetzlichen Ermächtigung, und keines richterlichen Befehls.[65] Der EGMR hat in der Vergangenheit ausgesprochen, dass eine gesetzliche Eingriffsgrundlage der „Trias“ Existenz, Zugänglichkeit und Vorhersehbarkeit entsprechen muss. In jüngeren Entscheidungen gewinnt das Kriterium der Rechtsstaatlichkeit jedoch immer mehr an eigenständiger Bedeutung.[66] Die ersten beiden Kriterien bereiten im Rahmen der österreichischen Rechtsordnung kaum Schwierigkeiten.[67] Eine Regelung ist vorhersehbar, wenn sie hinreichend bestimmt formuliert ist, damit der Normadressat – wenn auch nach entsprechender rechtlicher Beratung – Umstände und Bedingungen staatlichen Handelns voraussehen, und die Konsequenzen eigenen Verhaltens absehen kann. Eine genauere Bestimmung kann auch durch die einschlägigen Materialien bzw durch eine einheitliche Spruchpraxis erfolgen.[68] Laut Jud des

---

[60] Absoluter Richtervorbehalt. Hierauf explizit hinweisend: *Reindl*, Die nachträgliche Offenlegung von Vermittlungsdaten *des* Telefonverkehrs im Strafverfahren ("Rufdatenrückerfassung"), JBl 1999, 791. Vgl auch mwN *Wiederin* in: *Korinek/Holoubek*, StGG Art 10a Rz 19.

[61] Vgl *Öhlinger,* Verfassungsrecht[5] (2003) Rz 812.

[62] Vgl *Öhlinger,* Verfassungsrecht[5] Rz 826.

[63] Vgl *W Wessely,* aaO.

[64] EGMR 2.8.1984 *Malone/Vereinigtes Königreich* Rz 86 = EuGRZ 1985, 23.

[65] Vgl *W Wessely,* aaO.

[66] Vgl *Wiederin* in: *Korinek/Holoubek*, EMRK Art 8 Rz 16 und 20 mwN, der dieses Kriterium jedoch für entbehrlich hält.

[67] Einerseits wegen Art 18 B-VG, andererseits wegen dem BGBlG (Kundmachungsvorschriften sind nicht in allen Konventionsstaaten selbstverständlich). Näheres siehe bei *Wiederin* in: *Korinek/Holoubek*, EMRK Art 8 Rz 17 und 18.

[68] *Wiederin* in: *Korinek/Holoubek*, EMRK Art 8 Rz 19.

EGMR stellt die Überwachung des Fernmeldeverkehrs einen besonders schweren Eingriff in das Privatleben dar.[69]

Die hinreichende Konkretisierung der Rechtsgrundlage ist aus folgenden Erwägungen von besonderem Interesse: Soll die Identität eines Nutzers festgestellt werden, so handelt es sich hier iaR um Stammdaten. Dies ist aber nicht immer der Fall. Soll festgestellt werden, welche dynamische IP-Adresse einem Nutzer zu einem bestimmten Zeitpunkt zugeordnet war (oder viceversa), so hat der ISP Vermittlungsdaten zu erheben.[70] Ausgehend von der Jud des EGMR, stellt die Anordnung der Aushebung dieser Daten durch eine Behörde einen Eingriff in Art 8 EMRK dar, wobei der ISP in diesem Falle nur als verlängerte Hand fungiert. Es ist daher jede Rechtsgrundlage, mit der eine Auskunfts- oder Mitwirkungspflicht normiert wird, dahingehend zu prüfen, ob diese auch Vermittlungsdaten umfassen soll, und in weiter Folge, einen Eingriff in das Fernmelde- bzw Telekommunikationsgeheimnis erlaubt.[71] Von diesem Ansatz geht offenbar ebenfalls die StPO aus, denn § 149a Abs 1 schützt auch Stammdaten, wenn diese das Ergebnis einer Überwachung der Telekommunikation sind.

c) Weitere Ausführungsbestimmungen des TKG

aa) Alte Rechtslage: Das TKG 1997

Die Wahrung des Fernmeldegeheimnisses obliegt gem § 88 Abs 1 und 2 TKG 1997 den Betreibern (das sind Anbieter von öffentlichen Telekommunikationsdiensten) und allen Personen, die an der Tätigkeit des Unternehmens mitwirken. Wie bereits erwähnt, unterliegen dem Fernmeldegeheimnis Inhalts- und Vermittlungsdaten[72], wobei auch die näheren Umstände erfolgloser Verbindungsversuche umfasst sind. Diese Pflicht ist gem § 103 mit gerichtlicher Strafe bedroht. Nicht sanktioniert ist die Bestimmung des § 88 Abs 3, die eine Pflicht zur Einhaltung der Vertraulichkeit für jedermann normiert. Abs 4 verpflichtet überdies zur Geheimhaltung des Inhalts irrtümlicherweise empfangener Nachrichten.

---

[69] EGMR 16.2.2000 *Amann/Schweiz* Rz 56; vgl auch EGMR 24.4.1990 *Kruslin/Frankreich* Rz 33; EGMR 16.2.2000 *Amann/Schweiz* Rz 56, et alt. Der EGMR wendet hier einen dem österreichischen differenzierten Legalitätsprinzip vergleichbaren Grundsatz an.

[70] Vgl *Österreichische Akademie der Wissenschaften*, Beeinträchtigung der Privatsphäre in Österreich I (2000), http://www.oeaw.ac.at/ita/ebene5/d2-2a24a.pdf , 22. Über die rechtliche Bedeutung hat man sich allerdings in Österreich – im Gegensatz zu Deutschland – noch kaum Gedanken gemacht. Vgl zB *Landesbeauftragter für Datenschutz in Niedersachsen*, Orientierungshilfe für den Umgang mit personenbezogenen Daten http://www.lfd.niedersachsen.de/functions/downloadObject/0,,c1225720_s20,00.pdf , 7.

[71] Siehe bei den einzelnen Rechtsgrundlagen.

[72] Wörtlich heißt es: *"die näheren Umstände der Kommunikation, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war"*.

Strafrechtliche Sanktionen der Verletzung des Fernmeldegeheimnisses für jedermann sehen die §§ 119 ff StGB vor.

bb) Neue Rechtslage: Das TKG 2003

Die oben dargestellten Ausführungsbestimmungen sind nunmehr in § 93 TKG 2003 geregelt. Den EB[73] zu Folge handelt es sich hier überwiegend um Klarstellungen und Anpassungen. § 108 TKG 2003 bedroht den Verstoß gegen § 93 Abs 2 TKG 2003 (Geheimhaltungspflichten der Betreiber) mit gerichtlicher Strafe.

Exkurs: ISP als Betreiber öffentlicher (Tele-)Kommunikationsdienste

> § 87 Abs 1 Z 1 TKG 1997 definiert den Betreiber als *„Anbieter von Telekommunikationsdiensten iSd 3. Abschnitts"*. Ein Telekommunikationsdienst ist gem § 3 Z 14 TKG 1997 die gewerbliche Dienstleistung, die in der Übertragung und/oder Weiterleitung von Signalen auf Telekommunikationsnetzen besteht. Wie *Parschalk/Zuser/Otto*[74] ausführen, sind vor allem Access- und Backbone-Provider[75] unter diesen Begriff zu subsumieren, sofern sie keine bloßen Wiederverkäufer sind. Sie verwenden zur Weiterleitung bzw zur Übertragung *Router* oder *Switches* (also Vermittlungseinheiten). Ob ein Host-Provider Anbieter von Telekommunikationsdiensten ist, ist im Einzelfall anhand seiner konkreten Tätigkeit zu beurteilen. Betreibt der Host-Provider die Internetanbindung seines Host-Rechners (konkret: die damit verbundenen Übertragungs- und/oder Routing-Leistungen) selbst oder hat er hierfür Mietleitungen angeschafft, so kann man ihn als Anbieter von Telekommunikationsdiensten qualifizieren.[76]
>
> § 87 Abs 1 Z 1 TKG 1997 entspricht zwar dem § 92 Abs 1 Z 1 TKG 2003, dreht die Definition aber in diesem Sinne um, als jetzt der Anbieter als Betreiber von öffentlichen Kommunikationsdiensten umschrieben wird.
>
> Betreiber iSd TKG 2003 ist gem § 3 Z 1 *„ein Unternehmen, das ein öffentliches Kommunikationsnetz oder eine zugehörige Einrichtung bereitstellt, oder zur Bereitstellung hiervon befugt ist"*. Z 3 leg cit enthält auch eine spezielle Definition für das Betreiben von Kommunikationsdiensten: "*das Ausüben der rechtlichen Kontrolle über die Gesamtheit der Funktionen, die zur Erbringung des jeweiligen Kommunikationsdienstes notwendig sind"*. Angemerkt sei, dass der Begriff der Telekommunikation fast vollständig von jenem der Kommunikation abgelöst wurde. Unter Kommunikationsdienst ist gem Z 9 leg cit zu verstehen: Die *„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*

---

[73] aaO.

[74] TKR 153 f.

[75] Zu diesen Begriffen siehe weiter unten, S 4 ff.

[76] Vgl *Otto/Parschalk,* Anzeige- und Konzessionspflicht von Internet Service Providern nach dem TKG, MR 2001, 420.

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;".[77] Abweichend von der alten Rechtslage, ist auch der Wiederverkauf von Kommunikationsdiensten mitumfasst, soferne der Dienst nicht nur eine Nebenleistung darstellt.[78]

Des weiteren zählt § 3 Z 10 bei der Definition des Kommunikationsnetzes das Internet explizit zu den anderweitigen Ressourcen, welche die elektronische Übertragung von Signalen über feste Netze ermöglichen.

Diese Begriffsfülle erscheint kaum gelungen, auch wenn die Konzessionspflicht nach § 14 TKG 1997 gefallen ist, und somit jedes Telekommunikationsunternehmen zur Bereitstellung von Kommunikationsnetzen berechtigt ist, sobald es die Aufnahme seiner Tätigkeit anzeigt (vgl § 14 TKG 2003). Materielle Änderungen zur alten Rechtslage sind mE nicht ersichtlich.

3. Recht auf Datenschutz

a) Datenschutzgesetz 2000[79]

Das Grundrecht auf Datenschutz iSd § 1 DSG enthält Ansprüche auf Geheimhaltung, Auskunft und Richtigstellung bzw Löschung von personenbezogenen Daten, soweit schutzwürdige Geheimhaltungsinteressen daran bestehen. Eingriffe sind im Rahmen des materiellen Gesetzesvorbehalts zulässig, welcher wortgleich mit Art 8 Abs 2 EMRK ist und einen Verweis auf diesen enthält. Es ist bislang das einzige Grundrecht der österreichischen Rechtsordnung, das mit unmittelbarer Drittwirkung ausgestattet ist (§ 1 Abs 5). Gem § 4 Z 1 sind personenbezogene Daten Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist. Somit genießen auch Stammdaten „grundrechtlichen" Schutz.

Das Problem, dass zwischen dynamischen und statischen IP-Adressen differenziert werden muss, stellt sich in diesem Zusammenhang nicht, denn aus der Sicht des Access-Providers als Verwender der Daten[80] sind IP-Adressen – gleich ob dynamisch oder statisch – immer personenbezogene Daten.[81] Dies natürlich unter der Voraussetzung, dass die Daten überhaupt noch vorhanden sind.

---

[77] ME sollen mit den letzten beiden Sätzen Content Provider von der Definition ausgenommen werden.

[78] aaO 4.

[79] BG über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000) (NR: GP XX RV 1613 AB 2028 S 179. BR: 5992 AB 6034 S 657.) (CELEX-Nr: 395L0046) StF: BGBl I 165/1999 idF BGBl I 136/2001 (NR: GP XXI RV 742 AB 824 S 81. BR: 6458 AB 6459 S 681).

[80] Vgl *Drobesch/Grosinger,* Datenschutzgesetz (2000) 113.

[81] Vgl auch *Jahnel,* der die Ansicht vertritt, dynamische IP-Adressen seien nur indirekt-personenbezogene Daten (Datenschutz im Internet - Rechtsgrundlagen, Cookies und Web-Logs, ecolex 2001, 84). Dies jedoch in Bezug auf Web-Logs, dh

§ 15 verpflichtet den Auftraggeber, den Dienstleister und seine Mitarbeiter zu Wahrung des Datengeheimnisses, dh sie *„haben Daten aus Datenanwendungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen Daten besteht.“*.

Neben dem Straftatbestand des § 51 (Datenverwendung in Gewinn- oder Schädigungsabsicht), enthält § 52 ua folgende Verwaltungsübertretungen, die mit Geldstrafen bis zu Euro 18.890 bedroht sind: Die vorsätzliche Verletzung des Datengeheimnisses iSd § 15, die Verweigerung der Auskunft, der Richtigstellung oder der Löschung, obwohl ein rechtskräftiges Urteil oder ein rechtskräftiger Bescheid vorliegt, sowie die Löschung von Daten, obwohl bereits ein Auskunftsverlangen eingebracht wurde.[82]

Exkurs: Datenweitergabe nach DSG

Auskunftspflichten bedingen denknotwendig eine Datenweitergabe. § 7 Abs 2 normiert die Voraussetzungen für eine rechtmäßige Datenübermittlung. Unter Datenübermittlung versteht § 4 Z 12 die Weitergabe von Daten einer Datenanwendung[83] an einen Dritten, insbes auch die Veröffentlichung von Daten und die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers.

aa) 1. Prüfungsschritt: § 7 Abs 2 (Datenübermittlung)

Eine Datenübermittlung ist unter folgenden Voraussetzungen zulässig:

1. Die Daten müssen aus einer zulässigen Datenanwendung stammen.
2. Der Dritte muss glaubhaft machen, dass er eine gesetzliche Zuständigkeit bzw eine rechtliche Befugnis[84] zur Erlangung der Daten hat.
3. Schutzwürdige Geheimhaltungsinteressen des Betroffenen[85] dürfen nicht verletzt werden.

Punkt 1. ist bei Kundendaten unproblematisch.[86] Punkt 2. ist wohl bei Bestimmungen wie § 18 Abs 4 ECG, die Befugnisse nach dem SPG usw erfüllt.

---

nicht aus der Sicht des Access-Providers. Vgl auch *Brandl,* Datenschutz im Internet, in: *Studiengesellschaft für Wirtschaft und Recht* (Hrsg), Internet und Recht – Rechtsfragen von E-Commerce und E-Government 128.

[82] Je nach Inhalt der Auskunftspflicht kann auch uU das Fernmeldegeheimnis verletzt sein. Zu den Sanktionen siehe dort.

[83] Vgl § 4 Z 7.

[84] Das sind im privaten Bereich bspw Vereinstatuten oder Berufsausübungsvorschriften (Vgl *Drobesch/Grosinger,* Datenschutzgesetz 135).

[85] Vgl § 4 Z 3, das ist jene Person, deren Daten verwendet werden.

[86] Vgl Standardanwendung 22 der VO des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2000 - StMV) StF: BGBl II 201/2000 idF BGBl II 232/2003.

bb) 2. Prüfungsschritt: § 8 (Verletzung schutzwürdiger Geheimhaltungsinteressen bei nicht-sensiblen Daten)

Bei der Prüfung, ob schutzwürdige Geheimhaltungsinteressen des Betroffenen verletzt werden, ist zu differenzieren, ob sensible[87] oder nicht-sensible Daten weitergegeben werden. Kundendaten von Providern sind iaR nicht-sensible Daten, weshalb für die Prüfung, ob schutzwürdige Geheimhaltungsinteressen verletzt sind, § 8 zu Anwendung kommt.

> *„§ 8. (1) Gemäß § 1 Abs. 1 bestehende schutzwürdige Geheimhaltungsinteressen sind bei Verwendung nicht-sensibler Daten dann nicht verletzt, wenn*
> *1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung der Daten besteht oder*
> *2. der Betroffene der Verwendung seiner Daten zugestimmt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt, oder*
> *3. lebenswichtige Interessen des Betroffenen die Verwendung erfordern oder*
> *4. überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern.*[…]*“*

Z 1 bezieht sich nur auf ausdrückliche Rechtsgrundlagen[88]. Hierauf kann man die Datenübermittlungen nach § 53 SPG, der StPO, des § 99 Abs 3 FinStrG etc stützen. Z 2 und Z 3 werden hier iaR nicht anwendbar sein[89].

Abs 1 Z 4 erfährt eine nähere Konkretisierung in Abs 3, der eine demonstrative Aufzählung enthält, wann iSd Z 4 die schutzwürdigen Geheimhaltungsinteressen nicht verletzt sind:

> *„(3) Schutzwürdige Geheimhaltungsinteressen sind aus dem Grunde des Abs. 1 Z 4 insbesondere dann nicht verletzt, wenn die Verwendung der Daten*
>
> *1. für einen Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe ist oder*
> *2. durch Auftraggeber des öffentlichen Bereichs in Erfüllung der Verpflichtung zur Amtshilfe geschieht oder*
> *3. zur Wahrung lebenswichtiger Interessen eines Dritten erforderlich ist oder*
> *4. zur Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeber und Betroffenem erforderlich ist oder*
> *5. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder* […]*“.*

---

[87] Vgl § 3 Z 2, das sind Daten über rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder das Sexualleben.

[88] Vgl *Drobesch/Grosinger,* Datenschutzgesetz 138.

[89] Denkbar wäre allerdings eine Anwendbarkeit bei Betreibern mobiler Sprachtelephonie, zB bei einer Weitergabe von Standortdaten zur Rettung eines Lawinenopfers. Siehe dazu auch unten im Kapitel Strafprozessordnung und Telekommunikationsgesetz, S 62, und Sicherheitspolizeigesetz, S 72.

Das Erfordernis der wesentlichen Voraussetzung iSd Z 1 ist nicht als *condition sine qua non* zu verstehen, sondern als wesentliche Erleichterung des Verwaltungshandelns.[90] Z 2 betrifft vorwiegend das PolizeikooperationsG[91]. Unter „*lebenswichtigen Interessen"* sind keine Fälle zu verstehen, bei denen der Dritte lediglich eine Vermögenseinbuße erleiden würde (siehe dazu S 19 in der FN). Z 5 zählt nur den Auftraggeber selbst auf, nicht aber den Dritten. Folglich können Auskunftspflichten nach § 18 Abs 4 ECG und § 87b UrhG auf diese Ausnahme nicht gestützt werden, sodass die Weitergabe von Daten an Dritte zwecks Rechtsverfolgung nach der allgemeinen Generalklausel des § 8 Abs 1 Z 4 zu beurteilen ist. Es ist daher im Einzelfall zu prüfen, wessen Interessen überwiegen: jene des Betroffenen auf Geheimhaltung oder jene des Dritten auf Rechtsverfolgung.

Zu den zivilrechtlichen Sanktionen bei Datenübermittlungen entgegen den Bestimmungen des DSG siehe im Kapitel E-Commerce-Gesetz, S 41.

b) Alte Rechtslage: TKG 1997

Das Sonderdatenschutzrecht des TKG 1997 enthält verschiedene Bestimmungen zur Datensicherheit, Legitimität der Datenverarbeitung und Auskunftspflichten (betreffend die verarbeiteten Daten und der Dauer der Speicherung).[92]

Stammdaten dürfen gem § 92 nur zu Vertragszwecken, zur Verrechnung der Entgelte und zur Erstellung von Teilnehmerverzeichnisses ermittelt und verarbeitet werden. Sie sind grundsätzlich nach Ende der Vertragsbeziehungen mit dem Teilnehmer zu löschen.

Vermittlungsdaten sind gem § 93 Abs 1 grundsätzlich nach Beendigung der Verbindung zu löschen oder zumindest zu anonymisieren. Dies gilt allerdings nicht, wenn sie für die Entgeltverrechnung benötigt werden bzw kehrt Abs 2 diesen Grundsatz geradezu um, als er bestimmt, dass die Betreiber innerhalb der Verjährungsfrist bzw der Einspruchsfrist zur Aufbewahrung dieser Daten verpflichtet sind, wobei 6 Monate ab Rechnungslegung branchenüblich sind.[93] Zur Entgeltverrechnung sind Vermittlungsdaten insbes dann notwendig, wenn der Access-Provider zeit- oder volumenabhängig abrechnet, bspw bei *flat rate*-Tarifen mit beschränktem Downloadvolumen.[94]

---

[90] Vgl zB DSK 23.3.2001, 210.380/001-DSK/2001; DSK 18.05.2000, 120.686/3-DSK/00.

[91] So auch *Drobesch/Grosinger,* Datenschutzgesetz, 139. Siehe im Kapitel Sicherheitspolizeigesetz, 72.

[92] Den Auskunfts- bzw Informationspflichten wird meist durch Aufnahme in die AGB nachgekommen. Von einer weiteren Behandlung wird abgesehen.

[93] Was aber aus Kostengründen zT nicht gemacht wird. MwH: *Parschalk/Zuser/Otto,* TKR 133 f, die gem § 1486 ABGB eine Verjährungsfrist von 3 Jahren ab Fälligkeit annehmen. Siehe auch: *Prachner,* Datenschutz in der Telekommunikation, in: *Forgó/Feldner/Witzmann/Dieplinger* (Hrsg), Probleme des Informationsrechts (2003), 362 = http://www.it-law.at/papers/intern/mt-Pracher.Datenschutz.pdf , 11.

[94] Siehe *Prachner,* Datenschutz in der Telekommunikation, 363 = http://www.it-law.at/papers/intern/mt-Pracher.Datenschutz.pdf , 12. Insbes bei *flat-rate* Accounts soll die Speicherung von Vermittlungsdaten idR nicht notwendig sein. Dies ist allerdings

Je nach Internetanbindung kann die Speicherung von Einwahlnummer, Datum, Uhrzeit, Dauer und Datenmenge notwendig sein. Mangels Einwahlnummer bei manchen Internetanbindungen, kann es für den Access-Provider ieS auch notwendig sein, die IP-Adresse zu speichern.[95] Durch diese Speicherverbote kommt es in praxi häufig zum Problem, dass ISP den Strafverfolgungsbehörden gar keine Auskunft über ältere Daten geben können, da diese bereits gelöscht sind.[96]

Inhaltsdaten sind gem § 95 unverzüglich zu löschen, es sei denn, ihre Speicherung ist der wesentliche Inhalt des Telekommunikationsdienstes.

c) Neue Rechtslage: TKG 2003

Das TKG 2003 enthält die einschlägigen datenschutzrechtlichen Bestimmungen in den §§ 96 bis 99. Grundsätzliche Änderungen ergeben sich mE nicht.

4. *Nemo-Tenetur*-Grundsatz

Aus dem Anklageprinzip im Strafprozess (Art 90 B-VG) wird vom VfGH, neben dem Recht auf Parteistellung eines Beschuldigten, auch sein Recht abgeleitet, nicht gezwungen zu werden, gegen sich selbst Zeugnis abzulegen (*nemo tenetur se ipsum accusare)*. Daraus folgt, dass man nicht zur Mitwirkung gezwungen werden darf, wenn man sich selbst belasten würde.[97] Der ISP darf daher sowohl Auskunft, als auch Mitwirkung verweigern, wenn er sich selbst der Gefahr einer verwaltungsstrafbehördlichen oder strafgerichtlichen Verfolgung aussetzen würde.[98]

5. Eigentum und Verbot der Zwangs- und Pflichtarbeit

Auskunfts-, und insbes Mitwirkungspflichten, greifen auch in das verfassungsmäßig garantierte Recht auf Eigentum[99], bzw in das Verbot der Zwangs- und Pflichtarbeit[100], ein.

---

strittig; vgl zur Lage in Deutschland: Datenschützer halten IP-Nummern-Speicherung für unzulässig, Heise Online, http://www.heise.de/newsticker/data/hod-21.01.03-000/ .

[95] Bspw bei Internetanbindungen mittels Telekabel. Vgl hierzu auch *Prachner,* Datenschutz in der Telekommunikation, 365 = http://www.it-law.at/papers/intern/mt-Pracher.Datenschutz.pdf , 15.

[96] Was aber des öfteren wohl eine bloße Behauptung ist. Vor dem Hintergrund dieser Problematik sind auch die einzelnen Auskunftspflichten zu sehen. Ein Verbot der Löschung solcher Daten bei Kenntnis der Strafverfolgung enthalten bspw der ISPA-Kodex, S 37, und der verfahrensrechtliche Teil der CCC, S 64.

[97] Vgl *Öhlinger,* Verfassungsrecht[5] Rz 971. Zum Strafprozess: *Seiler,* Strafprozessrecht[6] (2003) Rz 455; *Schmoller,* Erzwungene selbstbelastende Aussagen im Strafprozeß, Zugleich ein Beitrag zu den Beweisverwertungsverboten, JBl 1992, 69.

[98] MwH: *Berka,* Grundrechte (1999) Rz 850.

[99] Art 5 StGG, Art 1 1. ZPEMRK. Vgl hierzu: *Öhlinger,* Verfassungsrecht[5] Rz 867 ff.

[100] Art 7 StGG, Art 4 EMRK. Vgl hierzu: *Öhlinger,* Verfassungsrecht[5] Rz 754 f.

Providern entstehen oftmals nicht unbeträchtliche Aufwendungen, wenn sie aufgrund eines Auskunftsverlangens die gewünschten Daten ausheben sollen. Dies berührt grundsätzlich den Schutzbereich des Eigentumsrechts, denn nach der Jud des VfGH ist auch das Vermögen an sich eigentumsrechtlich geschützt.[101] Dem Großteil der hier behandelten Auskunftspflichten ist kostenlos nachzukommen (SPG, MBG, FinStrG). Das ECG äußert sich zu einem allfälligen Kostenersatz überhaupt nicht. Für die Überwachung des Fernmeldeverkehrs iSd StPO sah das TKG 1997 bis zum VfGH Erkenntnis v 27.02.2003[102] in seinem § 89 Abs 1 vor, dass die Mitwirkungsverpflichteten alle Einrichtungen bereitzustellen hätten, die zur Überwachung des Fernmeldeverkehrs nach den Bestimmungen der StPO erforderlich sind. Für die einzelne Mitwirkung war gem Abs 2 leg cit der Ersatz der angemessenen Kosten vorgeschrieben. Die Bereitstellung der Einrichtungen hatte nach Maßgabe des Abs 3 leg cit, der eine Verordnungsermächtigung vorsieht, zu erfolgen. Die auf dieser Grundlage ergangene ÜVO[103] ordnet für die Überwachung des Fernmeldeverkehrs als besonders kostspieliges Erfordernis an, dass die Schnittstellen, an der die zu überwachende Telekommunikation bereitgestellt wird, dem sog ETSI-Standard entsprechen müssen.[104] Der VfGH hob § 89 Abs 1 letzter S des TKG 1997 als verfassungswidrig auf, wobei er den Zeitpunkt des Inkrafttretens seines Erkenntnisses mit 31.12.2003 festlegte. Das Höchstgericht sprach aus, dass – im Einklang mit seiner stRsp - die Indienstnahme Privater zur Erfüllung behördlicher Aufgaben verfassungsrechtlich nicht zu beanstanden sei, aber die Tragung der Kosten nur durch die Betreiber dem Verhältnismäßigkeitsgrundsatz widerspräche, und nicht sachlich gerechtfertigt sei.[105] Die Bundesregierung brachte in diesem Zusammenhang als einziges Gegenargument lediglich „budgetäre Gründe“ vor. Das TKG 2003 berücksichtigt dieses Erkenntnis: Die Mitwirkungsverpflichtungen enthält nun § 94 Abs l leg cit und ist bis auf den letzten Satz (der eben jene „Kostenlosigkeit“ enthielt) wortgleich mit seiner Vorgängerbestimmung. § 94 Abs 3 TKG 2003 enthält wieder eine Verordnungsermächtigung.

---

[101] Vgl *Berka,* Grundrechte Rz 712.

[102] VfGH 27.2.2003, G 37/02-16, G 118/02-14, G 122/02-19 et alt.

[103] Verordnung der Bundesministerin für Verkehr, Innovation und Technologie über die Überwachung des Fernmeldeverkehrs (Überwachungsverordnung - ÜVO) BGBl II 418/2001.

[104] Die ETSI-Standards sind europarechtlich vorgeschrieben („Enfopol-Dokumente“). Vgl hierzu ausführlich: *Primig,* Verfahrensrechtliche Regelungsversuche der Telekommunikationsüberwachung auf europäischer Ebene (2002), http://www.rechtsprobleme.at/doks/primig-2-telekom-ueberwachung_europaeisch.pdf , 10, 18 ff. Eine übersichtliche Zusammenfassung betreffend Enfopol bieten auch *Philippi/Pracher,* Eingriffe in die Grundrechte von Betreibern und Konsumenten von Telekommunikationsdiensten durch polizeiliche Überwachungsmaßnahmen: Zu Natur und Konsequenzen einer europäischen Überwachungsverordnung (ENFOPOL-98-Dokument), http://www.it-law.at/papers/phillipi-pra-tretter.pdf .

[105] Der VfGH hat sich hier im Ergebnis auf den Gleichheitsgrundsatz berufen. Zum Verhältnis Eigentumsgarantie und Gleichheitssatz, insbes im Hinblick auf die Sonderopfertheorie, siehe *Berka,* Grundrechte Rz 735.

II. Ausgangsfälle

Um die Anwendbarkeit der einzelnen Rechtsgrundlagen zu veranschaulichen und zur Herstellung eines Praxisbezugs, werden im Folgenden sowohl reale, als auch fiktive Sachverhalte beschrieben. Die Beurteilung der Fälle erfolgt am Ende dieser Arbeit.

1. *RiAA* vs *Verizon*: Auskunft Access-Provider an einen Privaten

Die RIAA (Recording Industry Association of America) beantragte gem Art 512 des Digital Millennium Copyright Acts (DMCA[106]) die Erlassung eines Beschlusses gegen die Firma Verizon Internet Service - einem Access-Provider - mit dem Inhalt, ein Auskunftsbegehren betreffend der Identität eines Kunden von Verizon zu erzwingen. Dem betreffenden Kunden wurde vorgeworfen die peer-to-peer Software von Kazaa genutzt zu haben, um Musik online auszutauschen. Verizon lehnte die Auskunftserteilung mit der Begründung ab, es sei außerhalb des Anwendungsbereiches des DMCA. Im Jänner 2003 wurde der Antragstellerin in 1. Instanz Recht gegeben. Verizon focht die Entscheidung an, die in 2. Instanz bestätigt wurde.[107]

2. Variante *RiAA* vs *Verizon*: Beteiligung eines Strafgerichts

Die Antragstellerin wendet sich an ein Strafgericht, und beantragt dort die Bestrafung des Kunden des Providers gem § 86 Abs 1 Z 3 iVm § 91 UrhG[108] wegen unerlaubten öffentlichen Zurverfügungstellen, und gibt gleichzeitig eine IP-Adresse bekannt, mit der der Kunde vorgeblich an einem bestimmten Datum eingeloggt war. Das Strafgericht leitet ein Verfahren gegen unbekannten Täter ein, und stellt ein Auskunftsbegehren nach § 18 Abs 2 ECG iVm § 143 StPO an den Access-Provider.

3. Überwachung des Fernmeldeverkehrs auf Anordnung eines Gerichtes

A verbreitet in diversen Foren verbotsgesetzwidrige Äußerungen. Daraufhin leitet die Staatsanwaltschaft ein Verfahren gegen unbekannten Täter wegen

---

106 Abrufbar unter: http://www.loc.gov/copyright/legislation/dmca.pdf .

107 Siehe das RIAA v. Verizon Case Archive, http://www.eff.org/Cases/RIAA_v_Verizon/ . Vgl auch: US-Regierung unterstützt Musikindustrie, orf futurezone, http://futurezone.orf.at/futurezone.orf?read=detail&id=156066&tmp=44229 . Dies bestärkte die RiAA in ihrem Kampf gegen die Musiktauschbörsen, siehe zB RIAA mahnt Verizon-Kunden ab, orf futurezone, http://futurezone.orf.at/futurezone.orf?read=detail&id=165569&tmp=12520 ; Gesetzentwurf gegen Tauschbörsennutzer, orf futurezone, http://futurezone.orf.at/futurezone.orf?read=detail&id=172029 .

108 BG über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte, StF: BGBl 111/1936 idF UrhG-Nov 2003, BGBl I 32/2003.

§ 3h VerbotsG ein, und beantragt die Täterausforschung. Im ersten Schritt ordnet der Untersuchungsrichter die Überwachung der Vermittlungsdaten an. Daraus ergibt sich, dass sich A ausschließlich mit seinem Laptop mittels öffentlich zugänglichem, anonymen[109] WLAN[110] zum pre-paid Tarif verbindet. Der Provider verfügt somit über keine persönlichen Daten von A. Aufgrund der Daten beim Einloggen kann aber bestimmt werden, ob es sich jeweils um A handelt. Die Staatsanwaltschaft beantragt daher die Täterausforschung durch Standortanpeilung.

4. Auskünfte an Verwaltungsbehörden

I. A betreibt über seine Homepage einen Versandhandel mit pyrotechnischen Erzeugnissen - gem § 94 Z 18 GewO ein reglementiertes Gewerbe - ohne die Pflichtangaben nach § 5 ECG. Auch hat er die Domain unter einem falschen Namen registrieren lassen. Die Gewerbebehörde vermutet, dass A über keine Gewerbeberechtigung verfügt, und leitet daher ein Verwaltungsstrafverfahren gem § 366 Abs 1 Z 1 GewO ein.

II. A bietet überdies seine Waren ohne Verrechnung der Mehrwertsteuer über Ebay an.[111] Laut AGB ist Ebay berechtigt, personenbezogene Daten zu speichern. Die Finanzstrafbehörde leitet ein Verfahren wegen § 33 Abs 2 lit a FinStrG (Abgabenhinterziehung) ein.

III. Die Sicherheitsbehörden erfahren gleichfalls von diesen Vorfällen, und vermuten die Personenidentität von A mit einer bereits aktenkundigen Person, die mehrfach wegen einschlägiger Delikte vorbestraft ist. Die Sicherheitsbehörde leitet daher ein Verwaltungsstrafverfahren gem § 31 PyrotechnikG ein. Auch sie möchte vom Host-Provider den Namen des Täters erfahren.

5. Mobilfunkbetreiber als Access-Provider

Ein Mehrwertdiensteanbieter versendet SMS, in denen der Empfänger aufgefordert wird, eine Mehrwertdienstenummer anzurufen. Die SMS enthält folgenden Text: *"Ich habe mich in Dich verliebt und muss es Dir endlich sagen! Weißt Du, wer ich bin? Ruf zurück, 0900/xxx."*. Da der Hinweis auf die Kostenpflicht erst am Ende des SMS steht, besteht der Verdacht des Betrugs. Deshalb leitet die Staatsanwaltschaft ein Verfahren gegen unbekannte Täter ein. Auch die Bezirksverwaltungsbehörde leitet mit Ermittlungen wegen Verstoßes gegen § 107 Abs 2 TKG 2003.

---

[109] Solche Dienste bietet bspw die Firma metronet an; vgl die Standorte unter http://www.metronet.at/locations/standort.pl?tag=show&state=w .

[110] *Wireles Local Area Network* ermöglicht eine drahtlose Verbindung mit dem Internet über Funk. Zum Teil wird WLAN auf Universitäten angeboten (so auf der WU), zum Teil kann man in manchen Lokalen mittels einer Wertkarte WLAN verwenden. Näheres hierzu: *Lichtenstrasser/Mosing/Otto,* Wireless LAN - Drahtlose Schnittstelle für Datenmissbrauch?, ÖJZ 2003/14.

[111] Vgl die Fälle in Deutschland: Steuerprüfer nehmen eBay-User ins Visier, orf futurezone, http://futurezone.orf.at/futurezone.orf?read=detail&id=164949 .

III. Das E-Commerce-Gesetz

A. Anwendungsbereich

Wie bereits mehrfach erwähnt, nimmt das ECG direkten Bezug auf Access-, Cashing- und Host-Provider. Die genaue Abgrenzung des Anwendungsbereichs des ECG ist aber erforderlich, da seine Regelungen (Haftungsprivilegien, Auskunftspflichten etc) nur anwendbar sind, wenn der Diensteanbieter einen Dienst der Informationsgesellschaft iSd § 3 Z 1 bereitstellt und seinen Sitz im Inland hat.

1. Sachlicher Anwendungsbereich

Der sachliche Anwendungsbereich bestimmt sich primär durch den Begriff des Dienstes der Informationsgesellschaft (§ 3 Z 1).[112] Dies ist ein in der Regel gegen Entgelt elektronisch im Fernabsatz auf individuellen Abruf bereitgestellter Dienst, insbes der Online-Vertrieb von Waren und Dienstleistungen, Online-Informationsangebote, 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[113] speichern. Das Providing selbst ist daher bereits ein Dienst der Informationsgesellschaft.

Zur Definition des Dienstes der Informationsgesellschaft verweist die EC-RL auf Art 1 Z 2 der Transparenzrichtlinie[114], welche ein Notifikationsverfahren für technische Normen regelt. Die österreichische Umsetzung dieses Verfahrens erfolgte im NotifG[115], und übernahm dieses wörtlich die Definition aus der Transparenzrichtlinie. Entsprechend verweist § 3 Z 1 auf § 1 Abs 1 Z 2 NotifG, allerdings mit der geringfügigen sprachlichen Modifikation, dass es im ECG *„elektronisch* […] *bereitgestellter Dienst"* heißt, und das NotifG von *„elektronisch erbrachter Dienstleistung"* spricht.[116] Das NotifG enthält ebenso wie die Richtlinie einen Anhang mit

[112] Vgl *Brenn,* ECG 171.

[113] Unter Nutzer sind gem § 3 Z 4 ECG alle jene natürlichen und juristischen Personen und sonstigen rechtsfähigen Einrichtungen zu verstehen, die einen Dienst der Informationsgesellschaft in Anspruch nehmen. Dies unabhängig davon, ob zum Diensteanbieter ein vertragliches Verhältnis besteht oder nicht.

[114] Richtlinie 98/34/EG, ABl L 204 v 21.7.1998, 37, idF Änderungsrichtlinie 98/48/EG, ABl L 217 v 5.8.1998, 18.

[115] BG zur Durchführung eines Informationsverfahrens auf dem Gebiet der technischen Vorschriften, der Vorschriften für die Dienste der Informationsgesellschaft und der Normen (Notifikationsgesetz 1999 - NotifG 1999), BGBl I 1999/183.

[116] Gemeint ist allerdings das gleiche: Erfasst sein soll quasi alles was im Internet vertrieben wird.

einer demonstrativen Aufzählung, welche Dienste jedenfalls keinen Dienst der Informationsgesellschaft darstellen.

Zu betonen ist, dass nicht bereits das Medium[117] selbst der Dienst ist. Dies ist insbes bei der individuellen Kommunikation zu beachten: Eine E-Mail ist nicht schon für sich allein ein Dienst der Informationsgesellschaft. Der Dienst ist die dahinter stehende Dienstleistung, also bspw bei der Werbe-E-Mail die kommerzielle Kommunikation (vgl § 3 Z 6).[118]

a) In der Regel gegen Entgelt

Die EB[119] verweisen für den Begriff der Entgeltlichkeit auf die Jud des EuGH[120], wonach das Entgelt die wirtschaftliche Gegenleistung für die betreffende Leistung darstellen muss. Es sind somit nur jene Dienste erfasst, die unter Gewinnerzielungs- bzw Erwerbsabsicht erbracht werden. Staatlich bereitgestellte Dienste werden idR ohne dieser Absicht erbracht, weshalb der elektronische Zugang zu Firmen- und Grundbuch, zur Insolvenzdatei und zu sonstigen Dienstleistungen des elektronischen Rechtsverkehrs nicht in den Anwendungsbereich des ECG fallen, auch wenn für die Nutzung Gebühren verlangt werden.[121] Nicht notwendigerweise muss der Nutzer selbst den Dienst vergüten.[122] Daher fallen auch Websites, die unentgeltliche Dienste anbieten, und sich durch Bannerwerbung finanzieren, unter das ECG. Da aber schon Bannerwerbung reicht, um das Element der Entgeltlichkeit zu erfüllen, unterliegt auch die RIS-Datenbank[123] dem ECG.[124]

Des weiteren sind gem § 19 Abs 2 die Vorschriften der §§ 13 bis 19 Abs 1 auch auf Anbieter unentgeltlicher elektronischer Dienste anzuwenden. Unter diesen Bestimmungen finden sich auch die Auskunftspflichten, und ist das Kriterium der Entgeltlichkeit daher für vorliegende Arbeit von untergeordneter Bedeutung.

b) Auf individuellen Abruf des Empfängers

Diese Anforderung wird durch einen Dienst, der durch die Übertragung von Daten auf individuelle Anforderung erbracht wird, erfüllt.

> Gem lit C der Anlage 1 des NotifG zählen zu den nicht „auf individuellen Abruf eines Empfängers“ erbrachte Dienste, jene die im Wege einer Übertragung von

---

[117] Medium ist hier iwS zu verstehen und nicht nach dem Begriffsverständnis des MedienG.

[118] Die EB (abgedruckt in: *Brenn,* ECG 183) merken hierzu an: *„Damit soll das Missverständnis vermieden werden, dass elektronische Post als solche einen Dienst der Informationsgesellschaft bildet.“* Allerdings ist das Versenden von E-Mail als Vertriebsform sehr wohl ein Dienst der Informationsgesellschaft. Vgl auch *Blume/Hammerl,* ECG-Kommentar 48.

[119] Abgedruckt in: *Brenn,* ECG 183 ff.

[120] EuGH 7.12.1993, Rs C-109/92, *Wirth/Landeshauptstadt Hannover*, Slg 1993 I-06447 Rz 15.

[121] Vgl *Brenn,* ECG 191 f.

[122] Vgl 18. ErwGr der EC-RL.

[123] Rechtsinformationssystem des Bundes: http://www.ris.bka.gv.at .

[124] So auch *Zankl,* ECG-Handbuch Rz 72.

> Daten ohne individuellen Abruf gleichzeitig für eine unbegrenzte Zahl von einzelnen Empfängern erbracht werden (Punkt-zu-Mehrpunkt-Übertragung): 1. Fernsehdienste (einschließlich zeitversetzter Video-Abruf) nach Art. 1 lit. a der Richtlinie 89/552/EWG; 2. Hörfunkdienste; 3. Teletext (über Fernsehsignal).

Die EB[125] führen hierzu aus: *„Der jeweilige Nutzer muss also in der Lage sein, den Inhalt des Dienstes (die Information oder Kommunikationsdaten) gesondert in Anspruch zu nehmen. Nicht individuell abrufbar sind Dienste, die gleichzeitig für eine unbegrenzte Zahl von Empfängern bereitgestellt werden, etwa Fernseh-, Rundfunk- und Teletextdienste. Ein Hilfsmittel für die Beurteilung der Frage, ob ein individuell abrufbarer Dienst der Informationsgesellschaft vorliegt, kann darin bestehen, ob der Dienst interaktiv erbracht wird. In einem solchen Fall hängt die übermittelte Information überwiegend von den Eingaben des Empfängers ab.“ Brenn*[126] definiert den Begriff des „interaktiven Dienstes“, der dadurch charakterisiert wird, dass der Nutzer den an ihn übermittelten Inhalt maßgeblich durch seine Eingaben bestimmt: *„Entscheidend ist also, dass der übertragene (gesendete) und zugänglich gemachte Output maßgeblich vom Input des Nutzers abhängt.“,* wobei auch die zeitliche Komponente eine wesentliche Rolle spiele: *“Der Output muss in unmittelbarem zeitlichen Zusammenhang mit dem Input stehen, also durch den Input sofort ausgelöst werden.“* Bei aller Interaktivität sollte nicht vergessen werden, dass der „interaktive Dienst“ lediglich ein Hilfskriterium ist. Etwas deutlicher wird der Begriff bei *Blume/Hammerl*[127] erklärt: Die Verbindung für die Erbringung des Dienstes muss zumindest technisch gesehen eine Punkt-zu-Punkt-Verbindung (*point-to-point,* im Gegensatz zum *broadcasting* des Rundfunks, das durch „ein Sender - viele Empfänger“ charakterisiert wird) sein[128] und es muss eine bidirektionale Übertragung möglich sein. Weiters wird ausgeführt, dass der Dienst über diesen Kanal steuerbar sein muss, und die Entscheidung über die Inanspruchnahme, insbes die Datenübertragung, erst auf Nachfrage des Nutzers erfolgt. Dies gilt aber nicht uneingeschränkt. Bewirbt ein Unternehmen seine Produkte auf seiner Website, so liegt ebenfalls ein Dienst der Informationsgesellschaft vor. Der „individuelle Abruf“ erklärt sich hier aus der Möglichkeit, diese Seite anzusteuern. Das bloße Zusenden elektronischer Post ist allerdings auch ein Dienst der Informationsgesellschaft.[129] Hier und bei vergleichbaren individuellen Kommunikationsmitteln soll es auch irrelevant sein, ob die Informationsübermittlung auf Wunsch des Nutzers erfolgt.[130]

---

[125] Abgedruckt in: *Brenn,* ECG 185 f.

[126] ECG 193.

[127] ECG-Kommentar 43.

[128] Wobei allerdings darauf hingewiesen wird, dass es auch interaktive Punkt-zu-Mehrpunkt-Übertragungen (*broadcasting*) gibt: siehe aaO, FN 70.

[129] Vgl 18. ErwGr S 7 der EC-RL. Nicht aber die E-Mail „an sich“. Siehe hierzu schon oben, S 25

[130] So *Blume/Hammerl,* ECG-Kommentar 48 f. Man könnte allerdings ergänzen, dass der Nutzer E-Mails im Internet und mittels einem Client abruft, und daher auf eigenen Wunsch auf seinem PC empfängt.

c) Elektronisch

Ein Dienst wird elektronisch bereitgestellt, wenn er mittels Geräten für die elektronische Verarbeitung, einschließlich digitaler Kompression, und Speicherung von Daten am Ausgangspunkt gesendet, und am Endpunkt empfangen und vollständig über Draht, Funk, auf optischem oder anderem elektromagnetischen Weg gesendet, weitergeleitet und empfangen wird.

> Gem lit B der Anlage 1 zum NotifG werden folgende Dienste nicht „elektronisch" erbracht: 1. Dienste, die zwar mit elektronischen Geräten, aber in materieller Form erbracht werden: a) Geldausgabe- oder Fahrkartenautomaten; b) Zugang zu gebührenpflichtigen Straßennetzen, Parkplätzen usw., auch wenn elektronische Geräte bei der Ein- und Ausfahrt den Zugang kontrollieren und/oder die korrekte Gebührenentrichtung gewährleisten; 2. Offline-Dienste: Vertrieb von CD-ROM oder Software auf Disketten; 3. Dienste, die nicht über elektronische Verarbeitungs- und Speicherungssysteme erbracht werden: a) Sprachtelefondienste; b) Telefax-/Telexdienste; c) über Sprachtelefon oder Telefax erbrachte Dienste; d) medizinische Beratung per Telefon/Telefax; e) anwaltliche Beratung per Telefon/Telefax; f) Direktmarketing per Telefon/Telefax.

Von obigen Ausnahmen kann abgeleitet werden, dass auch für dieses Tatbestandselement eine *point-to-point* Übertragung charakteristisch ist. Die Abgrenzung fällt allerdings nicht immer leicht. So ist die Sprachtelephonie zwar explizit ausgenommen, dem steht aber nicht entgegen, dass andere Dienste, insbes Datendienste im Bereich der mobilen Sprachtelephonie, über die Infrastruktur der Sprachtelephonie elektronisch erbracht werden können. Die EB[131] zählen daher SMS-Dienste, WAP-Dienste, UMTS-Dienste und Mehrwertdienste, die über Dialer-Programme in Anspruch genommen werden, sehr wohl zu den Diensten der Informationsgesellschaft.[132] Als weiterer Dienst könnten noch die *Location Based Services*[133] angeführt werden. AA ist *Brenn*[134], mit der Begründung, rein nicht-interaktive Dienste seien keine Dienste der Informationsgesellschaft (siehe schon oben), und: Die Informationspflichten nach § 5 könnten kaum erfüllt werden. Zu letzterem Argument führen die EB[135] zu § 5 aus: *"Bei Diensten der Informationsgesellschaft, die über ein Mobiltelephon bereitgestellt werden, wird es aus Platzgründen genügen, wenn ein Hinweis auf eine über das Internet zugängliche Homepage gegeben wird;"*. An den Informationspflichten soll die Anwendbarkeit des ECG auf SMS- und andere Datendienste daher nicht scheitern.

---

[131] Abgedruckt in: *Brenn,* ECG 186.

[132] So auch *Zankl,* ECG-Handbuch Rz 182.

[133] Das ECG auf diese Dienste für anwendbar erklärend: S*pindler/Fallenböck,* Das Herkunftslandprinzip der E-Commerce-Richtlinie und seine Umsetzung in Deutschland und Österreich (Teil I), ZfRV 2002/23.

[134] ECG 194. Vgl auch *Brenn,* ECG 173.

[135] Abgedruckt in: *Brenn,* ECG 204.

d) Im Fernabsatz bereitgestellter Dienst

Sowohl das NotifG als auch § 5a KSchG[136] (mit geringfügigen Abweichungen) verstehen unter „im Fernabsatz", dass die beteiligten Parteien nicht gleichzeitig körperlich anwesend sind.

> Gem lit A der Anlage 1 des NotifG sind keine „im Fernabsatz" erbrachten Dienste, selbst wenn dabei elektronische Geräte benutzt werden: 1. Untersuchung oder Behandlung in der Praxis eines Arztes mit Hilfe elektronischer Geräte, aber in Anwesenheit des Patienten; 2. Konsultation eines elektronischen Katalogs in einem Geschäft in Anwesenheit des Kunden; 3. Buchung eines Flugtickets über ein Computernetz, wenn sie in einem Reisebüro in Anwesenheit des Kunden vorgenommen wird; 4. Bereitstellung elektronischer Spiele in einer Spielhalle in Anwesenheit des Benutzers.

2. Persönlicher Anwendungsbereich

Das ECG knüpft überwiegend am Begriff des Diensteanbieters an, um seinen persönlichen Anwendungsbereich zu bestimmen. Somit ist der Diensteanbieter Haupt-Normadressat des ECG.[137] Gem § 3 Z 2 ist der Diensteanbieter eine natürliche oder juristische Person oder sonstige rechtsfähige Einrichtung, die einen Dienst der Informationsgesellschaft bereitstellt. Dieser Begriff ist weiters nicht problematisch.

Arbeitsverträge fallen aus dem Anwendungsbereich heraus, der Arbeitgeber ist daher seinen Arbeitnehmern gegenüber kein ISP.[138]

a) Access-Provider iSd § 13

Der Access-Provider wird in § 13 definiert als Diensteanbieter, der von einem Nutzer eingegebene Informationen in einem Kommunikationsnetz übermittelt oder den Zugang zu einem Kommunikationsnetz vermittelt. Es handelt sich bei seiner Tätigkeit um eine reine Durchleitung fremder Information in einem Kommunikationsnetz.[139]

Exkurs: Network- und Backbone-Provider als Access-Provider?

Vor dem Hintergrund, dass Diensteanbieter – und somit auch Provider – einen Dienst iSd § 3 Z 1 anbieten müssen, um in den Anwendungsbereich des ECG zu fallen, mag es zweifelhaft sein, ob Network-Provider bzw *Carrier* unter § 13 zu subsumieren sind. *Blume/Hammerl*[140] treffen hier eine

---

[136] Eingefügt durch das FernabsatzG, BGBl I 185/1999.

[137] Vgl mwH *Blume/Hammerl*, ECG-Kommentar 33.

[138] Vgl die EB, abgedruckt in: *Brenn,* ECG 271. Er ist im Übrigen auch kein Anbieter öffentlicher Telekommunikationsdienstleistungen iSd TKG 1997: OGH 13. 6. 2002, 8 Ob A 288/01p = wbl 2002/353.

[139] *Brenn,* ECG 263.

[140] ECG-Kommentar 115. Abl *Zankl,* Der Entwurf zum E-Commerce-Gesetz, NZ 2001, 325. Vgl auch *Spindler* in: *Hoeren/Sieber*, Handbuch zum Multimediarecht 29 Rz 356.

[140] *Zankl,* ECG-Handbuch Rz 193.

Differenzierung: Betreiben die Provider leitungsvermittelte Dienste[141] so fallen sie heraus. Paketvermittelte Dienste sollen jedenfalls umfasst sein.

Was den Backbone-Provider betrifft, so werden sie von *Blume/Hammerl*[142] offensichtlich gleichfalls zu den Diensteanbietern iSd § 13 gezählt: Access-Provider ist jeder Provider, der in irgendeiner Form an der Übertragung der Information beteiligt ist, was logischerweise zu einer Kette von Diensteanbieter führt. Hierzu gehört auch der Backbone-Provider. Dem ist wohl zuzustimmen, und wenn im Folgenden vom Access-Provider die Rede ist, sind auch Network- und Backbone-Provider gemeint.

b) Cashing-Provider iSd § 15

Der Cashing-Provider übermittelt ebenfalls eine vom Nutzer eingegebene Information in einem Kommunikationsnetz, stellt aber Server zur Verfügung, auf denen die Information zu Effizienzgründen zeitlich begrenzt gespeichert wird. Darunter fallen also vorwiegend Proxy-Server-Betreiber. Wegen ihrer Nähe zum Access-Provider werden sie nicht gesondert behandelt.

c) Host-Provider iSd § 16

Die Tätigkeit des Host-Providers besteht im Speichern fremder Inhalte. Den EB[143] ist zu entnehmen, dass nicht nur das Bereitstellen von Speicherplatz, also der Infrastruktur (*hosting*) hierunter fällt, sondern auch das Ermöglichen der Eingabe von Informationen auf seinem Dienst der Informationsgesellschaft (siehe hierzu schon in der Einleitung, S 5).

3. Räumlicher Anwendungsbereich

Gem § 1 Abs 2 bestimmt sich der räumliche Anwendungsbereich innerhalb des EWR nach dem Herkunftslandprinzip. Außerhalb des EWR gelten die Regeln des internationalen Privatrechts.[144] MaW: Schließt eine Person mit (Wohn-)Sitz im Inland Geschäfte mit den USA ab, so ist das ECG nicht anwendbar. Hat der Vertragspartner seinen Sitz in Spanien, so kommt das ECG zur Anwendung.

Im koordinierten Bereich iSd § 3 Z 8, dem „*Anwendungsbereich des Herkunftslandsprinzips*“[145] (§ 20) - zu dem auch die Auskunftspflichten der Diensteanbieter gehören -, unterliegen diese dem Recht ihres Sitzstaates.[146]

---

[141] Dienste bis zur Vermittlungsschicht (OSI-Schicht 3). Näheres zum ISO/OSI Referenzmodell zB *Payer*, http://www.payer.de/cmc/cmcs03.htm .

[142] ECG-Kommentar 117.

[143] Abgedruckt in: *Brenn,* ECG 279 f.

[144] Siehe *Brenn,* ECG 175. Zum anwendbaren Recht nach Internationalem Privatrecht im Internet siehe: *Mottl,* Anwendbares Recht und Gerichtsstand im Internet, in: *Brenn,* ECG 134 ff.

[145] EB, abgedruckt in: *Brenn,* ECG 189.

[146] MwH: *Brenn,* ECG 200, 308; *Blume/Hammerl,* ECG-Kommentar 34.

4. Ausnahmen vom Anwendungsbereich

§ 2 bestimmt, dass Belange des Abgabenwesens, des Datenschutzes und des Kartellrechts unberührt bleiben. Dies bedeutet, dass das DSG, das KartG, die BAO usw auf den elektronischen Geschäftsverkehr volle Anwendbarkeit finden.[147] Diese Ausnahmen gehen zurück auf Art 1 Abs 5 bzw die Erwägungsgründe 12 bis 14, wo es ua heißt, dass insbes Angelegenheiten der Mehrwertsteuer von der Richtlinie nicht berührt werden dürfen, und sollen mit der EC-RL auch keine neuen steuerlichen Verpflichtungen festgelegt werden. Ziel und Zweck dieser Ausnahmebestimmungen ist es, diese Materien nicht dem Herkunftslandprinzip zu unterwerfen.

5. Zusammenfassung

Aus dem bereits Dargestellten lässt sich erkennen, wie problematisch die Definition des Dienstes der Informationsgesellschaft ist. Insbes gegen die Anerkennung von SMS-, UMTS- und WAP-Diensten als Dienste der Informationsgesellschaft werden Bedenken gehegt. Im Übrigen ist – zumindest dem Juristen - nicht immer ganz klar, womit ein Provider überhaupt sein Geld verdient, sprich, welche Tätigkeit er ausübt und ob diese Tätigkeit einen Dienst der Informationsgesellschaft darstellt.[148]

B. Auskunftspflichten

Art 15 Abs 1 EC-RL verbietet es den Mitgliedsstaaten Überwachungspflichten für die von Access-, Host- und Cashing-Providern übermittelten oder gespeicherten Informationen, zu normieren (Ausschluss der Überwachungspflicht). Dies steht aber gem Abs 2 leg cit behördlichen oder gerichtlichen Auskunftsersuchen betreffend der Identität von Nutzern nicht entgegen.

Die Umsetzung dieser Bestimmungen erfolgte in § 18, der in seinem Abs 1 die in den §§ 13 bis 17[149] genannten Diensteanbieter von der Verpflichtung befreit, den Datenverkehr nach rechtswidrigen Informationen zu überwachen oder von sich aus danach zu forschen. In § 18 Abs 2 bis 4 werden Auskunftspflichten für bestimmte Diensteanbieter normiert, wobei Abs 4 (Auskunftspflichten gegenüber Privaten) ein Austriacum ist: Eine derartige Auskunftspflicht ist in der EC-RL nicht enthalten.

Ergänzend zu diesen Bestimmungen wurden von der ISPA[150] - dem Branchenverband der österreichischen Provider - die Verhaltensrichtlinien[151] und ein Verhaltenskodex[152] erarbeitet. Mitglieder der ISPA sind laut § 4 Abs 2

[147] Vgl die EB, abgedruckt in: *Brenn*, ECG 179.

[148] Siehe hierzu auch bei der Beurteilung der Ausgangsfälle.

[149] Das sind Host-, Access-, und Cashing-Provider, Linksetzer und Suchmaschinenbetreiber.

[150] Internet Service Provider Austria, www.ispa.at.

[151] http://www.ispa.at/www/getFile.php?id=22 .

[152] http://www.ispa.at/www/getFile.php?id=100 .

ihrer Statuten[153] Internet Service Provider. Was die ISPA unter diesem Begriff versteht, geht aus ihrem Anmeldeformular[154] hervor: Content-Provider (die primär Inhalte anbieten), Access-Provider (die Zugänge für Endkunden anbieten), Backbone-Provider (die internationale Bandbreiten anbieten), Hosting-Provider (die Hosting Services anbieten). Der Verhaltenskodex stellt einen Akt der freiwilligen Selbstkontrolle iSd 49. ErwGr und Art 16 der EC-RL dar.[155] Er regelt den Umgang mit Kundendaten, die Auskunftspflichten und Haftungsausschlüsse. ZT gibt er lediglich den Gesetzestext wider.

Vorausgeschickt sei, dass gem § 18 Abs 5 Auskunfts- und Mitwirkungspflichten von Diensteanbietern gegenüber Behörden nach anderen gesetzlichen Bestimmungen, wie etwa nach § 89 TKG 1997 bzw § 94 TKG 2003, unberührt bleiben.

1. Auskunftspflichten gegenüber Gerichten (§ 18 Abs 2)[156]

> *„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."*

a) Auskunftsverpflichtet

Zur Erteilung einer Auskunft sind Host- und Access-Provider verpflichtet.

b) Auskunftsberechtigt

Das Auskunftsbegehren muss von einem gesetzlich befugten inländischem Gericht stammen, und zwar von einem Strafgericht. Dies ergibt sich ohne weiteres daraus, dass Zivilgerichte keine strafbaren Handlungen verfolgen dürfen.

Zu betonen ist, dass die Strafgerichte, im Gegensatz zu den Verwaltungsbehörden, eine eigene Ermächtigungsnorm zur Erhebung von Stammdaten benötigen (*„gesetzlich befugtes"*). In diesem Zusammenhang werden daher als Rechtsgrundlagen primär folgende Bestimmungen der StPO in Betracht kommen: die angeordnete Überwachung des Fernmeldeverkehrs gem §§ 149a ff, die Herausgabe von Beweisunterlagen nach § 143 Abs 2, und die Hausdurchsuchung nach § 139 ff (hierzu im einzelnen im Kapitel Strafprozessrecht und Telekommunikationsrecht, S 51 ff).[157]

---

[153] http://www.ispa.at/downloads/d70e979f989f_ispa_statuten.pdf .

[154] http://www.ispa.at/www/getFile.php?id=99 .

[155] Verhaltenskodices von Verbänden anderer Staaten sind abrufbar unter: http://normative.zusammenhaenge.at/selbstregulierung.html .

[156] Vgl auch Punkt 2.2. des ISPA-Verhaltenskodex.

[157] *Brenn,* aaO.

c) Voraussetzungen

Formelle und materielle Voraussetzung des Auskunftsverlangens ist die Anordnung eines Gerichtes zur Verhütung, Ermittlung, Aufklärung oder Verfolgung gerichtlich strafbarer Handlungen.

Hieraus lässt sich ableiten, dass das Auskunftsbegehren beschlussmäßig zu erfolgen hat (und nicht etwa in Form einer Note).[158] Bemerkenswert ist, dass § 18 Abs 2 auch die Verhütung strafbarer Handlungen als Auskunftszweck beinhaltet[159]: Die Gefahrenabwehr ist vielmehr Aufgabe der Sicherheitsbehörden[160], während die Strafverfolgung in die Zuständigkeit der Strafgerichte fällt[161].[162] Diese Bestimmung ist daher entsprechend teleologisch zu reduzieren.

Aufgrund der weiten Formulierung des Gesetzestextes, wird es ausreichend sein, wenn das Strafgericht die Übermittlung von Stammdaten eines nur dem Pseudonym nach bekannten Täters verlangt, solange dieser Kunde beim Provider ist.[163] Gleiches muss gelten, wenn das Gericht nur über eine E-Mail Adresse verfügt.

d) Inhalt

Der Provider muss alle Informationen übermitteln, mit denen die Nutzer seines Dienstes zwecks Verhütung, Ermittlung, Aufklärung oder Verfolgung gerichtlich strafbarer Handlungen ermittelt werden können. Dies wird vor allem Stammdaten betreffen, uU auch Vermittlungsdaten, also zB Name, Adresse, IP-Adresse des Computers des Kunden.[164] E-Mail Adressen sind wohl zu beauskunften, wenn sie für die Feststellung der Identität notwendig sind.

Hat der (Host-)Provider die Stammdaten bei der Registrierung nicht verlangt, kann ihm dies aber nicht zu Nachteil gereichen. Keinesfalls verpflichtet diese Bestimmung den Provider zum „Horten“ oder Erheben bestimmter Daten. Er muss nur solche Daten herausgeben, über die er verfügt.

2. Auskunftspflichten gegenüber Verwaltungsbehörden (§ 18 Abs 3)[165]

> *„Die in § 16 genannten Diensteanbieter haben auf Grund der Anordnung einer Verwaltungsbehörde dieser den Namen und die Adressen der Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Speicherung von Informationen abgeschlossen haben, zu übermitteln, sofern die Kenntnis dieser Informationen*

---

158 So auch die EB, abgedruckt in: *Brenn,* ECG 296.

159 Diese Formulierung ist anscheinend dem Art 3 der EC-RL entnommen. Allerdings befinden sich dort die Ausnahmen vom Herkunftslandprinzip.

160 MwH: *Demmelbauer/Hauer,* Sicherheitsrecht (2002) Rz 1.

161 MwH: *Demmelbauer/Hauer,* Sicherheitsrecht Rz 110, 211.

162 So *Zankl,* ECG-Handbuch Rz 279.

163 Ein in praxi wohl relevanter Fall: so treten User in Foren regelmäßig mit Phantasienamen auf (sog *Nick-Names*).

164 *Brenn,* ECG 300.

165 Vgl auch Punkt 2.3. des ISPA-Verhaltenskodex.

eine wesentliche Voraussetzung der Wahrnehmung der der Behörde übertragenen Aufgaben bildet.“

a) Auskunftsverpflichtet

Abweichend von Abs 2, sind nach Abs 3 ausschließlich Host-Provider zur Auskunft verpflichtet.

b) Auskunftsberechtigt

Auskunftsberechtigt sind Verwaltungsbehörden. Die EB[166] erwähnen ausdrücklich die Gewerbe- und Finanzmarktaufsichtsbehörden.[167]

c) Voraussetzungen

Auch hier verwendet das Gesetz wieder den Begriff „Anordnung“. Es wäre wünschenswert, wenn der Gesetzgeber eine bestimmte Art des Verwaltungshandelns definiert hätte. Laut *Blume/Hammerl*[168] muss es sich, ohne nähere Begründung, um einen Bescheid handeln.

Die geforderten Informationen müssen eine wesentliche Voraussetzung für die Wahrnehmung der dieser Behörde übertragenen Aufgaben[169] bilden. Sie muss ihr Begehren entsprechend begründen. Allerdings bedarf die Behörde keines Materiengesetzes, das ihr – vergleichbar zu den Gerichten – erst eine Ermächtigung verleiht.[170] Selbstverständlich unterliegt auch § 18 Abs 3 den verfassungsrechtlichen Schranken.[171] Grundsätzlich ist die Auskunft nur auf Stammdaten gerichtet, allerdings kann es natürlich auch sein, dass zur Ermittlung der Stammdaten die Erhebung von Vermittlungsdaten notwendig ist.[172] Es stellt sich die Frage, inwieweit § 18 Abs 3 eine taugliche Rechtsgrundlage für einen Eingriff in Vermittlungsdaten bietet, und damit auch das Erheben von Stammdaten anhand dynamischer IP-Adressen ermöglicht. In Anwendung der bereits zitierten Jud des EGMR zur Ausgestaltung einer gesetzlichen Grundlage, die einen Eingriff in Art 8 MRK ermöglicht[173], ist davon auszugehen, dass § 18 Abs 3 die Erhebung von Vermittlungs- bzw Verkehrsdaten nicht rechtfertigt. Neben der Identifikation

---

166 Abgedruckt in: *Brenn,* ECG 298.

167 Vgl allerdings *Zank* (ECG-Handbuch Rz 282), der gestützt auf § 2, davon ausgeht, Finanzbehörden hätten kein Auskunftsrecht.

168 ECG-Kommentar 168.

169 Vgl Näheres zum Begriff der „wesentlichen Voraussetzung“ im Kapitel Sicherheitspolizeigesetz (S 71).

170 Im ursprünglichen Entwurf war noch vorgesehen, dass auch die Verwaltungsbehörde einer Ermächtigung durch ein Materiengesetz bedarf. Dies wurde durch den Abänderungsantrag des JA (abgedruckt in: *Brenn,* ECG 298) geändert.

171 Etwas überschießend meint *Brenn,* (ECG 302), dass bei einem Eingriff des Auskunftsbegehren in das Fernmeldegeheimnis, ausschließlich die Bestimmungen der StPO und des TKG zu Anwendung gelangen würden.

172 Was auch ohne richterlichen Befehl zulässig ist. Siehe zu diesem Problem schon in der Einleitung, S 14.

173 Siehe hierzu schon in der Einleitung, S 14.

einer Person anhand einer IP-Adresse kann diese wohl auch durch eine E-Mail Adresse erfolgen.

Punkt 2.3. des ISPA-Verhaltenskodex fordert des weiteren eine genaue Beschreibung der Tathandlung durch die Behörde sowie die deutliche und *„ernsthafte*“ Bezeichnung der Stelle, an der die rechtsverletzende Information gespeichert ist (zB URL). Die Behörde muss diese Voraussetzungen glaubhaft nachweisen.

d) Inhalt

Der Provider hat nur Namen und Adressen (die geographische Anschrift, nicht die E-Mail Adresse[174]) jener Nutzer des Dienstes, mit denen Vereinbarungen über die Speicherung von Informationen abgeschlossen wurden, bekannt zu geben. Nach dem Gesetzestext müssen also nur die verfügbaren (siehe bereits oben, S 33) Stammdaten von Vertragspartnern mitgeteilt werden.

3. Auskunftspflichten gegenüber Privaten (§ 18 Abs 4)[175]

> *„Die in § 16 genannten Diensteanbieter haben den Namen und die Adresse eines Nutzers ihres Dienstes, mit dem sie Vereinbarungen über die Speicherung von Informationen abgeschlossen haben, auf Verlangen dritten Personen zu übermitteln, sofern diese ein überwiegendes rechtliches Interesse an der Feststellung der Identität eines Nutzers und eines bestimmten rechtswidrigen Sachverhalts sowie überdies glaubhaft machen, dass die Kenntnis dieser Informationen eine wesentliche Voraussetzung für die Rechtsverfolgung bildet.“*

a) Auskunftsverpflichtet

Auch gegenüber Privaten besteht nur für Host Provider eine Auskunftspflicht.

b) Auskunftsberechtigt

Auskunftsberechtigt sind Dritte, wie Verwertungsgesellschaften (bei Urheberrechtsverletzungen) oder sonstige Private (zB bei Verletzungen von Persönlichkeitsrechten).

c) Voraussetzungen

Materielle Voraussetzung ist ein überwiegendes rechtliches Interesse an der Feststellung der Identität eines Nutzers und eines bestimmten rechtswidrigen Sachverhalts (zB Verletzung eines Marken- oder Urheberrechts der betreffenden Person). Der Dritte muss glaubhaft machen, dass die Kenntnis

[174] Siehe zur näheren Begründung *Zankl,* ECG-Handbuch Rz 280.
[175] Vgl auch Punkt 2.4. des ISPA-Verhaltenskodex.

der geforderten Informationen eine wesentliche Voraussetzung für seine Rechtsverfolgung bildet.[176]

Punkt 2.5. des ISPA Verhaltenskodex führt hierzu ergänzend aus, dass das Interesse an einer konkreten Rechtsverfolgung in einer Weise zu bescheinigen ist, dass auch ein Laie nachvollziehen kann, dass die Interessen der Rechtsverfolgung des Dritten den Interessen des Kunden an der Geheimhaltung seiner Daten deutlich überwiegen. Zusätzlich muss der Dritte glaubhaft und nachvollziehbar darlegen, wieso die Kenntnis der Daten eine wesentliche Voraussetzung für die Rechtsverfolgung bildet. Für die Identifikation anhand einer E-Mail Adresse gilt das bereits Gesagte.

d) Inhalt

Der Host-Provider hat nur Namen und Adressen jener Nutzer des Dienstes, mit denen Vereinbarungen über die Speicherung von Informationen abgeschlossen wurden, bekannt zu geben, also wieder nur von Kunden (E-Mail Adressen sind hiervon wiederum nicht erfasst).

Zankl[177] kommt mit einer wenig einleuchtenden Argumentation zu einer allzu restriktiven Auslegung: Der Diensteanbieter müsse ohnehin den Informationspflichten nach § 5 nachkommen, und daher sei diese Auskunftspflicht jedenfalls subsidiär und könne nur auf die Verfolgung solcher Rechte bezogen werden, mit denen der Provider zumindest in technischer Verbindung steht. So könne keine Auskunft verlangt werden, wenn es um die Durchsetzung vertraglicher Rechte gehe, die keinerlei elektronische Bezüge haben. Darüber hinaus müsse der Nutzer, dessen Identität preisgegeben werden soll, selbst im Verdacht stehen, den rechtswidrigen Sachverhalt verwirklicht zu haben. Dem ist zu entgegnen, dass sich die Informationspflichten nach § 5 nur auf kommerzielle Anbieter beziehen, den Auskunftspflichten unterliegen aber auch die unentgeltlichen Diensteanbieter. Die von *Zankl* vorgebrachte Redundanz liegt daher nicht notwendigerweise vor. Eine „technische" Verbindung des Providers mit der Rechtsverletzung wird vom Gesetz nicht verlangt. Sehr wohl aber – dem ist zuzustimmen – muss der Auskunftswerber einen eigenen Anspruch verfolgen, und der Nutzer selbst Täter sein (nicht notwendigerweise aber unmittelbarer Täter).[178]

e) Bemerkungen

Diese Bestimmung ist sehr problematisch, denn sie bürdet dem Unternehmer die Vornahme einer Interessensabwägung auf, mit der traditionellerweise auch Juristen ihre Schwierigkeiten haben. Hinzu kommt die kumulative Anwendbarkeit des Datenschutzrechts: Der ursprüngliche

---

[176] Bei der Interpretation, was eine wesentliche Voraussetzung für eine Rechtsverfolgung bildet, können mE die Grundsätze zur wesentlichen Voraussetzung nach SPG herangezogen werden. Siehe hierzu im Kapitel Sicherheitspolizeigesetz, S 71.

[177] ECG-Handbuch Rz 283 f.

[178] So auch die EB, abgedruckt in: *Brenn,* ECG 297 f.

Entwurf[179] enthielt in § 18 Abs 4 noch einen expliziten Verweis auf § 8 Abs 1 Z 4 DSG[180]. Dieser wurde zwar fallengelassen, die Regelungen des Datenschutzrechts kommen aber durch § 2 zur Anwendung.

Bedenkt man, dass der Großteil der ISP über keine eigene Rechtsabteilung verfügt, wird der Unternehmer die Interessensabwägung wohl selbst vornehmen.[181] Er ist dabei als Laie gezwungen, eine Prognose über das Bestehen oder Nichtbestehen eines Anspruches abzugeben. Die EB[182] räumen immerhin ein, dass diese Bestimmung *„in der Praxis Schwierigkeiten bereiten kann",* jedoch bei der Beurteilung ohnehin auf die Fähigkeiten und das Wissen eines juristischen Laien abzustellen sei (vgl auch § 16). Es müsse daher auch für einen Nicht-Fachmann offenkundig sein, dass eine Rechtsverletzung vorliege.[183]

4. Abstellungsaufträge / Sperrverfügungen

§ 19 Abs 1 normiert, dass die §§ 13 bis 18 gesetzliche Vorschriften unberührt lassen, nach denen ein Gericht oder eine Behörde dem Diensteanbieteter die Unterlassung, Beseitigung oder Verhinderung einer Rechtsverletzung auftragen kann, unberührt bleiben.[184] Dies bedeutet allerdings nicht, dass aus § 19 eine Befugnis zur Anordnung einer Unterlassung, Beseitigung oder Verhinderung des rechtswidrigen Verhaltens abgeleitet werden könnte. Es bedarf daher einer eigenen gesetzlichen Ermächtigung.[185]

Im Bereich des Zivilrechts kommt die gesamte Palette der zivilrechtlichen Unterlassungs- und Beseitigungsansprüche in Betracht, also Ansprüche nach UrhG, UWG, § 1330 ABGB usw.[186] [187]

Strafrechtliche Abstellungsaufträge können in Österreich nicht erlassen werden, denn es existiert keine Rechtsgrundlage die es einem Strafgericht

---

[179] Abgedruckt in: *Brenn,* ECG 304.

[180] Jetzt verweisen nur mehr die EB darauf. Abgedruckt in: *Brenn,* ECG 298.

[181] Natürlich funktionieren auch ISP wie jedes andere Unternehmen, und werden sie wohl für die Lösung von Rechtsproblemen bei Fehlen einer eigenen Rechtsabteilung, externe Rechtsberater heranziehen. Das *outsourcing* von juristischem Know-How hat jedoch den Nachteil, dass bei der Beratung unmittelbar Kosten anfallen. Unter der Annahme, dass Unternehmen nach betriebswirtschaftlichen Kriterien arbeiten, wird wohl nicht immer professioneller juristischer Rat eingeholt werden. Wird er doch eingeholt, so werden die Unternehmer idR enttäuscht werden, denn bei Rechtsgebieten wie dem Datenschutz, welche primär von einer Interessensabwägung beherrscht werden, werden sie selten eindeutige Aussagen erhalten.

[182] Abgedruckt in: *Brenn,* ECG 298.

[183] „Parallelwertung in der Laiensphäre". Siehe hierzu auch: *Tonninger,* Rechtsverletzung im Internet - Providerhaftung?, ecolex 1999, 251. Entsprechend der Schuldtheorie ist ein Rechtsirrtum vorwerfbar, wenn man sich nicht anlassbezogen erkundigt (vgl *Reindl,* E-Commerce und Strafrecht (2003) 274).

[184] Vgl Art 14 Abs 3 EC-RL.

[185] Vgl die EB, abgedruckt in: *Brenn,* ECG 305.

[186] Vgl die EB, aaO. Vgl auch ausdrücklich in Art 8 Abs 3 und Art 5 Abs 1 lit a der InfoSoc-RL. Details hierzu siehe im Kapitel Urheberrechtsgesetz, S 44.

[187] MwH *Schanda,* Verantwortung und Haftung im Internet nach dem neuen E-Commerce-Gesetz, ecolex 2001, 920.

ermöglichen würde, ein strafrechtswidriges Verhalten zu untersagen.[188] Allenfalls kann die Fortsetzung des Verhaltens über die Regeln der Beschlagnahme verhindert werden (siehe dazu im Kapitel Strafprozessordnung und Telekommunikationsgesetz, insbes die Bestimmungen des MedienG und des UrhG, S 51 f).

Gleichfalls unmöglich ist in Österreich - anders als in Deutschland – die Sperrung von Websiten auf Grundlage des Verwaltungsrechts.[189]

Es existieren allerdings einige Vorschriften, die den Provider zur Sperrung verpflichten (siehe dazu auch unten). Nach § 4 der ISPA-Verhaltensrichtlinien[190] verpflichten sich die ISPA-Mitglieder nach Kenntnisnahme illegaler Inhalte, die sich in ihrem Einflussbereich befinden, mittels ihnen zur Verfügung stehender, zumutbarer Handlungen unverzüglich den Zugang zu diesen Inhalten zu sperren bzw nachweislich die unverzügliche Sperrung des Zugangs zu diesen Inhalten, falls sich der betroffene Server im Einflussbereich ihrer Kunden befindet, zu veranlassen. Des weiteren wird bestimmt, dass - soweit wirtschaftlich und technisch zumutbar - entsprechendes Beweismaterial für die Dauer eines Kalendermonats zu sichern ist und auf keinen Fall solches Beweismaterial bewusst zu löschen.[191]

§ 75 Abs 2 TKG 1997 verpflichtet Host-Provider[192] und andere Betreiber von Telekommunikationsdiensten zur Verhinderung der missbräuchlichen Verwendung[193] von Endgeräten[194], dies gewährt aber keiner Behörde die Befugnis, eine solche Anordnung zu erlassen. Die Bestimmung ist gem § 104 Z 4 ff mit Verwaltungsstrafe bis zu Euro 3.633 bedroht. § 65 TKG 1997 gewährt dem Betreiber von Telekommunikationsdiensten lediglich das Recht, störende oder nicht zugelassene Endgeräte vom Netz zu trennen. Diese

---

[188] Vgl *Ebensperger,* Die Verbreitung von NS-Gedankengut im Internet und ihre strafrechtlichen Auswirkungen unter besonderer Berücksichtigung des E-Commerce-Gesetzes, ÖJZ 2002, 132.

[189] So ordnete die Bezirksregierung Düsseldorf die Sperrung mehrerer Nazi-Seiten gem § 22 Abs 2 Mediendienstestaatsvertrag an. Siehe hierzu: Bundesweites Vorgehen gegen rechtsextreme Webseiten angemahnt, Heise Online, http://www.heise.de/newsticker/data/jk-21.03.03-007/; Unter http://normative.zusammenhaenge.at/faelle_de.html findet sich eine Linksammlung zu den einzelnen Beschlüssen dieses Verfahrens. Zur Schwierigkeit der technischen Umsetzung der Anordnungen, siehe: Chaotische Umsetzung der Sperrungsverfügung in NRW, Heise Online, http://www.heise.de/newsticker/data/tol-15.06.03-004/ .

[190] http://www.ispa.at/www/getFile.php?id=22 .

[191] Vgl hierzu auch: *Ebensperger* Die Verbreitung von NS-Gedankengut im Internet und ihre strafrechtlichen Auswirkungen unter besonderer Berücksichtigung des E-Commerce-Gesetzes, ÖJZ 2002, 132.

[192] Zu den Voraussetzungen, wann Host-Provider Telekommunikationsdienste anbieten, siehe in der Einleitung, S 15.

[193] Hierunter wird bspw die Nachrichtenübermittlung entgegen der öffentlichen Ordnung und Sicherheit bzw gesetzlicher Vorschriften, die Belästigung und Verängstigung anderer Nutzer udgl verstanden. Access-Provider sind explizit von dieser Verpflichtung ausgenommen (siehe *Parschalk/Zuser/Otto,* TKR 41).

[194] Zur Subsumption eines PCs unter den Begriff Endgerät siehe im Kapitel Strafprozessordnung und Telekommunikationsgesetz, S 56.

Bestimmung betrifft aber ausschließlich technische Angelegenheiten.[195] Das TKG 2003 hat an dieser Rechtslage nichts geändert (§ 75 und § 65 TKG 1997 entsprechen § 78 bzw § 72 TKG 2003).

5. Durchsetzung, Sanktionen und Rechtsfolgen

a) Durchsetzung der Auskunftspflichten mittels Zwang

Behördliche Zwangsmaßnahmen gegen Provider sind im ECG nicht vorgesehen, ebenso wenig wie der Verstoß gegen die Auskunftspflicht nach Abs 4 verwaltungsstrafrechtlich sanktioniert ist. Eine diesbezügliche Rechtsgrundlage muss daher anderen Gesetzen entnommen werden, zB dem AVG, dem VStG oder der StPO.[196]

Fraglich ist eine Durchsetzung im Zivilrechtsweg: Im Anwendungsbereich des Urheberrechts kommt diese zweifellos in Betracht, dort ist das Auskunftsrecht explizit als Anspruch formuliert.[197] Laut *Zankl*[198] sei *„nach allgemeinen Regeln“* eine Einklagbarkeit der Auskunftspflichten (bzw der entsprechenden Rechte) des ECG anzunehmen, bei schuldhafter Verletzung gebühre Schadenersatz. Dem ist wohl zu folgen.[199]

b) Schadenersatz wegen Auskunftsverweigerung

Wie lässt sich ein Schadenersatz begründen, wenn dem abgewiesenen Auskunftswerber durch die Auskunftsverweigerung ein Schaden entsteht (zB wegen Verjährung oder Unmöglichkeit der Rechtsverfolgung). IaR wird der Auskunftswerber kein Vertragspartner des ISP sein, weshalb nur eine Haftung ex delicto in Betracht kommt.[200]

1. Rechtswidrigkeit:
    a. Diese kann sich im Bereich der deliktischen Haftung aus der Verletzung von Schutzgesetzen iSd § 1311 Abs 2 ABGB[201]

---

[195] Vgl auch *Parschalk/Zuser/Otto*, TKR 42. Sie gehen auch davon aus, dass § 65 von § 11 FTEG (BG über Funkanlagen und Telekommunikationsendeinrichtungen BGBl I 134/2001) verdrängt worden sei.

[196] *Brenn,* ECG 302.

[197] Siehe dazu unten im Kapitel Urheberrechtsgesetz, 46 ff.

[198] ECG-Handbuch Rz 290.

[199] Vgl auch *Bienert-Nießl,* Materiellrechtliche Auskunftspflichten im Zivilprozeß, 219 f, die bei Auskunftspflichten von einer Einklagbarkeit mittels Leistungsklage ausgeht, und zwar unabhängig vom Hauptanspruch. Von den Auskunftspflichten sind allerdings die Aufklärungsobliegenheiten zu unterscheiden (zB im VersVG uä).

[200] Zu den Rechtsfolgen bei Auskunftsverweigerung einer Partei im Zivilprozess siehe *Bienert-Nießl,* Materiellrechtliche Auskunftspflichten im Zivilprozeß 367 ff.

[201] *„§ 1311. Der bloße Zufall trifft denjenigen, in dessen Vermögen der Person er sich ereignet. Hat aber jemand den Zufall durch ein Verschulden veranlaßt; hat er ein Gesetz, das den zufälligen Beschädigungen vorzubeugen sucht, übertreten; oder, sich ohne Noth in fremde Geschäfte gemengt; so haftet er für allen Nachtheil, welcher außer dem nicht erfolgt wäre.“*

ergeben[202]. Das sind Bestimmungen, die zufälligen Schädigungen vorbeugen zu suchen.[203] Ob eine Norm als derartiges Schutzgesetz anzusehen ist, muss aus dem Gesetzeszweck unter dem Gesichtspunkt bestimmt werden, ob die betreffende Norm ein abstrakt gefährliches Verhalten verbieten will, um so Einzelpersonen oder bestimmte Kreise von Personen vor Verletzungen ihrer Güter zu bewahren.[204] Sinn und Zweck der Auskunftspflichten nach ECG ist die Ermöglichung der Rechtsverfolgung, geschützt ist jeweils eine Einzelperson. So billigt etwa die Jud den öffentlich-rechtlichen Bestimmungen über die Aussagepflicht von Zeugen, Schutzgesetzcharakter zu: Gibt ein Zeuge den Namen des Täters unberechtigterweise nicht preis, kann dieser auf Ersatz der Ausforschungskosten geklagt werden.[205] Daher erscheint es durchaus vertretbar, die Auskunftspflichten nach ECG als Schutzgesetze zu qualifizieren.

b. Des weiteren ist die Verletzung absolut geschützter Rechte und Rechtsgüter[206] grundsätzlich rechtswidrig. Die Möglichkeit zur Rechtsverfolgung ist kein absolut geschütztes Gut.

2. Kausalität[207] und Adäquanz[208]: Werden iaR unproblematisch sein.
3. Verschulden: Bei einer Schutzgesetzverletzung ist es ausreichend, dass sich das Verschulden auf die Normübertretung bezieht.[209] Diese ist im konkreten Einzelfall zu prüfen. Der ISP wird häufig die Auskunft mit der Begründung verweigern, die Rechtsverletzung sei nicht offenkundig. Im österreichischen Zivilrecht handelt fahrlässig, und nicht vorsätzlich, jener Täter, dem mangels gehöriger Willensanspannung die Rechtswidrigkeit seines Verhaltens nicht bewusst war. Ist ihm sein Rechtsirrtum nicht vorwerfbar, so liegt kein Verschulden vor.[210] Geht der ISP daher im guten Glauben davon aus, dass der Anspruch des Privaten auf Auskunft gar nicht besteht, handelt er schuldlos, und ist somit haftungsfrei.
4. Schaden: Denkbar sind etwa Detektivkosten zur Ausforschung des Täters, oder auch die Unmöglichkeit der Rechtsverfolgung, die Verjährung des Anspruchs udgl.

---

[202] Hierzu ausführlich: *Koziol,* Haftpflichtrecht I^3 148.

[203] Vgl *Koziol,* Haftpflichtrecht II^2 (1984) 102.

[204] *Koziol*, aaO.

[205] OGH 13.10.1981, 5 Ob 680/81 = JBl 1983, 208 (*Wilhelm)*: Es ist unerheblich ist, dass Zeugenpflichten mittels Beugestrafen erzwungen werden können (vgl insbes § 333 Abs 3 ZPO) oder ob die Verweigerung der Zeugenaussage ein strafbares Verhalten darstellt. Siehe auch EFSlg 54.230; *Koziol,* Haftpflichtrecht I^3 254.

[206] *Koziol,* Haftpflichtrecht I^3 149 ff; II^2 2 ff.

[207] Wird die Auskunft verweigert, so liegt kein Tun, sondern ein rechtswidriges Unterlassen vor (zur Problematik der Kausalitätsprüfung bei Unterlassungshandlungen siehe *Koziol,* Haftpflichtrecht I^3 96).

[208] Ädäquanz bedeutet, dass der eingetretene Schaden nicht atypisch für die Rechtsverletzung sein darf (vgl hierzu ausführlich: *Koziol,* Haftpflichtrecht I^3 240.)

[209] *Koziol,* Haftpflichtrecht II^2 110.

[210] Vgl *Koziol,* Haftpflichtrecht I^3 203.

Der ISP kann diese deliktische Haftung nicht beschränken, denn grundsätzlich ist davon auszugehen, dass die Einschränkung der Haftung durch einseitige Erklärung keine Wirkung hat.[211]

c) Schadenersatz wegen rechtswidriger Datenweitergabe an einen Privaten

aa) Schadenersatz ex delicto

Hat der ISP mit dem Betroffenen kein Vertragsverhältnis (was in diesem Zusammenhang allerdings kaum denkbar ist), und gibt er die Daten entgegen der Bestimmungen des DSG weiter, so kommt ein deliktischer Schadenersatzanspruch in Betracht. Gem § 33 Abs 1 DSG kommen bei schuldhaften Verstößen gegen das DSG die Schadenersatzregeln des ABGB zur Anwendung[212], wobei aber Abs 4 leg cit eine Beweislastumkehr zu Gunsten des Betroffenen bestimmt. *Drobesch/Grosinger*[213] führen unter Hinweis auf die EB aus, dass das DSG als solches ein Schutzgesetz iSd § 1311 ABGB sei, da es abstrakte Gefährdungsverbote normiert, die auf den Schutz der Mitglieder eines bestimmten Personenkreises (von einer Datenverarbeitung Betroffene) vor Verletzung eines Rechtsgutes (das Datengeheimnis) abzielen. Wie bereits ausgeführt, bedarf es keiner Vorhersehbarkeit des Schadens bei einer Verbotsübertretung. In praxi mag allerdings häufig der Fall eintreten, dass gar kein materieller Schaden eingetreten ist.[214] Denkbar wäre, dass der ISP durch die Datenweitergabe eine Prozessführung gegen den Betroffenen ermöglicht.

bb) Schadenersatz ex contractu

Der ISP hat iaR eine Vertragsbeziehung mit dem Nutzer, dessen Daten er weitergegeben hat.

Daraus ergeben sich zwei Konsequenzen

1. Bei einer datenschutzwidrigen Weitergabe von Kundendaten haftet er ex contractu.
2. Er kann sich vertraglich gegen allfällige Haftungen absichern.

Ad 1.

Man denke an den Fall, dass der ISP durch die rechtswidrige Datenweitergabe eine Prozessführung gegen seinen Kunden ermöglicht. Kann

---

[211] Vgl *Koziol,* Haftpflichtrecht I[3] 558, der allerdings auch einige Ausnahmen zulässt, zB bei der Verkehrseröffnung aus reiner Freigiebigkeit oder der Auskunftsgewährung ohne gesetzliche Verpflichtung.

[212] § 33 DSG regelt auch immateriellen Schadenersatz, der hier aber nicht weiters relevant ist.

[213] Datenschutzgesetz 245.

[214] Da das DSG auch immateriellen Schadenersatz explizit erwähnt, wird man kaum behaupten können, es wolle als Ganzes auch das bloße Vermögen schützen (vgl *Koziol*, Haftpflichtrecht I[3] 248).

dieser ihn dann auf den dadurch entstandenen Schaden klagen? Es stellt sich hier das umgekehrte Problem zur Nichterfüllung von Auskunftspflichten.

1. Rechtswidrigkeit: Ergibt sich aus der Verletzung nebenvertraglicher Schutzpflichten[215] [216]
2. Kausalität und Adäquanz: Wird im Einzelfall zu prüfen sein.
3. Verschulden: Siehe oben, S 39.
4. Schaden: Im vertraglichen Schadenersatzrecht werden jedenfalls auch reine Vermögensschäden ersetzt.

Ad 2.

Der ISP hat selbstverständlich die Möglichkeit, sich in den Grenzen der des § 879 ABGB und des § 6 Abs 1 Z 9 KSchG gegen das Risiko einer Fehleinschätzung bei der Interessensabwägung abzusichern.[217]

d) Sonstige Rechtsfolgen

Host-Provider (in eingeschränkten Maße auch Cashing-Provider) verlieren ihr Haftungsprivileg ab Wissentlichkeit von den rechtswidrigen Inhalten, es sei denn, sie sperren den Zugang zu den Inhalten unverzüglich bzw entfernen diese (§§ 15 und 16). Erhalten sie ein behördliches oder gerichtliches Auskunftsverlangen, wird wohl idR Wissentlichkeit[218] vorliegen, da das Auskunftsverlangen jedenfalls als *„qualifizierter Hinweis"* zu werten ist. Dies gilt laut *Brenn* auch, wenn dem Provider *„der rechtswidrige Inhalt vor Augen geführt wird",* zB im Rahmen eines Abmahnschreibens, das einen *Screen-Shot*[219] enthält[220], welches von einem Privaten übermittelt wird.[221] Wird die Website nicht gesperrt, so hat dies – wie bereits erwähnt – den Verlust des Haftungsprivilegs zur Folge.[222] Des weiteren ermöglicht § 8 der ISPA-Verhaltensrichtlinien als Sanktion den Ausschluss des betreffenden Mitglieds

---

[215] Vgl *Zankl,* ECG-Handbuch Rz 291.

[216] Eine gesetzliche Befugnis zur Weitergabe von Daten rechtfertigt idR die Verletzung von Vertragspflichten. Die Weitergabe darf daher nicht nach DSG erlaubt sein, um zu einer Haftung zu gelangen. Zu § 1305 ABGB vgl *Harrer* in: *Schwimann*, ABGB Praxiskommentar VII[2] § 1305 Rz 1.

[217] Vgl *Zankl,* ECG-Handbuch Rz 244 FN 416. Allgemein zur Zulässigkeit von vertraglichen Haftungsbeschränkungen gegenüber Unternehmern und Konsumenten siehe *Koziol,* Haftpflichtrecht I[3] 538 ff.

[218] Zum Begriff der Wissentlichkeit: *Zankl*, ECG-Handbuch 235 f; *Kainz/Trappitsch*, Praxisrelevante Fragen der Haftungsfreistellungen des ECG, ecolex 2002, 737. Ausführlich, insbes zum Unrechtsbewusstsein (Vorsatz- oder Schuldtheorie): *Reindl,* E-Commerce und Strafrecht, 273 f.

[219] Bei einem Sreen-Shots „kopiert" man den Inhalt, der gerade auf einem PC-Monitor angezeigt wird, in eine Datei.

[220] Details hierzu siehe *Brenn,* ECG 282 f.

[221] Mit weiteren Beispielen: *Reindl,* E-Commerce und Strafrecht, 271

[222] Zur Problematik, dass die Verpflichtung zur Löschung uU den Tatbestand der Beweismittelunterdrückung erfüllt, siehe *Reindl,* E-Commerce und Strafrecht 278: Der Anwendungsbereich dieses Tatbestandes ist sehr klein und um sicher zu gehen, sollte das Material vom Host-Provider nicht sofort gelöscht werden. Es reicht idR die Sperrung des Zugangs.

aus der Vereinigung.[223] Sperrt der Provider die Site aufgrund einer behördlichen Anordnung, so muss dieser wohl keine vertraglichen Schadenersatzansprüche seiner Nutzer fürchten, denn er befolgt lediglich einen behördlichen bzw gerichtlichen Befehl.[224] Erlangt der Provider Kenntnis aufgrund eines „privaten" Schreibens, so sind allfällige Schadenersatzansprüche nach dem Vertragsverhältnis zwischen dem Provider und Nutzer zu beurteilen.[225]

Zu den strafrechtlichen Sanktionen bei rechtswidriger Datenweitergabe udgl nach TKG, siehe bereits in der Einleitung, S 15.

[223] Vgl hierzu auch: *Ebensperger* Die Verbreitung von NS-Gedankengut im Internet und ihre strafrechtlichen Auswirkungen unter besonderer Berücksichtigung des E-Commerce-Gesetzes, ÖJZ 2002, 132.

[224] Rechtfertigungsgrund der gesetzlichen Ermächtigung/behördliche Genehmigung (*Koziol,* Haftpflichtrecht I[3] 187). Eine andere Situation stellt sich dem insbes dem Host-Provider, wenn er seine Haftungsprivilegien erhalten möchte: siehe *Zankl,* ECG-Handbuch Rz 234.

[225] Vgl hierzu auch *Zankl*, ECG-Handbuch Rz 243. ZT enthalten AGB die Befugnis auf Verdacht zu sperren, vgl bspw http://www.cyberservice.org/agb/cyberservice_agb_20020724_final.htm .

IV. Urheberrechtsgesetz

A. Die InfoSoc-RL

Art 8 Abs 3 der – bereits erwähnten - Richtlinie 2001/29/EG vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft verpflichtet die Mitgliedsstaaten vorzusehen, dass *„Rechteinhaber gerichtliche Anordnungen gegen Vermittler beantragen können, deren Dienste von einem Dritten zur Verletzung eines Urheberrechts oder verwandter Schutzrechte genutzt werden."* Es handelt sich hier primär um verschuldensunabhängige Unterlassungsansprüche.[226]

Der 50. ErwGr der EC-RL erwähnt ausdrücklich die InfoSoc-RL bzw der 16. ErwGr des InfoSoc-RL die EC-RL: Beide Erwägungsgründe betonen die Notwendigkeit des gleichzeitigen Inkrafttretens der beiden RL mit der Begründung, dass zur Frage der Haftung der Vermittler bei Verstößen gegen das Urheberrecht und verwandte Schutzrechte auf Gemeinschaftsebene ein klares Regelwerk begründet werden soll. Unter Vermittler versteht das Gemeinschaftsrecht Access-, Cashing- und Host-Provider (dazu im Folgenden).

B. Die österreichische Umsetzung

Der Ministerialentwurf[227] zur Umsetzung der InfoSoc-RL wurde im August 2002 zur Begutachtung ausgesandt. Das vorzeitige Ende der XXI. Gesetzgebungsperiode machte ein neuerliches Einbringen im Nationalrat notwendig. Die Novelle wurde im Mai 2003 vom Nationalrat beschlossen.[228]

Die von der InfoSoc-RL vorgeschriebenen Unterlassungsansprüche wurden in § 81 Abs 1a UrhG umgesetzt. Gem § 87b Abs 3 haben Vermittler iSd § 81 Abs 1a dem Verletzten Auskunft über die Identität des Verletzers (Name und Anschrift) zu geben. Dieses Auskunftsrecht der Rechteinhaber ist in der InfoSoc-RL nicht enthalten. Die EB[229] führen hierzu aus, dass auch „*ein Anspruch auf Auskunft über die Identität von Rechtsverletzern im Ergebnis der Verhinderung künftiger Rechtsverletzungen und der Beseitigung des durch eine Rechtsverletzung geschaffenen Zustands dient."* Daher *„sollen diese*

---

[226] Vgl auch *Brenn*, ECG 307.

[227] Ministerialentwurf betreffend ein Bundesgesetz, mit dem das Urheberrechtsgesetz geändert wird (Urheberrechtsgesetz-Novelle 2002 - UrhG-Nov 2002).

[228] Urheberrechtsgesetz-Novelle 2003 - UrhG-Nov 2003 (NR: GP XXII RV 40 AB 51 S 12. BR: 6777 AB 6783 S 696), BGBl I 32/2003.

[229] EB zur UrhG-Nov 2003, 40 BlgNR XXII. GP 44, http://www.parlinkom.gv.at/pd/pm/XXII/I/his/000/I00040_.html .

Unterlassungs- und Beseitigungsansprüche durch einen Anspruch auf Information über die Identität des Verletzers ergänzt werden.".

Exkurs: Zum Begriff des Vermittlers

§ 87b Abs 3 verweist zur Definition des persönlichen Anwendungsbereichs dieser Norm auf § 81 Abs 1a, diese Bestimmung enthält jedoch eine solche Definition nicht. Auch erscheint es reichlich merkwürdig, dass sich der österreichische Gesetzgeber des Begriffes Vermittler bedient, hat er doch im ECG diesen Begriff vermieden. Die EB[230] führen hierzu aus: *"*[…] *hier ist zur Bedeutung des Begriffs „Vermittler" zu bemerken, dass diese* (sic!) *nicht nach innerstaatlichen Terminologie zu bestimmen ist, sondern nach dem Verständnis der Info-RL: Sowohl aus dem Erwägungsgrund 59 als auch der Entstehungsgeschichte der Richtlinie ergibt sich, dass Art 8 Abs 3 Info-RL eine Ergänzung zu Art 5 lit a Info-RL ist und dass damit primär im Sinn der letztgenannten Bestimmung gedacht ist; es geht dort um die Übertragung von Werken oder sonstigen Schutzgegenständen in einem Netz zwischen Dritten durch einen Vermittler"*. Beim Lesen dieser Erklärungen drängt sich dem Leser das Gefühl auf, der österreichische Gesetzgeber wusste selbst nichts mit diesem Begriff anzufangen. Vielmehr versucht er ihn mittels einer Tautologie zu erklären. Grundsätzlich würde man wohl instinktiv davon ausgehen, dass lediglich Access- und Cashing-Provider Inhalte in einem Netz zwischen Dritten übertragen können, nicht aber Host-Provider. So führt auch *Walter*[231] im Hinblick auf Art 5 Abs 1 (zwingende Ausnahmen vom Vervielfältigungsrecht ohne eigenständige wirtschaftliche Bedeutung) aus, dass diese Regelung auf Hosting nicht anwendbar sei, da hier weder flüchtige noch begleitendende Vervielfältigungen vorliegen, und auch die Voraussetzungen einer fehlenden eigenständigen wirtschaftlichen Bedeutung nicht gegeben sein werden. Dies liegt in der Natur der Sache und entspricht auch der Zielsetzung der InfoSoc-RL, die freie Werknutzung tunlichst einzuschränken, hat aber mE auf das allgemeine Begriffsverständnis von „Vermittler" außerhalb des Art 5 Abs 1 keinen Einfluss.

Es ist aber davon auszugehen, dass der europäische Gesetzgeber iSd Einheitlichkeit der Rechtsordnung vom gleichen Begriffsverständnis ausgegangen ist, wie es bereits von der EC-RL geprägt worden ist: Die Überschrift des 4. Abschnitts (Art 12 bis 14) der EC-RL lautet *"Verantwortlichkeit der Vermittler",* und werden in diesem Abschnitt Access-, Cashing- und Host-Provider geregelt. In der englischen Fassung der EC-RL wird von „*intermediary service providers"* gesprochen, in jener der InfoSoc-RL heißt es *„intermediaries"*. Außerdem wäre es wohl sinnwidrig, wenn die Unterlassungsansprüche gerade für Host-Provider nicht gelten sollte, denn auf ihren Servern liegt das inkriminierte Material.[232] Vermittler nach diesen Bestimmungen sind daher die aufgezählten Provider.[233]

[230] aaO 42.

[231] (Hrsg), Europäisches Urheberrecht (2001), Rz 114 und Rz 148 zur Info-RL.

[232] Man könnte allerdings auch argumentieren, dass Auskunftsansprüche gegen Host-Provider ohnehin abschließend in der EC-RL geregelt sind.

[233] Vgl auch *Brenn,* ECG 173, 263.

1. Unterlassungs- und Beseitigungsanspruch (§ 81 Abs 1a, § 82)

„§ 81 Abs 1a Bedient sich derjenige, der eine solche Verletzung begangen hat oder von dem eine solche Verletzung droht, hiezu der Dienste eines Vermittlers, so kann auch dieser auf Unterlassung nach Abs. 1 geklagt werden."

„§ 82 Abs 1 Wer in einem auf dieses Gesetz gegründeten Ausschließungsrechte verletzt wird, kann verlangen, daß der dem Gesetz widerstreitende Zustand beseitigt werd; § 81 Abs. 1a gilt sinngemäß."

Die Exklusivrechte nach UrhG gewähren seinem Inhaber den gegen jedermann gerichteten Anspruch, Handlungen, die in diese Rechte eingreifen, zu unterlassen (§ 81 Abs 1).[234] Der Abs 1a leg cit erweitert - in Umsetzung des Art 8 Abs 3 InfoSoc-RL – den Anwendungsbereich dieser Norm – unnötigerweise - ausdrücklich auch auf ISP. Ebenso Ausfluss eines absoluten Rechtes ist der Beseitigungsanspruch. § 82 erklärt daher den § 81 Abs 1a für sinngemäß anwendbar. Der Rechteinhaber kann daher den ISP auch auf Entfernung des urheberrechtswidrigen Materials, das bspw auf seinen Servern liegt, klagen. Dies stellt aber kein Novum dar.

2. Auskunftspflichten (§ 87 Abs 3) und das Verhältnis zum ECG

„§ 87b. (3) Vermittler im Sinn des § 81 Abs. 1a haben dem Verletzten Auskunft über die Identität des Verletzers (Name und Anschrift) zu geben."[235]

Diese zusätzliche Auskunftspflicht wurde zur Durchsetzung von Urheberrechten in Umsetzung der InfoSoc-RL normiert. Fraglich ist, in welchem Verhältnis § 87 Abs 3 und § 18 Abs 4 ECG zueinander stehen. Es ist wohl davon auszugehen, dass das UrhG als *lex posterior* und *lex specialis* dem ECG derogiert, soweit es ihm widerspricht:[236] Im Bereich des UrhG steht einem Dritten, soferne er Rechteinhaber ist, daher auch ein Auskunftsrecht gegenüber Access-Providern zu, und zwar ohne weitere Voraussetzungen. Die Identifikation des Verletzers kann anhand der IP-Adresse oder einer E-Mail Adresse erfolgen. Da § 87b Abs 3 ausdrücklich von Anschrift spricht, ist die Beauskunftung einer E-Mail Adresse ausgeschlossen.

3. Durchsetzung, Sanktionen und Rechtsfolgen

Unterlassungs- und Beseitigungsansprüche werden im Klagsweg durchgesetzt. Auskunftspflichten nach § 87b Abs 1 (Anspruch auf

---

[234] Zu Unterlassungs- und Beseitigungsanspruch nach UrhG: Vgl *Dillenz,* Praxiskommentar zum österreichischen Urheberrecht und Verwertungsgesellschaftenrecht (1999) 223 ff, 227 ff; *Dittrich,* Österreichisches und Internationales Urheberrecht (1998), § 81 bzw § 81.

[235] Zur Entstehungsgeschichte dieser Auskunftspflicht vgl die EB: Regierungsvorlage zur UrhG-Nov 2003, 40 BlgNR XXII. GP 43, http://www.parlinkom.gv.at/pd/pm/XXII/I/images/000/I00040__2478.pdf .

[236] Scheinbarer Normwiderspruch, vgl hierzu: *Koziol/Welser*, Bürgerliches Recht I[12] (2002) 34 f.

Rechnungslegung) können laut OGH[237] mittels Stufenklage[238] durchgesetzt werden. Diese ist allerdings nur bei einem Anspruch auf Rechnungslegung anwendbar. Bei der gegenständlichen Auskunftspflicht nach Abs 3 besteht ein solcher allerdings nicht. Die Auskunftspflicht ist daher in einem selbstständigen Verfahren durchzusetzen. Allerdings kann es in praxi wohl vorkommen, dass es im Rahmen eines bereits anhängigen Verfahrens notwendig wird, Auskunftsverlangen zu stellen, wenn bspw eine falsche Person geklagt worden ist. [239]

Eine rechtswidrige Datenweitergabe ist nach den Regeln des TKG bzw des DSG zu beurteilen (dazu schon oben, S 15, 17.)

C. Ausblick: Richtlinienvorschlag über die Maßnahmen und Verfahren zum Schutz der Rechte an geistigem Eigentum

Im Jänner 2003 stellte die EU-Kommission einen Richtlinienvorschlag zur Durchsetzung der Rechte an geistigem Eigentum vor. Das unter dem Aktenzeichen KOM(2003) 46 endg[240] veröffentlichte Dokument befasst sich mit der Verletzung aller gemeinschaftsweit harmonisierten Rechte an geistigem Eigentum (Immaterialgüterrechte). Der RL-Vorschlag betrifft daher das Urheberrecht, die verwandten Leistungsschutzrechte und das gewerbliche Eigentum (beispielsweise Marken oder Gebrauchsmuster). Hauptstoßrichtung sind Rechtsverletzungen, die zu gewerblichen Zwecken erfolgen oder den Rechteinhabern erheblichen Schaden zufügen. Das Instrumentarium, das in der gesamten EU bereitgestellt werden soll, beinhaltet unter anderem Verfügungen zur Unterbindung des Handels mit Nachahmungen und Raubkopien, einstweilige Maßnahmen, wie bspw die Sperrung der Bankkonten von Verdächtigen, bestimmte Befugnisse für die Justizbehörden zur Beweismittelbeschaffung sowie zur Durchsetzung von Schadenersatzzahlungen seitens der Rechtsverletzer an die Rechteinhaber für entgangene Gewinne.

Dieser Vorschlag stieß bei den ISP und anderen Telekommunikationsunternehmen auf herbe Kritik, da sich diese vom Entwurf besonders betroffen fühlen.[241] So sei darin die Sperrung von Websiten vorgesehen, ebenso wie eine Erweiterung der Strafbestimmungen zum Schutz geistigen Eigentums, wenn die Verletzung absichtlich und zu kommerziellen

---

[237] OGH 5. 11. 2002, 4 Ob 237/02k = ÖBl 2003/26.

[238] Vgl Art XLII der EGZPO. Näheres zur Stufenklage und ihrer Funktion: *Rechberger/Simotta,* Zivilprozessrecht[6] Rz 391 f.

[239] Zu den strafprozessualen Zwangsmitteln siehe im Kapitel Strafprozessordnung und Telekommunikationsgesetz, S 51 ff.

[240] Der Vorschlag und weitere Materialien sind abrufbar unter: http://europa.eu.int/comm/internal_market/de/intprop/docs/ .

[241] Internet-Provider kritisieren neue Urheberrechtsrichtlinie, Heise Online, http://www.heise.de/newsticker/data/anw-23.06.03-004/ . Vgl auch: EU eröffnet Jagd auf Tauschbörsennutzer, orf futurezone, http://futurezone.orf.at/futurezone.orf?read=detail&id=178009&tmp=12276 .

Zwecken erfolgt. Dem hält die Kommission in den FAQ[242] entgegen, dass die Rechteinhaber einen Anspruch auf Kontrolle der Nutzung ihres geistigen Eigentums haben und soll diese Richtlinie die *„Nutzung des Internet als wahrhaft schöpferisches Medium fördern"* anstatt ein Werkzeug der Produktpiraterie und der Verletzung des geistigen Eigentums zu sein. Die Richtlinie schaffe auch einen angemessenen Ausgleich zwischen den Interessen der Rechteinhaber und den rechtmäßigen Nutzern einerseits und den größeren Möglichkeiten durch das Internet andererseits, da nur gewerbliche Rechtsverletzer von der Richtlinie erfasst sein sollen. Die Richter seien überdies an das Verhältnismäßigkeitsgebot gebunden. Die Richtlinie habe auch eminente Bedeutung für die Entwicklung des E-Commerce, da der Online-Vertrieb von Waren und Dienstleistungen erst dann Erfolg haben werde, wenn die Händler einen legitimen Gewinn aus ihrer Tätigkeit erwirtschaften können.

1. Beweismittel (Art 7 RL-Entw)

Dieser Artikel befasst sich mit der Herausgabe von Beweismitteln, die sich in der Verfügungsgewalt der gegnerischen Partei befinden (Abs 1), und der Befugnis von Gerichten die Herausgabe von Bank-, Finanz- oder Handelsunterlagen gegenüber Dritten anzuordnen (Abs 2). Bereichsspezifische Probleme bei der Anwendbarkeit auf ISP sind nicht ersichtlich.

2. Beweissicherungsverfahren (Art 8 RL-Entw)

Diese Bestimmung regelt bei einer tatsächlichen oder drohenden Verletzung eines Rechts an geistigem Eigentum den Schutz von Beweismitteln. Ähnlich wie § 384 ZPO, ermöglicht dieses Beweissicherungsverfahren schon vor Einleitung eines Verfahrens die gerichtliche Beschlagnahme durch Beschreibung mit oder ohne Einziehung von Mustern oder die dingliche Beschlagnahme der rechtsverletzenden Ware, sowie gegebenenfalls der zugehörigen Unterlagen, wenn die Gefahr der Beweismittelvernichtung besteht. Binnen 31 Tagen muss der Antragsteller, bei sonstiger Unwirksamkeit der Sicherung, Klage beim zuständigen Gericht einbringen.

Allenfalls kommt hier die Beschlagnahme von Datenträgern in Betracht. Die Befugnis zur Erlassung einer Löschungsanordnung kann aus einer solchen Beschlagnahmeermächtigung nicht abgeleitet werden.

3. Recht auf Auskunft (Art 9 RL-Entw)

Auf Antrag können Gerichte, im Rahmen eines Verfahrens zur Feststellung der Verletzung eines Rechts an geistigem Eigentum oder eines Beweissicherungsverfahrens, sofern keine besonderen Gründe entgegenstehen, jeder Person zu verpflichten, Auskünfte über den Ursprung und die

[242] Pressemitteilung der GD Binnenmarkt, Richtlinienvorschlag zur Durchsetzung der Rechte an geistigem Eigentum: Häufig gestellte Fragen, http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=MEMO/03/20|0|RAPID&lg=DE&display= .

Vertriebswege von Waren oder Dienstleistungen zu erteilen, bei denen Verdacht auf Verletzung eines Rechts an geistigem Eigentum besteht. Diese Person muss allerdings entweder selbst im Besitz der inkriminierten Ware sein, rechtsverletzende Dienstleistungen zu gewerblichen Zwecken in Anspruch genommen haben oder als Ausgangspunkt oder Bindeglied im Vertriebsweg solcher Waren oder Dienstleistungen identifiziert worden sein. Letzteres trifft wohl auf Host-Provider zu, wenn auf ihren Servern Websites gespeichert sind, über die bspw unberechtigterweise vervielfältige Software angeboten wird.[243]

Diese Auskünfte beziehen sich gem Abs 2 leg cit auf Namen und Adresse der Hersteller, Vertreiber, Lieferer und anderer Vorbesitzer der Ware oder Dienstleistung sowie der gewerblichen Abnehmer und Verkaufsstellen, sowie auf Angaben über die Menge der hergestellten, ausgelieferten, erhaltenen oder bestellten Waren und über die Preise, die für die betreffenden Waren oder Dienstleistungen gezahlt wurden.

Ferner sieht Abs 4 eine originelle „Anzeigepflicht" von Behörden an Private vor. Die Behörden müssen die Rechteinhaber über Rechtsverletzung des geistigen Eigentums informieren, um diesem die Einleitung eines Verfahren zu ermöglichen.

4. Einstweilige Maßnahmen zum Schutz geistigen Eigentums (Art 10 RL-Entw)

Nach Art 10 räumen die Mitgliedsstaaten den zuständigen Gerichten die Möglichkeit ein, „*gegen den vermeintlichen Verletzter oder gegen eine Mittelsperson, die deren Dienste von einem Dritten zwecks Verletzung eines Rechts in Anspruch genommen werden* (sic!)*, eine einstweilige Verfügung zu erlassen, um eine drohende Verletzung geistigen Eigentums zu verhindern oder einstweilig und unter Androhung von Beugemitteln die Fortsetzung angeblicher Rechtsverletzungen zu untersagen oder die Fortsetzung an die Stellung von Garantien zu knüpfen, die die Entschädigung des Rechteinhabers sicherstellen sollen."* Des weiteren müssen die Gerichte befugt sein, die Vorlage aller vernünftigerweise verfügbaren Beweise vom Rechteinhaber zu verlangen, um sich mit ausreichender Sicherheit davon überzeugen zu können, „*dass der Antragsteller der Rechtsinhaber ist und dass das Recht des Antragstellers verletzt wird oder dass eine solche Verletzung droht."*

Fest steht, dass mit dieser Bestimmung auch Unterlassungsverfügungen gegenüber ISP erlassen werden können. Dies wäre allerdings nur dann ein Novum, wenn diese Bestimmung auch für den Strafprozess gelte. Der Entwurf selbst enthält einige strafrechtliche Regelungen (vgl Art 20). Art 10 scheint wohl eher auf ein kontradiktorisches Verfahren iSd ZPO abzustellen (arg „Antragsteller", „Gegenpartei"), und Art 5 zählt nur die Rechteinhaber

[243] Ware ist eine bewegliche körperliche Sache. Im Bereich des IPR (EVÜ und UN-Kaufrecht) wird Software als Ware angesehen (vgl mwH: *Mochar/Seidl*, Internationales Verbraucherschutzrecht, ÖJZ 2003/13). Im Umsatzsteuerrecht wird diese Qualifikation allerdings abgelehnt. So *Thiele* (Umsatzsteuerliche Behandlung von Internetgeschäften in der EU und Österreich, ÖStZ 2000/697), der die E d EuGH Rs C-79/89, *Brown Boveri & Cie AG/Hauptzollamt Mannheim*, Slg 1991 I-1853 Rz 21 zitiert.

(allenfalls auch Verwertungsgesellschaften) zu den berechtigten Antragstellern, nicht aber Strafverfolgungsbehörden. Allerdings sind die Delikte gegen das geistige Eigentum allesamt Privatanklagedelikte. Art 10 könnte daher zur ersten Rechtsgrundlage für die Anordnung einer Sperrverfügung durch ein Strafgericht führen (zu diesem Thema siehe auch im Kapitel Strafprozessordnung und Telekommunikationsgesetz, S 51 ff bzw ECG, S 37).

V. Strafprozessordnung und Telekommunikationsgesetz

A. Allgemeines

Für Private besteht gem § 89 StPO keine Anzeigepflicht, sondern lediglich ein Anzeigerecht. Gem § 143 Abs 1 StPO ist jedermann dazu verpflichtet, Gegenstände, die für die Untersuchung von Bedeutung sein können oder dem Verfall oder der Einziehung unterliegen, insbesondere auch Urkunden, auf Verlangen herauszugeben (Editionspflicht).[244] Ebenso wird in § 150 die Pflicht statuiert, als Zeuge vor Gericht zu erscheinen und eine wahrheitsgemäße Aussage abzugeben. Beide Pflichten sind durch die Entschlagungsrechte des § 152 beschränkt.[245] Die StPO bindet die Zwangsmittel streng an den Begriff des „Gegenstandes", also körperlicher Sachen. Die Sicherstellung bzw Beschaffung unkörperlicher Sachen, wie Daten, ist nur im Ausnahmefall geregelt. Dies ist einer der Gründe, wieso die Lit zahlreiche Umwegkonstruktionen entwickelt hat, und insbes die Regelungen über die Beschlagnahme hilfsweise herangezogen werden müssen.

B. Mitwirkungspflichten bei der Datenerhebung

Mitwirkungspflichten unbeteiligter Dritter im Rahmen der Sicherungsmittel des Vorverfahrens sind - abgesehen von den bereits erwähnten - in der StPO teils explizit enthalten (zB bei der Überwachung des Fernmeldeverkehrs), teils wurden sie erst von der Lehre entwickelt (so insbes bei der Beschlagnahme).

1. Beschlagnahme

Zweck der Beschlagname ist die Sicherstellung von Gegenständen, die in einem Strafverfahren zu Beweiszwecken dienen könnten, oder dem Verfall iSd § 20b StGB bzw der Einziehung iSd § 26 StGB unterliegen könnten. Jeder Hausdurchsuchungsbefehl rechtfertigt auch die Beschlagnahme von Gegenständen. Sog „Zufallsfunde" - also Beweisgegenstände die nicht konnex mit dem Verfahren sind – dürfen gem § 144 beschlagnahmt werden, soweit es sich um von Amts wegen zu verfolgende Straftaten handelt. Dies ist insbes im Urheberrecht nicht der Fall, da dort ausschließlich Privatanklagedelikte vorgesehen sind (§ 91 Abs 3 UrhG). Voraussetzung für die Beschlagnahme ist – wenn nicht schon ein Hausdurchsuchungsbefehl vorliegt – ein richterlicher

[244] Vgl *Seiler,* Strafprozessrecht[6] Rz 359.

[245] Zum *nemo-tenetur*-Grundsatz: siehe schon in der Einleitung, S 21. Näheres zu den Entschlagungsrechten im Strafprozess: vgl *Seiler,* Strafprozessrecht[6] Rz 454 ff.

Beschlagnahmebefehl. Bei Gefahr in Verzug können die Sicherheitsbehörden allerdings auch ohne richterlichen Befehl eine Beschlagnahme durchführen.[246]

Zur Sicherung der Abschöpfung der Bereicherung oder des Verfalls kann der Untersuchungsrichter auf Antrag der Staatsanwaltschaft eine einstweilige Verfügung gem § 144a erlassen, wenn die Befürchtung besteht, dass anderenfalls die Einbringung gefährdet oder wesentlich erschwert würde. Als Sicherungsmittel können – unter Außerachtlassung der dort normierten Voraussetzungen – jene nach § 379 Abs 3 EO ergriffen werden. So kommt insbes das Drittverbot (Verbot einen Geldbetrag an einen anderen auszuzahlen) in Betracht.[247]

Gem § 143 Abs 2 ist jedermann zur Herausgabe von Beweisgegenständen verpflichtet (Editionspflicht). Ist der Inhaber des Gegenstandes nicht selbst verdächtig oder hat er ein Entschlagungsrecht, so kann er zur Herausgabe der Sache mittels Beugestrafen in der Höhe bis Euro 726 bzw Beugehaft bis zu 6 Wochen, gezwungen werden. Die Beugemittel müssen gem § 143 Abs 3 entsprechend dem Verhältnismäßigkeitsgrundsatz angewandt werden. Gem § 143 Abs 4 sind dem Betroffenen die ortsüblichen, angemessenen Kosten die ihm durch die Trennung von den Beweisgegenständen bzw Anfertigung von Kopien notwendigerweise entstanden sind, zu ersetzen.

Sonderbestimmungen finden sich in der StPO zur Kontoauskunft und zur Beschlagnahme von Briefen bzw außerhalb der StPO, im UrhG und im MedienG. Im Folgenden wird zu prüfen sein, wie diese Bestimmungen auf Daten bzw Datenträger anwendbar sind. Mangels Relevanz für das hier behandelte Thema wird auf die Bestimmungen zur Kontoauskunft bzw zur Beschlagnahme von Briefen[248] nicht näher eingegangen.

a) Die Beschlagnahme von Datenträgern im Allgemeinen

Soweit nicht die Bestimmungen über die Beschlagnahme von Papieren (dazu unten) oder Sonderregeln der Überwachung des Fernmeldeverkehrs zur Anwendung gelangen, sind Datenträger nach den allgemeinen Vorschriften zu behandeln.[249] Durch die Anwendung der Bestimmungen über die Beschlagnahme darf der Schutz des Fernmeldegeheimnisses nicht umgangen werden. Dies betrifft überwiegend jene Fälle, bei denen Vermittlungs- oder Inhaltsdaten auf den Datenträgern gespeichert sind.[250]

In praxi wird sich das Problem stellen, dass bspw eine Website bei einem Provider gehostet wird, diese aber nicht die einzige Site auf dem Server ist. Eine Beschlagnahme der Festplatte wäre wohl unverhältnismäßig, da hiermit nicht nur die inkriminierte Site vom Netz genommen würde, sondern auch alle anderen, die auf der Festplatte gespeichert sind. Gem § 143 Abs 2 ist im

---

[246] Vgl *Seiler,* Strafprozessrecht[6] Rz 355.

[247] Näheres siehe bei *Seiler,* Strafprozessrecht[6] Rz 357.

[248] E-Mails erfüllen nicht die Voraussetzungen eines Briefes idS.

[249] Vgl bei *W Wessely,* Sicherheitspolizeiliche und strafprozessuale Erhebungen im Internet, ÖJZ 1996, 612.

[250] OGH 18.1.2001, 12 Os 152/00 = ÖJZ 2001/115 (EvBl); vgl mwH auch *Reindl*, Die nachträgliche Offenlegung von Vermittlungsdaten des Telefonverkehrs im Strafverfahren ("Rufdatenrückerfassung"), JBl 1999, 791,

Rahmen der Editionspflicht auch die Anfertigung von Kopien zur Beweiserhebung zulässig. Die Herstellung einer identen Kopie muss für diese Zwecke ausreichend sein, und daher kann die Originalfestplatte beim Provider verbleiben.[251] Diese Verpflichtung ist jedoch nach *Muskatelz*[252] nicht durchsetzbar. Der Provider kann daher nicht gezwungen werden, eine Kopie herzustellen und diese herauszugeben. Diesfalls könnte jedoch die Originalfestplatte beschlagnahmt werden. Gibt der Provider freiwillig eine Kopie der Festplatte heraus, ist ihm anzuraten, im Einvernehmen mit den Behörden, den Zugang zur der inkriminierten Site zu sperren bzw diese (auf der im Server verbleibenden Festplatte) zu löschen.[253]

In diesem Zusammenhang ist auch von Interesse, wieweit die Mitwirkungspflichten des Providers reichen. Muss zB der ISP, wenn die Daten in verschlüsselter Form vorliegen oder Passwörter für den Zugang zum Computersystem notwendig sind, diese Informationen herausgeben? Grundsätzlich ist davon auszugehen, dass die meisten Passwörter und Verschlüsselungen „geknackt" werden können. Die Herausgabe dieser Informationen stellt allerdings eine beträchtliche Aufwandsersparnis für die Strafverfolgungsbehörden dar. *Muskatelz*[254] lehnt die Durchsetzung dieser Herausgabe mit der fehlenden Rechtsgrundlage für eine solche Mitwirkung ab. Auch die Ermittlung der notwendigen Informationen durch Zeugenvernehmung ist abzulehnen, da die Frage, wie der Betroffene seine Daten absichert, inhaltlich in keinem Zusammenhang mit der Strafsache steht.[255]

Zu betonen ist, dass die Beschlagnahme die einzige Möglichkeit im österreichischen Strafrecht ist, rechtswidrige Inhalte aus dem Internet zu entfernen, da es – wie bereits im Kapitel E-Commerce-Gesetz (S 37) erwähnt – ansonsten keine Rechtsgrundlagen für ein solches Vorgehen gibt. Wie sich aus den obigen Ausführungen ergibt, ist aber auch die Beschlagnahme kein wirklich passendes Mittel.

---

[251] Siehe auch den Hinweis des Justizministeriums des Freistaates Thübingen (http://www.thueringen.de/de/justiz/publikationen/online/u4/u_start.html): *"Für den Beweiswert der Daten ist zu berücksichtigen, dass der Originalzustand durch Weiterbenutzung zumeist verändert wird. Es muss daher durch geeignete Maßnahmen (etwa durch Kopie der File-Allocation-Tabelle) dokumentiert werden, wie der Original-Datenbestand zum Zeitpunkt der Sicherstellung ausgesehen hat. Es kann u.U. erforderlich sein, neben reinen Daten-Dateien auch Programm-Dateien und Passwortlisten sicherzustellen."* Vgl *Muskatelz,* Der Datenzugriff im Strafverfahren (2000) 79 f. Siehe auch § 145a Abs 2 StPO.

[252] aaO. In weiterer Folge lehnt er auch die Beschlagnahme von Daten als *„Abfolge elektrischer Impulse"* im Wege der Datenübertragung, zB via Modem oder Netzwerkverbindung, mit der Begründung ab, die StPO biete für die Beschlagnahme unkörperlicher Sachen keine Rechtsgrundlage.

[253] Zur Kollision von Löschungsverpflichtung und Beweismittelunterdrückung siehe schon oben in der FN S 42.

[254] Vgl *Muskatelz,* Der Datenzugriff im Strafverfahren 84.

[255] So *Muskatelz,* Der Datenzugriff im Strafverfahren 89.

b) Die Beschlagnahme von Papieren

Unter Papieren sind Aufzeichnungen, wie Tagebücher, Gedächtnisprotokolle, Urkunden etc zu verstehen.[256] Sie besitzen nicht den Charakter verschlossener Postsendungen und können daher ohne weitere Voraussetzungen beschlagnahmt werden (§ 145). § 452 Z 4 schließt im BG-Verfahren die Beschlagnahme von Papieren bei Dritten generell aus. Gem § 145 Abs 2 hat der Inhaber der Papiere die Möglichkeit, Widerspruch gegen die Kenntnisnahme des Inhalts der Papiere durch die Behörde, zu erheben. Diese sind dann zu versiegeln, und der Ratskammer vorzulegen, die beschließt, ob die Papiere durchsucht werden oder zurückzustellen sind.

Reindl[257] vertritt in diesem Zusammenhang, dass die Bestimmungen über die Beschlagnahme von Papieren auch auf Datenträger anzuwenden sind. Dies mit der Begründung, Schriftstücke seien als Einheit von Daten und Papier anzusehen. *„Die einstige Einheit von Daten und Papier wird lediglich durch die neue Verbindung von Daten und Diskette oder Festplatte ersetzt.“*. Diese Meinung vertritt auch der BGH[258]. Enthalten daher Datenträger vertrauliche Informationen iSd § 145, so kann der Inhaber des Datenträgers Widerspruch erheben, und folglich ist der Datenträger der Ratskammer vorzulegen.

c) Sonderbestimmungen nach MedienG

Das MedienG enthält eine Reihe von Sonderbestimmungen zur Beschlagnahme (§ 36) und überdies ein Verbreitungsverbot (§ 38). Websiten sind nach hA Medien iSd § 1 Abs 1 Z 1 MedienG, aber mangels Körperlichkeit keine Medienwerke iSd Z 3 leg cit.[259] Die genannten Sonderbestimmungen gehen von *„der zur Verbreitung bestimmten Stücke eines Medienwerkes“* aus. Daraus folgt, dass diese Bestimmungen auf Websiten nicht anwendbar sind. Ebenso wenig sind sie auf Server-Festplatten anwendbar, denn diese sind kein zur Verbreitung bestimmtes Stück eines Medienwerkes, womit das einzelne Buch, die Zeitschrift oder auch eine Diskette gemeint ist.[260]

---

[256] Vgl *Seiler,* Strafprozessrecht[6] Rz 372.

[257] Die nachträgliche Offenlegung von Vermittlungsdaten des Telefonverkehrs im Strafverfahren ("Rufdatenrückerfassung"), JBl 1999, 791. Die Anwendbarkeit des § 145 auf Datenträger ebenso andenkend: *Muskatelz,* Der Datenzugriff im Strafverfahren 87. Er lässt jedoch die Frage im Ergebnis offen.

[258] In seiner Jud zu § 110 dStPO, vgl *Radtke*, Rechtsbehelfe gegen die "Durchsicht" (§ 110 StPO) von EDV-Anlagen durch Strafverfolgungsbehörden, JurPC Web-Dok 173/1999 Abs 18 ff = http://www.jurpc.de/aufsatz/19990173.htm#fn1 .

[259] Ausführlich bei: *Brandstetter/Schmid*, Mediengesetz Kommentar[2] (1999) § 1 Rz 4, 16, 19. Siehe auch OLG Wien 3.10.2002, 17 Bs 249/02 = MR 2002, 373.

[260] Vgl *Brandsteller/Schmid,* Mediengesetz[2] Vorbemerkungen Rz 8; Vgl auch *Schmölzer,* Strafrecht, in: in: *Jahnel/Schramm/Staudegger* (Hrsg), Informatikrecht[2] 377.

d) Sonderbestimmungen nach UrhG

§ 92 UrhG behandelt – als Pendant zum zivilrechtlichen Beseitigungsanspruch[261] - die Vernichtung und Unbrauchbarmachung von Eingriffsgegenständen und Eingriffsmitteln iSd § 90b sowie des § 90c Abs 3. Eingriffsmittel iSd § 90b sind Mittel, die in Verkehr gebracht oder zu Erwerbszwecken besessen werden, und allein dazu bestimmt sind, die unerlaubte Beseitigung oder Umgehung von technischen Mechanismen zum Schutz von Computerprogrammen, zu erleichtern. Diese Rechtsgrundlage könnte es einem Rechtinhaber ermöglichen, einen ISP zu zwingen, Key-Generatoren[262] von einer bei ihm gehosteten Website zu löschen. § 90c schützt technische Maßnahmen zur Verhinderung von Verletzungen von Ausschließlichkeitsrechten im Allgemeinen (also nicht nur bezogen auf Computerprogramme). Zur Durchsetzung des § 92 kann der Privatankläger gem § 93 die Beschlagnahme der Eingriffsgegenstände und –mittel beantragen. Als Rechtsgrundlage für die Sperrung einer Website können die §§ 92 f nicht herangezogen werden.

2. Hausdurchsuchung

Die StPO regelt in den §§ 139 ff die Durchsuchung von zum Hauswesen gehörigen Räumlichkeiten zur Auffindung von verdächtigen Personen oder von Sachen, die für eine bestimmte Untersuchung von Bedeutung sein könnten. Bereits vor der Untersuchung muss der begründete Verdacht bestehen, dass sich in diesen Räumlichkeiten eine solche Person oder Sache befindet (materielle Voraussetzung). Der Hausdurchsuchungsbefehl muss angeben, welche Gegenstände man verdächtigt, in dieser Wohnung zu sein (formelle Voraussetzung). Wem diese Räumlichkeiten gehören, ist ohne Belang.[263] Entsprechend dem Verhältnismäßigkeitsgrundsatz ist gem § 140 Abs 1 derjenige, gegen den die Hausdurchsuchung geführt wird, vorher zu vernehmen. Gibt der Betroffene die gesuchten Gegenstände freiwillig heraus, ist die Hausdurchsuchung abzubrechen. Schon erläutert wurde, dass jede Hausdurchsuchung auch die Beschlagnahme der in den Räumlichkeiten gefundenen Gegenstände, rechtfertigt.[264]

Gem § 142 Abs 2 ist der Inhaber der Räumlichkeiten aufzufordern, bei der Durchsuchung anwesend zu sein.

Die Vornahme einer Hausdurchsuchung ist grundsätzlich nur aufgrund eines richterlichen Befehls zulässig. Bei Gefahr in Verzug kann eine Hausdurchsuchung auch von Beamten der Sicherheitsbehörden vorgenommen werden bzw von Sicherheitsorganen aus eigener Macht.

Wie bereits erwähnt, können die Sicherheitsbehörden die Herstellung und Ausfolgung einer Datenträger-Kopie nicht erzwingen. Es stellt sich somit die

---

[261] *Dillenz*, Praxiskommentar zum UrhG 249.

[262] An Hand dieser Key-Generators kann man Seriennummern zur Freischaltung von einer (unentgeltlichen) Testversion zur (kostenpflichtigen) Vollversion eines Computerprogramms generieren.

[263] Vgl *Seiler,* Strafprozessrecht[6] Rz 342 f.

[264] Vgl *Seiler,* Strafprozessrecht[6] Rz 344.

Frage, ob im Rahmen einer Hausdurchsuchung vor Ort Datenbestände durchsucht werden dürfen, was gelegentlich auch die Inbetriebnahme der

Rechner des Providers voraussetzen kann.[265] Zur Benützung von angefundenen Gegenständen im Rahmen von Hausdurchsuchungen existiert bis dato keine Judikatur. Da die Benützung eines fremden Gegenstandes jedoch einen Eingriff in das Eigentumsrecht dar stellt, und sich hierfür in der StPO keine taugliche Rechtsgrundlage iSd Art 5 StGG findet, ist eine solche Benützung wohl unzulässig.[266]

a) Aufgrund richterlichen Befehls

Gem § 140 Abs 3 ist formelle Voraussetzung für eine Hausdurchsuchung ein mit Gründen versehener richterlicher Befehl. Dieser ist den Beteiligten sogleich oder binnen 24 Stunden zuzustellen. Vollziehende Organe sind iaR Sicherheitsorgane.

b) Bei Gefahr in Verzug

§ 141 Abs 1 erlaubt bei Gefahr in Verzug den Beamten der Sicherheitsbehörden, eine Hausdurchsuchung auch ohne richterlichen Befehls durchzuführen. Das Organ ist mit einer schriftlichen Ermächtigung auszustatten. Gefahr in Verzug wird allerdings recht selten vorliegen, denn der Richter darf nicht einmal telephonisch erreichbar sein, um den Durchsuchungsbefehl mündlich zu erteilen.[267]

c) Aus eigener Macht

Sicherheitsorgane können gem § 141 Abs 2 auch aus eigener Macht eine Hausdurchsuchung vornehmen, wenn gegen den Beteiligten ein Haft- oder Vorführbefehl erlassen wurde oder wenn jemand auf frischer Tat ertappt, durch öffentliche Nacheile oder öffentlichen Ruf als einer strafbaren Handlung verdächtig bezeichnet oder im Besitze von Gegenständen betreten wird, die auf die Beteiligung an einer solchen hinweisen.

3. Überwachung des Fernmeldeverkehrs

Mit dem STRÄG 2002[268] wurden nicht nur die neuen „Computerdelikte“ eingeführt, sondern auch die Überwachung des Fernmeldeverkehrs neu geregelt,[269] insbes brachte es Klarstellungen betreffend Vermittlungsdaten.[270]

---

[265] IaR handelt es sich hier allerdings um Server, die ohnehin praktisch nie abgeschaltet werden.

[266] Vgl die Nachweise bei *Muskatelz,* Der Datenzugriff im Strafverfahren 83 f.

[267] Bei den Straflandesgerichten sind Journaldienste eingerichtet.

[268] Strafrechtsänderungsgesetz 2002, BGBl I 143/2002 (NR: GP XXI RV 1166 AB 1213 S 110. BR: 6695 AB 6738 S 690.).

[269] Siehe nur *Maleczky,* Das Strafrechtsänderungsgesetz 2002, JAP 2002/2003, 134.

§ 149a Abs 1 bietet nunmehr auch einige brauchbare Definitionen:

- Telekommunikation (Z 1): Für den Begriff Telekommunikation wird auf § 3 Z 13 TKG 1997 verwiesen. Darunter ist das Aussenden, Übermitteln und Empfangen von Nachrichten jeglicher Art mittels dazu dienender technischer Einrichtungen zu verstehen. Jedenfalls auch unter den Begriff Telekommunikation fallen das Internet und seine Dienste, wie E-Mail, das www udgl.[271] Durch das TKG 2003 ergeben sich keine wesentlichen Unterschiede, auch wenn dieses keine Definition der Telekommunikation mehr enthält, sondern lediglich unter Telekommunikationsdienst iSd § 3 Z 21 einen Kommunikationsdienst mit Ausnahme des Rundfunks versteht.
- Überwachung (Z 1): Das Überwachen der Telekommunikation kann sich sowohl auf den Inhalt von Nachrichten beziehen (Mithören, Abhören, Aufzeichnen, Abfangen) als auch auf die Feststellung, welche Teilnehmeranschlüsse Ursprung und Ziel der Telekommunikation sind oder waren (aktive oder passive Rufdatenrückerfassung). Es geht hier also um die Ermittlung von Inhalts- und Vermittlungsdaten. Letzteren gleichgestellt werden nun auch die Standortdaten (Z 1 lit a), worunter die Feststellung des räumlichen Bereiches, in dem sich ein durch einen bestimmten Teilnehmeranschluss gekennzeichnetes Endgerät befindet oder befunden hat, verstanden wird. Diese Bestimmung zielt zwar vorwiegend auf den mobilen Sprachtelephonieverkehr ab[272], unter den Begriff Endgerät ist allerdings auch ein PC zu subsumieren.

Vgl § 3 Z 2 TKG 1997 der unter Endgerät *„eine Einrichtung, die unmittelbar an die Netzabschlußpunkte*[273] *eines öffentlichen Telekommunikationsnetzes angeschlossen werden soll oder die mit einem öffentlichen Telekommunikationsnetz zusammenarbeiten und dabei unmittelbar oder mittelbar an die Netzabschlußpunkte eines öffentlichen Telekommunikationsnetzes angeschlossen werden soll;“* versteht. § 3 Z 22 TKG 2003 kennt den Begriff der *„Telekommunikationsendeinrichtung“*, und definiert sie als *„ein die Kommunikation ermöglichendes Erzeugnis oder ein wesentlicher Bauteil davon, der für den mit jedwedem Mittel herzustellenden direkten oder indirekten Anschluss an Schnittstellen von öffentlichen Telekommunikationsnetzen bestimmt ist;“*. Die Qualifikation des PC als Endgerät stellen nunmehr auch die EB zum

---

[270] Zur Problematik der alten Rechtslage vgl *Reindl,* Die nachträgliche Offenlegung von Vermittlungsdaten des Telefonverkehrs im Strafverfahren ("Rufdatenrückerfassung"), JBl 1999, 791.

[271] Vgl *Seiler,* Strafprozeßrecht[6] Rz 374. So auch die EB zum STRÄG 2002, 1166 BlgNR XXI. GP 34, http://www.parlinkom.gv.at/pd/pm/XXI/I/texte/011/I01166__784.pdf .

[272] *Seiler* (Strafprozeßrecht[6] Rz 375) nennt sie – wohl die EB zitierend - „rufbegleitende Daten“. Zur Anwendbarkeit auf WLAN siehe bei der Beurteilung der Ausgangsfälle.

[273] Vgl § 3 Z 6 TKG 1997: *“alle physischen Verbindungen und technischen Zugangsspezifikationen, die Bestandteile des öffentlichen Telekommunikationsnetzes sind und die für den Zugang zu diesem Netz und zur effizienten Kommunikation mittels dieses Netzes erforderlich sind.“*

TKG 2003[274] zu § 92 fest (wenn auch einschränkend auf die Zwecke der elektronischen Post). Im Zusammenhang mit der Begründung einer Garantenstellung von Providern iSd § 2 StGB iVm § 75 TKG 1997 wird diese Problematik ebenfalls diskutiert. So befürworten *Reindl*[275] und *Behm*[276] die Qualifizierung eines Web-Servers als Endgerät in diesem Sinne. AA sind offenbar *Blume/Hammerl*[277] die eine Garantenstellung aufgrund der Haftungsprivilegien des § 16 Abs 1 Z 2 ECG annehmen wollen, bzw alternativ von Ingerenz ausgehen.

- Teilnehmeranschluss (Z 3): Die Adresse, welche die technische Einrichtung, die Ursprung oder Ziel einer Telekommunikation ist, kennzeichnet. § 3 Z 22 TKG 2002 definiert den Teilnehmeranschluss als *„die physische Verbindung, mit dem der Netzanschluss in den Räumlichkeiten des Teilnehmers an den Hauptverteilerknoten oder an eine gleichwertige Einrichtung im festen öffentlichen Telefonnetz verbunden wird;“*. Die EB zum STRÄG 2002 führen zu diesem Begriff aus, dass damit die in § 2 Z 2 ÜVO[278] enthaltene Umschreibung in sprachlich vereinfachter Form übernommen und sichergestellt sei, dass sämtliche technische Einrichtungen, die dem Senden, Übermitteln und Empfangen einer Telekommunikation dienen, dem Anwendungsbereich der §§ 149a bis 149c und 149m unterliegen. Es werden somit weiterhin sowohl die bei der Übertragung im Funkweg die Signale umsetzende Sendestation als auch die zur Aussendung oder zum Empfang von Nachrichten dienenden Endgeräte von diesem Begriff umfasst.[279]
- Ergebnis der Überwachung einer Telekommunikation (Z 2): Jedes durch die Telekommunikation gewonnenes Stamm-, Vermittlungs- oder Inhaltsdatum (iSd TKG). Aus dieser Formulierung ergibt sich, dass ein Stammdatum dann durch das Fernmeldegeheimnis geschützt ist, wenn es das Ergebnis einer Überwachung ist.[280]

Zusätzlich enthält § 149a Abs 4 eine Normierung des Verhältnismäßigkeitsgrundsatzes. Insbes bei Eingriffen in Rechtspositionen Dritter ist auf diesen zu achten und zu trachten, das gelindeste Mittel zu finden, um den angestrebten Erfolg zu erzielen. § 149a Abs 3 schließt die Überwachung bei entschlagungsberechtigten Personen aus bzw werden strengere Erfordernisse bei der Überwachung von Medienunternehmen bestimmt.

---

[274] aaO.

[275] E-Commerce und Strafrecht 264 f.

[276] Providerhaftung, in: *Lattenmayer/Behm,* Aktuelle Rechtsfragen des Internets (2001) 52.

[277] ECG-Kommentar 147 f.

[278] Dieser lautet *“die technische Einrichtung, die Ursprung oder Ziel der Telekommunikation ist und durch eine Adresse eindeutig gekennzeichnet ist (physikalischer Anschluss), oder die Adresse, die der Teilnehmer einem physikalischen Anschluss fallweise zuordnen kann.“*.

[279] EB zum STRÄG 2002, aaO 36.

[280] Siehe dazu schon in der Einleitung, S 14.

a) Verpflichtet

Anbieter öffentlicher Telekommunikationsdienste sind gem § 149c Abs 1 StPO und § 89 TKG 1997 verpflichtet (letzterer spricht von „Betreibern"), an der Überwachung des Fernmeldeverkehrs mitzuwirken. Wie bereits festgestellt, sind ISP grundsätzlich unter diesen Begriff zu subsumieren. Allerdings gilt die Verpflichtung, ihre Einrichtungen für die Überwachung entsprechend zu adaptieren, nur nach Maßgabe einer nach Abs 3 erlassenen Verordnung. Die entsprechende Verordnung, die ÜVO[281], definiert den Betreiber allerdings insofern abweichend, als damit nur die Betreiber konzessionspflichtiger Telekommunikationsdienste iSd § 14 TKG 1997 gemeint sind (§ 2 Z 1 ÜVO), und ISP solche Dienste – insbes Sprachtelephonie – iaR nicht erbringen.[282] ISP sind daher nur im Rahmen des § 89 Abs 2 TKG 1997 mitwirkungspflichtig, und sie müssen ihre Netze nicht entsprechend „überwachungstauglich" gestalten.[283]

Aufgrund der Änderungen durch das TKG 2003 sind einige Überlegungen anzustellen. Wie bereits in der Einleitung erwähnt, ändert sich am Betreiberbegriff des TKG selbst nichts. Höchst fraglich ist das Schicksal der ÜVO, die bislang die ISP von der Verpflichtung befreite, ihre technischen Einrichtungen entsprechend zu adaptieren. Gem § 133 Abs 10 TKG 2003 bleiben die NVO, die Verordnung über die Festlegung von Zugangskennzahlen für Notrufdienste[284], sowie die Entgeltverordnung[285], solange in Kraft bis entsprechende Verordnungen, die auf das TKG 2003 gestützt werden, erlassen werden. Diese Bestimmung wäre nach allgemein hA nicht notwendig, bleiben doch Verordnungen auch bei Änderung des Gesetzes so lange in Kraft als sie darin noch Deckung finden oder ihnen formell derogiert wird.[286] Einen Sonderfall stellt die Herzog-Mantel-Theorie[287] dar. Diese kommt zum Tragen, wenn die gesetzliche Grundlage der Verordnung ersatzlos gestrichen wird.[288] ME kann aus § 133 Abs 10 TKG 2003 nicht *e-contrario* auf eine formelle Derogation aller übrigen Verordnungen geschlossen werden, und bietet § 94 Abs 1 TKG 2003 eine ausreichende

---

[281] Siehe schon in der Einleitung, S 21.

[282] Vgl auch *Otto/Parschalk,* Anzeige- und Konzessionspflicht von Internet Service Providern nach dem TKG, MR 2001, 420.

[283] Vgl auch *Brenn,* ECG 301; *Ebensperger,* Die Verbreitung von NS-Gedankengut im Internet und ihre strafrechtlichen Auswirkungen unter besonderer Berücksichtigung des E-Commerce-Gesetzes, ÖJZ 2002, 132.

[284] BGBl II Nr 278/1999.

[285] BGBl II Nr 158/1999.

[286] *Raschauer,* Allgemeines Verwaltungsrecht (1998) Rz 843.

[287] Diese Bezeichnung entstammt dem internen Sprachgebrauch des VfGH (*Raschauer,* Allgemeines Verwaltungsrecht aaO):*„Wenn der Herzog fällt, muss auch der Mantel fallen"* (vgl *Neisser/Schantl/Welan,* ÖJZ 1974, 365. Im *Schiller'*schen Original (Die Verschwörung des Fiesko in Genua. Ein republikanisches Trauerspiel, 1783, 5. Aufzug, 16. Auftritt) heißt es: *"Fiesko: ‚Was zerrst du mich so am Mantel?' – er fällt! – Verrina (mit fürchterlichem Hohn: 'Nun wenn der Purpur fällt, muß auch der Herzog nach!' (Er stürzt ins Meer)."* (zitiert nach: Schillers sämtlicher Werke, 1. Band, Stuttgart 1879, J. G. Cotta'sche Buchhandlung).

[288] Beispiele finden sich bei *Raschauer,* Allgemeines Verwaltungsrecht Rz 845.

gesetzliche Grundlage für die ÜVO. Diese ist nunmehr sinngemäß anzuwenden. Wie bereits erwähnt, versteht die ÜVO den Betreiber als denjenigen, *„der einen konzessionspflichtigen Dienst gemäß § 14 TKG erbringt und in dessen Netz physikalische Teilnehmeranschlüsse vorhanden sind;“*. Das TKG 2003 kennt aber keine konzessionspflichtigen Dienste mehr. Nach § 14 TKG 1997 waren konzessionspflichtig: die Erbringung von öffentlichen mobilen und festen Sprachtelephoniediensten und das Anbieten von öffentlichen Mietleitungen mittels selbst betriebener Netze. Es ist davon auszugehen, dass weiterhin nur Betreiber dieser Dienste gem § 94 Abs 1 TKG 2003 verpflichtet sind, da die ÜVO ISP offenbar nicht erfassen wollte.

b) Berechtigt

Bei Gefahr in Verzug, mit Zustimmung des Anschlussinhabers oder bei der Ermittlung von Vermittlungs- bzw Standortdaten ist gem § 149b Abs 1 ein Beschluss des Untersuchungsrichters ausreichend. Sollen Inhaltsdaten überwacht werden, ist die Ratskammer zuständig. Wird die Überwachung wegen Gefahr in Verzug angeordnet, so ist der Beschluss der Ratskammer unverzüglich zur Genehmigung vorzulegen.

c) Voraussetzungen der Überwachung

aa) Materielle Voraussetzungen

Gem § 149a Abs 2 ist die Überwachung in folgenden Fällen zulässig:

Z 1. Jegliche Art von Daten mit Zustimmung des Anschlussinhabers, wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen, mit mehr als sechsmonatiger Freiheitsstrafe bedrohten strafbaren Handlung gefördert werden kann.[289]

Z 2. Vermittlungsdaten und Standortdaten: Es soll die Aufklärung einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung im Hinblick auf die Ermittlung von Daten des Verdächtigen gefördert werden. Der zu überwachende Anschluss muss nicht jener des Tatverdächtigen sein.[290]

Z 3. Inhaltsdaten: Die Überwachung muss zur Aufklärung einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung erforderlich erscheinen. Ergänzend muss eine der beiden Voraussetzungen vorliegen:

[289] Die Überwachung ist daher auch mit Zustimmung des Anschlussinhabers jedenfalls ausgeschlossen zB bei Ehrendelikten (§§ 111 ff StGB), beim Großteil der Indiskretionsdelikte (§ 118 ff StGB, hierzu gehören auch die „Computerdelikte“), bei nicht qualifizierten Vermögensdelikten und beim Besitz von kinderpornographischen Materials (§ 207a Abs 3 StGB).

[290] *Seiler,* Strafprozessrecht[6] Rz 378.

lit a. Der Inhaber des Teilnehmeranschlusses ist selbst dringend verdächtig[291], die Tat begangen zu haben.

lit b. Es liegen Gründe für die Annahme vor, dass eine der Tat dringend verdächtige Person den Teilnehmeranschluss benützen oder eine Verbindung mit ihm herstellen wird. Dies betrifft daher auch Anschlüsse, deren Inhaber nicht der Verdächtige ist.

Man beachte den Unterschied zwischen Z 1 bzw Z 2 und Z 3: Liegt die Zustimmung des Anschlussinhabers vor oder geht es – ohne Zustimmung – um Vermittlungs- oder Standortdaten, so reicht die Erwartung, dass die Aufklärung der strafbaren Handlung gefördert werden wird. Geht es um die Ermittlung von Inhaltsdaten, so muss die Überwachung für diese Zwecke erforderlich erscheinen.

bb) Formelle Voraussetzungen

Zu den zuständigen Organen siehe bereits oben, S 60. Der Überwachungsbeschluss hat gem § 149b Abs 2 zu enthalten:

Den Namen des Beschuldigten, die Tat, deren er verdächtig ist, und ihre gesetzliche Bezeichnung; den Namen des Inhabers des Teilnehmeranschlusses und dessen Bezeichnung; den Zeitpunkt des Beginns und der Beendigung der Überwachung; die Tatsachen, aus denen sich die Erforderlichkeit und Verhältnismäßigkeit der Überwachung ergibt; die Tatsachen, aus denen sich der Tatverdacht ergibt.

Da auch der Name des Beschuldigten anzugeben ist, würde dies prima-facie ausschließen, dass bspw eine Standortanpeilung von einem noch unbekannten Täter angeordnet wird, von dem allerdings eine Handynummer bekannt ist. Handelt es sich um ein Wertkarten-Mobiltelephon, so wird auch eine Anfrage beim Netzbetreiber keinen Namen liefern. Die Bestimmungen über die Überwachung zielen aber auch darauf ab, die Identität des Verdächtigen zu ermitteln. Der Name des Beschuldigten ist daher nur anzugeben, wenn er bekannt ist.

d) Inhalt

Siehe oben, S 60.

e) Kostenersatz

Wie bereits erwähnt, gebührt den Betreibern für die Mitwirkung an der Überwachung gem § 89 Abs 2 TKG 1997 ein angemessenes Entgelt.[292] Das

[291] Vgl § 180 Abs 1 StPO. Dringender Tatverdacht liegt vor, wenn der Beschuldigte mit hoher Wahrscheinlichkeit der Täter ist und als solcher auch überführt werden kann (siehe *Bertel/Venier,* Strafprozessrecht[7] (2002) Rz 402).

[292] Die Bestimmung der Höhe dieses Entgelts ist in praxi höchst problematisch, auch weil die Kosten von Betreiber zu Betreiber – je nach Netzkonfiguration – variieren können. Veröffentliche Judikatur hierzu existiert allerdings kaum. Vgl OGH

TKG 2003 enthält nunmehr eine Verordnungsermächtigung für den BMJ, der im Einvernehmen mit dem BMVIT, dem BMF, dem BMI und dem BMLV, durch Verordnung einen angemessenen Kostenersatz vorsehen kann, wobei insbesondere auf die wirtschaftliche Zumutbarkeit des Aufwandes, auf ein allfälliges Interesse des betroffenen Unternehmers an den zu erbringenden Leistungen und auf eine allfällige durch die gebotenen technischen Möglichkeiten bewirkte Gefährdung, der durch die verlangte Mitwirkung entgegengewirkt werden soll, Bedacht zu nehmen ist.

f) Sonstiges

Die StPO ermöglicht zwar weitreichende Eingriffe in das Fernmeldegeheimnis, enthält aber keine explizite Regelung betreffend den Stammdaten eines Verdächtigen, obwohl es reichlich Verfahren gegen unbekannte Täter gibt. Es ist wohl davon auszugehen, dass jedenfalls § 143 iVm § 18 Abs 2 ECG eine taugliche Rechtsgrundlage bieten.[293]

Gem § 149c Abs 1 ist dem Betreiber mittels Beschluss eine Geheimhaltungsverpflichtung betreffend der mit der gerichtlichen Anordnungen verbundenen Tatsachen und Vorgänge gegenüber Kunden und Dritten aufzuerlegen.

C. Weitere Auskunftspflichten nach dem TKG 2003

Das TKG 2003 enthält noch eine Reihe weiterer Auskunftspflichten von Betreibern öffentlicher Kommunikationsdienste.[294]

- § 90 Abs 6: *„Betreiber von Kommunikationsdiensten sind verpflichtet, Verwaltungsbehörden auf deren schriftliches und begründetes Verlangen Auskunft über Stammdaten im Sinn von § 92 Abs. 3 Z 3 lit. a bis e von Teilnehmern zu geben, die in Verdacht stehen, durch eine über ein öffentliches Telekommunikationsnetz gesetzte Handlung eine Verwaltungsübertretung begangen zu haben.“* Die EB[295] zu § 90 merken hierzu an, dass dieses Auskunftsrecht für die Zwecke von Verwaltungsstrafverfahrens notwendig ist. Den Verwaltungsstrafbehörden steht daher in Ergänzung zu § 18 Abs 3 ECG auch ein Auskunftsrecht gegenüber Access-Providern zu. Zur Bestimmung des Inhaltes der Auskunft wird auf die Stammdaten verwiesen.[296] E-Mail Adressen sind daher seit dem TKG 2003 zu beauskunften. Die Identifikation des

18.5.1998, 15 Os 40/98; OGH 22.5.2001, 14 Os 40/01; OLG Innsbruck 3.3.1998, 6 Bs 27/98; OLG Innsbruck 13.10.1998, 6 Bs 219/98; OLG Wien 9.6.2001, 21 Bs 226/01.

[293] Von der Zulässigkeit eines solchen Ersuchens geht offenbar auch § 96 Abs 7 TKG 1997 bzw § 103 Abs 4 TKG 2003 aus. Siehe hierzu schon oben im Kapitel E-Commerce-Gesetz, S 32 f, bzw bei der Beurteilung der Ausgangsfälle, 85 f.

[294] Auf die Darstellung weiterer Auskunftspflichten nach dem TKG 1997 wird verzichtet, ebenso wie auf die Auskünfte im Rahmen der Teilnehmerverzeichnisse und gegenüber der Regulierungsbehörde.

[295] aaO 17.

[296] Hierzu siehe in der Einleitung, S 8.

Teilnehmers kann anhand einer (statischen) IP-Adresse oder E-Mail Adresse erfolgen.

- § 96 Abs 3 betrifft die Informationspflicht von Betreibern über die Dauer der Speicherung von Kundendaten etc.
- § 98 gewährt den Betreibern von Notrufdiensten ein Auskunftsrecht in Notfällen. Laut EB wurde auf die Definition des Notrufdienstes verzichtet, man versteht darunter *„Einrichtungen, die mit der Abwehr unmittelbarer Gefahren für Leib, Leben, Gesundheit und Eigentum von Menschen befasst sind."* Diesen Betreibern sind auf Verlangen Auskünfte über Stammdaten iSv § 92 Abs 3 Z 3 lit a bis d sowie über Standortdaten iSd § 92 Abs 3 Z 6 zu erteilen. Voraussetzung für ein solches Begehren ist ein Notfall, der nur durch Bekanntgabe dieser Informationen abgewehrt werden kann. Die Notwendigkeit der Informationsübermittlung ist vom Betreiber des Notrufdiensten zu dokumentieren und dem Auskunftsverpflichteten, unverzüglich oder spätestens binnen 24 Stunden, nachzureichen. Die Darlegung der Notfallsituation ist jedoch keine Voraussetzung für die Informationsübermittlung selbst. Das Risiko der Fehleinschätzung einer solchen Notlage trifft ausschließlich den Betreiber des Notrufdienstes. Die EB[297] führen aus, dass die Entsprechung eines glaubhaften Übermittlungsersuchens durch den Auskunftsverpflichteten dieser im Falle eines missbräuchlichen Ersuchens von der Verantwortung befreit ist.

D. Durchsetzung, Sanktionen und Rechtsfolgen

Nach alter Rechtslage war ein Verstoß gegen die Mitwirkungspflichten nach § 89 Abs 2 TKG 1997 verwaltungsstrafrechtlich nicht sanktioniert.[298] § 109 Abs 3 Z 14 TKG 2003 bedroht nunmehr die Verweigerung der erforderlichen Mitwirkung nach § 94 Abs 2 TKG 2003 mit Verwaltungsstrafe mit bis zu Euro 8.000. Nach alter Rechtslage war auch allenfalls ein Konzessionsentzug durch die Regulierungsbehörde nach § 23 Abs 3 S 2 Fall 1 TKG 1997 denkbar. Aufgrund der Tatsache, dass die wenigsten ISP konzessionspflichtig iSd § 14 TKG 1997 waren, kam dieser Sanktion wohl wenig Praxisrelevanz zu. Eine gerichtliche Strafbarkeit wegen Begünstigung von Straftätern gem § 299 StGB wäre bei Verweigerung der Mitwirkung bei der Strafverfolgung denkbar.

Gegen Beschlüsse des Untersuchungsrichters (zB Anordnung der Fernmeldeüberwachung, Bestimmung des Kostenersatzes) kann sich der Betreiber gem § 113 StPO bei der Ratskammer beschweren.[299] Die Beschwerden haben allerdings keine aufschiebende Wirkung.

Ist der Betreiber gleichzeitig Inhaber des Anschlusses, so kann er sich jedenfalls auch gem § 149b Abs 6 an das OLG wenden, und sich gegen die

[297] aaO 18.

[298] § 104 Abs 3 Z 20 TKG 1997 stellt allerdings § 89 Abs 1 TKG 1997 unter Verwaltungsstrafdrohung. Nach dem TKG 2003 ist dies ebenso (§ 94 Abs 2 iVm § 109 Abs 4 Z 7).

[299] Vgl auch den Erlass des BMJ v 26.7.2002, JMZ 318015/43/II1/02.

Anordnung der Überwachung wehren. Zu den weiteren Konsequenzen wie Verlust des Haftungsprivilegs, siehe schon im Kapitel E-Commerce-Gesetz, S 39.

Gem § 109 Abs 3 Z 13 TKG 2003 ist die Verweigerung der Auskunft nach § 90 Abs 6 mit Verwaltungsstrafe mit bis zu Euro 37.000 bedroht. Gem Z 17 leg cit ist die Verweigerung der Auskunft an Betreiber von Notrufdiensten gem § 98 TKG 2003 gleichfalls verwaltungsstrafbewehrt.

E. Ausblick

1. Strafreformprozessgesetz

Der Entwurf zu einer umfassenden Reform des Vorverfahrens der StPO wurde bereits in der XXI. Gesetzgebungsperiode eingebracht, und absolvierte das Begutachtungsverfahren. Das Strafreformprozessgesetz ereilte allerdings das gleiche Schicksal wie die UrhG-Nov und des neuen TKG: Durch die vorzeitige Beendigung der Legislaturperiode im Herbst 2002 wurde die weitere parlamentarische Behandlung verhindert. Der Entwurf wurde daher in der XXII. Gesetzgebungsperiode fast unverändert eingebracht.[300] Er wurde dem Unterausschuss des Justizausschusses betreffend Strafprozessreformgesetz 25 dB vom 5. Juni 2003, zugewiesen.[301]

2. Convention on Cyber-Crime

Die Convention on Cyber-Crime (CCC)[302] des Europarats wurde am 23.11.2001 in Budapest beschlossen und zur Unterzeichnung aufgelegt.

---

[300] Vgl die Kurzfassung der Parlamentskorrespondenz, http://www.parlinkom.gv.at/pd/pk/2003/PK0177.html. Der Entwurf, die EB und die Protokolle der Beratungen des Unterausschusses sind abrufbar unter: http://www.parlinkom.gv.at/pd/pm/XXII/I/his/000/I00025_.html . Die eingelangten Stellungnahmen im Rahmen des Begutachtungsverfahren sind abrufbar unter: http://www.parlinkom.gv.at/pd/pm/XXI/ME/his/002/ME00214_.html .

[301] Allgemeines zur Reform des Vorverfahrens: *Machacek,* Die Reform des StPO-Vorverfahrens aus der Sicht des Rechtsschutzbeauftragten - Erweiterte Fassung der dem BMJ am 14. 9. 2001 erstatteten Stellungnahme des RSB, AnwBl 2002, 76; *Demmelbauer/Hauer*, Sicherheitsrecht Rz 212. Siehe auch schon *Reindl,* Telefonüberwachung zweimal neu?, JBl 2002, 69. Vgl die Hinweise unten bei der CCC, S 64.

[302] Convention on Cybercrime, ETS No: 185. Der englische und französische Volltext einschließlich des *Explanatory Reports* und anderer Dokumente finden sich unter: : http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185&CM=8&DF=28/08/03 . Ferner existiert noch ein Zusatzprotokoll betreffend rassistischer und fremdenfeindlicher Handlungen die durch Computersysteme begangen werden, aufgelegt zur Unterzeichnung in Straßburg am 23.1.2003: Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS No: 189, http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=189&CM=8&DF=28/08/03 .

Bislang haben 30 Staaten, darunter auch Österreich, die Konvention unterschrieben. Ratifiziert wurde die Konvention bisher nur von Albanien, Kroatien und Estland. Der materiellrechtliche Abschnitt und manche prozessrechtliche Bestimmungen wurden in Österreich zT durch das STRÄG 2002 umgesetzt. Der übrige prozessrechtliche Teil soll im Strafreformprozessgesetz umgesetzt werden[303], weshalb dieser im Folgenden kurz dargestellt wird.[304]

Traditionelle Eingriffsbefugnisse enthalten Art 19 (Durchsuchung und Beschlagnahme gespeicherter Daten), Art 20 und Art 21 (Aufzeichnung von Übertragungsdaten und Überwachung von Kommunikationsinhalten in Echtzeit). § 111 Abs 2 des Entw zum Strafreformprozessgesetz ermöglicht in Umsetzung des Art 19 die Durchsuchung und Beschlagnahme von auf Datenträgern gespeicherter Information sowie die Anfertigung und Ausfolgung von Kopien und Herstellung einer Sicherheitskopie. Die Art 20 und 21 fanden bereits im STRÄG 2002 bzw in der ÜVO ihre Umsetzung.

Neben den bereits erwähnten Befugnissen, enthält die CCC auch gelindere Mittel, die weniger eingriffsintensiv sind als Durchsuchung, Beschlagnahme und Überwachung. So sieht Art 16 die Einstweilige Sicherung gespeicherter Daten zu Beweiszwecken durch den Verfügungsberechtigten vor (*production order)*, zB durch den Host-Provider. Ergänzend enthält Art 17 Sonderbestimmungen für Übertragungsdaten. Der Entw zum Strafreformprozessgesetz sieht bislang keine Umsetzung dieser Bestimmungen vor. Nach Art 18 ist die Möglichkeit vorgesehen, Aufträge an unbeteiligte Dritte, einschließlich Provider, zur Herausgabe von Daten, zu erteilen. Bei den Daten handelt es sich um *subscriber information,* was im Wesentlichen dem österreichischen Verständnis von Stammdaten entspricht. Explizite Umsetzung gibt es noch keine, das Herausgabeverlangen solcher Informationen wird von Gerichten auf § 143 StPO gestützt (siehe dazu im Kapitel E-Commerce-Gesetz, S 32 und bei der Beurteilung der Ausgangsfälle, S 85).

---

303 Vgl auch: Was wurde aus dem Cybercrime-Abkommen?, ARGE-Daten, http://www.argedaten.at/news/20030422.html .

304 Die Darstellung orientiert sich an *Zeder,* Internet und Strafrecht, in: *Studiengesellschaft für Wirtschaft und Recht* (Hrsg), Internet und Recht – Rechtsfragen von E-Commerce und E-Government (2002) 102 ff. *Zeder* geht allerdings noch vom älteren Entwurf zum Strafreformprozessgesetz aus. Näheres auch bei *Primig,* Verfahrensrechtliche Regelungsversuche der Telekommunikationsüberwachung auf europäischer Ebene (2002), http://www.rechtsprobleme.at/doks/primig-2-telekom-ueberwachung_europaeisch.pdf , 53 ff .

VI. Sicherheitspolizeigesetz

Im Hinblick auf die im SPG[305] normierten Auskunfts- und Mitwirkungspflichten, werden im Folgenden auch Anwendungsbereich, Aufgaben und Befugnisse der Sicherheitsbehörden dargestellt. Von besonderer Bedeutung für ISP ist die Bestimmung des § 53 Abs 3a. Die Darstellung der Aufgaben ist ferner für die Auskunftspflichten nach ECG relevant, denn den Verwaltungsbehörden stehen die Auskunftsrechte nur im Rahmen der ihnen übertragenen Zuständigkeiten zu. Das ECG und das SPG kommen nebeneinander zur Anwendung.

A. Allgemeines

1. Anwendungsbereich und Aufgaben

Das SPG regelt die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei. Die Sicherheitspolizei ist ein Aufgabengebiet der Sicherheitsverwaltung und dient der Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit, und der Leistung der ersten allgemeinen Hilfeleistungspflicht (§§ 2 und 3). Diese Befugnisse werden auch häufig unter dem Begriff „Gefahrenabwehr" zusammengefasst.[306] Die Sicherheitsbehörden nehmen allerdings im Dienste der Strafjustiz auch Aufgaben wahr (Kriminalpolizei). Sie sind dann Justizorgane im funktionellen Sinn und unterliegen den Bestimmungen der StPO.[307]

a) Die Aufrechterhaltung der öffentlichen Sicherheit

Unter öffentlicher Sicherheit wird die Sicherheit des Staates, von Personen (Leben, körperliche Integrität, Gesundheit, Freiheit, Ehre) sowie von Sachgütern verstanden.[308] Gem § 20 umfasst sie die Gefahrenerforschung, Gefahrenabwehr, den vorbeugenden Schutz von Rechtsgütern, die Fahndung, die kriminalpolizeiliche Beratung und die Streitschlichtung.

aa) Gefahrenerforschung

§ 20 Abs 4 definiert die Gefahrenerforschung als die Festestellung einer Gefahrenquelle und des für die Abwehr einer Gefahr sonst maßgeblichen

[305] BG über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz - SPG), StF: BGBl 566/1991 idF BGBl I 104/2002.

[306] Und sind demnach von der Strafverfolgung durch die Justizbehörden abzugrenzen, siehe schon im Kapitel E-Commerce-Gesetz, S 32; vgl *Demmelbauer/Hauer,* Sicherheitsrecht Rz 1, 110.

[307] *Demmelbauer/Hauer,* Sicherheitsrecht Rz 211.

[308] *Demmelbauer/Hauer,* aaO.

Sachverhaltes. Die Annahme einer Gefahrensituation muss durch bestimmte Tatsachen gerechtfertigt sein. Die Erfüllung dieser Aufgabe erfolgt primär durch Informationssammlung (§ 53 Auskunftsrecht, § 34 Auskunftsverlangen). Den Sicherheitsbehörden obliegt auch die erweiterte Gefahrenerforschung gem § 21 Abs 3, die auf die Aushebung von extremistischen Gruppen abzielt.[309]

bb) Abwehr allgemeiner Gefahren

Gem § 16 Abs 1 liegt eine allgemeine Gefahr bei einem gefährlichen Angriff oder einer kriminellen Verbindung vor. Unter gefährlichem Angriff iSd § 16 Abs 2 ist die Bedrohung eines Rechtsgutes durch die Begehung einer gerichtlich strafbaren Vorsatztat nach der StPO, dem SMG oder dem VerbotsG, die von Amts wegen zu verfolgen ist (Offizialdelikt), zu verstehen. Abs 3 leg cit ergänzt diese Definition und bestimmt, dass auch ein Verhalten, das darauf abzielt und geeignet ist, eine Bedrohung iSd Abs 2 vorzubereiten, als gefährlicher Angriff zu verstehen ist.[310]

Eine kriminelle Verbindung ist gem § 16 Abs 1 Z 2 die Verbindung von drei oder mehr Menschen, mit dem Vorsatz, fortgesetzt gerichtlich strafbare Handlungen zu begehen.

cc) Der vorbeugende Schutz von Rechtsgütern

Unter diese Bestimmung fällt insbes die Verpflichtung der Sicherheitsbehörden, nach einem gefährlichen Angriff – unbeschadet der Aufgaben nach der StPO – die maßgeblichen Umstände, einschließlich der Identität des dafür Verantwortlichen zu klären, soweit dies für die Gefahrenabwehr (Prävention) erforderlich ist (Abs 3).[311]

dd) Fahndung

Den Sicherheitsbehörden obliegt gem § 24 auch die Ermittlung des Aufenthaltsortes eines Menschen, nach dem gesucht wird, und zwar wenn gegen ihn ein aufrechter Haftbefehl besteht, jemand vermisst wird, nach einem psychisch Behinderten gesucht wird oder wenn ein Minderjähriger abgängig ist.

b) Die öffentliche Ordnung und Ruhe

Die öffentliche Ordnung ist die Summe der öffentlich-rechtlichen Rechtsordnung und jener ungeschriebenen Regeln, *„deren Befolgung nach allgemeiner Auffassung unentbehrliche Voraussetzung für ein gedeihliches*

[309] Vgl *Demmelbauer/Hauer*, Sicherheitsrecht Rz 118 f.

[310] Mithin bildet nicht nur der Versuch einen gefährlichen Angriff, sondern uU auch schon Vorbereitungshandlungen, vgl *Demmelbauer/Hauer*, Sicherheitsrecht Rz 121.

[311] MwH: *Demmelbauer/Hauer*, Sicherheitsrecht Rz 123 ff.

Zusammenleben der Menschen ist."[312] Die öffentliche Ruhe hat in diesem Zusammenhang keine eigenständige Bedeutung.[313]

c) Die erste allgemeine Hilfeleistungspflicht

Gem § 19 trifft die Sicherheitsbehörden die Leistung der ersten allgemeinen Hilfeleistungspflicht, worunter die gegenwärtige bzw unmittelbar bevorstehende Gefährdung von Leben, Gesundheit, Freiheit oder Eigentum von Menschen fällt, soweit es sich um Sachverhalte handelt, für welche die Verwaltungsbehörden oder die Feuerpolizei zuständig sind bzw die Gefährdung zum Hilfs- und Rettungswesen gehört.
Diese Verpflichtung ist vor dem Hintergrund zu sehen, dass vielfach die Sicherheitsbehörden als erste Behörde von solcherlei Sachverhalten Kenntnis erlangen und damit oft schneller eingreifen können, als die zuständigen Verwaltungsbehörden.[314]

2. Sicherheitsbehörden

Die Sicherheitsverwaltung wird gem § 4 vom Bundesminister für Inneres (bzw der Generaldirektion für die öffentliche Sicherheit) als oberste Sicherheitsbehörde besorgt. Ihm unmittelbar unterstellt sind die neun Sicherheitsdirektionen, diesen nachgeordnet die Bezirksverwaltungsbehörden (Gendarmerie) und Bundespolizeidirektionen.[315]

Der im SPG häufig vorkommende Begriff des Organs des öffentlichen Sicherheitsdienstes bestimmt sich nach § 5 Abs 2. Hierzu gehören Angehörige der Bundesgendarmerie, der Bundessicherheitswachekorps, der Kriminalbeamtenkorps, der Gemeindewachkörper sowie des rechtskundigen Dienstes bei den Sicherheitsbehörden, wenn diese Organe zur Ausübung unmittelbarer Befehls- und Zwangsgewalt ermächtigt sind. Gem § 5 Abs 1 versehen diese Organe den Exekutivdienst der Sicherheitsbehörden.

B. Besondere Befugnisse

Das SPG gibt den Sicherheitsbehörden bzw ihren Organen zur Erfüllung der obengenannten Aufgaben diverse Befugnisse in die Hand.[316] Es unterscheidet in allgemeine und besondere Befugnisse. Die allgemeinen Befugnisse werden in den §§ 32 und 33 geregelt und betreffen die erste allgemeine Hilfeleistungspflicht und die Beendigung gefährlicher Angriffe. Die §§ 34 bis 48 normieren besondere Befugnisse, wobei im Hinblick auf mögliche Auskunfts- und Mitwirkungspflichten insbes von Interesse sind: Auskunftsverlangen (§ 34), Identitätsfeststellung (§ 35), Betreten und Durchsuchen von Grundstücken, Räumen und Fahrzeugen (§ 39),

[312] *Demmelbauer/Hauer,* Rz 132.
[313] *Demmelbauer/Hauer,* Rz 1.
[314] Vgl *Demmelbauer/Hauer*, Sicherheitsrecht Rz 130 f.
[315] Näheres zur Organisation der Polizeiverwaltung vgl *Demmelbauer/Hauer,* Sicherheitsrecht Rz 15 ff.
[316] *Demmelbauer/Hauer*, Sicherheitsrecht Rz 135.

Sicherstellung von Sachen (§ 42), Ermittlung und Verarbeitung personenbezogener Daten (§ 53). Im Folgenden wird der von *Demmelbauer/Hauer*[317] vorgeschlagenen Systematik gefolgt.

1. Informationssammlung

a) Auskunftsverlangen (§ 34)

> *„Die Organe des öffentlichen Sicherheitsdienstes sind ermächtigt, von Menschen Auskunft zu verlangen, von denen anzunehmen ist, sie könnten in Fällen der ersten allgemeinen Hilfeleistungspflicht sachdienliche Hinweise über das Vorliegen einer Gefährdung und über die Gefahrenquelle geben. Die Ausübung von Zwangsgewalt zur Durchsetzung dieser Befugnis ist unzulässig."*

Zu ergänzen ist, dass die Auskunft wahrheitsgemäß zu erfolgen hat und die Verweigerung der Auskunft nicht sanktioniert ist.[318] Die Anwendbarkeit dieser Vorschrift auf ISP ist insofern fraglich, als diese selten sachdienliche Hinweise über das Vorliegen einer Gefährdung bzw die Gefahrenquelle iSd Bestimmung werden geben können.

b) Identitätsfeststellung (§ 35)

Diese Bestimmung bezieht sich auf die Identitätsfeststellung in Anwesenheit der betroffenen Person (zB mutmaßlicher Täter, Opfer oder Zeuge)[319], und ist in diesem Zusammenhang nicht weiters relevant.

c) Polizeiliche Datenverwendung (§ 53)

Das SPG enthält in seinem 4. Teil Bestimmungen über die Verwendung personenbezogener Daten im Rahmen der Sicherheitspolizei. Es handelt sich hier um Sonderdatenschutzrecht für die Verwendung personenbezogener Daten zu sicherheits-, insbes staatspolizeilichen, Zwecken. Das DSG 2000 bleibt hiervon unberührt, soweit nicht ausdrücklich das Gegenteil angeordnet wird. (§ 51 Abs 2).[320]

§ 53 Abs 1 regelt die Zulässigkeit der Ermittlung, Verarbeitung und Übermittlung personenbezogener Daten. So dürfen diese nach Abs 1 nur für die Erfüllung nachstehender Aufgaben ermittelt[321] und weiterverarbeitet werden:

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

---

317 Sicherheitsrecht Rz 145.

318 Vgl *Demmelbauer/Hauer*, Sicherheitsrecht Rz 146. Dort heißt es auch ohne nähere Erläuterungen, dass die Auskunftsverweigerung schadenersatzrechtliche Konsequenzen bewirken kann.

319 Vgl *Demmelbauer/Hauer*, Sicherheitsrecht Rz 147.

320 Vgl *Demmelbauer/Hauer*, Sicherheitsrecht Rz 173.

321 Vgl § 4 Z 10 DSG: *"das Erheben von Daten in der Absicht, sie in einer Datenanwendung zu verwenden."*

Z 2. für die Abwehr krimineller Verbindungen (§§ 16 Abs 1 Z 2 und 21);

Z 2a. für die erweiterte Gefahrenerforschung (§ 21 Abs 3), jedoch unter Beteiligung des Rechtsschutzbeauftragten.

Z 3. für die Abwehr gefährlicher Angriffe (§§ 16 Abs 2 und 3 sowie 21 Abs 2);

Z 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;

Z 5. für Zwecke der Fahndung (§ 24);

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

Die Abs 2, 3 und 4 des § 53 beziehen sich auf die Ermittlung von Daten aus eigenen Datenbeständen, via Auskunftsersuchen im Rahmen der Amtshilfe und aus öffentlich zugänglichen Registern.[322] Abs 3a[323] normiert eine Auskunftspflicht von Betreibern öffentlicher Telekommunikationsdienste. Diese Bestimmung wurde 1999 eingeführt, um auch nach der Privatisierung der PTV eine Grundlage für Auskünfte über Telephonnummern und Anschlüsse, dh Stammdaten, zu erhalten. Stellen, die über Stamm- oder Vermittlungsdaten verfügen, sind dazu verpflichtet, den Sicherheitsbehörden diese Daten auszuhändigen. Laut den EB[324] stelle der Zugriff auf diese Daten keinen Eingriff in das Fernmeldegeheimnis gem Art 10a StGG dar. Der Gesetzgeber übersieht allerdings, dass § 53 Abs 3a S 2 („kleine passive Rufdatenrückerfassung“) die Ermittlung von Vermittlungsdaten gestattet, und daher einen Eingriff in Art 8 EMRK darstellt.[325]

aa) Auskunftspflicht nach § 53 Abs 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

322 Näheres hierzu siehe: *Demmelbauer/Hauer*, Sicherheitsrecht Rz 175; *Trawnicek/Lepuschitz,* Sicherheitspolizeigesetz[3] (2000) 238.

323 Eingefügt durch die SPG-Nov 1999, BGBl I 146/1999.

324 Erläuternde Bemerkungen zum SPG bzw zur SPG-Nov 1999, abgedruckt in: *Trawnicek/Lepuschitz,* Sicherheitspolizeigesetz[3] 238.

325 Vgl *Berka,* Lehrbuch Grundrechte (2000) 113. Dies offensichtlich verkennend: *Hauper/Keplinger,* Sicherheitspolizeigesetz[2] (2001) 472. Siehe dazu schon in der Einleitung, S 13 ff.

passiven Teilnehmernummer erfolgen. Die ersuchte Stelle ist verpflichtet, die Auskunft unverzüglich und kostenlos zu erteilen."

(1) Auskunftsverpflichtet

Zur Auskunft sind Betreiber öffentlicher Telekommunikationsdienste verpflichtet.

(2) Auskunftsberechtigt

Sicherheitsbehörden (aber nicht schlichte Organe des öffentlichen Sicherheitsdienstes) sind zur Stellung dieser Auskunftsverlangen befugt.

(3) Voraussetzungen

Die verlangten Daten müssen eine wesentliche Voraussetzung für die Erfüllung der den Sicherheitsbehörden übertragenen Aufgaben sein. Das Erfordernis der wesentlichen Voraussetzung ist nicht iS einer *condition sine qua non* zu verstehen, sondern als wesentliche Erleichterung des Verwaltungshandelns.[326] Bestimmte Stammdaten dürfen daher unbeschränkt zur Erfüllung aller der oben genannten Aufgaben erhoben werden. Soll eine „kleine passive Rufdatenrückerfassung" durchgeführt werden (dazu im Folgenden), ist diese auf die erste allgemeine Hilfeleistungspflicht und die Abwehr gefährlicher Angriffe beschränkt.

(4) Inhalt

Der Betreiber hat Name, Anschrift und Teilnehmernummer eines bestimmten Anschlusses bekannt zugeben. Ferner ist aber auch eine sog „kleine passive Rufdatenrückerfassung" zulässig[327]: Im Rahmen der ersten allgemeinen Hilfeleistungspflicht und der Abwehr gefährlicher Angriffe kann von der auskunftswerbenden Stelle auch schlicht bekannt gegeben werden, dass zu einem bestimmten anderen Anschluss zu einem gegebenen Zeitpunkt telephoniert worden ist. Unter Anschluss sind Telephon- und andere Fernmeldeanschlüsse zu verstehen.[328]

Der Erlass des BMI[329] präzisiert die den Sicherheitsbehörden offenstehenden Informationen:

- Auskünfte nach § 53 Abs 3a S 1:
  - Bekanntgabe einer Person um ihre Teilnehmernummer(n) zu erfahren.

---

[326] *Hauper/Keplinger* (Sicherheitspolizeigesetz[2] 471) ziehen für die Erläuterung dieses Begriffes die Spruchpraxis der DSK zu § 7 Abs 2 DSG heran. Siehe auch schon oben in der Einleitung, S 19.

[327] Zur Verfassungskonformität dieser Bestimmung siehe *Wiederin* in: *Korinek/Holoubek* StGG Art 10a Rz 17; *Hauper/Keplinger,* Sicherheitspolizeigesetz[2] 472.

[328] Vgl *Demmelbauer/Hauer,* Sicherheitsrecht Rz 176.

[329] Erlass des BMI vom 21.12.1999, Zl 61.183/279-II/20/99, zitiert bei *Hauper/Keplinger,* Sicherheitspolizeigesetz[2] 467.

  - Bekanntgabe einer Teilnehmernummer um den Namen der Person und der Anschrift des Inhabers dieses Anschlusses zu erfahren.
- Auskünfte nach § 53 Abs 3a S 2:
  - Bekanntgabe des Zeitpunkts und der passiven Teilnehmernummer einer Verbindung, um die entsprechende aktive Teilnehmernummer und den Inhaber dieses Anschlusses zu erfahren.

Wie ist diese Bestimmung nun auf ISP anzuwenden? Den Sicherheitsbehörden wird iaR lediglich eine IP-Adresse bekannt sein (allenfalls auch ein Pseudonym oder eine E-Mail Adresse). Wie bereits in der Einleitung festgestellt, sind IP-Adressen als Teilnehmernummern zu qualifizieren. Ferner erscheint es vertretbar, unter dem Begriff „Gespräch" Kommunikation im allgemeinen zu verstehen. Die Auskunftspflicht kann daher mE auf § 53 Abs 3a S 1 gestützt werden.. In diesem Zusammenhang ist es wohl auch unproblematisch, wenn es sich um dynamische IP-Adressen handelt. Eine Auskunft wäre diesfalls aber auf § 53 Abs 3a S 2 zu stützen, da ein Eingriff in Vermittlungsdaten erfolgt.[330] Jedenfalls abzulehnen ist eine Beauskunftung aufgrund der E-Mail-Adresse oder der E-Mail Adresse selbst. Diese ist nämlich weder eine Teilnehmernummer noch eine Anschrift noch ein Anschluss iSd Norm.

Normzweck ist die Feststellung der Identität einer Person. Ausgeschlossen ist daher die Erhebung von Daten über das Surfverhalten eines Nutzers, also wann eine bestimmte Person welche Seite angesurft hat.

(5) Sanktion

Die Auskunft ist unverzüglich und kostenlos zu erteilen. Durchsetzung mittels Zwang ist nicht möglich.[331]

bb) Sonstige Bemerkungen

Zwar nicht ISP betreffend, aber vorgeblich ein relevanter Fall ist folgender Sachverhalt:

> A geht – mit seinem Mobiltelephon ausgerüstet – auf eine Schi-Bergtour. Er wird von einer Lawine verschüttet. Die Sicherheitsbehörde verlangt vom Betreiber, eine Standortanpeilung durchzuführen.

---

[330] Dies ist jedoch in praxi nicht unstrittig. So sollen sich eine Reihe von ISP die Auskunft mit der Begründung verweigern, IP-Adressen seinen Vermittlungsdaten und daher von § 53 Abs 3a - der sich lediglich auf Stammdaten bezieht – nicht erfasst. Ferner beziehe sich diese Bestimmung ausschließlich auf Sprachtelephonie, und sei daher auf das Internet im allgemeinen nicht anwendbar (arg „Gespräch", „Teilnehmernummer"). In praxi werden aber Auskunftsbegehren auch für das Internet immer wieder auf diese Bestimmung gestützt.

[331] Vgl § 53: *"Sollen personenbezogene Daten durch Einholen von Auskünften ermittelt werden, so haben die Sicherheitsbehörden auf den amtlichen Charakter sowie auf die Freiwilligkeit der Mitwirkung hinzuweisen."*. Siehe auch: IT-Kriminalität – Niemandsland für Kriminelle, Öffentliche Sicherheit, http://www.bmi.gv.at/oeffentlsicherheit/2001/07_08/artikel_9.asp .

Eine Standortanpeilung greift in das Telekommunikationsgeheimnis ein (siehe dazu schon im der Einleitung, S 8). Die StPO eignet sich allerdings als Rechtsgrundlage nicht, da hier keine Strafverfolgung bezweckt wird. Allenfalls könnte die Standortanpeilung als im Rahmen der ersten allgemeinen Hilfeleistungspflicht erfolgen. Das SPG bietet allerdings – wie sich aus obigen Ausführungen ergibt – keine ausreichende Befugnis zur Durchführung einer Standortanpeilung. Führt der Betreiber sie trotzdem durch, kann er sich wohl auf eine mutmaßliche Einwilligung berufen.

Das TKG 2003 ermöglicht nunmehr Betreibern von Notrufdiensten ein solches Auskunftsverlangen.[332] Der oben genannte Lawinen-Opfer-Fall wird als ein solcher Notfall anzusehen sein.

§ 53 Abs 2a kommt auch im Rahmen der Amtshilfe zur Anwendung: So gestattet § 5 Abs 3 Z 3 PolizeikooperationsG[333] das Ermitteln von Daten zum Zwecke der Amtshilfe durch Einholen von Auskünften von Betreibern öffentlicher Telekommunikationsdienste nach Maßgabe des § 53 Abs 3a SPG.

2. Durchsuchung von Menschen und Objekten[334]

a) Betreten von Grundstücken oder Räumen (§ 39 Abs 1 und 2)

Soferne zur Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder der Abwehr eines gefährlichen Angriffs notwendig, dürfen Organe des öffentlichen Sicherheitsdienstes ua Räume betreten. Ein besonderer Anwendungsbereich für ISP ergibt sich mE hier nicht.

b) Durchsuchen von Grundstücken, Räumen und Fahrzeugen (§ 39 Abs 3)

> *„Die Organe des öffentlichen Sicherheitsdienstes sind ermächtigt, Grundstücke, Räume und Fahrzeuge zu durchsuchen, soweit dies der Suche 1. nach einem Menschen dient, dessen Leben oder Gesundheit unmittelbar gefährdet erscheint; 2. nach einem Menschen dient, von dem ein gefährlicher Angriff ausgeht; 3. nach einer Sache dient, die für einen gefährlichen Angriff bestimmt ist.“*

Nach einem gefährlichen Angriff gelten, – wie bereits erwähnt – die Bestimmungen der StPO. Einzig die Z 3 könnte bezogen auf Host-Provider bereichsspezifische Probleme aufwerfen. Als Beispiele werden bei *Demmelbauer/Hauer*[335] die Suche nach einem versteckten Sprengkörper oder

---

[332] Siehe hierzu schon oben in der Einleitung, im Kapitel Strafprozessrecht und Telekommunikationsrecht, 62.

[333] BG über die internationale polizeiliche Kooperation (Polizeikooperationsgesetz - PolKG) Bundesgesetz, mit dem ein Polizeikooperationsgesetz erlassen und das Sicherheitspolizeigesetz geändert wird (NR: GP XX RV 746 AB 774 S 81. BR: AB 5505 S 629.) StF: BGBl I 104/1997 idF BGBl I 146/1999 (NR: GP XX RV 1479 AB 2023 S 182. BR: 6016 AB 6025 S 657.).

[334] Es ergeben sich hier im wesentlichen die gleichen Probleme wie bei den gerichtlichen Zwangsmitteln. Es wird daher nicht neuerlich darauf eingegangen.

[335] Sicherheitsrecht Rz 156.

nach zum Verkauf bestimmten Suchtgift genannt. Im Zusammenhang mit ISP wäre vorstellbar, dass bei einem Host-Provider nach dem Speicherort von kinderpornographischem Material gesucht wird; die Abwehr des gefährlichen Angriffes würde in casu in der Verhinderung des Anbietens liegen (§ 207a Abs 1 Z 2 StGB). ME ist jedoch der Anwendungsbereich eher gering, da hier iaR ohnehin bereits nach den Bestimmungen der StPO vorgegangen wird (weil der Tatbestand nach § 207a Abs 1 Z 1 schon erfüllt ist, und damit Strafverfolgung vorliegt).

c) Öffnen und Durchsuchen von Behältnissen (Abs 5 und 6)

Diese Bestimmung ermächtigt Organe des öffentlichen Sicherheitsdienstes, Behältnisse zu öffnen, wenn die Voraussetzungen der Betretung vorliegen, bzw zu durchsuchen, wenn die Voraussetzungen der Durchsuchung gegeben sind. Ein besonderer Anwendungsbereich für ISP ergibt sich hier nicht, denn das Öffnen von Servern ist nicht besonders zweckmäßig zur Ermittlung rechtswidriger Inhalte. Eine analoge Anwendung auf die Durchsuchung der Festplatte nach Daten scheidet wohl – ebenso wie bei der StPO – aus.[336]

3. Zugriffsbefugnisse auf Sachen

a) Sicherstellung von Sachen (§ 42)

> *„Die Organe des öffentlichen Sicherheitsdienstes sind ermächtigt, Sachen sicherzustellen, 1. wenn dies bei gefährlichen Angriffen dazu dient, eine (weitere) Bedrohung des Lebens, der Gesundheit, der Freiheit oder des Eigentums von Menschen zu verhindern; 2. die sich in der Gewahrsame eines Festgenommenen befinden und besonders geeignet sind, während dessen Anhaltung a) seine eigene oder die körperliche Sicherheit anderer unmittelbar zu gefährden oder b) ihm die Flucht zu ermöglichen oder zu erleichtern; 3. denen unbefugte Beschädigung oder Wegnahme droht, sofern der Eigentümer oder rechtmäßige Besitzer nicht in der Lage ist, selbst für ihren Schutz zu sorgen; 4. die von ihnen aufgefunden werden und sich in niemandes Gewahrsame befinden."*

Unter Sicherstellung ist zwangsweise Begründung eines öffentlich-rechtlichen Verwahrungsverhältnisses zu Sicherungszwecken, zu verstehen.[337] Sie entspricht der Beschlagname der StPO.

Auch wird als Beispiel (für Z 1) die Sicherstellung von zum Verkauf bestimmen Suchtmittels genannt.[338] Es könnte also uU die Sicherstellung von Festplatten mit § 207a StGB-widrigen Material auf diese Bestimmung gestützt werden, wobei sich allerdings die Frage stellt, inwiefern dieses Material eine Bedrohung für Leben, Gesundheit, Freiheit oder des Eigentums von Menschen darstellt.

---

[336] Zur Begründung siehe im Kapitel Strafprozessrecht und Telekommunikationsrecht, S 52 f.

[337] *Demmelbauer/Hauer,* Sicherheitsrecht Rz 162.

[338] Vgl *Demmelbauer/Hauer,* aaO.

b) Inanspruchnahme von Sachen (§ 44)

> *„(1) Die Organe des öffentlichen Sicherheitsdienstes dürfen fremde Sachen in Anspruch nehmen, wenn deren Gebrauch zur Abwehr eines gefährlichen Angriffes oder für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht unerläßlich erscheint.[…]“*

Standardbeispiel für diese Befugnis ist der PKW, der im Zuge einer Verfolgsjagd in Anspruch genommen wird. Ein Anwendungsfall für ISP ist mE nicht ersichtlich.

VII. Finanzstrafgesetz & Militärbefugnisgesetz

§ 99 Abs 3 FinStrG[339] lautet:

„Die Finanzstrafbehörde ist ferner berechtigt, für Zwecke des Finanzstrafverfahrens von den Betreibern öffentlicher Telekommunikationsdienste Auskunft über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses zu verlangen. Die ersuchte Stelle ist verpflichtet, diese Auskunft unverzüglich und kostenlos zu erteilen."

§ 22 Abs 2a MBG[340] lautet:

„Militärische Organe und Dienststellen nach Abs. 1 dürfen von den Betreibern öffentlicher Telekommunikationsdienste jene Auskünfte über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses verlangen, die diese Organe und Dienststellen als wesentliche Voraussetzung zur Erfüllung von Aufgaben der nachrichtendienstlichen Aufklärung oder Abwehr benötigen. Die ersuchte Stelle ist verpflichtet, die Auskunft unverzüglich und kostenlos zu erteilen."

Diese beiden Bestimmungen sind – wie sich aus den Fußnoten ergibt - erst kürzlich eingeführt worden. Sie wurden nach Vorbild des § 53 Abs 3a SPG geschaffen. Folgende Frage soll gemeinsam betrachtet werden: Rechtfertigen diese Auskunftsrechte auch den Eingriff in Vermittlungsdaten? ME ist dies aus folgenden Erwägungen abzulehnen. § 53 Abs 3a S 1 SPG, § 99 Abs 3 FinStrG und § 22 Abs 2a MBG sind praktisch ident formuliert (Auskunftsbegehren über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses), und ermächtigen nicht zu einem Eingriff in das Telekommunikationsgeheimnis (so auch explizit die EB zum MBG, siehe dazu unten). Sehr wohl gewährt die „kleine passive Rufdatenrückerfassung" gem § 53 Abs 3a S 2 SPG einen solchen Eingriff, diese Bestimmung wurden aber weder ins MBG noch ins FinStrG übernommen. Soll der Nutzer daher anhand einer dynamischen IP-Adresse festgestellt werden, dürfte der ISP dieses Begehren ablehnen. Ferner stehen diesen Behörden die Auskunftsrechte nach § 18 Abs 3 ECG und § 90 Abs 6 TKG 2003 zu, die aber ebenso wenig einen Eingriff in das Telekommunikationsgeheimnis erlauben.

Abweichend von den Ausführungen zum SPG ergeben sich lediglich zwei erläuterungsbedürftige Themenkreise:

---

339 BG v 26. Juni 1958, betreffend das Finanzstrafrecht und das Finanzstrafverfahrensrecht (Finanzstrafgesetz - FinStrG.) StF: BGBl 129/1958 idF BGBl I 97/2002 (NR: GP XXI IA 666/A AB 1128 S 103. BR: AB 6656 S 688.).

340 BG über Aufgaben und Befugnisse im Rahmen der militärischen Landesverteidigung (Militärbefugnisgesetz - MBG) (NR: GP XXI RV 76 AB 218 S 33. BR: AB 6203 S 667.) StF: BGBl I 86/2000 idF BGBl I 103/2002 – Reorganisationsbegleitgesetz - (NR: GP XXI IA 658/A AB 1119 S 107. BR: 6670 AB 6671 S 689.). Mit der letzten Novelle wurde auch § 22 Abs 2a eingeführt.

1. Behördenzuständigkeiten uä des FinStrG.
2. Aufgaben der nachrichtendienstlichen Aufklärung oder Abwehr nach dem MBG.

A. Finanzstrafgesetz

§ 99 Abs 3 wurde mit dem Abgaben-Rechtsmittel-Reformgesetz[341] in das FinStrG eingefügt.[342] Die EB[343] führen hierzu aus, dass § 120 FinStrG eine Beistandspflicht auch der Dienststellen der Post- und Telegraphenverwaltung für Zwecke des Finanzstrafverfahrens vorsieht. Durch die Privatisierung der PTV biete aber § 120 FinStrG keine ausreichende Rechtsgrundlage für Auskünfte über Stammdaten mehr. Solche seien für die Zwecke des FinStrG aber unverzichtbar. Die Regelung erfolge nach Vorbild des § 53 SPG.

1. Auskunftspflichtig

Betreiber öffentlicher Telekommunikationsdienste.

2. Auskunftsberechtigt

Justizbehörden sind keine Finanzstrafbehörden.[344] Zuständige Behörden 1. Instanz sind gem § 58 die Hauptzollämter und die Finanzämter; diese entscheiden ab bestimmten Wertbeträgen in Spruchsenaten (§ 58 Abs 2). Gem § 62 Abs 1 wird der Unabhängige Finanzsenat als Finanzstrafbehörde 2. Instanz tätig.

3. Voraussetzungen

Auskünfte können im Rahmen des finanzstrafbehördlichen Vorverfahrens eingeholt werden. Dieses ist gem § 82 Abs 1 einzuleiten, wenn genügend Verdachtsmomente gegen eine Person vorliegen.

4. Inhalt

Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses.

---

[341] Abgaben-Rechtsmittel-Reformgesetz – AbgRmRefG (NR: GP XXI IA 666/A AB 1128 S 103. BR: AB 6656 S 688.) BGBl I 97/2002.

[342] Zusätzlich wurden mit dieser Novelle auch die Unabhängigen Finanzsenate eingeführt. Diese lösten die Berufungssenate der Finanzlandesdirektionen als 2. Instanz ab.

[343] Initiativantrag zum AbgRmRefG, 666/A BlgNR XXI. GP, http://www.parlinkom.gv.at/pd/pm/XXI/A/texte/006/A00666_.html .

[344] Dies ergibt sich systematisch aus mehreren Bestimmungen: § 53, insbes Abs 6; § 58, § 63.

B. Militärbefugnisgesetz

§ 22 Abs 2a wurde erst durch einen Abänderungsantrag[345] in das ReorganisationsbegleitG aufgenommen. Als Begründung wird angeführt, dass nach Vorbild des § 53 Abs 2a SPG auch den militärischen Nachrichtendiensten die Möglichkeit zur Eruierung bestimmter „Stammdaten" eröffnet werden soll. Die Normierung der „kleinen passiven Rufdatenrückerfassung" sei nicht notwendig, da gemäß § 2 Abs 2 MBG in solchen Fällen die Sicherheitspolizei grundsätzlich zur weiteren Veranlassung zuständig ist. Bemerkenswert ist, dass man sich in diesem Zusammenhang Gedanken über die Kostentragung gemacht hat. Aufgrund der geringen Zahl der zu erwartenden Anfragen sei eine kostenlose Zur-Verfügung-Stellung vertretbar.[346] Im Rahmen des SPG und des ECG hat man solche Überlegungen nicht angestellt. Die EB betonen weiters, dass das Fernmeldegeheimnis nicht berührt ist, da nach hA Stammdaten nicht davon geschützt seien.

Des weiteren enthält das MBG in § 7 eine Befugnis zum Einholen von Auskünften (Auskunftsverlangen) parallel zu § 34 SPG.[347]

1. Auskunftspflichtig

Betreiber öffentlicher Telekommunikationsdienste.

2. Auskunftsberechtigt

Militärische Organe[348] und Dienststellen nach § 22 Abs 1 sind berechtigt, entsprechende Auskünfte zu verlangen. Voraussetzung ist, dass sie mit Aufgaben der nachrichtendienstlichen Aufklärung oder Abwehr betraut sind. Militärische Organe sind gem § 1 Abs 1 Soldaten und Angehörige der Heeresverwaltung, wenn diese Organe ermächtigt sind, Befugnisse nach dem MBG auszuüben, soweit sie mit der Erfüllung von Aufgaben militärischer Landesverteidigung betraut sind. Abs 2 leg cit definiert militärische Dienststellen als alle Dienststellen im Vollziehungsbereich des Bundesministers für Landesverteidigung.

3. Voraussetzungen

Die Information muss wesentliche Voraussetzung zur Erfüllung von Aufgaben der nachrichtendienstlichen Aufklärung oder Abwehr benötigen.

Gem § 20 Abs 1 dient die nachrichtendienstliche Aufklärung der Beschaffung, Bearbeitung, Auswertung und Darstellung von Informationen über das Ausland betreffend militärische und hiermit zusammenhängende Tatsachen, Vorgänge und Vorhaben. Nach Abs 2 dient die nachrichtendienstliche Abwehr dem Eigenschutz durch Beschaffung,

---

345 StenProt NR 223 GP XXI, http://www.parlinkom.gv.at/pd/pm/XXI/NRSP/NRSP_107/107_223.html .

346 StenProt NR 223 GP XXI, aaO.

347 Zur Abgrenzung von SPG und MBG vgl § 2 MBG.

348 Man beachte hier den Unterschied zu § 53 Abs 2a SPG, wo nur die Behörde, nicht aber deren Organe, auskunftsberechtigt ist.

Bearbeitung, Auswertung und Darstellung von Informationen über Bestrebungen und Tätigkeiten, die vorsätzliche Angriffe gegen militärische Rechtsgüter[349] zur Beeinträchtigung der militärischen Sicherheit erwarten lassen. Es geht hier vorwiegend um den Schutz militärischer und verfassungsmäßiger Einrichtungen.[350] Zuständige Stellen sind daher der Heeresnachrichtendienst und das Heeresabwehramt.[351]

4. Inhalt

Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses.

[349] Vgl zu diesem Begriff § 1 Abs 7.
[350] Vgl *Demmelbauer/Hauer,* aaO.
[351] Vgl *Demmelbauer/Hauer,* Sicherheitsrecht Rz 30.

VIII. Datenschutzgesetz

Im Unterschied zu den bislang behandelten Auskunftspflichten, zielt § 26 weniger auf die Feststellung der Identität einer Person ab, sondern gewährt dem Betroffenen einer Datenanwendung ein Auskunftsrecht bezüglich seiner verarbeiteten Daten, und ermöglicht es ihm festzustellen, ob eine Verletzung des DSG stattgefunden hat. Insofern dient auch diese Auskunftspflicht der Feststellung der Identität zwecks Rechtsverfolgung. § 26 stellt die Ausführungsbestimmung zur Verfassungsbestimmung des § 1 Abs 3 dar. Das Auskunftsrecht ist daher Teil des Grundrechts auf Datenschutz.[352]

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

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

1. des Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich oder

2. der Sicherung der Einsatzbereitschaft des Bundesheeres oder

3. der Sicherung der Interessen der umfassenden Landesverteidigung oder

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

5. der Vorbeugung, Verhinderung oder Verfolgung von Straftaten ergeben.

Die Zulässigkeit der Auskunftsverweigerung aus den Gründen der Z 1 bis 5 unterliegt der Kontrolle durch die Datenschutzkommission nach § 30 Abs. 3 und

[352] Auch Art 20 Abs 4 B-VG enthält eine datenschutzrechtliche Auskunftspflicht gegenüber Organen der Bundes-, Landes- und Gemeindeverwaltung sowie von Körperschaften des öffentlichen Rechts. Diese Bestimmung wird durch das Auskunftspflicht-Grundsatzgesetz BGBl 286/1987, für den Bereich der Verwaltung des Bundes durch das AuskunftspflichtG BGBl 286/1987 idF 158/1998 und für die Landesverwaltung durch die jeweiligen Ausführungsgesetze, umgesetzt. Diese Auskünfte betreffen Angelegenheiten des Wirkungsbereiches der jeweiligen Behörde, und zwar auch dann, wenn er nicht Betroffener iSd DSG ist. Vgl zur Verhältnis des DSG und der AuskunftspflichtG: *Jahnel,* Das Auskunftsrecht nach dem Datenschutzgesetz, ZfV 1991, 243.

dem besonderen Beschwerdeverfahren vor der Datenschutzkommission gemäß § 31 Abs. 4.

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

(4) Innerhalb von acht Wochen nach Einlangen des Begehrens ist die Auskunft zu erteilen oder schriftlich zu begründen, warum sie nicht oder nicht vollständig erteilt wird. Von der Erteilung der Auskunft kann auch deshalb abgesehen werden, weil der Betroffene am Verfahren nicht gemäß Abs. 3 mitgewirkt oder weil er den Kostenersatz nicht geleistet hat.

(5) […]

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

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

(8) […]*"*

1. Auskunftspflichtig

Zur Erteilung der Auskunft ist der Auftraggeber verpflichtet. Auftraggeber ist gem § 4 Z 4 eine natürliche oder juristische Person, Personengemeinschaften oder Organe einer Gebietskörperschaft bzw die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten für einen bestimmten Zweck zu verarbeiten, und zwar unabhängig davon, ob sie die Verarbeitung selbst durchführen oder hiezu einen anderen heranziehen.[353]

2. Auskunftsberechtigt

Nur der Betroffene ist berechtigt, eine Auskunft zu verlangen. Dies ist jene Person, deren Daten verarbeitet werden (§ 4 Z 3). Der Betroffene ist im erforderlichen Ausmaß zur Mitwirkung verpflichtet, um ungerechtfertigten und unverhältnismäßigen Aufwand beim Auftraggeber zu vermeiden (§ 26 Abs 3). Voraussetzung ist allerdings, dass der Betroffene vom Auftraggeber zur Mitwirkung aufgefordert wird.[354]

[353] Näheres zum Begriff des Auftraggebers und seiner Abgrenzung zum Dienstleister siehe *Drobesch/Grosinger,* Datenschutzgesetz 113 f.

[354] Vgl Näheres bei *Drobesch/Grosinger,* Datenschutzgesetz 207.

3. Voraussetzungen

Der Betroffene muss die Auskunft in schriftlicher Form verlangen, und seine Identität in geeigneter Form nachweisen. Der Auftraggeber kann allerdings auch zustimmen, dass das Auskunftsbegehren mündlich gestellt wird. Schriftlich ist in diesem Zusammenhang als „schriftlich iSd § 13 AVG" zu verstehen (dh als Gegensatz zu mündlich, und nicht als Unterschriftlichkeit iSd § 886 ABGB), dh man könnte auch via E-Mail eine Auskunft verlangen, wobei sich dann allerdings ein Problem mit dem Identitätsnachweis stellen wird. Dem könnte man – abgesehen von der Verwendung einer elektronischen Signatur - bspw durch das Faxen eines amtlichen Lichtbildausweisen nachkommen, wenn die Auskunft mittels eingeschriebenem Briefs retourniert wird.[355] *Jahnel*[356] hält die Übermittlung der Auskunft an eine persönliche E-Mail-Adresse für ausreichend, um sicherzustellen, dass der Betroffene die Auskunft erhält. Das Rundschreiben des BKA zur Durchführung des Auskunftsrechtes, 810.031./1-V/3/87[357] schlägt als geeignete Formen des Identitätsnachweises vor: bei persönlicher Vorsprache durch Vorlage eines Lichtbildausweises, bei schriftlicher Antragstellung die Beglaubigung der Unterschrift und bei Auskunftsanträgen juristischer Personen den Nachweis der Vertretungsbefugnis anhand eines Firmenbuchauszuges oä.

a) Verweigerung der Auskunft

§ 26 Abs 2 zählt taxativ[358] jene Fälle auf, bei denen die Verweigerung der Auskunft zulässig ist. Die Auskunft ist nicht zu erteilen, wenn dies zum Schutz des Betroffenen aus besonderen Gründen notwendig ist oder überwiegende Interessen des Auftraggebers oder eines Dritten – worunter auch öffentliche Interessen zu verstehen sind – der Auskunftserteilung entgegenstehen. In weiterer Folge werden beispielhaft solche überwiegenden Interessen aufgezählt. Die Bedeutung der Auskunftsverweigerung spielt jedoch im privaten Bereich eine untergeordnete Rolle.[359]

4. Inhalt

Der Auftraggeber hat Auskunft zu erteilen über:

---

[355] Diese Art des Identitätsnachweises sieht auch bspw § 365o GewO vor. Siehe auch § 40 Abs 8 BWG, eingefügt durch BGBl I 35/2003. Zu erwägen wäre auch, ob das Einscannen und Verschicken via E-Mail ein ausreichender Identitätsnachweis ist.

[356] Datenschutzrecht, in: *Jahnel/Schramm/Staudegger* (Hrsg), Informatikrecht[2] 262.

[357] *Drobesch/Grosinger,* Datenschutzgesetz 203, befürworten weiterhin eine inhaltliche Anwendbarkeit.

[358] Vgl *Drobesch/Grosinger,* Datenschutzgesetz 207.

[359] *Drobesch/Grosinger* (Datenschutzgesetz, aaO) führen aus, dass dem Schlusssatz des Abs 2 „*in erster Linie klarstellende Bedeutung"* zukommt. *„Normativer Inhalt könnte ihm nur für die kaum denkbaren Fälle beigemessen werden, in denen sich ein Auftraggeber des privaten Bereichs auf die Z 1 bis 5 beruft.".*

- Verarbeitete Daten: Darunter fallen alle Daten auf die ein in § 4 Z 9[360] genannter Verarbeitungsschritt zutrifft, worunter auch das Löschen von Daten fällt. Da aber Auskünfte über gelöschte Daten schon rein faktisch nicht möglich sind und nur auf verfügbare Daten abgestellt wird, ist die Bestimmung entsprechend teleologisch zu reduzieren.[361]
- Verfügbare Informationen über deren Herkunft: Diese bezieht sich nur auf den unmittelbaren Vormann. Weiterreichende Nachforschungspflichten bestehen laut OGH[362] nicht.[363]
- Allfällige Empfänger von Übermittlungen: Diese Informationen sind jedenfalls zu beauskunften und nicht erst auf explizites Verlangen.[364]
- Zweck der Datenverwendung und Rechtsgrundlagen für die Datenverarbeitung: Diese Angaben sollen es dem Betroffenen ermöglichen, die Zulässigkeit der Datenverarbeitung zu überprüfen.[365]

5. Sonstiges

Grundsätzlich hat die Auskunft schriftlich binnen acht Wochen zu erfolgen, mit Zustimmung des Betroffenen kann sie auch mündlich erfolgen, worauf dieser aber keinen Anspruch hat. Auskunftsverweigerungen sind stets schriftlich mitzuteilen.[366]

Gem § 26 Abs 6 ist die Auskunft unentgeltlich zu erteilen, wenn sie den aktuellen Datenbestand betrifft und der Betroffene im laufenden Jahr noch kein Auskunftsersuchen zum selben Aufgabengebiet des Auftraggebers gestellt hat. In allen anderen Fällen darf ein Mindestkostenersatz von Euro 18,89 verrechnet werden, soweit nicht tatsächlich höhere Kosten angelaufen sind. Unter aktuellem Datenbestand sind solche Daten zu verstehen, auf die man Direktzugriff hat, maW die ohne weitere Manipulationen erhoben werden können. Nicht darunter zu subsumieren sind bspw die Herbeischaffung archivierter Datenträger.[367]

Nach § 26 Abs 7 besteht ein Löschungsverbot von Daten hinsichtlich derer bereits ein Auskunftsverlangen vorliegt. Die Sperrfrist dauert 4 Monate ab Zeitpunkt der Kenntnis dieses Auskunftsverlangens bzw im Falle eines Verfahrens vor der DSK, bis zu dessen rechtskräftigem Abschluss.

---

[360] Dieser lautet:*„das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen (Z 11), Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten einer Datenanwendung durch den Auftraggeber oder Dienstleister mit Ausnahme des Übermittelns (Z 12) von Daten;“*.

[361] Vgl *Drobesch/Grosinger,* Datenschutzgesetz 204. Allerdings besteht in gewissen Umfang eine Protokollpflicht (§ 14 DSG).

[362] OGH 28.10.1999, 3 Ob 132/99d = ARD 5157/18/2000.

[363] Vgl auch das Urteil des OGH 5. 5. 1988, 6 Ob 9/88 = EvBl 1988/150: Das Höchstgericht wies eine Klage auf Auskunftserteilung mit der Begründung ab, die Herkunft der Daten sei nicht mehr bestimmbar und somit die eingeklagte Leistung unmöglich.

[364] Vgl *Drobesch/Grosinger,* Datenschutzgesetz 205.

[365] Vgl *Drobesch/Grosinger,* Datenschutzgesetz aaO.

[366] Vgl *Drobesch/Grosinger,* Datenschutzgesetz 205 f.

[367] Siehe Vgl *Drobesch/Grosinger,* Datenschutzgesetz 209.

6. Sanktion und Durchsetzung

Das Löschungsverbot ist gem § 52 Abs 1 Z 4 verwaltungsstrafbewehrt.

In Abweichung vom Grundsatz, dass das Grundrecht auf Datenschutz gegenüber Auftraggebern aus dem privaten Bereich vor den Zivilgerichten geltend zu machen ist, bestimmen § 1 Abs 5 und § 31 Abs 1 (in Gegensatz zum DSG 1978) betreffend dem Auskunftsrecht die Alleinzuständigkeit der DSK, was insbes für die Kostentragung von Bedeutung ist.[368] Die DSK entscheidet in Bescheidform. Erkennt sie auf Verletzung des Auskunftsrechts, besteht neben dem Ausspruch der Rechtswidrigkeit allenfalls die Möglichkeit der Erhebung einer Feststellungsklage nach § 32 Abs 5 durch die DSK.[369] Zur Wirkung der Bescheide der DSK sieht § 40 Abs 4 vor, dass bei Feststellung der Verletzung des DSG durch einen Auftraggeber des öffentlichen Bereichs, dieser unverzüglich den der Rechtsanschauung der DSK entsprechenden Zustand herzustellen hat. Der Gesetzgeber hat hier wohl an eine öffentlich-rechtliche Weisung gedacht.[370] Fraglich ist, ob diese Regelung auch auf den privaten Bereich anzuwenden sind, und in weiterer Folge, wie die Bescheide der DSK zu exekutieren sind. Im Kern geht es um die Frage, ob die DSK einen Leistungsbescheid erlässt (der dann nach den Regeln des VVG durchzusetzen ist) oder lediglich einen Feststellungsbescheid. Überdies bedroht § 52 Abs 1 Z 4 die Verletzung der Auskunftspflicht mit Verwaltungsstrafen bis zu Euro 18.890, was vermutlich gegen einen Leistungsbescheid sprechen würde. Da die DSK allerdings selbst von der unmittelbaren Exekutierbarkeit ihrer Bescheide ausgeht[371], ist wohl anzunehmen, dass es sich um Leistungsbescheide handelt.

---

[368] Siehe hierzu (allerdings zum DSG 1978, wo dieser Grundsatz unbeschränkt galt): *Jahnel,* Das Auskunftsrecht nach dem Datenschutzgesetz, ZfV 1991, 243.

[369] Vgl *Drobesch/Grosinger,* Datenschutzgesetz 231.

[370] Vgl *Drobesch/Grosinger,* Datenschutzgesetz 258.

[371] ZB: DSK 25.3.2003, K120.749/006-DSK/2003: *"Dem belangten Auftraggeber wird aufgetragen, binnen vier Wochen bei sonstiger Exekution dem Beschwerdeführer dem Gesetz entsprechend kostenlos Auskunft über die zu seiner Person verarbeiteten Daten zu geben.";* DSK 3.12.2002, K120.804/016-DSK/2002, spricht von Leistungsbegehren der Partei und trägt der belangten Partei bei sonstiger Exekution auch die Auskunftserteilung auf.

IX. Beurteilung der Ausgangsfälle

1. Der Fall *RIAA* vs *Verizon*: Auskunft Access-Provider an Privaten

Auf Basis des ECG ist eine Auskunftspflicht nicht zu begründen, denn 1. liegt uU gar kein strafbares Verhalten des Nutzers vor[372], und 2. haben Private kein Auskunftsrecht gegenüber Access-Providern (§ 18 Abs 4).

Gem § 87b UrhG besteht allerdings eine Auskunftspflicht des Access-Providers. Der Fall wäre also mittlerweile ebenso zu beurteilen, wie in den USA.

2. Variante *RIAA* vs *Verizon*: Beteiligung eines Strafgerichts

1. Auskunftsverpflichtet: Auch Access-Provider sind auskunftspflichtig
2. Auskunftsberechtigt: Eine brauchbare gesetzliche Befugnis wäre § 143 Abs 2 StPO (Allgemeine Mitwirkungspflicht), die auf die Herausgabe von Beweisgegenständen gerichtet ist. Hier wäre allerdings zu differenzieren: Muss der Provider in das Telekommunikationsgeheimnis eingreifen, weil der Untersuchungsrichter ihm nur den Zeitpunkt einer möglichen Verbindung bekannt gibt, und er daher Vermittlungsdaten erheben muss, um die Identität des Kunden zu bestimmen[373], wären die Bestimmungen gem §§ 149a ff StPO[374] anzuwenden. Die Erhebung der Daten wäre jedoch ausgeschlossen, da § 91 Abs 1 UrhG eine Strafdrohung von bis zu 6 Monaten vorsieht, aber § 149a Abs 2 Z 2 StPO eine mindestens 1jährige Strafdrohung voraussetzt. Anders stellt sich die Situation dar, wenn das Gericht zumindest eine IP-Adresse vorweisen kann, vorausgesetzt es handelt sich um eine statische, die gemeinsam mit den Stammdaten des Kunden gespeichert. Eine dynamische IP-Adresse

---

372 Ob nach der Rechtslage vor der UrhG-Nov 2003 das bloße Herunterladen von Musikfiles, wenn sie auch unrechtmäßig in Verkehr gebracht worden sind, rechtswidrig ist, ist strittig: vgl *Haller,* Music on Demand (2001) 140; zuletzt: *Schmidbauer,* Up and Down, http://www.internet4jurists.at/news/aktuell46.htm . Dies soll auch nach der UrhG-Nov 2003 gelten (vgl *Schmidbauer,* FAQ zum Urheberrecht, http://www.internet4jurists.at/urh-marken/faq_urh1.htm , Punkt 10. Tauschbörsen). Der RiAA geht es aber offensichtlich nicht nur die Verfolgung um sogenannte *Poweruser*, vgl zB RIAA gibt Einblick in ihre Jagdmethoden gegen P2P-User, Heise Online, http://www.heise.de/newsticker/data/wst-28.08.03-001/ .

373 Vgl § 149a Abs 1 StPO: *"Im Sinne dieses Bundesgesetzes ist „1. „Überwachung einer Telekommunikation" (§ 3 Z 13 TKG)* […] *b) die Feststellung, welche Teilnehmeranschlüsse Ursprung oder Ziel einer Telekommunikation sind oder waren".*

374 Näheres zu diesen Bestimmungen, insbes zur Beschlagnahme von Datenträgern die nach TKG geschützte Daten enthalten, siehe im Kapitel Strafprozessordnung und Telekommunikationsgesetz, S 52.

wäre wiederum problematisch, wenn festgestellt werden müsste, wann der Kunde eingeloggt war.
3. Voraussetzungen: Ein schriftlicher Beschluss unter Angabe der Rechtsgrundlagen, einschließlich einer Begründung, warum anhand der Auskunft eine gerichtlich strafbare Handlung verhütet, ermittelt, aufgeklärt oder verfolgt werden kann.
4. Inhalt der Auskunft: Stammdaten des Kunden.

3. Überwachung des Fernmeldeverkehrs auf Anordnung eines Gerichtes

1. Verpflichtet: Der WLAN-Betreiber ist ein Access-Provider, und daher ein Anbieter öffentlicher (Tele-)Kommunikationsdienste.
2. Berechtigt: Als Rechtsgrundlage kommt § 149a StPO in Betracht. Da jedenfalls keine Inhaltsdaten überwacht werden sollen, reicht ein Beschluss des Untersuchungsrichters aus (§ 149b StPO).
3. Voraussetzungen: Abgesehen vom Beschluss des Untersuchungsrichters, ist für die Überwachung von Vermittlungs- oder Standortdaten der Verdacht der Begehung einer strafbaren Handlung notwendig, die mit mehr als einjähriger Freiheitsstrafe bedroht ist, und die Aufklärung der strafbaren Handlung im Hinblick auf die Ermittlung der Daten des Verdächten gefördert werden kann. Gem § 3h iVm § 3g VerbotsG ist ein Verstoß gegen diese Bestimmungen mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen, und der Täter könnte durch ein Auskunftsverlangen an den WLAN-Betreiber ausgeforscht werden. Fraglich ist, ob das Feststellen, in welchem Internet-Cafe sich der Täter befindet vom Begriff der Standortermittlung umfasst ist. Die Standortpeilung als Unterfall der Überwachung der Telekommunikation ist die Feststellung des räumlichen Bereiches, in dem sich ein durch einen bestimmten Teilnehmeranschluss gekennzeichnetes Endgerät befindet oder befunden hat. Der Laptop ist als Endgerät zu qualifizieren. Teilnehmeranschluss ist in casu das WLAN, da er iSd EB[375] eine technische Einrichtung ist, die dem Senden, Übermitteln und Empfangen einer Telekommunikation dient. ME sind daher die Bestimmungen über die Standortanpeilung auch bei WLAN anwendbar.
4. Inhalt: Standortdaten

4. Auskünfte an Verwaltungsbehörden

I. Gewerbebehörde:

§ 18 Abs 3 ECG stellt eine taugliche Rechtsgrundlage für Auskunftsverlangen an den Host-Provider dar, bei dem die Website gehostet ist.[376] Dieser hat nur Auskunft über die verfügbaren Stammdaten zu leisten. Es darf angenommen werden, dass die geforderte Information wesentliche Voraussetzung für die der Gewerbebehörde übertragenen Aufgaben bildet.

---

[375] Siehe oben, S 60.

[376] Dieser ist anhand einer Abfrage bei der Registrierungsstelle, der nic.at, zu ermitteln, und zwar über http://www.nic.at .

II. Finanzstrafbehörde:

Drei Rechtsgrundlagen bieten sich hier an: einerseits § 99 Abs 3 FinStrG bzw § 90 Abs 6 TKG 2003, und § 18 Abs 3 ECG. Die erstgenannten Bestimmungen verpflichten Anbieter von (Tele-) Kommunikationsdiensten zur Auskunft über Stammdaten. Fraglich ist jedoch, ob Ebay als Anbieter von solcher Dienste zu werten ist. Unterstellt man, dass Ebay seine Host-Rechner selbst betreibt (vgl Einleitung, S 15), wovon aufgrund der Größe dieses Unternehmens auszugehen ist, unterliegt Ebay der Auskunftspflicht, soweit Stammdaten vorhanden sind. Das Auskunftsbegehren kann aber auch auf § 18 Abs 3 ECG gestützt werden, womit jedenfalls Host-Provider erfasst sind.

III. Sicherheitsbehörde:

Die Sicherheitsbehörde kann sich wegen des Verstoßes gegen das PyrotechnikG in ihrem Auskunftsbegehren auf § 53 Abs 3a S 1 SPG (es sei denn, es liegt zusätzlich ein gefährlicher Angriff vor, dann könnte auch S 2 herangezogen werden), § 90 Abs 6 TKG 2003 und § 18 Abs 3 ECG stützen. Ein Verstoß gegen § 107 Abs 2 TKG 2003 (Zusendung unerwünschter Nachrichten) stellt gem § 109 Abs 3 Z 20 TKG 2003 eine Verwaltungsübertretung dar.

5. Mobilfunkbetreiber als Access-Provider

Dieser Fall wird auch von *Schmidtbauer* geschildert.[377]

> *Wilhelm*[378] beschäftigt sich ebenfalls damit, jedoch unter Bezugnahme auf den Mobilfunkbetreiber. Er gelangt zu dessen Haftung, wobei er davon ausgeht, dass der Mobilfunkbetreiber die Mehrwertdienstenummern an die Diensteanbieter zuteilt, und gelangt so zu einer Zurechnung. Dem ist zu entgegnen, dass Mehrwertdienstenummern von der RTR GmbH zur selbständigen Verwaltung in Rufnummernblöcken dem Dienstenetzbetreiber zugeteilt werden (vgl § 14 NVO), und nicht dem Mobilfunkbetreiber.[379] Auch besteht iaR kein Vertragsverhältnis zwischen Mobilfunkbetreiber und Mehrwertdiensteanbieter.[380] Die Haftung des Mobilfunkbetreibers kann daher auf die Nummernvergabe nicht gestützt werden.

Der Mehrwertdiensteanbieter ist Kunde bei einem Alternativen Netzbetreiber (einem Dienstenetzbetreiber[381]), der ihm die Leitungen zwecks Anbieten des Mehrwertdienstes zur Verfügung stellt. Es stellt sich nun die

---

[377] M-Love, http://www.internet4jurists.at/news/aktuell30.htm .

[378] Ich habe mich in dich verliebt - bitte ruf 0900 87654…, ecolex 2003, 73.

[379] Zum Verfahren und den div Richtlinien der RTR GmbH zur Vergabe von Mehrwertdienstenummern nach alter Rechtslage: http://www.rtr.at/web.nsf/deutsch/Telekommunikation_Nummerierung . Nach neuer Rechtslage http://www.rtr.at/web.nsf/deutsch/Portfolio_Konsultationen_bisherige_bisherigeKonsultationen_Nummernzuteilung .

[380] Zur üblichen Konstruktion bei Mehrwertdiensten siehe *K Wessely /Eugen*, Ich war es nicht! oder: Haftung für die Inanspruchnahme von Mehrwertdiensten durch Geschäftsunfähige, MR 2003, 3.

[381] Vgl *K Wessely/Eugen,* aaO.

Frage, ob der Netzbetreiber hier als Diensteanbieter iSd § 3 Z 3 ECG zu qualifizieren ist. In casu übermittelt er Informationen in Form einer SMS in einem elektronischen Kommunikationsnetz (die Übertragung erfolgt paketvermittelt), was gem § 3 Z 1 ECG ein Dienst der Informationsgesellschaft ist. Er unterliegt somit dem ECG, und kommt in den „Genuss" von Haftungsprivilegien und Auskunftspflichten.

> Insofern ist die oben kurz dargestellte Ansicht *Wilhelms* zweifelhaft: Der Mobilfunkbetreiber übermittelt ebenfalls nur die SMS an den Empfänger, der Nutzer iSd ECG ist. Allerdings besteht zwischen Nutzer und Mobilfunkbetreiber ein Vertragsverhältnis. Vertragliche Ansprüche werden von den Haftungsprivilegien des ECG selbstverständlich nicht ausgeschlossen.[382] ME schließt aber § 18 Abs 1[383] (keine Überwachungspflicht für Diensteanbieter) auch die Haftung aufgrund nebenvertraglicher Schutzpflichten aus.[384]

Die Staatsanwaltschaft kann daher beim Untersuchungsrichter die Einholung einer Auskunft gem § 18 Abs 2 ECG iVm § 143 Abs 1 StPO beantragen, um die Identität des Mehrwertdiensteanbieters zu erfahren. Dieser ist zweifelsohne Nutzer iSd § 3 Z 4 ECG.

---

[382] *Brenn,* ECG 285.

[383] Der im Übrigen eine *lex specialis* zu § 75 TKG 1997 ist, wobei diese Bestimmung auf Access-Provider ohnedies nicht anwendbar ist (vgl auch *Brenn,* ECG 300; aA offensichtlich *Zankl,* ECG-Handbuch Rz 272).

[384] So ähnlich auch die EB zum ECG, abgedruckt in: *Brenn*, ECG 295.Vgl auch *Koziol,* Haftpflichtrecht I[3] (1997) 147:*"Als rechtswidrig wird ein Verhalten bezeichnet, wenn unter Außerachtlassung der objektiven Sorgfaltsanforderungen Verhaltenspflichten verletzt werden".* Es stellt daher keinen Verstoß gegen die erforderliche Sorgfalt dar, wenn keine Überwachung von Informationen erfolgt, um solche Schäden zu verhindern. Auch ist Telekommunikation grundsätzlich keine gefährliche Sache, über die man aufklären müsste. Zu einem anderen Ergebnis mag man bei den sog Dialern kommen, denn diese verursachen tatsächlich unbemerkt horrende Kosten (vgl hierzu die Empfehlungen der RTR, http://www.rtr.at/web.nsf/deutsch/Telekommunikation~Konsumentenservice~Schlichtungsstelle+RTR~SchlichtungsstelleRTR~Empfehlung ; in Deutschland gibt es bereits einige Entscheidungen zu diesem Thema, vgl zB bei http://www.jurpc.de).

X. Übersicht über die wichtigsten Auskunftspflichten

Rechtsgrundlage	Verpflichtet	Berechtigt	Voraussetzungen	Inhalt	Durchsetzung mittels Zwang
§ 18 Abs 2 ECG	Host-, Access-Provider	Inländisches Strafgericht	Beschluss, zur Verhütung, Ermittlung, Aufklärung oder Verfolgung gerichtlich strafbarer Handlungen	Stamm- und Vermittlungsdaten (je nach Rechtsgrundlage)	je nach Rechtsgrundlage
§ 18 Abs 3 ECG	Host-Provider	Verwaltungsbehörden	Bescheid, wesentliche Voraussetzung der der Behörde übertragenen Aufgaben	Stammdaten	nein
§ 18 Abs 4 ECG	Host-Provider	Private	Überwiegendes rechtliches Interesse an der Feststellung des Nutzers und eines rechtswidrigen Sachverhaltes. Glaubhaftmachung, dass Informationen eine wesentliche Voraussetzung für die Rechtsverfolgung bildet.	Stammdaten	zivilrechtlich

§ 87b UrhG	Host-, Access-Provider	Rechteinhaber	Verletzung eines Ausschließlichkeitsrechts	Stammdaten	zwangsweise Abnahme von Datenträgern
§ 149a StPO	Access-Provider, (Host-Provider)	Untersuchungsrichter bzw Ratskammer	Formeller Überwachungsbeschluss, je nach Datum unterschiedlich hohe Strafdrohung notwendig	Vermittlungs- und Inhaltsdaten	Verwaltungsstrafen
§ 143 StPO	Jedermann	Untersuchungsrichter, Sicherheitsbehörden	Beschluss, zwecks Sicherstellung von Beweismitteln	Stammdaten	Beugestrafen bzw -haft
§ 53 Abs 3a SPG	Access-Provider, (Host-Provider)	Sicherheitsbehörden	Wesentliche Voraussetzung für die den Sicherheitsbehörden übertragenen Aufgaben bzw bei der „kleinen passiven Rufdatenrückerfassung“ nur im Rahmen der Hilfeleistungspflicht und Abwehr gefährlicher Angriffe	Stammdaten, zT Vermittlungsdaten	keine
§ 99 Abs 3 FinStrG	Access-Provider, (Host-Provider)	Finanzstrafbehörden	Für Zwecke des Finanzstrafverfahrens	Stammdaten	keine

§ 22 Abs 2a MBG	Access-Provider, (Host-Provider)	Militärische Organe und Dienststellen	wesentliche Voraussetzung zur Erfüllung von Aufgaben der nachrichtendienstlichen Aufklärung oder Abwehr	Stammdaten	keine
§ 90 Abs 6 TKG 2003	Access-Provider, (Host-Provider)	Verwaltungsstrafbehörden	Schriftliches und begründetes Verlangen bei Verdacht einer Verwaltungsübertretung	Stammdaten	Verwaltungsstrafen

Abkürzungsverzeichnis

aA	=	anderer Ansicht
aaO	=	am angegebenen Ort
AB	=	Ausschussbericht
Abs	=	Absatz
ABGB	=	Allgemeines bürgerliches Gesetzbuch, JGS 946/1811
abl	=	ablehnend
ABl	=	Amtsblatt der Europäischen Gemeinschaften
AGB	=	Allgemeine Geschäftsbedingungen
AnwBl	=	Österreichisches Anwaltsblatt
arg	=	argumento
AVG	=	Allgemeines Verwaltungsverfahrensgesetz, BGBl 1950/172
BAO	=	Bundesabgabenordnung, BGBl 194/1961
BG	=	Bundesgesetz
BGBl	=	Bundesgesetzblatt
BGBlG	=	Bundesgesetz über das Bundesgesetzblatt 1996, BGBl 660/1996
BKA	=	Bundeskanzleramt, Bundeskriminalamt
BMF	=	Bundesministerium für Finanzen
BMI	=	Bundesministerium für Inneres
BMJ	=	Bundesministerium für Justiz
BMLV	=	Bundesministerium für Landesverteidigung
BMVIT	=	Bundesministerium für Verkehr, Innovation und Technologie
BlgNR	=	Beilage(-n) zu den stenographischen Protokollen des Nationalrates
BR	=	Bundesrat
bspw	=	beispielweise
B-VG	=	Bundesverfassungsgesetz 1920 idF v 1929
bzw	=	beziehungsweise
CCC	=	Convention on Cyber-Crime des Europarates
Datenschutz-RL	=	Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl L 201 vom 31.7.2002, 37
dh	=	das heißt
dies	=	dieselbe
div	=	diverse
DMCA	=	Digital Millennium Copyright Act
DSG	=	Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000), BGBl I 165/1999
DSG 1978	=	Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz), BGBl 565/1978
DSK	=	Datenschutzkommission
dStPO	=	deutsche Strafprozessordnung, deutsches BGBl 1950, 455, 512, 629
E	=	Entscheidung
EB	=	Erläuternde Bemerkungen

ECG	=	Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden (E-Commerce-Gesetz), BGBl I 152/2001
EC-RL	=	Richtlinie 2000/31/EG über bestimmte Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt E-Commerce-Richtlinie, ABl L 178 vom 17. Juli 2000, 1
ecolex	=	Fachzeitschrift für Wirtschaftsrecht
EGMR	=	Europäischer Gerichtshof für Menschenrechte
EGZPO	=	Einführungsgesetz zur Zivilprozessordnung, RGBl 112/1895
EfSlg	=	Ehe- und Familienrechtliche Entscheidungen des OGH
EMRK	=	Europäische Menschenrechtskonvention, BGBl 210/210
Entw	=	Entwurf
EO	=	Exekutionsordnung, RGBl 79/1896
ErgLfg	=	Ergänzungslieferung
ErwGr	=	Erwägungsgrund
et alt	=	und andere
ETS-No	=	European Treaty Series – Number
ETSI	=	European Telecom Standard Institute
etc	=	et cetera
EuGH	=	Gerichtshof der Europäischen Gemeinschaften
EuGI	=	Gericht der Europäischen Gemeinschaften I. Instanz
EuGRZ	=	Europäische Grundrechte Zeitschrift
EvBl	=	Evidenzblatt für Rechtsmittelentscheidungen (ÖJZ)
EWR	=	Europäischer Wirtschaftsraum
f, ff	=	folgende
FAQ	=	frequently asked questions
FinStrG	=	Finanzstrafgesetz, BGBl 129/1958
FN	=	Fußnote
G	=	Gesetz
GD	=	Generaldirektion der Europäischen Gemeinschaften
gem	=	gemäß
GewO	=	Gewerbeordnung 1994, BGBl 194/1994
GP	=	Gesetzgebungsperiode
Hrsg	=	Herausgeber
iaR	=	in aller Regel
idF	=	in der Fassung
idR	=	in der Regel
idS	=	in diesem Sinne
ieS	=	im engeren Sinn
insbes	=	insbesondere
InfoSoc-RL	=	Richtlinie 2001/29/EG vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, ABl L 167 v 22.6.2001, 10, berichtigt durch ABl L 6 v 10.1.2002, 71.
Info-RL	=	InfoSoc-RL
IP	=	Internet Protokoll
IPR	=	Internationales Privatrecht
iS	=	im Sinne
iSd	=	im Sinne des, - der
ISDN	=	Integrated Services Digital Network
ISDN-RL	=	Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung

		personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, ABl L 24 v 30.1.1998, 1
ISP	=	Internet Service Provider
ISPA	=	Internet Service Provider Austria
iSv	=	im Sinne von
iVm	=	in Verbindung mit
iwS	=	im weiteren Sinn
JA	=	Justizausschuss
JAP	=	Juristische Ausbildung und Praxisvorbereitung
JBl	=	Juristische Blätter
Jud	=	Judikatur
JurPC	=	JurPC, Internet-Zeitschrift für Rechtsinformatik
KartG	=	Bundesgesetz vom 19. Oktober 1988 über Kartelle und andere Wettbewerbsbeschränkungen (Kartellgesetz 1988 - KartG 1988), BGBl 600/1988
KSchG	=	Konsumentenschutzgesetz, BGBl. 140/1979
leg cit	=	legis citatae (der zitierten Vorschrift)
Lfg	=	Lieferung
Lit	=	Literatur
lit	=	litera
maW	=	mit anderen Worten
MBG	=	Militärbefugnisgesetz, BGBl I 86/2000
mE	=	meines Erachtens
mA	=	meiner Ansicht
MR	=	Zeitschrift für Medien und Recht
mwH	=	mit weiteren Hinweisen
mwN	=	mit weiteren Nachweisen
NotifG	=	BG zur Durchführung eines Informationsverfahrens auf dem Gebiet der technischen Vorschriften, der Vorschriften für die Dienste der Informationsgesellschaft und der Normen (Notifikationsgesetz 1999 - NotifG 1999), BGBl I 1999/183.
Nov	=	Novelle
NR	=	Nationalrat
NVO	=	Verordnung des Bundesministers für Wissenschaft und Verkehr über die Nummerierung (Nummerierungsverordnung), BGBl II 416/1997
NZ	=	Notariatszeitung
oä	=	oder ähnliches
OGH	=	Oberster Gerichtshof
OLG	=	Oberlandesgericht
ÖBl	=	Österreichische Blätter für gewerblichen Rechtsschutz und Urheberrecht
ÖJZ	=	Österreichische Juristen-Zeitung
ÖStZ	=	Österreichische Steuerzeitung
POTS	=	Plain Old Telephony Service
PTV	=	Post- und Telegraphenverwaltung
RdW	=	Österreichisches Recht der Wirtschaft
RiAA	=	Recording Industry Association of America
RGBl	=	Reichsgesetzblatt

RL	=	Richtlinie der Europäischen Gemeinschaften
Rs	=	Rechtsache
Rsp	=	Rechtsprechung
RTR (GmbH)	=	Rundfunk- und Telekom Regulierungs-GmbH
Rz	=	Randzahl
RV	=	Regierungsvorlage
S	=	Satz, Seite
Slg	=	Sammlung
SMS	=	Short Message Service
sog	=	sogenannt, -e, -er, -es
SPG	=	Sicherheitspolizeigesetz, BGBl 566/1991
StF	=	Stammfassung
StGB	=	Strafgesetzbuch, BGBl 1974/60
StGG	=	Staatsgrundgesetz, RGBl 142/1867
StPO	=	Strafprozessordnung 1975, BGBl 631/1975
StenProt	=	stenographische(s) Protokoll(e)
STRÄG 2002	=	Strafrechtsänderungsgesetz 2002, BGBl I 143/2002
stRsp	=	ständige Rechtsprechung
SZ	=	Entscheidungen des österreichischen Obersten Gerichtshofes in Zivilsachen
TKG	=	Telekommunikationsgesetz
TKG 1997	=	Telekommunikationsgesetz, BGBl I 100/1997
TKG 2003	=	Telekommunikationsgesetz 2003, BGBl I 70/2003
ua	=	und andere
uä	=	und ähnliches
udgl	=	und dergleichen
UMTS	=	Universal Mobile Telecommunications System
UrhG	=	Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte (Urheberrechtsgesetz), BGBl 111/1936
UrhG-Nov	=	Urheberrechtsgesetz-Novelle
URL	=	Uniform Resource Locator
uU	=	unter Umständen
ÜVO	=	Verordnung der Bundesministerin für Verkehr, Innovation und Technologie über die Überwachung des Fernmeldeverkehrs (Überwachungsverordnung), BGBl II 418/2001
usw	=	und so weiter
UWG	=	Bundesgesetz gegen den unlauteren Wettbewerb, BGBl 448/1984
v	=	vom, von
va	=	vor allem
VersVG	=	Bundesgesetz vom 2. Dezember 1958 über den Versicherungsvertrag (Versicherungsvertragsgesetz 1958), BGBl 2/1959
vgl	=	vergleiche
VO	=	Verordnung
VfGH	=	Verfassungsgerichtshof
VVG	=	Verwaltungsvollstreckungsgesetz, BGBl 53/1991
VwGH	=	Verwaltungsgerichtshof
WAP	=	Wireless Application Protcol
wbl	=	Wirtschaftsrechtliche Blätter
Web-Dok	=	Web (Internet) Dokument

WLAN	=	Wireless Local Area Network
VStG	=	Verwaltungsstrafgesetz 1991, BGBl 52/1991
Z	=	Ziffer
zB	=	zum Beispiel
ZfRV	=	Zeitschrift für Rechtsvergleichung
ZPMRK	=	Zusatzprotokoll zur Europäischen Menschenrechtskonvention
ZPO	=	Zivilprozessordnung, RGBl 113/1895
zT	=	zum Teil

Literaturverzeichnis

Behm, Providerhaftung, in: *Lattenmayer/Behm,* Aktuelle Rechtsfragen des Internet (2001) 45
Berka, Grundrechte (1999)
Berka, Lehrbuch Grundrechte (2000)
Bertel/Venier, Strafprozessrecht[7] (2002)
Bienert-Nießl, Materiellrechtliche Auskunftspflichten im Zivilprozeß – Zugleich eine Untersuchung der prozessualen Mitwirkungspflichten der Parteien (2003)
Blume/Hammerl, E-Commerce-Gesetz Kommentar (2002)
Brandl, Telekommunikationsrecht, in: *Jahnel/Schramm/Staudegger* (Hrsg), Informatikrecht[2] 273
Brandl, Datenschutz im Internet, in: *Studiengesellschaft für Wirtschaft und Recht* (Hrsg), Internet und Recht – Rechtsfragen von E-Commerce und E-Government 111.
Brandl/Mayer-Schönberger, Die Haftung von Online-Diensten für übermittelte Inhalte, ecolex 1996, 129
Brandstetter/Schmid, Mediengesetz Kommentar[2] (1999)
Brenn (Hrsg), E-Commerce-Gesetz (2002)

Ciresa, Österreichisches Urheberrecht, 1. Lfg (1999)

Demmelbauer/Hauer, Sicherheitsrecht (2002)
Dillenz, Praxiskommentar zum österreichischen Urheberrecht und Verwertungsgesellschaftenrecht (1999)
Dittrich, Österreichisches und Internationales Urheberrecht (1998)
Dorazil/Harbich, Finanzstrafgesetz I 24. ErgLfg (2003)
Drobesch/Grosinger, Datenschutzgesetz (2000)

Ebensperger, Die Verbreitung von NS-Gedankengut im Internet und ihre strafrechtlichen Auswirkungen unter besonderer Berücksichtigung des E-Commerce-Gesetzes, ÖJZ 2002, 132

Fischer, Die Haftung der Internet-Provider (Diss Salzburg 2001), http://www.privatrecht.sbg.ac.at/forum/fischer.pdf.
Forgó/Feldner/Witzmann/Dieplinger (Hrsg), Probleme des Informationsrechts (2003)
Funk, Militärischer Eigenschutz und innere Sicherheit - Erweiterte Überwachungs- und Eingriffsmöglichkeiten im Militärbefugnisrecht, ZfV 2003/1

Haller, Music on Demand (2001)
Hauper/Keplinger, Sicherheitspolizeigesetz[2] (2001)
Hoeren/Sieber, Handbuch zum Multimediarecht

Jahnel, Datenschutz im Internet - Rechtsgrundlagen, Cookies und Web-Logs, ecolex 2001, 84
Jahnel/Schramm/Staudegger (Hrsg), Informatikrecht[2] (2003)
Jahnel, Datenschutzrecht, in: *Jahnel/Schramm/Staudegger* (Hrsg), Informatikrecht[2] 241
Jahnel, Das Auskunftsrecht nach dem Datenschutzgesetz, ZfV 1991, 243.

Kainz/Trappitsch, Praxisrelevante Fragen der Haftungsfreistellungen des ECG, ecolex 2002, 737
Kodek, Die Verwertung rechtswidriger Tonbandaufnahmen und Abhörergebnisse im Zivilverfahren, ÖJZ 2001, 287
Korinek/Holoubek (Hrsg), Österreichisches Bundesverfassungsrecht III 5. ErgLfg (2002)

Koziol Haftpflichtrecht I[3] (1997)
Koziol, Haftpflichtrecht II[2] (1984)
Koziol/Welser, Bürgerliches Recht I[12] (2002)

Lattenmayer/Behm (Hrsg), Aktuelle Rechtsfragen des Internets (2001)
Lichtenstrasser/Mosing/Otto, Wireless LAN - Drahtlose Schnittstelle für Datenmissbrauch?, ÖJZ 2003/14
Leitner, Handbuch des österreichischen Finanzstrafrechts[2] (2002)

Machacek, Die Reform des StPO-Vorverfahrens aus der Sicht des Rechtsschutzbeauftragten - Erweiterte Fassung der dem BMJ am 14. 9. 2001 erstatteten Stellungnahme des RSB, AnwBl 2002, 76
Maleczky, Das Strafrechtsänderungsgesetz 2002, JAP 2002/2003, 134
Mochar/Seidl, Internationales Verbraucherschutzrecht, ÖJZ 2003/13
Mosing, Cookies and Log Files: The "Transparent Internet User" or Data Protection on the Internet in the EU?!, http://www.it-law.at/papers/mosing_log-files_cookies_english.pdf
Mottl, Anwendbares Recht und Gerichtsstand im Internet, in: *Brenn,* ECG 134
Müllschitzky, Namensrechtliche Probleme von Domainnamen (Master Thesis 2000), http://members.aon.at/mamue/dokumente/pdf/domain_names.pdf
Muskatelz, Der Datenzugriff im Strafverfahren (2000)

Öhlinger, Verfassungsrecht[5] (2003)
Otto/Parschalk, Anzeige- und Konzessionspflicht von Internet Service Providern nach dem TKG, MR 2001, 420

Parschalk/Zuser/Otto, Telekommunikationsrecht (2002)
Philippi/Pracher, Eingriffe in die Grundrechte von Betreibern und Konsumenten von Telekommunikationsdiensten durch polizeiliche Überwachungsmaßnahmen: Zu Natur und Konsequenzen einer europäischen Überwachungsverordnung (ENFOPOL-98-Dokument), http://www.it-law.at/papers/phillipi-pra-tretter.pdf
Prachner, Datenschutz in der Telekommunikation, in: *Forgó/Feldner/Witzmann/Dieplinger* (Hrsg), Probleme des Informationsrechts (2003), 365 = http://www.it-law.at/papers/intern/mt-Pracher.Datenschutz.pdf
Primig, Verfahrensrechtliche Regelungsversuche der Telekommunikationsüberwachung auf europäischer Ebene (2002), http://www.rechtsprobleme.at/doks/primig-2-telekom-ueberwachung_europaeisch.pdf
Primig, Formalrechtliche Möglichkeiten und Grenzen nationaler Telekommunikationsüberwachung, http://www.rechtsprobleme.at/doks/primig-3-telekom-ueberwachung_national.pdf
Radtke, Rechtsbehelfe gegen die „Durchsicht" (§ 110 StPO) von EDV-Anlagen durch Strafverfolgungsbehörden, JurPC Web-Dok 173/1999 Abs 18 ff = http://www.jurpc.de/aufsatz/19990173.htm#fn1
Raschauer, Allgemeines Verwaltungsrecht (1998)
Rechberger/Simotta, Zivilprozeßrecht[6] (2003)
Reindl, Die nachträgliche Offenlegung von Vermittlungsdaten des Telefonverkehrs im Strafverfahren („Rufdatenrückerfassung"), JBl 1999, 791
Reindl, E-Commerce und Strafrecht (2003)

Schanda, Verantwortung und Haftung im Internet nach dem neuen E-Commerce-Gesetz, ecolex 2001, 920
Schmidbauer, Up and Down, http://www.internet4jurists.at/news/aktuell46.htm.
Schmidtbauer, M-Love, http://www.internet4jurists.at/news/aktuell30.htm
Schmölzer, Strafrecht, in: *Jahnel/Schramm/Staudegger* (Hrsg), Informatikrecht[2] 335
Schmölzer, Rückwirkende Überprüfung von Vermittlungsdaten im Fernmeldeverkehr - Anmerkungen zu OGH 6. 12. 1995, 13 Os 161/95 = JBl 1997, 211

Schmölzer, Prozessuale Zwangsmittel im Fernmeldewesen - Beschlagnahme oder Überwachung?, RZ 1988, 247
Schmoller, Erzwungene selbstbelastende Aussagen im Strafprozeß, Zugleich ein Beitrag zu den Beweisverwertungsverboten, JBl 1992, 69
Schwimann (Hrsg), ABGB Praxiskommentar VII[2] (1997)
Seiler, Strafprozessrecht[6] (2003)
S*pindler/Fallenböck,* Das Herkunftslandprinzip der E-Commerce-Richtlinie und seine Umsetzung in Deutschland und Österreich (Teil I), ZfRV 2002/23
Studiengesellschaft für Wirtschaft und Recht (Hrsg), Internet und Recht – Rechtsfragen von E-Commerce und E-Government (2002)
SWK, Abgaben-Rechtsmittel-Reformgesetz 2001 geht in Begutachtung Umfangreiches Finanzgerichtsgesetz als Kern der Reform Ministerialentwurf zum AbgRmRefG 2001 fertig gestellt, SWK 2001 T 112

Thiele, Umsatzsteuerliche Behandlung von Internetgeschäften in der EU und Österreich, ÖStZ 2000/697
Tonninger, Rechtsverletzung im Internet - Providerhaftung?, ecolex 1999, 251
Trawnicek/Lepuschitz, Sicherheitspolizeigesetz[3] (2000)

Venier/Ebensperger, Internet und Strafrecht, in: *Brenn,* ECG 118

Walter/Mayer, Verwaltungsverfahrensrecht[7] (1999)
Walter/Mayer, Bundesverfassungsrecht[9] (2000)
Wessely K/Eugen, Ich war es nicht! oder: Haftung für die Inanspruchnahme von Mehrwertdiensten durch Geschäftsunfähige, MR 2003, 3
Wessely W, Das Fernmeldegeheimnis - ein unbekanntes Grundrecht?, ÖJZ 1999, 491
Wessely W, Sicherheitspolizeiliche und strafprozessuale Erhebungen im Internet, ÖJZ 1996, 612
Walter (Hrsg), Europäisches Urheberrecht (2001)
Welser, Haftung für Rat, Auskunft und Gutachten – Zugleich ein Beitrag zur Bankauskunft (1983)
Wilhelm, Ich habe mich in dich verliebt - bitte ruf 0900 87654…, ecolex 2003, 73

Zankl, E-Commerce-Gesetz Kommentar und Handbuch (2002)
Zankl, Der Entwurf zum E-Commerce-Gesetz, NZ 2001, 325 (= E-Commerce-Gesetz in Sicht, AnwBl 2001, 459)
Zeder, Internet und Strafrecht, in: *Studiengesellschaft für Wirtschaft und Recht* (Hrsg), Internet und Recht – Rechtsfragen von E-Commerce und E-Government (2002) 73

Sonstige Quellen und online Datenbanken (annotiert)

http://bundesrecht.juris.de

„Deutsches RIS“, beschränkt auf das Bundesrecht (nicht vollständig!).

http://europa.eu.int

Europaserver. Zu empfehlen ist die Suche über die Tätigkeitsbereiche, da die einzelnen GD brauchbare Zusammenfassungen der Normen und sonstigen Materials bieten.

http://www.curia.eu.int

Website des EuGH bzw EuGI. Ermöglicht die Suche nach Urteilen der beiden Gerichte, zT mittels Zugriff auf die (sonst kostenpflichtige) Celex-Datenbank.

http://futurezone.orf.at

Nicht immer juristisch fundiert, aber enthält doch immer aktuelle Informationen rund um die Telekombranche. Bietet zwar keine Suchfunktion, aber die gängigen Suchmaschinen durchsuchen diese Site.

http://normative.zusammenhaenge.at/

Website von Klaus Richter, mit IT-Recht FAQs, Beiträgen zu IT-Recht und Politik, Fällen und Entscheidungen (national und international) und Materialien zum IT-Recht.

http://ris.bka.gv.at

Rechtsinformationssystem des Bundes (RIS); ermöglicht die Abfrage des Großteils des Bundes- und Landesrecht, Judikatur der Höchstgerichte, DSK udgl.

http://www.argedaten.at

Laut ihrer Website ist die Arge Daten (Österreichische Gesellschaft für Datenschutz) die wichtigste Privacy Organisation Österreichs. Sie setzt laufend Initiativen zum Schutz der Privatsphäre im Zeitalter globaler Vernetzung.

http://www.bmi.gv.at/oeffentlsicherheit/

Online-Ausgabe des Magazins des BMI „Öffentliche Sicherheit".

http://www.coe.int/portalT.asp

Website des Europarates.

http://hudoc.echr.coe.int/hudoc/

Enthält die Urteile des EGMR im Volltext in englischer und französischer Sprache

http://conventions.coe.int/Treaty/EN/cadreprincipal.htm

Treaty Office des Europarates mit Suchfunktion.

http://www.google.at ; http://www.google.de ; http://www.google.com

Suchmaschine

http://www.heise.de

Info-Portal des Heise Zeitschriften Verlag GmbH & Co. KG.

http://www.internet4jurist.at

Website von Franz Schmidtbauer, aktuelle und brauchbare Darstellung internetrelevanter Rechtsprobleme.

http://www.internet-strafrecht.de/

Website von Jürgen P Graf, Richter am deutschen Bundesgerichtshof.

http://www.ispa.at

Website des Dachverbandes der österreichischen Internet Service Provider.

http://www.it-law.at

Website der Interessensgemeinschaft it-law, dem Absolventenverein des Universitätslehrganges für Informationsrecht und Rechtsinformation. Manche Absolventen des Lehrgangs für Informationsrecht und Rechtsinformation haben hier ihre Master Thesen veröffentlicht.

http://www.lycos.at; http://www.lycos.de ; http://www.lycos.com

Suchmaschine

http://www.parlikom.gv.at

Website des österreichischen Parlaments; bietet die Abfrage der parlamentarischen Materialien ab der XX. Gesetzgebungsperiode.

http://www.rechtsprobleme.at

Laut Selbstbeschreibung ist rechtsprobleme.at eine unabhängige, kostenlos zugängliche Informationsplattform, die neben einschlägigen oberstgerichtlichen Urteilen und Nachrichten (in Zusammenarbeit mit dem E-Commerce Gütezeichen) auch Beiträge verschiedener Autoren zu Themen mit juristischem Bezug anbietet.