Curriculum Vitae

BERUFSERFAHRUNG

Ab 08/2010	Rechtsanwaltsanwärter bei **der Schönherr Rechtsanwälte GmbH** im Bereich Dispute Resolution.
Seit 10/2007	**Vizedirektor** des europäischen zentrums für e-commerce und internetrecht (www.e-center.eu) (Teilzeit).
04/2008-03/2009	Absolvierung der um drei Monate verlängerten **Gerichtspraxis** am BG für Handelssachen Wien, LG Wiener Neustadt (Strafzuteilung), LG für Zivilrechtssachen Wien und bei der StA Wien.
Seit 01/2008	Vorstandsmitglied der NGO „Asyl in Not" (www.asyl-in-not.org).
04/2007-12/2007	Absolvierung des **Zivildienstes** in der NGO „Asyl in Not" zuständig für die **Rechtsberatung und Vertretung** von Asylwerbern vor dem Bundesasylamt, dem Unabhängigen Bundesasylsenat und in fremdenpolizeilichen Causen.
10/2004-10/2007	**Wissenschaftlicher Mitarbeiter** des europäischen zentrums für e-commerce und internetrecht; Autor rechtswissenschaftlicher Studien, Gutachten und Veröffentlichungen. Seit 10/2006 **Key-Account-Assistant** für die Orange Austria Telecommunication GmbH (vormals One GmbH).
07/2004	Vierwöchiges **Internship** bei Dr. Estermann und Partner, 5230 Mattighofen, Stadtplatz 6.

AUSBILDUNG

Seit 04/2009	**Doktoratstudium.** Dissertationsthema: „Der Access-Provider in der Zwickmühle – Das Verhältnis zwischen Auskunfts- Mitwirkungs und Handlungspflichten einerseits sowie vertraglichen Schutzpflichten andererseits"
10/2002-12/2006	**Diplomstudium Rechtswissenschaften** an der Universität Wien. Abschluss als **drittbester des Jahrgangs.**
10/2001-10/2002	Studium der Theaterwissenschaft und Philosophie an der Universität Wien.
09/1994-06/2001	**Bundesrealgymnasium** Braunau/Inn. Fremdsprachenkenntnisse erworben in Englisch, Französisch und Italienisch.

AUSZEICHNUNGEN

10/2007	Ehrung als **drittbester Jahrgangsabsolvent** des Diplomstudiums für Rechtswissenschaften im Rahmen des „Best of the Best Programms".
09/2007	Verleihung des mit 3000 Euro dotierten **D.A.S.-Förderpreises 2006** für die Arbeit „Das Bundesgesetz über den Fernabsatz von Finanzdienstleistungen"

PUBLIKATIONEN, MEDIENBEITRÄGE UND VORTRÄGE

06/2010	§ 87b Abs 3 UrhG: Verfassungs- und gemeinschaftsrechtswidrig? Gemeinsam mit Stephan Steinhofer, erschienen in der Juli-Ausgabe des ecolex 2010.
03/2010	Mitarbeit an Zankl, Bürgerliches Recht, 5. Auflage 2010, erschienen bei Facultas-WUV.
10/2009	Zwischen Urheber und Kunde: Provider in der Zwickmühle, gemeinsam mit Stephan Steinhofer, Die Presse vom 4.10.2009.
09/2009	Innovation und internationale Rechtspraxis, Festschrift zum 50. Geburtstag von Prof. Dr. Wolfgang Zankl, herausgegeben gemeinsam mit Lukas Feiler, erschienen bei Facultas-WUV.
05/2009	Seminarvortrag für die IDC Austria zum Thema Datenschutz.

03/2009	Keine Chance gegen Facebook-Spionage, Interview, Die Presse vom 3.3.2009.
03/2009	Auf dem Weg zum Überwachungsstaat? Output März 2009.
02/2009	Beiträge in Zankl (Hrsg), Auf dem Weg zum Überwachungsstaat? Erschienen bei Facultas-WUV.
01/2008	Mitarbeit an Zankl, Bürgerliches Recht, 4. Auflage 2008, erschienen bei Facultas-WUV.
09/2007	Das FernFinG (Herausgegeben von der D.A.S.-Rechtsschutz-Versicherungs-AG).
06/2007	Vorratsdatenspeicherung – Kommt der Überwachungsstaat? Gemeinsam mit Lukas Feiler, Philipp Krautschneider und Terezia Stuhl, Anwalt Aktuell, Juni 2007.
01/2006	Mitarbeit an Zankl, Bürgerliches Recht, 3. Auflage 2006, erschienen bei Facultas-WUV.

Abstract

Die Rechtsordnung beinhaltet eine Reihe von Bestimmungen, die Access-Provider zur Auskunft bzw Mitwirkung verpflichten. Die Auskunftspflicht kann sowohl gegenüber Behörden (zB im Rahmen der §§ 134ff StPO) als auch gegenüber Privaten (zB aufgrund § 87b Abs 3 UrhG) bestehen. Die in dieser Arbeit abgehandelten Bestimmungen haben gemein, dass sie auf die Ermittlung personenbezogener Daten abzielen und somit einen Eingriff in die Privatsphäre des Kunden des Access-Providers darstellen. Der Schutz der Privatsphäre ergibt sich zum einen aus gesetzlichen Bestimmungen, die vor allem im TKG 2003 und im DSG 2000 zu finden sind. Zum anderen ist der Access-Provider seinem Kunden aufgrund des zwischen diesen bestehenden *vinculum iuris* überdies auch vertraglich zur Wahrung seiner Privatsphäre verpflichtet. Die vorliegende Arbeit konzentriert sich auf das Verhältnis zwischen dem Access-Provider und seinem Kunden und untersucht die vertraglichen Pflichten des Access-Providers zum Schutz der Privatsphäre seines Kunden.

Die vertraglichen Verpflichtungen hinsichtlich des Schutzes der Privatsphäre des Kunden stehen in engem Zusammenhang zu den einschlägigen gesetzlichen Regelungen. Das TKG 2003 unterscheidet in Anlehnung an die EK-Datenschutzrichtlinie zwischen verschiedenen Datenkategorien, für die jeweils unterschiedliche Schutzbestimmungen bestehen. So ist die Vertraulichkeit des Inhalts von Nachrichten besonders gut geschützt und ein Eingriff nur *„aufgrund eines richterlichen Befehls in Gemäßheit bestehender Gesetze*" zulässig (Art 10a StGG). Verkehrsdaten wie etwa IP-Adressen genießen nach einem (mE zutreffenden) Teil der Lehre und Rechtsprechung zwar nicht einen ganz so hohen Schutz, werden vom TKG aber stärker geschützt, als bloße Stammdaten wie etwa Name und Anschrift einer Person. Wird im Zuge der Erfüllung eines Auskunftsbegehrens zwischen Daten unterschiedlich hoher Schutzkategorien ein Zusammenhang hergestellt, sind mE stets die Bestimmungen der jeweils höheren Schutzkategorie zu beachten. Ist beispielsweise der Inhalt einer Nachricht bekannt (Inhaltsdaten) und soll der Name des Senders (Stammdaten) vom Access-Provider bekannt gegeben werden, ist ein richterlicher Befehl nötig, obwohl nur ein Stammdatum beauskunftet wurde. Dies ergibt sich aus teleologischen Erwägungen zu der Bestimmung, die das höher bewertete Datum schützt. Im genannten Beispiel wird durch die Auskunft bekannt, wer eine Nachricht mit bestimmtem Inhalt verschickte – eine Information die das Fernmeldegeheimnis mE auch schützen will.

Die Bestimmungen des TKG 2003 zum Datenschutz beruhen weitestgehend auf der EK-Datenschutzrichtlinie und präzisieren die aus dem

allgemeinen Datenschutzrecht bekannten Grundsätze auf dem Sektor der elektronischen Kommunikation. Zwei wichtige Prinzipien des Datenschutzrechts sind etwa der Grundsatz, dass jeder grundsätzlich über die ihn betreffenden Datenverwendungen umfassend im Bilde sein soll oder das Zweckbindungsprinzip. Nach Letzterem dürfen Daten nur für jene Zwecke verwendet werden, zu denen sie ursprünglich angelegt wurden. Diesen Prinzipien wurden bei der Entwicklung vertraglicher Schutzpflichten des Access-Providers besondere Beachtung geschenkt.

Die vorliegende Arbeit hat einige Auslegungsschwierigkeiten aufgezeigt und einer Lösung zuzuführen versucht, die sich bei der Interpretation von Bestimmungen des TKG 2003 oder aus dem Regelungszusammenhang zu Auskunftsbestimmungen ergeben. So sind die für die meisten Auskunftsbegehren benötigten Verkehrsdaten in der Mehrzahl der Fälle unmittelbar nach Verbindungsbeendigung zu löschen oder zu anonymisieren, es sei denn, sie werden für Verrechnungszwecke benötigt. Ausnahmebestimmungen sind möglich, müssen jedoch, um als Ausnahmebestimmungen iSd Art 15 EK-Datenschutzrichtlinie zu gelten, nach der aktuellen Entscheidung des OGH in der Sache *LSG gegen Tele 2* eine ausdrückliche Speicheranordnung treffen. Die vorliegende Arbeit zeigt etwa, weshalb Auskunftsbestimmungen wie jene des SPG, die keine ausdrückliche Speicheranordnung treffen, dennoch als Ausnahmebestimmungen iSd Art 15 EK-Datenschutzrichtlinie gelten können und somit nicht leer laufen.

Die den Access-Provider treffenden Schutzpflichten hinsichtlich der Privatsphäre seines Kunden lassen sich mittels ergänzender Vertragsauslegung unter Orientierung am Prinzip von Treu und Glauben konstruieren. Dabei wurden die erkennbaren Wertungen des Gesetz- bzw Richtliniengebers auf dem Gebiet des Datenschutzrechts berücksichtigt und der Vertragsergänzung zugrunde gelegt. Eine der wichtigsten in dieser Arbeit entwickelten vertraglichen Pflichten ist wohl die Benachrichtigungspflicht des Access-Providers. Soweit es ihm nicht verboten ist oder er das Risiko eingeht, sich straf- bzw haftbar zu machen, hat er seinen Kunden über die Erfüllung eines Auskunftsbegehrens zu informieren. Die Informationspflicht bringt für den Access-Provider keinen hohen Aufwand mit sich und ist daher wirtschaftlich zu rechtfertigen. Sie ergibt sich zudem aus einer – soweit ersichtlich – bislang noch nie erwogenen Auslegung des § 96 Abs 3 TKG 2003. Die Informationspflicht entfällt dort, wo den Auskunftswerber eine eindeutige Pflicht zur Information des Betroffenen trifft wie in der StPO. Sie entspricht dem erwähnten Prinzip, dass der Betroffene stets über die ihn betreffenden Datenverwendungen in Kenntnis sein soll, um seine Rechte wahrnehmen zu können. Eine Pflicht, sich im Interesse des Kunden gegen Auskunftsbegehren mittels Rechtsbehelfen zur Wehr zu setzen, trifft den Access-Provider aus Zumutbarkeitsgründen nicht. Je nachdem, wie die Begründungspflichten

des Auskunftswerbers dem Gesetz nach beschaffen sind, sehen auch die Prüfpflichten des Access-Providers hinsichtlich des Auskunftsbegehrens unterschiedlich aus. Soweit das Gesetz eine Begründung des Auskunftsbegehrens verlangt, hat der Access-Provider das Auskunftsbegehren auf dessen Vollständigkeit zu prüfen und die Auskunft bzw Mitwirkung nötigenfalls zu verweigern. Weiters bestehen Verweigerungspflichten in jenen Fällen, in denen der Access-Provider die zur Auskunftserfüllung erforderlichen Daten zwar de facto noch vorrätig hat, sie aufgrund der Bestimmungen des TKG 2003 jedoch bereits hätte löschen müssen.

Die gezeigten Schutzpflichten werden vom Access-Provider geschuldet wie jede andere vertragliche Pflicht. Diese Arbeit brachte das Ergebnis, dass für das Institut der positiven Vertragsverletzungen und dazu geltende Sonderregelungen im Gefüge des ABGB kein Platz ist. Das Institut der positiven Vertragsverletzung geht auf eine Erfindung des deutschen Juristen *Hermann Staub* zu Beginn des vergangenen Jahrhunderts zurück, der eine Lücke im BGB vermutete und diese mittels Analogie schloss. Wie gezeigt werden konnte, besteht diese Lücke weder im BGB und noch weniger im ABGB, weshalb die Verletzung von Schutzpflichten unter das positive Schadenersatz- und Leistungsstörungsrecht subsumiert werden kann. Die Schutzpflichten können stets nur auf eine endgültige (Unmöglichkeit) oder vorübergehende Art (Verzug) verletzt werden. Daher stehen bei Schutzpflichtverletzungen mE entgegen der hM grundsätzlich die in den §§ 918ff ABGB statuierten Rechtsbehelfe zu. Das gilt insbesondere auch für Rücktrittsrechte. Diese können jedoch ausnahmsweise ausscheiden, sofern sich deren Ausübung gemessen an der Schwere der Schutzpflichtverletzung als missbräuchlich erweist (§ 1295 ABGB). Die Schutzpflichten (etwa zur Benachrichtigung) können mE auch gesondert eingeklagt werden, sofern sie ausreichend bestimmt und fällig sind. Sofern die Verletzung der Schutzpflichten zu Vermögensschäden führt, ist der Access-Provider zu deren Ersatz verpflichtet. Die Prüfung von Ersatzansprüchen kann jedoch in einigen Fällen – etwa wenn die im Vermögen des Kunden eingetretene Vermögensminderung die Folge einer gegen ihn verhängten Strafe darstellt – ergeben, dass kein Rechtswidrigkeitszusammenhang vorliegt. Bei besonders erheblichen Verletzungen der Privatsphäre besteht gem § 1328a ABGB auch ein Anspruch auf den Ersatz des dadurch erlittenen immateriellen Schadens.

universität wien

DISSERTATION

Der Access-Provider in der Zwickmühle – das Verhältnis zwischen Handlungs-, Mitwirkungs- und Auskunftspflichten auf der einen und vertraglichen Schutzpflichten auf der anderen Seite

eingereicht an der
rechtswissenschaftlichen Fakultät
der Universität Wien

von

Mag. Maximilian Raschhofer

zur Erlangung des akademischen Grades
Doctor iuris (Dr. iur.)

Wien, im Juli 2010

Studienkennzahl: A 083 101
Dissertationsgebiet: Rechtswissenschaften
Erstbegutachter: ao. Univ.-Prof. Dr. Wolfgang Zankl
Zweitbegutachter: V.-Prof. Dr. Friedl Weiss

Inhaltsverzeichnis

Abkürzungsverzeichnis

aA	anderer Ansicht
AA	Abänderungsantrag
aaO	am angegebenen Ort
ABGB	Allgemeines Bürgerliches Gesetzbuch
ABl	Amtsblatt der Europäischen Union
Abs	Absatz
AcP	Archiv für die civilistische Praxis (deutsche Zeitschrift)
aF	alte Fassung
AG	Aktiengesellschaft
AGB	Allgemeine Geschäftsbedingungen
AHG	Amtshaftungsgesetz
aM	anderer Meinung
Anm	Anmerkung
AnwBl	Österreichisches Anwaltsblatt (Zeitschrift)
AöR	Archiv des öffentlichen Rechts (Zeitschrift)
Arb	Sammlung arbeitsrechtlicher Entscheidungen
ArbVG	Arbeitsverfassungsgesetz
arg	argumento (folgt aus)
Art	Artikel
ÄrzteG	Ärztegesetz
BB	Betriebs-Berater (deutsche Zeitschrift)
BG	Bundesgesetz
BGBl	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHZ	Entscheidungen des Bundesgerichtshofs in Zivilsachen
BlgNR	Beilagen zu den stenographischen Protokollen des Nationalrats
BlgHH	Beilagen zu den stenographischen Protokollen des Herrenhauses
BMI	BundesministerIn für Inneres
BMJ	BundesministerIn für Justiz
BMSK	Bundesministerium für Arbeit, Soziales und Konsumentenschutz
BMVIT	BundesministerIn für Verkehr, Innovation und Technologie
BVerfG	Bundesverfassungsgericht
B-VG	Bundes-Verfassungsgesetz
bzw	beziehungsweise
CD	Compact Disc
cic	culpa in contrahendo
DDR	Deutsche Demokratische Republik
CR	Computer und Recht (Zeitschrift)
d	der, die, das
dh	das heißt
dies	dieselbe
DSK	Datenschutzkommission
DSG	Datenschutzgesetz
dt	deutsch/e/r/s
DuD	Datenschutz und Datensicherheit (Zeitschrift)
EB	Erläuternde Bemerkungen

ECG	E-Commerce-Gesetz
ecolex	Fachzeitschrift für Wirtschaftsrecht
EFSlg	Sammlung ehe- und familienrechtlicher Entscheidungen
EG	Europäische Gemeinschaft
EGMR	Europäischer Gerichtshof für Menschenrechte
EK	Elektronische Kommunikation
ELR	European Law Reporter (Zeitschrift)
EMRK	Europäische Menschenrechtskonvention
ErgLf	Ergänzungslieferung
Erl	Erläuterungen
etc	et cetera
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EuGRZ	Europäische Grundrechtezeitschrift
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
EvBl	Evidenzblatt der Rechtsmittelentscheidungen
EWG	Europäische Wirtschaftsgemeinschaft
ff	und der (die) folgende(n)
FinStrG	Finanzstrafgesetz
FJ	Finanzjournal
FN	Fußnote
FS	Festschrift
gem	gemäß
GmbH	Gesellschaft mit beschränkter Haftung
GP	Gesetzgebungsperiode
GPS	Global Positioning System
GRURInt	Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil
hA	herrschende Ansicht
HH	Herrenhaus
HHB	HHB
hL	herrschende Lehre
hM	herrschende Meinung
Hrsg	Herausgeber
idF	in der Fassung
ie	id est
ieS	im engeren Sinne
iFamZ	interdisziplinäre Fachzeitschrift für Familienrecht
IKT	Informations- und Kommunikationstechnolgie
IMEI	International Mobile Equipment Identity
Immolex	Zeitschrift für neues Miet- und Wohnrecht
ImmZ	Österreichische Immobilienzeitung
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
iR	in Rente
iSd	im Sinne des/der
iwS	im weiteren Sinne
JA	Justizausschuss, Juristische Arbeitsblätter (Zeitschrift)
JAB	Bericht des Justizausschusses
JAP	Juristische Ausbildung und Praxis (Zeitschrift)

JBl	Juristische Blätter (Zeitschrift)
JRP	Journal für Rechtspolitk (Zeitschrift)
JSt	Journal für Strafrecht (Zeitschrift)
Jura	Juristische Ausbildung (Zeitschrift)
JuS	Juritische Schulung (Zeitschrift)
jusIT	IT-Recht, Datenschutz, Rechtsinformation (Zeitschrift)
JZ	Juristenzeitung (deutsche Zeitschrift)
K&R	Kommunikation und Recht (Zeitschrift)
KritV	Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft
LBS	Location Based Service
leg cit	legis citatae
lit	litera
MBG	Militärbefugnisgesetz
MDR	Monatszeitschrift für Deutsches Recht
ME	Ministerialentwurf
mE	meines Erachtens
MedienG	Mediengesetz
MietSlg	Sammlung mietrechtlicher Entscheidungen
MMR	Multimedia und Recht (Zeitschrift)
MR	Medien und Recht (Zeitschrift)
MR-Int	Medien und Recht International Edition
mwN	mit weiteren Nachweisen
nF	neue Fassung
NJW	Neue Juristische Wochenschrift
NotifG	Notifikationsgesetz
Nov	Novelle
Nr	Nummer
NR	Nationalrat
NStZ	Neue Zeitschrift für Strafrecht
NZ	Österreichische Notariatszeitung
oä	oder ähnliche
ÖBA	Österreichisches Bankarchiv (Zeitschrift)
ÖBl	Österreichische Blätter für gewerblichen Rechtsschutz und Urheberrecht
OGH	Oberster Gerichsthof
ÖJT	Österreichisches Juristentag
ÖJZ	Österreichische Juristenzeitung
OLG	Oberlandesgericht
ÖZW	Österreichische Zeitschrift für Wirtschaftsrecht
ÖZöffR	Österreichische Zeitschrift für öffentliches Recht
PDF	Portable Document Format
RdA	Recht der Arbeit (Zeitschrift)
RdM	Recht der Medizin (Zeitschrift)
RDV	Recht der Datenverarbeitung (Zeitschrift)
RdW	Recht der Wirtschaft
RAO	Rechtsanwaltsordnung
RFC	Request for Comments (technische Standards für das Internet)
RG	Reichsgericht
RGZ	Entscheidungen des (deutschen) Reichsgerichts in Zivilsachen
Rl	Richtlinie

Rs	Rechtssache
RV	Regierungsvorlage
Rz	Randziffer
RZ	Österreichische Richterzeitung
S	Siehe, Seite
s	siehe
Sess	Session
Slg	Sammlung
SIM	Subscriber Identity Module
SMS	Short Message Service
SPG	Sicherheitspolizeigesetz
SSt	Entscheidungen des österreichischen OGH in Strafsachen
SSV-NF	Entscheidungen des OGH in Sozialrechtssachen
StGB	Strafgesetzbuch
StGG	Staatsgrundgesetz
StPO	Strafprozessordnung
SZ	Entscheidungen des OGH in Zivilsachen
TKG	Telekommunikationsgesetz
U	Urteil
ua	und andere
uä	und ähnliche
ÜKVO	Überwachungskostenverordnung
UrhG	Urheberrechtsgesetz
usw	und so weiter
uva	und viele andere
uvm	und viele mehr
UVS	Unabhängiger Verwaltungssenat
UWG	Bundesgesetz gegen den unlauteren Wettbewerb
VDS	Vorratsdatenspeicherung-Rl
VfGH	Verfassungsgerichtshof
VfSlg	Sammlung der Erkenntnisse und wichtigsten Beschlüsse des VfGH
vgl	vergleiche
VO	Verordnung
Vor	Vorbemerkungen
vs	versus (gegen)
VStG	Verwaltungsstrafgesetz
VwSlg	Erkenntnisse und Beschlüsse des Verwaltungsgerichtshofes
wbl	wirtschaftsrechtliche Blätter (Zeitschrift)
wobl	Wohnrechtliche Blätter (Zeitschrift)
Z	Ziffer
Zak	Zivilrecht aktuell (Zeitschrift)
ZAS	Zeitschrift für Arbeitsrecht und Sozialrecht
zB	zum Beispiel
ZBl	Zentralblatt für die juristische Praxis
ZfRV	Zeitschrift für Rechtsvergleichung
ZfV	Zeitschrift für Verwaltung
ZgesStw	Zeitschrift für die gesamte Staatswissenschaft
ZGR	Zeitschrift für Unternehmens- und Gesellschaftsrecht
ZollR-DG	Zollrechts-Durchführungsgesetz

ZPO	Zivilprozessordnung
zT	zum Teil
ZUM	Zeitschrift für Urheber- und Medienrecht
ZVR	Zeitschrift für Verkehrsrecht

1. Einleitung und Ausblick

Vielen wird noch die vom ehemaligen Präsidenten des VfGH stammende Äußerung in Erinnerung sein, mit der er vor etwas mehr als zwei Jahren für Aufhorchen sorgte: Österreich sei auf dem Weg zu einem Überwachungsstaat nach dem Vorbild der DDR[1]. War das lediglich übertriebene Polemik, wie man sie aus der Tagespolitik nur zu gut kennt? Oder sollte man im Vertrauen auf seine Expertise in Panik geraten?

Fakt ist, dass sich in den letzten Jahren eine zunehmende legislatorische Tätigkeit in punkto Überwachungsmaßnahmen auf dem Sektor der Informations- und Kommunikationstechnologie feststellen lässt. Eingriffe in die Privatsphäre werden sowohl auf europäischer als auch auf österreichischer Ebene rasch vorangetrieben. Dabei werden immer häufiger Access-Provider in die Pflicht genommen, die ihren Kunden Zugang zu elektronischen Kommunikationsnetzen gewähren. So wäre in Österreich bereits bis 15.3.2009 die Richtlinie zur Vorratsdatenspeicherung[2] (fortan Vorratsdatenspeicherungsrichtlinie) vollständig umzusetzen gewesen. Diese zielt vereinfacht formuliert darauf ab, dass jeder Access-Provider zu Zwecken der Ermittlung, Feststellung und Verfolgung schwerer Straftaten für eine Dauer von sechs Monaten bis zwei Jahren speichern muss, wer wann mit wem – und im Falle mobiler Endgeräte – von wo aus kommuniziert hat[3]. Da die Richtlinie bis dato nicht in innerstaatliches Recht umgesetzt wurde, ist derzeit ein Vertragsverletzungsverfahren gegen die Republik Österreich anhängig[4], in welchem diese auch mit der Grundrechtswidrigkeit der Richtlinie argumentierte. Zu Beginn des Jahrs 2008 trat eine Novelle des Sicherheitspolizeigesetzes in Kraft, mit der weitgehende Überwachungsbefugnisse hinsichtlich der Benutzung des Internet und überdies auch die Befugnis eingeführt wurden, Menschen in bestimmten Situationen anhand ihrer mobilen Endgeräte zu lokalisieren. Diese Befugnisse werden von den Sicherheitsbehörden ohne gerichtliche Kontrolle und ohne Information des

---

[1] http://oe1.orf.at/inforadio/81240.html (Stand April 2010); das Interview kann dort auch als Audiofile abgerufen werden.

[2] Richtlinie 2006/24/EG des Europäischen Parlamentes und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG.

[3] Vgl dazu etwa *Boka/Feiler,* in *Zankl* (Hrsg), Auf dem Weg zum Überwachungsstaat? (2009) 126ff; Feiel, Datenspeicherung auf Vorrat und Grundrechtskonformität, JusIT 2008, 97ff; *Gitter/Schnabel*, Die Richtlinie zur Vorratsspeicherung und ihre Umsetzung in das nationale Recht, MMR 2007, 411ff; *Kosta/Dumortier*, The Data Retention Directive and the principles of European data protection legislation, MR-Int 2007, 130ff, 1; *Otto/Seitlinger*, Die "Spitzelrichtlinie", MR 2006, 227 ff; *Westphal*, Die neue EG-Richtlinie zur Vorratsdatenspeicherung, EuZW 2006, 555; *ders,* Die Richtlinie zur Vorratsdatenspeicherung von Verkehrsdaten – Neues aus Brüssel zum Verhältnis von Sicherheit und Datenschutz in der Informationsgesellschaft, juridikum 2006, 34ff.

[4] Klage der Kommission vom 28.5.2009, C-189/09, ABl L 2009/105, 54.

Betroffenen ausgeübt. Seit nun schon mindestens zwei Jahren will auch in Österreich die Diskussion über die Einführung der so genannten „Online-Durchsuchung“[5] und so genannter „Internetsperren“[6] nicht mehr abreißen.

Aber nicht nur der Staat streckt seine Hand nach immer mehr Daten aus und wendet sich dabei hilfesuchend an die Access-Provider. Auch Private sind teilweise auf deren Hilfe angewiesen, um ihre Ansprüche durchsetzen zu können. Man denke hierbei insbesondere an Urheber, die Auskünfte der Access-Provider benötigen um mutmaßliche Urheberrechtsverletzer im Zusammenhang mit file-sharing-Netzwerken identifizieren und verfolgen zu können.

Dass Access-Provider zunehmend in den Fokus der Aufmerksamkeit staatlicher wie nicht staatlicher Akteure geraten, liegt wohl an der stetig wachsenden Bedeutung der elektronischen Kommunikation. Wie das deutsche Bundesverfassungsgericht in seiner Entscheidung zur Online-Durchsuchung von vor knapp zwei Jahren festhielt, hat die Nutzung der Informationstechnik für die Persönlichkeit und die Entfaltung des Einzelnen eine früher nicht absehbare Bedeutung erlangt[7]. So ist der Anteil von Haushalten mit Internetzugang in Österreich im Zeitraum 2002 bis 2009 von 33,5 auf 69,8 % gestiegen. Bei den Haushalten mit Breitbandverbindungen konnte im selben Zeitraum eine Steigerung von 10,3 auf 57,8 % verzeichnet werden[8].

Je bedeutsamer der alltägliche Datenaustausch über elektronische Kommunikationsnetze wird, desto mehr Informationen muss der Access-Provider verarbeiten. So gelangt er in den Besitz eines stetig anwachsenden Bestands an Inhalts-, Verkehrs- und Standortdaten, der über seine Kunden immer mehr auszusagen vermag. Mit der steigenden Bedeutung elektronischer Kommunikation wird das aus den dabei anfallenden Datenmengen ablesbare Bild immer schärfer. Dies hielt auch das deutsche Bundesverfassungsgericht in der kürzlich ergangenen Entscheidung zur

---

[5] Vgl hiezu etwa den Bericht der *Interministeriellen Arbeitsgruppe „Online-Durchsuchung“ des BMI und BMJ,* Erweiterung des Ermittlungsinstrumentariums zur Bekämpfung schwerer, organisierter und terroristischer Kriminalitätsformen („Online-Durchsuchung“) (2008).

[6] Diese wurden etwa von der BMJ in einem Interview vom 29.9.2009 (abrufbar unter http://www.youtube.com/watch?v=kfgT0pYNht8 [Stand April 2010]) als geeignetes Mittel im Kampf gegen die Verbreitung pornografischer Darstellungen Minderjähriger über das Internet genannt.

[7] BVerfG 27.2.2008, 1 BvR 370/07 Rz 170ff; vgl dazu *Zerbes,* Das Urteil des deutschen Bundesverfassungsgerichts zur Online-Durchsuchung und Online-Überwachung, ÖJZ 2008, 834ff.

[8] *Statistik Austria*, Europäische Erhebungen über den IKT-Einsatz in Haushalten 2002-2009, erstellt am: 31.08.2009, abrufbar unter: http://www.statistik.at/web_de/statistiken/informationsgesellschaft/ikt-einsatz_in_haushalten/index.html (Stand April 2010).

Vorratsdatenspeicherung dankenswerterweise in aller Deutlichkeit fest[9]. Hinzu kommt, dass die Identifizierung und Ausforschung von Personen anhand ihrer digitalen Spuren im Vergleich zu herkömmlichen Ermittlungsmethoden meist einfacher und rascher vonstatten geht, vorausgesetzt, der Access-Provider verfügt über ausreichendes Datenmaterial, das er zu diesen Zwecken verarbeiten darf.

Der Ruf nach immer mehr Auskunfts-, Mitwirkungs- und Handlungspflichten des Access-Providers wird großteils mit sehr ähnlichen, teils schon nahezu phrasenhaft anmutenden Argumenten gerechtfertigt. So berufen sich normsetzende Organe meist auf eine Steigerung der Sicherheit, oder gar nur auf eine mit Überwachungsmaßnahmen einhergehende Steigerung des subjektiven Sicherheitsgefühls[10]. Als Reaktion auf die wiederholten Terroranschläge[11] in den vergangenen Jahren wird das Gleichgewicht zwischen Freiheit und Ordnung immer weiter zu Gunsten letzterer destabilisiert, wobei oft übersehen wird, dass ebendiese (Über)reaktion im Plan terroristischer Aktivitäten meist inbegriffen, ja vielleicht sogar deren Hauptziel ist[12]. So meinte bereits *Ulrike Meinhof,* dass es die Strategie des „antiimperialistischen Kampfes" sei, dass „*durch die Defensive, die Reaktion des Systems, die Eskalation der Konterrevolution [...] der Feind sich kenntlich macht, sichtbar – und so, durch seinen eigenen Terror, die Massen gegen sich aufbringt, die Widersprüche verschärft, den revolutionären Kampf zwingend macht*[13]." Zur Begründung der Inpflichtnahme von Access-Providern durch Private wird regelmäßig auf deren grundrechtliche geschützte Positionen, etwa auf deren Grundrechte auf Eigentum und auf eine wirksame Beschwerde verwiesen.

Die in diesem Zusammenhang aufgeworfenen grund-, verfassungs- und strafrechtlichen Fragen sind Gegenstand vieler spannenden Abhandlungen auf den Gebieten des (europäischen) öffentlichen Rechts[14]. Erkenntnisse, die dort erzielt wurden, werden freilich auch in der vorliegenden Abhandlung nicht außer Betracht bleiben

---

[9] BVerfG 2.3.2010; 1 BvR 256/08, Rz 210ff.

[10] Vgl zu diesem Begriff etwa *Schewe,* Subjektives Sicherheitsgefühl in *Lange* (Hrsg), Wörterbuch der inneren Sicherheit, Wiesbaden (2006) 322ff.

[11] So wird etwa im 10 Erwägungsgrund zur Vorratsdatenspeicherungsrichtlinie ausdrücklich auf die Terroranschläge in London 2005 Bezug genommen.

[12] Vgl etwa *Maier*, Strafrecht – Kriegsrecht – Ausnahmezustand? Der Rechtsstaat vor der Hausforderung des Terrorismus, JRP 27 (30) mwN.

[13] *Meinhof,* Die Dialektik von Revolution und Konterrevolution, in *Internationales Komitee zur Verteidigung politischer Gefangener in Westeuropa* (Hrsg), Letzte Texte von Ulrike (1976) 57 (57) abrufbar unter: http://www.scribd.com/doc/24588805/Letzte-Texte-von-Ulrike-Meinhof (Stand April 2010)

[14] Vgl etwa *Zankl* (Hrsg), Auf dem weg zum Überwachungsstaat? (2009).

können, da sie mit den hier interessierenden zivilrechtlichen Fragen oft in engem Zusammenhang stehen.

Diese Arbeit wird sich jedoch auf das komplizierte Spannungsverhältnis[15] konzentrieren, welchem sich der Access-Provider ausgesetzt sieht. Einerseits hat er ein Interesse daran, Auskunftsansprüchen zu entsprechen, um sich vor Sanktionen zu bewahren, die von den Auskunftswerbern ausgehen könnten. In jüngster Vergangenheit hatten sich sowohl OGH als auch EuGH mit komplizierten Rechtsfragen auseinanderzusetzen, die im Rahmen von Prozessen aufgeworfen wurden, in denen Urheber Access-Provider auf die Offenlegung der Identität mutmaßlicher Urheberrechtsverletzer geklagt hatten. Andererseits verbindet den Access-Provider mit seinem Kunden ein Vertrag, ein *vinculum iuris,* das ihn letzterem gegenüber zur Treue, Sorgfalt und zum Schutz seiner Rechtsgüter verpflichtet. Die Frage ist, wie weit diese Verpflichtungen gehen.

Noch vor einem Eingehen auf den konkreten Inhalt der Schutzpflichten wird jedoch der Frage nachgegangen, welche Sanktionen die Verletzung der Schutzpflichten nach sich zieht. Zu klären ist etwa, inwieweit allfällige Pflichtverletzungen auf Seiten des Access-Providers seinem Vertragspartner Instrumente in die Hand geben, sich vorzeitig aus dem Verhältnis zu lösen. Dabei werden insbesondere im Bezug auf die zustehenden Rücktrittsrechte Ansichten vertreten, die von der hL und Rechtsprechung abweichen.

Sodann wird das Vertragsverhältnis zwischen dem Access-Provider und seinem Kunden vorgestellt. In diesem Zusammenhang sind auch die gesetzlichen datenschutzrechtlichen Verpflichtungen des Access-Providers gegenüber seinem Kunden zu skizzieren. Es werden die einzelnen im TKG definierten Datenkategorien und das für sie geltende Schutzniveau vorgestellt.

In einem weiteren Kapitel wird sodann der Inhalt der Schutzpflichten erörtert. Dabei werden zunächst die dogmatischen Grundlagen vertraglicher Schutzpflichten erörtert und näher beleuchtet. Weiters wird das Schutzobjekt der vertraglichen Pflichten, die Privatsphäre, kurz skizziert. Sodann wird mittels ergänzender Vertragsauslegung der Inhalt der Schutzpflichten iS einer Informationspflicht gegenüber dem Kunden konkretisiert. Dabei geht es um die Frage, inwieweit der Access-Provider aufgrund der vertraglichen Beziehung zu seinem Kunden verpflichtet sein soll, diesen darüber zu informieren, wenn bei ihm Behörden oder private Dritte Auskunft über

---

[15] *Raschhofer/Steinhofer,* Zwischen Urheber und Kunde: Provider in der Zwickmühle, Die Presse vom 5.10.2009, abrufbar unter http://diepresse.com/home/techscience/internet/512779/index.do (Stand April 2010).

personenbezogene Daten des Kunden begehrt haben. Diese Pflicht lässt sich losgelöst von den unterschiedlichen konkreten Auskunftsbestimmungen darstellen.

Die sonstigen Schutzpflichten wie etwa die Pflicht zur Prüfung von Auskunftsbegehren werden im Zusammenhang mit den im Einzelnen dargestellten Auskunftsbestimmungen behandelt. Dabei werden neben bekannteren Bestimmungen wie jenen in der StPO oder im SPG auch eher unbekannte Auskunftsbefugnisse wie jene des Zollrechts-Durchführungsgesetzes abgehandelt. In diesem Zusammenhang wird auch die Frage behandelt werden, inwieweit der Access-Provider in Bezug auf die einzelnen Auskunftsbestimmungen zur Prüfung der Auskunftsbegehren bzw zur Verweigerung der Erfüllung bzw Mitwirkung verpflichtet ist. Auch der Frage, ob eine Pflicht zur Ergreifung von Rechtsbehelfen zum Schutz der Privatsphäre des Kunden besteht, wird im Zusammenhang mit den konkreten Auskunftsbestimmungen nachgegangen.

2. Grundlegende Begriffsbestimmungen

Da, wie sogleich zu zeigen ist, selbst bei so elementaren Begriffen des Schuldrechts wie jenen der Nebenleistungs- bzw Schutz- und Sorgfaltspflichten innerhalb der Literatur und Lehre Auffassungsunterschiede bestehen, soll an dieser Stelle eine Begriffsanalyse vorgenommen werden, um Missverständnissen von Anbeginn an vorzubeugen. Ein etwas genauerer Blick in die Tiefen des Schuldrechts zeigt bereits deutliche Unterschiede in der verwendeten Terminologie. Während beispielsweise die am nicht vertragsgemäßen weil verdorbenen Futter verendeten Tiere als das klassische Beispiel[16] eines Mangelfolgeschadens gelten[17], wird dieser Schaden von manchen auch als Begleitschaden bezeichnet[18]. Diese divergierenden und – wie dieses Beispiel zeigt – teilweise sogar gegenteiligen Begriffsverwendungen haben bei mir[19] im Zuge des Abfassens dieser Arbeit Verwirrung gestiftet, weshalb ich es für sinnvoll halte, dem Leser zu Anbeginn mein Begriffsverständnis darzulegen.

2.1. Andere Pflichten als Hauptleistungspflichten

2.1.1. Nebenleistungspflichten

Die Schuldner treffen nicht nur die das Vertragsverhältnis in erster Linie kennzeichnenden Hauptleistungspflichten, sondern auch Nebenleistungspflichten. Im Allgemeinen wird zwischen äquivalenten (selbstständigen) und inäquivalenten (unselbstständigen) Nebenleistungspflichten unterschieden. Unter ersteren versteht man solche Pflichten, die nicht unmittelbar dem Erfüllungszweck dienen. Die Erfüllung dieser Pflichten könnte auch weg gedacht werden, ohne dass es zu einer Gefährdung der reibungslosen Abwicklung der Hauptpflichten käme. Die inäquivalenten Nebenleistungspflichten ergeben sich noch mehr als die äquivalenten

---

[16] RG 9.7.1907, II 115/07, RGZ 66, 289ff: Es handelt sich um den so genannten „Pferdefutterfall".

[17] Vgl nur *Welser,* Bürgerliches Recht II[13] (2007) 87.

[18] *Larenz,* Lehrbuch des Schuldrechts (1953) 206.

[19] Und nicht nur bei mir: *Wittwer,* Die positive Vertrags- oder Forderungsverletzung, ÖJZ 2004, 161 (162), etwa bezeichnet sie als „mysteriöses Sammelsurium" und führt historische Gründe an.

Nebenleistungspflichten aus der Auslegung und stehen stets im engen Zusammenhang mit der Hauptleistungspflicht. So unterscheidet auch die deutsche Dogmatik zwischen den die Erfüllung der Hauptleistung vorbereitenden, unterstützenden und sichernden Nebenpflichten und den Schutzpflichten, die mit dem Vertragsinhalt nichts zu tun haben[20]. Sie sollen deren problemlose Erfüllung sicherstellen. Gelegentlich wird auch die Verletzung von Nebenpflichten zu den positiven Forderungsverletzungen gerechnet[21], was im Ergebnis mE richtig erscheint (siehe dazu unten).

2.1.2. Schutz- und Sorgfaltspflichten

Den Schuldner treffen auch Schutz- und Sorgfaltspflichten, deren Verletzung als positive Forderungsverletzung bezeichnet wird[22]. Ursprünglich wurde unter den positiven Forderungsverletzungen das Zuwiderhandeln gegen eine Unterlassungspflicht bzw eine Erfüllungshandlung des Schuldners verstanden, die den Gläubiger schädigte[23].

Häufiger wird dieser Gedankenkreis in der Literatur jedoch unter der Bezeichnung „positive Vertragsverletzung" diskutiert[24]. Damit ist jedoch stets dasselbe gemeint. Da Ansprüche aus dieser Rechtsfigur jedoch nicht zwingend einen gültigen

---

20 *Roth* in *Rebmann/Säcker* (Hrsg), Münchener Kommentar zum Bürgerlichen Gesetzbuch[3] (1994) § 242 Rz 183.

21 *Gschnitzer* in *Klang/Gschnitzer,* ABGB IV/1[2] (1968) 471; *derselbe,* Österreichisches Schuldrecht, Allgemeiner Teil[2] (1991), 119; *Esser,* Lehrbuch des Schuldrechts (1949) 155. Selbst *Staub,* Die positiven Vertragsverletzungen[2] (1913) 5, meint in seiner die Lehre von den positiven Vertragsverletzungen begründenden Schrift: „Es verpflichtet sich jemand, die ihm verkauften Lampen nicht nach Frankreich weiter zu verkaufen; er tut es doch." Damit beschreibt er nach dem oben skizzierten Begriffsverständnis eindeutig die Verletzung einer (äquivalenten) Nebenleistungspflicht, in deren Verletzung er eine positive Vertragsverletzung erblickt; vgl auch *Wittwer,* Die positive Vertrags- oder Forderungsverletzung, ÖJZ 2004, 161 (162).

22 OGH 7.9.1994, 3 Ob 544/94; 17.8.2000, 4 Ob 203/00g.

23 *Staub,* Die positiven Vertragsverletzungen[2] (1913) 6.

24 Ohne das seit der Lehre *Staubs* unüberschaubar gewordene Schrifttum abschließend anführen zu können: *Canaris,* Ansprüche wegen „positiver Vertragsverletzung" und „Schutzwirkung für Dritte" bei nichtigen Verträgen, JZ 1965, 475ff; *Glöckner,* Die positive Vertragsverletzung: die Geburt eines Rechtsinstitutes (2006); *Köpcke,* Die Typen der positiven Vertragsverletzung (1965); *Lehmann,* Die positiven Vertragsverletzungen, AcP 96 (1905), 60ff; *Schlesinger,* Die Lehre von den positiven Vertragsverletzungen und ihr Einfluss auf das österreichische Recht, ZBl 1926, 401ff und 721ff; *Staub*, Die positiven Vertragsverletzungen[2] (1913); *Stoll,* Abschied von der Lehre der positiven Vertragsverletzungen, AcP 136 (1932), 257ff uvm.

Vertrag voraussetzen[25], wird im Folgenden gegen die herrschende Literatur nur mehr der Begriff der positiven Forderungsverletzung verwendet.

Als „positiv" wird diese Art der Forderungsverletzung deshalb bezeichnet, weil sie nach dem Konzept ihres Schöpfers stets in einem positiven Tun besteht. Den unter dieser Bezeichnung zusammengefassten Verhaltensweisen sei nach *Staub* gemein, „das jemand tut, was er unterlassen soll"[26]. Ursprünglich waren Verletzungen einer Unterlassungspflicht oder den Gläubiger schädigende Schlechterfüllungen gemeint[27]. In diesen Fällen ergebe sich die Haftung anders als bei Unmöglichkeit und Mora nicht aus einem Unterlassen der (rechtzeitigen) Leistung, sondern aus einem positiven Tun. Diese Unterscheidung ist jedoch sachlich nicht richtig[28] und überdies überflüssig[29]. Dies zeigt etwa ein näherer Blick auf das berühmte Beispiel, in welchem die Tiere des Käufers am verdorbenen Futter des Verkäufers verenden. Die Lieferung des verdorbenen Futters stellt zwar ein positives Tun dar. Für den im Sterben der Tiere liegenden Mangelfolgeschaden muss der Verkäufer aber nur dann haften, wenn er schuldhaft, dh vorwerfbar handelte. Hier erkennt man, dass sich der haftungsbegründende Schuldvorwurf eigentlich nicht auf die Lieferung, sondern vielmehr auf die Außerachtlassung (ie ein Unterlassen) der gebotenen Sorgfalt gründet, die in weiterer Folge zur Lieferung des verdorbenen Futters führte. Für die Haftung ist es irrelevant, ob etwas trotz eines geschuldeten Tuns unterlassen wurde oder umgekehrt. Selbst *Staub* führt in seiner die Lehre von den positiven Forderungsverletzungen begründenden Schrift einleitend folgendes Beispiel an: *„Es liefert ein Kaufmann einem anderen einen von ihm fabrizierten Leuchtstoff, der explosive Bestandteile hat, ohne den Verkäufer aufmerksam zu machen; der Leuchtstoff richtet im Laden des Käufers großen Schaden an [...]*". Die „positive" Vertragsverletzung besteht in diesem Beispiel wohl darin, dass es der Verkäufer des Leuchtstoffes sorgloserweise *unterließ,* seinen Vertragspartner über die

---

[25] Grundlegend: *Canaris,* Ansprüche wegen „positiver Vertragsverletzung" und „Schutzwirkung für Dritte" bei nichtigen Verträgen, JZ 1965, 475 (476); *Leonhard,* Allgemeines Schuldrecht des BGB (1929) 541.

[26] *Staub,* Die positiven Vertragsverletzungen[2] (1913) 5.

[27] Und zwar im Anschluss an die Lehre *Staubs* auch in Österreich: *Schlesinger,* Die Lehre von den positiven Vertragsverletzungen und ihr Einfluss auf das österreichische Recht, ZBl 1926, 401 (411) mwN.

[28] So meint etwa *Himmelschein,* Erfüllungszwang und Lehre von den positiven Vertragsverletzungen, AcP 136 (1932) 255 (310): „Das positive Verhalten ist, wenn es widerrechtlich ist, nicht das Verhalten, das geschuldet wird. Wer noch so positiv gegen seine Pflicht handelt, der erfüllt sie eben nicht. Die Zuwiderhandlung gegen eine Unterlassungspflicht ist zugleich eine Nichterfüllung dieser Pflicht ..."; vgl auch *Leonhard,* allgemeines Schuldrecht des BGB (1929) 538.

[29] So auch *Köpcke,* Typen positiver Vertragsverletzung (1965) 69.

Gefährlichkeit des Kaufgegenstandes aufzuklären[30]. Nach der Schöpfung der positiven Forderungsverletzungen wurde zunehmend alles zu den positiven Forderungsverletzungen gezählt, was sich – scheinbar – weder als Unmöglichkeit noch als Verzug erwies[31]. *Enneccerus* schlägt den Begriff „Schlechterfüllung" vor, um die gezeigten Unzulänglichkeiten der herrschenden Terminologie zu überwinden[32]. Ebenso könnte man von „sonstigen Forderungsverletzungen" sprechen. Diese Bezeichnung wurde jedoch bereits als „farblos" abgelehnt[33]. Obwohl ich diese Einschätzung nicht teile, sehe ich dennoch ein, dass es kaum Sinn macht, gegen eine seit 1902 verwendete und von vielen vor mir letztlich erfolglos kritisierte Begrifflichkeit anzukämpfen.

Schutz- und Sorgfaltspflichten bedürfen keiner besonderen Vereinbarung, sie werden regelmäßig im Rahmen ergänzender Vertragsauslegung gewonnen (siehe dazu Kapitel 5.5.2ff). Ihre Einhaltung soll sicherstellen, dass der Gläubiger nicht an seinen Gütern geschädigt wird. Ihr Inhalt richtet sich nach der Art des Schuldverhältnisses, der Intensität des Vertrauensverhältnisses und den besonderen Umständen[34]. Ihre Begründung und die Art ihrer Bestimmung wird noch weiter unten ausführlich erörtert werden. Sämtlichen Fällen, die von der hM[35] unter den Begriff der positiven Forderungsverletzung subsumiert werden, ist gemein, dass der Schuldner eine Pflicht verletzt, die nicht mit der den Vertrag charakterisierenden Hauptleistungspflicht identisch ist. Der daraus resultierende Schaden an den sonstigen Gütern des Gläubigers ist nach hA ein anderer als jener, der aus der Verzögerung (ie Verzug iSd §§ 918ff ABGB) oder endgültigen Vereitelung (ie Unmöglichkeit iSd §§ 920ff ABGB) der Erfüllung der Hauptleistungspflicht erwächst[36].

> Beispiel: Nehmen wir an[37], es lässt sich durch Auslegung die Schutzpflicht eines Anbieters von Kommunikationsdiensten ableiten, welche ihn

---

[30] *Larenz,* Lehrbuch des Schuldrechts I (1953), 206, bezeichnet diesen Schaden als einen, „der gerade durch die Verletzung der Pflicht des Verkäufers zur sorgsamen Ausführung der Leistungshandlung in zurechenbarer („adäquater") Weise verursacht worden ist."

[31] *Stoll,* Abschied von der Lehre der positiven Vertragsverletzungen, AcP 136 (1932) 257 (262); *Wittwer,* Die positive Vertrags- oder Forderungsverletzung, ÖJZ 2004, 161 (162); vgl etwa auch unten die in Kapitel 3.1.1 angeführten vier von *Enneccerus* gebildeten Kategorien.

[32] *Enneccerus,* Lehrbuch des Bürgerlichen Rechts II, Das Recht der Schuldverhältnisse[12] (1932) 212.

[33] *Köpcke,* Typen positiver Vertragsverletzung (1965) 12.

[34] OGH 28.10.1980, 5 Ob 603/80.

[35] Auf die Gegenansicht *Gschnitzers* uva, wonach der Begriff der positiven Vertragsverletzung überflüssig sei, wird noch weiter unten eingegangen werden.

[36] Zur Gegenauffassung, wonach auch derartige Fälle als vom positiven Leistungsstörungsrecht des ABGB mitgeregelt sind, siehe unten Kapitel 3.2.2.

[37] Auf Frage des Bestands, des Umfangs und der Grenzen einer solchen Schutzpflicht wird noch weiter unten eingegangen werden (Kapitel 5 und 6).

verpflichtet, sämtliche behördliche Auskunftsbegehren gewissenhaft zu überprüfen. Wenn der Anbieter diese Pflicht verletzt, indem er einem offenkundig unzureichend begründeten Auskunftsbegehren ohne weiteres Folge leistet, führt dies zu einem empfindlichen – und nach dem eben Gesagten – vermeidbaren Eingriff in die Privatsphäre seines Kunden. Der Schaden, der seinem Kunden aus dieser Vertragsverletzung erwächst, ist nach hM ein völlig anderer als etwa jener, der ihm entstünde, wenn der Anbieter seine Hauptleistungspflicht, also die Erbringung von Kommunikationsdiensten, verletzt. Dem in seiner Privatsphäre verletzten Kunden helfen – scheinbar – weder die Regeln über den schuldhaften Verzug (§§ 918 ff ABGB) noch jene über die schuldhafte Unmöglichkeit (§§ 920ff ABGB).

2.1.3. Terminologische Differenzen

Es ist festzuhalten, dass sich für die hier zu behandelnden Pflichtenkomplexe in der gesamten österreichischen Zivilistik keine einheitliche Terminologie herausgebildet hat. Manchmal wird der Begriff der Nebenleistungspflichten in der Lehre[38] und Rechtsprechung[39] als Überbegriff verwendet, um darunter auch die Schutz- und Sorgfaltspflichten zu subsumieren, während andere diese Begriffe einander als gleichrangig gegenüberstellen[40]. Neben Obhuts-, Anzeige-, Mitwirkungs- und Fürsorgepflichten werden auch Auskunfts- sowie Mitteilungs- und Aufklärungspflichten als Nebenpflichten anerkannt[41]. *Gschnitzer* zählt etwa die Pflicht, bei Erfüllung die Güter des Gläubigers nicht zu beschädigen, zu den unselbstständigen Nebenpflichten[42]. Er kennt keine eigene Kategorie von Schutz- und Sorgfaltspflichten. Unter der von ihm ihrer Sinnhaftigkeit nach grundsätzlich in Frage gestellten positiven Forderungsverletzung

---

[38] *Gschnitzer/Faistenberger,* Österreichisches Schuldrecht, Allgemeiner Teil[2] (1991) 120; vgl etwa auch *Esser,* Lehrbuch des Schuldrechts[1] (1949) 43: er zählt etwa die Fürsorgepflicht des Arbeitgebers hinsichtlich der körperlichen Unversehrtheit des Arbeitnehmers zu den unselbstständigen Nebenleistungspflichten.

[39] OGH 25. 6. 1987, 7 Ob 33/87, ZVR 1988/70: *„[...] Zu den für den Vertrag typischen wesentlichen Hauptleistungspflichten treten in aller Regel Nebenleistungspflichten, welche die Vorbereitung und reibungslose Abwicklung der Hauptleistung ermöglichen sollen. Eine besonders wichtige Gruppe dieser Nebenleistungspflichten bilden die Schutz- und Sorgfaltspflichten. Die Vertragspartner haben die Erfüllungshandlung so zu setzen, daß der andere Teil weder an seiner Person noch an seinen Gütern geschädigt wird.*"; vgl auch OGH 19.6.1986, 8 Ob 511/86, SZ 59/109.

[40] *Welser,* Bürgerliches Recht II[13] (2007) 4ff; vgl auch *Larenz,* Lehrbuch des Schuldrechts, Allgemeiner Teil I[13] (1982), 11, der zwischen Haupt- und Nebenleistungspflichten auf der einen und „weiteren Verhaltenspflichten" (ie Schutz- und Loyalitätspflichten) auf der anderen Seite unterscheidet; *Stoll,* Die Lehre von den Leistungsstörungen (1936) 28, der Nebenpflichten und Schutzpflichten als nicht identisch einstuft, den Verstoß gegen die einen als auch die anderen hingegen zusammenfassend als positive Vertragsverletzung bezeichnet.

[41] *Esser,* Lehrbuch des Schuldrechts (1949) 43.

[42] *Gschnitzer/Faistenberger,* Österreichisches Schuldrecht, Allgemeiner Teil[2] (1991) 51; als Beispiel nennt auch er etwa krankes Vieh des Schuldners, welches das gesunde Vieh des Gläubigers ansteckt.

versteht er allgemein die Verletzung von Nebenpflichten[43]. Es stellt sich daher die Frage, ob es tunlich bzw überhaupt möglich ist, eine scharfe Grenze zwischen inäquivalenten Nebenpflichten einerseits und Schutz- und Sorgfaltspflichten andererseits zu ziehen. Eine solche Grenze zieht *Welser*. Zwar gesteht *Welser* dem Gläubiger grundsätzlich[44] weder bei den inäquivalenten Nebenleistungspflichten noch bei den Schutzpflichten ein Rücktrittsrecht nach § 918 ABGB zu, wenn der Schuldner mit diesen in Verzug gerät[45]. Ebenso wenig gesteht er einer dieser beiden Gruppen isolierte Einklagbarkeit zu[46]. Dennoch behandelt er ausschließlich die Verletzung von Schutz- und Sorgfaltspflichten als positive Forderungsverletzung[47]. Es mache Sinn, diese Fälle als besondere Gruppe zusammenzufassen, da sie sich von Verzug und Unmöglichkeit unterscheiden würden[48]. Da er nur an die Verletzung von Schutz- und Sorgfaltspflichten die Rechtsfolge der Haftung aus positiver Forderungsverletzung knüpft, ist anzunehmen, dass er davon ausgeht, dass sich eine Trennlinie zwischen Nebenpflichten und Schutz- und Sorgfaltspflichten ziehen lässt. Das den Schutz- und Sorgfaltspflichten angeblich eigentümliche Element, den Gläubiger vor Schäden an seinen sonstigen Gütern zu bewahren, ist jedoch auch in den meisten Nebenpflichten mehr oder weniger stark ausgeprägt zu finden. Als typische inäquivalente Nebenleistungspflicht, die auch den Schutz der sonstigen Güter des Gläubigers bewirkt, ist hier etwa die Rechnungslegungspflicht zu nennen. Sie ermöglicht dem Rechnungsempfänger die einfache Erfüllung seiner Hauptleistungspflicht, nämlich die Bezahlung des Entgelts. Gleichzeitig schützt sie aber auch das Vermögen des Rechnungsempfängers, indem sie unkorrekter Verrechnung zu seinen Lasten und damit einer unrechtmäßigen Schmälerung seines Vermögens vorbeugt. Tatsächlich gehen die Begriffe der (inäquivalenten) Nebenleistungspflichten und der Schutzpflichten ineinander über[49]. Eine exakte

---

[43] *Gschnitzer/Faistenberger,* Österreichisches Schuldrecht, Allgemeiner Teil[2] (1991) 119.

[44] Eine Ausnahme sei stets dann gegeben, wenn das gegenseitige Vertrauen durch die Pflichtverletzung so erschüttert werde, dass eine Fortsetzung nicht zumutbar sei.

[45] *Welser,* Bürgerliches Recht II[13] (2007) 56; er stützt sich dabei auf die Entscheidung des OGH vom 14.11.1984, 1 Ob 703/84, die diese Auffassung jedoch nur hinsichtlich der inäquivalenten Nebenleistungspflichten bestätigt; der OGH hat in diesem Punkt eine differenzierende Rechtsprechung, die unten (Kapitel 3.2.2) noch genauer dargestellt werden wird.

[46] *Welser,* Bürgerliches Recht II[13] (2007) 4ff.

[47] So scheinbar auch *Koziol*, Österreichisches Haftpflichtrecht II (1975) 66: „Aus einem – vertraglichen oder gesetzlichen – Schuldverhältnis ergeben sich für die Beteiligten nicht nur Haupt- und Nebenleistungsverpflichtungen, sondern auch umfassende Schutzpflichten gegenüber der Person und dem Vermögen des Partners [...]" (Hervorhebung durch den Verfasser).

[48] *Welser,* Bürgerliches Recht II[13] (2007) 88; zur Kritik an dieser Auffassung siehe ausführlich unten Kaptitel 3.2.2..

[49] *Esser,* Lehrbuch des Schuldrechts (1949) 155.

Grenzziehung ist mE letztlich unmöglich und auch nicht unbedingt sinnvoll. Das zeigt sich auch darin, dass manche völlig gleich gelagerte Probleme unter völlig unterschiedlichen Termini diskutieren. So meint etwa *Reischauer*, dass der Schaden, den eine fehlerhafte Maschine ihrem Käufer zufüge, ein Problem der fehlerhaften Haupt- oder Schlechtleistung sei und nicht zur Problematik der Schutzpflichten gehöre[50]. Das Beispiel mit der fehlerhaften Maschine (mangelhafte Erfüllung der Hauptleistungspflicht) entspricht dem Beispiel mit dem verdorbenen Viehfutter, das die Tiere des Käufers verenden lässt und von *Welser* als Beispiel einer Schutzpflichtverletzung wird, die zu einem Mangelfolgeschaden führt[51]. In beiden Fällen muss der Verkäufer für die in der Sphäre des Käufers an seiner Person bzw an seinem Vermögen eintretenden Schäden dann haften, wenn ihn ein Verschulden trifft, das eigentlich nur in der Sorglosigkeit bei der Auswahl der gelieferten Sache bestehen kann. Die sorglos ausgewählte und gelieferte Sache verursacht dann einen Schaden beim Käufer. Das für eine Schadenersatzpflicht haftungsbegründende Verhalten kann nicht in der bloßen objektiven Schlechtleistung bestehen, da diese ohne zumindest fahrlässige Unkenntnis des Mangels nicht vorwerfbar ist[52]. Für *Reischauer* zählt jedoch sogar die unterbliebene Aufklärung über die Gefährlichkeit eines an sich vertragsgemäßen Leistungsgegenstandes „zur Leistung" (!)[53].

Im Übrigen erscheint es inkonsequent, die schon im Hinblick auf ihre dogmatischen Grundlagen zweifelhafte Rechtsfigur[54] der positiven Forderungsverletzungen zwar einerseits zu übernehmen, um sie dann andererseits auf willkürlich abgegrenzte Pflichtverletzungen einzuschränken. *Staub* und auch die ihm folgende Lehre dachten bei den positiven Forderungsverletzungen zweifellos auch an die Verletzung von Pflichten, die nach dem heutigen Verständnis Nebenleistungspflichten darstellen. Hier wäre etwa sein Beispiel zu nennen, wonach es eine positive Vertragsverletzung darstelle, wenn jemand sich verpflichtet, die ihm verkauften Lampen nicht nach Frankreich weiter zu verkaufen und er es dann doch tut[55]. Der Begriff der Schutzpflichten wird daher im Folgenden im Bewusstsein darüber verwendet, dass er sich vom Begriff der (inäquivalenten) Nebenpflichten nicht abgrenzen lässt, was jedoch keine praktische Bedeutung hat.

---

[50] *Reischauer* in Rummel, ABGB I³ (2000) Vor §§ 918-933 Rz 5.

[51] *Welser,* Bürgerliches Recht II¹³ (2007) 87.

[52] So aber *Reischauer* in Rummel, ABGB I³ (2000) Vor §§ 918-933 Rz 5 und § 932 Rz 20i, der diese Fälle wie erwähnt als Probleme der fehlerhaften Haupt- bzw Nebenleistung betrachtet.

[53] *Reischauer* in *Rummel,* ABGB I³ (2000) Vor §§ 918-933 Rz 6.

[54] Zu dieser Kritik siehe unten Kapitel 3.2.1.

[55] Vgl FN 21.

2.2. Andere Schäden als das Erfüllungsinteresse

Auffassungsunterschiede bestehen auch bezüglich der Bezeichnungen von Schäden aus Vertragsverletzungen, die nicht im auf Hauptleistungspflicht bezogenen Erfüllungsinteresse bestehen. Es geht hier also um jene Schäden, die nach gültigem Vertragsabschluss aus der Verletzung anderer Pflichten als der Hauptleistungspflichten erwachsen.

Richtigerweise kann es sich auch bei diesen Schäden stets nur um Verzögerungs- oder Vereitelungsschäden handeln, denn auch hier kann es keine anderen Fälle als die Verzögerung oder die endgültige Vereitelung der Erfüllung einer Vertragsverbindlichkeit geben. Wird eine Schutzpflicht verletzt, ist zu untersuchen, ob diese Pflicht in endgültiger oder in nur vorübergehender Form verletzt wurde. Wird etwa einer vertraglichen Schutzpflicht zum Trotz etwas verraten, was eigentlich geheim gehalten werden hätte sollen, ist bezüglich dieser Schutzpflicht Unmöglichkeit eingetreten. Es mag zwar möglich sein, künftig wieder sämtlichen Geheimhaltungspflichten wieder nachzukommen, jedoch kann der geschuldete Erfolg nicht mehr erreicht werden[56]. Der Schaden mag ein anderer sein als das auf die Hauptleistungspflicht bezogene Erfüllungsinteresse, aber das ändert nichts daran, dass er das Resultat einer vorübergehenden oder endgültigen Vertragsverletzung darstellt[57].

Nach dem oben Gesagten könnte man daher konsequenterweise auf besondere Begrifflichkeiten für die hier interessierenden Schadenskategorien überhaupt gänzlich verzichten. So könnte man auch bei Schäden, die aus der Verletzung von Schutzpflichten resultieren, behaupten, der Schuldner hafte auf das Erfüllungsinteresse. Damit wäre freilich nicht das Interesse an der vereinbarungsgemäßen Erbringung der Hauptleistungspflicht gemeint, sondern das Interesse an der vertragskonformen Einhaltung der Schutzpflicht. Verursacht die vertragswidrige Beschaffenheit des Leistungsgegenstandes einen Schaden beim Gläubiger, ist dieser – Verschulden vorausgesetzt – so zu stellen, als hätte er seine Schutzpflicht nicht verletzt und eine vertragsgemäße Leistung erbracht. Die Begriffe „Erfüllungsinteresse" bzw „Nichterfüllungsschaden" werden zwar immer nur im Zusammenhang mit der Nichterfüllung der vertraglichen Hauptleistungspflicht verwendet. Da aber auch bei der Nichterfüllung von Neben- bzw Schutzpflichten ein Schaden entstehen kann, der bei ihrer Erfüllung ausgeblieben wäre, könnten diese Begriffe eigentlich auch für Schäden aus der

---

[56] *Leonhard,* Allgemeines Schuldrecht des BGB (1929) 537; vgl auch *Honsell,* Der Geheimnisschutz im Zivilrecht, in *Ruppe* (Hrsg) Geheimnisschutz im Wirtschaftsleben (1980) 45 (47).

[57] So auch *Gschnitzer* in *Klang/Gschnitzer*, ABGB IV/1[2] (1968) 472; aA *Leonhard,* Allgemeines Schuldrecht des BGB (1929) 541.

Verletzung von Schutzpflichten verwendet werden[58]. Systematisch betrachtet, ist der Schaden, der im verminderten Wert der Leistung besteht, nichts grundlegend anderes als der Schaden, der durch die mangelhafte Leistung im Vermögen des Gläubigers zusätzlich bewirkt wird. Beide Schäden haben gemein, dass sie ausgeblieben wären, wenn die verletzte Vertragspflicht erfüllt worden wäre. Im ersten Fall wurde eine Hauptleistungspflicht, im zweiten Fall wurde eine Schutzpflicht verletzt. In beiden Fällen wird der zu leistende Schadenersatz danach bestimmt, wie der Gläubiger bei ordnungsgemäßer Erfüllung gestanden wäre. Dennoch hat es sich eingebürgert, den Begriff Erfüllungsinteresse bzw Nichterfüllungsschaden nur mit der Verletzung von Hauptleistungspflichten in Verbindung zu bringen. Obwohl dies wie gezeigt eigentlich nicht restlos zu überzeugen vermag, wird wiederum aus pragmatischen Gründen vorgeschlagen, mit der hL bei besonderen Begrifflichkeiten für die aus Schutzpflichtverletzungen resultierenden Schäden zu bleiben.

Für die hier interessierenden Schadenskategorien werden jedoch sehr unterschiedliche Termini verwendet. Heute werden in Österreich im Allgemeinen zwei Kategorien positiver Vertragsverletzungen unterschieden: Es gibt die Fälle der Schlechterfüllung, in denen die Hauptleistungspflicht mangelhaft erfüllt wird und dies in weiterer Folge den Gläubiger über das Erfüllungsinteresse hinaus schädigt[59]. Diese Fälle werden von *Koziol* unter dem Begriff „Schlechterfüllung" zusammengefasst und die dadurch bewirkten Schäden werden von *Welser* als „Mangelfolgeschäden" bezeichnet[60]. Davon unterschieden werden jene Fälle, in denen der Schuldner lediglich eine Schutzpflicht verletzt und dadurch einen Schaden bewirkt. *Welser* bezeichnet diese Schäden als Begleitschäden[61]. Ebenso unterscheidet *Larenz* – allerdings ohne den Begriff Mangelfolgeschäden zu verwenden – zwischen Fällen der Schlechterfüllung und jenen, in welchen eine nur eine „weitere Verhaltenspflicht verletzt" worden ist[62].

Es gibt es aber auch völlig gegenteilige Begriffsverwendungen: So bezeichnet etwa *Leonard* den aus der vertragswidrigen Beschaffenheit des Leistungsgegenstandes erwachsenden zusätzlichen Schaden als „Begleitschaden". Auch

---

[58] Ebenso *Reischauer* in Rummel, ABGB I^3 (2000) Rz 4 zu §§ 918-933 ABGB.

[59] Diese Kategorie kannte auch schon *Staub*; dieser Begriff wurde erstmals verwendet von *Zittelmann,* Nichterfüllung und Schlechterfüllung, in Festgabe für *Paul Krüger* (1911), 265 (276).

[60] *Welser,* Bürgerliches Recht II^{13} (2007) 87.

[61] *Welser,* Bürgerliches Recht II^{13} (2007) 87.

[62] *Larenz,* Lehrbuch des Schuldrechts I (1953) 206.

Koziol betrachtet die Begriffe „Begleitschaden" und „Mangelfolgeschaden" im Gegensatz zu *Welser* als Synonyme[63].

Im Ergebnis ist das Begriffspaar „Begleitschäden-Mangelfolgeschäden" zu bevorzugen. Wenn man schon meint, man braucht für die Schäden, die aus der Verletzung von Schutz- und Sorgfaltspflichten resultieren, eigene Begriffe, dann macht es auch Sinn, zwischen diesen zwei Kategorien zu unterscheiden. Obwohl zwischen Mangelfolgeschäden und Begleitschäden (vor allem hinsichtlich der Rechtsfolgen) kein grundlegender Unterschied besteht, ist dennoch einzusehen, dass bei Begleitschäden der Zusammenhang zur Erbringung der Hauptleistungspflicht deutlich vermindert ist, weshalb eine Abgrenzung zumindest möglich ist. Diese Arbeit wird sich auch nur mit Schutzpflichten auseinandersetzen, die mit der Erbringung der Hauptleistungspflicht in keinem unmittelbaren Zusammenhang mehr stehen: Es geht schließlich um die Pflicht des Access-Providers gegenüber seinem Kunden, dessen Privatsphäre zu schützen. Diese Pflicht weist mit seiner Hauptleistungspflicht, der Erbringung von Kommunikationsdiensten, keinen direkten Zusammenhang auf.

Nach der Judikatur des OGH liegt Schlechterfüllung nicht nur vor, wenn die Leistung selbst mangelhaft erbracht wird, *„sondern auch dann, wenn – auch bei ordentlicher Erbringung der Leistung – sonstige Güter des Gläubigers verletzt werden ("positive Vertragsverletzung"); als haftungsbegründend wird die Verletzung von den Schuldner treffenden Schutzpflichten angesehen.*"[64] Der OGH spricht daher im Gegensatz zu *Welser* sowohl bei Mangelfolgeschäden als auch bei Begleitschäden von Schlechterfüllung[65]. Positiv ist an dieser Terminologie, dass sie zum Ausdruck bringt, dass kein grundlegender Unterschied zwischen den beiden Kategorien besteht. Einen Nachteil dieser Begrifflichkeit stellt es hingegen dar, dass der Begriff der „Schlechterfüllung" eigentlich aus dem Gewährleistungsrecht bekannt ist und dort die mangelhafte Erfüllung der Hauptleistungspflicht bezeichnet. Der OGH verwendet den Begriff als Synonym für die „positiven Vertragsverletzungen", weshalb er zudem als überflüssig zu betrachten ist.

Festzuhalten bleibt daher, dass kein substanzieller Unterschied zwischen Schäden besteht, die aus der Verletzung der Hauptleistungspflicht resultieren und solchen, welche auf die Verletzung von Schutzpflichten folgen. Im Rahmen dieser Arbeit werden ausschließlich jene Schäden aus reinen Schutzpflichtverletzungen untersucht (Begleistschäden).

---

[63] *Koziol,* Österreichisches Haftpflichtrecht II (1975) 68.

[64] OGH 17.08.2000, 4 Ob 203/00g, SZ 73/126.

[65] Ebenso: *Bydlinski,* Grundzüge des Privatrechts[3] (1997) Rz 550ff.

3. Forderungsverletzungen des Access-Providers

3.1. Analyse des Rechtsinstituts der positiven Forderungsverletzungen

Eines der zentralen Anliegen dieser Arbeit ist es, die Frage zu beantworten wie weit die Schutzpflichten des Access-Providers gehen, etwa inwieweit er verpflichtet ist, die Privatsphäre gegenüber Auskunft suchenden Behörden zu verteidigen. Diese Pflicht, so sie existiert, ist dem Komplex der (Neben-,) Schutz- und Sorgfaltspflichten zuzuordnen, deren Verletzung wie erwähnt als positive Forderungsverletzung bezeichnet wird[66]. Schäden, die dem Vertragspartner des Access-Providers durch die Verletzung dieser Pflicht entstehen können, können als Begleitschäden bezeichnet werden.

Wirft man einen Blick ins ABGB, findet man weder eine allgemeine Regel zu den Schutz- und Sorgfaltspflichten noch einen Paragraphen zu den positiven Forderungsverletzungen. Das liegt daran, dass es sich bei dieser Rechtsfigur um eine Erfindung der Rechtswissenschaft handelt. Erfunden wurde dieser Begriff von *Hermann Staub* im Jahre 1902[67]. Für die späteren Ableitungen in dieser Arbeit ist es unumgänglich, sich näher mit den dogmatischen Grundlagen der positiven Forderungsverletzungen bzw der Schutz- und Sorgfaltspflichten auseinanderzusetzen. So könnte der Vertragspartner eines Providers, in dessen Privatsphäre eingegriffen wurde, etwa ein Interesse haben, sich vom Vertrag zu lösen. Inwieweit er dazu berechtigt ist, hängt ua davon ab, wie man die positive Forderungsverletzung dogmatisch begründet. Die heute hL ist der Auffassung, dass die Verletzung von Schutzpflichten nur in seltenen Ausnahmefällen zu Vertragsauflösung führen kann. Die folgenden Ausführungen skizzieren die Grundlagen der Rechtsfigur der positiven Forderungsverletzungen und kritisieren diesen Begriff in Bezug auf das deutsche Recht. Anschließend wird die Übernahme der positiven Forderungsverletzungen ins österreichische Recht einer kritischen Analyse unterzogen.

---

[66] OGH 7.9.1994, 3 Ob 544/94.

[67] Erstmals: *Staub,* Die positiven Vertragsverletzungen, Festschrift für den 26. Deutschen Juristentag (1902) 31ff; danach gab es einige weitere Auflagen, in denen er bzw Bearbeiter dieser Auflagen seine Lehre verteidigten. Im Folgenden wird die zweite Auflage aus 1913 zitiert: *Staub,* Die positiven Vertragsverletzungen[2] (1913)

3.1.1. Die „Lückenhaftigkeit" des Gesetzes

Der Lehre der positiven Forderungsverletzungen liegt die Annahme zugrunde, dass es für derartige Fälle keine ausreichende Regelung im BGB – die österreichische Lehre und Rechtsprechung übernahmen diesen Gedanken auch hinsichtlich des ABGB[68] – gäbe. Das von *Staub* begründete Rechtsinstitut wurde den Leistungsstörungen des Verzuges und der Unmöglichkeit beiseite gestellt. Diese Lehre wurde in weiterer Folge heftig angegriffen[69], was aber nichts daran änderte, dass sie sich rasch auch in der Rechtsprechung zunehmend etablierte und heute bereits zu Recht auch als gewohnheitsrechtlich[70] verankert betrachtet werden kann.

Heftig umstritten ist die Frage betreffend die dogmatischen Grundlagen der positiven Vertragsverletzungen. *Staub* glaubte im System des BGB eine „Lücke" zu erkennen, die es durch Analogie der Regeln über Verzug zu schließen gelte. *Staub* zählte in seiner berühmten Schrift einleitend folgende Beispiele auf[71]: *„Es verpflichtet sich jemand, die ihm verkauften Lampen nicht nach Frankreich weiterzuverkaufen; er tut es doch. Es liefert ein Kaufmann einem anderen einen von ihm fabrizierten Leuchtstoff, der explosive Bestandteile hat, ohne den Käufer aufmerksam zu machen; der Leuchtstoff richtet im Laden des Käufers große Schaden an. Ein Agent gibt aus Nachlässigkeit unrichtige Berichte über die Solvenz eines von ihm gewonnen Kunden, ein anderer arbeitet fortgesetzt für ein Konkurrenzgeschäft, obwohl darin nach Lage der Sache eine arge Pflichtverletzung zu erblicken ist. Ein Kommis verkauft aus Fahrlässigkeit weit unter dem Einkaufspreise. Ein Prinzipal gibt seinem Handlungsgehilfen ein unrichtiges Zeugnis [...]*"

Nach Ansicht *Staubs* war keiner dieser Fälle unter eine Bestimmung des BGB zu subsumieren. Es liege kein Verzug vor, denn der Schuldner habe in keinem der Fälle etwas unterlassen, was er hätte tun sollen[72].

---

[68] Vor allem *Koziol* und *Welser* haben mit ihrem Standardlehrbuch einen entsprechenden Beitrag geleistet, dass dieser Rechtsgedanke Einzug in Literatur und Judikatur fand. Dafür wurden sie häufig kritisiert, vgl etwa: *Barta,* Zivilrecht (2000) 269.

[69] Die wichtigsten etwa: *Himmelschein,* Erfüllungszwang und Lehre von den positiven Vertragsverletzungen, AcP 135 (1932) 255ff; *Lehmann,* Die positiven Vertragsverletzungen, AcP 96 (1905) 60ff. *Stoll*, Abschied von der Lehre der positiven Vertragsverletzungen, AcP 136 (1932) 257ff; *Zitelmann* in FS für *Paul Krüger,* Nichterfüllung und Schlechterfüllung, 1911, 265ff; für Österreich: *Schlesinger,* Die vorläufige und endgültige Nichterfüllung, Die Lehre von den positiven Vertragsverletzungen und ihr Einfluss auf das österreichische Recht, Das Wesen der positiven Vertragsverletzungen; ZBl 1926, 1ff, 401ff, 721ff;

[70] So ausdrücklich etwa bereits *Leonhard,* Allgemeines Schuldrecht des BGB I (1929) 542; vgl auch *Schlechtriem,* Schuldrecht, Allgemeiner Teil[2] (1994) Rz 338; *Thiele,* Leistungsstörung und Schutzpflichtverletzung, JZ 1967, 649 (649).

[71] *Staub,* Die positiven Vertragsverletzungen[2] (1913) 5.

[72] *Staub,* Die positiven Vertragsverletzungen[2] (1913) 6.

Die Meinung, dass das BGB in diesem Punkte lückenhaft sei, teilten viele bedeutende Rechtswissenschaftler in Deutschland jeglicher Kritik zum Trotz. So meint etwa *Enneccerus*: *„Die Verfasser des BGB haben, wie es scheint, geglaubt, durch die Vorschriften über das Unmöglichwerden der Leistung und den Verzug alle schuldhaften Verletzungen von Forderungsrechten geregelt zu haben. Diese Annahme ist aber nicht zutreffend. Es gibt vielmehr zahlreiche Forderungsverletzungen, die weder Unmöglichkeit der Leistung noch Verzögerung bewirken und ferner andere, die zwar eine solche Folge haben, aber dem Gläubiger daneben einen über das Erfüllungsinteresse weit hinausgehenden Schaden zufügen.*"[73]

3.1.2. § 276 BGB

Nach *Staub* besteht keine allgemeine Vorschrift des BGB, aus der sich eine Schadenersatzpflicht ableiten ließe. Damit erteilte er der von manchen[74] nach seiner Schrift vertretenen Auffassung, dass sich eine Schadenersatzpflicht einfach aus § 276 Abs 1 BGB ableiten ließe, richtigerweise eine Absage. Diese Bestimmung lautet:

„Der Schuldner hat Vorsatz und Fahrlässigkeit zu vertreten, wenn eine strengere oder mildere Haftung weder bestimmt noch aus dem sonstigen Inhalt des Schuldverhältnisses, insbesondere aus der Übernahme einer Garantie oder eines Beschaffungsrisikos zu entnehmen ist. Die Vorschriften der §§ 827 und 828 finden entsprechende Anwendung."

Es gelang *Staub,* die von ihm angenommene gesetzliche Lücke zumindest insoweit erfolgreich zu verteidigen, als er nachvollziehbar darlegen konnte, dass § 276 Abs 1 BGB nichts weiter als die Definition der zivilrechtlichen Schuld beinhaltet[75]. § 276 BGB beantwortet nur die Frage, was als schuldhaft iSd BGB gilt, nämlich vorsätzliches und fahrlässiges Handeln. In welchen Fällen hingegen konkret gehaftet wird, ergibt sich aus anderen Bestimmungen[76]. „Vertreten müssen" bedeutet nicht „auf Schadenersatz

---

[73] *Enneccerus,* Lehrbuch des Bürgerlichen Rechts II, Das Recht der Schuldverhältnisse[12] (1932) 209.

[74] Etwa: *Crome,* System des Deutschen Bürgerlichen Rechts II (1902) 65: „Der Inhalt der Verpflichtung beschränkt sich meist darauf, dass ein gewisses Maß von Sorgfalt auf die Erfüllung verwendet werde. Deren Außerachtlassung (Vorsatz, Fahrlässigkeit) macht also schadenersatzpflichtig." § 276 BGB; *Dernburg,* Über das Rücktrittsrecht des Käufers wegen positiver Vertragsverletzung, DJZ 1903, 1; dieser Theorie schloss sich auch das Reichsgericht an: RG 29.11.1922, RGZ 106, 22 (25).

[75] *Staub,* Die positiven Vertragsverletzungen[2] (1913) 7ff.

[76] Vgl auch *Heck,* Die Entstehungsgeschichte des § 276 BGB, AcP 137 (1933), 259ff.

haften", sondern bedeutet nur, dass in diesen Fällen schuldhaftes Handeln vorliegt[77]. Dies ergibt sich, wie *Staub* zeigen konnte, insbesondere auch aus einem mE unwiderlegbaren systematischen Argument. Wäre bereits aus § 276 BGB unmittelbar eine Schadenersatzpflicht ableitbar, wären andere Bestimmungen, die Schadenersatzansprüche normieren, wie etwa § 286 BGB in seiner damaligen Fassung, überflüssig gewesen[78]. Weiter unten (Kapitel 3.2) wird noch auf die Frage einzugehen sein, ob nicht § 1295 ABGB in Österreich genau in jener allgemeinen Weise eine Schadenersatzpflicht normiert, welche die oben zitierten deutschen Juristen fälschlicherweise aus § 276 BGB herauslesen wollten. Vorerst kann aber festgehalten werden, dass man der Verteidigung *Staubs* insoweit folgen kann, als es im deutschen Zivilrecht keine allgemeine positive Bestimmung gibt, aus welcher sich die Schadenersatzpflicht in den von ihm skizzierten Fällen ergäbe.

3.1.3. Anwendbarkeit der Verzugs- und Unmöglichkeitsvorschriften?

Schwerer wird es, *Staubs* „Lücke" gegenüber jenen zu verteidigen, die behaupten, dass sich eine Schutzpflichtverletzung stets entweder unter Mora oder Unmöglichkeit einordnen lasse[79]. *Staubs* Lehre liegt jedenfalls der Gedanke zugrunde, dass in den von ihm als positiven Vertragsverletzungen bezeichneten Fällen der Schuldner nicht vertragsgemäß handelt und er den Vertrag somit verletzt. *Staub* meint wörtlich: *„Man ist hiernach berechtigt, auf Grund der nach der ganzen Sachlage nahe liegenden und zwingenden Analogie des § 286 BGB anzunehmen, dass ein Rechtsgrundsatz besteht, wonach derjenige, der eine Verbindlichkeit durch eine positive Handlung schuldhaft verletzt, dem anderen Teile den hierdurch entstehenden Schaden zu ersetzen hat [...]"*[80]

---

[77] *Staub* folgend etwa: *Henle,* Lehrbuch des Bürgerlichen Rechts II (1934) 486; *Lehmann,* Die positiven Vertragsverletzungen, AcP 96 (1905), 60 (82); *Larenz,* Lehrbuch des Schuldrechts I (1952) 207; *Leonhard,* Allgemeines Schuldrecht des BGB I (1929) 542; *Stoll,* Abschied von der Lehre der positiven Vertragsverletzungen, AcP 136 (1932), 257 (267).

[78] *Staub,* Die positiven Vertragsverletzungen^2 (1913) 7ff; *Lehmann,* Die positiven Vertragsverletzungen, AcP 96 (1905), 60 (82).

[79] *Goldmann/Lilienthal,* Das bürgerliche Gesetzbuch systematisch dargestellt I^2 (1903) 333; *Himmelschein,* Erfüllungszwang und Lehre von den positiven Vertragsverletzungen, AcP 135 (1932), 255 (268ff); für Österreich insbesondere: *Gschnitzer* in *Klang/Gschnitzer,* ABGB IV/1^2 (1968) 471; *ders,* Österreichisches Schuldrecht, Allgemeiner Teil^2 (1991) 120; *Schlesinger,* Die vorläufige und die endgültige Nichterfüllung. – Die Lehre von den positiven Vertragsverletzungen und ihr Einfluss auf das deutsche Recht. – Das Wesen der positiven Vertragsverletzungen, ZBl 1926, 1ff, 401ff, 721ff.

[80] *Staub,* Die positiven Vertragsverletzungen^2 (1913) 14.

Auch *Staub* geht somit schon nach seinen eigenen Worten eindeutig von der Verletzung einer geschuldeten Verbindlichkeit aus. Eine überzeugende Erklärung, warum sich diese Verletzung weder als Unmöglichkeit noch als Verzug qualifizieren lassen sollte, bleiben uns *Staub* und die ihm Folgenden letztlich schuldig. Deren Auffassung lässt sich nur durch eine Art Tunnelblick auf die Hauptleistungspflichten erklären. Nach dieser Ansicht können nur auf diese die Regeln über Verzug und Unmöglichkeit angewendet werden. Der Schuldner schuldet aber eben mehr als nur die Hauptleistungspflichten. Neben diesen – und das wird wie oben zitiert von *Staub* auch ausdrücklich anerkannt – schuldet er zudem Schutz- und Sorgfaltspflichten. Verletzt er diese, ist zu klären, ob die Erfüllung der Pflicht endgültig vereitelt wurde oder ob eine Nachholung noch möglich ist. Ersterenfalls liegt Unmöglichkeit, zweiterenfalls liegt Verzug vor.

> Beispiel: Nehmen wir wiederum an, den Provider trifft die Pflicht, ein von einer Sicherheitsbehörde an ihn herangetragenes Auskunftsbegehren gewissenhaft zu überprüfen und unzureichend begründeten Auskunftsbegehren keine Folge zu leisten. Er erhält ein mangelhaftes Auskunftsbegehren, das er eigentlich ablehnen müsste. Aus Unachtsamkeit des für die Prüfung bestellten Mitarbeiters werden die gewünschten Daten der Behörde dennoch preisgegeben. Die Pflicht, die Privatsphäre seines Kunden zu schützen, erfüllt der Provider so lange er unzureichende Auskunftsbegehren ablehnt und die Behörde von den unzulässigerweise abgefragten Daten keine Kenntnis nimmt. Da die Pflichtverletzung des Providers in diesem Beispiel irreversibel ist, liegt hier Unmöglichkeit vor. Ab der Preisgabe der Daten ist eine Rückkehr zu jenem Zustand, in welchem die Behörde keine Kenntnis von den Daten hatte und der Provider seine Schutzpflicht erfüllt, nicht mehr möglich.

Weigert man sich jedoch, die Bestimmungen über den Verzug bzw die Unmöglichkeit auch auf die Verletzungen von Nebenpflichten anzuwenden, ist es erforderlich, für Schutzpflichtverletzungen eine eigene Rechtsfigur zu erfinden[81]. Dieser Lehre liegt, wie von *Himmelschein* zu Recht betont wird, der Gedanke zugrunde, den Begriff Leistung mit seiner ökonomischen Parallele „Lieferung" gleichzusetzen[82]. Kein Zweifel kann indes daran bestehen, dass der Wortlaut der Bestimmungen des ABGB (und des BGB) zu Verzug und Unmöglichkeit eine Subsumtion von Schutzpflichtverletzungen unter die Bestimmungen zu Verzug und Unmöglichkeit jedenfalls erlaubt. In Bezug auf die deutsche Rechtslage wurde eine derartige Subsumtion zwar als „gekünstelt und geschraubt"[83] bzw als „allzu spitzfindig"[84] abgelehnt, aber es musste selbst von Kritikern

---

[81] *Gschnitzer* in *Klang/Gschnitzer,* ABGB IV/1[2] (1968) 472.

[82] *Himmelschein,* Erfüllungszwang und Lehre von den positiven Vertragsverletzungen, AcP 135 (1932), 255 (314).

[83] So *Staub,* Die positiven Vertragsverletzungen[2] (1913) 14.

[84] *Leonhard,* Allgemeines Schuldrecht des BGB I (1929) 537.

eingeräumt werden, dass diese Theorie zumindest denkbar und schlüssig ist[85]. Es wurde versucht, aufzuzeigen, dass dem Gesetz kein derart weiter Unmöglichkeitsbegriff zugrunde liege, sondern sich dieser Begriff stets nur auf die Hauptleistungspflicht beziehe. Gestritten wurde dabei auch darüber, welches Begriffsverständnis *Mommsen*[86] dem BGB zugrunde legte[87]. Derartigen Versuchen ist jedoch von vornherein mit Skepsis zu begegnen. Wo sich die Wissenschaft zu sehr auf den angeblichen Willen des Gesetzgebers konzentriert, werden insbesondere bei so alten Kodifikationen wie dem BGB oder dem ABGB schnell die Grenzen der historischen Interpretation deutlich, zumindest wenn man sich ausschließlich auf den nicht exakt dokumentierten Willen einzelner am Entstehungsprozess Beteiligter konzentriert. Neben dem Alter der Kodifikation steht vor allem auch die Komplexität des Gesetzgebungsprozesses bei einer so umfassenden Kodifikation einem einfachen Ausfindigmachen des einen gesetzgeberischen Willens entgegen[88]. So hilft es wenig, einzelne Sätze großer Vertreter der deutschen Zivilistik herauszugreifen und als Beweis für den einen oder anderen Standpunkt vorzulegen[89]. Am Gesetzgebungsprozess sind auch stets Personen beteiligt, deren persönlicher Willen, selbst wenn er sich exakt bestimmen ließe, mangels deren Legitimation für die Auslegung des Gesetzes eigentlich keine Bedeutung haben dürfte. Wieso sollte es beispielsweise in einer Demokratie entscheidend sein, was sich ein einzelner Legist in einem Ministerium beim Entwurf eines Gesetzestextes dachte? Selbst wenn man zur Auffassung gelangen sollte, dass es für die Auslegung des BGB darauf ankäme, was ein zur Gesetzgebung letztlich nicht legitimierter Jurist wie *Mommsen* gedacht hat, so wird man bald feststellen, dass andere mit gleichermaßen überzeugenden Argumenten zum gegenteiligen Ergebnis gelangen[90]. ME sollte daher die

---

[85] *Stoll,* Abschied von der Lehre der positiven Vertragsverletzungen, AcP 136 (1932), 257 (274); vgl auch *Ehrenzweig,* System des österreichischen Privatrechts II/1[6] (1929) 271, der es als „unnütze Künstelei" ablehnt, die positiven Vertragsverletzungen unter den Gesichtspunkt der Unmöglichkeit der Leistung zu bringen. Dies tut er allerdings mit Blick auf die österreichische Rechtslage (§ 1295 ABGB), siehe dazu noch unten 3.2.

[86] *Mommsen,* Beiträge zum Obligationenrecht, 1. Abtheilung, Die Unmöglichkeit der Leistung in ihrem Einfluss auf obligatorische Verhältnisse (1853).

[87] Vgl etwa *Stoll,* Abschied von der Lehre der positiven Vertragsverletzungen, AcP 136 (1932), 257 (269ff).

[88] *Himmelschein,* Erfüllungszwang und Lehre von den positiven Vertragsverletzungen, AcP 135 (1932), 255 (315ff), der diese Probleme ebenso erwähnt, aber der die Bedeutung der historischen Interpretation besonders betont.

[89] So tut dies etwa *Stoll,* Abschied von der Lehre der positiven Vertragsverletzungen, AcP 136 (1932), 257 (270): Er zitiert folgenden Satz *Mommsens*: „Eine solche Anzeige kann aber nie als eine unmögliche Leistung betrachtet werden." Durch diesen einzelnen Satz versucht *Stoll* nun zu beweisen, dass der Unmöglichkeitsbegriff *Mommsens* sich nicht auch auf Nebenverpflichtungen, wie die Verpflichtung zu einer Anzeige, beziehen könne.

[90] So meint etwa *Wittwer*, Die positive Vertrags- oder Forderungsverletzung, ÖJZ 2005, 161 (162) im Gegensatz zu *Stoll* (vgl FN 89), dass *Mommsens* Unmöglichkeitsbegriff weit gehe und daher auch Fälle der Schlechterfüllung erfasse.

Wortinterpretation des Gesetzes im Mittelpunkt stehen. Erkennt man an, dass wie alle anderen Pflichten auch Schutzpflichten geschuldet werden, kommt man zum Ergebnis, dass eine Erfüllung dieser Pflichten stets nur entweder endgültig vereitelt oder aber vorübergehend verhindert sein kann. Eine andere Konstellation ist denkunmöglich[91]. Für diese Fälle traf der Gesetzgeber Vorsorge, indem er Vorschriften über Verzug und Unmöglichkeit normierte. Es gibt keine „dritte Form" von Vertragsverletzungen und somit auch keine Lücke im BGB. Eine Subsumtion unter die Verzugs- bzw Unmöglichkeitsvorschriften ist problemlos möglich, weshalb nicht einzusehen ist, weshalb zunächst eine Lücke herbeigedichtet werden muss, die dann ohnedies wieder durch Analogien zu den Verzugsvorschriften geschlossen wird. Dabei sollte es keine Rolle spielen, ob dies auch von sämtlichen an der Entstehung des BGB beteiligten Personen so vorausgedacht wurde. *Staub* meint, wer das Gesetz so auslege, presse hier etwas in „das Prokrustesbett des Gesetzestextes"[92], was dort nicht hingehöre. Dabei übersieht er jedoch, dass nur weil diese Lesart seinem an dieser Stelle mehrfach angeführten „Gefühl" bzw einer von ihm behaupteten „natürlichen Auffassung" widerspricht, von einer „gewaltsamen Prokrustesauslegung"[93] nicht die Rede sein kann. Vielmehr gibt er impliziter zu, dass diese Auslegung – wenn auch nur unter „Zwang" – möglich ist[94]. Damit bringt er sich jedoch um die Grundlage jedweder Analogie. Ohne Lücke ist an die analoge Anwendung von Vorschriften nicht zu denken[95]. Lassen sich die von *Staub* angeführten Fälle unter bestehende Vorschriften subsumieren, liegt keine Lücke vor und die Bestimmungen sind anzuwenden.

---

[91] *Gschnitzer* in *Klang/Gschnitzer,* ABGB IV/1^2 (1968) 471.

[92] *Staub,* Die positiven Vertragsverletzungen^2 (1913) 13.

[93] *Staub,* Die positiven Vertragsverletzungen^2 (1913) 19.

[94] Auch andere räumen dies ein, vgl etwa: *Esser/Schmidt,* Schuldrecht I/1^8 (1992) 108.

[95] Vgl nur *Bydlinski,* Juristische Methodenlehre und Rechtsbegriff^2 (1991) 472; *ders* in Rummel*,* ABGB I^3 (2000) § 7 Rz 2, *ders*, Die Feststellung von Lücken im Gesetz, Besprechung des gleichnamigen Werkes von *Canaris,* JBl 1968, 221 (222); *Ehrlich*, Die Lücken im Recht, JBl 1888, 447 (447); *Öhlinger,* Auslegung des öffentlichen Rechts, JBl 1971, 284 (287ff); vgl auch OGH 23.03.1976, 4 Ob 313/76, SZ 49/45 = EvBl 1976/263 S 606 = JBl 1976, 490 = GRURInt 1977, 211; OGH 24.04.1990 10 ObS 135/90, JBl 1991, 57 = ZAS 1991, 210 (*Müller*) = SSV-NF 4/66.

3.2. Rechtsfolgen der positiven Forderungsverletzungen im ABGB

3.2.1. Historische Erwägungen

Oben wurde bereits ausgeführt, dass *Staub* mehr oder minder nachvollziehbar darzulegen versuchte, dass die von ihm bezeichneten Fälle – das Zuwiderhandeln gegen eine Unterlassungspflicht bzw die zu weiteren Schäden führende fehlerhafte Erfüllung der Hauptleistungspflicht – im BGB keine einschlägige Regelung erfahren hatten. Auch in Österreich sprechen Standardlehrbücher wie jenes von *Koziol* und *Welser* wie auch der OGH ganz selbstverständlich von den positiven Vertragsverletzungen, sodass auf den ersten Blick Zweifel an den dogmatischen Grundlagen dieses Rechtsinstitutes nie in Frage kommen würden. Nahe liegend wäre etwa die Vermutung, dass auch das österreichische Recht eine ähnliche „Lücke" wie das deutsche BGB enthält, die es in Anlehnung an die deutsche Lehre zu schließen galt. Als in Deutschland der von *Staub* vom Zaun gebrochene Streit rund um die positiven Vertragsverletzungen in Gang kam, stand das ABGB noch vor seinen 3 Teilnovellen[96]. Wie im Folgenden zu zeigen ist, enthielten die positiven Bestimmungen jedoch sowohl vor als auch nach den Novellierungen einschlägige Bestimmungen zu den von *Staub* skizzierten Fällen, weshalb die Übernahme des Instituts der positiven Forderungsverletzungen fragwürdig erscheint.

Der Herrenhausbericht (HHB) zur III. Teilnovelle geht offenkundig – wie auch *Staub* – davon aus, dass es sich bei den positiven Vertragsverletzungen um einen dritten Typ von Vertragsverletzungen neben Verzug und Unmöglichkeit handelt[97]. Der HHB versteht – im Unterschied zur RV[98] – im Anschluss an die Lehre *Staubs* unter dem Begriff der positiven Vertragsverletzungen sowohl das Zuwiderhandeln gegen Unterlassungspflichten als auch die den Gläubiger an seinem Vermögen schädigende Schlechterfüllung[99]. Allerdings ging die Herrenhauskommission, wie uns ihr Bericht eindeutig zeigt, auch davon aus, dass die positiven Vertragsverletzungen allesamt von

---

[96] 1. Teilnovelle vom 12. Oktober 1914, RGBl 276; 2. Teilnovelle vom 22. Juli 1915, RGBl 208; 3. Teilnovelle vom 19. März 1916, RGBl 69.

[97] HHB 78 BlgHH, XXI. Sess, 1912, 163.

[98] RV 2 BlgHH, XXI. Sess, 1911, 138: *„§ 146 behandelt den Fall der positiven Vertragsverletzung im engeren Sinne. Diese besteht darin, dass einer Verpflichtung zu einer Unterlassung zuwider gehandelt wird. Jede einzelne Zuwiderhandlung gegen die Unterlassungspflicht begründet an sich einen Schadenersatzanspruch, der in concreto auch in dem Anspruch auf Rückleistung des Entgelts sich verwirklichen kann[...]*"

[99] HHB 78 BlgHH XXI. Sess, 1912, 164.

den Regelungen des ABGB erfasst sind[100]. Vor der III. Teilnovelle haben die §§ 919 und 1295 ABGB, nach der Novellierung 1916 die §§ 918 Abs 1, 920 ABGB sowie 1295 ABGB lückenlos alle Fälle der so genannten positiven Vertragsverletzungen eindeutigen Regelungen zugeführt[101]. So meint der HHB: *„[...] Und diese alten Gesetzesworte[102] haben noch den großen Vorzug vor der moderneren Fassung, daß sie in jüngster Zeit auf dem Boden des Deutschen BGB lebhaft erörterten Zweifelsfall erledigen, dem die RV einen eigenen Paragraphen, § 146, widmen zu müssen glaubt (Erl 138): die so genannte „positive Vertragsverletzung". Damit wollte offenbar die Lücke des Deutschen Gesetzbuches ausgefüllt werden, die eine vielgenannte Abhandlung von Staub „Die positiven Vertragsverletzungen" (1904) aufgedeckt hat (vgl Kiß aaO) – eine Lücke, die dadurch entsteht, daß das BGB nur die Haftung des Schuldners, falls die Leistung durch einen von ihm zu vertretenden Umstand „unmöglich wird" (§§ 280, 325 BGB), oder falls er mit der Leistung „im Verzuge" ist (§§ 286, 326 BGB), regelt, während eine gleiche Vorschrift fehlt „für die zahlreichen Fälle, in denen jemand eine Verbindlichkeit durch positives Tun verletzt, in denen jemand tut, was er unterlassen soll, oder die Leistung zwar bewirkt, aber fehlerhaft bewirkt (Staub aaO S 5). Für das ABGB, wenn anders seine einschlägigen Sätze in ihrer Einfachheit erhalten bleiben, existiert diese Lücke gar nicht. Denn der „allgemeine Rechtsgrundsatz", den Staub (aaO S 6) für das deutsche Recht praeter legem postuliert, steht uns bereits im Gesetze, § 1295 ABGB. Schon die Gleichstellung deliktischer Beschädigung (die ja zumeist Verletzung einer Unterlassungspflicht ist) und der Übertretung einer Vertragspflicht in § 1295 genügt, um jeden Zweifel daran auszuschließen, daß auch das Zuwiderhandeln gegen eine vertragsmäßige Unterlassungspflicht oder mangelhafte Vertragserfüllung grundsätzlich dieselben Rechtsfolgen hat wie das Ausbleiben einer positiven Leistung. Und dasselbe bestätigt § 912 ABGB („Ersatz dessen, was dem anderen daran liegt, daß die Verbindlichkeit nicht gehörig erfüllt worden") und wird auch künftig von § 918 bezüglich der neu normierten Rechtsfolgen bestätigen, indem er, wie bisher § 919 ABGB, diese Rechtsfolgen für alle Fälle statuiert, wo nicht auf die bedungene Weise geleistet wird. Endlich wird es, sobald einmal die Gleichheit der Folgen positiver und negativer Vertragsverletzungen feststehen, gewiß keinem Bedenken unterliegen, bei dauernder*

---

[100] Das bedeutet, durch die III. Teilnovelle sollte gerade nicht die in Deutschland erfundene und immer weiter entwickelte Lehre der positiven Vertragsverletzungen ins österreichische Recht übernommen werden, so auch *Kerschner,* Probleme der Sachmängelhaftung. Oder: Das ABGB ist tot – Es lebe das BGB! JBL 1989, 541 (542); aA *Honsell,* Aktuelle Probleme der Sachmängelhaftung, JBl 1989, 205 (209).

[101] HHB 78 BlgHH XXI. Sess, 1912, 163ff.

[102] Damit ist die Textierung des weiter unten wiedergegebenen § 919 ABGB idF vor der III. Teilnovelle gemeint. Insbesondere die damals in § 919 ABGB und heute in § 918 Abs 1 ABGB vorzufindende Wendung „nicht auf die bedungene Weise" erfasst nach Ansicht der Herrenhauskommission auch die in Deutschland unter der Bezeichnung „positive Vertragsverletzung" erfassten Phänomene.

Unterlassungspflicht das einmalige Zuwiderhandeln als eine „teilweise Vereitelung" (Mahr, 79) unter die Sanktion des (neuen) § 920 zu stellen[103]*, die dem praktischen Bedürfnisse (Rücktritt vom Vertrage, wenn die spätere Einhaltung der Unterlassungspflicht für den anderen „kein Interesse mehr hat") vollkommen genügt. Deshalb konnte § 146 RV (gegen dessen Fassung auch sonst schon begründete Einwendungen erhoben wurden, Wellspacher I, 20) gestrichen werden.*"

Die Übertretung einer Vertragspflicht – egal ob negativer oder positiver Natur – machte seit dem In-Kraft-Treten des ABGB und damit bereits vor der III. Teilnovelle gemäß § 1295 ABGB ersatzpflichtig. § 932 ABGB ordnete in seiner damaligen Fassung eine Ersatzpflicht für Mangelfolgeschäden an:

„[...] in beiden Fällen aber auch den Ersatz des weiteren Schadens, und, dafern der andere Theil unredlich gehandelt hat, auch den entgangenen Gewinn fordern."[104]

Zu jenem Zeitpunkt, als in Deutschland *Staub* sein erstes Werk zu den positiven Vertragsverletzungen veröffentlichte, hatte § 919 ABGB folgende Fassung:

„Wenn ein Theil den Vertrag entweder gar nicht; oder nicht zu der gehörigen Zeit; an dem gehörigen Orte; oder auf die bedungene Weise erfüllet; so ist der andere Theil, außer den in dem Gesetze bestimmten Fällen, oder einem ausdrücklichen Vorbehalte, nicht berechtigt, die Aufhebung, sondern nur die genaue Erfüllung des Vertrages und Ersatz zu fordern."

Auch *Schlesinger* kommt zum Ergebnis, dass alle jene Fälle, für die im deutschen BGB mühsam nach einer Lösung gesucht werden musste, immer schon durch die §§ 919 (in seiner Fassung vor der III. Teilnovelle) bzw 918 Abs 1 (in seiner Fassung nach der III. Teilnovelle) und 1295 ABGB geregelt waren bzw sind[105]. Sofern eine Vertragsverletzung vorliege, mache diese nach § 1295 ABGB stets schadenersatzpflichtig. Die Schadenersatzpflicht ergibt sich daraus, dass hier eine

---

[103] Anders hingegen die RV 2 BlgHH XXI. Sess, 1911, 138: *„Ist aber die Wiederholung der Zuwiderhandlung möglich, so entsteht für den Gläubiger, da sich § 143 des Entwurfes auf diese Fälle nicht anwenden lässt, aus der Vorschrift des § 919 ein der Absicht der Parteien beim Vertragsabschlusse sicherlich nicht entsprechender Zustand der Schutzlosigkeit. Parallel dem im § 143 gewährten Rechte zur Festsetzung einer Nachfrist gewährt daher der Entwurf im § 146 das Recht des Rücktritts für den Fall wiederholter Zuwiderhandlung [...]*"

[104] Vgl dazu auch *Stubenrauch,* Commentar zum Allgemeinen bürgerlichen Gesetzbuche II^5 (1888) 281; allerdings hatte sich lange Zeit die Rechtsprechung verfestigt, dass der Übergeber nur den durch seine Mangelunkenntnis erlittenen Schaden zu ersetzen habe, vgl dazu *Binder* in *Schwimann,* ABGB V^2 (1997) Rz 69ff zu § 932.

[105] *Schlesinger,* Die Lehre von den positiven Vertragsverletzungen und ihr Einfluss auf das österreichische Recht, ZBl 1926, 401 (407ff); zum selben Ergebnis kommt auch *Lenhoff,* Positiven und negative Vertragsverletzungen gegenseitiger Verträge, ZBl 1917, 385 (387); ebenso *Schöndorf*, Über den Entwurf einer Novelle zum österreichischen ABGB, Archiv für Bürgerliches Recht 39 (1913) 120 (188).

Vertragspflicht übertreten wurde. Für diese Ersatzpflicht müsste der Begriff der positiven Forderungsverletzungen eigentlich nicht bemüht werden[106].

§ 919 ABGB idF vor der III. Teilnovelle räumt dem Vertragspartner desjenigen, der nicht „auf die bedungene Weise erfüllet" das Recht ein, die genaue Erfüllung des Vertrages und außerdem Ersatz zu fordern[107]. Die Wendung „auf die bedungene Weise" bedeutete somit stets, dass der Gläubiger die präzise Leistung durch den Schuldner fordern konnte. Der Schuldner ist dem Gläubiger zur exakten, dh auch alle Nebenpflichten umfassenden, Erfüllung der Verbindlichkeit verpflichtet. Die Rechtsfolgen aus einem Verstoß gegen diese Verpflichtung wurden durch die Teilnovelle geändert. Während § 918 Abs 1 ABGB dem Gläubiger heute den Rücktritt ermöglicht, zwang § 919 ABGB den Gläubiger außer bei Unmöglichkeit grundsätzlich am Vertrag festzuhalten und verwies ihn auf Schadenersatzansprüche. Das ändert aber nichts daran, dass der Fall, dass ein Schuldner seine Verbindlichkeit nicht exakt erfüllt, indem er eine ihn ebenfalls treffende Schutz- bzw Sorgfaltspflicht verletzt, im ABGB seit jeher geregelt war.

1917 ging man auch davon aus, dass das ABGB in seiner novellierten Fassung die positiven Forderungsverletzungen eindeutig regle: *„Jedenfalls hat aber die Novelle durch ihre Normierung jene Schwierigkeiten überwunden, mit welchen die deutsche Rechtswissenschaft in der Lehre von den positiven Vertragsverletzungen zu rechnen hat [...]"*[108].

3.2.2. Die Anwendbarkeit des Leistungsstörungsrechts auf die positiven Forderungsverletzungen

In Österreich hat sich all diesen Erwägungen und der berechtigten Kritik[109] zum Trotz der Begriff der positiven Vertragsverletzungen etabliert[110] und wird heute von

---

[106] So auch *Reischauer* in Rummel, ABGB I³ (2000) §§ 918-933 Rz 4.

[107] *Stubenrauch,* Commentar zum österreichischen allgemeinen Gesetzbuche II⁵ (1888) Anm 2 zu § 919.

[108] *Lenhoff,* Positive und negative Vertragsverletzungen gegenseitiger Verträge, ZBl 1917, 385 (388); aA *Ehrenzweig,* System des österreichischen Privatrechts II/1² (1928) 209; *Pisko,* Die subjektiven Voraussetzungen des Rücktrittsrechts nach § 918 ABGB, JBl 1920, 241 (241); die beiden letzten schlüssig widerlegend: *Schlesinger,* Die Lehre von den positiven Vertragsverletzungen, ZBl 1926, 401 (414ff).

[109] *Barta,* Zivilrecht (2000), 269; *Gschnitzer* in *Klang/Gschnitzer,* ABGB IV/1² (1968) 472; *ders/Faistenberger,* Österreichisches Schuldrecht, Allgemeiner Teil² (1991) 120; *Ehrenzweig/Mayrhofer,* Das Recht der Schuldverhältnisse, Allgemeine Lehren³ (1986) 352ff; *Reischauer* in Rummel, ABGB I³ (2000) Vor §§ 918-933 Rz 4; *Schlesinger,* Die Lehre von den positiven Vertragsverletzungen, ZBl 1926, 401 (407ff); in der 2. Auflage meint *Binder* in *Schwimann,* Praxiskommentar ABGB V² (1997) Rz 48 zu § 918 noch wörtlich: *„[...] Es ist daher mit – Mayrhofer und Reischauer – weiterhin zweckmäßiger Weise die Nichterfüllung iwS in Verzug, Vereitelung und Schlechtleistung zu unterteilen. Dies entspricht auch dem Aufbau des ABGB. Zur Schaffung eines Auffangbeckens für jene Schäden, die nicht unmittelbar aus der gänzlichen oder teilweisen Nichterbringung der Leistung resultieren, also der*

der Rechtsprechung in einer Vielzahl von Entscheidungen verwendet[111]. Begründet wurde dies etwa damit, dass der Schaden aus positiven Forderungsverletzungen gegenüber Verzugs- und Unmöglichkeitsschäden die Eigenheit aufweise, dass er bei völliger Nichterfüllung nie entstanden wäre[112]. Der entstandene Schaden sei von jenem zu unterscheiden, der in der gänzlichen oder teilweisen Nichterbringung der geschuldeten Leistung bestehe[113]. Das mag vielleicht zutreffen, offen bleibt freilich jedoch, inwieweit diese Eigenart nach der Einführung eines gesetzlich nicht positivierten Rechtsinstituts verlangt. Sieht man etwa in der Offenbarung der Identität eines Kunden durch den Provider gegenüber einer Auskunft suchenden Behörde eine Schutzpflichtverletzung, so wurde die (Geheimhaltungs-)pflicht irreversibel verletzt. Die Erfüllung der Geheimhaltungspflicht ist nicht mehr möglich, es liegt daher Unmöglichkeit in Bezug auf die verletzte Schutzpflicht vor. Der Schaden, der hieraus resultiert, ist, systematisch betrachtet, kein anderer als jener, der aus der Unmöglichkeit der Erfüllung einer Hauptleistungspflicht resultiert. Es ist ein Schaden, der sich aus der Nichterfüllung einer Pflicht ergibt.

Auch Befürworter dieser Begrifflichkeit räumen selbst ein, dass sich die Haftung für Schäden aus der positiven Vertragsverletzung unmittelbar aus den allgemeinen positiven Grundlagen des Schadenersatzrechts, insbesondere aus § 1295 ABGB ergebe[114]. Auch sie stützen die Ersatzpflicht wohl auf die Wendung „Übertretung einer Vertragspflicht". Diese „Übertretung" lässt sich jedoch stets unter das bestehende Leistungsstörungsrecht subsumieren.

Mangelfolgeschäden und Schäden aus allgemeinen Schutzpflichtverletzungen, besteht mE kein Bedarf." In der 3. Auflage änderte Binder allerdings seine Auffassung, siehe FN 110.

110 *Welser,* Bürgerliches Recht II[13] (2007) 5; *Bydlinksi P.,* Grundzüge des Privatrechts[2] (1994) 152; Neuerdings befürwortet auch *Binder* die Aufrechterhaltung dieses Rechtsinstitutes (*Binder/Reidinger* in *Schwimann,* Praxiskommentar ABGB IV[3] (2005) § 918 Rz 21): *„[...] Obwohl dem Aufbau unseres Gesetzes entsprechend weiterhin die Nichterfüllung iwS in Verzug, Vereitelung und Schlechtleistung zu unterteilen ist, macht die Schaffung eines Auffangbeckens für jene Schäden, die nicht unmittelbar aus der gänzlichen oder teilweisen Nichterbringung der Leistung resultieren, also der Mangelfolgeschäden oder Schäden aus allgemeinen Schutzpflichtverletzungen, gegen einen Teil der Lehre durchaus Sinn.*"

111 Vgl dazu etwa OGH 7.9.1994, 3 Ob 544/94: *„[...] Entgegen den Ausführungen von Reischauer* in *Rummel[2] Rz 4 vor §§ 918 bis 933 ABGB, daß diese Rechtsfigur als Scheinkategorie zivilisierten Rechtsordnungen (wozu er die deutsche offensichtlich nicht zählt) unbekannt ist und der Oberste Gerichtshof gut daran tut, sie bis jetzt grundsätzlich zu ignorieren, verwendete der Oberste Gerichtshof sehr wohl diese juristische Begriffsbildung bereits in den Entscheidungen SZ 59/159 und SZ 64/9. Sie eignet sich sehr wohl zur Charakterisierung der Verletzung vertraglicher Schutzpflichten während des Bestehens eines Dauerschuldverhältnisses (vgl Koziol in JBl 1994, 211).*" Das ließ *Reischauer* natürlich nicht auf sich sitzen, s *Reischauer* in Rummel, ABGB I[3] (2000) Rz 4 Zu §§ 918-933.

112 *P. Bydlinksi,* Grundzüge des Privatrechts[2] (1994) 152.

113 OGH 11.3.1998, 3 Ob 382/97s.

114 *P. Bydlinksi,* Grundzüge des Privatrechts[2] (1994) 152.

Nachdem die Verletzung einer vertraglichen Schutzpflicht nach dem oben Gesagten stets nur in einer Verzögerung oder Vereitelung bestehen kann, muss man konsequenterweise auch eine Rücktrittsmöglichkeit nach den §§ 918ff ABGB zugestehen. Dazu konnte sich die Rechtsprechung jedoch bislang kaum durchringen. So meinte der OGH in einem Fall, in welchem er die vertragswidrige Untervermietung grundsätzlich als positive Vertragsverletzung anerkannte: *„Es nicht richtig, dass jede Vertragsverletzung das Recht zur Auflösung des Vertrages gibt, denn § 918 ABGB handelt nur von der Nichterfüllung des Vertrages, nicht aber von den so genannten positiven Vertragsverletzungen, die nur dann, wenn dies im Gesetz oder Vertrag begründet ist, ein Rücktrittsrecht geben, und seine Anwendung ist überhaupt ausgeschlossen bei jenen Verträgen, bei welchen das Gesetz Sonderbestimmungen über die Auflösung enthält, wie dies bezüglich des Bestandvertrages laut § 1118 ABGB der Fall ist [...]"*[115].

Mit *Schlesinger* ist jedoch anzunehmen, dass dem Gläubiger auch dann ein Rücktrittsrecht zustehen kann, wenn der Schuldner die Erfüllung einer Schutzpflicht verzögert oder vereitelt[116]. Das legt schon der Wortlaut des § 918 Abs 1 ABGB („oder nicht auf die bedungene Weise") eindeutig nahe. Ebenso geht der HHB (siehe dazu schon oben) wie gezeigt eindeutig davon aus, dass auch Schutzpflichtverletzungen zu den in den §§ 918ff ABGB angeordneten Rechtsfolgen führen. Es ist auch nicht notwendig, die Verzögerung oder Vereitelung von Nebenpflichten der Verzögerung oder Vereitelung von Teilleistungen gleichzustellen und darauf die im ABGB enthaltenen Regeln (§§ 918 Abs 2, 920 2. Satz) analog anzuwenden[117]. Die Lückenschließung durch Analogie würde zunächst eine Lücke voraussetzen, die noch dazu planwidrig sein müsste. Dass der Gesetzgeber auf die Verletzung von Schutz- und Sorgfaltspflichten vergessen hätte, kann ihm vor dem Hintergrund des oben dargestellten HHB[118] nicht ernsthaft unterstellt werden. Dennoch versuchen es manche. *Gschnitzer*[119] etwa gesteht zunächst zwar ein, dass der Wortlaut des § 918 ABGB auch die „Verzögerung oder Vereitelung von

---

[115] OGH 7.10.1930, 4 Ob 430/30, ZBl 1930, Entscheidung 139; In eine andere Richtung weist etwa OGH 17.2.1920, Rv III 44/20, SZ II/12: Dort gerät der Käufer mit einer Vorleistung (Lieferung von Gebinden für den gekauften Most) in Verzug. Der OGH sprach aus, dass dies keinen Annahmeverzuge darstelle, sondern als Nebenpflichtverletzung den Verkäufer gemäß § 918 ABGB zum Rücktritt berechtige.

[116] *Schlesinger,* Das Wesen der positiven Vertragsverletzungen, ZBl 1926, 721 (733); ebenso *Gschnitzer/Faistenberger,* Österreichisches Schuldrecht, Allgemeiner Teil^2 (1991) 119; aA etwa *Ehrenzweig,* System des österreichischen allgemeinen Privatrechts^2 (1928) 207, der allerdings meint, dass eine Leistung – mag sie auch als Nebenleistung zu qualifizieren sein – wenn der Gläubiger an ihr ein besonderes Interesse hat, als Hauptleistung zu werten ist und diesfalls ein Rücktritt möglich ist.

[117] So aber *Pisko,* Lehrbuch des österreichischen Handelsrechts (1923) 185; *Gschnitzer* in *Klang/Gschnitzer,* ABGB IV/1^2 (1968) 468; *Bydlinksi* in *Klang/Gschnitzer,* ABGB IV/2^2 (1978) 324ff.

[118] HHB 78 BlgHH XXI. Sess, 1912, 163ff.

[119] *Gschnitzer* in *Klang/Gschnitzer,* ABGB IV/1^2 (1968) 468.

Nebenpflichten[120] zu decken scheint" und meint allerdings in weiterer Folge, dass „kein Verkehrsbedürfnis" nach einem in so weitem Umfang gewährten Rücktrittsrechte bestünde[121]. Daher seien die Bestimmungen der §§ 918ff ABGB insofern teleologisch so zu reduzieren, dass sie die Fälle der Verletzung von Nebenleistungspflichten nicht erfassen. Die Verletzung von Nebenpflichten gleiche allerdings in gewissen Punkten den Fällen der teilweisen Nichterfüllung einer Hauptleistungspflicht, weshalb die diesbezüglichen Bestimmungen des ABGB – §§ 918 Abs 2, 920, 2. Satz, – analog angewendet werden könnten. Einen Text derart auszulegen, sodass er plötzlich Fälle nicht mehr regelt, die er nach dem klaren Wortlaut und seiner Historie sehr wohl mitbedacht hat, um in weiterer Folge die Existenz einer Lücke behaupten zu können, die es durch Analogie zu schließen gilt, darf zumindest als kühn bezeichnet werden.

Dass eine derartige Auslegung des Gesetzes nicht besonders überzeugend ist, wird auch bei *Koziol* deutlich[122]: Er verteidigt zunächst wiederum die Existenzberechtigung des Rechtsinstituts der positiven Forderungsverletzungen mit dem Argument, dass sich diese von den Leistungsstörungen Verzug und Unmöglichkeit besonders deutlich unterscheiden würden. Ein Grund, weshalb die Verletzung von Schutzpflichten sich von Verzug und Unmöglichkeit unterscheide, sei, dass bei Schutzpflichtverletzungen meist kein Rücktrittsrecht zustehe. Dabei handelt es sich mE um einen Zirkelschluss: Richtigerweise müssten Schutzpflichtverletzungen unter die §§ 918ff ABGB subsumiert und konsequenterweise ein Rücktrittsrecht zugestanden werden. Aus der gebräuchlichen Praxis, die entgegen dem Wortlaut der §§ 918ff ABGB kein Rücktrittsrecht zugesteht, die Eigentümlichkeit der positiven Forderungsverletzungen abzuleiten erscheint mir unzulässig.

Die Unzulässigkeit eines Rücktritts bei Schutzpflichtverletzungen wird zT auch mit dem Argument gerechtfertigt, dass die Schutzpflichten nicht im Austauschverhältnis stehen und das Leistungsstörungsrecht nur auf die im Synallagma stehenden Pflichten zugeschnitten sei[123]. Dass der eine Vertragspartner eine ihn treffende Schutzpflicht nach dem Prinzip „do ut des" nicht gerade wegen einer den anderen treffenden Schutzpflicht eingeht, wie dies bei den Hauptleistungspflichten der Fall ist, soll indes auch gar nicht bestritten werden. Dennoch akzeptiert ein Vertragspartner die ihn neben seinen Hauptleistungspflichten treffenden Schutzpflichten wohl nur deshalb, weil er darauf vertraut, dass auch der andere Vertragspartner die ihn

---

[120] Damit meint er freilich auch Schutzpflichten.

[121] In Deutschland werden zu § 326 BGB ähnliche Auffassungen vertreten, vgl etwa *Staub/Koenige,* Kommentar zum HGB[12] (1926) § 374 Anm 163.

[122] *Koziol,* Österreichisches Haftpflichtrecht II (1975) 67.

[123] *Koziol/Welser,* Bürgerliches Recht[12] II (2001) 3ff, 53.

treffenden Schutzpflichten einhält. Die wechselseitigen Schutzpflichten sind vor allem vom Vertrauensgedanken dominiert (vgl dazu ausführlich unten Kapitel 5.1.1). Wüsste er bereits vor Vertragsabschluss, dass sein Vertragspartner die ihn treffenden Schutzpflichten verletzen wird, würde ihn dies vermutlich vom Vertragsabschluss und somit auch vom Eingehen seiner Hauptleistungspflichten abhalten. Insofern besteht auch ein gewisser Zusammenhang zwischen den jeweiligen Schutzpflichten der beiden Vertragspartner und überdies auch zwischen deren Hauptleistungspflichten auf der einen und deren Schutzpflichten auf der anderen Seite. Es ist vor dem Hintergrund dieses Zusammenhangs nicht einzusehen, weshalb die Verletzung einer Schutzpflicht sich nicht etwa in Form eines Rücktritts auch auf die gegenseitigen Hauptleistungspflichten auswirken sollte.

Es ist schwierig, in diesem Punkt eine einheitliche Judikaturlinie des OGH zu bestimmen. Obwohl eine Tendenz dazu besteht, die §§ 918ff ABGB so zu reduzieren wie von *Gschnitzer* vorgeschlagen[124], gibt es auch Entscheidungen, die in eine ganz andere Richtung weisen. Teilweise wird auch bei Vereitelungen von Nebenpflichten (Schutzpflichten) ein Rücktritt gemäß § 920 ABGB zugestanden[125].

Diese dogmatisch nur mehr schwer nachvollziehbare und teils fast willkürlich anmutende Entscheidungspraxis ist noch am ehesten zu systematisieren, indem man auf das Interesse des Gläubigers nach der Pflichtverletzung abstellt: Hat die Pflichtverletzung zur Folge, dass der Gläubiger an der weiteren Vertragserfüllung sein Interesse verliert, wird ihm wie in 8 Ob 171/65 ein Rücktrittsrecht zuerkannt[126]. Ist die durch die Vertragsverletzung bewirkte Vertrauenserschütterung weniger schwer wiegend und besteht das Interesse des Gläubigers an der Vertragserfüllung weiter[127], steht kein

---

[124] So auch OGH 30.6.1966, 1 Ob 172/66, SZ 39/120.

[125] OGH 15.6.1965, 8 Ob 171/65: hier wurde die vereinbarte Nebenleistungspflicht des Verkäufers (befristetes Konkurrenzverbot im Ausland) verletzt, was dem Käufer den Rücktritt gem § 920 ABGB eröffnete.

[126] Vgl auch OGH 14.11.1984, 1 Ob 703/84, SZ 57/175: *„[...] die Verletzung von unselbstständigen Nebenpflichten rechtfertigt im Regelfall nicht den Rücktritt vom Vertrag gemäß § 918 ABGB; nur ausnahmsweise wird das Recht zum Rücktritt anerkannt, wenn die Verletzung der Nebenpflicht zugleich eine schwere Vertrauenserschütterung beinhaltet oder das Interesse an der Erfüllung des Vertrages überhaupt beseitigt.*" Vgl auch OGH 26.09.1951, 3 Ob 500/51, SZ 25/299; ähnlich urteilte auch das deutsche Reichsgericht seit der Erfindung der positiven Forderungsverletzungen, vgl RG 17.9.1918, III 100/18, RGZ 93, 285 (286): *„[...] Das Berufungsgericht hat das Vorliegen einer positiven Vertragsverletzung mit der Begründung verneint, daß der Beklagte die Erfüllung des Vertrages nicht endgültig verweigert habe. Dabei lässt es sich von einer zu engen Auffassung des bezeichneten Rechtsbegriffs leiten. Unter diesen fallen nach der feststehenden Rechtsprechung des Reichsgerichts alle solche vom Schuldner zu vertretenden positiven Zuwiderhandlungen gegen die Vertragspflichten, welche den Vertragszweck dergestalt gefährden, daß dem vertragstreuen Teile bei Berücksichtigung der Umstände des Falles die Fortsetzung des Vertrages nach Treu und Glauben nicht zuzumuten ist.*" *Staub,* Die Positiven Vetragsverletzungen[2] (1913), 20, schlägt vor, dass immer dann ein Rücktrittsrecht zustehen soll, wenn jemand „positive Rechtsverletzungsakte vornimmt, welche die Erreichung des Vertragszweckes gefährden."

[127] OGH 30.6.1966, 1 Ob 172/66, SZ 39/120.

Rücktrittsrecht zu[128]. Der Gläubiger, der sich wegen einer Schutzpflichtverletzung vom Vertrag lösen möchte, muss darauf hoffen, dass der Richter mit ihm zum Ergebnis kommt, dass die Verletzung eine schwerwiegende Vertrauenserschütterung darstellt. Dieses Ergebnis mag vielleicht befriedigend sein, der dorthin führende Weg ist aus dogmatischer Sicht jedoch weniger zufrieden stellend. Zu bevorzugen ist hier eine Auslegung, die sich mehr am Wortlaut und den eindeutigen historischen Argumenten orientiert. Das will heißen, dass der, der eine Schutzpflicht verletzt „nicht auf die bedungene Wiese leistet" und dem anderen daher stets eine Rücktrittsmöglichkeit eröffnet. Auch der Gläubiger einer vorübergehend oder endgültig vereitelten Nebenleistungspflicht muss nicht beweisen, dass er an der Leistung kein Interesse mehr hat. Die §§ 918ff ABGB gewähren ihm ohne weiteres den Rücktritt. Im Ergebnis ist dem OGH wohl zuzustimmen und es wird Fälle geben, in denen der Rücktritt aus dem Grunde der Verletzung einer Schutzpflicht unangemessen erscheint. In diesen Ausnahmefällen kann das Rücktrittsrecht aus den im nachfolgenden Kapitel erläuterten Gründen nicht gegeben sein. Die von mir vorgeschlagene Lösung kommt ohne das von den §§ 918ff ABGB nicht vorausgesetzte Kriterium des Wegfalls des Interesses an der Aufrechterhaltung des Vertrages aus.

3.2.3. Missbräuchliche Ausübung von Rücktrittsrechten

Nun möchte man vielleicht einwenden, dass es doch nicht angehen könne, wenn auch bereits die kleinste Verletzung von Neben- oder Schutzpflichten dem Gläubiger dieser Pflichten das Recht zum Rücktritt geben würde. Aber auch dafür kann im positiven Recht eine Lösung gefunden werden: Das ABGB enthält zwar kein dem § 226 dt BGB vergleichbares Schikaneverbot, jedoch kann man in Österreich mittels Rechtsanalogie zum gleichen Ergebnis kommen. *Gschnitzer* stellt die Behauptung auf, dass „auch die Bestimmung des § 1295 Abs 2 keinen hinlänglichen Schutz" gegen ausufernde Rücktrittsausübungen wegen Verletzungen von Nebenpflichten böte[129]. Er lässt für diese Feststellung jedoch in weiterer Folge jegliche Begründung vermissen, und zitiert nur die zutreffende Gegenmeinung *Schlesingers*[130]. Der Auffassung, das ABGB böte keinen Schutz vor missbräuchlicher Ausübung von Rücktrittsrechten darf hier entgegen getreten werden. In jenen Fällen, in denen die Ausübung des nach den §§ 918 bzw 920 ABGB an sich zustehenden Rücktrittsrechts gemessen an der Schwere der

---

[128] So auch *Bydlinski* in *Klang/Gschnitzer,* ABGB IV/2^2 (1978) 323.

[129] *Gschnitzer* in *Klang/Gschnitzer,* ABGB IV/1^2 (1968) 468; die Rechtsprechung folgt ihm dabei wörtlich: 30. 6. 1966, 1 Ob 172/66.

[130] *Schlesinger,* das Wesen der positiven Vertragsverletzungen, ZBl 1926, 721 (733).

Schutzpflichtverletzung schikanös wäre, darf dies einredeweise eingewendet werden. Das lässt sich freilich nicht ohne weiteres aus dem positiven Recht ableiten. § 1295 Abs 2 ABGB ist anders als § 226 dt BGB nicht als allgemeines Schikaneverbot formuliert[131]. Er bestimmt eigentlich nur, dass missbräuchliche Rechtsausübung schadenersatzpflichtig macht. Die Rechtsprechung hat allerdings erkannt, dass *„doch die Stellung missbräuchlicher Rechtsausübung unter die Sanktion der Schadenersatzpflicht (§ 1295 ABGB), ferner die rechtliche Gleichstellung des gegen die guten Sitten verstoßenden Tatbestandes mit dem gegen ein gesetzliches Verbot verstoßenden Tatbestand (§ 879 ABGB) sowie das Vorhandensein einer Reihe von Spezialbestimmungen des Gesetzes, die sich gegen missbräuchliche Rechtsausübung wenden (§§ 1212, 830 ABGB) die rechtliche Schlussfolgerung ergeben, dass einer missbräuchlichen Rechtsausübung einredeweise entgegengetreten werden kann.*"[132]

Das bedeutet, dass das Rücktrittsrecht wegen positiver Vertragsverletzung nur soweit ausgeübt werden darf, als diese Ausübung nicht als missbräuchlich qualifiziert werden kann. Bei der Beurteilung der Missbräuchlichkeit wird man mit dem gängigen von der Rechtsprechung entwickelten Kriterium wohl keine befriedigenden Ergebnisse erzielen. Nach der Rechtsprechung (insbesondere zu § 1295 Abs 2 ABGB) liegt Missbrauch dann vor, wenn dem Ausübenden *„jedes andere Interesse abgesprochen werden muss als eben das Interesse, dem anderen Schaden zuzufügen.*"[133] Dieses Kriterium müsste freilich an die hier erörterten Fälle angepasst werden. Nach dieser Formulierung wäre nämlich bei synallagmatischen Verträgen (§ 917 ABGB) eine missbräuchliche Ausübung des Rücktrittsrechts eigentlich denkunmöglich. Neben dem Interesse, dem anderen einen Schaden zuzufügen, wird der die Auflösung Begehrende stets zumindest auch deshalb am Rücktritt ein Interesse haben, da er dadurch selbst von seiner Verbindlichkeit befreit wird. Damit könnte sein Rücktritt aber nie mehr als missbräuchlich qualifiziert werden.

Grundsätzlich ist daher davon auszugehen, dass wie oben ausführlich dargelegt jegliche Vereitelung bzw Verzögerung vertraglicher Pflichten dem vertragstreuen Teil grundsätzlich eine Rücktrittsmöglichkeit eröffnet. Allerdings ist die Schwere der Vertragsverletzung zu berücksichtigen. Minder schwere Verletzungen können durchaus so beschaffen sein, dass sie bei objektiver Würdigung das Interesse des vertragstreuen Teils am Fortbestand des Vertragsverhältnisses unverändert fortbestehen

---

[131] Vgl allerdings *Ehrenzweig*, System des österreichischen allgemeinen Privatrechts II/1[2] (1928) § 391, 623: *„Die neue Bestimmung bietet also der Einrede der Arglist [...] die erwünschte gesetzliche Grundlage und stellt ihr eine entsprechende Klage zur Seite.*"

[132] OGH 11.5.1955, 7 Ob 227/55.

[133] Zuletzt: OGH 26.05.2009 1 Ob 239/08s.

lassen. Im Ergebnis wird daher auf ähnliche Kriterien abzustellen sein, wie es die Judikatur bislang in den meisten Fällen ohnedies schon tut. Der Vorteil dieser Lösung besteht jedoch darin, dass sie dogmatisch sauberer ist, da der Rücktritt – im Einklang mit dem Wortlaut und den Materialien – grundsätzlich zusteht und nur ausnahmsweise ausgeschlossen sein kann.

3.2.4. Einklagbarkeit von Schutzpflichten

Wie *Larenz* zu Recht betont, ist die gesonderte Einklagbarkeit von Schutzpflichten oft ein Problem, weil es ihnen meist an der Bestimmtheit fehlt, die für eine gerichtliche Leistungsklage eine von Amts wegen zu beachtende Klagsvoraussetzung[134] (§ 226 ZPO) ist. Die allgemeine Pflicht zum Schutz der Privatsphäre des Kunden erfüllt dieses Bestimmtheitsgebot nicht. Was diese Pflicht im Einzelnen mit sich bringt, welche Ausprägung sie im konkreten Fall annimmt, hängt von den Umständen des Einzelfalls ab[135]. In der Regel führt daher erst die schuldhafte Verletzung von Schutzpflichten zu vertraglichen sekundären Leistungspflichten[136]. Sollte die in Frage stehende Schutzpflicht jedoch im Einzelfall ausreichend konkretisierbar sein, ist die gesonderte Einklagbarkeit der Schutzpflicht mE zu bejahen[137]. Dies gilt etwa für Klagen über die Auskunft darüber, ob und bejahendenfalls welches Auskunftsbegehren erfüllt wurde. Kein überzeugendes Argument gegen die gesonderte Einklagbarkeit bildet mE der Einwand, dass Schutzpflichten keine Gegenleistungspflicht gegenüberstehe[138]. Die Hauptleistungspflichten aus unentgeltlichen Verträgen sind ebenfalls einklagbar. Jene Schutzpflichten, die sich wie die meisten Unterlassungspflichten ausreichend konkretisieren lassen, sollten mE gesondert eingeklagt werden können. Dies ergibt sich schon daraus, dass zwischen Hauptleistungspflichten und Schutz- und Sorgfaltspflichten wie bereits gezeigt kein substanzieller Unterschied besteht. Für manche Pflichten, die auch als Schutzpflichten hinsichtlich der Privatsphäre des Kunden aufgefasst werden können, gibt es auch ausdrückliche Rechtsgrundlagen. So bestimmt etwa § 27 Abs 1 DSG 2000, dass jeder Auftraggeber unrichtige oder entgegen den Bestimmungen des DSG 2000 verarbeitete Daten richtig zu stellen oder zu löschen hat.

---

[134] OGH 12.3.1991, 4 Ob 16/91, ÖBl 1991, 108.

[135] *Stürner,* Der Anspruch auf Erfüllung von Treue- und Sorgfaltspflichten, JZ 1976, 384 (386).

[136] *Larenz,* Lehrbuch des Schuldrechts I/1[13] (1982) 11ff; gegen jegliche Einklagbarkeit von Schutzpflichten *Welser*, Bürgerliches Recht II[13] (2007) 6

[137] *Stürner,* Der Anspruch auf Erfüllung von Treue- und Sorgfaltspflichten, JZ 1976, 384 (388).

[138] Dies andeutend *Welser*, Bürgerliches Recht II[13] (2007) 6.

Problematisch ist in diesem Zusammenhang auch die Voraussetzung, dass die Verurteilung zu einer Leistung gemäß § 406 ZPO nur zulässig ist, wenn die Fälligkeit zur Zeit der Urteilsschöpfung bereits eingetreten ist. Man denke etwa an die bei bestimmten Auskunftsbegehren bestehende Schutzpflicht, das von dritter Seite an den Access-Provider herangetragene Auskunftsbegehren zu überprüfen, bzw durch Ergreifung von Rechtsschutzmaßnahmen zu bekämpfen. Möchte man eine drauf gerichtete Leistungsklage einbringen, steht man alsbald vor dem Problem der noch nicht eingetretenen Fälligkeit. Die Klage müsste schon zu einem Zeitpunkt eingebracht werden, zu welchem es noch gar kein konkretes Auskunftsbegehren gibt und die Überprüfungspflicht somit noch nicht fällig ist. Zu erwägen wäre dann noch eine Feststellungsklage mit dem Begehren, dass der Access-Provider seinem Vertragspartner die sorgfältige Überprüfung von Auskunftsbegehren schuldet. Aber auch für eine Feststellungsklage muss das rechtliche Interesse iSd § 406 ZPO für den Zeitpunkt des Verhandlungsschlusses gegeben sein[139]. Ein rechtliches Interesse ist nach der Rechtsprechung des OGH jedoch nur dann gegeben, wenn einaktueller Anlass zur präventiven Klärung eines strittigen Rechtsverhältnisses besteht[140]. Die Klage bedarf eines konkreten Anlasses, der zur Hintanhaltung einer tatsächlichen und ernstlichen Gefährdung des Klägers eine alsbaldige gerichtliche Entscheidung erfordert[141]. Erforderlich ist eine ernsthafte Unsicherheit[142]. Ob eine Klage in einem Fall, in welchem dem Kläger keinerlei konkrete an seinen Access-Provider gerichtete Auskunftsbegehren bekannt sind, diese Kriterien erfüllt, erscheint zweifelhaft. In solchen Fällen wird sich der aus den Schutzpflichten ergebende Schutz daher auf die Geltendmachung von Schadenersatzansprüchen beschränken.

3.2.5. Die Ersatzfähigkeit von Vermögenseinbußen, die durch Schutzpflichtverletzungen verursacht wurde

Die schuldhafte und rechtswidrige Verletzung der Privatsphäre (vgl dazu Kapitel 5.4.1) führt zu einer Pflicht des Ersatzes der dadurch entstandenen Vermögensschäden. Das gilt auch für die Verletzung von vertraglichen Schutzpflichten. In diesem Kapitel soll die Frage untersucht werden, inwieweit sämtliche Einbußen, die als Konsequenz der Verletzung einer vertraglichen Schutzpflicht auftreten, auf den Access-Provider überwälzt werden können. Es soll geklärt werden, inwieweit der Kunde des

---

[139] OGH 23.5.1977, 6 Ob 621/77, MietSlg 29.614 uva.

[140] OGH 7.4.2000, 7 Ob 68/00a, wobl 2001/110.

[141] OGH 27.4.1989, 7 Ob 12/89, ZVR 1990/93.

[142] OGH 22.02.2001, 6 Ob 335/00h.

Access-Providers auf Letzteren Verluste überwälzen kann, die er durch sein unrechtmäßiges Handeln mit verursachte.

> Beispiel: Ein Urheber entdeckt, dass auf einer bestimmten Website ein Verhalten gesetzt wird, das seine urheberrechtlich geschützten Rechtspositionen verletzt. Er kennt die IP-Adresse jener Netzwerkschnittstelle, von der aus dieses verletzende Verhalten gesetzt wurde. Er wendet sich an den Access-Provider und verlangt gestützt auf § 87b Abs 3 UrhG Auskunft über den Namen und die Anschrift jenes Nutzers, dem diese IP-Adresse zum Zeitpunkt der Rechtsverletzung vom Access-Provider zugeordnet wurde. Da der Access-Provider die zur Erfüllung dieses Auskunftsbegehrens erforderlichen Daten eigentlich gar nicht mehr gespeichert haben dürfte, trifft ihn die vertragliche Pflicht, die Auskunft zu verweigern (vgl Kapitel 6.5.7). Der Access-Provider verletzt diese Pflicht schuldhaft und liefert somit seinen Kunden der Rechtsverfolgung durch den Verletzten aus. So gelingt es letzterem, die Rechtsverletzung durch den Kunden des Access-Providers in einem zivilgerichtlichen Verfahren zu beweisen und erfolgreich seine Ansprüche auf angemessenes Entgelt bzw Schadenersatz (§§ 86ff UrhG) geltend zu machen. Er erhält einen Exekutionstitel gegen den Kunden des Access-Providers über den Betrag X. Kann der Kunde des Access-Providers nun von letzterem den Betrag X ersetzt verlangen?

Der Gedanke einer derartigen Ersatzpflicht wirkt auf den ersten Blick befremdlich, steht doch der Kunde dem Schaden gefühlsmäßig näher, als dessen Access-Provider. Der Kunde war es schließlich, der in die Rechte des Urhebers eingriff. Prinzipiell hat jeder die an seinen Gütern entstehenden Schäden selbst zu tragen (§ 1311 ABGB), wenn nicht ausnahmsweise Gründe gegeben sind, welche die Verlagerung erlauben. Ob und welche dieser Zurechnungsvoraussetzungen gegeben sind, soll im Folgenden untersucht werden.

Grundlegende Voraussetzung für einen Ersatzanspruch wäre zunächst, die eingetretene Vermögensminderung als Schaden iSd § 1293 ABGB aufzufassen. Nach § 1293 ABGB ist der Schaden jener Nachteil, welcher jemanden an Vermögen, Rechten oder der Person zugefügt wird. Ein Nachteil am Vermögen ist jede Vermögensveränderung nach unten[143]. Die in Geld messbare Vermögenseinbuße, die der Kunde infolge der Bekanntgabe seiner Identität hat, ist ein Nachteil an seinem Vermögen. Der rechnerische Vergleich der durch das schädigende Ereignis eingetretenen Vermögenslage mit jener, die sich ohne die Bekanntgabe ergeben hätte[144], führt zum Ergebnis einer Verminderung der Aktiven im Vermögen des Kunden des Access-Providers. Fraglich ist, welche Bedeutung dem Umstand beigemessen werden muss, dass der Nachteil sich aus einer rechtlichen Verpflichtung ergibt. Der Nachteil entsteht dem Kunden des Access-Providers etwa in Form einer Geldstrafe (§ 91 Abs 1 UrhG) oder

---

[143] OGH, 11.3.1993, 2 Ob 598/92, EFSlg 72.159 = SZ 66/31 = JBl 1994,46 = NZ 1993, 280 = ÖJZ 1993, 656.

[144] *Koziol*, Haftpflichtrecht I³ (1997) 325.

seiner Pflicht zur Leistung eines angemessenen Entgelts (§ 86 UrhG). Ein Schaden kann jedoch bereits mit der Entstehung von Forderungen gegen den Beschädigten entstehen[145]. Dass der Nachteil in einer von durch die Rechtsordnung vorgegebenen Verbindlichkeit besteht, kann dessen Qualifikation als Schaden nicht verhindern. Auch die gesamten Unterhaltsansprüche, die aus der Geburt eines behinderten Kindes erwachsen, wurden vom OGH bereits als ersatzfähiger Schaden anerkannt[146]. Das ABGB geht von einem denkbar weiten Schadensbegriff aus[147]. Nach den zitierten in Lehre und Rechtsprechung zum Schadensbegriff verwendeten Formeln wäre die vom Kunden zu tragende Geldstrafe ebenso ein Schaden, wie der von ihm zivilrechtlich zu leistende Schadenersatz bzw allfällige Benutzungsentgelte. Die Ursache des Schadens ist für die Frage, ob ein Schaden vorliegt, ohne Belang. Von der Frage der Existenz des Schadens ist die Frage der Ersatzpflicht streng zu trennen[148]. Somit stellen Vermögensminderungen, die nicht eingetreten wären, wenn der Access-Provider seinen Schutzpflichten hinreichend wahrgenommen hätte, Schäden iSd § 1293 ABGB dar.

Das für eine Haftung des Access-Providers ebenso wichtige Kriterium der Kausalität der Vertragsverletzung für die eingetretene Vermögensminderung bereitet in den hier interessierenden Fällen keine besonderen Schwierigkeiten. Nach der Äquivalenztheorie ist ein Ereignis für den Schadenseintritt kausal, wenn es die conditio sine qua non darstellt, wenn es also nicht weggedacht werden kann, ohne dass auch der Schaden entfiele[149]. Denkt man die pflichtwidrige Auskunft des Access-Providers weg, wird dadurch die straf- bzw zivilrechtliche Rechtsverfolgung unmöglich und die Vermögensminderung entfällt daher.

Da die hier erörterten Fälle die Verletzung von Schutzpflichten durch den Access-Provider voraussetzen, scheint zunächst auch die Rechtswidrigkeit[150] gegeben zu sein. Allerdings muss hier untersucht werden, ob die Verhinderung des geltend

---

145 OGH 24.11.1964, 8 Ob 266/64, SZ 37/168.

146 OGH 11.12.2007, 5 Ob 148/07m, Zak 2008, 95 = RdM 2008, 47 = EF-Z 2008, 108 = ÖJZ 2008, 436 = *Grüblinger*, Zak 2008, 143 = *Hinghofer-Szalkay/Hirsch*, iFamZ 2008, 120 = iFamZ 2008, 127 = ÖJZ-LS 2008/27 = *Pletzer*, JBl 2008, 490 = JBl 2008, 521 = ecolex 2008, 322 = RdM 2008, 181 = *Leitner*, ecolex 2008, 417 = *Koziol/Steininger*, RZ 2008, 138 = RZ 2008, 161 = EFSlg 117.259 = ZVR 2008, 128.

147 *Harrer* in *Schwimann,* ABGB VI^3 (2006) § 1293 Rz 1.

148 *Reischauer* in *Rummel,* ABGB II^3 (2007) § 1293 Rz 1.

149 *Bydlinski F.,* Probleme der Schadensverursachung (1964) 7ff; OGH 22.5.1978, 1 Ob 32/77, JBl 1979, 148.

150 Der Begriff Rechtswidrigkeit wird hier wie bei *Koziol,* Haftpflichtrecht I^3 (1997) 147, verwendet: Die bloße Nichteinhaltung einer Verhaltenspflicht wird als tatbestandsmäßig bezeichnet, als rechtswidrig wird dieses Verhalten erst dann bezeichnet, wenn die Verletzung der Verhaltenspflicht unter Außerachtlassung der objektiven Sorgfaltsanforderungen erfolgte. Die subjektive Sorgfaltswidrigkeit hingegen wird erst auf Verschuldensebene geprüft.

gemachten Schadens vom Normzweck der übertretenen Sorgfaltspflichten umfasst ist. Das Verhalten des Access-Providers wird ihn nur dann haftbar machen, wenn es der Sinn und Zweck der verletzten Schutzpflicht war, seinen Kunden vor den Strafen bzw erwähnten Forderungen Dritter zu bewahren. Die Grundsätze der Haftungsbegrenzung durch Beachtung des Rechtswidrigkeitszusammenhangs gelten auch für die Vertragshaftung[151]. Bei Vertragsverletzungen ergibt sich nach der Rechtsprechung des OGH der Rechtswidrigkeitszusammenhang aus den Interessen[152], die der Vertrag schützen sollte[153]. Zuerst ist auf das von den Parteien direkt Bezweckte abzustellen[154]. Bei den noch weiter unten im Rahmen ergänzender Vertragsauslegung gewonnenen Schutzpflichten fehlt es naturgemäß an konkret vereinbarten Normen, aus denen ein Zweck ableitbar wäre. Aber auch die den hypothetischen Parteilwillen ermittelnde ergänzende Vertragsauslegung orientiert sich an grundsätzlichen Zielsetzungen der Partei. Insofern lässt sich jedenfalls auch den qua Vertragsergänzung ermittelten Schutzpflichten ein bestimmter Zweck entnehmen. Die Norm muss nicht nur den Schutz des beeinträchtigten Rechtsguts bezwecken, sondern auch den konkreten Schaden verhindern wollen[155].

Dies ist in den hier interessierenden Fällen wohl zu verneinen. Soweit es um vom Kunden des Access-Providers zu bezahlende Geldstrafen geht, hätte die Abwälzbarkeit des Schadens die Sanktionslosigkeit der verletzten Strafnorm zur Folge. Der Rechtswidrigkeitszusammenhang und die Ersatzfähigkeit solcher Schäden sind daher auszuschließen[156]. Die noch weiter unten zu konstruierenden Schutzpflichten haben einzig den Zweck, die Privatsphäre des Kunden des Access-Providers zu schützen. Sie bezwecken jedoch keinesfalls, ihn vor den Folgen seines rechtswidrigen Handelns zu bewahren. In der (deutschen) Judikatur wird eine Ersatzpflicht ex contractu für die vom Vertragspartner zu tragenden Geldstrafen nur dann angenommen, wenn eine besondere Verpflichtung bestand, den Vertragspartner von der Begehung der Straftat abzuhalten

---

[151] OGH 15.1.1992, 2 Ob 575/91, SZ 65/8 = ecolex 1992, 319; BGH 30.1.1990, XI ZR 63/89, NJW 1990, 2057.

[152] Vgl auch *Rabel,* Das Recht des Warenkaufs (1936) 496; *Schack,* Der Schutzzweck als Mittel der Haftungsbegrenzung im Vertragsrecht, JZ 1986, 305 (309ff); *Wilburg,* Elemente des Schadenersatzrechts (1941) 244.

[153] OGH 12. 1. 1983, 3 Ob 651/82, JBl 1984, 41.

[154] OGH 9.7.1992 7 Ob 583/92, EvBl 1993/15 = JBl 1993, 394.

[155] *Reischauer* in *Rummel*, ABGB II^3 (2007) § 1295 Rz 8.

[156] Ebenso zum Ersatz von Schäden, die infolge einer Verletzung des Bankgeheimnisses (zB Steuernachzahlungen) entstehen *Koziol,* Österreichisches Haftpflichtrecht I^3 (1997) 270; differenzierend BGH 31.1.1957, II ZR 41/56, BGHZ 23, 222 (der BGH stellt darauf ab, ob eine vertragliche Pflicht verletzt wurde, die den Inhalt hat, den Täter vor der Begehung einer Straftat zu schützen).

oder ihn in rechtmäßiger Weise vor Strafen zu bewahren[157]. Nur in diesen Fällen erfordert es der Zweck der verletzten Pflicht, die durch die Verletzung entstandenen Schäden zu ersetzen. Die hier in Frage stehenden Straftaten (etwa Urheberrechtsverletzungen) können vom Access-Provider mangels Vorhersehbarkeit gar nicht verhindert werden, er kann seinem Kunden auch nicht dabei behilflich sein, die Straftat zu vermeiden. Er könnte höchstens deren Verfolgung verhindern. Die Bewahrung vor Strafen liegt jedoch nicht in jenem Bereich von Gefahren, vor denen die Schutzpflicht bewahren möchte. Vom Schutzzweck ebenso wenig erfasst sind die mit der Strafverfolgung im Zusammenhang stehenden Kosten (etwa eines Verteidigers). Dies gilt mE auch in jenen Fällen, in denen sich letztlich herausstellt, dass das verfolgte Verhalten nicht strafbar ist.

Ebenso wenig wie Strafen wird der Kunde Vermögensminderungen infolge erfolgreich gegen ihn geltend gemachter zivilrechtlicher Ansprüche auf den Access-Provider abwälzen können. Auch hier scheitert der Ersatzanspruch mE am fehlenden Rechtswidrigkeitszusammenhang. Die Schutzpflichten des Access-Providers dienen nicht dem Zweck, dass der Kunde des Access-Providers unbehelligt und rechtswidrig in die Rechte Dritter eingreifen kann.

Da die Ersatzfähigkeit der gezeigten Schäden bereits an der mangelnden Rechtswidrigkeit scheitert, kann die Frage des Mitverschuldens des Kunden (§ 1304 ABGB) hier dahinstehen.

3.3. Zwischenergebnis

Der Begriff der positiven Forderungsverletzungen wurde 1902 vom deutschen Juristen *Herrmann Staub* erfunden, da er der Ansicht war, das deutsche BGB enthalte eine Lücke. Nach seiner Auffassung hielt das Gesetz nur für jene Fälle eine Regelung bereit, in denen jemand wie beim Verzug oder der Unmöglichkeit etwas unterlässt, was er eigentlich hätte tun sollen. Ungeregelt hingegen seien jene Fälle, in welchen jemand durch positives Handeln gegen eine Unterlassungspflicht verstößt, bzw in denen zwar jemand eine Leistung bewirkt, aber dies so mangelhaft, dass weitere Schäden entstehen. Diese Lücke sei mithilfe des von ihm erfundenen Rechtsinstituts zu schließen. In der Folge wurde seine Schrift zahlreich kritisiert, was jedoch nichts daran änderte, dass er und seine Nachfolger sie in zahlreichen Neuauflagen letztlich erfolgreich gegen alle Kritik verteidigten. Insbesondere das Argument, dass auch die Verletzung

---

[157] OLG Köln, 8.7.1992, 11 U 43/92, BB 1992, 2174; BGH 31.1.1957, II ZR 41/56, BGHZ 23, 222; RG 10.6.194, III ZR 14/42, RGZ 169, 267.

einer Schutzpflicht stets nur entweder endgültiger (Unmöglichkeit) oder vorübergehender (Verzug) Natur sein könne und sich daher immer unter die Verzugs- bzw Unmöglichkeitsvorschriften subsumieren lasse, wurde nicht akzeptiert. So kam es, dass die positiven Vertragsverletzungen auch in der Rechtsprechung dauerhaft als eine neue Kategorie von Leistungsstörungen extra legem anerkannt wurden.

Der Streit um die positiven Forderungsverletzungen begann in Deutschland noch bevor in Österreich dass ABGB drei Mal teilnovelliert wurde. In Österreich gab es jedoch seit 1811 § 1295 ABGB, der bestimmt, dass Schadenersatz zu leisten ist, wenn der Schaden „durch Übertretung einer Vertragspflicht" verursacht wurde. § 919 ABGB enthielt vor der dritten Teilnovelle so wie heute § 918 ABGB eine Regelung für den Fall, dass ein Teil „nicht auf die bedungene Weise" leistet. Daher könnte man annehmen, dass es mangels gesetzlicher Lücke für die heftige in Deutschland geführte Diskussion in Österreich keinen Boden gegeben haben kann. Dennoch wurde das Institut der positiven Vertragsverletzungen auch in Österreich eingeführt und bildet heute einen fixen Bestandteil der Rechtsprechung. Dies verwundert, da sogar die Gesetzesmaterialien zur dritten Teilnovelle des ABGB eindeutig belegen, dass die Herrenhauskommission damals davon ausging, dass jene Fälle, die in Deutschland unter dem Begriff „positive Vertragsverletzungen" diskutiert wurden, im ABGB geregelt seien.

Zu einer rechtspolitisch erwünschten Schadenersatzpflicht kommt man in diesen Fällen stets über § 1295 ABGB, der bestimmt, dass im Falle der Übertretung einer Vertragspflicht Schadenersatz zu leisten ist. Besteht also eine bestimmte Vertragspflicht und wird diese übertreten, bedarf es zumindest in Österreich keines Rückgriffs auf das Institut der positiven Forderungsverletzungen.

In Österreich wurden die positiven Vertragsverletzungen jedoch als eigene Kategorie den dem ABGB bekannten Leistungsstörungen beiseite gestellt. Im Allgemeinen unterscheidet man zwei Gruppen positiver Forderungsverletzungen: Zum einen gibt es reine Schutzpflichtverletzungen, die in keinerlei Zusammenhang mit der Erfüllung der Hauptleistungspflicht stehen (Begleitschäden) und zum anderen gibt es jene Fälle, in denen die Hauptleistungspflichten so mangelhaft erfüllt werden, dass dem Gläubiger weitere Schäden entstehen (Mangelfolgeschäden). Im Laufe der weiteren Arbeit wird ausschließlich nur die erste Kategorie eine Rolle spielen. Da man die positiven Forderungsverletzungen als eigenständiges Institut betrachtete, war es auch möglich, völlig neue Regeln zu erfinden. So ist es gegen den Wortlaut des § 918 ABGB heute ständige Rechtsprechung, dass ein Rücktrittsrecht bei positiven Vertragsverletzungen nur ganz ausnahmsweise zustehen kann. Richtigerweise muss dem vertragstreuen Teil jedoch grundsätzlich immer ein Rücktrittsrecht zustehen, wenn der andere Teil eine Schutzpflichtverletzung begeht. Dieses darf nur ausnahmsweise dann nicht zugestanden

werden, wenn die Ausübung wegen der minderen Schwere der Verletzung der Vertragspflicht als missbräuchlich zu beurteilen wäre.

Da die Schutzpflichten genauso geschuldet werden, wie auch die Hauptleistungspflichten, können sie mE auch gesondert eingeklagt werden, vorausgesetzt, sie sind hinreichend bestimmt und fällig. Dies hängt von den Umständen des Einzelfalls ab.

Grundsätzlich sind sämtliche Vermögensschäden zu ersetzen, die dem Gläubiger einer Schutzpflicht durch die Verletzung dieser Pflicht erwachsen. Die Ersatzpflicht kann jedoch aufgrund des mangelnden Rechtswidrigkeitszusammenhangs zwischen der übertretenen Schutzpflicht und dem Schaden ausscheiden. Dies ist regelmäßig dann der Fall, wenn der Gläubiger der Schutzpflicht die Vermögensminderung durch sein eigenes rechtswidriges Verhalten mit verursacht hat. Wenn ein Access-Provider etwa entgegen seinen vertraglichen Verpflichtungen Daten an Dritte weiter gibt, ermöglicht er dadurch die zivil- und/oder strafrechtliche Verfolgung seines Kunden, die zur Verhängung von Geldstrafen bzw zur Verurteilung zur Leistung von Schadenersatzansprüchen führen kann. Diese Vermögenseinbußen kann der Kunde nicht auf seinen Access-Provider überwälzen.

4. Die Beziehung zwischen Access-Provider und Kunden

Im Folgenden soll zunächst ganz allgemein die Struktur des Vertragsverhältnisses zwischen einem Access-Provider und seinem Kunden durchleuchtet werden und die Begriffe „Access-Provider" und „Kunde" beleuchtet werden.

4.1. Der Begriff des „Access-Providers"

Dieser dem täglichen Sprachgebrauch entnommene und auch von Lehre[158] und Rechtsprechung[159] ständig verwendete Begriff kommt als solcher in keinem einzigen österreichischen Bundesgesetz vor.

Das einzige österreichische Gesetz, dass eine Definition enthält, die – ohne das dieser Begriff vom Gesetz ausdrücklich verwendet wird – gemeinhin als Definition des Begriffes Access-Provider verstanden wird, ist das ECG[160]. Auch die EB zur RV zum ECG verwenden diesen Begriff[161]. Access-Provider iSd ECG sind Diensteanbieter, die von einem Nutzer eingegebene Informationen in einem Kommunikationsnetz übermitteln oder den Zugang zu einem Kommunikationsnetz vermitteln, ohne diese Übermittlung zu veranlassen, den Empfänger auszuwählen und ohne die Informationen auszuwählen oder zu verändern (§ 13 ECG).

Diese Definition grenzt den Begriff des Access-Providers für die Regelungszwecke des ECG ab, wo es unter anderem um die Haftung der Provider für fremde rechtswidrige Inhalte geht. Für die Zwecke dieser Arbeit empfiehlt es sich jedoch, über den Regelungsbereich des ECG hinaus noch nach anderen einschlägigen Definitionen zu suchen. Dies legen schon die Bestimmungen in der StPO oder im SPG nahe, die Auskunftspflichten statuieren und dabei nie auf § 13 ECG Bezug nehmen. Nichts desto trotz gelten die durch die im SPG oder in der StPO verpflichteten Personen gemeinhin als Access-Provider. Ein wesentliches Anliegen des ECG ist es, die Verantwortlichkeit für fremde vermittelte, gespeicherte bzw durchgeleitete Inhalte im

---

158 *Brenn,* ECG (2002), 263ff; *Burgstaller/Minichmayr,* E-Commerce-Gesetz (2002) 103ff; *Bresich/Pesta,* Haftung für offenes WLAN? RdW 2007, 647 (648); *Laga/Sehrschön/Ciresa,* E-Commerce-Gesetz[2] (2007) 65, *Zankl*, E-Commerce Gesetz in Sicht, AnwBl 2001, 459 (460), *ders*, E-Commerce-Gesetz (2002); *ders* Online-Privilegien für Unterlassungsansprüche? ecolex 2004, 361 (361), *ders*, Proxy, Cache und Unterlassung, ecolex 2004, 941 (941) uvm.

159 OGH 14.7.09, 4 Ob 41/09x, MR 2009, 251 oder OGH 26.07.2005 11 Os 57/05z uva.

160 BGBl I 152/2001.

161 RV 817 BlgNR XXI. GP, 13.

elektronischen Verkehr zu regeln. Die diesbezüglichen Bestimmungen im 5. Abschnitt des ECG unterscheiden zwischen drei Arten von Providern: Provider die Zugang zum Netz vermitteln bzw bloß durchleiten (Access-Provider), Provider, die automatische zeitlich begrenzte Zwischenspeicherungen vornehmen (Caching) sowie Provider die fremde Inhalte speichern (Host-Provider). Je nach Art des Providers sieht das ECG unterschiedlich weit reichende Haftungsprivilegien vor (§§ 13ff ECG).

Die Definition von Access-Providern im ECG hat also primär den Zweck, in Anlehnung an die Definitionen in Rl 2000/31/EG[162] (fortan: E-Commerce-Richtlinie; Art 12ff) diesen Begriff von den Begriffen des Host-Providings bzw Cachings abzugrenzen. Sie entsprechen dabei Wesentlichen gleichartigen Bestimmungen wie § 5 des deutschen Teledienstegesetzes oder dem Titel II des US-Digital Millenium Copyright Act[163]. Die Voraussetzungen, um als Access-Provider nach § 13 ECG haftungspriviligiert zu sein, sind leichter zu erfüllen, als jene um als Host-Provider haftungsfrei zu sein. Der Richtliniengeber wollte Diensteanbieter, die selbst nur rein technische, passive bzw automatisierte Zugangs- und Übermittlungsdienstleistungen betreiben, ohne mit den betroffenen Informationen in einer weiter reichenden Verbindung zu stehen, weitestgehend von ihrer Verantwortlichkeit befreien (vgl die Erwägungsgründe 42ff). Die Regelungen des ECG bzw der E-Commerce-Richtlinie haben also nicht den Zweck das Vertragsverhältnis zwischen Access-Provider und seinem Kunden zu charakterisieren, sondern sollen jene Fälle abgrenzen, in denen die Verbindung zwischen dem Provider und den verarbeiteten Informationen besonders gering ist und er daher nicht bzw nur begrenzt zur Verantwortung gezogen werden soll. Die Haftungsprivilegien des ECG gelten außerdem nicht für vertragliche Ansprüche[164], die den Hauptgegenstand dieser Abhandlung bilden.

Für die Zwecke dieser Arbeit sind die im TKG 2003[165] enthaltenen Begriffsbestimmungen (siehe dazu sogleich) besonders einschlägig. Besonders zu beachten sind hier die Bestimmungen des zwölften Abschnitts des TKG 2003 (§§ 92-107), welche den Zweck haben, die datenschutzrechtliche Beziehung von Anbietern und Benutzern zu regeln. Dieser Regelungszweck legt nahe, die dortigen Definitionen auch zur Abgrenzung der im Rahmen dieser Arbeit interessierenden Personengruppen heranzuziehen.

---

[162] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt, ABl L 2000/178, 1.

[163] RV 817 BlgNR XXI. GP, 13.

[164] *Zankl,* Bürgerliches Recht[5] (2010) Rz 269.

[165] BGBl I 70/2003.

§ 92 Abs 3 Z 1 TKG 2003 definiert als „Anbieter" die Betreiber öffentlicher Kommunikationsdienste. Die Terminologie ist nach den Materialien an den umgesetzten Richtlinien orientiert[166], insbesondere der Rl 2002/21/EG (fortan Rahmenrichtlinie)[167]. § 3 Z 3 TKG 2003 definiert als „Betreiben eines Kommunikationsdienstes" das „ Ausüben der rechtlichen Kontrolle über die Gesamtheit der Funktionen, die zur Erbringung des jeweiligen Kommunikationsdienstes notwendig sind." Ein „Kommunikationsdienst" ist gemäß Z 9 leg cit „*eine gewerbliche Dienstleistung, die ganz oder überwiegend in der Übertragung von Signalen über Kommunikationsnetze besteht, einschließlich Telekommunikations- und Übertragungsdienste in Rundfunknetzen, jedoch ausgenommen Dienste, die Inhalte über Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben. Ausgenommen davon sind Dienste der Informationsgesellschaft iSd von § 1 Abs 1 Z 2 des Notifikationsgesetzes*[168]*, BGBl. I Nr. 183/1999, die nicht ganz oder überwiegend in der Übertragung von Signalen über Kommunikationsnetze bestehen.*" Das Tatbestandsmerkmal, dass die Dienstleistung „ganz oder überwiegend in der Übertragung von Signalen über Kommunikationsnetze" bestehen muss, wird hier in einem Absatz gleich zwei Mal normiert. Das Gesetz übernimmt die redundante und dadurch etwas unverständliche Formulierung der Richtlinie (Art 2 lit c Rl 2002/21/EG). Gemeint ist, dass es Dienste der Informationsgesellschaft gibt, die gleichzeitig auch in den Anwendungsbereich der Richtlinie 2002/21/EG fallen. Zu den Diensten der Informationsgesellschaft zählen schließlich auch Dienste, „*die Informationen über ein elektronisches Netz übermitteln, die den Zugang zu einem solchen vermitteln oder die Informationen eines Nutzers speichern*" (§ 3 Z 1 ECG bzw § 1 Abs 1 Z 2 Notifikationsgesetz). Im zweiten Satz in § 3 Z 9 TKG 2003 wird überflüssigerweise wiederholt, dass solche Dienste nur dann elektronische Kommunikationsdienste darstellen, wenn sie ganz oder überwiegend in der Übertragung von Signalen über Kommunikationsnetze bestehen[169].

Es geht somit um die gewerbliche Übermittlung von Sprach- oder Datenpaketen über elektronische Kommunikationsnetze. Ein typischer elektronischer Kommunikationsdienst, ist die Zur-Verfügung-Stellung von Internet-Connectivity, eine

---

166 RV 128 BlgNR XXI. GP, 4.

167 Richtlinie 2002/21/EG des Europäischen Parlamentes und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie), ABl L 2002/108, 33.

168 Diese Definition entspricht wortgleich jener in § § Z 1 ECG: *„[...] ein in der Regel gegen Entgelt elektronisch im Fernabsatz auf individuellen Abruf des Empfängers bereitgestellter Dienst, insbesondere der Onlinevertrieb von Waren und Dienstleistungen [...], sowie Dienste, die Informationen über ein elektronisches Netz übermitteln, die den Zugang zu einem solchen vermitteln oder die Informationen eines Nutzers speichern*".

169 Vgl auch Erwägungsgrund 10 der Rahmen-Rl.

zentrale Funktionalität des Internets. Es geht also ausschließlich um Transportdienstleistungen[170], nicht erfasst sind daher Content-Provider. Erfasst sind auch die reinen Signalübertragungsdienstleistungen im Bereich des Rundfunks, bei denen keine Kontrolle über den Inhalt der übermittelten Information ausgeübt wird. Der Begriff des Telekommunikationsdienstes umfasst hingegen ausschließlich Kommunikationsdienste ohne Rundfunk (§ 3 Z 21 TKG). Die Bereitstellung von Internet gestützten Inhalten kann einen Dienst der Informationsgesellschaft iSd ECG bzw des Notifikationsgesetzes darstellen, ist jedoch kein elektronischer Kommunikationsdienst (vgl Erwägungsgrund 10 der Rahmen-Rl).

Die Übertragung von Signalen kann nur über ein Kommunikationsnetz erfolgen. Das bedeutet, dass der Betreiber von Kommunikationsdiensten entweder mit dem Betreiber elektronischer Kommunikationsnetze in einer Person zusammenfällt, oder das ersterer von letzterem die Kommunikationsdienste auf Wholesale-Ebene bezieht und an seine eigenen Endkunden auf der Retail-Ebene weiter verkauft.

Der Wiederverkauf ist nach den Materialien als Hauptdienstleistung vom Begriff des Kommunikationsdienstes mit umfasst. Sofern der Wiederverkauf allerdings eine untergeordnete Nebendienstleistung darstellt (wie etwa in einem Hotel), ist dieser nicht als Kommunikationsdienst zu werten[171]. Im Rahmen dieser Arbeit sind freilich nur Telekommunikationsdienste, dh Kommunikationsdienste mit Ausnahme von Rundfunk (§ 3 Z 21 leg cit) relevant. Erfasst sind sowohl Kommunikationsdienste an festen Standorten sowie Kommunikationsdienste für mobile Teilnehmer[172].

Die wichtigsten Auskunftsbestimmungen in der österreichischen Rechtsordnung, die sich an jene richten, die gemeinhin als Access-Provider gelten, richten sich an Betreiber von Kommunikationsdiensten iSd § 92 Abs 3 Z 1 TKG 2003. Dies gilt etwa für § 53 Abs 3a und 3b SPG[173], für § 138 Abs 2 StPO[174] oder § 22 Abs 2a MBG[175]. Die beiden erstgenannten Bestimmungen richten sich auch an Diensteanbieter iSd ECG. Soweit diese Diensteanbieter jedoch keine Internet-Connectivity anbieten und damit nicht gleichzeitig auch Betreiber von elektronischen Kommunikationsdiensten sind,

---

[170] *Schuster* in *Büchner/Ehmer/Geppert/Kerkhoff/Piepenbrock/Schütz/Schuster,* Beck'scher TKG Kommentar (2000) Rz 4 zu § 4.

[171] RV 128 BlgNR XXI. GP, 4.

[172] *Zanger/Schöll,* Telekommunikationsgesetz[2] (2004) Rz 95 zu § 3.

[173] BGBl I 566/1991 idF BGBl I 114/2007.

[174] BGBl 631/1975 idF BGBl 19/2004.

[175] BGBl I 86/2000 idF BGBl I 85/2009.

erbringen sie keine Dienstleistungen, die man gemeinhin als „Access-Providing", dh als Zugangsverschaffung zu einem Kommunikationsnetz, versteht.

Bei den in dieser Arbeit abgehandelten Pflichten handelt es sich somit um Pflichten der Anbieter iSd § 92 Abs 3 Z 1 TKG 2003. Da diese Definition aber letztlich aufgrund des impliziten Verweises auf § 3 Z 3 und 9 TKG 2003 auch jene umfasst, die Signale über elektronische Kommunikationsnetze im Bereich des Rundfunks übertragen, soll hier noch eine Einschränkung iSd § 3 Z 21 leg cit vorgenommen werden: Unter „Access-Providern" sind im Folgenden ausschließlich Betreiber von Kommunikationsdiensten mit Ausnahme von Rundfunk zu verstehen.

4.2. Der Begriff des „Kunden" des Access-Providers

Der bisher nicht näher definierte Begriff „Kunde" des Access-Providers ist ebenso kein dem Gesetz entnommener Begriff. Auch hier empfiehlt es sich zur Begriffsbestimmung einen Blick ins TKG 2003 zu werfen. Das TKG 2003 kennt den Begriff des „Benutzers" (§ 92 Abs 3 Z 2), den es als eine natürliche Person, die einen öffentlichen Kommunikationsdienst für private oder geschäftliche Zwecke nutzt, ohne diesen Dienst zwangsläufig abonniert zu haben, definiert. Davon unterscheidet es „Nutzer", die auch juristische Personen sein können, die einen öffentlich zugänglichen Kommunikationsdienst in Anspruch nehmen oder beantragen (§ 3 Z 14). Unter „Teilnehmern" versteht es schließlich natürliche oder juristische Personen, die mit einem Betreiber einen Vertrag über die Bereitstellung dieser Dienste geschlossen haben (§ 3 Z 19). „Nutzer" und „Benutzer" iSd TKG nehmen also faktisch die Dienste des Providers in Anspruch, während eine Teilnehmereigenschaft nur bei einem aufrechten Vertragsverhältnis vorliegt. Dabei kommt es freilich meist zu Überschneidungen. Nimmt der Vertragspartner des Access-Providers dessen Dienste in Anspruch, ist er zugleich Teilnehmer als auch Benutzer. Die datenschutzrechtlichen Bestimmungen im 12. Abschnitt des TKG 2003 stellen nicht auf das Vorliegen eines Vertragsverhältnisses ab, sondern erstrecken sich auch auf Benutzer. Die §§ 92 ff TKG 2003 dienen den Vorgaben der Rl 2002/58/EG[176] (fortan: EK-Datenschutzrichtlinie) entsprechend als Ergänzung und Präzisierung (siehe dazu auch unten Kapitel 4.5.1) zum nicht sektorspezifischen Datenschutzrecht im DSG 2000. Das DSG 2000 schützt ebenfalls, ohne auf das Vorliegen

[176] Richtlinie 2002/58/EG des europäischen Parlamentes 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 2002/201, 37.

eines Vertrages abzustellen, sämtliche Betroffene, die es in § 4 Z 3 als alle vom Auftraggeber (§ 4 Z 4 leg cit) verschiedene natürliche oder juristische Personen oder Personengemeinschaften, deren Daten verwendet (§ 4 Z 8 leg cit) werden, definiert.

Diese Arbeit setzt sich mit den Rechten des Vertragspartners des Access-Providers – das heißt mit dem Teilnehmer iSd der obigen Definitionen – auseinander. Sofern der Begriff „Kunde" verwendet wird, ist er demnach in diesem Sinne zu verstehen.

4.3. Das Vertragsverhältnis zwischen dem Access-Provider und seinem Kunden

Oben haben wir gesehen, dass Access-Provider Dienstleistungen erbringen, die zur Gänze oder überwiegend in der Übertragung von Signalen über ein Kommunikationsnetz bestehen. Dabei handelt es sich um die Hauptleistungspflicht. Bekanntlicherweise erschöpft sich das Schuldverhältnis jedoch nicht in seinen Hauptpflichten, sondern es treten neben diese auch andere Pflichten vgl dazu schon oben 2.1). Die Gesamtheit dieser Pflichten wird als „Organismus" bezeichnet[177].

Die Hauptpflichten charakterisieren das Schuldverhältnis. Je nachdem wie diese vertraglich gestaltet werden, liegt entweder ein gesetzlich geregeltes Schuldverhältnis oder ein Elemente aus verschiedenen gesetzlichen Vertragstypen beinhaltendes gemischtes Schuldverhältnis oder aber ein überhaupt atypischer Vertrag vor. Diese Arbeit setzt sich in erster Linie nur mit den vertraglichen Schutzpflichten und den Konsequenzen aus ihren Verletzungen auseinander. Daher soll hier bezüglich der zivilrechtlichen Einordnung von Verträgen über die Erbringung elektronischer Kommunikationsdienste nur ein kursorischer Überblick gegeben werden.

Nach Auffassung des OGH[178] weisen die Hauptleistungspflichten zumindest bei Mobilfunkverträgen Charakteristika von Mietverträgen und von freien Dienstverträgen auf[179]. Er schloss sich damit insbesondere auch der Meinung *Zankls*[180] an, nach welchem der Access-Provider die Zur-Verfügung-Stellung der Netzinfrastruktur schulde. Diese Netzinfrastruktur arbeite gewissermaßen „von selbst", was mietvertraglichen Charakteristika entspreche. Der geschuldete „Erfolg" liege sohin in der zur Verfügung gestellten Netzinfrastruktur. Das Vertragsverhältnis sei mit der Vermietung eines Autos

---

[177] *Stoll,* Die Lehre von den Leistungsstörungen (1936) 26.

[178] 21.4.2005, 6 Ob 69/05y.

[179] So auch *Graf von Westphalen/Grote/Pohle,* Der Telefondienstvertrag (2000) 172.

[180] *Zankl*, Qualifikation und Dauer von Mobilfunkverträgen, ecolex 2005, 29ff.

zu vergleichen. Gem § 1096 ABGB schulde der Vermieter, dass dieses Auto anspringe, sohin auch gewissermaßen einen Erfolg, welcher dem Vertragsgegenstand immanent sei und nicht wie beim Werkvertrag erst eigens hergestellt werden müsse. Da die Zur-Verfügung-Stellung entgeltlich erfolge, sei das Vertragsverhältnis als Miete zu qualifizieren[181]. Der OGH konnte aber auch der Auffassung des BGH etwas abgewinnen, wonach die Hauptleistungspflichten des Providers beim Mobilfunkvertrag dienstvertraglicher Natur sind[182]. Nach der Rechtsprechung des BGH verpflichtet sich bei Mobilfunkverträgen der Access-Provider seinen Kunden *„[...] den Zugang zum Mobilfunknetz zu eröffnen und somit unter Aufbau abgehender und Entgegennahme ankommender Telefonverbindungen mit beliebigen dritten Teilnehmern eines Mobilfunknetzes oder Festnetzes Sprache auszutauschen.*" Die dienstvertraglichen Elemente leitete der OGH – nach ausdrücklichem Eingeständnis, dass dies dogmatisch kein besonders überzeugendes Argument sei – aus der Terminologie des TKG 2003 ab, wo ua von „Dienstleistungen" die Rede sei. Daher könne man im Anschluss an die Judikatur des BGH auch von dienstvertraglichen Zügen des Vertragsverhältnisses ausgehen[183]. Allerdings meinte der OGH auch, dass die Gewährleistungsansprüche des Verbrauchers (vgl § 25 Abs 4 Z 4 TKG 2003) gegen die Qualifikation als Dienstvertrag sprechen würden, da beim Dienstvertrag Gewährleistungsansprüche überwiegend abgelehnt wurden. Im Ergebnis sei daher davon auszugehen, dass es sich beim Mobilfunkvertrag um einen Mischvertrag sui generis mit dienstvertraglichen und mietvertraglichen Elementen handle. Der Auffassung, es handle sich beim Mobilfunktvertrag um einen Wertvertrag, wurde somit eine klare Absage erteilt und zwar vor allem mit der Begründung, dass kein Erfolg geschuldet werde. Der OGH meinte, dass selbst wenn man in der Verpflichtung des Netzbetreibers, dem Kunden auf Vertragsdauer den Zugang zum öffentlichen Telekommunikationsnetz und so die Möglichkeit zum Austausch von Sprache und Daten zu eröffnen, einen vom Unternehmer herzustellenden Erfolg und damit ein werkvertragliches Element erblickte, dieses Element deutlich hinter dem mietrechtlichen Vertragselement zurücktrete.

Unverständlich bleibt, weshalb der OGH sich letztlich auch zu der Annahme kam, dass der Mobilfunkvertrag auch Elemente eines – mangels persönlicher Abhängigkeit des Access-Providers von seinem Kunden – freien Dienstvertrages enthält. § 25 Abs 4 TKG 2003 bestimmt in Z 2, dass die AGB von Betreibern von Kommunikationsdiensten in ihren AGB die Qualität ihrer Dienste festzulegen haben und

---

[181] So auch *Hahn,* AGB in TK-Dienstleistungsverträgen, MMR 1999, 251 (255)

[182] BGH 18.4.2002, III ZR 199/01; 22.11.2001, III ZR 5/01.

[183] Dienstvertragliche Züge ebenfalls bejahend etwa: OLG , 31.10.1996, 6 U 206/95, BB 1994, 2643.

in Z 4, dass auch Entschädigungs- und Erstattungsregelungen bei Nichteinhaltung der vertraglich vereinbarten Dienstqualität in die AGB aufzunehmen sind. Daraus ergibt sich eindeutig, dass Betreiber von elektronischen Kommunikationsdiensten hinsichtlich ihrer Leistungen gewisse Gewährleistungspflichten treffen. Das steht jedoch der Einstufung als Dienstvertrag entgegen, da den Dienstnehmer grundsätzlich keine Gewährleistungspflichten gegenüber dem Dienstgeber treffen[184]. Dies auch ausdrücklich anerkennend kam der OGH letztlich jedoch zu obigem Ergebnis.

Die Überlegungen und das Ergebnis des OGH lassen sich größtenteils auch auf andere Verträge über die Erbringung elektronischer Kommunikationsdienste übertragen. Der OGH charakterisierte den Mobilfunkvertrag folgendermaßen: „*Der wesentliche Leistungsinhalt des Betreibers besteht darin, dass er dem Kunden das gesamte Funknetz samt technischen Einrichtungen, das als unverbrauchbare Gesamtsache iSd § 1090 ABGB zu qualifizieren ist, zum Gebrauch zur Verfügung stellt. Dem Verbraucher werden auf Vertragsdauer gegen Entgelt Nutzungsrechte eingeräumt.*" Genau dasselbe passiert auch bei allen anderen Verträgen über die Erbringung von elektronischen Kommunikationsdiensten, unabhängig von der Art der übertragenen Daten und unabhängig davon, ob es um standortgebundene oder mobile Anschlüsse geht. Es wird dem Kunden stets ein Kommunikationsnetz zur Verfügung gestellt, dass dieser für die Übertragung von Daten nutzt. Die Erwägungen des OGH zur rechtlichen Qualifikation des Mobilfunkvertrags lassen sich daher auch auf andere Verträge über die Erbringung von elektronischen Kommunikationsdiensten übertragen.

4.4. Im Zusammenhang mit Kommunikationsdiensten verarbeitete Daten

Im Zusammenhang mit der Erbringung elektronischer Kommunikationsdienste muss der Access-Provider eine Reihe von Daten verarbeiten. Dabei unterscheidet das TKG 2003 zwischen folgenden Datenkategorien, die sich an der EK-Datenschutzrichtlinie orientieren[185]:

---

184 Vgl *Schrammel,* Gewährleistung für schlechte Dienste, in *Fischer-Cermak/Kletecka/Schauer/Zankl*, Festschrift zum 65. Geburtstag von Rudolf Welser (2004) 585 (590) mwN.

185 RV 128 BlgNR XXII.GP, 17.

4.4.1. Stammdaten (§ 92 Abs 3 Z 3 TKG 2003)

Das sind alle personenbezogenen Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind. Das sind a) Familien- und Vorname, b) akademischer Grad, c) Wohnadresse, d) Teilnehmernummer und sonstige Kontaktinformation für die Nachricht, e) Information über die Art des Vertragsverhältnisses, f) Bonität. Die meisten Begriffe dieser nach herrschender Ansicht taxativen[186] Liste sind selbsterklärend, unter Kontaktinformationen sind all jene Daten zu verstehen, die der Absender benötigt, um seine Nachricht an den gewünschten Empfänger zu adressieren (insbesondere auch E-Mail-Adressen). Unter Informationen über das Vertragsverhältnis sind Daten zu verstehen, die das Vertragsverhältnis hinsichtlich Tarifgestaltung Laufzeit uä charakterisieren. Teilnehmernummern können je nach den Umständen sowohl Stamm- als auch Verkehrsdaten sein. Abgespeichert in einer Kundendatei stellen sie ein Stammdatum dar. Soweit sie zum Aufbau einer Verbindung dienen, gelten sie als Verkehrsdaten[187]. Teilnehmernummern haben genau wie statische IP-Adressen also einen doppelfunktionalen Charakter, ihre Einordnung hängt vom Einzelfall ab.

4.4.2. Verkehrsdaten (§ 92 Abs 3 Z 4 TKG 2003)

Das sind Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden. Diesbezüglich ist auf den 15. Erwägungsgrund der EK-Datenschutzrichtlinie zu verweisen, der eine demonstrative Aufzählung von Verkehrsdaten enthält. Hiezu zählen insbesondere Informationen über die verwendeten Leitwege, die Dauer, den Zeitpunkt oder die Datenmenge einer Nachricht, das verwendete Protokoll sowie Zahlungsinformationen wie etwa Angaben zur Zahlungsweise oder über die Sperrung eines Anschlusses. Die Definition entspricht der wortgleichen deutschen authentischen Fassung der EK-Datenschutzrichtlinie und erfasst dem Wortlaut nach Informationen, die zur Weiterleitung einer Nachricht über ein Kommunikationsnetz benötigt werden, nicht. In der englischen Fassung der Richtlinie heißt es *„ [...] traffic data means any data processed for the purpose of the conveyance of a communication <u>on</u> an electronic communications network or for the billing thereof*." Angesichts dieser ebenfalls authentischen Fassung der Richtlinie lässt sich die aus der Formulierung „an ein

---

186 *Damjanovic/Holoubek/Kassai/Lehofer/Urbanitsch,* Handbuch des Telekommunikationsrechts (2006) 247 mwN.

187 *Reindl-Krauskopf/Tipold/Zerbes,* in *Fuchs/Ratz* (Hrsg), Wiener Kommentar zur Strafprozessordnung (2009) § 134 Rz 29.

Kommunikationsnetz" ergebende Beschränkung nur als legistisches Versehen auffassen[188].

Verkehrsdaten unterliegen zwar dem Schutz des Art 8 EMRK (siehe unten Kapitel 5.4), werden jedoch nach zutreffender Ansicht[189] nicht vom Schutz des Fernmeldegeheimnisses (Art 10a StGG[190]) erfasst. Dies ergibt sich vor allem aus der systematischen Erwägung, dass Art 10a StGG in Anlehnung an Art 10 StGG geschaffen wurde, der ebenfalls nur den Inhalt verschlossener Briefe schützen soll. Allerdings scheint auch der Gesetzgeber teilweise davon auszugehen, dass Verkehrsdaten dem Fernmeldegeheimnis unterliegen. So meinte er in den EB zur RV zur StPO-Reform 2004, dass *„auf Grund verfassungsrechtlicher Vorgaben (Art 10 und 10a StGG) auch in Fällen der Auskunft über Standort- oder Vermittlungsdaten [...] eine gerichtliche Bewilligung erforderlich sein soll, weil ein Eingriff in das Fernmeldegeheimnis vorliegt, der nur auf Grund einer gerichtlichen Entscheidung zulässig ist.*"[191] Diese Feststellung kann aber aus mehreren Gründen hinterfragt werden. Zum einen werden Standortdaten, soweit ersichtlich, von niemandem dem Schutzbereich des Art 10a StGG zugeordnet[192]. Auch aus den EB ergibt sich nicht, worauf sie sich die Einbeziehung von Standortdaten zu stützen vermag. Hinzu kommt, dass sich aus den Materialien zur SPG-Novelle 2007 eine ganz andere Sichtweise des Gesetzgebers ableiten lässt. Dort heißt es: *„Solange*

---

[188] Auch aus der Regierungsvorlage ergibt sich, das eine derartige Einschränkung wohl nicht beabsichtigt sein kann: RV 128 BlgNR XXII. GP, 18.

[189] *Raschhofer* in *Zankl* (Hrsg), auf dem Weg zum Überwachungsstaat? (2009) 54; *Thiele,* in *Triffterer/Rosbaud/Hinterhofer* (Hrsg), Salzburger Kommentar zum StGB (15. ErgLf 2007) § 119 Rz 10; *Stomper,* Auskunftsanspruch gegen Internet-Provider nach österreichischem Recht, MR-Int 2005, 99 (100); *Wessely,* Das Fernmeldegeheimnis – ein unbekanntes Grundrecht? ÖJZ 1999, 491 (494), *Wiederin* in *Korinek/Holoubek*, Österreichisches Bundesverfassungsrecht III, Art 10a StGG Rz 12 mwN; aM etwa vor allem strafrechtliche Entscheidungen: OGH 6.12.1995, 13 Os 161/95 JBl 1997, 260; 17.6.1998, 13 Os 68/98, EvBl 1998/19, VwGH 27.5.2009, 2007/05/0280, *Damjanovic/Holoubek/Kassai/Lehofer/Urbanitsch,* Handbuch des Telekommunikationsrechts (2006) 243; *Mayer-Schönberger/Brandl,* Telekommunikationsgesetz und Datenschutz, ecolex 1998, 272 (273); *Reindl-Krauskopf/Tipold/Zerbes,* in *Fuchs/Ratz* (Hrsg), Wiener Kommentar zur Strafprozessordnung (2009) § 134 Rz 28; *Reindl,* Die nachträgliche Offenlegung von Vermittlungsdaten des Telefonverkehrs im Strafverfahren („Rufdatenrückerfassung"), JBl 1999, 791 (797); *Schmölzer,* Rückwirkende Überprüfung von Vermittlungsdaten im Fernmeldeverkehr, JBl 1997, 211 (214); *Helmreich,* Auskunftspflicht des Access-Providers bei Urheberrechtsverletzungen? ecolex 2005, 379 (379); *Kunnert,* Der sicherheitspolizeiliche Griff nach Telekommunikationsdaten. Möglichkeiten – Grenzen – Kritik, in *Jahnel* (Hrsg), Datenschutzrecht und E-Government: Jahrbuch 2008 (2008) 123; *Satenig,* Stille Nacht, heimliche Macht Zur SPG-Novelle 2007 und der Erweiterung sicherheitspolizeilicher Ermittlungsbefugnisse, juridikum 2008, 130 (131); *Zyklan*, Zum Verhältnis des Auskunftsanspruchs gem § 87b Abs 3 UrhG zum Datenschutz: OGH 14. 7. 2009, 4 Ob 41/09x, MR 2009, 251 – Keine Auskunft über die Identität von Inhabern dynamischer IP-Adressen, jusIT 2009, 206 (209).

[190] BGBl 8/1974.

[191] RV 25 BlgNR XXII. GP, 190.

[192] *Raschhofer* in *Zankl*, Auf dem weg zum Überwachungsstaat? (2009) 100; *Reindl-Krauskopf/Tipold/Zerbes, Fuchs/Ratz* (Hrsg), Wiener Kommentar zur Strafprozessordnung (2009) § 134 Rz 29

Standortdaten nicht auf dem Übertragungsweg abgefangen werden sollen, sondern durch Erhebung beim Diensteanbieter gewonnen werden, liegt kein Eingriff in das Fernmeldegeheimnis des Art 10a StGG vor. Nur Inhaltsdaten sind dem Fernmeldegeheimnis iSd Art 10a StGG zuzurechnen, ihre Erhebung ist unter Gesetzes- und Richtervorbehalt zu stellen (vgl dazu Wessely, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht, ÖJZ 1999, 491)."[193] Aufgrund dieser Widersprüchlichkeit ist aus den EB zur StPO- und zur SPG-Novelle nichts Brauchbares abzuleiten. Anders verhält es sich mit den EB zum derzeitigen Umsetzungsentwurf zur RI 2006/24/EG des Ludwig Boltzmann Instituts für Menschenrechte (fortan „aktueller Umsetzungsentwurf zur VDS-RI"), die zu § 99 Abs 5 Z 2 detailliert darlegen, weshalb Art 10a StGG auch Verkehrsdaten umfassen soll. Diese befassen sich ausführlich mit dem hier interessierenden Problem und erklären, dass Art 10a StGG Verkehrsdaten schützt[194]. Dabei handelt es sich der Sache nach jedoch in Wahrheit um eine authentische Interpretation von Art 10a StGG, die gem § 8 ABGB als Gesetz beschlossen und kundgemacht werden muss[195]. Soll Art 10a StGG authentisch interpretiert werden, wie dies die EB im Ergebnis versuchen, ist eine Verfassungsbestimmung vonnöten. Ohne eine solche Bestimmung kommt den EB hinsichtlich der Auslegung formell derselbe Wert zu, wie auch den zitierten Gegenmeinungen in der Literatur und Judikatur. Insbesondere sind die EB nicht geeignet, den subjektiven Willen des historischen Gesetzgebers von 1974, der das Fernmeldegeheimnis in das StGG einfügte, zu bestimmen. Die ausführliche Begründung und fundierte Auseinandersetzung mit dem Thema in den EB stellt aber einen wertvollen Beitrag zu diesbezüglichen Diskurs dar.

Der VfGH musste sich in diesem Punkt bis dato bedauerlicherweise noch nie exakt festlegen. Im Jahr 2008 brachten mehrere Personen Individualanträge gegen die durch die SPG-Novelle 2007[196] novellierten § 53 Abs 3a und 3b SPG ein, die Auskunftsverlangen hinsichtlich Standortdaten und IP-Adressen normieren[197]. Diese Individualanträge wurden jedoch mangels aktueller und unmittelbarer Betroffenheit (Art 140 B-VG) zurückgewiesen, weshalb sich der VfGH auch in diesen Fällen nicht mit der hier interessierenden Frage auseinandersetzen musste. Eine diesbezügliche Klarheit stiftende Einordnung von Verkehrsdaten durch den VfGH wäre sehr wünschenswert.

---

[193] RV 272 BlgNR XXIII. GP, 3.

[194] EB ME 117 BlgNR XXIV. GP 15ff.

[195] *Posch* in *Schwimann*, ABGB I^3 (2005) § 8 Rz 3.

[196] BGBl I 114/2007.

[197] VfGH 1.7.2009, G 29/08, G 30/08, G 31/08, G 35/08, 147/08.

4.4.3. Zugangsdaten § 92 Abs 3 Z 4a TKG 2003

"Zugangsdaten" 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. Diese Daten dienen somit zur Identifikation von Teilnehmern an einer Internetkommunikation[198]. Hierher gehören etwa IP-Adressen[199], die gleichzeitig auch Verkehrsdaten sind[200]. Der aktuelle Umsetzungsentwurf zur VDS-RI enthält diesbezüglich auch eine ausdrückliche Klarstellung. Der durch die Novelle einzuführende § 92 Abs 3 Z 16 bestimmt: *„[...] Öffentliche IP-Adressen sind Zugangsdaten im Sinne des § 92 Abs 3 Z 4a. Wenn eine konkrete öffentliche IP-Adresse einem Teilnehmer für die Dauer des Vertrages zur ausschließlichen Nutzung zugewiesen ist, handelt es sich zugleich um ein Stammdatum im Sinne des § 92 Abs 3 Z 3.*"

4.4.4. Inhaltsdaten § 92 Abs 3 Z 5 TKG 2003

Darunter sind die Inhalte übertragener Nachrichten zu verstehen. Nachrichten sind Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet wird (siehe dazu Z 7 leg cit). Nachrichten müssen nach den Begriffsbestimmungen der EK-Datenschutzrichtlinie nicht zwingend zwischen Menschen ausgetauscht worden, es ist auch der Informationsaustausch zwischen Maschinen erfasst[201]. Wenn jemand mit einem Server seines Access-Providers kommuniziert, stellen die übertragenen Daten Inhaltsdaten von Nachrichten dar[202]. Inhaltsdaten sind besonders geschützt und

---

198 AB 128 BlgNR XXII. GP, 3.

199 *Einzinger/Schubert/Schwabl/Wessely/Zykan*, Wer ist 217.204.27.214? MR 2005, 113 (116); DSK 29.9.2006, K 213.000/0005-DSK/2006.

200 *Einzinger/Schubert/Schwabl/Wessely/Zykan*, Wer ist 217.204.27.214?, MR 2005, 113 (116); *Helmreich*, Auskunftspflicht des Access-Providers bei Urheberechtsverletzungen? ecolex 2005, 379 (379); *Parschalk/Otto/Weber/Zuser*, Telekommunikationsrecht (2006) 206 FN 654; *Wiebe*, Auskunftsverpflichtung der Access-Provider, Beilage zu MR 2005/4, 13 ff; *Zanger/Schöll*, Telekommunikationsgesetz[2] (2004) § 92 Rz 51; differenzierend *Stomper*, Zur Auskunftspflicht von Internet-Providern, MR 2005, 118 (119).

201 *Zanger/Schöll*, Telekommunikationsgesetz[2] (2004) § 92 Rz 32.

202 *Feiler* in *Zankl* (Hrsg), Auf dem Weg zum Überwachungsstaat? (2009) 54.

unterliegen nicht nur dem Schutz des Art 8 EMRK, sondern auch unbestritten dem Fernmeldegeheimnis gem Art 10a StGG[203]. Siehe auch unten Kapitel 6.11.5.

4.4.5. Standortdaten § 92 Abs 3 Z 6 TKG 2003

Das sind Daten, die in einem Kommunikationsnetz verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben. Standortdaten sind also Informationen über den Aufenthaltsort der Telekommunikationseinrichtung zB über geografische Länge, Breite oder Höhe (vgl Erwägungsgrund 14 der EK-Datenschutzrichtlinie). Gewisse Standortdaten – etwa die Information darüber, in welcher Funkzelle sich eine Telekommunikationsendeinrichtung befindet – können auch für die Weiterleitung der Nachrichten nötig sein und damit ebenfalls unter den Begriff der Verkehrsdaten fallen. Daten, die den Standort des Endgerätes des Nutzers genauer angeben[204], als es für die Erbringung des Kommunikationsdienstes nötig wäre (etwa eine punktgenaue Standortbestimmung via GPS) unterliegen einem besonderen Schutz gem § 102 Abs 1 TKG 2003 (vgl auch Erwägungsgrund 35 und Art 9 der EK-Datenschutzrichtlinie). Die Verarbeitung derartiger Daten darf, wenn keine besondere Einwilligung des Nutzers vorliegt, nur anonymisiert erfolgen.

All diese Daten können Gegenstand von Auskunftsverlangen Privater oder von Behörden sein. Der verfassungs- und datenschutzrechtliche Schutz dieser Daten variiert. So werden etwa Inhaltsdaten durch Art 10a StGG stärker geschützt als Standortdaten, die nach einhelliger Auffassung nicht in den Schutzbereich des Art 10a StGG fallen[205]. Ob sich aus diesen unterschiedlichen Schutzniveaus auch Rückschlüsse auf die Schutzpflichten ziehen lassen, wird noch zu besprechen sein.

4.4.6. Der Zusammenhang zwischen den Datenkategorien

Wie erwähnt bestehen für die unterschiedlichen Datenkategorien unterschiedliche Schutzniveaus. Ein besonders hohes Schutzniveau ergibt sich aus dem

---

203 *Reindl-Krauskopf/Tipold/Zerbes, Fuchs/Ratz* (Hrsg), Wiener Kommentar zur Strafprozessordnung (2009) § 134 Rz 28; *Wiederin* in *Korinek/Holoubek*, Österreichisches Bundesverfassungsrecht III, Art 10a StGG Rz 12 mwN.

204 Zur wirtschaftlichen Verwertbarkeit von Standortdaten etwa zur standortbezogenen Werbung vgl *Schrey/Meister*, Beschränkte Verwendbarkeit von Standortdaten – Hemmschuh für den M-Commerce, K&R 2002, 177ff.

205 *Raschhofer* in *Zankl*, Auf dem weg zum Überwachungsstaat? (2009) 100; *Reindl-Krauskopf/Tipold/Zerbes, Fuchs/Ratz* (Hrsg), Wiener Kommentar zur Strafprozessordnung (2009) § 134 Rz 29.

Fernmeldegeheimnis. So besteht für Inhaltsdaten der höchste Schutz. Art 10a StGG bestimmt, dass Eingriffe in das Fernmeldgeheimnis nur aufgrund „eines richterlichen Befehles in Gemäßheit bestehender Gesetze zulässig" sind. Diese Vorgaben binden zunächst vor allem den Gesetzgeber, der bestimmte Auskunftsbegehren nur bei gleichzeitiger Implementierung einer gerichtlichen Kontrolle normieren darf. Sieht man daher auch Verkehrsdaten (unzutreffenderweise[206]) als vom Schutz des Fernmeldegeheimnisses umfasst an, dürften darauf abzielende Auskunftsbegehren nicht ohne Richtervorbehalt statuiert werden. Nach dieser Auffassung wäre daher § 53 Abs 3a Z 2 SPG, der bestimmt, dass Auskunft über eine „Internetprotokolladresse (IP-Adresse) zu einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung" zu erteilen ist, verfassungswidrig. Für den Vollzug einfachgesetzlicher Vorschriften bedeutet dies, dass Generalklauseln ohne Richtervorbehalt wie § 22 Abs 1 MBG[207], die zwar grundsätzlich hinsichtlich der Ermittlung keine Beschränkung von Methoden oder Quellen normieren[208], nicht zur Ermittlung von Inhaltsdaten herangezogen werden dürfen. Dies ergibt sich aus einer verfassungskonformen Auslegung solcher Bestimmungen.

Fraglich ist, inwieweit bei der Beurteilung der Konformität eines Gesetzes bzw eines Aktes der Vollziehung mit dem höherrangigen Recht der Zusammenhang zwischen den betroffenen Datenkategorien ausgeblendet werden darf. Nehmen wir an, die Sicherheitspolizei kommt in den Besitz einer Nachricht, von der sie den Inhalt kennt und von der sie den Zeitpunkt des Versendens kennt. Überdies ist sie in Kenntnis der IP-Adresse, die jener Netzwerkschnittstelle zugeordnet war, von der aus die Nachricht versendet wurde. Nun wendet sie sich an den Access-Provider damit dieser ihr Auskunft über die Identität der hinter der IP-Adresse stehenden Person gibt. Das Auskunftsbegehren kann mit der bloßen Bekanntgabe des Namens und der Anschrift erfüllt werden. Sowohl Name als auch Anschrift zählen nach den Begriffsbestimmungen des TKG zu den so genannten Stammdaten, die keinesfalls dem Fernmeldegeheimnis unterliegen. Bei isolierter einzig auf die erteilten Auskünfte bezogener Betrachtungsweise könnte man daher vertreten, es habe kein Eingriff in das Fernmeldegeheimnis stattgefunden, da ja nur Stammdaten bekannt gegeben wurden. Allerdings ist diese Sichtweise bei einer ganzheitlichen am telos der berührten Vorschriften orientierten Betrachtung deutlich zu kurz geraten und nicht haltbar: Das Fernmeldegeheimnis will die Inhalte von Kommunikation einem besonderen Schutz unterstellen. Möchte der Staat Kenntnis davon erlangen, wer mit wem was kommuniziert, hat er die Kautelen des

---

[206] Siehe dazu oben Kapitel 4.4.2.

[207] BGBl I 86/2000 idF I 85/2009.

[208] *Hauer/Keplinger/Kreutner,* MBG (2005) § 22 A.6.ff; *Raschauer/Wessely,* Militärbefugnisgesetz[2] (2007) § 22 Anm 3; *Wiederin,* Privatsphäre und Überwachungsstaat (2003) 169.

Art 10a StGG zu beachten. Genau diese würde er aber nicht einhalten, wenn ihm in obigem Beispiel ohne gerichtliche Prüfung Auskunft erteilt werden würde. Der Staat kennt in diesem Beispiel zwar das „was", dh den Inhalt der Kommunikation. Diese Information ist für ihn aber völlig wertlos, solange er nicht erfährt, wer mit wem diese Inhalte ausgetauscht hat. Bekommt er diese Information, ist genau das eingetreten, was das Fernmeldegeheimnis verhindern wollte: Die ohne gerichtliche Prüfung erfolgende Kenntnisnahme davon, wer mit wem was kommunizierte. Der Eingriff in das Fernmeldegeheimnis ergibt sich in obigem Beispiel reflexartig[209]. Sofern Auskünfte über Daten mit einem Schutzniveau A erteilt werden, ist daher immer auch zu fragen, ob dadurch auch neue Information über Daten eines höheren Schutzniveaus B erlangt werden. Dies ist immer dann der Fall, wenn zwischen den Daten wie in obigem Beispiel ein eindeutiger Zusammenhang besteht. Sollte dies der Fall sein, sind mE stets die Vorschriften, die das höhere Schutzniveau B begründen, zu beachten. Dies gilt nicht nur im Verhältnis zwischen Inhaltsdaten und Daten, die ein geringeres Schutzniveau genießen, sondern ganz allgemein immer dann, wenn ein unterschiedliches Schutzniveau besteht.

Die oben beschriebene zu kurzsichtige Sichtweise teilte der OGH etwa in einer Entscheidung im Jahr 2005, in der er aussprach, dass Stammdaten nach § 103 Abs 4 TKG 2003 formlos bekannt gegeben werden könnten. In diesem Fall war die IP-Adresse einer Internetkommunikation bekannt, und es sollten vom Access-Provider Name und Anschrift jener Person bekannt gegeben werden, denen diese IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet war. Da sich die Auskunft nur auf Stammdaten beziehe, kämen die einschränkenden Bestimmungen der StPO in ihrer alten und auch nach In-Kraft-Treten der StPO-Novelle 2004 geltenden Fassung nicht zur Anwendung[210]. Die einschränkenden Bestimmungen kämen nur dann zur Anwendung kommen, wenn das Auskunftsbegehren auf Verkehrsdaten abzielte. Nur wenn die IP-Adresse Gegenstand des Auskunftsbegehrens gewesen wäre, wäre ein Eingriff nach § 149 Abs 1 Z 1 lit b StPO aF bzw § 134 Z 2 StPO nF vorgelegen. Dass der OGH in diesem Punkt vor allem deshalb nicht völlig richtig lag, weil die begehrte Auskunft zwingend zu einer Verarbeitung von Verkehrsdaten führte[211], hat er mittlerweile im Ergebnis auch bereits selbst eingeräumt.

---

[209] So auch *Feiler* in *Zankl*, Auf dem Weg zum Überwachungsstaat? (2009) 67, vgl auch *Funk/Krejci/Schwarz,* Zur Registrierung von Ferngesprächsdaten durch den Dienstgeber, RdA 1984, 285 (289): Diese meinen, dass „äußere Gesprächsdaten", worunter sie im Ergebnis „Verkehrsdaten iSd heutigen Terminologie verstehen, immer dann vom Schutz des Art 10a StGG umfasst seien, wenn sich daraus Rückschlüsse auf den Inhalt zeihen ließen.

[210] OGH 26.7.2005, 11 Os 57/05z, EvBl. 2005/176 = MR 2005, 352 = JBl 2006, 130 = RZ 2006/17, vgl in diesem Zusammenhang auch *Bergauer,* Auskunftspflicht der Access-Provider: Zwei kontroverse Beschlüsse des OLG Wien, RdW 2005, 467ff.

[211] Worauf auch die DSK eindringlich hinwies, vgl DSK 29.9.2006, GZ K213.000/0005-DSK/2006.

So meinte er: *„Der einfache Weg, allein auf die Bekanntgabe von Stammdaten abzustellen und die Vorgänge bei deren Ermittlung völlig auszublenden, ist damit gemeinschaftsrechtlich nicht gangbar (ebenso zur vergleichbaren Problematik im Strafverfahren DSK GZ K 213.000/0005 – DSK/2006). Vielmehr ist anzunehmen, dass Art 6 der RL 2002/58/EG und dessen Umsetzung in § 99 TKG 2003 der – im vorliegenden Fall erforderlichen – Verarbeitung von Verkehrsdaten für die Erteilung der hier begehrten Auskunft entgegensteht. Denn nach Absatz 1 dieser Bestimmung sind „Verkehrsdaten, die sich auf Teilnehmer und Nutzer beziehen und vom Betreiber eines öffentlichen Kommunikationsnetzes oder eines öffentlich zugänglichen Kommunikationsdienstes verarbeitet und gespeichert werden, [...] unbeschadet der Absätze 2, 3 und 5 des vorliegenden Artikels und des Artikels 15 Absatz 1 zu löschen oder zu anonymisieren, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden."* [212]

Der OGH stützte sich dabei begründend vor allem auf die in diesem Verfahren ergangene Vorabentscheidung des EuGH[213]. Aus dieser wie auch einer ähnlichen Entscheidung des EuGH[214] ergibt sich, dass auch der EuGH Auskünfte über Stammdaten, die zu einer Verarbeitung von Verkehrsdaten führen, grundsätzlich als durch Art 6 der EK-Datenschutzrichtlinie verboten betrachtet. Nur unter den Voraussetzungen des Art 15 leg cit lässt der EuGH solche Eingriffe zu. Daraus ergibt sich, dass mittlerweile sowohl EuGH als auch OGH Auskunftsbegehren nicht nur stur danach bewerten, was beauskunftet wird, sondern auch darauf achten, welche Rückschlüsse sich dadurch auf bereits vorhandene Informationen liefern lassen.

Erfreulicherweise hat auch das Ludwig Boltzmann Institut bei der Erarbeitung des aktuellen Umsetzungsentwurfs zur VDS-RI[215] der Vorratsdatenspeicherungsrichtlinie diesen Zusammenhang erkannt und entsprechend berücksichtigt. So wird die Auskunftspflicht über Stammdaten im neu eingeführten § 90 Abs 6 TKG 2003 an die Voraussetzung geknüpft, dass die Erteilung ohne Verarbeitung von Verkehrsdaten möglich ist[216].

---

[212] OGH 14.7.2009, 4 Ob 41/09x, MR 2009, 251.

[213] EuGH Beschluss vom 19.2.2009, C-557/ 07 LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH gegen Tele2 Telecommunication GmbH.

[214] EuGH 29.1.2008, C-275/06, Productores de Música de España (Promusicae) gegen Telefónica de España SAU, Slg 2008 I-00271.

[215] ME 117 BlgNR XXIV. GP.

[216] EB ME 117 BlgNR XXIV. GP 9.

4.5. Datenschutzrechtliche Verpflichtungen im Verhältnis zwischen dem Access-Provider und dem Benutzer

Wie oben bereits erwähnt ist dieses Verhältnis vor allem in den Bestimmungen der §§92ff TKG 2003 ausdrücklich gesetzlich geregelt. Diese Bestimmungen sollen zunächst kursorisch dargestellt werden, um daraus später Ableitungen für die Konstruktion der schuldrechtlichen Verpflichtungen des Access-Providers gewinnen zu können.

4.5.1. Allgemeines

Das TKG 2003 ist lex specialis zum DSG 2000. § 92 TKG 2003 bestimmt ausdrücklich, dass das DSG 2000 anwendbar ist, soweit dieses Gesetz nichts anderes bestimmt. So sind etwa die Bestimmungen des Datengeheimnisses und der Datensicherheit gem § 14 DSG 2000 zu beachten (vgl § 95 TKG 2003). Insbesondere ist auch das mit unmittelbarer Drittwirkung ausgestattete Recht auf Geheimhaltung von Daten gem § 1 DSG 2000 zu beachten. Den sektorspezifischen Risiken hinsichtlich der bei elektronischer Kommunikation verarbeiteten Daten soll ein für diesen Sektor besonders detaillierter Schutz entgegen gesetzt werden. Ein ausdrücklicher Vorrang gegenüber den Bestimmungen des TKG wird der StPO in § 92 Abs 2 TKG 2003 eingeräumt. Hinsichtlich sonstiger Gesetze, die vergleichbare Auskunftspflichten statuieren (SPG, MBG,...) fehlt eine derartige Vorrangbestimmung. Das bedeutet, dass diese Gesetze parallel anzuwenden sind und Konkurrenzen, soweit möglich, über den Grundsatz *lex specialis derogat legi generali* zu lösen sind (zu dieser Problematik siehe unten die Kapitel 4.5.4 und 5.5.8.3).

Das TKG enthält einige auf alle Datenkategorien zugeschnittene Bestimmungen. Diese enthalten etwa Informationspflichten, das Kommunikationsgeheimnis und die Normierung einer strikten Zweckbindung. Dazu kommen noch Spezialvorschriften für einzelne Datenkategorien.

4.5.2. Kommunikationsgeheimnis

Das einfachgesetzliche Kommunikationsgeheimnis, das nicht mit dem verfassungsrechtlichen Fernmeldegeheimnis gem Art 10a StGG verwechselt werden darf, umfasst nicht nur Inhalts- sondern auch Standort- und Verkehrsdaten. Unzutreffend ist daher jedenfalls die Behauptung, durch § 93 TKG 2003 soll der Begriff des

Fernmeldegeheimnisses näher umschrieben werden[217]. Das Kommunikationsgeheimnis erstreckt sich auch auf erfolglose Verbindungsversuche und bindet Betreiber und alle an der Tätigkeit der Betreiber mitwirkenden Personen auch nach Beendigung der Tätigkeit. Gem § 93 Abs 3 TKG 2003 ist das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen ohne Einwilligung der Nutzer unzulässig. Ausnahmen bestehen nur bei Notrufen und technisch notwendigen kurzen Speicherungen. Nimmt man diese Bestimmung wörtlich, so wäre jedes Aufzeichnen von Verkehrs- und Standortdaten außerhalb dieser Ausnahmen unzulässig. Diese Bestimmung hat aber vorrangig nur im Auge, dass niemand Unbefugter vom Inhalt von Nachrichten Kenntnis nimmt und schützt daneben auch „die damit verbundenen Verkehrsdaten". Für die Verarbeitung von Verkehrsdaten ist daher in erster Linie § 99 TKG 2003 zu beachten. Dieser erlaubt etwa das Aufzeichnen von Verkehrsdaten, soweit dies für die Verrechnung nötig ist. § 99 leg cit ist somit lex specialis zu § 96 Abs 3 leg cit. Der Tatbestand der letzteren Bestimmung verlangt nur das Vorliegen der Verkehrsdateneigenschaft. Als Rechtsfolge wird ein allgemeines Aufzeichnungs-, dh Speicherverbot normiert. Der Tatbestand des § 99 leg cit ist demgegenüber genauer, da er nicht nur auf die Verkehrsdateneigenschaft abstellt, sondern darüber hinaus auch verlangt, dass die Verkehrsdaten zu Verrechnungszwecken verarbeitet werden. Diesfalls wird die Rechtsfolge der ausnahmsweisen Zulässigkeit der Speicherung normiert.

4.5.3. Zweckbindung bei Datenverwendungen und Selbstbestimmung

Eine grundlegende für alle Datenkategorien geltende Regel stellt § 96 TKG 2003 auf. Nach dieser Bestimmung dürfen Stamm-, Verkehrs-, Standort- und Inhaltsdaten nur für Zwecke der Besorgung eines Kommunikationsdienstes ermittelt oder verarbeitet werden. Unerklärlich ist dabei, weshalb der Gesetzgeber hier neben dem Begriff des „Verarbeitens" auch den Begriff des „Ermittelns" erwähnt. Nach den diesbezüglich eindeutigen EBRV wollte der Gesetzgeber sich an den Begriffsbestimmungen der EK-Datenschutzrichtlinie orientieren[218]. Deren Begriffsbestimmungen orientieren sich gem Art 2 Abs 1 EK-Datenschutzrichtlinie an jenen der Rl 1995/46/EG[219] (fortan: allgemeine Datenschutzrichtlinie). Diese versteht

---

[217] So aber *Zanger/Schöll,* Telekommunikationsgesetz[2] (2004) § 93 Rz 9.

[218] RV 128 BlgNR XXII. GP, 17.

[219] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 1995/281, 31.

ebenso wie das DSG 2000 und die meisten Landesdatenschutzgesetze unter „Verarbeiten" einen Überbegriff, der auch den Begriff des „Ermittelns" immer einschließt (§ 4 Z 9 DSG 2000, Art 2 lit b allgemeine Datenschutzrichtlinie). Vor diesem durch das DSG und die allgemeine Datenschutzrichtlinie vorgegebenen Begriffsverständnis erscheint das „ermitteln" im Begriffspaar „ermitteln und verarbeiten" überflüssig.

Nicht erfasst vom Begriff des „Verarbeitens" ist jener des „Übermittelns"[220]. Darunter versteht man gem § 4 Z 12 DSG 2000 insbesondere die Weitergabe von Daten einer Datenanwendung an andere Empfänger als den Betroffenen (§ 4 Z 3 DSG 2000), den Auftraggeber (§ 4 Z 4 leg cit) oder einen Dienstleister (§ 4 Z 5 leg cit). Für das „Übermitteln" von Daten wird in § 96 Abs 2 TKG 2003 eine besondere Regelung getroffen, wonach sämtliche Datenkategorien nur soweit übermittelt werden dürfen, als dies für die Erbringung jenes Kommunikationsdienstes, für den diese Daten ermittelt und verarbeitet worden, erforderlich ist. Unklar ist, worin sich die Abs 1 und 2 leg cit hinsichtlich der Zulässigkeitsvoraussetzungen unterscheiden. Abs 1 leg cit stellt auf die „Besorgung eines Kommunikationsdienstes", Abs 2 leg cit stellt auf die „Erbringung" desselben ab. *Zanger* und *Schöll* meinen, dass die Übermittlung „zweckerforderlich" und die Verarbeitung hingegen nur „zweckbezogen" sein müsse[221]. Diesen Unterschied vermag ich nicht zu erkennen[222]. Schließlich ist wegen §§ 1 und 6 DSG 2000 die Erforderlichkeit ohnedies Maßstab und Grenze für jede Datenverwendung[223]. Legte man § 96 Abs 1 TKG 2003 so aus, dass die Verarbeitung für die Erbringung des Kommunikationsdienstes nicht erforderlich sein müsste, sondern nur irgendwie diesem Zweck dienen müsse, stünde dies mit zentralen Prinzipien des Datenschutzrechts im Widerspruch. Zusammenfassend lässt sich daher festhalten, dass sowohl die Verarbeitung als auch die Übermittlung nur dann zulässig sein soll, wenn dies zur Erbringung bzw Besorgung von Kommunikationsdiensten erforderlich ist[224].

Ausnahmsweise dürfen die Stamm-, Verkehrs-, Standort- und Inhaltsdaten zur Vermarktung von Kommunikationsdiensten oder zur Bereitstellung von Diensten mit

---

220 „Verwenden" ist der Überbegriff, der sowohl das Verarbeiten als auch das Übermitteln erfasst.

221 *Zanger/Schöll*, Telekommunikationsgesetz[2] (2004) § 96 Rz 27.

222 Der OGH (16.3.2004, 4 Ob 7/04i, ecolex 2004, 854 = wbl 2004, 390 = RdW 2004, 475 = MR 2004, 221 = SZ 2004/33) schließt sich der Auffassung *Zangers* und *Schölls* ohne nähere Begründung an.

223 *Damjanovic/Holoubek/Kassai/Lehofer/Urbanitsch,* Handbuch des Telekommunikationsrechts (2006) 249.

224 Aus den Materialien (RV 128 BlgNR XXII. GP, 17) lässt sich hinsichtlich dieser Frage auch nichts ableiten, da diese eigentlich nur auf die EK-Datenschutzrichtlinie verweisen. Letztere enthält jedoch keine § 96 TKG 2003 vergleichbare Bestimmung, die sich auf alle Datenkategorien bezieht.

Zusatznutzen verwendet werden, wenn diesbezüglich eine jederzeit widerrufbare Zustimmung des Betroffenen vorliegt. Die Zulässigkeit „sonstiger Übermittlungen" kann nach dem Wortlaut des Gesetzes ohne Zweckbindung vereinbart werden. Aus dieser Formulierung lässt sich mE erschließen, dass die Privatautonomie hinsichtlich der Datenverwendung begrenzt ist. Neben der Datenverwendung zum Zweck der Erbringung von Kommunikationsdiensten (§ 96 Abs 1, 2 TKG 2003) dürfen Verwendungen nur noch für Vermarktung und Zusatzdienste vereinbart werden.

Darüber hinausgehende Verarbeitungen untersagt das Gesetz. Nur für „sonstige Übermittlungen" steht es nach dem Wortlaut der Bestimmung den Parteien frei, einen beliebigen Zweck festzulegen. Dieses Ergebnis erscheint freilich befremdlich. Wieso sollte eine Verarbeitung außerhalb der Erbringung von Kommunikationsdiensten nur für bestimmte Zwecke vereinbart werden dürfen, während eine Übermittlung für jeden beliebigen Zweck vereinbart werden darf?

Der Grundsatz der Privatautonomie ist schließlich auch im allgemeinen Datenschutzrecht verwirklicht: Gem § 1 Abs 2 DSG 2000 ist die Zulässigkeit von Beschränkungen des Grundrechts auf Geheimhaltung personenbezogener Daten nicht vom Überwiegen der Interessen anderer abhängig, wenn der Betroffene der Verwendung zustimmt. Dieses Prinzip findet sich auch in den einfachgesetzlichen Regelungen der §§ 7ff DSG 2000 wieder. Gem § 7 Abs 1 leg cit dürfen Daten nur verarbeitet werden, wenn keine schutzwürdigen Geheimhaltungsinteressen verletzt werden. Übermittlungen setzen gem Abs 2 leg cit vor allem voraus, dass die Daten aus einer gem Abs 1 leg cit zulässigen Datenanwendung stammen (Z 1) und keine schutzwürdigen Geheimhaltungsinteressen des Betroffenen verletzt werden (Z 2). § 8 Abs 1 Z 2 DSG 2000 bestimmt, dass bei der Verwendung nicht sensibler Daten schutzwürdige Geheimhaltungsinteressen nicht verletzt werden, soweit eine jederzeit widerrufbare Zustimmung vorliegt. Somit kann der Betroffene sich seines durch das DSG gewährten Schutzes jederzeit durch entsprechende Zustimmungen begeben. Eine Zustimmung ist gem § 4 Z 14 leg cit „die gültige, insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen, daß er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt". Aus der Wendung „in Kenntnis der Sachlage" folgt, dass der Betroffene genauestens darüber zu informieren ist, welche Daten für welchen Zweck verwendet werden[225]. Nach hA ist die bei nicht sensiblen Daten auch in konkludenter Form mögliche[226] Willenserklärung nach zivilrechtlichen Regeln zu beurteilen. Das bedeutet, dass die Zustimmungserklärung etwa wegen Irrtums oder List, wegen mangelnder Geschäftsfähigkeit, Sittenwidrigkeit oder Wuchers angefochten

---

[225] OGH 22.3.2001, 4 Ob 28/01y, ecolex 2001, 438 = ÖBA 2001, 645.

[226] Dies folgt e contrario aus § 9 Z 6 DSG 2000.

werden kann[227]. Die Prüfbarkeit nach dem Tranzparenzgebot gem § 6 Abs 3 KSchG wurde vom OGH bereits bejaht[228].

Es lässt sich daher festhalten, dass die Selbstbestimmung im allgemeinen Datenschutzrecht ein zentrales Prinzip darstellt. Dies verleitet zum Schluss, dass dieses Prinzip auch im auf den Sektor der elektronischen Kommunikation beschränkten Datenschutz gilt[229]. Eine derartige Sichtweise lässt sich jedoch mit dem äußerst möglichen Wortsinn der Abs 1 und 2 des § 96 TKG 2003 nicht mehr vereinbaren. Während Abs 1 leg cit die Verarbeitung für Zwecke außerhalb der Besorgung von Kommunikationsdiensten untersagt, lässt Abs 2 leg cit bei Zustimmung des Betroffenen gewisse Ausnahmen zu. Die Verarbeitung von Daten zu anderen Zwecken als der Vermarktung von Kommunikationsdiensten oder der Bereitstellung von Diensten mit Zusatznutzen bildet keine dieser Ausnahmen. Nur die Übermittlung von Daten darf zu anderen Zwecke vereinbart werden.

Bleibt die Frage nach einem Größenschluss (a maiori ad minus): wenn sogar die Übermittlung, dh die Weitergabe von Daten an Dritte für jeden beliebigen Zweck vereinbart werden darf, wieso sollte dann nicht auch die bloße Verarbeitung von Daten frei gestaltet werden können? Doch auch dieser Größenschluss muss aus den oben genannten Gründen versagen. Der Größenschluss (argumentum a fortiori) kann als verstärkte Abart des Analogieschlusses[230] – sofern man seine Rechtfertigung überhaupt bejaht[231] – nur dort angewendet werden, wo es eine Lücke im Gesetz gibt[232]. Im vorliegenden Falle liegt jedoch mE keine planwidrige Unvollständigkeit, sondern eine

---

[227] Gutachten des Verfassungsdienstes des Bundeskanzleramtes, GZ 810.093/4-V/3/92, 9ff; *Dohr/Pollirer/Weiss/Knyrim,* Datenschutzrecht[2] (2009), 6. ErgLf, § 14 Anm 15; zur alten in diesem Punkt jedoch identischen Rechtslage nach dem DSG 1978: Die Anwendbarkeit zivilrechtlicher Vorschriften bejahend hinsichtlich Willensmängeln, in punkto Geschäftsfähigkeit jedoch aufgrund des öffentlich rechtlichen Charakters der Zustimmungserklärung nur auf „natürliche Einsichtsfähigkeit" abstellend *Kuderna,* Die Zustimmung zur Übermittlung von Daten, RdA 1992, 721 (727ff); die Anwendbarkeit des Zivilrechts bejahend: *Matzka/Kotschy,* Datenschutzrecht für die Praxis (1986) § 7 K, 3.3; aA *Mayer,* Willensmängel im öffentlichen Recht, ecolex 1992, 812 (813ff), der die zwangsläufig analoge Anwendung der Vorschriften des ABGB ablehnt, da keine Lücke bestehe.

[228] OGH 27.1.1999, 7 Ob 170/98w, ARD 5023/25/99 = ecolex 1999, 484 = KRES 1d/42 = RdW 1999, 458.

[229] So *Damjanovic/Holoubek/Kassai/Lehofer/Urbanitsch,* Handbuch des Telekommunikationsrechts (2006) 250, die jegliche Verwendungen für zulässig erachten, wenn eine informierte Zustimmung des betroffenen iSd § 4 Z 14 DSG 2000 vorliegt, wobei sie sich jedoch mit der besonderen Formulierung in § 96 Abs 2 TKG 2003 nicht auseinandersetzen.

[230] *Bydlinski,* Juritische Methodenlehre und Rechtsbegriff (1982) 479.

[231] Dagegen etwa *Klug,* Juritische Logik[3] (1966) 132ff, der meint, dass sich dieses Argument letztlich immer durch nicht mehr logisch nachvollziehbare am Telos orientierte Wertungen gründet.

[232] *Bydlinski,* Juritische Methodenlehre und Rechtsbegriff (1982) 479; Larenz, Methodenlehre der Rechtswissenschaft[5] (1983) 365, 373ff.

klare Regelung vor. Diese Regelung mag angesichts der oben gezeigten voll verwirklichten Privatautonomie im allgemeinen Datenschutzrecht systemfremd erscheinen und wäre daher zu korrigieren. Solange dies jedoch nicht der Fall ist, führt an obiger Auslegung mE kein Weg vorbei.

Zusammenfassend lässt sich daher festhalten, dass die Übermittlung von Daten, wenn sie nicht zur Besorgung des Kommunikationsdienstes erfolgt, grundsätzlich eine jederzeit widerrufbare Zustimmung des Betroffenen voraussetzt. Die meisten Auskunftsbestimmungen, die zur Übermittlung von Daten des Betroffenen an Dritte führen, sehen jedoch keine Zustimmung des Betroffenen vor und stehen damit in einem Spannungsverhältnis zu § 96 Abs 2 TKG 2003, worauf im sogleich folgenden Kapitel ausführlich eingegangen werden wird.

4.5.4. Übermittlungsverbot gem § 96 Abs 2 TKG 2003

Fraglich ist, wie das Übermittlungsverbot gem § 96 Abs 2 TKG 2003 mit eindeutigen Übermittlungspflichten wie etwa jener gem § 53 Abs 3a Z 2 SPG in Einklang zu bringen ist. Gem § 92 Abs 2 TKG 2003 bleiben nur die Bestimmungen der StPO durch den 12. Abschnitt des TKG unberührt. Während § 96 Abs 2 TKG 2003 die Übermittlung nur für zulässig erklärt[233], soweit dies zur Erbringung von Kommunikationsdiensten durch den Betreiber erforderlich ist, lässt § 53 Abs 3a Z 2 SPG die Übermittlung dann zu, *„wenn bestimmte Tatsachen die Annahme einer konkreten Gefahrensituation rechtfertigen und sie* [Anm: die Sicherheitsbehörden] *diese Daten als wesentliche Voraussetzung für die Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben benötigen.*" Das TKG selbst enthält in § 90 Abs 6 eine ähnliche Auskunftsbestimmung: *„Betreiber von Kommunikationsdiensten sind verpflichtet, Verwaltungsbehörden auf deren schriftliches und begründetes Verlangen Auskunft über Stammdaten iSv § 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*." Schließlich enthält auch § 98 TKG 2003 eine Auskunftsbestimmung, aufgrund derer im Ergebnis personenbezogene Daten übermittelt werden.

§ 96 Abs 2 TKG 2003 schließt die Übermittlung für alle Fälle, in denen sie nicht zur Erbringung von Kommunikationsdiensten erforderlich ist, kategorisch aus[234]. Im

---

[233] Diese Bestimmung geht den Zulässigkeitsvoraussetzungen einer Datenübermittlung in § 7 Abs 2 DSG 2000 aufgrund § 92 Abs 1 TKG 2003 vor.

[234] So auch *Kassai,* Der Einsatz von Location Based Services – eine erste Analyse rechtlicher Problemfelder, MR 2004 (433) (435).

2. Satz leg cit wird die Zulässigkeit „sonstiger" – dh nicht für die Erbringung von Kommunikationsdiensten erforderlicher – Übermittlungen an das Erfordernis der ausdrücklichen Zustimmung des Betroffenen geknüpft. Andererseits gibt es sogar im TKG 2003 gesetzliche Ansprüche auf Übermittlung bestimmter Daten, die keinesfalls für die Erbringung von Kommunikationsdiensten erforderlich sind[235]. Kann dieser Widerspruch mit dem Grundsatz „lex specialis derogat legi generali" gelöst werden?

Dieser Lösungsweg käme nur dann in Frage, wenn die Bestimmung des SPG im Verhältnis zu jener des TKG als die engere, dh speziellere Norm zu betrachten ist. § 53 Abs 3a Z 2 SPG müsste dazu alle Tatbestandelemente von § 96 Abs 2 TKG 2003 und noch mindestens ein zusätzliches enthalten[236]. Der Anwendungsbereich der spezielleren Norm muss völlig in jenem der allgemeineren Norm aufgehen[237]. Dies ist jedoch im Verhältnis der angesprochenen Normen des TKG und des SPG (genau wie bei den meisten anderen vergleichbaren Normen wie § 22 Abs 2a MBG, 14a UWG) nicht der Fall. Als Rechtsfolge normieren sowohl § 96 Abs 2 TKG 2003 als auch die Auskunftsbestimmungen die Unzulässigkeit bzw Zulässigkeit der Übermittlung bestimmter Datenkategorien. Die Tatbestände stehen jedoch nicht im Verhältnis der Spezialität zueinander: Während das SPG eine Gefahr und die Notwendigkeit zur Aufgabenerfüllung als Übermittlungsvoraussetzung normiert, kommt es nach dem TKG auf die Notwendigkeit zur Erbringung der Kommunikationsdienste an. Auch die erwähnten Auskünfte nach den Bestimmungen im TKG (§§ 90 Abs 6, 98) sind nicht erforderlich, um Kommunikationsdienste zu erbringen. Weil beispielsweise die Weitergabe von Stammdaten des Mehrwertdiensteanbieters an den Kunden des Access-Providers nicht für die Erbringung des Kommunikationsdienstes erforderlich ist, wird diese in Literatur[238] und Judikatur[239] für unzulässig erachtet. Anwendungsfälle der Auskunftsbestimmungen sind somit nicht auch gleichzeitig Anwendungsfälle des § 96 Abs 2 TKG, wie dies zur Bejahung eines Spezialitätsverhältnisses erforderlich wäre. Ein unter § 53 Abs 3a Z 2 SPG subsumierbarer Sachverhalt kann nicht gleichzeitig auch unter § 96 Abs 2 TKG 2003 subsumiert werden. Diese Überlegung gilt auch für die meisten anderen Bestimmungen außerhalb der StPO, in denen Übermittlungspflichten hinsichtlich bestimmter Stamm-, Verkehrs- oder Standortdaten angeordnet werden. Es

---

[235] Vgl auch *Wiebe,* Auskunftsverpflichtung der Access-Provider – Verpflichtung zur Drittauskunft bei Urheberrechtsverletzungen von Kunden, die an illegalem File-Sharing teilnehmen, MR 2005, H 4 Beilage, 12.

[236] *Bydlinski,* Juristische Methodenlehre und Rechtsbegriff (1982) 465.

[237] *Larenz,* Methodenlehre der Rechtswissenschaft[5] (1983) 256.

[238] *Zanger/Schöll,* Telekommunikationsgesetz[2] (2004) § 97 Rz 25.

[239] OGH 16.3.2004, 4 Ob 7/04i, ecolex 2004, 854 = wbl 2004, 390 = RdW 2004, 475 = MR 2004, 221 = SZ 2004/33.

liegt somit eine klare Antinomie vor[240]. Das gilt auch für § 87b Abs 3 UrhG, der vor allem von Urhebern heran gezogen wird, um die Identität eines mutmaßlichen Verletzers, der sich hinter einer bestimmten IP-Adresse verbirgt, zu eruieren. Soweit aus dieser Norm ein Anspruch auf Übermittlung von Stammdaten abgeleitet wird[241], widerspricht sich auch diese Bestimmung mit § 96 Abs TKG 2003. Die Übermittlung von Stammdaten zur Ermittlung der Identität einer Person ist nicht zur Erbringung eines Kommunikationsdienstes erforderlich. Diesen Umstand übersieht auch der OGH in der aktuellen Entscheidung 4 Ob 41/09x (aus Gründen der einfacheren Identifizierbarkeit fortan nur mehr: *LSG gegen Tele 2)*[242], in der er zum Verhältnis zwischen § 96 Abs 1 TKG 2003 und § 87b Abs 3 UrhG meint: *„Zwar dürfen auch Stammdaten nach § 96 Abs 2 TKG 2003 nur übermittelt werden, soweit das für die Erbringung jenes Kommunikationsdienstes erforderlich ist, für den sie ermittelt und verarbeitet wurden; weiters ist die Ermittlung und Verarbeitung solcher Daten nach § 97 TKG 2003 nur eingeschränkt zulässig. § 87b Abs 3 UrhG kann aber insofern als speziellere Norm verstanden werden, die eine Übermittlung von Stammdaten auch für den dort geregelten Fall vorsieht*." In diesem Punkt ist dem OGH unter Berufung auf die oben angeführten Argumente entschieden zu widersprechen. Der OGH argumentiert, dass die Übermittlung auch zulässig sein muss, da § 97 Abs 2 TKG 2003 bestimmt, dass die Speicherung von Stammdaten ausnahmsweise auch noch nach Beendigung der vertraglichen Beziehung zulässig ist, soweit diese Daten benötigt werden, um „sonstige gesetzliche Verpflichtungen" zu erfüllen. Auch wenn dies nahe legt, dass der Gesetzgeber dabei an die Übermittlung von Stammdaten zu anderen Zwecken als der Besorgung eines Kommunikationsdienstes gedacht haben mag, beseitigt dies nicht die erwähnte Antinomie.

Welche Konsequenzen lassen sich aus dieser Erkenntnis ziehen? Liegt eine unaufgelöste Antinomie vor, die eine Gesetzeslücke hinterlässt und daher mithilfe der natürlichen Rechtsgrundsätze zu lösen ist[243]? Dieses Ergebnis würde von der Praxis wohl nie akzeptiert werden. Näher liegt es daher, die auftretenden Widersprüchlichkeiten

---

[240] Dieses Ergebnis wird von den meisten freilich übersehen und § 96 Abs 2 TKG 2003 als „Grundregel" bezeichnet, vgl etwa *Parschalk/Otto/Weber/Zuser,* Telekommunikationsrecht (2006) 216; *Klingenbrunner/Bresich,* Telekommunikationsunternehmen: Beschränkter Rechtsschutz gegen Polizeihandeln, ecolex 2008, 475 (476).

[241] 40 RV BlgNR XXII. GP, 44.

[242] OGH 14.7.2009, 4 Ob 41/09x, MR 2009, 251; zT wird der Fall in der Literatur auch unter dem Begriff „Mediasentry" bzw „Vermittler" diskutiert, vgl etwa: *Neubauer,* Zur Haftung und Auskunftsverpflichtung von Providern – Aktuelles zu Unterlassungs- und Auskunftspflichten in Österreich mit einem Vergleich zur aktuellen Rechtslage in Deutschland im Zivil- und Strafrecht, MR-Int 2008, 25 (27); OGH 4 Ob 141/07z, *Vermittler*, MR 2007, 437 (*Walter*).

[243] So etwa *Bydlinski,* Juristische Methodenlehre und Rechtsbegriff (1982) 464.

mithilfe des Satzes „lex posterior derogat legi priori"[244] zu lösen. Somit derogieren jedenfalls alle Auskunftsbestimmungen, die nach 20.8.2003 in Kraft getreten sind, dem § 96 Abs 2 TKG 2003[245].

Offen bleibt aber, was mit Auskunftsbestimmungen wie § 99 Abs 3 FinStrG[246] geschieht. Vor einer gesetzgeberischen Korrektur kann man es mit einem Vorschlag *Larenz*' versuchen, der in bestimmten Fällen die Verdrängung einer Norm auch ohne Spezialitätsverhältnis zulässt, wenn dies der Zeck einer besonderen Norm verlangt[247]. Diese Lösung stößt jedoch freilich bereits an die Grenzen der Nachvollziehbarkeit. In der Praxis werden Bestimmungen wie § 99 Abs 3 FinStrG wohl ungeachtet der gezeigten Schwierigkeiten weiter angewendet werden, da sie meist wie gezeigt ohnedies als „Spezialnorm" betrachtet werden.

Hinsichtlich der §§ 90 Abs 6 und 98 TKG 2003, die (auch) auf die Übermittlung von Stammdaten abzielen, ist überdies auf § 97 leg cit zu verweisen. Nach diesem dürfen Stammdaten „unbeschadet der §§ 90 Abs 6 und 96 Abs 2" für die „Erteilung von Auskünften an Notrufträger" ermittelt und verarbeitet werden. Aus der Formulierung lässt sich einerseits ableiten, dass aus Sicht des Gesetzgebers aus den oben genannten Gründen die durch § 97 erlaubten Datenverarbeitungen prinzipiell im Widerspruch mit den in § 96 Abs 2 leg cit getroffenen Anordnungen stehen. Daher mussten „unbeschadet § 96 Abs 2" bestimmte Datenverarbeitungen von Stammdaten gesondert geregelt werden. Andererseits wird, obwohl diese Bestimmung nur von „ermitteln" und „verarbeiten" spricht, doch die gesetzgeberische Absicht, Übermittlungen von Stammdaten in den Fällen der §§ 90 Abs 6 und 98 leg cit für zulässig zu erklären, überdeutlich. Die Erteilung von Auskünften an Notrufträger ist nur dann möglich, wenn auch Daten übermittelt werden dürfen und nicht nur – wie dies dem Wortlaut nach der Fall wäre – nur „ermittelt" und „verarbeitet" werden dürfen. Ebenso ist davon auszugehen, dass der Gesetzgeber § 90 Abs 6 TKG 2003 wie auch sonstige Auskunftspflichten unzutreffenderweise für Spezialfälle hält, in denen eine Übermittlung ausnahmsweise zulässig ist. Auch die Praxis hat das hier dargestellte Problem noch nie erkannt und wendet die Auskunftsbestimmungen an, ohne dem Konflikt mit § 96 Abs 2 TKG 2003 Beachtung zu schenken. Letztlich wird aber eine saubere Lösung nur in einem korrigierenden Eingreifen des Gesetzgebers bestehen können.

---

[244] Zu dessen Begründung eingehend *Merkl,* Die Rechteinheit des österreichischen Staates. Eine staatsrechtliche Untersuchung auf Grund der Lehre von der lex posterior, Archiv für öffentliches Recht 1918, 56ff.

[245] Der Grundsatz „ lex posterior derogat legi priori" ist auch in der Judikatur anerkannt, vgl etwa OGH 04.10.1994, 4 Ob 88/94, SZ 67/160.

[246] Diese Bestimmung trat am 26.6.2002 in Kraft und wurde seitdem nicht verändert.

[247] *Larenz,* Methodenlehre der Rechtswissenschaft[5] (1983) 258.

4.5.5. Information gem 96 Abs 3 TKG 2003

Besonders hervorzuheben ist die Informationsbestimmung gem § 96 Abs 3 TKG 2003, deren Verletzung verwaltungsstrafrechtlich sanktioniert ist (§ 109 Abs 3 Z 16 TKG 2003). Sie lässt sich, wie noch zu zeigen sein wird, auch für die Entwicklung vertraglicher Schutzpflichten nutzbar machen.

Der Anbieter ist verpflichtet, den Teilnehmer oder Benutzer darüber zu informieren, welche personenbezogenen Daten er ermitteln, verarbeiten und übermitteln wird, auf welcher Rechtsgrundlage und für welche Zwecke dies erfolgt und für wie lange die Daten gespeichert werden. Die Daten dürfen nur für die bekannt gegebenen Zwecke verwendet werden. Dies ergibt schon aus dem Prinzip der Zweckbindung gem § 6 Abs 1 Z 2 DSG 2000[248]. Dabei ist auf die oben dargestellten Beschränkungen der Privatautonomie hinzuweisen. Aus § 96 Abs 1 und 2 TKG 2003 ergibt sich, dass bestimmte Datenverwendungen unabhängig vom Parteiwillen unzulässig sind. Der Benutzer hat auch auf das Recht die Verarbeitung zu verweigern und ist darauf auch hinzuweisen. Technisch nötige kurze Zwischenspeicherungen und Verarbeitungen zum Zweck eines vom Benutzer ausdrücklich gewünschten Dienstes sind auch ohne Zustimmung zulässig. Die Informationspflicht nach § 96 Abs 3 TKG 2003 ist spätestens bei Aufnahme der Rechtsbeziehung zu erfüllen.

Inwieweit die Informationsverpflichtung gegenüber einem bloß faktischen Benutzer erfüllt werden soll, ist unklar. Der Access-Provider, der zum rein faktischen Nutzer seiner Kommunikationsdienste in keiner vertraglichen Beziehung steht, kann technisch unmöglich nachvollziehen, wann sein Vertragspartner und wann ein bloß faktischer Nutzer seine Kommunikationsdienste in Anspruch nimmt. Daher wird es ihm auch schwer fallen, seinen Informationspflichten aus § 96 Abs 3 TKG 2003 nachzukommen. Die Materialien schweigen sich zu diesem Thema aus. Man wird das Gesetz wohl so verstehen müssen, dass eine Information etwa im Rahmen der AGB grundsätzlich immer als ausreichend zu betrachten ist. Nur wenn der Access-Provider aufgrund besonderer Umstände ausnahmsweise davon Kenntnis erlangt, dass jemand anderer als sein Vertragspartner seine Kommunikationsdienste nützt, hat er diesen nochmals gesondert zu informieren.

Fraglich ist das Verhältnis zur Informationspflicht gem § 24 Abs 2 DSG 2000, insbesondere ob auch die erweiterte Informationspflicht gem Abs 2 leg cit besteht, wenn Treu und Glauben dies erfordern. Diese Informationspflicht darf keinesfalls nach

---

[248] Vgl auch *Damjanovic/Holoubek/Kassai/Lehofer/Urbanitsch,* Handbuch des Telekommunikationsrechts (2006) 247.

Ermittlung der Daten erfüllt werden[249]. Der letzte Satz in § 96 Abs 3 TKG 2003 bestimmt, dass das Auskunftsrecht nach dem DSG 2000 von dieser Bestimmung unberührt bleibt. Dies führt zur Frage, ob nun daraus geschlossen werden kann, dass dies für die Informationspflicht nach dem DSG nicht gilt. Dies wäre mE verfehlt, da schon der Hinweis, dass das Auskunftsrecht gem § 26 DSG unberührt bleibt, wegen § 92 Abs 1 TKG 2003 überflüssig ist. Nach letzterer Bestimmung sind ohnedies auf alle im TKG geregelten Sachverhalte, wenn nichts anderes bestimmt wird, auch die Vorschriften des DSG 2000 anzuwenden. Die Bestimmung, dass das Auskunftsrecht unberührt bleibt, ist damit redundant und trägt damit zu unnötiger Verwirrung bei. Hinsichtlich der Informationspflichten könnte jedoch vertreten werden, dass § 96 Abs 3 TKG 2003 etwas „anderes bestimmt" als § 24 DSG 2000 und daher die letztere Bestimmung gem § 92 Abs 1 TKG 2003 unangewendet zu bleiben hat. § 96 Abs 3 TKG 2003 enthält zum Teil andere Informationspflichten als § 24 DSG 2000. Allerdings ordnen die §§ 24 DSG 2000 und 96 Abs 3 TKG 2003 keine unvereinbaren Rechtsfolgen an. Die wichtigsten Informationspflichten decken sich sogar. Daneben ordnet das TKG Informationspflichten an, die im DSG nicht ausdrücklich genannt werden (zB Speicherdauer) und umgekehrt (für die Verarbeitung nach „Treu und Glauben" nötige Informationspflichten gem § 24 Abs 2 DSG 2000). Somit ist davon auszugehen, dass sich diese beiden Bestimmungen ergänzen und sämtliche dort normierten Informationspflichten beachtlich sind.

Klärungsbedürftig ist auch die Frage, ob aus § 96 Abs 3, 1. Satz, TKG 2003 eine Verpflichtung des Anbieters abgeleitet werden kann, Teilnehmer oder Nutzer über die in Erfüllung gesetzlicher Auskunftsansprüche bevorstehende Übermittlung personenbezogener Daten zu informieren. Nach dem Wortlaut der Bestimmung wäre dies eindeutig der Fall. Für den Bereich der StPO ist auf deren § 138 Abs 3 zu verweisen, aus welchem sich eine Verschwiegenheitspflicht des Anbieters ergibt[250]. Es gibt aber auch Auskunftsbestimmungen, die auf die Normierung einer gesetzlichen Verschwiegenheit verzichten. So enthalten etwa weder das SPG[251], das MBG[252], das UWG[253] noch das FinStrG[254] ein an den Access-Provider gerichtetes Verbot, den Nutzer bzw Teilnehmer über Datenermittlungen in Kenntnis zu setzen. Die §§ 91d Abs 3 SPG bzw 57 Abs 6 MBG enthalten lediglich an die Rechtsschutzbeauftragten gerichtete Verbote. Sie bestimmen

---

249 *Dohr/Weiss/Pollirer,* DSG 2000[2], 9. ErgLf. (2002) § 24 Anm 3.

250 Vgl dazu *Reindl-Krauskopf, Fuchs/Ratz* (Hrsg), Wiener Kommentar zur Strafprozessordnung (2009) § 138 Rz 16.

251 § 53 Abs 3a und 3b SPG, BGBl 566/1991 idF BGBl I Nr. 114/2007.

252 § 22 MBG, BGBl I 87/2000 idF BGBl I 85/2009.

253 § 14a UWG, BGBl 448/1984 idF BGBl I 79/2007.

254 § 99 FinStrG, BGBl 129/1985 idF BGBl I 161/2005.

im Wesentlichen, dass eine Information des Betroffenen dann nicht stattfinden darf, wenn bestimmte höherrangige Interessen das Unterbleiben der Information rechtfertigen (vgl § 26 Abs 2 DSG 2000). Da der Gesetzgeber bei diesen Bestimmungen im Gegensatz zur StPO auf eine Verschwiegenheitsverpflichtung des Access-Providers verzichtete, liegt die Annahme einer bewussten gesetzgeberischen Entscheidung nahe.

Mangels spezieller Verschwiegenheitsverbote müsste daher die in § 96 Abs 3 TKG 2003 ausdrücklich normierte Informationspflicht zum Tragen kommen. Dem steht auch § 26 Abs 2 DSG 2000 nicht entgegen, da dieser nur die vom Betroffenen begehrte Auskunft in bestimmten Fällen ausschließt. Überdies sind die Bestimmungen des TKG gegenüber jenen des DSG leges speciales. Daraus folgt, dass der Access-Provider eigentlich den Nutzer oder Teilnehmer darüber zu informieren hätte, bevor er etwa einem Auskunftsersuchen gem § 53 Abs 3a SPG nachkommt. § 96 Abs 3, 2. Satz bestimmt zwar, dass auch über ein allfälliges Recht, die Übermittlung zu verweigern, zu informieren ist, sodass davon ausgehen kann, dass der Gesetzgeber auch Datenverwendungen vor Augen hatte, die der Kunde verweigern kann. Damit können freilich nicht Bestimmungen wie jene des SPG oder MBG gemeint sein, in welchen dem Kunden kein Weigerungsrecht zusteht. Die Pflicht zur Information besteht in meinen Fällen nur dort, wo auch tatsächlich ein Weigerungsrecht besteht.

Anders sieht das der Bundesminister für Inneres in der Beantwortung einer parlamentarischen Anfrage zur „Datenabfrage durch die Sicherheitsbehörden bei Internet- und Telefoniebetreibern gemäß §§ 53ff SPG“[255]. Die Abgeordneten wollten wissen, auf welche Weise die Betroffenen über Auskunftsverlangen nach dem SPG informiert werden (Frage 9), ob der BMI davon ausgehe, dass die Provider zu einer Information verpflichtet seien (Frage 10) oder dazu zumindest berechtigt (Frage 11) seien bzw welche Rechtsgrundlage ein Informationsverbot hätte (Frage 12)[256]. Dass die Sicherheitsbehörde seiner Ansicht nach auch keine nachträgliche Informationspflicht treffe, stützte der BM auf § 24 Abs 3 Z 1 DSG 2000. Nach dieser Bestimmung kann eine Informationsverpflichtung gem Abs 1 leg cit dann entfallen, wenn die Datenverwendung durch Gesetz oder Verordnung vorgesehen ist. Die Fragen 10-12 wurden pauschal damit beantwortet, dass sich eine Informationsverpflichtung der Provider weder aus dem DSG 2000 noch aus dem TKG 2003 ergebe, insbesondere da kein Widerspruchsrecht gegen allfällige Übermittlungen gemäß § 28 DSG 2000 bestehe. Die Frage, ob die Provider zu einer Information wenigstens berechtigt seien, blieb gänzlich unbeantwortet. Aus dieser Anfragebeantwortung ist für die hier relevante Fragestellung nichts zu gewinnen, zumal sie jegliches Eingehen auf § 96 Abs 3, 1. Satz, TKG 2003 vermissen lässt.

---

[255] 4148/AB XXIII. GP, 2.

[256] 4130/J XXIII. GP, 3.

Der geheime Charakter bestimmter Auskunftsbegehren ist meist entscheidend für den Erfolg der Maßnahme[257]. Diese Überlegung trifft auf viele der Auskunftsbestimmungen im SPG, MBG und der StPO gleichermaßen zu. Zum Ausgleich für das Informationsdefizit sehen diese Gesetze das Institut eines Rechtsschutzbeauftragten vor, der die Rechte der Betroffenen kommissarisch wahrnehmen soll. Aus den Materialien zum TKG 2003 ergibt sich, dass durch § 96 TKG 2003[258] die Bestimmungen der EK-Datenschutzrichtlinie umgesetzt werden sollten und die Informationspflicht eine „datenschutzrechtliche Voraussetzung" sei. Der Gesetzgeber denkt dabei wohl vor allem an das Prinzip im DSG 2000, dass Betroffene über Datenverwendungen grundsätzlich immer zu informieren sind (§ 24 DSG 2000). Ein Blick in die EK-Datenschutzrichtlinie legt nahe, dass es dem Gesetzgeber nur darum ging, in § 96 Abs 3 TKG 2003 eine Informationspflicht in Bezug auf jene Datenverwendungen zu normieren, die er im eigenen Interesse vornimmt. Sowohl der 26. Erwägungsgrund als auch Art 5 Abs 3 der EK-Datenschutzrichtlinie betreffen ausschließlich das Verhältnis zwischen dem Access-Provider und dem Teilnehmer. Sowohl dem Gesetz- als auch dem Richtliniengeber ging es offenkundig darum, sicherzustellen, dass die Teilnehmer ausreichend über die sie im Rahmen der Erbringung der Kommunikationsdienste betreffenden Datenverwendungen informiert werden. Darauf deutet auch hin, dass diese Informationen spätestens zum Zeitpunkt der Aufnahme der Rechtsbeziehungen gegeben werden müssen. Noch vor dem Zustandekommen des Vertragsverhältnisses soll der Kunde über alle voraussehbaren und für die im Rahmen der Abwicklung des Vertragsverhältnisses erfolgenden Verwendungen umfassend in Kenntnis gesetzt werden. Dass die Information jedoch nicht immer vor Aufnahme der Rechtsbeziehung zu erteilen ist, ergibt sich aber daraus, dass die Information nach dem Gesetz auch Nutzern zu erteilen ist, die zum Access-Provider in keinerlei vertraglicher Beziehung stehen.

Die Formulierung, dass darüber zu informieren ist, welche Daten der Anbieter übermitteln „wird", lässt den Schluss zu, dass der Gesetzgeber dabei keine Übermittlungen, die in Erfüllung eines gesetzlich verankerten Auskunftsanspruches erfolgen, vor Augen hatte. Es wird nicht verlangt, dass er angeben müsste, welche Daten er übermitteln könnte, sondern welche er (definitiv) übermitteln wird. Darüber kann der Anbieter jedoch zum Zeitpunkt der Aufnahme der Rechtsbeziehungen noch keine konkreten Angaben machen. Ungeachtet dieses historischen Arguments lässt der Wortlaut der Bestimmung auch eine Deutung zu, wonach der Access-Provider stets vor der Übermittlung von Daten – etwa an Urheber – zu informieren hat. Dies würde dann

---

[257] *Machacek,* Der Rechtsschutzbeauftragte nach der StPO: Weisungsfreier Sachwalter des Rechtsschutzes oder weisungsgebunden eine Horrorvision, AnwBl 2004, 90 (90).

[258] 128 BlgNR XXII. GP, 18.

zwar nach Aufnahme der Rechtsbeziehungen geschehen, was prima facie nicht mit der Bestimmung konform geht, dass die Information spätestens bei Beginn der Rechtsbeziehung zu erfolgen hat. Da diese Bestimmung jedoch wie oben gezeigt auch in anderen Fällen – nämlich bei der Information an sonstige Nutzer – unmöglich eingehalten werden kann, ist diesem Widerspruch keine Bedeutung beizumessen.

Andererseits hat die Informationspflicht ähnlich wie § 24 DSG 2000 den Zweck, den Nutzer bzw Teilnehmer umfassend über die ihn betreffenden Datenverwendungen in Kenntnis zu setzen. Dadurch soll er in die Lage versetzt werden, effizient seine Rechte wahrzunehmen. Deshalb ist er auch darüber zu informieren, dass er die Verarbeitung personenbezogener Daten verweigern kann. So gesehen fordert der telos sogar die bisher – soweit ersichtlich – nie ernsthaft diskutierte Auslegung, nach welcher auch bei gesetzlich vorgesehenen Datenübermittlungen die Informationspflicht gemäß § 96 Abs 3 TKG 2003 greift.

Dies gilt nur, soweit nicht die Zwecke bestimmter Auskunftsbestimmungen die Geheimhaltung einer bestimmten Maßnahme erfordern. Diesfalls ist die Bestimmung des § 96 Abs 3 TKG 2003 daher mE im Ergebnis teleologisch zu reduzieren[259] und keine Auskunft zu erteilen. In diesen Fällen ergibt sich aus dem Sinn der Auskunftsbestimmungen, dass die Informationspflicht hier nicht bestehen darf. Eine Information im Nachhinein kann sich gleichfalls nicht aus § 96 Abs 3 TKG 2003 ergeben, da nach dem Wortlaut nur über Übermittlungen zu informieren ist, die künftig erfolgen werden.

Jene Auskunftsbestimmungen (etwa § 87b Abs 3 UrhG), deren Zweck jedoch keine Geheimhaltung verlangt, fordern diese teleologische Reduktion nicht. § 87b Abs 3 UrhG will dem in seinen Rechten Verletzten einen Auskunftsanspruch geben, der diesen in die Lage versetzt, seine Rechte gerichtlich durchzusetzen[260]. Dieser Zweck wird jedoch durch eine Information des Betroffenen darüber, dass seine Identität gegenüber einem Dritten offen gelegt werden wird, nicht konterkariert. In solchen Fällen, in denen der Zweck der Auskunftsbestimmung keine Geheimhaltung erfordert, erscheint es daher vertretbar, § 96 Abs 3 TKG 2003 wörtlich auszulegen und den Betroffenen vor der Übermittlung zu informieren. Diese Auslegung ist jedoch in der Praxis trotz des eindeutigen Wortlauts nicht gebräuchlich.

---

[259] Vgl dazu *Larenz,* Methodenlehre der Rechtswissenschaft[5] (1983) 375ff.

[260] RV 40 BlgNR XXII. GP, 44; vgl etwa *Neubauer*, Zur Haftung und Auskunftsverpflichtung von Providern, MR-Int 2008, 25 (27).

4.5.6. Verpflichtungen hinsichtlich Stammdaten

§ 97 TKG 2003 legt die Zwecke fest, für die eine Verarbeitung und Ermittlung[261] von Stammdaten erfolgen darf. Abs 1 Z 1 und 2 leg cit lassen sich noch mit dem Prinzip in § 96 Abs 2 leg cit[262] Einklang bringen, wonach Daten nur für die Erbringung von Kommunikationsdiensten verarbeitet werden dürfen. Nach Z 3 dürfen Stammdaten aber auch für die Erstellung von Teilnehmerverzeichnissen und nach Z 4 für die Erteilung von Auskünften an Notrufträger verarbeitet werden. Der dadurch entstehende mit § 96 Abs 2 leg cit Konflikt wird durch die Formulierung des § 97 leg cit gelöst (arg „unbeschadet der §§ 90 Abs 6 und 96 Abs 2"). Obwohl das Gesetz nur von „ermitteln" und „verarbeiten" spricht, ist wohl davon auszugehen, dass der Gesetzgeber an dieser Stelle auch das „Übermitteln" für zulässig erklären wollte (siehe dazu schon oben 4.5.4). Ohne Übermittlung personenbezogener Daten kann etwa die in § 98 TKG 2003 normierte Auskunftspflicht gegenüber Betreibern von Notrufdiensten nicht erfüllt werden. Daher meinen die EB auch wörtlich: *„Diese Bestimmung ist geltendes Recht, es wurde ausdrücklich klargestellt, dass diese Daten an Notrufträger übermittelt werden dürfen*."[263] Damit liegen sie zwar falsch, weil der Begriff des „Verarbeitens" eben gerade nicht auch den Begriff des „Übermittelns" erfasst, aber sie lassen den eindeutigen Willen des Gesetzgebers erkennen.

Stammdaten sind gem § 97 Abs 2 TKG 2003 spätestens dann zu löschen, wenn die Rechtsbeziehung zum Teilnehmer beendet wird. Sofern sie jedoch für die in Abs 1 aufgezählten Zwecke nicht mehr benötigt werden, sind sie schon vorher zu löschen (arg „spätestens"). Ausnahmen sind für die Zwecke nachfolgender Verrechnungen und Beschwerdebearbeitungen oder die „Erfüllung sonstiger gesetzlicher Verpflichtungen" möglich. Das kann jedoch nicht bedeuten, dass die Stammdaten ohne konkreten Anlass auf Vorrat zu speichern sind. Gerade dass soll durch diese Bestimmung ja verhindert werden[264]. Müsste der Access-Provider Stammdaten nach Beendigung der Rechtsbeziehung im Hinblick auf eventuelle künftig an ihn gerichtete Auskunftsbegehren speichern, so würde dies im Ergebnis auf eine ewige Speicherpflicht hinauslaufen. Diesfalls müsste der Access-Provider die Daten nämlich solange bereithalten, solange es Gesetze gibt, die Auskunftsansprüche normieren. Die dritte Ausnahme in § 97 Abs 3 TKG 2003 kann also nur so gemeint sein, dass die Stammdaten nur dann nach Beendigung der Vertragsbeziehung weiter aufbewahrt werden müssen, wenn zu diesem Zeitpunkt

---

[261] Zur Kritik an dieser Formulierung vgl schon oben Kapitel 4.5.3.

[262] *Zanger/Schöll*, Telekommunikationsgesetz[2] (2004) § 97 Rz 9.

[263] RV 128 BlgNR XXII. GP, 18.

[264] *Zanger/Schöll,* Telekommunikationsgesetz[2] (2004) § 97 Rz 2.

bereits ein konkretes Auskunftsbegehren an den Access-Provider herangetragen wurde. Nur zur Erfüllung derartiger gesetzlicher Verpflichtungen dürfen Stammdaten weiter gespeichert werden.

Stammdaten sind daher erst später als Verkehrsdaten zu löschen. Daraus ergibt sich ein niedereres Schutzniveau. Dennoch ist bei der Auskunft über Stammdaten immer zu berücksichtigen, ob auch Verkehrsdaten verarbeitet werden müssen. Dieser Umstand wurde im aktuellen Umsetzungsentwurf zur VDS-Rl erfreulicherweise berücksichtigt[265]. Auf den Zusammenhang zwischen den Datenkategorien und die sich für das Schutzniveau daraus ergebenden Konsequenzen wurde bereits oben (vgl Kapitel 4.4.6) ausführlich eingegangen.

4.5.7. Verpflichtungen hinsichtlich Verkehrsdaten

Der besondere Schutz von Verkehrsdaten wird in § 99 TKG 2003 in enger Anlehnung an die Vorgaben der EK-Datenschutzrichtlinie (vgl Art 6) normiert. In Ergänzung zu § 96 Abs 1 TKG 2003 bestimmt § 99 Abs 1 leg cit, dass Verkehrsdaten außer in den gesetzlich geregelten Fällen nicht gespeichert werden dürfen und vom Betreiber nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren sind. Diese Bestimmung lässt demnach selbst Raum für Sonderbestimmungen zu, nach welchen Verkehrsdaten ausnahmsweise auch für andere Zwecke als die Erbringung von Kommunikationsdiensten gespeichert werden dürfen. Ansonsten gilt aber der Grundsatz, dass Daten nur soweit verarbeitet werden dürfen, als dies für die Erbringung von Kommunikationsdiensten erforderlich ist. Da die Verarbeitung von Verkehrsdaten regelmäßig nur bis zum Ende der Verbindung erforderlich ist, sind Verkehrsdaten danach grundsätzlich unverzüglich zu löschen. Abs 4 leg cit enthält noch eine Ausnahme hinsichtlich der Verarbeitung zu Marketingzwecken oder zur Bereitstellung von Diensten mit Zusatznutzen.

Abs 2 leg cit verpflichtet[266] überdies dazu, Verkehrsdaten zum Zwecke der Verrechnung von Entgelten zu speichern. Die Speicherdauer entspricht der Frist, binnen derer die Rechung rechtlich angefochten werden kann und damit in der Regel der privatautonomen Vereinbarung. Branchenüblich ist meist eine Einspruchsfrist von vier bis sechs Wochen[267]. Die Daten sind im Streitfall der entscheidenden Einrichtung sowie der

---

[265] EB ME 117 BlgNR XXIV. GP 17.

[266] Die EK-Datenschutzrichtlinie enthält diesbezüglich hingegen eine bloße Berechtigung.

[267] Die Angaben beziehen sich auf die AGB der größten Kommunikationsdienstebetreiber (Stand April 2009): Telekom Austria/mobilkom austria: sechs Wochen, T-Mobile/Telering: vier Wochen, Orange: vier Wochen, Hutchison 3g: vier Wochen, UPC-Telekabel: vier Wochen.

Schlichtungsstelle unverkürzt zur Verfügung zu stellen. Wird ein Verfahren über die Höhe der Entgelte eingeleitet, dürfen die Daten bis zur endgültigen Entscheidung über die Höhe der Entgelte nicht gelöscht werden. Aus dem letzten Satz in Abs 2 leg cit, wonach die Speicherung auf das unbedingt nötige Minimum beschränkt werden muss, ergibt sich, dass auch zu Verrechnungszwecken nur soweit gespeichert werden darf, als dies bei der Verrechnung und zum Beweis dafür, dass die verrechneten Verbindungen tatsächlich stattfanden, unbedingt erforderlich ist. Für die Speicherung von IP-Adressen, die wie erwähnt immer (auch) Zugangs- bzw Verkehrsdaten sind, bedeutet dies, dass diese nur im Falle von zeit- bzw volumenabhängigen Verrechnungen zu speichern sind. Bei flatrate-Tarifen hingegen ist eine Speicherung zu Verrechnungszwecken nicht nötig[268]. Werden die Daten nicht gelöscht, obwohl die Verbindungen bereits beendet sind und sie für die Verrechnung nicht mehr erforderlich sind, liegt eine Verletzung der §§ 93 Abs 1 und 99 Abs 1 TKG 2003 vor[269].

Somit lassen sich zusammenfassend folgende Ausnahmefälle, in welchen Verkehrsdaten ausnahmsweise auch nach Verbindungsbeendigung verarbeitet werden dürfen, zusammenfassen:

- Speicherung zu Verrechnungszwecken (Art 6 Abs 2 EK-Datenschutzrichtlinie; Umsetzung in § 99 Abs 2 TKG 2003) für die Dauer, binnen derer die Rechnung angefochten werden kann.
- Verarbeitung zu Vermarktungszwecken oder zur Bereitstellung von Diensten mit Zusatznutzen mit Einwilligung des Teilnehmers (Art 6 Abs 3 EK-Datenschutzrichtlinie; Umsetzung in § 99 Abs 4 TKG 2003)
- Speicherung in Umsetzung der Vorratsdatenspeicherungsrichtlinie (Rl 2006/24/EG sowie Art 15 Abs 1a EK-Datenschutzrichtlinie idF ABl L 2006/105 , 54; Umsetzung in Ö bis dato nicht erfolgt)
- Speicherung aufgrund besonderer gesetzlicher Vorschriften, sofern diese gem Art 13 der allgemeinen Datenschutzrichtlinie für die nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen

---

[268] *Jahnel,* Datenschutz im Internet, ecolex 2001, 84 (89); *Pracher*, Datenschutz in der Telekommunikation, in *Forgó/Feldner* et al (Hrsg), Probleme des Informationsrechts (2003) 351 (359ff); *Wiebe,* Auskunftsverpflichtung der Access-Provider – Verpflichtung zur Drittauskunft bei Urheberrechtsverletzungen von Kunden, die an illegalem File-Sharing teilnehmen, MR 2005, H 4 Beilage, 12.

[269] DSK 29.09.2006, K 213.000/0005-DSK/2006.

Gesellschaft notwendig, angemessen und verhältnismäßig ist (Art 15 Abs 1 EK-Datenschutzrichtlinie; Umsetzung in § 99 Abs 1 TKG 2003).

Dieser Katalog an Ausnahmen ist taxativer Natur. Dies ergibt sich aus der Konstruktion einer grundsätzlich umfassenden Löschungsverpflichtung. Ausnahmen sind daher nur dort zulässig, wo sie ausdrücklich normiert wurden. Nach Beendigung der Verbindung ist eine weitere Verarbeitung von Verkehrsdaten durch den Access-Provider daher nur zulässig, wenn er sich auf eine der vier oben genannten Ausnahmen stützen kann.

4.5.7.1. Speicherpflicht zur Erfüllung von Auskunftspflichten?

Anlass zur Diskussion gab in der Vergangenheit die Wendung *„außer in den gesetzlich besonders geregelten Fällen*" in Abs 1 leg cit. Diese Wendung entspricht den Regelungen in Art 6 Abs 1 und Art 15 Abs 1 der EK-Datenschutzrichtlinie. Während ersterer ein grundsätzliches Löschungsgebot für alle Verkehrsdaten aufstellt, lässt letzterer Ausnahmebestimmungen dann zu, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der allgemeinen Datenschutzrichtlinie *„für die nationale Sicherheit, (dh die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist*".

Es wurde vertreten, dass Auskunftspflichten wie etwa jene gem § 87b Abs 3 UrhG solche gesetzlichen Sonderbestimmungen seien, die implizite Speicheranordnungen enthalten[270]. Dies ist jedoch unzutreffend. Eine derartige Sonderbestimmung muss so beschaffen sein, dass sie die Speicherung von Verkehrsdaten ausdrücklich vorschreibt. Nur dann kann von einem im Verhältnis zum allgemeinen Speicherverbot „gesetzlich besonders geregelten Fall" die Rede sein. Auch der zweite Satz des Art 15 Abs 1 der EK-Datenschutzrichtlinie legt diesen Schluss nahe. Er bestimmt, dass Rechtsvorschriften erlassen werden dürfen, wonach Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden dürfen. Eine Vorschrift, die eine Auskunftspflicht normiert, die nur aufgrund der Verarbeitung von Verkehrsdaten erfüllt werden kann, ist keine solche Vorschrift.

Erfreulicherweise hat sich auch der OGH dieser Auffassung angeschlossen und klargestellt, dass aus einem bloßen materiellrechtlichen Anspruch keine

---

[270] *Schachter* in *Kucsko* (Hrsg), Urheber.recht : systematischer Kommentar zum Urheberrechtsgesetz (2008) §87b 3.4.; *Schanda*, Auskunftspflicht über Inhaber dynamischer IP-Adressen contra Verpflichtung zur Löschung von Verkehrsdaten, MR 2007, 213 (215), *ders,* Auskunftsanspruch gegen Access-Provider über die IP-Adressen von Urheberrechtsverletzern, MR 2005 18 (20); OLG 12. 4. 2007, 5 R 193/06y.

Speicherverpflichtung abgeleitet werden kann und damit der oben dargestellten Gegenauffassung eine ausdrückliche Absage erteilt[271]. Zusätzlich zu den obigen Argumenten verweist der OGH auch darauf, dass sich aus einer Auskunftspflicht wie § 87b Abs 3 UrhG aufgrund der Verjährungsvorschriften eine 30-jährige Speicherpflicht ergeben würde, wenn man solchen Vorschriften unterstellen würde, dass sie implizite Speicherverpflichtungen enthalten. Dass dies nicht im Sinne eines auf europäischer Ebene intendierten Datenschutzes sein kann, ergebe sich zum einen schon aus Art 15 der EK-Datenschutzrichtlinie, der ausnahmsweise Speicherverpflichtungen nur für „eine begrenzte Zeit" zulasse. Zudem sei sogar die Speicherdauer hinsichtlich Verkehrsdaten in der Vorratsdatenspeicherungsrichtlinie mit maximal zwei Jahren limitiert.

Ohne auf den in diesem Punkt in der Literatur bestehenden Diskurs einzugehen, entschied auch der VfGH kürzlich, dass aus einer Auskunftsbestimmung wie § 53 Abs 3a SPG keine Speicherverpflichtung abgeleitet werden könne. Mit der Novellierung[272] dieser angefochtenen Bestimmung sei zwar eine gesetzliche Grundlage für die Übermittlung der IP-Adresse an die Sicherheitsbehörden, aber keine neue Verpflichtung zur Speicherung von IP-Adressen geschaffen worden. Das SPG enthalte keine zusätzliche Speicherverpflichtung, wie sie in § 99 Abs 1 TKG 2003 ermöglicht würde[273].

Da die Rechtsprechung dieser beiden Höchstgerichte in diesem Punkt identisch und gut begründet ist, dürfte sich die dargestellte Gegenauffassung wohl nicht mehr durchsetzen.

4.5.7.2. Auswirkungen der Umsetzung der Vorratsdatenspeicherungsrichtlinie

Fraglich ist, ob sich durch die Umsetzung der Vorratsdatenspeicherungsrichtlinie in Österreich an der oben geschilderten Rechtslage etwas ändern wird[274]. Nach Art 3 der Vorratsdatenspeicherungsrichtlinie sind eine Reihe von Verkehrsdaten (vgl Art 5) für eine Dauer von sechs Monaten bis zu zwei Jahren (vgl Art 5) auf Vorrat zu speichern. Unter diesen Vorratsdaten befinden sich auch IP-Adressen. Die Umsetzung der Richtlinie in österreichisches Recht könnte somit jene gesetzliche Speicherpflicht mit sich bringen, deren Fehlen wie oben beschrieben manche Auskunftsansprüche bislang oft de facto scheitern ließ.

---

[271] OGH 14.7.09, 4 Ob 41/09x, MR 2009, 251.

[272] BGBl I 114/2007.

[273] VfGH 1.7.2009, G 31/08.

[274] Vgl dazu auch *Raschhofer*, Der urheberrechtliche Auskunftsanspruch gem § 87b Abs 3 UrhG gegen Access-Provider in *Feiler/Raschhofer*, Innovation und internationale Rechtspraxis, Festschrift für Wolfgang Zankl (2009) 661 (673).

Der vom BMVIT im Jahr 2007[275] ausgearbeitete Umsetzungsentwurf ist mittlerweile als obsolet zu betrachten, da bereits ein neuer vom Ludwig Boltzmann Institut für Menschenrechte erarbeiteter aktueller Entwurf zur Umsetzung der VDS-RI[276] samt EB[277] vorliegt. Beide Entwürfe enthalten einen neu einzufügenden § 102a TKG, der jeweils normiert, dass Vorratsdaten nur für ganz bestimmte Zwecke[278] gespeichert werden dürfen. Dies entspricht der Vorratsdatenspeicherungsrichtlinie, deren Art 1 bestimmt, dass die Mitgliedstaaten sicherzustellen haben, dass *„die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Staat in seinem nationalen Recht bestimmt werden, zur Verfügung stehen.*"

Die Definition der „schweren Straftaten" ist zwar den Mitgliedstaaten überlassen, jedoch ist diesbezüglich in Österreich auch auf die doppelte Normbindung zu verweisen. Innerhalb jenes Spielraumes, den das Gemeinschaftsrecht den Mitgliedstaaten bei der Umsetzung belässt, sind auch die durch die österreichische Bundesverfassung gezogenen Grenzen besonders zu beachten. Das bedeutet, dass bei der Definition „schwerer Straftaten" insbesondere auch die Grundrechte gem Art 8 EMRK, 1 DSG 2000, 2 StGG bzw 7 B-VG zu beachten sind.

Dies legt von vornherein die Deutung nahe, dass Vorratsdaten nicht für die Erfüllung von Auskunftsbegehren verwendet werden dürfen, die außerhalb der StPO – etwa im UrhG – geregelt sind. Auskunftsbegehren, die nur der Durchsetzung zivilrechtlicher Ansprüche dienen (vgl etwa §§ 14a UWG, 87b Abs 3 UrhG), dürfen daher überhaupt nicht zur Verarbeitung von Vorratsdaten führen. Die Definition der „schweren Straftaten" liegt im Ermessen der Mitgliedstaaten. Bereits der erste Entwurf definierte die schweren Straftaten in einer Weise, sodass bestimmte gesetzliche Auskunftsbegehren wie etwa § 90 Abs 6 TKG oder § 87b Abs 3 UrhG nicht durch Verarbeitung von Vorratsdaten hätten erfüllt werden dürfen.

Der aktuelle Umsetzungsentwurf zur VDS-Rl ist sich der hier erörterten Problematik anders als der alte Entwurf in besonderem Maße bewusst und daher von dem Gedanken getragen, die Verarbeitung von Vorratsdaten auf die Zwecke zu beschränken, deretwegen sie gespeichert wurden. Zunächst sieht der aktuelle Umsetzungsentwurf zur VDS-Rl vor, dass § 99 Abs 1 TKG neu Verkehrsdaten *„außer in*

---

[275] ME 61 BlgNR XXIII. GP.

[276] ME 117 BlgNR XXIV. GP.

[277] EB ME 117 BlgNR XXIV. GP

[278] Im alten Entwurf heißt es, dass die Daten „nur zum Zwecke der Ermittlung, Feststellung und Verfolgung von mit beträchtlicher Strafe bedrohten Handlungen (§ 17 SPG) einschließlich der Tatbestände der §§ 107 und 107a StGB zu speichern zu speichern sind", der neue Entwurf sieht vor, dass die Daten „ausschließlich zum Zweck der Ermittlung, Feststellung und Verfolgung schwerer Straftaten" gespeichert werden dürfen.

den in diesem Gesetz geregelten Fällen weder gespeichert noch verwendet" werden dürfen und „*vom Betreiber nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren*" sind. Damit wird im Gesetz ausdrücklich klar gestellt, dass nur das TKG eine Rechtsgrundlage für eine Speicherpflicht sein kann. Die Verarbeitung von Verkehrsdaten zu Auskunftszwecken wird in § 99 Abs 5 neu geregelt:

„Eine Verarbeitung von Verkehrsdaten zu Auskunftszwecken ist nur zulässig

1. *zur Auskunft über Daten einer Nachrichtenübermittlung (§ 134 StPO) an die nach der StPO zur Ermittlung, Feststellung und Verfolgung von Straftaten zuständigen Behörden, wenn eine gerichtliche Bewilligung vorliegt;*
2. *(Verfassungsbestimmung) zur Auskunft über Verkehrsdaten und zur Auskunft über Stammdaten, wenn hierfür die Verarbeitung von Verkehrsdaten erforderlich ist*[279]*, sowie zur Auskunft über Standortdaten an nach dem SPG zuständige Sicherheitsbehörden, wenn diese Auskunft als wesentliche Voraussetzung zur Abwehr einer konkreten Gefahr für das Leben oder die Gesundheit eines Menschen notwendig ist. Ist eine aktuelle Standortfeststellung nicht möglich, darf ausnahmsweise die Standortkennung (Cell-ID) zum letzten Kommunikationsvorgang der Endeinrichtung des gefährdeten Menschen verarbeitet werden, obwohl hierfür ein Zugriff auf gemäß § 102a Abs 3 Z 6 lit d) gespeicherte Vorratsdaten erforderlich ist. Der Anbieter hat den betroffenen Teilnehmer über eine Auskunft über Standortdaten nach dieser Ziffer spätestens mit Ablauf der Rechnungsperiode zu informieren.*

In beiden Fällen hat die gesetzliche Auskunftsermächtigung ausdrücklich auf diesen Absatz zu verweisen, die konkreten Datenkategorien aufzuzählen, die berechtigten Behörden zu benennen und den Datenumfang auf das notwendige und verhältnismäßige Ausmaß zu beschränken. Eine Verpflichtung zur Speicherung von Verkehrsdaten allein aufgrund dieses Absatzes besteht nicht. Eine über die genannte Ausnahme hinausgehende Verarbeitung von Vorratsdaten aufgrund dieses Absatzes ist unzulässig. Auf Auskünfte nach

---

[279] Bemerkenswert ist, dass der Entwurf die Auskunft über Stammdaten der Auskunft über Verkehrsdaten gleichstellt, wenn dafür Verkehrsdaten verarbeitet werden müssen, vgl dazu oben Kapitel 4.4.6 bzw die EB ME 117 BlgNR XXIV. GP 17: *„[...] Darüber hinaus besteht auch dann ein Eingriff in das verfassungsrechtlich geschützte Fernmeldegeheimnis (Art. 10a StGG), wenn Gegenstand der Auskunft zwar bloß Stammdaten sind, diese jedoch durch eine Verarbeitung von Verkehrsdaten auf Seiten des Anbieters ermittelt werden*."

diesem Absatz ist eine gemäß § 94 Abs 2 erlassene Verordnung zur Kostenerstattung anzuwenden.

Z 2 ist als Verfassungsbestimmung konzipiert worden, da sie nach der unzutreffenden Ansicht der Verfasser[280] einen Eingriff in das Fernmeldegeheimnis des Art 10a StGG enthält. Durch die hervorgehobenen Teile der Bestimmung wird klargestellt, dass Vorratsdaten grundsätzlich nur zum Zweck der Ermittlung, Feststellung und Verfolgung schwerer Straftaten zulässig ist (§ 102a neu TKG 2003). Die einzige Ausnahme besteht gem § 99 Abs 5 Z 2 neu TKG 2003 hinsichtlich Standortdaten aus der Vergangenheit[281]. In Ergänzung dazu bestimmt § 102b Abs 1 neu TKG 2003:

„Eine Auskunft über Vorratsdaten darf ausschließlich aufgrund einer gerichtlichen Bewilligung und nur nach Maßgabe einer ausdrücklich auf § 102a verweisenden gesetzlichen Bestimmung erteilt werden. Die Auskunft ist nur zum Zweck der Ermittlung, Feststellung und Verfolgung schwerer Straftaten an die nach den Bestimmungen der StPO über die Auskunft über Daten einer Nachrichtenübermittlung zuständigen Behörden zulässig."

Das bedeutet, dass zur Erfüllung von Auskunftsbegehren, die außerhalb der StPO normiert werden, weiterhin nur jene Daten verarbeitet werden dürfen, die auch bisher schon als Daten zu Verrechnungszwecken gem § 99 Abs 2 TKG 2003 zur Verfügung standen. Sofern Verkehrsdaten ihre Eigenschaft als Billing-Daten verlieren und nur mehr aufgrund der Speicherverpflichtung gem § 102a neu TKG 2003 als Vorratsdaten gespeichert werden, dürfen sie gem § 99 Abs 5 neu iVm § 102a neu TKG 2003 nur mehr für Auskunftsbegehren nach Standortdaten aus der Vergangenheit bzw für die in der StPO geregelten Auskunftsbestimmungen verwendet werden[282]. Die Bestimmung des § 102c TKG 2003, wonach die Speicherung der Vorratsdaten so zu erfolgen hat, „*dass eine Unterscheidung von nach Maßgabe der §§ 96, 97, 99, 101 und 102 gespeicherten Daten möglich ist*" dient der Identifizierbarkeit von Vorratsdaten und ergänzt somit die erwähnten Bestimmungen.

Sollte die VDS-Rl daher so umgesetzt werden, wie dies der aktuelle Entwurf vorsieht, wird sich die Position all jener, die sich auf Auskunftsbestimmungen außerhalb der StPO stützen, nicht verbessern, da ihnen der Zugriff auf die künftig zu speichernden Vorratsdaten verwehrt bleiben wird.

---

[280] Vgl oben Kapitel 4.4.

[281] Vgl zu dieser Problematik *Raschhofer* in *Zankl* (Hrsg), Auf dem weg zum Überwachungsstaat? (2009) 98ff.

[282] EB ME 117 BlgNR XXIV. GP 17.

4.5.8. Verpflichtungen hinsichtlich Standortdaten

Da die StPO und das SPG (§ 135 Abs 2 StPO, § 53 Abs 3b SPG) Fälle regeln, in denen den Behörden der Zugriff auf die Standortdaten mobiler Endgeräte ermöglicht werden soll, müssen auch die Verpflichtungen des Access-Providers hinsichtlich Standortdaten untersucht werden. Standortdaten, die den geografischen Standort eines mobilen Endgerätes eines Nutzers angeben, werden meist zur Erbringung eines Kommunikationsdienstes benötigt. Positionsdaten werden bei jedem Verbindungsaufbau mit übertragen und im Switch verarbeitet[283]. Dieser Teil der Standortdaten fällt daher auch unter den Begriff der Verkehrsdaten[284], da sie zur Weiterleitung einer Nachricht in einem Kommunikationsnetz benötigt werden. Dies unterstreicht der aktuelle Umsetzungsentwurf zur VDS-Rl, der in § 99 Abs 5 Z 2 TKG 2003 unter der Überschrift „Verarbeitung von Verkehrsdaten" auch die Übermittlung von Standortdaten regelt. Soweit unterliegen sie den Bestimmungen der §§ 93, 96, 98 und 99 TKG 2003. Sie dürfen daher nach Verbindungsbeendigung nur noch zu Verrechnungszwecken gespeichert werden. Da der Standort für das vom Nutzer zu entrichtende Entgelt regelmäßig ohne Belang ist, sind kaum Fälle denkbar, in denen Standortdaten gespeichert werden dürfen[285]. Selbst im Falle von Roaming ist fraglich, ob die Standortdaten tatsächlich zu Verrechnungszwecken gespeichert werden müssen. In diesen Fällen ist der Anbieter mit Forderungen des Betreibers jenes Kommunikationsnetzes konfrontiert, in welchem geroamt wurde. Diese Forderungen in Verbindung mit den vom Roaming-Netzbetreiber gespeicherten Verkehrsdaten dürften zum Nachweis des Zustandekommens der Roaming-Verbindungen ausreichen. Die EB zum aktuellen Umsetzungsentwurf zur VDS-Rl gehen davon aus, dass Standortdaten aus der Vergangenheit stets nur Vorratsdaten, dh niemals Billing-Daten sein können[286].

Andere Standortdaten, die nicht der Weiterleitung von Nachrichten innerhalb eines Kommunikationsnetzes dienen, unterliegen der besonderen Bestimmung gemäß § 102 TKG 2003. Dabei handelt es sich etwa um die exakten GPS-Daten des Nutzers. Für die Weiterleitung von Nachrichten ist lediglich die Kenntnis des Access-Providers darüber erforderlich, in welcher Funkzelle sich der Nutzer befindet. Die

---

283 *Pracher*, Datenschutz in der Telekommunikation, in *Forgó/Feldner/Witzmann/Dieplinger,* Probleme des Informationsrechts (2003) 352 (356).

284 RV 128 BlgNR XXII. GP, 20; Missverständlich *Pfarl,* Gefunden! LBS im Mobilfunkbereich, ecolex 2005, 569 (570), der meint, dass Standortdaten den geografischen Standort des Endgeräts meist genauer angeben, als dies zur Nachrichtenübermittlung erforderlich wäre. Dabei meint er offenbar nur die in § 102 TKG 2003 geregelte Datenkategorie.

285 Ebenso *Hellmich,* Location Based Services, MMR 2002, 152 (154); *Fallenböck,* Der Einsatz von Location Based Services – eine erste Analyse rechtlicher Problemfelder, MR 2002, 182 (184).

286 EB ME 117 BlgNR XXIV. GP 14.

Verarbeitung exakterer Positionsdaten ist daher für die Erbringung von Kommunikationsdiensten nicht erforderlich. Solche besonderen Standortdaten dürfen gem § 102 TKG 2003 unbeschadet des § 98 TKG 2003 (siehe dazu unten) nur in anonymisierter Form bzw bei Einwilligung des Nutzers verarbeitet werden.

§ 102 TKG 2003 regelt nur die „Verarbeitung" von anderen Standortdaten als Verkehrsdaten. Fraglich ist daher, ob derartige Daten unter den dort genannten Voraussetzungen auch übermittelt werden dürfen. Dies ist im Ergebnis zu bejahen, da durch diese Bestimmung Art 9 der EK-Datenschutzrichtlinie umgesetzt werden sollte[287]. Art 2 leg cit sieht vor, dass, sofern nichts anderes bestimmt wird, die Begriffsbestimmungen der allgemeinen Datenschutzrichtlinie gelten. Art 2 lit b der allgemeinen Datenschutzrichtlinie bestimmt, dass unter der „Verarbeitung personenbezogener Daten" ua „die Übermittlung durch Weitergabe" zu verstehen ist. Der Begriff Verarbeitung iSd Art 2 lit b der allgemeinen Datenschutzrichtlinie entspricht somit dem Begriff des Verwendens gem § 4 Z 8 DSG 2000. Der Begriff „Verarbeiten" in § 102 TKG 2003 kann somit im Sinne von „verwenden" gem § 4 Z 8 DSG 2000 verstanden werden[288]. Dies ergibt sich auch aus § 102 Abs 3 TKG 2003, der die Verarbeitung von Standortdaten durch andere Personen als den Anbieter impliziter voraussetzt.

Willigt der Nutzer ein, dass seine Daten (nicht anonymisiert) verarbeitet werden, so kann er diese Zustimmung jederzeit widerrufen. Die Verarbeitung muss auf das unbedingt erforderliche Mindestmaß beschränkt werden. Diese Einschränkung gilt sowohl für den Anbieter als auch für Dritte, die einen Zusatzdienst anbieten. Die Bestimmung dient vor allem der Regulierung so genannter location based services (LBS)[289].

Da nach den obigen Ausführungen historische Standortdaten von den Anbietern öffentlicher Kommunikationsdienste außer bei informierter Zustimmung des Nutzers so gut wie nie gespeichert werden dürfen, wird die Umsetzung der Vorratsdatenspeicherungsrichtlinie erhebliche Veränderungen mit sich bringen. Gem Art 5 Abs 1 lit f Z 1 sind die Bezeichnung der Funkzelle (Cell-ID) zu Beginn jeder Verbindung und gem Z 2 leg cit die Daten zur geografischen Ortung von Funkzellen zu speichern. Hinsichtlich vorbezahlter anonymer Dienste bestimmt Art 5 Abs 1 lit e Z 2 sublit vi, dass Datum und Uhrzeit der ersten Aktivierung sowie die Cell-ID zu diesem Zeitpunkt gespeichert werden müssen. Dieser Speicherpflichten werden vom aktuellen

---

[287] RV 128 BlgNR XXII. GP, 20.

[288] *Kassai,* Der Einsatz von Location Based Services – eine erste Analyse rechtlicher Problemfelder, MR 2004 (433) (434).

[289] Vgl dazu etwa *Pfarl,* Gefunden! LBS im Mobilfunkbereich, ecolex 2005, 569ff; *Fallenböck,* Der Einsatz von Location Based Services – eine erste Analyse rechtlicher Problemfelder, MR 2002, 182ff; *Hellmich,* Location Based Services, MMR 2002, 152.

Umsetzungsentwurf zur VDS-Rl in § 102a Abs 3 Z 6 lit c und b umgesetzt. In Ergänzung dazu fügt der Entwurf in § 90 TKG 2003 einen neuen Abs 8 ein. Dieser sieht vor, dass Betreiber von Mobilfunknetzen Aufzeichnungen über den geografischen Standort der zum Betrieb ihres Dienstes eingesetzten Funkzellen zu führen haben. Dieser Bestimmung trägt dem Umstand Rechnung, dass sich die Bezeichnungen von Funkzellen bzw der Standort von Funkzellen ändern können. Die Betreiber sollen aber nicht nur in der Lage sein, die Cell-ID bei Verbindungsaufbau zu benennen, sondern diese Information auch mit einem bestimmten geografischen Standort in Verbindung bringen können. Um diese Pflicht erfüllen zu können, sind auch Aufzeichnungen darüber zu führen, wo sich welche Funkzelle wann befand.

Der aktuelle Umsetzungsentwurf zur VDS-Rl ist von dem Gedanken getragen, dass die Vorratsdaten, wurden sie erst einmal angelegt, auch tatsächlich nur für die ursprünglich vorgesehenen Zwecke verwendet werden sollen. Diese Zwecke werden in der Richtlinie dahin gehend definiert, dass die Speicherung nur zur Ermittlung, Feststellung und Verfolgung von „schweren Straftaten" erfolgen soll. Da der aktuelle Entwurf zur VDS-Rl wie erwähnt davon ausgeht, dass Standortdaten ab Verbindungsbeendigung in praxi mangels Verrechnungsrelevanz nur mehr als Vorratsdaten vorkommen, wird deren Verwendung (abgesehen von Fällen der informierten Zustimmung) auch grundsätzlich auf diese Zwecke beschränkt.

Die einzige Ausnahme davon normieren die §§ 98 Abs und 99 Abs 2 Z 5 TKG 2003 des aktuellen Entwurfes zur VDS-Rl. Diese erlauben für den Fall, dass eine aktuelle Standortfeststellung anhand neu generierter Standortdaten nicht möglich ist, dass ausnahmsweise die auf Vorrat gespeicherten Stanortdaten des letzten Kommunikationsvorgangs verarbeitet werden dürfen. Diese Bestimmungen sollen die Ortung von Personen in Notsituationen ermöglichen. Sie sprechen an sich nur von „verarbeiten", was nach der Terminologie des DSG 2000 die „Übermittlung" von Daten ausschließen würde. Dennoch ist davon auszugehen, dass diese Bestimmung gerade auch die Übermittlung von Standortdaten an die Sicherheitsbehörde ermöglichen soll. Obwohl nur der Begriff des „Verwendens" iSd § 4 Z 8 DSG 2000 auch den Begriff des „Übermittelns" iSd § 4 Z 12 leg cit mit einschließt, ergibt sich diese Absicht klar aus den Materialien, aus denen hervorgeht, dass diese Bestimmung vor allem in Ergänzung zu § 53 Abs 3b SPG idF BGBl 114/2007 geschaffen wurde[290]. Daher ist hier eine Auslegung angezeigt, wonach die Stanortdaten aufgrund dieser Bestimmungen übermittelt werden können, auch wenn diese Interpretation mit den Begriffsbestimmungen des DSG 2000 nicht völlig im Einklang stehen mag. Besser wäre es freilich, die Formulierung noch entsprechend anzupassen. Bei der Übermittlung von auf Vorrat gespeicherten

[290] EB ME 117 BlgNR XXIV. GP 17.

Standortdaten handelt es sich nach dem aktuellen Umsetzungsentwurf zur VDS-Rl um den einzigen Fall, in welchem Vorratsdaten ohne gerichtliche Bewilligung verwendet werden dürfen.

4.5.8.1. Information des Betroffenen über die Weitergabe von Standortdaten

Der aktuelle Entwurf zur VDS-Rl sieht vor, dass der Anbieter den betroffenen Teilnehmer über die Erteilung einer Auskunft über Standortdaten nach den §§ 98 bzw 99 Abs 5 Z 2 TKG 2003 spätestens mit Ablauf der Rechnungsperiode zu informieren hat. Dies erscheint mit Blick auf die Art 8 und 13 EMRK sowie § 1 DSG 2000 auch geboten. Die Information entspricht dem für das gesamte Datenschutzrecht fundamentalen Prinzip, dass grundsätzlich jeder über die ihn betreffenden Datenverwendungen in Kenntnis sein soll. Dieses Prinzip wird später bei der Entwicklung vertraglicher Schutzpflichten des Access-Providers (vgl Kapitel 5.5.6) noch als wichtige Grundlage für die im Rahmen der Vertragsergänzung erzielten Ergebnisse dienen. Die Übermittlung von Standortdaten an eine Sicherheitsbehörde bzw den Betreiber eines Notrufdienstes stellt jedenfalls einen Eingriff in das Recht auf Achtung des Privat- und Familienlebens dar. Im Falle *Malone* entschied der EGMR, dass die Weitergabe von Informationen über die angewählten Nummern eines Anschlusses bzw die Dauer und Zeitpunkt der Verbindungen an die Polizei zwar etwas grundlegend anderes sei, als die Ermittlung des Inhalts solcher Gespräche, jedoch nichts desto trotz ein Eingriff in den durch Art 8 EMRK geschützten Bereich vorliege[291]. Verkehrsdaten werden auch in der Literatur dem Schutzbereich des Art 8 EMRK zugeordnet[292]. Zwischen Verkehrs- und Standortdaten besteht in qualitativer Hinsicht kein Unterschied. Wie bereits gezeigt wurde, sind die meisten Standortdaten zugleich auch Verkehrsdaten. Auch aus den Standorten während einer mobil geführten Kommunikation lassen sich Rückschlüsse auf Umstände ziehen, die zum geschützten Privatleben zählen. Auch der VfGH hat zum sachlichen Anwendungsbereich des Art 8 EMRK bereits ausgesprochen, dass in einer von Achtung der Freiheit geprägten Gesellschaft, wie sie die Präambel zur MRK voraussetzt, der Bürger ohne triftigen Grund niemandem Einblick zu gewähren hat „wo er die Nacht verbringt[293]." Der Aufenthaltsort eines Menschen ist daher vom Schutzbereich des Art 8 EMRK umfasst. Ebenso stellt die Information über den Standort eines Menschen ein personenbezogenes Datum dar, weshalb die Weitergabe auch einen Eingriff in § 1 DSG

---

[291] EGMR U 2.8.1984, *Malone*, Nr 8691/79, Rz 84.

[292] *Grabenwarther,* Europäische Menschenrechtskonvention[3] (2008) 207; Berka, Lehrbuch Grundrechte (2000) Rz 297; Wessely, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht? ÖJZ 1999, 491 (495).

[293] VfGH 14.3.1991, G 148-151/90.

2000 darstellt. Steht somit fest, dass die Auskunft über Standortdaten einen Eingriff in den durch Art 8 EMRK bzw § 1 DSG 2000 geschützten Bereich darstellt, muss dem Betroffenen auch die Möglichkeit gegeben werden, sich entsprechend gegen Eingriffe in seine grundrechtliche geschützten Rechtspositionen zu wehren.

Dies ergibt sich zum einen aus dem rechtsstaatlichen Prinzip der österreichischen Bundesverfassung. Dieses verlangt ein System von Rechtsschutzeinrichtungen, die es ermöglichen, Rechtsakte am Maßstab der im Stufenbau der Rechtsordnung höherrangigen Rechtskate zu überprüfen. Der Verfassungsgerichtshof hat in diesem Kontext stets auf *„das Kriterium der faktischen Effektivität eines solchen Rechtsschutzes hingewiesen, das dann verfehlt wird, wenn ein behördliches Fehlverhalten eine dauernde Belastung des Betroffenen bewirkt (vgl insbesondere die Erkenntnisse VfSlg 11 196/1986, 11 590/1987, 12 683/1991, 13 003/1992, 13 182/1992, und 13 805/1994 sowie das Erkenntnis V116/96 vom 26.2.1997). Nach diesen Grundsätzen ist mit Bezug auf geheime Formen der Ermittlung personenbezogener Daten zu fordern, dass der Gesetzgeber solche faktisch wirksamen Rechtsschutzeinrichtungen vorsieht, die gewährleisten, dass schwere Verletzungen der Grundrechte nach Art 8 EMRK und § 1 DSG 2000 festgestellt werden (können). An eine solche Feststellung kann eine Wiedergutmachung, insbesondere nach Maßgabe von Amtshaftungsansprüchen anschließen*[294]*."*

Zum anderen ist in diesem Zusammenhang auch auf Art 13 EMRK zu verweisen, der bestimmt, dass wenn die in der vorliegenden Konvention festgelegten Rechte und Freiheiten verletzt worden sind, der Verletzte das Recht hat Beschwerde bei einer nationalen Instanz einzulegen. Entgegen dem Wortlaut dieser Bestimmung muss nach der aktuellen Rechtsprechung des EGMR für die Geltendmachung des Rechts auf eine wirksame Beschwerde nicht schon eine tatsächliche Verletzung nachgewiesen werden, sondern es reicht eine vertretbare Behauptung einer solchen Verletzung („arguable claim") dazu aus[295]. Eine Beschwerde setzt aber logisch die Kenntnis über eine bestimmte Maßnahme voraus. Übermittelt der Access-Provider aufgrund der §§ 98 bzw 99 Abs 5 Z 2 iVm 53 Abs 3b SPG die Standortdaten des Nutzers, so erlangt dieser davon zunächst keine Kenntnis. Wird der Nutzer in weiterer Folge aufgefunden, kann er womöglich aus den Umständen bzw Informationen durch die Sicherheitsbehörden ableiten, dass er nur aufgrund der Weitergabe seiner Standortdaten gefunden wurde. Wird er aber nicht gefunden oder erfährt er aus anderen Gründen nicht von der Übermittlung der Standortdaten, hat er keine Möglichkeit, die Rechtmäßigkeit der

---

[294] VfGH 23.1.2004 G 363/02, VfSlg 17.102.

[295] *Fowein/Peukert,* EMRK-Kommentar[2] (1996) Art 13 EMRK Rz 2; EGMR U 25.3.1983, *Silver and Others*, 5947/72*,* Rz 113 mwN.

Übermittlung prüfen zu lassen. Dies steht im Widerspruch zu Art 13 EMRK und den oben beschriebenen Anforderungen der faktischen Effizienz des Rechtsschutzes. Der EGMR hat zwar ausgesprochen, dass es in bestimmten Fällen die Natur einer Überwachungsmaßnahme verlange, dass eine Information des Betroffenen zunächst unterbleibt. In diesen Fällen kann auch aus Art 13 EMRK kein Recht auf Information über die Maßnahme abgeleitet werden[296]. Umgekehrt ist der Betroffene jedoch sobald von der Maßnahme zu informieren, sobald es der Zweck zulässt[297]. Sowohl § 53 Abs 3b SPG[298] als auch § 98 TKG 2003[299] sollen die Weitergabe von Standortdaten eines gefährdeten Menschen zur Rettung desselben ermöglichen. Der Zweck dieser Auskunftsbestimmungen erfordert es daher in aller Regel nicht, dass der Betroffene über die Weitergabe seiner Standortdaten im Dunklen bleibt[300]. Ausnahmen können bestehen, soweit etwa eine Person geortet werden soll, die zwar gefährdet ist, aber gleichzeitig auch andere gefährdet (zB Selbstmordattentäter). Eine umgehende Information dieser Person kann wiederum dem Zweck der Maßnahme widersprechen und daher vorübergehend unzulässig sein. Ansonsten ergibt sich aus Art 13 EMRK und aus dem rechtsstaatlichen Prinzip die Notwendigkeit der Information der Betroffenen. Dies haben die Verfasser des aktuellen Umsetzungsentwurfs zur VDS-Rl dankenswerterweise erkannt und deshalb erstmals eine Informationspflicht des Betroffenen durch den Access-Provider aufgenommen. In jenen Fällen, in denen das Gesetz keine Informationspflichten der Auskunftswerber statuiert, kann den erwähnten Erfordernissen des Rechtsschutzes durch eine vertragliche Informationspflicht des Access-Providers Rechnung getragen werden (vgl dazu unten Kapitel 5.5.6).

4.5.9. Verpflichtungen hinsichtlich Inhaltsdaten

Inhaltsdaten sind grundsätzlich immer zu löschen, es sei denn, die Speicherung stellt einen wesentlichen Bestandteil des Kommunikationsdienstes dar (§ 101 TKG 2003). Inhaltsdaten genießen innerhalb aller Datenkategorien den höchsten Schutz. Ein Zugriff darauf bedarf jedenfalls eines richterlichen Befehls (Art 10a StGG). Der direkte Zugriff auf Inhaltsdaten ist nur in engen in der StPO geregelten Grenzen möglich. Teilweise sind andere Auskunftsbestimmungen jedoch so beschaffen, dass sie etwa im Wege der Auskunft über Stammdaten reflexhaft Informationen zu Inhaltsdaten

[296] EGMR U 6.9.1978, *Klass and Others*, Nr 5029/71, RZ 68.

[297] EGMR U 29.6.2006, *Weber and Savaria*, Nr 54934/00, Rz 135.

[298] RV 272 BlgNR XXIII. GP, 5.

[299] RV 128 BlgNR XXII. GP, 18ff.

[300] Vgl auch *Raschhofer* in *Zankl*, Auf dem Weg zum Überwachungsstaat? (2009) 112ff.

liefern. Diese Problematik wurde bereit oben erörtert (vgl Kapitel 4.4.6) und Lösungsvorschlägen zugeführt. Da die Inhalte einer Kommunikation besonders weit reichende Aufschlüsse über die Privatsphäre zulassen, ist bezüglich dieser Daten tendenziell auch ein besonders strenger Maßstab an die damit zusammenhängenden Schutzpflichten des Access-Providers anzulegen.

4.6. Zwischenergebnis

Soweit in dieser Arbeit der Begriff „Access-Provider" verwendet wird, ist darunter jeder Anbieter öffentlicher Kommunikationsdienste iSd § 92 Abs 3 Z 1 TKG 2003 (mit Ausnahme des Rundfunks) zu verstehen. Diese übermitteln Sprach- und Datenpakete über öffentliche Kommunikationsnetze. Das Abstellen auf die im TKG 2003 enthaltene Definition empfiehlt sich, weil die wichtigsten Auskunftsbestimmungen ebenfalls auf die Begriffsbestimmungen des TKG verweisen. Als „Kunde" gilt für Zwecke dieser Arbeit der Vertragspartner des Access-Providers, dem letzterer aufgrund des zwischen ihnen bestehenden vertraglichen Bandes zur besonderen Sorgfalt verpflichtet ist.

Unter Berücksichtigung der Rechtsprechung des OGH zur Rechtsnatur von Mobilfunkverträgen lassen sich nahezu sämtliche Verträge zwischen Access-Providern und deren Kunden als Mischverträge sui generis mit mietvertraglichen Zügen und Elementen eines freien Dienstvertrages auffassen. Sollte jedoch das Vertragsverhältnis ausnahmsweise so ausgestaltet sein, dass der Access-Provider nur im Falle erfolgreicher Verbindungsherstellungen einen Anspruch auf Entgelt erwirbt, überwiegen mE werkvertragliche Elemente.

Im Zuge der Erfüllung seiner vertraglichen Pflichten verarbeitet der Access-Provider Stammdaten (etwa Name und Anschrift), Verkehrsdaten (etwa Teilnehmernummer oder IP-Adresse), Inhaltsdaten (zB Gesprächsinhalt) und im Falle mobiler Endgeräte auch Standortdaten seines Kunden. Für die Verarbeitung dieser Daten präzisiert das TKG in den §§ 92ff die auch schon aus dem allgemeinen Datenschutzrecht bekannten Prinzipien. So ist das sektorspezifische Datenschutzrecht des TKG vom Gedanken getragen, dass Daten prinzipiell nur für die Erbringung des Kommunikationsdienstes verarbeitet werden dürfen (Zweckbindung). Die aufgrund ausdrücklicher Zustimmung des Kunden möglichen Datenverarbeitungen werden vom Gesetz zumindest dem Wortlaut nach auf die Zwecke Marketing bzw Zur-Verfügung-Stellung von Diensten mit Zusatznutzen beschränkt. Nur die Übermittlung der Daten an Dritte kann nach dem Wortlaut des § 96 Abs 2 auch für andere Zwecke vereinbart werden.

§ 96 Abs 3 TKG 2003 verfolgt das für das Datenschutzrecht typische Ziel, dass jeder wissen soll, welche Daten von ihm zu welchen Zwecken wie lange verarbeitet werden. Diese Bestimmung kann mE so ausgelegt werden, dass sie den Access-Provider in bestimmten Fällen dazu verpflichtet, seinen Kunden darüber zu informieren, bevor er Daten aufgrund eines Auskunftsbegehrens an eine Behörde oder Dritte übermittelt. Diese Pflicht wird freilich dann nicht bestehen können, wenn dadurch der Zweck der Maßnahme – etwa der Ermittlungserfolg strafrechtlicher Untersuchungen – gefährdet wird. Ansonsten lässt sich jedoch eine derartige soweit ersichtlich noch nie praktizierte Auslegung sowohl unter den Wortlaut als auch unter den Telos der Bestimmung fassen.

Die erwähnten Datenkategorien unterliegen unterschiedlichen Schutzniveaus. Den höchsten Schutz genießen Inhaltsdaten, welche nur aufgrund eines richterlichen Befehls preisgegeben werden dürfen. Ist zur Erfüllung eines Auskunftsbegehrens, das auf die Preisgabe von Daten einer niederen Schutzkategorie (zB Stammdaten) abzielt, die Verarbeitung von Daten mit höherem Schutz erforderlich, müssen mE die Schutzbestimmungen der höheren Stufe beachtet werden. Mittlerweile lassen sich in Abkehr von früheren Entscheidungen auch bereits in der Judikatur des OGH Tendenzen in diese Richtung nachweisen. Der aktuelle Entwurf zur Umsetzung der VDS-Rl berücksichtigt den Zusammenhang zwischen den unterschiedlichen Datenkategorien in ebendieser Weise, was zu begrüßen ist.

5. Schutzpflichten hinsichtlich der Privatsphäre

5.1. Grundlagen

Jedermann hat gem Art 8 der Europäischen Menschenrechtskonvention[301] (EMRK) das Recht auf Achtung des Privatlebens. Dieses Grundrecht – bindet wie alle sonstigen Grundrechte auch – in erster Linie den Staat gegenüber seinen Bürgern. Im Folgenden wird die Frage erörtert, wie weit der Access-Provider gegenüber seinem Kunden aufgrund von Schutz- und Sorgfaltspflichten dazu gehalten ist, dessen Privatsphäre zu schützen. Um diese Frage fundiert beantworten zu können, ist es unerlässlich, sich mit den dogmatischen Grundlagen der Schutzpflichten auseinanderzusetzen. Bei näherer Betrachtung stößt man dabei wiederum auf eine überraschende Meinungsvielfalt.

Schutzpflichten, die nach der hL einen Teil der vertraglichen Verpflichtungen ausmachen[302], werden kaum ausdrücklich vertraglich vereinbart. Im Gesetz sind Schutzpflichten, die das vom Austausch der Hauptleistungen nicht betroffene Vermögen schützen sollen, ebenfalls nur sehr vereinzelt vorzufinden (vgl etwa § 1157 ABGB).

Ein Beispiel für eine einschlägige gesetzliche Schutzpflicht wären etwa die Bestimmungen im aktuellen Umsetzungsentwurf zur VDS-Rl, nach welchen der Anbieter den Teilnehmer von der Auskunft über Standortdaten spätestens mit Ablauf der Rechnungsperiode zu informieren hat (vgl dazu Kapitel 4.5.8.1). Nach den EB haben diese Bestimmungen den Zweck, den Teilnehmer in die Lage zu versetzen, die ihm zu Gebote stehenden seine Rechtsschutzinstrumente einzusetzen[303]. Die Ergreifung eines Rechtsmittels zur Wahrung der Rechtsposition des Betroffenen setzt voraus, dass er über die Weitergabe seiner Standortdaten in Kenntnis ist. Somit dient die Pflicht der Wahrung von Rechtspositionen des Teilnehmers und kann somit als gesetzliche Schutzpflicht aufgefasst werden, die bislang allerdings noch im Entwurfsstadium steckt.

---

[301] Konvention zum Schutze der Menschenrechte und Grundfreiheiten, BGBl. Nr. 210/1958, idF BGBl III 179/2002.

[302] Zur Gegenauffassung *Reischauers*, wonach es sich um keine vertraglichen Verpflichtungen handelt, sondern um allgemeine Sorgfaltspflichten deliktischer Qualität, siehe unten.

[303] EB ME 117 BlgNR XXIV. GP 17ff.

Woher also kommen die Schutzpflichten? Was ist ihre dogmatische Grundlage? Sind sie eine Erweiterung des Parteiwillens oder finden sie ihre Grundlage im Gesetz? Die folgenden Ausführungen befassen sich mit den dogmatischen Grundlagen, wie sie in der Judikatur und Literatur entwickelt wurden. Diese Grundsätze sind zu analysieren und für die Zielsetzungen dieser Arbeit nutzbar zu machen.

5.1.1. Schuldverhältnis ohne primäre Leistungspflicht

Es stellt sich die Frage, ob die Schutzpflichten rein vertraglicher Natur sind. Vor allem der Umstand, dass bei Wegfall des Vertragsverhältnisses (etwa nach den §§ 870ff ABGB) dann auch die Schutzpflichten entfallen müssten, was oft zu unbilligen Ergebnissen führen würde, hat dazu geführt, dass manche behaupteten, dass die Schutzpflichten vom Parteiwillen unabhängig und damit „gesetzlicher" Natur seien[304]. Die Schutzpflichten bestehen nach dieser Auffassung also kraft Gesetzes und bilden ein „Schuldverhältnis ohne primäre Leistungspflicht". Die positive Grundlage dafür wurde in Deutschland vor allem in § 242 BGB erblickt, der den Schuldner verpflichtet, die Leistung so zu bewirken, wie Treu und Glauben mit Rücksicht auf die Verkehrssitte es erfordern[305]. Es wird auch vertreten, dass die Schutzpflichten überhaupt aus einer Beurteilung der Interessenlage heraus aus den Grundsätzen von Treu und Glauben zu entwickeln sind[306]. Das Schuldverhältnis ohne primäre Leistungspflicht sei vor allem vom Vertrauensgedanken getragen. Dieses Vertrauensverhältnis trete neben das Leistungsverhältnis[307]. Es werde im Unterschied zum Leistungsverhältnis, das jedenfalls bei synallagmatischen Verträgen stets vom Austauschgedanken geprägt sei, vom

---

304 *Canaris,* Ansprüche wegen „positiver Vertragsverletzung" und „Schutzwirkung für Dritte" bei nichtigen Verträgen, JZ 1965, 475 (476): die Schutzpflichten beruhen weder auf dem Willen der Parteien, noch auf seiner Ergänzung oder Auslegung; *Gerhardt,* der Haftungsmaßstab im gesetzlichen Schuldverhältnis (Positive Vertragsverletzung, culpa in contrahendo), Juritische Schulung 1970, 597 (598), *ders*, Die Haftungsfreizeichnung innerhalb des gesetzlichen Schuldverhältnisses, JZ 1970, 535 (536); *Picker,* Vertragliche und deliktische Schadenshaftung, JZ 1987, 1041 (1044).

305 *Kreß,* Lehrbuch des allgemeinen Schuldrechts (1929) 580.

306 *Roth* in Rebmann/Säcker (Hrsg), Münchener Kommentar zum Bürgerlichen Gesetzbuch II^2 (1985) Rz 125 und Rz 127 zu § 242.

307 Die Eigenständigkeit der Schutzpflichten betonend: *Bydlinski* in *Klang/Gschnitzer,* ABGB IV/2^2 (1978) 182; *Canaris,* Ansprüche wegen „positiver Vertragsverletzung" und „Schutzwirkung für Dritte" bei nichtigen Verträgen, JZ 1965, 475 (475ff); *Müller,* Die Haftung des Stellvertreters bei culpa in contrahendo und positiver Vertragsverletzung, NJW 1969, 2169 (2172ff); *Picker,* Vertragliche und deliktische Schadenshaftung, JZ 1987, 1041 (1044); aA *Ehrenzweig/Mayerhofer,* Schuldrecht, Allgemeiner Teil^3 (1986) 224; *Larenz,* Schuldrecht, Allgemeiner Teil^{10} (1970) 268, der die Auffassung vertritt, dass es keinen Sinn mache, das aus den Schutzpflichten bestehende Schuldverhältnis ohne primäre Leistungspflicht nach Vertragsabschluss noch fortbestehen zu lassen, es gehe dann vielmehr im Vertragsverhältnis auf.

Vertrauensgedanken dominiert[308]. Trotz der gesetzlichen Natur dieses „Schuldverhältnisses ohne primäre Leistungspflicht" werde nach vertraglichen Maßstäben gehaftet, was insbesondere bedeutet, dass auch für das Verhalten von Erfüllungsgehilfen einzustehen sei (§§ 278 BGB bzw 1313a ABGB)[309]. Das bedeutet, dass auch jene die von einer gesetzlichen Natur der Schutzpflichten ausgehen, eine Beweislastumkehr zugunsten des Kunden annehmen würden. Ebenso würden sie den Access-Provider gegenüber dem Kunden für reine Vermögensschäden haften lassen und überdies die Beweislastumkehr gem § 1298 ABGB greifen lassen.

5.1.2. Dogmatische Begründungsversuche in Österreich

Die dogmatischen Begründungsversuche der Schutzpflichten in Österreich sind vielfältig. Die Wahl der Grundlage hat praktische Konsequenzen, insbesondere für den nachvertraglichen Bereich. *Koziol*[310] meint, dass die Schutzpflichten eine gesetzliche Ergänzung des Schuldverhältnisses sind. Sie stellen die Fortsetzung jener vorvertraglichen Pflichten dar, für die im Rahmen der culpa in contrahendo gehaftet wird. Dabei beruft er sich auf *Canaris*[311]. Andererseits meint *Koziol* dann aber doch wieder, dass die Schutzpflichten ab Vertragsabschluss kein eigenständiges Schuldverhältnis mehr ausmachen würden, sondern im begründeten Schuldverhältnis aufgehen[312], was jedoch dem zentralen Gedanken *Canaris'* – einem unabhängigen Nebeneinander von Leistungspflichten und Schutzpflichten – widerspricht[313]. Die Auffassung *Koziols* führt auf den ersten Blick[314] vor allem zu dem oben geschilderten Ergebnis, dass mit Wegfall des Schuldverhältnisses auch sämtliche Schutzpflichten erlöschen, will man ihnen keinen

---

308 *Stoll,* Die Lehre von den Leistungsstörungen (1926) 27.

309 *Larenz,* Culpa in contrahendo, Verkehrssicherungspflicht und „sozialer Kontakt", MDR 1954, 515 (516).

310 *Koziol,* Österreichisches Haftpflichtrecht II (1975) 66.

311 *Canaris,* Ansprüche wegen „positiver Vertragsverletzung" und „Schutzwirkung für Dritte" bei nichtigen Verträgen, JZ 1965, 475 (476ff).

312 *Larenz,* Lehrbuch des Schulrechts, Allgemeiner Teil I^{13} (1982) 114ff; zur Kritik daran vgl *Roth* in Rebmann/Säcker*,* Münchener Kommentar zum Bürgerlichen Gesetzbuch II^{2} (1985) Rz 126 zu § 242.

313 Andererseits meint *Koziol* aber an anderer Stelle unter ausdrücklicher Berufung auf Canaris, dass die Schutzpflichten nicht auf dem Willen der Parteien beruhen und daher vom Bestand des Vertragsverhältnisses unabhängig seien: *Koziol,* Delikt, Verletzung von Schutzgesetzen und Zwischenbereich, JBl 1994, 209 (211).

314 Bei näherer Betrachtung spricht jedoch nichts dagegen, die Schutzpflichten dort wo kein gültiges Vertragsverhältnis besteht, dem gesetzlichen Schuldverhältnis und dort wo ein Vertrag besteht, den daraus entspringenden Pflichten zuzuordnen, vgl dazu unten 5.1.5.

unabhängigen Bestehensgrund zuerkennen. Dies kann zu befremdlichen Ergebnissen führen.

> Beispiel: Oben (vgl Kapitel 3.2.2) wurde dargelegt, dass die Verletzung von Schutzpflichten nach zutreffender Ansicht ein Recht zum Rücktritt vom Vertrag eröffnen kann. Man nehme an, der Access-Provider verstößt gegen seine Pflicht, die Privatsphäre seines Kunden zu schützen, indem er unzulässigerweise Daten des Kunden preisgibt, worauf der Kunde des Access-Providers daraufhin vom Vertrag zurücktritt. Man nehme weiters an, die soeben erwähnte Schutzpflicht sei rein vertraglicher Natur. Mit dem Rücktritt ginge dann mangels unabhängigen Bestehensgrunds der Schutzpflichten auch der Anspruch auf Einhaltung derselben verloren. Findet der Kunde im positiven Recht (etwa DSG) keine Möglichkeit, seine Interessen durchzusetzen, läge ein äußerst unbefriedigendes Ergebnis vor, vor allem deshalb, da er nicht mehr in den Genuss der Erfüllungsgehilfenhaftung kommt. Für ein Fehlverhalten von Mitarbeitern des Access-Providers kann er letzteren nicht mehr nach § 1313a ABGB verantwortlich machen.

5.1.3. Lösungsansätze in der Judikatur

Der OGH geht in manchen Entscheidungen ohne nähere Begründung von einer Fortwirkung der Schutzpflichten auch nach Beendigung des Schuldverhältnisses aus[315]. In einer Entscheidung[316] berief er sich dabei auf eine Stelle bei *Esser* und *Schmidt*[317]. Die beiden letztgenannten sprechen von einer „gegenüber der Vertragshaftung eigenständigen Primärhaftpflicht aus Schutzpflichtverletzung" und gehen somit wie *Canaris* (siehe oben) von einem unabhängigen Nebeneinander der Leistungspflichten auf der einen und den Schutzpflichten auf der anderen Seite aus[318]. Somit hat sich der OGH zumindest in dieser Entscheidung impliziter jener Auffassung *Canaris'* angeschlossen, wonach die Schutzpflichten ihre Rechtsgrundlage weder im Willen der Parteien noch in dessen Auslegung bzw Ergänzung, sondern ausschließlich im Gesetze haben. Nach *Canaris* sind Schutzpflichten von den Hauptleistungspflichten aufgrund ihrer strukturellen Unterschiedlichkeit völlig unabhängig. Während Hauptleistungspflichten ihren Inhalt durch „Parteiwillen und Vertragszweck erhalten", werden Schutzpflichten „nur durch die tatsächlichen Beziehungen der Parteien zueinander"[319] bestimmt[320]. Das Schutzpflichtverhältnis wird so gesehen als gesetzliches

---

[315] Vgl etwa OGH 12.1.1983, 1 Ob 827/82, SZ 56/3.

[316] OGH 17.1.1991, 8 Ob 38/90, RdW 1991, 261.

[317] *Esser/Schmidt,* Schuldrecht, Allgemeiner Teil I^{6} (1984) 428.

[318] *Esser/Schmidt,* Schuldrecht, Allgemeiner Teil I/2^{7} (1993) 132.

[319] *Canaris,* Ansprüche wegen „positiver Vertragsverletzung" und „Schutzwirkung für Dritte" bei nichtigen Verträgen, JZ 1965, 475 (478ff [FN 34]).

[320] Vgl auch *Siebert* in *Soergel/Siebert,* BGB I^{9}(1969), § 242 Rz 102.

Schuldverhältnis[321] gesehen, das sich der privatautonomen Gestaltung weitestgehend entzieht. *Welser* meint ebenfalls, dass das Gesetz unmittelbar aufgrund des Gesetzes entsteht[322]. *Koziol* schließt sich in einem Aufsatz der Auffassung *Canaris* sogar ausdrücklich an[323].

5.1.4. Positive Grundlage

Fraglich ist allerdings, auf welcher positiven Grundlage das oben dargestellte Ergebnis beruht. In Deutschland wurde die Idee des Schutzpflichtverhältnisses auf § 242 BGB gestützt[324]. Dabei spielt es keine Rolle, dass diese Bestimmung ihrem Wortlaut nach eigentlich das Bestehen eines gültigen Vertragsverhältnisses voraussetzt, da sie anerkanntermaßen auch für die Beurteilung von Sonderbeziehungen herangezogen wird, die kein Rechtsverhältnis im engeren Sinne sind[325]. Eine § 242 BGB exakt entsprechende Bestimmung ist im ABGB nicht vorhanden[326]. Dennoch hat das Prinzip von Treu und Glauben, das historisch betrachtet auf die *bona fides* im römischen Recht[327] zurückgeht, in nahezu allen europäischen Rechtsordnungen eine so große Bedeutung erlangt, dass auch von einem europäischen Rechtsprinzip gesprochen werden kann[328]. Nach der Auslegungsregel des § 914 ABGB ist „der Vertrag so zu verstehen, wie es der Übung des rechtlichen Verkehrs entspricht". Die Begriffe „Übung des redlichen Verkehrs" und der Grundsatz von Treu und Glauben werden vom OGH teilweise gleichgesetzt[329]. Eine bloße Auslegungsregel für Verträge wie § 914 ABGB wird aber wohl nur schwerlich zur positiven Grundlage für außervertragliche

---

321 *Thiele,* Leistungsstörung und Schutzpflichtverletzung, JZ 1967, 649 (651).

322 *Welser,* Bürgerliches Recht II[13] (2007) 13.

323 *Koziol,* Verletzung von Schuldverhältnissen und Zwischenbereich, JBl 1994, 209 (211) FN 8.

324 *Canaris,* Ansprüche wegen „positiver Vertragsverletzung" und „Schutzwirkung für Dritte" bei nichtigen Verträgen, JZ 1965, 475 (476); vgl auch *Roth* in *Rebmann/Säcker* (Hrsg) Münchener Kommentar zum Bürgerlichen Gesetzbuch[2] (1985) § 242 Rz 121ff.

325 *Roth* in *Rebmann/Säcker* (Hrsg) Münchener Kommentar zum Bürgerlichen Gesetzbuch[2] (1985) § 242 Rz 53.

326 *Reischauer* in Rummel, ABGB I[3] (2000) § 914 Rz 17.

327 Vgl dazu *Schermaier*, Bona fides in Roman contract law, in *Zimmermann/Whittacker,* Good faith in European contract law (2000) 63.

328 *Krüger* in Rebmann/Säcker*/Rixecker (*Hrsg) Münchener Kommentar zum Bürgerlichen Gesetzbuch[4] (2003) § 242 Rz 140.

329 Vgl etwa OGH 25.4. 1963, 6 Ob 86/63, SZ 36/68, wo es heißt: *„Es ist [...] die Absicht der Parteien zu erforschen und der Vertrag so zu verstehen, wie es der Übung des redlichen Verkehrs – also den Grundsätzen von Treu und Glauben – entspricht."*

Haftung nach vertraglichen Grundsätzen gemacht werden können. Für die Haftung im vorvertraglichen Bereich, für die ein späteres Zustandekommen des Vertrages keine Voraussetzung ist, lassen sich die Schutzpflichten aus einer Analogie insbesondere aus den §§ 878 Satz 3, 874 ABGB ableiten[330]. Allerdings tritt etwa *Rummel* dafür ein, entsprechend der Rechtsfortbildung im Bereich der culpa in contrahendo insbesondere über ergänzende Vertragsauslegung nachvertragliche Schutzpflichten anzuerkennen[331]. Auch in Österreich hat die Erfüllung, Durchführung und Abwicklung von Verträgen nach der Übung des redlichen Verkehrs und nach den über die Pflicht zur Wahrung der guten Sitten hinausgehenden Anforderungen von Treu und Glauben zu erfolgen[332]. Nach der Judikatur bildet das Prinzip von Treu und Glauben einen das bürgerliche Recht beherrschenden Grundsatz[333]. Auch die Lehre anerkennt, dass die Vertragsparteien einander auch ohne eine § 242 BGB entsprechende Bestimmung im ABGB mit Treu und Glauben zu begegnen haben[334]. Der Grundsatz von Treu und Glauben ist daher dem österreichischen ABGB immanent, wobei diese Auffassung vor allem auf die §§ 863 und 914 ABGB gestützt wird[335]. So gesehen lassen sich die deutsche Lösung auch auf die österreichische Rechtslage übertragen und sich Schutzpflichten ohne ein (fort)bestehendes Schuldverhältnis konstruieren, für deren Verletzung nach vertraglichen Maßstäben (vor allem § 1313a ABGB) zu haften ist. Anders lässt sich die oben gezeigte Entscheidungspraxis des OGH[336] nicht erklären. Daher hat jeder Vertragspartner auch nach der Erfüllung[337] bzw nach Wegfall des Vertrages dafür Sorge zu tragen, dass dem anderen keine Nachteile entstehen. Das bedeutet, dass den Access-Provider auch nach Vertragsbeendigung – etwa aufgrund eines Rücktritts des Kunden infolge einer Schutzpflichtverletzung – noch Schutzpflichten hinsichtlich der Privatsphäre seines Kunden treffen. Für deren Verletzung hat er nach vertraglichen Maßstäben einzustehen.

---

330 Vgl dazu etwa *Ehrenzweig/Mayerhofer,* Schuldrecht, Allgemeiner Teil[3] (1986) 225.

331 *Rummel* in Rummel, ABGB I[3] (2000) § 859 Rz 30, vgl auch *Bar,* "Nachwirkende Vertragspflichten, AcP 179 (1979), 452 (467); *Koziol,* Delikt, Verletzung von Schuldverhältnissen und Zwischenbereich, JBl 1994, 209 (211).

332 OGH 3.12.1980, 1 Ob 680/80, SZ 53/164.

333 OGH 3.6.1953, 1 Ob 474/53, JBl 1953, 625; 08.01.1958 7 Ob 600/57, MietSlg 6280 = JBl 1958,362 = ImmZ 1959,59 = ImmZ 1958, 260; 28.08.2003 8 ObA 83/03v uva.

334 *Mayerhofer/Ehrenzweig*, Schuldrecht, Allgemeiner Teil[3] (1986), 20; *Gschnitzer/Faistenberger,* Österreichisches Schuldrecht, Allgemeiner Teil[2] (1985) 50.

335 *Rummel* in Rummel, ABGB I[3] (2000) § 863 Rz 2, § 914 Rz 17.

336 Vgl auch OGH 14. 1. 1992 4 Ob 122/91, JBl 1992, 451 = RdW 1992, 239.

337 OGH 25.3.1987, 1 Ob 716/86, JBl 1982, 782.

5.1.5. Rechtsnatur der Schutzpflichten

Nach den obigen Ausführungen lässt sich festhalten, dass Schutzpflichten neben die Hauptleistungspflichten treten können und vor allem die von den Hauptleistungen nicht betroffenen Güter der Vertragspartner schützen sollen. Sie können unabhängig vom Zustandekommen oder Bestehen eines Vertragsverhältnisses existieren. Das bedeutet, dass sie auch vor Abschluss (culpa in contrahendo), nach Beendigung sowie nach erfolgreicher Anfechtung des Vertragsverhältnisses noch Platz greifen können. Dies ist deshalb von besonderer Bedeutung, weil der Kunde im Falle der Verletzung von Schutzpflichten wohl oft ein Interesse an der Auflösung des Vertrages haben wird und dies mE wie erwähnt über die §§ 918ff ABGB auch durchsetzen kann (vgl oben Kapitel 3.2.2). Aber auch nach Vertragsauflösung wird er ein Interesse haben, eine allfällige Haftung des Access-Providers nach vertraglichen Maßstäben durchzusetzen.

In seltenen Fällen ist es möglich, Schutzpflichten direkt aus dem Gesetz abzuleiten, ebenfalls nur äußerst selten werden Schutzpflichten ausdrücklich vereinbart. Sofern die Gültigkeit des Vertragsverhältnisses außer Zweifel steht, lassen sich die Schutzpflichten aus der ergänzenden Vertragsauslegung (siehe dazu unten Kapitel 5.5.2) gewinnen. Zusätzlich lassen sich Schutzpflichten stets, insbesondere auch bei erfolgreich angefochtenen Verträgen, auf das Prinzip von Treu und Glauben stützen. Dieses Prinzip ist, wie noch weiter unten ausführlich zu zeigen sein wird, auch Grundlage und Korrektiv für die ergänzende Vertragsauslegung, sodass Inhalt und Umfang von Schutzpflichten, die weder im Gesetz begründet noch vereinbart wurden, nach den Regeln der ergänzenden Vertragsauslegung zu bestimmen sind[338].

Nachdem für die Verletzung dieser Schutzpflichten stets nach vertraglichen Grundsätzen gehaftet werden soll, erscheint es sinnvoll, die Schutzpflichten – wo möglich – mit *Larenz* den vertraglichen Pflichten zuzuordnen[339] und sie nicht wie *Canaris* auch während des gültigen aufrechten Vertrages dem gesetzlichen Schuldverhältnis ohne primäre Leistungspflicht zuzuordnen[340]. Das bedeutet, dass die zunächst dem gesetzlichen Schuldverhältnis zuzuordnenden Schutzpflichten mit dem Zustandekommen des Rechtsgeschäftes in diesem aufgehen[341]. Sollte es danach zu einer Beseitigung des

---

[338] OGH 13.11.1985, 1 Ob 661/85, JBl 1986,452 = SZ 58/4 = EvBl 1986, 400 mwN; vgl auch *Stefula,* Haftung des Erfüllungsgehilfen nach vertraglichen Grundsätzen, RZ 2001, 216 (218), der die ergänzende Vertragsauslegung als dogmatische Grundlage der Schutz- und Sorgfaltspflichten bezeichnet.

[339] *Blomeyer,* Allgemeines Schuldrecht (1964) 73; *Mayerhofer/Ehrenzweig*, Schuldrecht, Allgemeiner Teil[3] (1986), 224; *Larenz,* Lehrbuch des Schulrechts, Allgemeiner Teil I[13] (1982) 114ff.

[340] *Canaris,* Ansprüche wegen „positiver Vertragsverletzung" und „Schutzwirkung für Dritte" bei nichtigen Verträgen, JZ 1965, 475 (479).

[341] *Koziol,* Österreichisches Haftpflichtrecht II[2] (1984) 79.

Vertrages kommen, kann wiederum auf die Pflichten aus dem gesetzlichen Schuldverhältnis zurückgegriffen werden. Die Schutzpflichten können sich daher auf unterschiedliche Geltungsgrundlagen stützen, für ihre Verletzung wird aber dennoch immer nach vertraglichen Maßstäben gehaftet. Dagegen wurde vor allem vorgebracht, dass die Schutzpflichten sich strukturell und inhaltlich nicht ändern würden, weshalb ein Wechsel der Geltungsgrundlage nur schwer nachvollziehbar sei[342]. Das ist nicht ganz unrichtig, da die Schutzpflichten inhaltlich ja wie erwähnt nach den Regeln ergänzender Vertragsauslegung bestimmt werden. Obwohl ein derartiger Wechsel der Rechtsnatur auf den ersten Blick etwas willkürlich erscheinen mag, darf jedoch nicht übersehen werden, dass sämtliche Schutzpflichten rechtsschöpfend gewonnen wurden und man sich insbesondere im Bereich der culpa in contrahendo und der nachvertraglichen Schutzpflichten juristischer Kunstgriffe bemühen musste, die zum positiven Recht bereits eine gewisse Distanz aufweisen. All diese Kunstgriffe haben gemein, dass man sich mit der schlichten Haftung nach deliktischen Grundsätzen nicht begnügen wollte und den Geschäftsherrn auch für das Verhalten seiner Erfüllungsgehilfen haften lassen und dem Geschädigten die Vorzüge der Beweislastumkehr zugestehen möchte[343]. Das ist der wahre Grund, weshalb von Lehre und Rechtsprechung das vorvertragliche Schuldverhältnis und nachvertragliche Schutzpflichten aus der Taufe gehoben wurden. Letztlich waren wohl die Bedürfnisse der Praxis ausschlaggebend dafür, dass diese mit dem positiven Recht nur eingeschränkt begründbaren Rechtsfiguren sich durchsetzen konnten und mehrheitlich akzeptiert wurden. Wo es jedoch möglich ist, die Schutzpflichten als Ergänzung des Parteiwillens und somit in ihrer rein vertraglichen Natur anzuerkennen, sollte dies auch geschehen. In diese Richtung gehen womöglich auch einige Entscheidungen des OGH, in denen er meint, dass es sich bei dem vorvertraglichen Schuldverhältnis um eines ohne Hauptleistungspflicht handelt, wenn der in Aussicht genommene Vertrag nicht zustande kommt[344]. Mit Blick auf die österreichische Rechtsprechung kann jedoch nicht geleugnet werden, dass der OGH in einer Reihe von Entscheidungen – ohne freilich auf die hier erörterten Problemstellungen einzugehen – die Schutzpflichten durch ergänzende Vertragsauslegung bestimmt und somit meist impliziter von deren vertraglicher Geltungsgrundlage ausgeht[345]. Richtigerweise ist das vor- bzw nachvertragliche (auf Schutzpflichten begrenzte) Schuldverhältnis gesetzlicher Natur weil es in diesen Phasen naturgemäß keinen Vertrag

---

342 *Canaris,* Ansprüche wegen „positiver Vertragsverletzung" und „Schutzwirkung für Dritte" bei nichtigen Verträgen, JZ 1965, 475 (479).

343 Dies konstatiert auch *Koziol,* Delikt, Verletzung von Schuldverhältnissen und Zwischenbereich, JBl 1994, 209 (212).

344 OGH 6.7.1976, 5 Ob 626/76, SZ 49/94; OGH 8.10.1975, 1 Ob 191/75, SZ 48/102.

345 Vgl *Binder* in *Schwimann,* ABGB V^2 (1997) § 914 Rz 153ff.

(mehr) gibt. Der Inhalt der Schutzpflichten ergibt sich aber auch hier im Wesentlichen aus der ergänzenden Vertragsauslegung. Mithilfe dieses Instruments werden noch weiter unten (siehe Kapitel 5.5.2ff) der Inhalt und Reichweite der Schutzpflichten des Access-Providers bestimmt werden. Das gilt auch für jene Fälle, in denen der Vertrag ex nunc oder ex tunc beseitigt wird und die Pflichten sich aus dem erwähnten gesetzlichen Schuldverhältnis ergeben.

5.1.6. Die sachliche Rechtfertigung der Schutzpflichten

Umstritten ist aber nicht nur die Rechtsnatur der Schutzpflichten, sondern auch deren sachliche Rechtfertigung: Schutzpflichten liegt der Gedanke zugrunde, dass die Vertragspartner wegen der vertraglichen Verbindung zueinander in einer Sonderbeziehung stehen und sich besonderes Vertrauen entgegenbringen[346]. Aufgrund der Sonderbeziehung sind sie in der Lage, in besonderer Weise aufeinander einzuwirken und in die Sphäre des jeweils anderen einzudringen[347].

5.1.6.1. Vertrauen

Schon früh wurde die Auffassung vertreten, dass die Vertragspartner durch das sie verbindende Schuldverhältnis (und den vorausgehenden Kontakt) zueinander eine besondere Beziehung aufbauen, die in besonderem Maße wechselseitiges Vertrauen voraussetzt[348]. Allerdings sind weder das gegenseitig gewährte Vertrauen noch die mit Vertragsabschlüssen einhergehende Einwirkungsmöglichkeit für sich alleine ausreichend, um eine vertragliche Haftung aus Schutzpflichten zu begründen[349]. Dass es alleine auf das Vertrauen nicht ankommen kann, ergibt sich schon aus dem Umstand, dass es sich beim Vertrauen stets um etwas Subjektives handelt, das dem anderen Vertragspartner nur schwer bzw überhaupt nicht zugänglich ist. Ob den Access-Provider eine Schutzpflicht hinsichtlich der Privatsphäre seines Kunden trifft, kann nicht einzig davon abhängen, ob der Kunde ihm diesbezüglich vertraut. Handelt es sich bei dem Vertragspartner des Access-Providers um eine paranoide Person, die niemandem vertraut und daher davon ausgeht, der Access-Provider würde ihre Daten missbrauchen, würde

---

346 *Esser/Schmidt,* Schuldrecht, Allgemeiner Teil I/1[7] (1992) 106; *Stoll,* Die Lehre von den Leistungsstörungen (1926) 26.

347 AA *Reischauer* in Rummel, ABGB II[3] (2000) Rz 4 zu Vor §§ 918-932.

348 *Stoll,* Die Lehre von den Leistungsstörungen (1926) 26; hinsichtlich der Haftung aus culpa in contrahendo: *Ballerstedt,* Zur Haftung für culpa in contrahendo, AcP 151 (1950/52), 501 (506); dagegen *Emmerich* in Rebmann/Säcker, Münchener Kommentar zum Bürgerlichen Gesetzbuch II[3] (1994) Rz 55 zu Vor § 275.

349 So im Hinblick auf die culpa in contrahendo als Vertrauenshaftung auch *Flume,* Allgemeiner Teil des bürgerlichen Rechts II (1965) 129.

die Schutzpflicht entfallen[350]. Dieses Ergebnis wäre jedoch äußerst unbefriedigend. Um dieses Problem zu entschärfen, ist das Vertrauen gewissermaßen zu objektivieren und zu fragen, worauf eine redliche Vertragspartei üblicherweise vertraut[351]. Gegen das Vertrauen als sachliche Rechtfertigung für das Bestehen bestimmter Vertragspflichten wurde auch eingewandt, dass es sich hier um einen Zirkelschluss handle. Vertrauen darf man, weil eine Anspruchsgrundlage besteht, diese aber entsteht, weil man ihr vertraut[352].

5.1.6.2. Einwirkungsmöglichkeiten

Dass durch den Vertragsabschluss die Einwirkungsmöglichkeit von Vertragspartnern auf die Sphäre ihres Gegenübers erhöht wird und dass durch diese Erhöhung der Gefährdung ein besonderes Schutzbedürfnis entspricht, wird vom OGH in ständiger Rechtsprechung judiziert[353] und entspricht überdies der hL[354].

Bestritten wird dies von *Reischauer* mit dem wenig überzeugenden Argument, dass etwa ein wildfremder Schifahrer vielmehr Einwirkungsmöglichkeiten auf die Güter anderer Pistenbenutzer habe als üblicherweise ein Geschäftspartner[355]. Er bringt an dieser Stelle noch einige Beispiele, die allesamt in dieselbe Kerbe schlagen: Aufgezählt werden Fälle, in denen fremde Personen in bestimmten Konstellationen auf jemanden weit höheren Einfluss ausüben können, als dessen Vertragspartner. Seiner Ansicht nach hat der Vertragspartner hier nicht für die Verletzung vertraglicher Pflichten, sondern für die Verletzung allgemeiner Sorgfaltspflichten einzustehen[356]. Dabei lässt er

---

350 Vgl auch *Medicus,* Grenzen der Haftung für culpa in contrahendo, Juristische Ausbildung 1965, 209 (213), der etwa hinsichtlich der culpa in contrahendo etwa darauf verweist, dass gerade im vorvertraglichen Stadium den Äußerungen des potenziellen Vertragspartners gegenüber häufig erhebliches Misstrauen besteht.

351 Vgl mit ähnlichem Beispiel zu ähnlichem Ergebnis kommend *Thiele,* Leistungsstörung und Schutzpflichtverletzung, JZ 1967, 649 (652).

352 *Von Bar,* Vertrauenshaftung ohne Vertrauen – Zur Prospekthaftung bei der Publikums-KG in der Rechtsprechung des BGH, ZGR 1983, 467 (500).

353 OGH 08.03.1978, 1 Ob 520/78, JBl 1979, 201 = SZ 51/26 uva, zuletzt etwa 24.06.2005, 1 Ob 124/05z.

354 *Bydlinski,* Vertragliche Sorgfaltspflichten zugunsten Dritter, JBl 1960 359 (361); *ders* in *Klang/Gschnitzer*, ABGB IV/2[2] (1968), 182; *Klang/Gschnitzer*, ABGB IV/1[2] (1968), 57; *Canaris,* Ansprüche wegen „positiver Vertragsverletzung" und „Schutzwirkung für Dritte" bei nichtigen Verträgen, JZ 1965, 475 (476); *Mayerhofer/Ehrenzweig*, Schuldrecht, Allgemeiner Teil[3] (1986), 226; *Stoll,* Die Lehre von den Leistungsstörungen (1926), 28; (hinsichtlich cic) *Ballerstedt,* Zur Haftung für culpa in contrahendo, AcP 151 (1950/51), 501 (506)

355 *Reischauer* in Rummel, ABGB I[3] (2000) Vor §§ 918-932 Rz 4.

356 Die Nähe zwischen vertraglichen Schutzpflichten und allgemeinen Sorgfaltspflichten wird auch deutlich bei *Dölle ,* Außergesetzliche Schuldpflichten, ZGesStW 1943, 67 (74), der die besondere Haftung für Schutzpflichtverletzungen darin begründet sieht weil, „insoweit die Beteiligten einander oder wenigstens der eine Beteiligte dem anderen ein besonderes Vertrauen entgegengebracht haben, indem sie die eigenen Rechtsgüter bewusst – zur Erreichung des mit dem sozialen Kontakt verfolgten Zwecks – dem Einfluß und damit der

jedoch unberücksichtigt, dass keineswegs behauptet wird, dass die den Vertragspartnern durch die vertragliche Beziehung offen stehenden Einwirkungsmöglichkeiten immer gleich hoch sind. Es wurde auch an keiner Stelle behauptet, dass ein Vertragsabschluss stets dazu führt, dass die Vertragspartner einander eine im Umfang nicht steigerbare Einflussnahmemöglichkeit einräumen[357]. Freilich gibt theoretisch jeder Verkehrsteilnehmer im Straßenverkehr allen anderen die Gelegenheit, nachteilig auf seine körperliche Integrität einzuwirken. Allerdings ist dieser Kontakt im Bezug auf den einzelnen Verkehrsteilnehmer weder gewollt noch gezielt[358]. Während man sich seinen Vertragspartner gezielt aussucht und sich in der Regel wohl auch genau überlegt, ob man diesem vertrauen kann, ist dies gegenüber der Allgemeinheit nicht der Fall. Dem Vertragspartner werden durch den Abschluss eines Rechtsgeschäftes Einflussnahmemöglichkeiten eingeräumt, die in Umfang und Intensität variieren können und die sonst niemandem offen stehen: Nur der Access-Provider verfügt gewöhnlich über jene Informationen, die nötig sind, um das Kommunikationsverhalten seines Kunden nachzuvollziehen. Diese Möglichkeit gewährt der Kunde freilich nicht gänzlich aus freien Stücken, er hat vielmehr keine andere Wahl, als sich in diesem Punkt seinem Vertragspartner anzuvertrauen[359]. Wenn man einen Installateur zur Durchführung von Reparaturarbeiten in seine Wohnung lässt, dann gibt man ihm dadurch eine Gelegenheit nachteilig auf die in der Wohnung befindlichen Güter einzuwirken wie sonst keinem Fremden[360]. Die Begründung der besonderen Haftung nach vertraglichen Grundsätzen

---

Obhut und Sorgfalt des andern anvertrauten und in diesem Vertrauen nicht enttäuscht werden dürfen." *Dölle* geht aber noch einen entscheidenden Schritt weiter und meint, dass diese Besonderheiten nicht nur auf Vertragsverhandlungen zutreffen, sondern überhaupt auf jenen sozialen Kontakt, vermöge dessen eine Person zur Erreichung eines bestimmten Zweckes ihre Lebensgüter [...] einer anderen Person anvertraut." Schuldpflichten können bei ihm ohne Vertrag und ohne vorvertragliche Handlungen unmittelbar aus objektivem sozialem Kontakt erwachsen und eine Haftung begründen.

357 Überdies finden sich in der Literatur auch Stimmen, die in bestimmten Konstellationen, in denen Personen gegenüber einander besondere Einwirkungsmöglichkeiten haben – hier Arbeitnehmer untereinander –, quasi gesetzliche Schuldverhältnisse orten: *Mayer-Maly*, Das Rechtsverhältnis zwischen Arbeitnehmern, in *Tomandl* (Hrsg) Innerbetriebliche Arbeitnehmerkonflikte aus rechtlicher Sicht (1977) 63ff; begründet wird dies damit, dass *„das Arbeitsverhältnis die Persönlichkeit eines Arbeitnehmers in der Regel sehr weitgehend erfaßt und deshalb Arbeitskollegen zwangsläufig Einblicke in Bereiche der Persönlichkeitsentfaltung ihrer Kollegen bekommen [...]".*

358 *Thiele,* Leistungsstörung und Schutzpflichtverletzung, JZ 1967, 649 (651).

359 Vgl auch *Schlesinger,* Das Wesen der positiven Vertragsverletzungen, ZBl 1926, 721 (744ff), der das Problem folgendermaßen auf den Punkt bringt: *„Die Erfüllung fast aller Typen von Schuldverhältnissen bringt es notwendig mit sich, daß dem Schuldner die Möglichkeit geboten werden muß, auf die Interessen- und Rechtssphäre des Gläubigers in größerem oder geringerem Maße einzuwirken, sie nötigt den Gläubiger sozusagen, der Gegenpartei die Eingangspforte zu seinem Vermögensbereich zu öffnen, sich ihr in mancher Hinsicht anzuvertrauen. Dieser für den Gläubiger bestehenden Zwangslage entspricht von der anderen Seite eine Rechtspflicht des Schuldners [...]".*

360 Vgl auch die treffende Formulierung von *Esser/Schmidt,* Schuldrecht, Allgemeiner Teil I/2[7] (1993) 129: *„Treten Personen namentlich zur Aufnahme rechtsgeschäftlicher Beziehungen gezielt in einen Sonderkontakt zueinander, so verlassen sie jenes allgemeine Nebeneinander mit seinen zufälligen Kollisionsmöglichkeiten, für das der anonymisierende deliktsrechtliche*

damit, dass durch den rechtsgeschäftlichen Kontakt und später durch den Abschluss dem Vertragspartner besondere Einwirkungsmöglichkeiten eröffnet werden, erweist sich daher als zutreffend.

5.2. Ziele und Inhalt von Schutzpflichten

5.2.1. Erhaltungszweck

Die Schutz- und Sorgfaltspflichten haben vor allem den Zweck, dass die bestehenden Güter des Vertragspartners geschützt werden. Nach der Rechtsprechung des OGH hat sich jeder Vertragspartner *„so zu verhalten, wie es der andere in der gegebenen Situation mit Rücksicht auf den konkreten Vertragszweck, die besondere Art der Leistung und die Erfordernisse eines loyalen Zusammenwirkens erwarten darf, damit die Erreichung des Vertragszweckes nicht vereitelt, sondern erleichtert und Schaden verhütet wird. Diese weiteren Verhaltenspflichten können auch die Verpflichtungen umfassen, dem anderen den ihm nach dem Vertrag zukommenden Vorteil zu erhalten und dafür zu sorgen, sodaß ihm für die Zeit nach der Beendigung des Vertragsverhältnisses keine Nachteile entstehen*[361]." Der Status der Güter des Vertragspartners soll, soweit es nicht um die Erfüllung der primären Hauptspflichten geht, unberührt bleiben[362]. Daher spricht man auch von einer Erhaltungspflicht[363]. Insofern weisen sie freilich eine gewisse Nähe zur deliktischen Haftung auf, die ähnliche Ziele verfolgt.

5.2.2. Nähe zu allgemeinen Sorgfaltspflichten

Reischauer meint, dass für Schutzpflichtverletzungen überhaupt nur nach deliktischen Regeln zu haften sei. Die Erfüllungsgehilfenhaftung – sie ist der wohl der maßgeblichste Grund für die Einbeziehung der Schutzpflichten in das Vertragsverhältnis – könne man auch direkt aus § 1313a ABGB ableiten, dafür bedürfe es nicht des Kunstgriffs, die deliktischen Sorgfaltspflichten zu einer Vertragspflicht zu machen. Die

---

Grundsatz des „neminem laedere" typisch ist, und wechseln in den speziellen Status eines Miteinander über, den ein spezifisches Vertrauen gerade in dieses Gegenüber kennzeichnet und der überdies gesteigerte Einwirkungsmöglichkeiten in die „Besitzstände" der Beteiligten mit sich bringt."

361 OGH 01.12.1981 4 Ob 558/81, SZ 54/179.

362 *Thiele,* Leistungsstörung und Schutzpflichtverletzung, JZ 1967, 649 (650).

363 *Gschnitzer* in *Klang/Gschnitzer,* ABGB IV/1^2 (1968) 473.

ratio von § 1313a ABGB sei die Interessensverfolgung gegenüber dem Geschädigten[364]. Den von der hL ebenfalls den Schutzpflichtverletzungen zugeordneten Mangelfolgeschaden sieht er als Problem der fehlerhaften Erbringung der Hauptleistungspflicht (zur Kritik daran siehe oben Kapitel 2.1.3).

5.3. Intensität und Dauer des Schuldverältnisses

Je länger das Rechtsgeschäft angelegt ist, desto intensiver und dichter sind die das Leistungsverhältnis flankierenden Schutzpflichten[365]. Die Dauer des Vertragsverhältnisses spielt mE in Bezug auf den Umfang der Schutzpflichten jedenfalls dann stets eine besondere Rolle, wenn die Einwirkungsmöglichkeiten mit ihr gemeinsam zunehmen. Das gilt für sämtliche Rechtsgüter der Vertragspartner, insbesondere jedoch für die Privatsphäre. Je länger ein Vertragsverhältnis andauert, desto mehr Umstände aus der Privatsphäre werden gewöhnlich dem jeweils anderen Vertragspartner bekannt. Neben der Dauer der vertraglichen Beziehung sind auch andere Umstände zu berücksichtigen. Wie oben dargelegt, bringen Vertragsabschlüsse typischerweise stets eine mehr oder minder ausgeprägte Einwirkungsmöglichkeit mit sich. Dieser Umstand wird richtigerweise als ein Grund dafür gesehen, warum für diese Schutzpflichten nach vertraglichen Grundsätzen zu haften ist (siehe dazu schon oben). Konsequenterweise müssen sich der Umfang und die Intensität der sich durch ein Rechtsgeschäft ergebenden Einwirkungsmöglichkeiten auch auf die Schutzpflichten des Vertragspartners auswirken. Je mehr Einwirkungsmöglichkeiten sich durch einen Vertragsabschluss ergeben, desto stärker werden auch die Schutzpflichten ausgeprägt sein. Für die hier interessierende Fragestellung ergibt sich daraus, dass für den Fall der Bejahung einer Schutzpflicht des Access-Providers gegenüber seinem Kunden an diese wohl besonders strenge Maßstäbe anzulegen sind. Dies ergibt sich daraus, dass die meisten Verträge über die Erbringung von elektronischen Kommunikationsdiensten auf Dauer angelegt sind und dem Access-Provider Einblicke von besonderer Qualität in das Privatleben seines Vertragspartners ermöglichen. Nach Umsetzung der Vorratsdatenspeicherungsrichtlinie in Österreich wird der Access-Provider grob gesagt für eine Dauer von mindestens sechs Monaten zu speichern haben, wer wann mit wem von wo aus kommuniziert. Aus dem so angehäuften Datenbestand lassen sich vielfältige Schlüsse ziehen: So lässt sich alleine aus den Verkehrs- und Standortdaten ableiten, wo der Betroffenen gewöhnlich seine Nacht

---

[364] *Reischauer* in Rummel, ABGB I³ (2000) Vor §§ 918-933 Rz 5.

[365] *Larenz,* Lehrbuch des Schuldrechts, Allgemeiner Teil I¹³ (1982) 11.

verbringt, wo er arbeitet, mit wem er tagsüber telefoniert, wo er seine Wochenenden verbringt usw. Gleicht man dieses Datenmaterial mit dem Datenmaterial von Personen ab, mit denen er häufig kommuniziert, lassen sich Rückschlüsse auf seinen Freundeskreis, seine Lebensgefährten usw ziehen. Freilich wäre eine derartige eigenmächtige Auswertung durch den Provider nicht mit den Grundsätzen des DSG 2000 bzw TKG 2003 in Einklang zu bringen und damit rechtswidrig. Der oben erwähnte Grundsatz bezieht jedoch nur auf die abstrakte Einwirkungsmöglichkeit. Diese Einwirkungsmöglichkeit ist bei Verträgen über die Erbringung elektronischer Kommunikationsdienste ganz besonders stark ausgeprägt. Daraus kann ein hoher Maßstab für die Schutzpflichten des Access-Providers hinsichtlich der Privatsphäre abgeleitet werden.

5.4. Schutzobjekt Privatsphäre

Bevor geklärt werden kann, ob und inwieweit Pflichten des Access-Providers zum Schutz der Privatsphäre seines Kunden bestehen, ist zunächst das betroffene Schutzgut – die Privatsphäre – näher zu skizzieren:

Gemäß § 16 ABGB hat jeder Mensch angeborene, schon durch die Vernunft einleuchtende Rechte und ist daher als Person zu betrachten. Darunter ist kein Programmsatz zu verstehen, sondern vielmehr eine *„Zentralnorm unserer Rechtsordnung, mit normativem subjektive Rechte gewährenden Inhalt. Sie anerkennt die Persönlichkeit als Grundwert. In seinem Kernbereich schützt § 16 ABGB die Menschenwürde."*[366] Die Norm ist bewusst generalklauselhaft formuliert und lässt dem Rechtsanwender einen weiten Interpretationsspielraum zur Findung neuer Persönlichkeitsrechte. Nach Ansicht der Verfasser des Gesetzestextes war eine taxative Aufzählung aller Persönlichkeitsrechte unmöglich[367]. § 16 ABGB ist Anknüpfungspunkt für die Anerkennung privater Persönlichkeitsrechte[368]. Die Bestimmung wurde aufgrund ihres naturrechtlichen Hintergrundes nach ihrem In-Kraft-Treten lange Zeit vernachlässigt[369] und erst später immer häufiger bei der Rechtsfindung herangezogen.

---

[366] OGH 27.2.1990, 1 ObS 40/90, SZ 63/32 = JBl 1990, 734.

[367] *Zeiller,* Commentar über das allgemeine bürgerliche Gesetzbuch für die gesammten deutschen Erbländer der oesterreichischen Monarchie I (1811) 106; vgl auch *Reischauer,* Das Persönlichkeitsrecht auf Achtung des Fernsprechgeheimnisses (§ 16 ABGB) und seine Bedeutung für das Dienstverhältnis, RdA 1973, 207 (212 FN 54) mwN.

[368] *Wellspacher,* das Naturrecht und das ABGB, in Festschrift zur Jahrhundertfeier des ABGB (1911) 173 (178).

[369] Vgl etwa die ablehnende Haltung *Ungers,* System des österreichischen allgemeinen Privatrechts I[5], 496ff.

Das Gesetz ermöglicht somit auch die Berücksichtigung grundrechtlich verbürgter Rechte, die in erster Linie nur den Staat binden sollen[370] (mittelbare Drittwirkung[371]). Das Grundrecht auf Datenschutz genießt als einziges Grundrecht der österreichischen Bundesverfassung eine gesetzlich normierte unmittelbare Drittwirkung. § 1 Abs 5 leg cit bestimmt:

„Gegen Rechtsträger, die in Formen des Privatrechts eingerichtet sind, ist, soweit sie nicht in Vollziehung der Gesetze tätig werden, das Grundrecht auf Datenschutz mit Ausnahme des Rechtes auf Auskunft auf dem Zivilrechtsweg geltend zu machen. In allen übrigen Fällen ist die Datenschutzkommission zur Entscheidung zuständig, es sei denn, daß Akte der Gesetzgebung oder der Gerichtsbarkeit betroffen sind."

Zur Auslegung von § 16 ABGB sind aber nicht nur die in grundrechtlichen Bestimmungen, sondern auch die aus einfachgesetzlichen Bestimmungen ableitbaren Wertungen heranzuziehen. Die österreichische Rechtsordnung schützt die Privatsphäre in einer Vielzahl unterschiedlichster Bestimmungen. Zu denken ist etwa an die Art 8 EMRK, 10 und 10a StGG, an die §§ 118ff, 301 StGB, 1, 14 DSG 2000, 9 Abs 2 RAO, 37 NO, 54 ÄrzteG, 115 ArbVG, 6 und 7 MedienG, 77 UrhG, die §§ 92ff TKG 2003 sowie das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten[372] und dessen Zusatzprotokoll[373]. Die Privatsphäre war somit bereits vor der Einfügung des § 1328a ABGB durch das Zivilrechts-Änderungsgesetzes 2004[374] durch § 16 ABGB geschützt[375]. Der OGH hat erstmals in der Entscheidung 4 Ob 91/78 das Recht auf „Achtung der Geheimsphäre" als Persönlichkeitsrecht iSd § 16 ABGB anerkannt[376]. Der besondere Stellenwert, den der Gesetzgeber dem Datenschutz im Bereich der Telekommunikation einräumt, ergibt sich auch aus § 1 Abs 2 Z 3 lit b und d TKG 2003. Lit b leg cit erklärt ein hohes Datenschutzniveau und lit d leg cit die Sicherstellung von Integrität und Sicherheit von öffentlichen Kommunikationsnetzen zu einem Ziel der Regulierung. Diese Ziele entsprechen den in Art 1 der EK-Datenschutzrichtlinie formulierten Zielen. Die EK-Datenschutzrichtlinie dient der Ergänzung und Detaillierung des durch die allgemeine Datenschutzrichtlinie

---

370 *Ermacora*, Handbuch der Grundfreiheiten und der Menschenrechte (1963) 257.

371 Vgl dazu etwa *Marhold,* Kommentar zu OGH 24. 10. 1978, 4 Ob 91/78, ZAS 1979, 177; *Bydlinski*, Bemerkungen über Grundrechte und Privatrecht öZöffR 1962/63, 423.

372 BGBl 317/1988; vgl dazu etwa *Burkert,* Die Konvention des Europarats zum Datenschutz, CR 1988, 751ff.

373 BGBl III 91/2008.

374 BGBl I 2003/93.

375 *Lukas,* Schadenersatz bei Verletzung der Privatsphäre, RZ 2004, 33 (33).

376 OGH 24.10.1978 4 Ob 91/78, SZ 51/146 = Arb 9742 = ZAS 1979, 176 = RdA 1979, 394.

eingeräumten Schutzes. Aus all diesen Bestimmungen lässt sich sowohl auf europäischer als auch auf nationaler Ebene ganz allgemein eine deutliche Wertung zugunsten des Schutzes der Privatsphäre ableiten.

Persönlichkeitsrechte sind absolute Rechte und damit auch von Dritten zu beachten. Ob jedoch ein Eingriff in die durch § 16 ABGB geschützten Rechtspositionen im Einzelfall als rechtswidrig zu beurteilen ist, hängt vom Ergebnis einer durchzuführenden Interessensabwägung ab. Dabei müssen das Interesse des eingreifenden und das Interesse am durch § 16 ABGB geschützten Gut gegenübergestellt werden. Eine Überspannung des Schutzes könnte in vielen Fällen zu einer unzumutbaren Beschränkung der Interessen anderer bzw der Allgemeinheit führen. Das Recht auf Wahrung der Geheimnissphäre hat jedoch im höchstpersönlichen Lebensbereich absolute Wirkung[377]. Da diese Prüfung jedoch nur den deliktischen Bereich betrifft und sich diese Arbeit mit vertraglichen Schutzpflichten auseinandersetzt, kann es mit diesem kurzen Hinweis sein Bewenden haben. Allerdings lassen sich aufgrund des schon oben erwähnten Naheverhältnisses zwischen Schutzpflichten und allgemeinen Verhaltenspflichten Erkenntnisse über § 16 ABGB in seiner Ausprägung als Persönlichkeitsrecht auf Achtung der Privatsphäre für die Entwicklung entsprechender vertraglicher Schutzpflichten heranziehen.

Die grundrechtliche Bestimmung des Art 8 EMRK vermag über § 16 ABGB somit mittelbar auch inter privatos zur Geltung zu gelangen. Die Grenzen dieser Wirkung verlaufen aber jedenfalls dort, wo man sich durch gültige privatautonome Rechtsgestaltung des Schutzes begibt[378]. Der Begriff des Privatlebens iSd Art 8 EMRK lässt sich nicht endgültig definieren[379], es kommt jedoch vor allem auf den fehlenden Öffentlichkeitsbezug an[380]. Die Verwendung, dh insbesondere das Sammeln und Speichern personenbezogener Daten stellt ohne Zweifel einen Eingriff in den Schutzbereich von Art 8 EMRK dar[381]. Besonders bedeutsam für die hier interessierenden Fragestellungen ist auch die Entscheidung des EGMR in der Rechtssache *Malone vs. The United Kingdom*, in welcher er aussprach, dass nicht nur der Inhalt, sondern auch die äußeren Umstände der Kommunikation (hier etwa angewählte Telefonnummern) in den

---

377 *Posch* in *Schwimann,* ABGB I[3] (2005) § 16 Rz 39.

378 *Bydlinski*, Bemerkungen über Grundrechte und Privatrecht, ZöffR 1962/63, 423 (433ff); RV 173 BlgNR XXII. GP, 17.

379 EGMR U 16.12.1992, *Niemitz*, Nr 13710/88, Rz 29.

380 *Wiederin* in *Korinek/Holoubek* (Hrsg), Österreichisches Bundesverfassungsrecht III, Grundrechte, Art 8 EMRK Rz 30 mwN.

381 EGMR U 26.3.1987, *Leander*, Nr 9248/81, Rz 48.

Schutzbereich des Art 8 EMRK fallen[382]. Im Jahr 1984 dachte der EGMR freilich noch nicht an die im Zusammenhang mit heutigen modernen Kommunikationsformen anfallenden Daten. Dennoch vermögen etwa IP-Adressen, sofern sie mit Personenbezug gespeichert werden, über die Teilnehmer einer per E-Mail geführten Kommunikation mindestens ebensoviel auszusagen, wie die Telefonnummern zu einem Telefongespräch. Es liegt daher nahe, auch alle sonstigen Verkehrsdaten iSd TKG 2003 dem Schutzbereich des Art 8 EMRK zuzuordnen[383]. Konsequenterweise sollte somit auch § 16 ABGB vor der Preisgabe dieser Daten schützen. Geschützt sind auch die Daten, die im Rahmen beruflicher Kommunikation erzeugt werden[384], wobei sich der Schutz von Geschäfts- und Betriebsgeheimnissen nach überwiegender Ansicht nicht auf § 16 ABGB stützen lässt[385], da diese Norm vorwiegend den Schutz ideeller Persönlichkeitsgüter bewirken soll[386].

Das Recht auf Achtung der Privatsphäre ist auch durch verschuldensunabhängige Unterlassungs- und Beseitigungsansprüche geschützt. Kommt es etwa zur (nicht notwendigerweise schuldhaften) rechtswidrigen Verwendung von Daten durch den Access-Provider, können gegen diesen neben den im DSG 2000 verankerten Ansprüchen (§ 32 Abs 2 DSG 2000) auch Beseitigungsansprüche und (bei Wiederholungsgefahr) Unterlassungsansprüche erfolgreich geltend gemacht werden[387]. Es kommen überdies einstweilige Verfügungen in Betracht (§ 381 EO), die gem § 32 Abs 3 DSG 2000 auch dann erlassen dürfen, wenn die in § 381 EO genannten Voraussetzungen nicht gegeben sind.

Art 8 EMRK sichert dem Bürger nach *Wiederin* die Kontrolle über Informationen, die seine Person und sein Verhalten betreffen[388]. Diese Kontrolle wird in erster Linie dadurch gewährleistet, dass jedem ein Recht auf Geheimhaltung seiner Daten zukommt. Sinnvollerweise wird dieses durch das Recht auf Löschung unzulässig verarbeiteter Daten ergänzt. Nur durch die Löschung kann, wenn überhaupt, dem Anspruch auf Geheimhaltung wieder zum Durchbruch verholfen werden. Der Löschungsanspruch ist somit eine Art Beseitigungsanspruch[389], mit welchem der

---

382 EGMR U 2.8.1984, *Malone*, Nr 8691/79 Rz 84.

383 *Raschhofer* in *Zankl* (Hrsg), Auf dem Weg zum Überwachungsstaat? (2009) 211.

384 EGMR U 16.2.2000, *Amann*, Nr 27798/95, Rz 65f.

385 *Koziol,* Österreichisches Haftpflichtrecht II^2 (1984) 16.

386 *Posch* in *Schwimann,* ABGB I^3 (2005) § 16 Rz 40.

387 *Reischauer* in *Rummel,* ABGB II^3 (2004) § 1328a Rz 15.

388 *Wiederin,* Privatsphäre und Überwachungsstaat (2003) 28.

389 Vgl etwa DSK 23.8.2002, K120.819/003-DSK/2002.

unrechtmäßige Eingriff wieder behoben und der rechtmäßige Zustand wieder hergestellt werden soll. Gleich einem nachbarrechtlichen Anspruch auf Entfernung unrechtmäßig abgeladenen Schutts soll durch die Löschung unrechtmäßig verarbeiteter Daten der Status quo ante herbeigeführt werden. Hierbei tritt jedoch der immaterielle Charakter des geschützten Rechtsguts Privatsphäre als Hindernis einer vollständigen Restitution deutlich zu Tage: Das geschützte Rechtsgut sind nicht die bloßen Informationen, die man nach Belieben zum ursprünglichen „Besitzer" oder „rechtmäßigen Eigentümer" zurückstellen kann. Geschützt ist vielmehr der geheime Charakter dieser Informationen. Um das Wesen des Rechtsguts Privatsphäre richtig zu erfassen, darf man seine Aufmerksamkeit nicht auf die geschützten Informationen beschränken. Vielmehr kommt es auf die Beziehung zwischen diesen und den daran Berechtigten und Unberechtigten an. So kommt es häufig zu Situationen, in denen die Löschung unzulässig erworbener und verarbeiteter Daten dem Betroffenen im Ergebnis nicht mehr viel weiterhilft. Man denke etwa an das aktuelle Beispiel eines Steuersünders[390], dessen Bankdaten, die unzulässigerweise verarbeitet wurden, nun an die Finanzbehörde weitergegeben wurden. Selbst wenn es ihm gelänge, einen Anspruch auf Löschung durchzusetzen, wäre die Finanzbehörde bereits in Kenntnis seiner Identität und der aus seiner Sicht so gewertete hauptsächliche Zweck seines Rechts auf Geheimhaltung bereits vereitelt[391]. Die Kenntnis der Behörde über bestimmte Informationen, also etwa über die Identität eines Menschen und dem Umstand, dass dieser am Fiskus vorbei geschleustes Geld im Ausland veranlagte, lässt sich nicht mehr beseitigen. Genau diese Information ist es aber, welche die Ermittler auf den Plan ruft um weitere Erhebungen durchzuführen, die womöglich zur Überführung führen werden. So verhält es sich auch mit vielen Auskunftsansprüchen gegen Access-Provider. Übermitteln diese etwa den Sicherheitsbehörden nach § 53 Abs 3b SPG die IMSI und Informationen darüber, in welcher Funkzelle sich der Betroffene befindet, wird die Behörde sofort eine Ortung vornehmen. Wenn sich im Nachhinein herausstellen sollte, dass die gesetzlichen Voraussetzungen des Auskunftsbegehrens nicht vorhanden waren und der Betroffene sein Recht auf Löschung erfolgreich geltend macht, vermag dies nur teilweise die faktischen Wirkungen der Rechtsverletzung zu beseitigen. So wird er damit leben müssen, dass die konkreten Organe des öffentlichen Sicherheitsdienstes, welche an der Ortung beteiligt waren, Kenntnis von seinem Aufenthaltsort zu einem bestimmten Zeitpunkt haben. Diese Kenntnis lässt sich nicht mehr „löschen". Die Unkenntnis über den Aufenthaltsort ist jedoch Bestandteil des Schutzobjekts Privatsphäre. Insofern wurde das Schutzobjekt irreversibel verletzt.

---

390 Vgl nur http://www.zeit.de/politik/deutschland/2010-02/schweiz-steuerhinterzieher-merkel (Stand April 2010).

391 Vgl zu diesem Problem auch *Honsell,* Der Geheimnisschutz im Zivilrecht, in *Ruppe* (Hrsg) Geheimnisschutz im Wirtschaftsleben (1980) 45 (47).

Schadenersatzansprüche werden oft einem bezifferbaren Schaden scheitern, den Ersatz immaterieller Schäden durch die Verletzung der Privatsphäre regelt nunmehr § 1328a ABGB (siehe dazu sogleich nächstes Kapitel) in restriktiver und abschließender Weise.

Das Rechtsgut Privatsphäre wird also bereits dadurch verletzt, dass jemand Kenntnis von Informationen nimmt, die er eigentlich nicht kennen dürfte. Der Anspruch des Betroffenen, unzulässig verarbeitete Daten zu löschen, ist daher wichtig, um weiteren Fällen der Kenntnisnahme und damit einher gehenden weiteren Beeinträchtigungen vorzubeugen. Diese Erkenntnis ist für die Entwicklung vertraglicher Schutzpflichten wichtig. Insbesondere ist sie bei der Beantwortung der Frage zu beachten, inwieweit der Access-Provider zur Information über die Erfüllung eines Auskunftsbegehrens verpflichtet ist. Schutzpflichten haben nämlich den Zweck, den Berechtigten vor Schäden an dessen Gütern zu bewahren[392]. Beauskunftet der Access-Provider eine Behörde oder einen Privaten, könnte selbst im Fall der Unrechtmäßigkeit dieses Vorgangs die Auffassung vertreten werden, dass eine Information deshalb nicht angezeigt sei, da abgesehen von der bereits stattgefundenen Beeinträchtigung keine weiteren mehr drohen. Die Information des Betroffenen wäre also nicht nötig, um ihn vor weiteren Schäden zu bewahren[393]. Es besteht aber wie gezeigt alleine aufgrund der Verfügungsmacht des Unberechtigten über die Daten das Risiko, dass weitere Personen unbefugt davon Kenntnis nehmen und damit das Rechtsgut Privatsphäre erneut verletzen. Daher können weitere Beeinträchtigungen nur verhindert werden, indem der Betroffene informiert und dadurch in die Lage versetzt wird, die Rechtmäßigkeit der Beauskunftung zu überprüfen. Im Falle der Unrechtmäßigkeit der Erhebung der Daten wird der Betroffene sein Löschungsrecht geltend machen und so wenigstens weiteren Beeinträchtigungen vorbeugen können. Daher kann die Konstruktion einer umfassenden Benachrichtigungspflicht zumindest nicht am Argument scheitern, es drohen keine weiteren Beeinträchtigungen der Privatsphäre.

---

[392] OGH 25.04.1972, 8 Ob 60/72, JBl 1972, 609.

[393] So argumentiert etwa *Feiler,* Data Breach Notification, MR 2009, 281 (284) in Bezug auf die Pflicht zur Aufklärung über die Verletzung der Sicherheit personenbezogener Daten. Zu beachten ist allerdings, dass hier die Sachlage freilich eine andere ist. Die Information des Betroffenen, es habe eine Verletzung der Sicherheit der Daten durch einen Unbekannten gegeben, versetzt diesen nicht in die Lage seine Rechte durchzusetzen, da er nicht weiß, gegen wen er dies tun sollte. Daher kommt *Feiler* zum Schluss, dass eine Information des Betroffenen in so einem Fall keinen weiteren Schäden vorzubeugen vermag, weshalb eine diesbezügliche Schutzpflicht ausscheide. Die hier interessierenden Sachverhalte sehen freilich anders aus: Hier kennt der Access-Provider die Identität der Auskunft suchenden Stelle, weshalb eine Information des Betroffenen darüber diesem die Möglichkeit eröffnet, seine Rechte wahrzunehmen.

5.4.1. § 1328a ABGB

Wie erwähnt erfuhr der auf § 16 ABGB gestützte in Lehre und Rechtsprechung schon vorher vertretene Schutz der Privatsphäre durch die Zivilrechtsnovelle 2004 eine ausdrückliche Anerkennung durch den Gesetzgeber in § 1328a ABGB[394]. Wer rechtswidrig und schuldhaft in die Privatsphäre eines Menschen eingreift oder Umstände aus der Privatsphäre eines Menschen offenbart oder verwertet[395], hat ihm den dadurch entstandenen Schaden zu ersetzen. Ersatzberechtigt sind ausschließlich natürliche Personen (arg „Menschen"[396]). Die Materialien nennen das Abhören eines Telefons ohne ausreichende gesetzliche Grundlage unter Verletzung des Fernmeldegeheimnisses ebenso als Beispiel für einen rechtswidrigen Eingriff wie das unzulässige Speichern von Informationen über einen Betroffenen[397].

§ 1328a ABGB begründet nicht die Rechtswidrigkeit für jeden Eingriff in die Privatsphäre, die in der Norm angesprochenen Rechtsfolgen setzen diese vielmehr voraus. Ob der Eingriff in das Rechtsgut Privatsphäre rechtswidrig ist, hängt, sofern nicht konkrete gesetzlicher Verbote bzw Eingriffstatbestände bestehen, auch nach Einfügung des § 1328a ABGB weiterhin von einer Interessensabwägung ab[398]. ME ist *Harrer* zuzustimmen, der die vom OGH verwendete Formel, dass der (schädliche) Erfolg die Rechtswidrigkeit in der Regel indiziere[399], als wenig sinnvoll kritisiert[400]. Diese Indizwirkung erspart dem Geschädigten keinesfalls den Nachweis der Rechtswidrigkeit, selbst wenn er seine Ansprüche aus einer Haftung ex contractu ableitet, weil die Beweislastumkehr des § 1298 ABGB ausschließlich für das Verschulden gilt. Daher ist der Mehrwert dieser Formel in der Tat fraglich. Wenn der Eingriff sich nicht auf ein Gesetz zu stützen vermag, sind das Interesse des Einzelnen auf Wahrung seiner Geheim-, Privat- und Intimsphäre den Interessen anderer Personen oder der Allgemeinheit gegenüber zu stellen. Eingriffe in die Privatsphäre, die zur Durchsetzung hoch- oder höherwertiger Interessen vorgenommen werden, können keinen Schadenersatzanspruch des Einzelnen

---

394 Vgl auch in *Reischauer* in *Rummel,* ABGB II³ (2004) § 1328a Rz 1.

395 Die Begriffe „Offenbaren" und „Verwerten" sind dem strafrechtlichen Geheimnisschutz entlehnt: *Helmich,* Schadenersatz bei Eingriffen in die Privatsphäre, ecolex 2008, 888 (888).

396 *Lukas,* Schadenersatz bei Verletzung der Privatsphäre, RZ 2004, 33 (38).

397 173 RV BlgNR XXI. GP, 17ff; vgl auch *Dittrich/Tades,* ABGB[36] (2009) § 16 Rz 5aff.

398 *Harrer* in *Schwimann,* ABGB VI³ (2006) § 1328a Rz 3; *Helmich,* Schadenersatz bei Eingriffen in die Privatsphäre, ecolex 2008, 888 (888); vgl etwa OGH 14.5.1997, 7 Ob 89/97 g, JBl 1997, 641.

399 Vgl nur OGH 09.10.1984 2 Ob 606/84, JBl 1986, 248 = RdW 1985, 244 = ZVR 1985, 148; vgl auch *Welser*, Bürgerliches Recht II[13] (2007) 312 mwN.

400 *Harrer* in *Schwimann,* ABGB VI³ (2006) § 1294 Rz 6ff.

nach sich ziehen[401]. Dabei ist zu betonen, dass der Eingreifende grundsätzlich stets das gelindeste noch zum angestrebten Erfolg führende Mittel zu wählen hat[402].

Ist der Eingriff in die Privatsphäre bzw die Offenbarung oder Verwertung von Umständen aus der Privatsphäre durch ein Gesetz gedeckt, ist die Rechtswidrigkeit stets zu verneinen (vgl auch § 8 Abs 1 Z 1 DSG 2000). Diesfalls wird kein rechtswidriger Erfolg herbeigeführt. Die Rechtswidrigkeit kann sich freilich auch aus einer Vertragsverletzung ergeben[403]. Ein haftungsbegründender Vertragsbruch kann etwa vorliegen, wenn sich die Weitergabe personenbezogener Daten nicht auf eine gesetzliche Grundlage zu stützen vermag und der Access-Provider eine vertragliche Schutzpflicht schuldhaft verletzt hat. Die bloße Weitergabe personenbezogener Daten des Access-Providers ohne gesetzliche Grundlage auf behördlichen Auftrag ist zwar rechtswidrig, idR aber nicht schuldhaft. Treffen ihn aber etwa Schutzpflichten zur Kontrolle der Rechtmäßigkeit des Auskunfts- bzw Mitwirkungsbegehrens und verletzt er diese, haftet er, da er diesfalls Umstände aus der Privatsphäre offenbarte, indem er eine Vertragspflicht schuldhaft verletzte. Der Frage wann und inwieweit derartige Schutzpflichten bestehen, wird in den folgenden Kapiteln nachgegangen werden.

Da gem § 1 Abs 1 AHG der Bund, die Länder, die Bezirke, die Gemeinden, sonstige Körperschaften des öffentlichen Rechts und die Träger der Sozialversicherung nach den Bestimmungen des bürgerlichen Rechts für den Schaden am Vermögen oder an der Person, den die als ihre Organe handelnden Personen in Vollziehung der Gesetze durch ein rechtswidriges Verhalten wem immer schuldhaft zugefügt haben, haften, kommt auch eine Haftung nach dem AHG in Betracht[404]. Rechtswidrige und schuldhafte Eingriffe eines Organs in die Privatsphäre des Betroffenen können den Rechtsträger daher (auch hinsichtlich des immateriellen Schadens) ersatzpflichtig machen. Werden also etwa Daten ohne Rechtsgrundlage verwendet, ist an einen Ersatzanspruch nach dem AHG iVm § 1328a ABGB zu denken. Dabei schließt selbst strafgesetzwidriges Verhalten des Organs eine Zurechnung an den Rechtsträger nicht aus. Auch schikanöses bzw eigennütziges Handeln ist dem Rechtsträger noch zuzurechnen. Nur wenn ein Organ Handlungen vornimmt, die mit den Aufgaben seines Amtes in keinem Zusammenhang

---

[401] RV 173 BlgNR XXII. GP, 16; aM *Reischauer* in *Rummel,* ABGB II^3 (2004) § 1328a Rz 7, der die Formel, dass bei Eingriffen in absolut geschützte Rechtsgüter die Rechtswidrigkeit nur auf Grundlage einer umfassenden Interessensabwägung beurteilt werden kann, generell nicht toleriert; vgl auch *Reischauer* in Rummel*,* ABGB I^3 (2000) § 1294 Rz 19a.

[402] OGH 30.1.1997, 6 Ob 2401/96y, SZ 70/18.

[403] RV 173 BlgNR XXII. GP, 15.

[404] RV 173 BlgNR XXII. GP, 19.

stehen, kommt eine Zurechnung dieser Handlungen an den Rechtsträger nicht in Betracht[405].

Wie bisher haftet der Eingreifende für durch die rechtswidrige und schuldhafte Verletzung der Privatsphäre entstehende Vermögensschäden. Bei grobem Verschulden ist auch der entgangene Gewinn von der Ersatzpflicht umfasst (§ 1324 ABGB).

Neu ist jedoch die in § 1328a Abs 1 2. Satz aufgenommene Bestimmung, dass bei erheblichen Verletzungen der Privatsphäre der Ersatzanspruch auch eine Entschädigung für die erlittene persönliche Beeinträchtigung umfasst. Damit wird erstmals auch durch eine allgemeine Bestimmung der Ersatz immaterieller Schäden, die aus der Beeinträchtigung der Privatsphäre erwachsen, angeordnet. Die uneinheitliche Rechtslage bezüglich des Ersatzes immaterieller Schäden bei der Beeinträchtigung der Privatsphäre wurde als unbefriedigend empfunden[406]. Dabei kommt es nicht auf den Grad des Verschuldens, sondern lediglich auf das Ausmaß der erlittenen Beeinträchtigung an[407]. Die Beeinträchtigung muss eine gewisse Erheblichkeitsschwelle erreichen[408]. § 1328a ABGB wurde gerade deshalb eingefügt, um Ersatzansprüche für jene Fälle zu schaffen, in denen die Voraussetzungen der spezielleren Tatbestände (etwa §§ 33 DSG 2000, 7ff MedienG, 78 und 87 Abs 2 UrhG) nicht erfüllt sind. So soll ein Ersatzanspruch etwa auch dann zustehen, wenn es sich nicht um besonders sensible Daten iSd § 18 Abs 2 DSG 2000 handelt, bzw die sonstigen Voraussetzungen eines Ersatzanspruchs gem § 33 DSG 2000 nicht gegeben sind[409]. Der Gesetzgeber wollte den Schutz der Privatsphäre erhöhen, was bedeutet, dass nunmehr durch mehr Sachverhalte ein Ersatzanspruch verwirklicht wird. Zweifellos wird die Verwendung von Daten, die Rückschlüsse auf das Sexualleben des Betroffenen zulassen, die für den Ersatzanspruch geforderte Erheblichkeitsschwelle überschreiten. Die Eignung zur Bloßstellung in der Öffentlichkeit ist keine zwingende Voraussetzung, sondern lediglich ein Beispiel des

---

405 OGH 20.5.1981, 1 Ob 14/81, SZ 54/80.

406 *Hinteregger,* Der Schutz der Privatsphäre durch das österreichische Schadenersatzrecht – de lege lata et de lege ferenda, in *Koziol/Spier,* Liber Amicorum Pierre Widmer (2003) 143 (159ff); 173 BlgNR XXII. GP, 5.

407 *Reischauer* in *Rummel,* ABGB II³ (2004) § 1328a Rz 11; Ebenso *Harrer* in *Schwimann,* ABGB VI³ (2006) § 1328a Rz 7, anders die Materialien (RV 172 BlgNR XXII: GP, 19), die den Grad des Verschuldens als Kriterium für die Bejahung des Ersatzanspruchs anführen. Diese Auffassung ist jedoch abzulehnen, weil sie im Wortlaut des § 1328a ABGB keine Deckung findet und die Proportionalität von Schuld und Haftung keinen umfassenden Leitgedanken des geltenden Schadenersatzrechts bildet: OGH (verstärkter Senat) 24.3.1998, 1 Ob 315/97y, SZ 71/56 = EvBl 1998/119 = JBl 1998, 312 = ecolex 1998, 392 = ARD 4938/21/98 = RdW 1998, 333 = ZVR 1998/80.

408 Vgl auch *Karner/Koziol,* Der Ersatz ideellen Schadens im österreichischen Recht und seine Reform, in 15. ÖJT Band II/1 (2003) 36ff.

409 RV 173 BlgNR XXII. GP, 20.

Gesetzgebers, mit welchem er die geforderte Erheblichkeit des Eingriffs illustrieren wollte. Die erforderliche Beeinträchtigung der Privatsphäre muss diesem Beispiel wertungsmäßig gleichkommen. ME ist dies beispielsweise bei der rechtsgrundlosen Verwendung der Verkehrs- und Standortdaten aus einem mehrere Monate umfassenden Zeitraum der Fall. Damit muss zwar nicht unbedingt eine öffentliche Bloßstellung verbunden sein, das Ausmaß der Beeinträchtigung ergibt sich in diesen Fällen aus den umfassenden Schlüssen, die aus dem Datenbestand über das Privatleben des Betroffenen gezogen werden können. Wie das deutsche Bundesverfassungsgericht in seiner Entscheidung zur Vorratsdatenspeicherung zutreffend festhielt, lassen sich aus Vorratsdaten tiefe Einblicke in das soziale Umfeld und die Intimsphäre des Betroffenen gewinnen[410]. Neben Bewegungsprofilen lassen sich aus den Verkehrs- und Standortdaten einiger Monate vielfach Aussagen über politische Neigungen, über das Beziehungsleben eines Menschen und dessen persönliche Vorlieben ableiten. Die Verwendung dieses Datenbestandes stellt somit einen Engriff dar, dessen Schwere wertungsmäßig einer Bloßstellung vergleichbar ist. Welche Eingriffe in das Privatleben die vom Gesetz für den Ersatz des immateriellen Schadens geforderte Erheblichkeit aufweisen, wird letztlich der Richter anhand einer wertenden Betrachtungsweise entscheiden müssen.

Durch § 1328a ABGB ist das Problem der Ersatzfähigkeit immaterieller Schäden einer abschließenden Regelung zugeführt worden. Das bedeutet, dass in Fällen, in welchen die Voraussetzungen des § 1328a ABGB nicht gegeben sind, der Ersatz immaterieller Schäden nicht auf allgemeine Erwägungen zum Ersatz ideeller Schäden[411] gestützt werden kann.

5.4.2. Mögliche Erscheinungsformen der Schutzpflichten

Nach dem oben Gesagten haben Vertragspartner darauf zu achten, dass sie dem jeweils anderen keinen Schaden an dessen vom Leistungsaustausch nicht betroffenen Rechtsgütern zufügen (Kapitel 5.2). Die Privatsphäre stellt ein solches Rechtsgut dar (Kapitel 5.4). Was bedeutet dies nun konkret in Bezug auf die beim Access-Provider im Zuge der Erbringung von elektronischen Kommunikationsdiensten verarbeiteten Daten?

---

[410] BVerfG 2.3.2010, 1 BvR 256/08, Rz 211.

[411] Vgl etwa *Bydlinski,* Der Ersatz ideeller Schäden als sachliches und methodisches Problem, JBl 1965, 173 (179); *Strasser*, Der immaterielle Schaden im österreichischen Recht (1964); OGH 16.5.2001, 2 Ob 84/01v, RZ 2001, 232 = ZVR 2001, 284 = ecolex 2001, 668 = JBl 2001, 660 = Schobel, RdW 2002, 206 = SZ 74/90 = EFSlg 97.045 = ZfRV 2007, 44 = ZVR 2008, 49.

Zunächst einmal lassen sich daraus Verhaltenspflichten des Access-Providers gegenüber seinem Kunden ableiten. Hierher gehört vor allem die Pflicht Daten nur im unbedingt nötigen Ausmaß anzulegen und sie so bald als möglich zu löschen. Die meisten dieser Pflichten sind jedoch bereits unmittelbar im Gesetz (vgl insbesondere die §§ 92 ff TKG 2003, siehe dazu oben Kapitel 4.5) enthalten, sodass eine Konstruktion vertraglicher Schutzpflichten in diesem Verhältnis nur ergänzende Funktion hat. Wie noch zu zeigen sein wird, lassen sich aus diesen datenschutzrechtlichen Bestimmungen aber Prinzipien und Wertungen ableiten, die für die Entwicklung von Schutzpflichten nutzbar gemacht werden können. Wie oben erwähnt, werden Schutzpflichten insbesondere durch Rückgriff auf das Prinzip von Treu und Glauben sowie im Rahmen ergänzender Vertragsauslegung entwickelt. Um zu nachvollziehbaren Ergebnissen zu kommen, empfiehlt es sich hierbei, klar erkennbare gesetzgeberische Wertungen zu berücksichtigen.

Weiters werden Pflichten des Access-Providers im Zusammenhang mit Dritten zu erörtern sein. Dabei geht es vor allem um Geheimhaltungsansprüche des Vertragspartners des Access-Providers in jenen Fällen, in denen etwa eine Behörde oder eine Privatperson mit einem Auskunftsbegehren an den Access-Provider herantritt. In diesem Zusammenhang wird zu erörtern sein, in wieweit der Access-Provider verhalten ist, sich gegen die Erfüllung des Auskunftsbegehrens zu stellen, dh die Erfüllung des Auskunftsbegehrens zu verweigern bzw etwa durch Ergreifung von Rechtsmitteln zu bekämpfen. Hierher gehört auch die Frage, ob den Access-Provider die Pflicht treffen soll, seinen Vertragspartner über an ihn heran getragene Auskunftsbegehren zu informieren. Der Frage nach einer Informationspflicht kann unterschiedslos im Bezug auf sämtliche Auskunftsbestimmungen nachgegangen werden. der Frage nach einer Pflicht, sich Auskunftsbegehren entgegenzustellen, kann jedoch zunächst nur in Grundzügen nachgegangen werden, da es hierbei auf die Gestaltung der konkreten gesetzlichen Auskunftsbestimmungen ankommt. Abschließend kann diese Frage dann erst im Rahmen der Erörterung der einzelnen Auskunftsbestimmungen geklärt werden.

All die angesprochenen möglichen Pflichten haben gemein, dass sie letztlich den Schutz der Privatsphäre des Kunden des Access-Providers bezwecken. Sie dienen also dessen Interesse an der Erhaltung seiner Privatsphäre. Es geht also um Erhaltungspflichten[412] des Access-Providers. Bei der Entwicklung der Schutzpflichten werden die bisherigen Ausführungen über die dogmatischen Grundlagen und die sachliche Rechtfertigung der Schutzpflichten ebenso zu berücksichtigen sein, wie die Wertungen, die sich allgemein aus den oben skizzierten datenschutzrechtlichen Bestimmungen ergeben.

---

[412] *Gschnitzer* in *Klang/Gschnitzer,* ABGB IV/1^2 (1968) 473.

5.5. Schutzpflichten als Informationspflichten

5.5.1. Gesetzliche Auskunftspflichten

5.5.1.1. § 24 DSG 2000

An gesetzlichen Auskunftspflichten ist zunächst an § 24 DSG 2000 zu denken, der wie oben geschildert (Kapitel 4.5.5), parallel zu den in § 96 Abs 3 normierten Informationspflichten zu beachten ist. Während § 24 Abs 1 DSG 2000 zur Erteilung von Informationen verpflichtet, die schon nach § 96 Abs 3 TKG 2003 zu erteilen sind, sieht § 24 Abs 2 DSG 2000 vor, dass über Abs 1 leg cit hinaus gehende Informationen zu erteilen sind, wenn dies für eine Verarbeitung nach Treu und Glauben erforderlich ist. Fraglich ist nun, ob daraus abgeleitet werden kann, dass der Access-Provider seinen Kunden über an Dritte erteilte Auskünfte zu informieren hat. Ziel dieser Informationsverpflichtung ist es, dass der Betroffene von der Verwendung seiner Daten erfährt und umfassend über die Bedingungen der Erhebung informiert wird[413]. Dadurch soll es dem Betroffenen erleichtert werden seine Rechte zu wahren[414].

Aus Abs 3 leg cit ergibt sich, dass diejenigen, die Daten aus Datenanwendungen anderer Auftraggeber ermitteln, den Betroffenen nicht zu informieren haben, wenn die Datenverwendung gesetzlich vorgesehen ist. Das bedeutet, dass denjenigen, der vom Access-Provider gestützt auf eine gesetzliche Grundlage beauskunftet wird, keine Informationspflicht trifft. Darauf stützt sich auch die Rechtsansicht des BMI, dass die Sicherheitsbehörden bei Auskünften gem § 53 Abs 3a bzw 3b SPG keine Informationspflicht gegenüber dem Betroffenen besteht[415]. Wenn schon derjenige, der die Daten ermittelt, im Falle gesetzlicher Auskunftspflichten von der Informationspflicht befreit ist, muss dies eigentlich noch viel mehr für den Access-Provider gelten, der die Information schließlich nicht selbst initiiert.

Hinzukommt, dass zumindest § 24 Abs 1 DSG 2000 eindeutig vorschreibt, dass die Information aus Anlass der Ermittlung zu geben ist und somit keinesfalls später als zum Ermittlungszeitpunkt[416]. Auch aus Abs 3 leg cit ergibt sich, dass der Gesetzgeber hier eine Informationsverpflichtung statuieren wollte, die stets nur aus Anlass der Datenermittlungen greifen soll. Abs 2 leg cit will in bestimmten Fällen, in denen dies nach

---

[413] Vgl auch Erwägungsgrund 38 zur allgemeinen Datenschutzrichtlinie.

[414] RV 1316 BlgNR XX. GP, 45.

[415] 4148/AB XXIII. GP, 2, siehe dazu schon oben Kapitel 4.5.5.

[416] *Dohr/Pollirer/Weiss/Knyrim,* Datenschutzrecht[2] (2009), Grundlieferung, § 24 Anm 3.

Treu und Glauben geboten ist, dem Betroffenen mehr Informationen zukommen lassen, als in Abs 1 leg cit vorgesehen. Dabei soll jedoch nach der auf Abs 1 Bezug nehmenden Formulierung nichts am grundsätzlichen Auslöser der Informationsverpflichtung, nämlich der Ermittlung von Daten, geändert werden. Daraus folgt mE, dass sich aus Abs 2 leg cit – anders als im Falle § 96 Abs 3 TKG – keine Informationspflicht für den Fall ergibt, dass der Access-Provider Daten in Erfüllung eines gesetzlichen Auskunftsanspruches übermittelt. Zu diesem Zeitpunkt hat er die Daten bereits längst ermittelt und den Betroffenen darüber auch bereits informiert[417].

5.5.1.2. § 96 Abs 3 TKG 2003

Inwieweit aus § 96 Abs 3 TKG 2003 Informationspflichten abgeleitet werden können, wurde bereits oben (siehe Kapitel 4.5.5) behandelt. Zusammenfassend ist hier nochmals kurz festzuhalten, dass eine am Wortlaut und am telos dieser Bestimmung orientierte Auslegung zum Ergebnis führt, dass diese Bestimmung den Anbieter in jenen Fällen zur Information über die bevorstehende Datenübermittlung verpflichtet, in denen dies möglich ist, ohne den Zweck der Auskunftsbestimmungen zu gefährden. Auf den Umstand, dass dies eine Auslegung ist, die in praxi bislang trotz des eindeutigen Wortlauts noch nie angedacht wurde, ist bereits oben hingewiesen worden.

5.5.2. Grundlegendes zur Entwicklung von Nebenpflichten durch ergänzende Vertragsauslegung

Die einfache Vertragsauslegung steht am Anfang jedes Interpretationsvorgangs. Eine Durchsicht der AGB der größten Access-Provider in Österreich ergibt jedoch, dass keines dieser Unternehmen die Frage, ob der Kunde über die Erteilung einer Auskunft zu informieren ist, in seinen Vertragsbestimmungen geregelt hat. Die AGB der Hutchison 3G Austria GmbH[418] enthalten zwar in Punkt 26.1. einen Hinweis, dass aus der Weitergabe von Daten aufgrund gesetzlicher Verpflichtung der Kunde keine Ansprüche ableiten kann. Selbst diese Bestimmung erweist sich jedoch als lückenhaft, lässt sie doch beispielsweise jene Fälle ungeregelt, in denen die gesetzliche Verpflichtung zur Weitergabe der Daten gerade nicht besteht und der Access-Provider dies sorgfaltswidrig nicht erkennt und die Daten dennoch übermittelt.

---

[417] So auch *Feiler,* Security Breach Notification, in *Feiler/Raschhofer (Hrsg),* Innovation und internationale Rechtspraxis, Praxisschrift für Wolfgang Zankl (2009) 147 (149).

[418] Abrufbar unter: http://www.drei.at/portal/media/960/metadanavigation/agbs/AGBII_Sept2008_layouted.pdf (Stand April 2010).

Außerdem fehlt es – abgesehen von der erwähnten Auslegung der Informationsverpflichtung gem § 96 Abs 3 TKG 2003 – auch an gesetzlichen Bestimmungen hinsichtlich dieser Frage. Dennoch gibt es eine Reihe bereits erwähnter Bestimmungen, die darauf abzielen, den Betroffenen über die ihn betreffenden Datenverwendungen stets umfassend in Kenntnis zu setzen. Datenverarbeitung nach Treu und Glauben setzt voraus, dass die betroffenen Personen in der Lage sind, das Vorhandensein einer Verarbeitung zu erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert zu werden, wenn Daten bei ihnen erhoben werden[419]. Dabei handelt es sich um ein fundamentales Prinzip des gesamten Datenschutzrechts, das sich in einer Vielzahl von Vorschriften widerspiegelt. Von diesem Grundsatz darf grob gesagt nur abgegangen werden, wenn dies im Interesse des Betroffenen geschieht oder überwiegende öffentliche Interessen oder die überwiegenden Interessen eines Dritten dies erfordern (vgl auch § 1 DSG 2000).

Für Fälle, für welche die Parteien keine Vereinbarung getroffen haben, ist der Vertrag ergänzend auszulegen. Es ist zu fragen, was die konkreten Parteien vereinbart hätten, wenn sie die ungeregelte Situation vorhergesehen hätten (hypothetischer Parteiwille)[420].

Das Kriterium der Unvorhersehbarkeit darf nicht überstrapaziert werden. So gibt es eine Reihe von Entscheidungen, in denen der OGH durch ergänzende Vertragsauslegung Sachverhaltsentwicklungen einer Regelung zuführte, die bei Vertragsabschluss sehr wohl vorhersehbar waren. Das berühmteste Beispiel ist wohl die durch ergänzende Vertragsauslegung konstruierte Nebenpflicht des Verkäufers eines Kraftfahrzeuges, dem Käufer einen urkundlichen Nachweis des Eigentumsüberganges zu verschaffen[421]. Dass er diese Papiere zur Anmeldung des Fahrzeuges benötigen wird, konnte der Käufer wohl auch bereits zum Zeitpunkt des Vertragsabschlusses erkennen. Dass auf die Anschaffung die Anmeldung eines Fahrzeuges folgt, entspricht dem typischen Verlauf und ist daher sicher kein unvorhergesehenes Ereignis. Gleiches gilt für sämtliche von der Judikatur anerkannten Konkurrenzverbote, soweit sie im Rahmen ergänzender Vertragsauslegung gewonnen werden[422] sowie für die Nebenpflicht, eine

---

[419] Erwägungsgrund 38 zur allgemeinen Datenschutzrichtlinie. Zu den zulässigen Ausnahmen im Interesse des Betroffenen oder zur Wahrung überwiegender Interessen Dritter bzw öffentliche Interessen siehe die Erwägungsgründe 42 und 43.

[420] *Gschnitzer* in *Klang/Gschnitzer,* ABGB IV/1^2 (1968) 408; *Binder* in *Schwimann,* ABGB IV^3 (2006) § 915 Rz 178.

[421] OGH 26. 9. 1951, 3 Ob 500/51, SZ 24/248.

[422] Vgl etwa OGH 14. 6. 1988 4 Ob 33/88, SZ 61/145 = MR 1988, 122.

Bedienungsanleitung mitzuliefern[423]. In keinem dieser Fälle wird man ernsthaft behaupten können, dass der Gläubiger der Schutzpflicht unter keinen Umständen seine missliche Situation, in der er ohne die Konstruktion einer Schutzpflicht wäre, nicht vorhersehen konnte. Das Vertragsverhältnis wird so nicht ob eines unvorhersehbaren sondern schlicht wegen eines von den Parteien *übersehenen* Problems ergänzt. Genau so scheint es *Gschnitzer* zu sehen, wenn er meint, dass die ergänzende Vertragsauslegung in solchen Lagen zur Anwendung komme, „die die Parteien nicht voraussahen, vielleicht gar nicht voraussehen konnten"[424]. Dass zum Zeitpunkt des Vertragsabschlusses zwischen dem Access-Provider und seinem Kunden beiden bereits bekannt war, dass ersterer möglicherweise von Dritten zu einer Auskunft verhalten wird, liegt ebenfalls auf der Hand. Daraus darf aber vor dem Hintergrund der erwähnten Judikatur keinesfalls geschlossen werden, dass dadurch die Möglichkeit der Gewinnung von Schutzpflichten durch ergänzende Vertragsauslegung eliminiert wird.

Aus dem Umstand alleine, dass die Parteien den Sachverhalt keiner Regelung zuführten, darf keinesfalls ohne weiteres geschlossen werden, dass dies planmäßig, dh die Lücke voraussehend, erfolgte. Dies ist schon deshalb unwahrscheinlich, weil das Fehlen einer entsprechenden Regelung ohne Korrektur meist zu einer einseitigen Belastung führt[425] und dies nicht im Plan beider Parteien vorgesehen sein kann[426]. Andererseits darf das richterliche Aufdrängen einer Regelung, welche die Parteien nicht gewollt haben, auch nicht zu einer Erweiterung des Vertragsgegenstandes führen[427]. Die von *Kerschner* erhobene Forderung, dass für die für die ergänzende Vertragsauslegung maßgeblichen Kriterien immer dem Vertrag selbst zu entnehmen sein müssen und stets konkrete Hinweise im Vertrag bzw in seinem Umfeld zu verlangen seien[428], geht zu weit[429]. Durch ergänzende Vertragsauslegung sollen ja genau jene Fälle

---

[423] OGH 3. 5. 1994, 1 Ob 555/94.

[424] *Gschnitzer* in *Klang/Gschnitzer,* ABGB IV/1^2 (1968) 408; Auch die Formulierung *Zeillers,* Commentar über das allgemeine bürgerliche Gesetzbuch für die gesammten deutschen Erbländer der oesterreichischen Monarchie I, 1811, 71, schließt diese Sichtweise nicht aus: „was sie wenn ihnen der zweifelhafte Fall vorgeschwebt hätte, bei einer (vorauszusetzenden) rechtlichen und billigen Denkungsart ausdrücklich verabredet haben würden."

[425] *Dullinger*, Kommentar zu OGH 4. 3. 1986, 14 Ob 12/8, ZAS 1987, 93 (96).

[426] Andererseits muss bei der Beurteilung, ob eine Lücke vorliegt und damit der Vertrag ergänzend ausgelegt werden darf, auch stets berücksichtigt werden, wer am Vertragsabschluss beteiligt war. Je mehr Expertise die Parteien hinsichtlich des Vertragsgegenstandes haben, desto unwahrscheinlicher erscheint eine planwidrige Lücke: OGH 13.5.1953, 3 Ob 207/53 und 3 Ob 208/53, ÖBl 1953, 41.

[427] *Busche* in *Säcker/Rixecker* (Hrsg)*,* Münchener Kommentar zum Bürgerlichen Gesetzbuch I^5 (2006) § 157 Rz 55 mwN.

[428] *Kerschner,* Wegfall der Geschäftsgrundlage bei unwiderruflichen Sozialleistungen, wbl 1988, 211 (217).

einer Regelung zugeführt werden, die von den Parteien nicht vorausgesehen wurden und für die es daher keine Kriterien gibt. Für die Vielzahl von durch ergänzende Vertragsauslegung gewonnenen Nebenpflichten[430] gibt es häufig nicht den geringsten konkreten Anhaltspunkt im faktischen Parteiwillen, sondern ergeben sich diese meist aus reinen Billigkeitserwägungen.

Der hypothetische Wille ist unter Würdigung der beim Vertragsabschluss maßgeblichen Umstände sowie der Natur des Geschäfts, dessen Zwecks, des gesamten Sinnzusammenhangs[431] und der Interessenlagen zu finden. Zudem hat sich die ergänzende Vertragsauslegung an der Übung des redlichen Verkehrs[432] und am Prinzip von Treu und Glauben[433] zu orientieren[434]. Soweit erkennbar, gibt es jedoch in Österreich hinsichtlich der hier interessierenden Frage keine Verkehrsübung. Wie die verschiedenen Access-Provider in der Praxis mit Auskunftsbegehren bzw deren Rechtsgrundlagen umgehen, ist soweit ersichtlich noch nie umfassend erhoben worden. Während manche Access-Provider sogar gegen aus ihrer Sicht grundrechtliche bedenkliche Bestimmungen (§ 53 Abs 3a und 3b SPG idF BGBl I 114/2007) vor dem VfGH mittels Individualantrag juristisch zu Felde ziehen[435], ist die Praxis der anderen im Falle von Auskunftsbegehren überhaupt nicht bekannt. Möglicherweise wird es aber auch solche geben, die um Schwierigkeiten mit der Auskunft suchenden Stelle zu vermeiden, anstandslos beauskunften und ihre Kunden nicht informieren um Schwierigkeiten mit diesen zu entgehen. Mangels einschlägiger Verkehrssitten wird man aus diesen keine Verpflichtung des Providers ableiten können, seine Kunden über die Erfüllung von Auskunftsbegehren gegenüber Dritten zu informieren. Daher sind hier in erster Linie der hypothetische Parteiwille und das Prinzip von Treu und Glauben maßgeblich[436]. Das eröffnet natürlich innerhalb der Grenzen der Billigkeit einen gewissen Interpretationsspielraum, was auch Gefahren willkürlicher Entscheidungen in sich birgt. Die Grenzen zwischen den einzelnen Auslegungsmitteln können dabei verschwimmen, da

---

429 So auch *Helmut Böhm*, Die "Altlastensanierung" als Problem ergänzender Vertragsauslegung bzw des Wegfalls der Geschäftsgrundlage, ÖZW 1990, 104 (105).

430 Vgl dazu hinsichtlich des Kaufvertrages etwa *Aicher* in Rummel, ABGB I³ (2000) § 1061 Rz 28ff.

431 *Larenz,* Methodenlehre der Rechtswissenschaft⁵ (1983) 287.

432 25. 4. 1963, 6 Ob 86/63, SZ 36/68; 15. 3. 1972, 1 Ob 14/72, SZ 49/86; 10.7.1997, 2 Ob 2133/96g uva.

433 OGH 29.6.1976, 5 Ob 550/76, SZ 49/86.

434 Vgl auch *Rummel* in Rummel, ABGB I³ (2000) § 914 Rz 11ff.

435 T-Mobile, vgl VfGH 1.7.2009, G 31/08 – G 29/08, G 30/08, G 35/08, G 147/08; http://futurezone.orf.at/stories/1618835/ (Stand April 2010).

436 *Rummel* in Rummel, ABGB I³ (2000) § 914 Rz 17.

der Richter, der bestimmt, was die Parteien gewollt hätten, sich stets auch vom Gedanken an Treu und Glauben leisten lassen wird (und muss, siehe dazu sogleich), dabei jedoch keinesfalls eigene Wertungen an die jener der Parteien setzen darf[437], selbst wenn die Vereinbarungen der Parteien unbillig erscheinen[438]. Bei der Beantwortung der Frage, was die konkreten Parteien das fragliche Problem vorhersehend vereinbart hätten, werden Anhaltspunkte für unredliche Absichten nicht berücksichtigt werden dürfen. Diese Erkenntnis wirkt sich, wie noch sogleich zu zeigen sein wird, entscheidend auf die Ergebnisse der Vertragsergänzung aus.

5.5.3. Die Redlichkeit als Dreh- und Angelpunkt ergänzender Vertragsauslegung

Ein unredlicher dem Prinzip von Treu und Glauben widersprechender hypothetischer Parteiwille kann als Ergebnis ergänzender Vertragsauslegung nicht akzeptiert werden. Auch in der Judikatur wird stets nur nach einem redlichen hypothetischen Parteiwillen gesucht[439].

> Beispiel: Nach einem Bericht der Frankfurter Rundschau hat die deutsche Telekom-AG nach Angaben des Bundeskriminalamtes nach den Terroranschlägen auf das World Trade Center und andere Ziele am 9.11.2001 Millionen von Kundendaten ohne jegliche Rechtsgrundlage für Rasterfahndungen zur Verfügung gestellt[440]. Im Rahmen der ergänzenden Vertragsauslegung stellt sich nun die Frage, ob dieses Unternehmen bereit gewesen wäre, sich vertraglich zu einer Information eines Kunden über erfolgte Datenübermittlungen zu verpflichten. Dass der Kunde einer derartigen ihn nur berechtigenden Klausel zugestimmt hätte, liegt auf der Hand. Die Beantwortung der Frage nach dem hypothetischen Willen der deutschen Telekom AG hängt davon ab, inwieweit man bereit ist, Anhaltspunkte für unredliche Absichten zu berücksichtigen. Wenn man als Ergebnis nur zulassen möchte, was *redliche* Parteien miteinander vereinbart hätten, darf der Umgang der Kundendaten der Telekom AG zur Erforschung des hypothetischen Parteiwillens nicht berücksichtigt werden. Stellt man bei der Erforschung des hypothetischen Parteiwillens jedoch auch auf Indizien für unredliche Absichten ab, wird man auch den Umgang mit den Kundendaten zu berücksichtigen haben. Diesfalls wird die Begründung von für den Kunden günstigen datenschutzrechtlichen Verpflichtungen im Rahmen der ergänzenden Vertragsauslegung schwierig.

---

437 *Larenz,* Methodenlehre der Rechtswissenschaft[5] (1983) 288; OGH 29.7.1977 5 Ob 891/76; HS X/XI 11.103;

438 OGH 07.12.1995, 2 Ob 89/95.

439 Vgl etwa OGH 31.5.1983, 5 Ob 714/81, JBl 1983, 592: „*Treten nach Abschluss eines Geschäfts Konfliktfälle auf, die bei Abschluss von den Parteien nicht bedacht und daher auch nicht geregelt wurden, so ist unter Berücksichtigung des von Parteien verfolgten Zwecks zu fragen, welche Lösung redliche und vernünftige Parteien vereinbart hätten.*"

440 Artikel abrufbar unter: http://www.fr-online.de/in_und_ausland/politik/aktuell/1707357_Bundeskriminalamt-Rasterfahndung-mit-Telekom-Daten.html&em_comment_page=2 (Stand April 2010).

Ein Unternehmen, das ohne entsprechender gesetzlicher Verpflichtung Millionen von Kundendaten ohne weiteres herausgibt, hat realistischerweise wohl wenig Interesse an für den Kunden günstigen Klauseln im Bereich des Datenschutzes.

Obwohl § 914 ABGB anders als das BGB (§ 157) das Prinzip von Treu und Glauben nicht ausdrücklich anordnet, ist es auch in Österreich zu beachten und Ergebnisse, die diesem Prinzip widersprechen, sind daher zu vermeiden. Daher fragt die Judikatur zutreffend nur danach, welche Lösung vernünftige und redliche Parteien vereinbart hätten[441].

Die Lückenschließung hat nach hM auch durch Berücksichtigung des dispositiven Gesetzesrechts[442], wobei auch unter Umständen Analogien zu Gesetzesbestimmungen[443] zu beachten sind, zu erfolgen. Nach Rummel nimmt die ergänzende Vertagsauslegung eine Mittelstellung zwischen Vertrags- und Gesetzesauslegung ein[444]. Nach der Rechtsprechung entsprechen die gesetzlichen Regelungen Im Regelfall dem hypothetischen Parteiwillen[445]. Dies ist nur dann zu bezweifeln, wenn klar erkennbar ist, dass die Parteien eine vom positiven Recht abweichende Lösung angestrebt haben, für den fraglichen Sachverhalt jedoch letztlich keine Regelung trafen. Insbesondere in diesen Fällen stellt sich die Frage nach einer Rangfolge der Mittel ergänzender Vertragsauslegung.

5.5.4. Das Verhältnis der einzelnen Methoden ergänzender Vertragsauslegung

Entscheidend für das Ergebnis der Vertragsergänzung sind sowohl die Wahl als auch das Verhältnis der einzelnen Methoden untereinander. *Rummel* lehnt eine Rangfolge der Auslegungsmittel (hypothetischer Parteiwille, Verkehrssitte, Treu und Glauben) mit Verweis auf das Verhältnis der Auslegungsmethoden von Gesetzesrecht grundsätzlich ab[446]. Demgegenüber meint *Böhm,* dass nach Anhaltspunkten im sonstigen Vertragstext und sonstigen Indizien für den faktischen Parteiwillen zunächst der

---

441 OGH 29.6.1976, 5 Ob 550/76, SZ 49/86; vgl auch *Larenz*, Allgemeiner Teil des deutschen bürgerlichen Rechts[7], , 1989, 541.

442 *Kerschner,* Wegfall der Geschäftsgrundlage bei unwiderruflichen Sozialleistungen, wbl 1988, 211 (216).

443 *Binder* in *Schwimann,* ABGB IV[3] (2006) § 914 Rz 178.

444 *Rummel* in Rummel*,* ABGB I[3] (2000) § 914 Rz 9.

445 OGH 20.6.1989, 5Ob617/88, JBl 1990, 105.

446 *Rummel* in Rummel*,* ABGB I[3] (2000) § 914 Rz 11; hinsichtlich des Verhältnisses von Verkehrssitte und dispositivem Recht nimmt er jedoch einen Vorrang des letzteren an, da es bei Vorliegen einer dispositiven Norm an der Lücke und sohin an der Voraussetzung ergänzender Vertragsauslegung schlechthin mangele.

hypothetische Wille der konkreten Parteien, sodann das, was vernünftige und redliche Parteien vereinbart hätten und erst zuletzt das dispositive Gesetzesrecht zu beachten sei[447]. Dem ist jedoch nicht zuzustimmen. Geradezu das Gegenteil ist der Fall. Auf den ersten Blick scheint die Behauptung, dass der faktische Parteiwille an erster Stelle zu beachten ist, überzeugend, da es ja hier um die Auslegung von Rechtsgeschäften geht, die im Rahmen der Privatautonomie zustande kamen. Maßgeblich soll daher primär das sein, was die Parteien wollten. Der freilich zu befürwortende dahinter stehende Gedanke ist, den Parteiwillen aufgrund des Prinzips der Privatautonomie so weit nur irgendwie möglich, zu berücksichtigen[448]. Voraussetzung dafür, dass ein Vertrag ergänzend ausgelegt wird, ist aber nun einmal der Mangel privatautonomer Rechtsgestaltung hinsichtlich bestimmter Punkte. Fraglich ist daher, wie viel für die Bestimmung des faktischen Parteiwillens überhaupt aus den vorhandenen Vertragsbestimmungen und den Umständen zu gewinnen ist. Ableitungen aus dem artikulierten faktischen Parteiwillen für ungeregelte Fragen können nur nach wertenden und niemals nach logischen Maßstäben erfolgen. Eine logische Subsumtion des Sachverhaltes unter eine bestimmte von Parteien beschlossene Regelung ist eben naturgemäß nicht möglich! Mangels Deduktion einer Vertragsbestimmung auf einen Sachverhalt fragt man daher nach einer Gesamtbetrachtung aller vorhandenen Bestimmungen, welche Wertungen der Vertragsparteien grundsätzlich erkennbar werden. Dabei kann schon die Auswahl jener Bestimmungen und Umstände, aus denen man etwas über den hypothetischen Willen zu erfahren hofft, nur willkürlich sein.

Dies gilt insbesondere in Bezug auf die Vereinbarungen hinsichtlich der Privatsphäre zwischen Kunden und Access-Provider. Die meisten AGB der größten Access-Provider in Österreich enthalten mehr oder minder umfangreiche Klauseln zum Datenschutz, wobei die Frage, ob Kunden über Auskunftserteilungen zu informieren sind, wie erwähnt nicht geregelt wird. Wer sich am artikulierten vor allem in den vorhandenen Vertragsklauseln zum Ausdruck kommenden Parteiwillen orientieren will, hat zunächst das Problem, überhaupt aussagekräftige Normen zu finden[449]. Wenn es heißt, man müsse sich bei der ergänzenden Vertragsauslegung an die Richtlinien halten, die sich aus

---

[447] *Helmut Böhm*, Die "Altlastensanierung" als Problem ergänzender Vertragsauslegung bzw des Wegfalls der Geschäftsgrundlage, ÖZW 1990, 104 (105ff).

[448] Ein ähnliches Konzept, bei welchem man sich die Auslegung je nach Feststellbarkeit des Parteiwillens schrittweise von diesem entfernt schlägt auch *Gschnitzer* in *Klang/Gschnitzer,* ABGB IV/1^2 (1968) 411, vor: „Beachtung des buchstäblichen Sinnes des Ausdrucks; Erforschung des Parteiwillens; seine Ergänzung und Korrektur; schließlich seine Vernichtung – das ist eine Reihe von immer einschneidernden Mitteln, bei denen das schärfere erst verwendet werden darf, wenn das mildere nicht mehr zum Ziele führt."

[449] Ebenso *Gschnitzer* in *Klang/Gschnitzer,* ABGB IV/1^2 (1968) 408 mit weiteren einleuchtenden Beispielen.

den im Vertrag geregelten Verhältnissen ergeben[450], so stellt sich die Frage, welche der sämtlichen geregelten Punkte es sind, an denen man sich orientieren soll. Anders als die Rechtsordnung, die eine Vielzahl von Bestimmungen enthält, aus denen tatsächlich Wertungen des Gesetzgebers oft recht klar erkennbar werden, umfassen die AGB typischer Verträge über die Erbringung von Kommunikationsdiensten meist nur wenige Druckseiten. Für Rückschlüsse auf den hypothetischen Parteiwillen hat man daher eigentlich nur die Wahl aus einer Reihe von meist recht unpassenden Klauseln. Je spezifischer die im Rahmen der ergänzenden Vertragsauslegung aufgeworfene Fragestellung ist, desto deutlicher tritt dieses Problem zu Tage. Welche Bestimmungen bzw Umstände sind zu berücksichtigen? Soll man etwa aus einer oberflächlichen Regelung des Datenschutzes auf eine prinzipielle Neigung des Access-Providers zu einer diesbezüglich eher kundenfeindlichen Haltung schließen? Oder soll man das Vertragswerk insgesamt betrachten und bei vergleichsweise kundenfreundlichen Verträgen annehmen, dass der Access-Provider auch im Bereich der Informationspflichten stets nur die kundenfreundlichste Lösung will? Auch der Blick auf die sonstigen Umstände, die nach hM[451] zur Erforschung des faktischen Parteiwillens zu berücksichtigen sind, ist möglich: So könnte man etwa behaupten, dass sich ein Access-Provider, der damit wirbt, besonderes Augenmerk auf seinen Servicebereich zu legen, auch zu einer Information des Kunden über die Erfüllung von Auskunftsbegehren verpflichtet hätte, wenn er das Problem ausdrücklich geregelt hätte. Die gezeigten Argumente sind einander bei logischer Betrachtungsweise völlig gleichwertig, keines von ihnen ist logisch „richtiger". Letztlich wird es also darauf ankommen, welches Argument dem Richter am meisten einleuchtet. Es besteht daher in diesem Bereich die Gefahr mehr oder weniger willkürlicher Entscheidungen[452].

Das Problem eingeschränkter Nachvollziehbarkeit ist dem Konzept ergänzender Vertragsauslegung immanent, lässt das Gesetz doch den Rückgriff auf ungeschriebene Normen zu, aus denen konkrete Verpflichtungen der Parteien abgeleitet werden sollen. Dass dies zu Entscheidungen führt, die ausschließlich nur mehr nach wertenden Gesichtspunkten getroffen werden können, hat der Gesetzgeber sehenden Auges in Kauf genommen.

Das von *Böhm* vorgeschlagene dreistufige Konzept erweist jedoch auch aus einem anderen Grund als nicht besonders praktikabel. So stellt sich die Frage, wodurch

---

[450] OGH 16.6.1987, 4 Ob 362/85, wbl 1987, 240.

[451] *Binder* in *Schwimann,* ABGB IV[3] (2006) § 914 Rz 180; *Rummel* in Rummel*,* ABGB I[3] (2000) § 914 Rz 11; *Kerschner,* Wegfall der Geschäftsgrundlage bei unwiderruflichen Sozialleistungen, wbl 1988, 211 (217).

[452] *Kerschner,* Wegfall der Geschäftsgrundlage bei unwiderruflichen Sozialleistungen, wbl 1988, 211 (217) FN 36.

sich die von ihm angeführten Stufen voneinander abgrenzen lassen. Wo liegen etwa in praxi die Unterschiede zwischen dem, was die konkreten Parteien vereinbart hätten und dem vernünftigen Ausgleich so wie ihn „redliche und vernünftige Parteien" beschlossen hätten, wenn man auch auf der ersteren Stufe nur redliche Absichten zulässt. *Böhm* selbst räumt ein, dass Treu und Glauben sowie die Verkehrssitte auch auf den ersten beiden Ebenen der Vertragsauslegung eine Rolle spielen und damit auch Maßstäbe für die Ermittlung des vermutlichen Parteiwillens darstellen[453]. Das bedeutet, dass auch auf jener Stufe, wo danach gefragt wird, was die konkreten Parteien vereinbart hätten, nur redliche Absichten der Parteien berücksichtigt werden dürfen. Dadurch sind aber keine Unterschiede mehr zwischen den beiden ersten von ihm skizzierten Stufen erkennbar. Sobald man Treu und Glauben in die „Gewinnung" des konkreten hypothetischen Parteiwillens einfließen lässt, objektiviert man bereits und der vermutete Parteiwille wird zum normativen Kriterium[454]. Das von ihm skizzierte Konzept dient zwar dem berechtigten Anliegen, den Willen der Parteien so weit wie nur möglich zu berücksichtigen, erweist sich jedoch für die praktische Handhabung als zu ziseliert. Das Ziel, die Privatautonomie der Parteien vor einer zu großen Einflussnahme durch den wertenden Richter zu schützen, lässt sich nur begrenzt verwirklichen. Wo keine Regelung vorhanden ist, muss diese nun einmal vom Richter nach wertenden Maßstäben entwickelt werden. Soweit möglich, sollte dabei jedoch auf bereits bekannte aus der Rechtsordnung klar ableitbare Wertungen abgestellt werden. Wie bereits mehrfach erwähnt, durchzieht das gesamte europaweit weitestgehend harmonisierte Datenschutzrecht, das fundamentale Prinzip, dass der Betroffene stets – soweit möglich – über die ihn betreffenden Datenverwendungen in Kenntnis sein soll, damit er seine Rechte ausreichend wahren kann. Diesem Ziel dienen zahlreiche Bestimmungen des Datenschutzgesetzes (insbesondere die §§ 16-26). Soweit Auskunftsbestimmungen betroffen sind, bei denen der Staat in die Rechte seiner Bürger eingreift, ist überdies an das rechtsstaatliche Prinzip zu denken. Nach diesem müssen Entscheidungen der Verwaltungsbehörden überprüfbar sein und zur Wahrung der Verfassung und der Gesetze einer Kontrolle unterzogen werden können[455].

Im Folgenden wird daher davon ausgegangen, dass die einzelnen zur Bestimmung des hypothetischen Parteilwillens verwendeten Methoden einander gleichrangig sind.

---

[453] *Helmut Böhm*, Die "Altlastensanierung" als Problem ergänzender Vertragsauslegung bzw des Wegfalls der Geschäftsgrundlage, ÖZW 1990, 104 (106).

[454] *Larenz*, Allgemeiner Teil des deutschen bürgerlichen Rechts[7], , 1989, 542.

[455] VfGH, 1.7.1994, G92/94, G93/94.

5.5.5. Die Rolle des Gesetzesrechts bei der ergänzenden Auslegung von Verträgen

Das Problem, dass man bei der Vertragsergänzung das Regime logischer Subsumtion außer Acht lassen und stattdessen Wertungen einfließen lassen muss, hat man natürlich auch, wenn man zur Erforschung dessen, was redliche und vernünftige Parteien vereinbart hätten, sein Augenmerk vorwiegend auf das Gesetzesrecht legt. Will man aus dem Gesetzesrecht Wertungen des Gesetzgebers herauslesen, um diese für die ergänzende Vertragsauslegung nutzbar zu machen, stößt man ebenfalls oft an die Grenzen exakter Nachvollziehbarkeit. Dennoch wird man häufig für den ungeregelten Sachverhalt viel einschlägigere Normen finden, da die Auswahl aus entsprechenden Normen schlicht viel größer ist. Daher scheint es ratsam, Gesetzesrecht nicht an letzter Stelle zu beachten. Will der Richter eine am Prinzip von Treu und Glauben orientierte Entscheidung treffen, ist er gut beraten, seine Begründung durch Bezugnahme auf einschlägige positive Normen nachvollziehbarer zu machen. Die dahinter stehenden Wertungen des Gesetzgebers lassen sich aus den Materialien meist einfacher und mit höherer Treffsicherheit ableiten. Einem Richter, der begründend auf klar erkennbare gesetzgeberische Wertungen verweisen kann, wird man schwerer den Vorwurf machen können, eigene Wertungen an Stelle jener der Parteien gesetzt zu haben[456].

Aus den einschlägigen Bestimmungen der Rechtsordnung lassen sich meist recht deutlich Wertungen des Gesetzgebers ableiten, die für die Bestimmung des hypothetischen Willens nutzbar gemacht werden können. Im Einzelfall kann es ausnahmsweise klare Anhaltspunkte geben, wie die hier interessierende Frage von den Parteien geregelt worden wäre. Solche Anhaltspunkte könnten sich etwa aus den AGB ergeben. Der klar erkennbare faktische Wille der Parteien steht einem in eine andere Richtung weisenden Ergebnis nach Treu und Glauben entgegen[457].

5.5.6. Die Schutzpflicht, den Kunden über die Erfüllung von Auskunftsbegehren zu informieren.

Die Pflicht des Access-Providers, den Kunden über die Erfüllung eines Auskunftsbegehrens zu informieren, kann als Benachrichtigungspflicht[458] oder als

---

[456] Vgl zum in dieser Hinsicht ähnlichen Problem der Lückenfüllung durch analoge Rechtanwendung *Zankl,* Bürgerliches Recht[5] (2010) Rz 16.

[457] Dem faktischen Willen kommt hinsichtlich der ergänzenden Vertragsauslegung somit sowohl begrenzende als auch steuernde Funktion zu: siehe *Mayer-Maly,* Die Bedeutung des tatsächlichen Parteiwillens für den hypothetischen, in *Jakobs/Knobbe-Keuk/Picker/Wilhelm,* Festschrift für Werner Flume zum 70. Geburtstag (1978) 621 (623ff).

[458] Diese Begrifflichkeit ist angelehnt an *Köpcke,* Typen der positiven Vertragsverletzung (1965) 104ff.

Auskunftspflicht verstanden werden. Nach ersterer hätte der Access-Provider ungefragt von sich aus seinen Kunden über die Erteilung von Auskünften an Dritte zu informieren. Die Pflicht, den Kunden nur auf dessen Nachfrage über die Erteilung von Auskünften zu informieren, kann als Auskunftspflicht bezeichnet werden. Bejaht man im Wege der ergänzenden Vertragsauslegung bereits eine Benachrichtigungspflicht, erübrigt sich die Frage nach einer Auskunftspflicht. Diese Terminologie ergibt sich nicht aus der Rechtsordnung, ist aber geeignet die qualitativen Unterschiede zum Ausdruck zu bringen. Die bloße Auskunftspflicht ist im Vergleich zur Benachrichtigungspflicht in qualitativer Hinsicht ein Minus, weil diese kein aktives Tätigwerden des Providers verlangt.

Wie *Graf* richtig beschreibt, geht es in der Praxis bei der ergänzenden Vertragsauslegung darum, die Interessen jener Partei zu schützen, zu deren Gunsten die Ergänzung stattfindet und die es verabsäumte, ihre Interessen adäquat abzusichern[459]. So wird zum Beispiel der Pflichtenkatalog des Verkäufers, der aufgrund der qua Vertragsergänzung gewonnenen Nebenpflicht auch die Fahrzeugpapiere aushändigen muss, im Interesse des Käufers einseitig erweitert. Hätte man den Kunden zum Zeitpunkt des Vertragsabschlusses gefragt, ob er sich im Rahmen des gesetzlich zulässigen ausbedingen möchte, dass der Access-Provider ihn über die Erfüllung von Auskunftsbegehren informieren soll, hätte er diese Frage gewiss bejaht. Zu fragen ist aber auch nach dem hypothetischen Willen des Access-Providers. Dabei ist jedoch wie oben dargelegt zu beachten, dass nur billige Absichten des Access-Providers zu berücksichtigen sind. Weiters darf auch die wirtschaftliche Überlegenheit des Access-Providers nicht berücksichtigt werden[460], auch wenn er es gewesen wäre, der die konkrete Klausel ausformuliert hätte. Das Argument, dass der Access-Provider, nie eine einseitig verpflichtende Klausel in sein Vertragswerk aufgenommen hätte, weil er selbst es ja ist, der die AGB formuliert, ist daher unzulässig. Vielmehr ist danach zu fragen, ob der redliche Access-Provider sich einer derartigen Pflicht unterworfen hätte.

Graf leitet aus dem Umstand, dass in unserer Rechtsordnung die ergänzende Vertragsauslegung zulässig ist, folgerichtig ab, dass sie jene Interessen des Gläubigers, zu deren Schutz die Vertragsergänzung stattfindet, höher bewertet, als das Interesse des Schuldners nicht mit einer weiteren Schutzpflicht belastet zu werden[461]. Andernfalls dürften nur die ausdrücklich oder schlüssig vereinbarten Leistungspflichten anerkannt werden. Durch ergänzende Vertragsauslegung kann somit dem Kunden des

---

[459] *Graf,* Vertrag und Vernunft (1997) 194.

[460] Binder in Schwimann*,* ABGB IV^3 (2006) § 914 Rz 181; ebenso *Rummel* in Rummel*,* ABGB I^3 (2000) § 914 Rz 12.

[461] *Graf,* Vertrag und Vernunft (1997) 198.

Access-Providers, der darauf vergaß sich einen Anspruch auf Information auszubedingen, geholfen werden.

Der Access-Provider verfügt über einen besseren Kenntnisstand als sein Kunde. Wenn er diesen mit letzterem teilt, versetzt er ihn dadurch in die Lage, seine Rechte wahrzunehmen. Die bessere Sachkenntnis des Gläubigers einer Schutzpflicht ist in vielen Fällen Ansatzpunkt für deren Konstruktion[462].

5.5.6.1. Die Zumutbarkeit als Kriterium für die Informationspflicht

Ob sich der Access-Provider zu einer Information des Kunden über die Erfüllung eines Auskunftsbegehrens verpflichten würde, hängt zunächst auch von der Zumutbarkeit einer derartigen Informationspflicht ab[463]. Dieses von sich aus einleuchtende Prinzip lässt sich damit begründen, dass die Parteien ihre wechselseitigen Recht und Pflichten in einem vom Grundsatz der Privatautonomie beherrschten System wie jenem des ABGB selber festlegen und dabei grundsätzlich keiner staatlichen Kontrolle unterliegen und vor korrigierenden Eingriffen weitgehend bewahrt werden sollen. Sie sind es, welche die wechselseitig zu erbringenden Leistungen bewerten und entscheiden, welche Pflichten einander aus ihrer Sicht äquivalent sein sollen. Dies gilt nicht nur für die Haupt- sondern auch für die Nebenleistungspflichten. Kommt es nun zu einem Eingriff des Richters, bei dem der Pflichtenkatalog der einen Seite erweitert wird, gerät das von den Parteien als solches akzeptierte Gleichgewicht ins Wanken. Daraus folgt, dass hinsichtlich derlei Eingriffen ein großes Maß an Zurückhaltung und Vorsicht geboten ist und die Interessen des zu Verpflichtenden möglichst geschont werden sollten. Es ist demzufolge auch auf eine ökonomische Betrachtungsweise abzustellen. Bei der Entwicklung von Schutzpflichten ist daher zu berücksichtigen, inwieweit eine allfällige Pflicht in die wirtschaftliche Sphäre des zu Verpflichtenden eingreift und diesen in dieser Hinsicht belastet[464]. Auch in die Judikatur wird bei der Entwicklung und Bestimmung des Umfangs von Nebenpflichten regelmäßig auch deren Zumutbarkeit hervorgehoben[465]. Dies gilt beispielsweise auch für Rechnungslegungspflichten, welche die Judikatur überall dort annimmt, wo das Wesen des Rechtsverhältnisses es mit sich bringt, *„dass der Berechtigte in entschuldbarer Weise über das Bestehen und den Umfang des Vermögens*

---

462 *Schlesinger,* Das Wesen der positiven Vertragsverletzung, ZBl 1926, 732 (742)

463 *Helmut Böhm*, Die "Altlastensanierung" als Problem ergänzender Vertragsauslegung bzw des Wegfalls der Geschäftsgrundlage, ÖZW 1990, 104 (107).

464 *Schmidt,* Zur Ökonomie ergänzender Vertragspflichten unter besonderer Berücksichtigung von Konkurrenzschutzgeboten, JA 1978, 597 (600).

465 Vgl etwa OGH 11. 8. 2008, 1 Ob 39/08d, Zak 2008,396 = Immolex 2009,19/4; OGH 29. 5. 2008, 2 Ob 79/08v, ÖGZ 2008, 57; zu entsprechenden Beispielen aus der Judikatur siehe insbesondere auch das folgende Kapitel.

im Ungewissen, der Verpflichtete aber in der Lage ist, unschwer eine solche Auskunft zu erteilen, und diese Auskunft dem Verpflichteten überdies nach den Grundsätzen von Treu und Glauben auch zugemutet werden kann"[466]. Das Kriterium der Zumutbarkeit wurde in der Judikatur in erster Linie auf die Entwicklung von Verkehrssicherungspflichten[467] angewandt, aber auch vertragliche Schutzpflichten dürfen nicht überspannt werden[468]. Dabei ist zu berücksichtigen, dass eine Benachrichtigungspflicht beim Access-Provider keinen besonders hohen Aufwand erzeugt. So könnte er einer vertraglichen Nebenpflicht durch eine automatisch generierte elektronische Nachricht (SMS, E-Mail) nachkommen, die den Hinweis enthält, dass der Kunde, sofern er nähere Angaben wünscht, sich an eine Hotline wenden kann. Verfügt er über keinerlei Kontaktdaten, die es ihm ermöglichen, eine Nachricht über das von ihm verwendete Kommunikationsnetz an seinen Kunden zu schicken, besteht die Möglichkeit, die Benachrichtigung mit der nächsten monatlichen Rechnung postalisch zu übermitteln, ohne dass dabei besonders schwerwiegende Kosten anfallen. Die wirtschaftliche Belastung, die eine Benachrichtigungspflicht mit sich bringt, ist so gesehen daher als relativ gering einzustufen, insbesondere wenn man sie mit den Belastungen vergleicht, die andere von der Judiktur bereits qua Vertragsergänzung entwickelte Pflichten mit sich bringen. Man denke etwa an die wirtschaftliche Belastung, die durch ein Konkurrenzverbot des Bestandnehmers gegenüber seinem Bestandgeber entsteht[469]. Hier wird ein Vertragspartner um wirtschaftlich nützliche Handlungsoptionen gebracht, die für ihn sehr bedeutsam sein können und für ihn die Aufgabe eines gesamten Geschäftzweiges darstellen können. Die damit verbundenen Verluste lassen den mit einer Benachrichtigungspflicht für Access-Provider verbundenen Aufwand vergleichsweise marginal erscheinen.

Zudem sehen einige Auskunfts- und Mitwirkungsbestimmungen (StPO, § 53 Abs 3b SPG) vor, dass dem Access-Provider ein angemessener Ersatz für seine Leistungen, zT nach der Überwachungskostenverordnung – ÜKVO – [470], zusteht. Bei Bestimmungen wie § 87b Abs 3 UrhG, die vorsehen, dass dem Access-Provider ein angemessener Kostenersatz zusteht, wird der Access-Provider die Kosten einer Benachrichtigung jedenfalls auf die Auskunft suchende Stelle überwälzen dürfen. Die

---

[466] OGH 29.10.1975, 1 Ob 222/75, SZ 48/114 = EvBl 1977/42.

[467] OGH 7.3.1978, 4 Ob 505/78.

[468] OGH, 10. 4. 2008, 2 Ob 60/08z, Zak 2008, 238 = immolex 2008/138 = ecolex 2008, 732 = ZVR 2008, 496 = wobl 2009/109

[469] OGH 29.06.1976, 5 Ob 550/76, ImmZ 1976,318 = SZ 49/86; vgl auch den Arztpraxentauschfall, bei welchem zwei Ärzte ihre Praxis tauschten und der Vertrag um die Pflicht ergänzt wurde, dem Vertragspartner keine Konkurrenz am ursprünglichen Tätigkeitsort zu machen: BGH 18.12.1954, II ZR 76/54, BGHZ 16, 71.

[470] BGBl. II Nr. 322/2004 idF BGBl. II Nr. 261/2009.

nach der ÜVKO zu ersetzende Beträge verstehen sich als Pauschbeträge[471], weshalb auch der im Zusammenhang mit der Information des Betroffenen entstandene Aufwand als mit abgegolten betrachtet werden kann. Daher scheint es besonders in diesen Fällen zumutbar, den Access-Provider mit einer Benachrichtigungspflicht zu belasten.

5.5.6.2. Strafbarkeits- und Haftungsrisiken

Der Benachrichtigung könnte allerdings das Risiko einer allfälligen Haft- oder Strafbarkeit entgegenstehen. Je größer dieses Risiko einzustufen ist, desto unzumutbarer wird es mE für den Access-Provider den Kunden zu informieren. Teilweise ist eine Information auch aufgrund ausdrücklicher gesetzlicher Bestimmungen bzw an deren Telos orientierter Überlegungen ausgeschlossen. Wird etwa nach den Bestimmungen der StPO die Auskunft über Daten eine Nachrichtenübermittlung (§ 135 Abs 2) erteilt oder findet eine Nachrichtenüberwachung statt (§ 135 Abs 3), kann dem Access-Provider durch die Staatsanwaltschaft die Geheimhaltung der mit der Anordnung und Bewilligung verbundenen Tatsachen und Vorgänge gegenüber Dritten aufgetragen werden. Anders als bei der Auskünften über Bankkonten und Bankgeschäfte (§ 116 StPO), bei welchen das Kreditinstitut dazu angehalten werden kann, die Anordnung sowohl Dritten als auch dem Kunden gegenüber geheim zu halten, besteht nach dem Wortlaut des § 138 Abs 3 StPO nur die Möglichkeit, die Geheimhaltung gegenüber Dritten anzuordnen. Dennoch ist davon auszugehen, dass es dem Access-Provider auch versagt ist, seinen Kunden zu informieren. Nach § 50 StPO darf die Information des Beschuldigten, dass gegen ihn ein Ermittlungsverfahren geführt wird, solange unterbleiben, als besondere Umstände befürchten lassen, dass ansonsten der Zweck der Ermittlungen gefährdet wäre, insbesondere weil Ermittlungen oder Beweisaufnahmen durchzuführen sind, deren Erfolg voraussetzt, dass der Beschuldigte keine Kenntnis von den gegen ihn geführten Ermittlungen hat[472]. Heimliche Überwachungsmaßnahmen wie die Überwachung von Nachrichten setzen per definitionem voraus, dass der Beschuldigte von ihrer Durchführung keine Kenntnis hat[473]. Gemäß § 138 Abs 5 StPO hat die Staatsanwaltschaft ihre Anordnung und deren gerichtliche Bewilligung dem Beschuldigten und den von der Durchführung der Ermittlungsmaßnahme Betroffenen erst nach Beendigung einer Ermittlungsmaßnahme nach den §§ 135 Abs 2 und 3 StPO zuzustellen.

---

471 *Hasberger,* Zum Kostenersatz für die Telekommunikations-Überwachung, MR 2008, 58 (59).

472 Kritisch dazu *Achammer,* in *Fuchs/Ratz (Hrsg),* Wiener Kommentar zur Strafprozessordnung[2] (2009) § 50 Rz 20.

473 RV 25 BlgNR XXII. GP, 69.

Gem § 138 Abs 2 StPO sind Anbieter iSd § 92 Abs 1 Z 3 TKG 2003[474] verpflichtet, Auskünfte über Daten einer Nachrichtenübermittlung zu erteilen und an der Überwachung von Nachrichten mitzuwirken. Da es sich dabei nach dem Konzept der StPO um geheime Überwachungsmaßnahmen handelt, beinhaltet die Pflicht gem § 138 Abs 2 StPO trotz des wie gezeigt insoweit unklaren Wortlauts wohl auch die Verpflichtung, die Maßnahmen gegenüber dem Beschuldigten geheim zu halten. Somit kann davon ausgegangen werden, dass es dem Provider bei Maßnahmen gemäß § 135 Abs 2 und 3 StPO aufgrund gesetzlicher Vorgaben verwehrt ist, seinen Kunden zu informieren.

Hinsichtlich anderer Auskunftsbefugnisse (etwa SPG, MBG etc.) fehlen vergleichbare Bestimmungen, aus denen sich ein Verbot der Information des Betroffenen durch den Access-Provider ableiten lässt.

Hinsichtlich der Auskünfte nach der StPO (§§ 134ff StPO), SPG (§ 53) und MBG (§ 22) ist auch noch das Risiko der Verwirklichung des Tatbilds des § 299 StGB zu untersuchen. Das Vergehen der Begünstigung begeht, wer einen anderen, der eine mit Strafe bedrohte Handlung begangen hat, der Verfolgung oder der Vollstreckung der Strafe oder vorbeugenden Maßnahme absichtlich ganz oder zum Teil entzieht. Maßnahmen wie die Überwachung von Nachrichten (§ 135 Abs 3 StPO) stellen Ermittlungsmaßnahmen dar und dienen dem Zweck der Strafverfolgung. Die Ergebnisse solcher Maßnahmen sollen im weiteren Strafverfahren als Beweismittel dienen. Informiert der Access-Provider seinen Kunden, der Beschuldigter in einem Strafverfahren ist, etwa darüber, dass seine Nachrichten überwacht werden, wird dieser sein Kommunikationsverhalten anpassen und darauf achten, dass seine Nachrichten keine verwertbaren Beweise mehr enthalten. Dadurch wird der erhoffte Erfolg der Ermittlungsmaßnahme beeinträchtigt und die Verfolgung des Beschuldigten erschwert. Nach der Judikatur des OGH umfasst der Begriff "Entziehen" in § 299 StGB nicht nur das "Verbergen" im engeren Sinn, sondern jede Handlung, die dem Ziele dient, den Vortäter der Strafverfolgung oder Strafvollstreckung zu entziehen[475]. Dabei reicht eine bloße Erschwerung der Verfolgbarkeit bereits aus[476]. Es ist zu fragen, ob aus der ex-ante sicht des Providers das rechtlich missbilligte Risiko besteht, dass seine Handlung die Verfolgung des Beschuldigten effektiv erschwert[477]. Der objektive Tatbestand der Begünstigung scheint damit zumindest bei einer Information des Beschuldigten, dass

---

[474] Dabei handelt es sich wohl um Redaktionsversehen, tatsächlich wird der Begriff des Anbieters nämlich nicht in Abs 1 Z 3 leg cit sondern in Abs 3 Z 1 leg cit definiert.

[475] OGH 23. 1. 1978, 13 Os 157/77, EvBl 1978/160.

[476] OGH 26. 4. 1977, 11 Os 22/77, SSt 48/39.

[477] *Pilnacek,* in *Höpfel/Ratz* (Hrsg), Wiener Kommentar zur Strafprozessordnung[2] (2004) § 299 Rz 14.

eine Überwachung von Nachrichten stattfindet, regelmäßig erfüllt sein. Anders verhält es sich bei der Benachrichtigung des Beschuldigten über die Erteilung einer Auskunft über Daten einer Nachrichtenübermittlung. Inwieweit eine derartige Benachrichtigung verfolgungsschädlich ist, hängt vom Einzelfall ab. Auch hier sind Fälle denkbar, in denen die Benachrichtigung zu einer Erschwerung der Verfolgung führt. Man denke etwa an unverzügliche Mitteilung des Access-Providers an seinen Kunden, in welcher er ihn darauf aufmerksam macht, dass er der Kriminalpolizei seine Standortdaten bekannt gab, was zur Flucht des Beschuldigten führt. Was den subjektiven Tatbestand anbelangt, ist insbesondere zu beachten, dass hinsichtlich der Verfolgungserschwerung bzw Verfolgungsvereitelung Absichtlichkeit vorliegen muss. Das bedeutet, dass es dem Provider darauf ankommen müsste, durch die Information des Betroffenen die Vereitelung der Strafverfolgung zu bewirken. Ob der subjektive Tatbestand verwirklicht wurde, ist eine Beweisfrage und daher kann daher nicht Gegenstand dieser Abhandlung sein. Sollte er jedoch nicht erfüllt sein, lässt sich das Risiko einer Strafbarkeit gem § 299 StGB nicht heranziehen um das Vorliegen einer vertraglichen Schutzpflicht zu verneinen.

Nachdem die Befugnisse im SPG und im MBG nicht der Strafverfolgung sondern der Verhinderung von Straftaten dienen[478], wird in den meisten Fällen wohl ausgeschlossen sein, dass eine Information des Betroffenen über Auskunftserteilungen nach diesen Gesetzen den Tatbestand des § 299 StGB erfüllt. Auch hier kann es jedoch Ausnahmen geben, da sich die Abgrenzung mitunter schwierig gestalten kann. Meist wird die Ausübung sicherheitspolizeilicher Befugnisse nach dem SPG wohl der Verhinderung von Straftaten – Gefahrenabwehr – dienen. Allerdings gilt es in diesem Zusammenhang auch § 21 Abs 2 SPG zu beachten. Nach diesem haben die Sicherheitsbehörden nach einem gefährlichen Angriff unbeschadet ihrer Aufgaben nach der StPO die maßgebenden Umstände, einschließlich der Identität des dafür Verantwortlichen, zu klären, soweit dies zur Vorbeugung weiterer gefährlicher Angriffe erforderlich ist[479]. Bedienen sie sich dazu ihrer Auskunftsbefugnisse und teilt dies der Access-Provider seinem Kunden mit, kann es im Einzelfall dazu kommen, dass auch die Verfolgung des Täters einer strafbaren Handlung erschwert wird.

Unzumutbar scheint es, dass der Access-Provider sich in Zweifelsfällen auf ein Risiko einlassen und seinen Kunden ungeachtet drohender Haftungs- bzw Strafbarkeitsszenarien informieren muss. Soweit ein derartiges Risiko besteht, kann mE keinesfalls eine Informationspflicht des Access-Providers konstruiert werden. Dies gilt

---

478 *Wiederin,* Einführung in das Sicherheitspolizeirecht (1998) Rz 291.

479 Vgl dazu auch *Ennöckl,* Der Rechtsschutz gegen sicherheitspolizeiliche Maßnahmen, JBl 2008, 409 (417ff).

sowohl für die (aktive) Benachrichtigungspflicht, als auch für die erst durch Nachfrage entstehende Auskunftspflicht.

5.5.6.3. Einfachheit und Notwendigkeit der Information

Liegt keines der oben geschilderten Strafbarkeits- bzw Haftungsrisiken vor, ist eine Benachrichtigungspflicht insbesondere auch wegen der Einfachheit des Access-Providers zu bejahen. Der Entscheidung 3 Ob 559/86[480] lag die Klage eines Vertragspartners eines Kreditkartenunternehmens zugrunde, mit welcher der Kläger von einer Kreditkartengesellschaft die Offenlegung der Identität eines ihrer Kunden begehrte. Der Kunde der Kreditkartengesellschaft hatte mit seiner Kreditkarte beim Kläger bezahlt, die Kreditkartengesellschaft weigerte sich jedoch in weiterer Folge die Rechnung zu bezahlen, da der Kläger bestimmte Verpflichtungen aus dem Vertrag mit dem Kreditkartenunternehmen verletzt hatte. Da somit der Anspruch gegen das Kreditkartenunternehmen wegfiel, wollte der Vertragspartner des Kreditkartenunternehmens von letzterem Namen und Anschrift des Kunden, um seine Ansprüche gegen diesen auf direktem Wege durchsetzen zu können. Das Kreditkartenunternehmen weigerte sich dem nachzukommen, nachdem es den Kreditkarteninhaber um Erlaubnis gefragt und dieser seine Zustimmung versagt hatte. Der Kläger benötigte in diesem Verfahren somit bestimmte Informationen um seine Rechte gegenüber Dritten ausreichend wahrnehmen zu können. In dieser Hinsicht entspricht der Sachverhalt den hier interessierenden Sachverhalten: Es geht um die Frage, inwieweit jemand seinem Vertragspartner Informationen schuldet, damit dieser Rechte gegenüber Dritten effizient wahrnehmen kann. Der OGH gab dem Kläger Recht. Aus dem Grundsatz von Treu und Glauben entstehe im Falle von Abwicklungsschwierigkeiten die Pflicht der Kreditkartengesellschaft dem Vertragsunternehmen den Namen und die Anschrift des Kreditkarteninhabers bekannt zu geben. Dies sei notwendig, damit das Vertragsunternehmen seine Ansprüche gegen den Kreditkarteninhaber auf direktem Wege durchsetzen könne. Der Kläger konnte sich bezüglich seines Anspruches auf keine Vereinbarung stützen, die Pflicht ist somit das Ergebnis ergänzender Vertragsauslegung[481]. Diese Entscheidung betraf Informationen, die nötig waren, dass der Gläubiger der durch Vertragsauslegung gewonnenen Verpflichtung seine Rechte gegenüber einem privaten Dritten durchsetzen kann. Ähnliche Zwecke werden auch verfolgt, soweit durch ergänzende Vertragsauslegung

---

[480] OGH 8.3.1988, 3 Ob 559/86, SZ 61/55 = EvBl 1989/1 = wbl 1988, 240 = RZ 1988/51 = ÖBA 1988, 1022.

[481] *Graf,* Vertrag und Vernunft (1997) 214ff.

Rechnungslegungspflichten gewonnen werden, die den Berechtigten in die Lage versetzen sollen, die Korrektheit von Abrechnungen zu überprüfen[482].

Für den Kunden ist die Benachrichtigung über die Erfüllung eines Auskunftsbegehrens überaus wertvoll. Sie versetzt ihn in die Lage, seine Interessen gegenüber der Auskunft suchenden Stelle wahrzunehmen. So kann er sich etwa mittels Beschwerde wegen Verletzung der Bestimmungen über den Datenschutz gem § 90 SPG an die Datenschutzkommission wenden, wenn er zur Auffassung gelangt, die Sicherheitsbehörde sei nicht berechtigt gewesen, eine Auskunft gemäß § 53 Abs 3a bzw 3b SPG einzuholen. Mangels Informationspflicht der Sicherheitsbehörden, kann es in diesen Fällen nämlich vorkommen, dass er ansonsten nicht von der Ausübung dieser Befugnisse erfährt. Diesfalls wird der Rechtsschutz einzig durch einen – glaubt man Medienberichten[483] – sehr stark ausgelasteten Rechtsschutzbeauftragten (§§ 91a ff SPG) ausgeübt. Dieser kommissarisch ausgeübte Rechtsschutz wird tendenziell qualitativ minderwertiger sein, als ein durch den Betroffenen selbst ausgeübter Rechtsschutz[484]. Auch im normativen Umfeld der meisten anderen Auskunftsbestimmungen ist keine Information des Betroffenen vorgesehen. Eine Ausnahme stellt in dieser Hinsicht die StPO dar, deren § 138 Abs 5 bestimmt, dass die Staatsanwaltschaft nach Beendigung einer Ermittlungsmaßnahme nach den §§ 135 Abs 2 und 3 sowie 136 ihre Anordnung und deren gerichtliche Bewilligung dem Beschuldigten und den von der Durchführung der Ermittlungsmaßnahme Betroffenen unverzüglich zuzustellen hat.

In den Fällen, in denen die Auskunft suchende Stelle zugleich gesetzlich verpflichtet wird, den Betroffenen zu informieren, erübrigt sich die Vertragsergänzung um eine Auskunftspflicht des Access-Providers. Dort wo der Beauskunftete so wie nach der StPO den Kunden des Access-Providers selber informieren muss, besteht keine Notwendigkeit den Kunden durch ergänzende Pflichten zu schützen. Das gilt mE auch dann, wenn der Access-Provider schon seit geraumer Zeit an der Auskunft über Daten einer Nachrichtenübermittlung bzw an Nachrichtenüberwachungen mitwirkt, ohne dass der Beschuldigte durch die Staatsanwaltschaft informiert wird. Aus § 138 Abs 5 StPO erhellt, dass einzig die Staatsanwaltschaft dazu berufen ist, über den Zeitpunkt der Information des Beschuldigten zu entscheiden. Der Access-Provider ist dazu gar nicht in der Lage, weil er keine Einsicht in das Verfahren gegen seinen Kunden bzw damit zusammenhängende Verfahren hat und demzufolge auch nicht beurteilen kann, inwieweit

---

[482] Vgl etwa OGH 1.9.1992, 9 ObA 225/92, wbl 1993, 53: Hier wurde dem Arbeitnehmer das recht auf eine genaue Lohnabrechnung eingeräumt, damit er überprüfen konnte, ob der Arbeitgeber die vom Arbeitslohn abzuführenden Steuern, Sozialversicherungsbeiträge und sonstigen Abgaben dem Gesetz entsprechend abgerechnet und abgeführt hat.

[483] http://futurezone.orf.at/stories/264593/ (Stand April 2010).

[484] *Raschhofer,* in *Zankl* (Hrsg), Auf dem Weg zum Überwachungsstaat? (2009) 110ff.

eine Information des Beschuldigten der Zweck dieses oder anderer Verfahren gefährdet werden würde.

Bei jenen Auskunftsbestimmungen, die wie das SPG keine Benachrichtigung des Betroffenen vorsehen, sieht die Sache freilich ganz anders aus. Für den Access-Provider stellt diese für seinen Kunden so wichtige Information keinen nennenswerten Aufwand dar. Die Information des Betroffenen ist wie erwähnt mittels kurzer automatisch generierter Nachricht möglich. Die Tatsache, dass die Benachrichtigungspflicht den Access-Provider nur geringfügig belastet, spricht zusätzlich dafür eine entsprechende Pflicht qua ergänzende Vertragsauslegung zu konstruieren. Die Wesentlichkeit des Gläubigerinteresses im Verhältnis zur Geringfügigkeit der dem Verpflichteten entstehenden Belastung legt dies nahe[485]. In der Entscheidung 1 Ob 716/86[486] hatte der OGH zu beurteilen, ob eine (nachwirkende) Schutzpflicht bestehe, einen Vertrag im Interesse des anderen zu ergänzen, wenn dies für den Verpflichteten keinen Nachteil mit sich bringt. In casu verkauften die Kläger eine Liegenschaft an die Beklagten zu einem Zeitpunkt, als dieser Vorgang noch nicht umsatzsteuerpflichtig war. In weiterer Folge wurde die Bestimmung, welche die Umsatzsteuerbefreiung vorsah, vom VfGH aufgehoben und die Kläger wurden umsatzsteuerpflichtig. Der Kläger begehrten darauf von den Beklagten, den Vertrag dahin abzuändern, dass sie die USt übernehmen, da sie vorsteuerabzugsberechtigt waren und ihnen dadurch in Wahrheit kein Aufwand entstand. Der OGH sprach aus, dass die Verweigerung der Zustimmung zu einer Vertragsänderung, die dem einen Vertragsteil wirtschaftliche Vorteile bringt und für den anderen mit keinerlei Nachteilen verbunden sei, sittenwidrig sei. Freilich steckt hinter dieser Gegenüberstellung – wesentliches Gläubigerinteresse versus Geringfügigkeit der Belastung des Verpflichteten – stets eine mehr oder minder unobjektivierbare Wertung. Man könnte auch einwenden, dass schließlich nur die primäre qua Vertragsauslegung gewonnene Schutzpflicht eine Kurznachricht zu verschicken „geringfügig" sei. Die sich aus ihrer Verletzung ergebenden Konsequenzen – Schadenersatz- und Unterlassungsansprüche, unter Umständen sogar Rücktrittsrechte – können den durch die Schutzpflicht Verpflichteten hingegen sehr hart treffen[487]. Das ist jedoch auch bei sehenden Auges vereinbarten Primärpflichten der Fall. Verletzt etwa der Verkäufer seine Pflicht auf Lieferung der Ware und tritt darauf hin der Käufer vom Vertrag zurück und klagt auf das Erfüllungsinteresse, kann dieses Erfüllungsinteresse für den Verkäufer ebenfalls unerwartet hoch ausfallen.

---

485 *Graf,* Vertrag und Vernunft (1997) 227.

486 OGH 25.3.1987, 1 Ob 716/86, JBl 1987, 782 = SZ 60/50.

487 So etwa *Schmidt,* Zur Ökonomie ergänzender Vertagsauslegung unter besonderer Berücksichtigung von Konkurrenzschutzgeboten, JA 1978, 597 (603), der betont, dass bei der Verteilung von Pflichten stets auch die Haftungsdimension mit zu berücksichtigen ist.

In der Entscheidung 3 Ob 632/76[488] nahm der OGH zu dem Problem Stellung, was gilt, wenn sich die qua Vertragsauslegung gewonnene Informationspflicht zum Nachteil des Verpflichteten auswirkt. In diesem Fall ging es darum, dass die Erbin eines verstorbenen Kommanditisten nach dem Gesellschaftsvertrag eine Erklärung hätte abgeben müssen um an die Stelle des verstorbenen Kommanditisten zu rücken. Davon wusste sie nichts und der Komplementär klärte sie auch nicht über diesen Umstand auf, da für ihn das Ausscheiden des Kommanditisten günstiger war. Der OGH gab der Erbin, die behauptete, der Komplementär hätte ihr eine entsprechende Information geschuldet, damit sie ihr Recht wahrnehmen könne, nicht Recht. Er sprach aus, dass ein Gebot, den Vertragspartner auf die Notwendigkeit einer Rechtshandlung hinzuweisen, welche diesen vor Nachteilen bewahrt, gleichzeitig aber die eigene Position verschlechtert, nur in zwei Fällen in Betracht kommen könne. Eine derartige Pflicht bestehe einerseits nur im Falle besonderer Fürsorge- bzw Treuepflichten und andererseits wenn der Nachteil auf Seiten des Vertragspartners bei Unterlassung der Handlung außergewöhnlich groß, jener des anderen Teils infolge dieser Rechtshandlung hingegen unverhältnismäßig gering wäre, also insoweit ein krasses Missverhältnis vorliegt[489]. Aus dieser Entscheidung lassen sich zwei wesentliche Erkenntnisse erzielen, die zwei meiner oben aufgestellten Thesen untermauern. Erstens darf eine im Wege ergänzender Vertragsauslegung gewonnene Schutzpflicht prinzipiell nicht so weit gehen, dass die Erfüllung dieser Pflicht die Güter des Verpflichteten gefährdet und dessen Interessen massiv gefährdet. Zweitens wird aber auch in dieser Entscheidung – wie auch in den anderen oben skizzierten – deutlich, dass der OGH jedes Mal eine Art Abwägung durchführt. Er setzt die durch die Pflichterfüllung entstehenden Nachteile mit den für den Gläubiger der Schutzpflicht entstehenden Vorteilen in Beziehung und gewichtet diese. Wenn der Nachteil, der dem Verpflichteten durch die Pflichterfüllung entsteht, als unverhältnismäßig klein im Vergleich zu den dem Gläubiger erwachsenden Vorteilen ist, wird die Schutzpflicht tendenziell eher bejaht. Überträgt man diese Überlegung auf die hier diskutierte Frage, so kann man eine Benachrichtigungspflicht des Access-Providers eigentlich nur bejahen: Der Nachteil, der dem Access-Provider entsteht, ist regelmäßig mit dem Aufwand für die für ihn günstigste Benachrichtigungsmöglichkeit (SMS, E-Mail, postalisches Benachrichtigungsschreiben) begrenzt. Abgesehen von den oben geschilderten Fällen, in denen gewisse Haftungs- bzw Strafbarkeitsrisiken bestehen, hat er nichts zu tun, als eine Nachricht über das von ihm betriebene oder genutzte Kommunikationsnetz zu verschicken. Dieser „Nachteil" ist gegenüber dem Nachteil, der seinem Kunden erwächst, wenn er über die Beauskunftung

---

[488] OGH 18. 1. 1977, 3 Ob 632/76, HS 10.993 = JBl 1978, 426 = NZ 1980, 26.

[489] Vgl auch *Schmidt,* Zur Ökonomie ergänzender Vertragspflichten unter besonderer Berücksichtigung von Konkurrenzschutzgeboten, JA 1978, 597 (599ff), der die pflichtbegrenzende Funktion des Kostenfaktors auf Seiten des durch Vertragsergänzung zu Verpflichtenden hervorhebt.

Dritter völlig im Dunkeln gelassen wird, als geringfügig iSd skizzierten Judikatur einzustufen. Angesichts dieses nur geringen Aufwandes, der dem Access-Provider entsteht, ist auch davon auszugehen, dass wenn ein Kunde bei Vertragsabschluss die erörterte Problematik vorausgesehen und demzufolge auf eine entsprechende Pflicht seines Providers gedrängt hätte, letzterer – Redlichkeit vorausgesetzt – dem wohl zugestimmt hätte.

5.5.6.4. Die mögliche Information durch die Auskunft suchende Stelle

Gegen all die oben angestellten Überlegungen ließe sich einwenden, dass nicht der Access-Provider sondern die Auskunft suchende Stelle, welche die Beauskunftung schließlich initiierte, in erster Linie für die Information des Betroffenen zuständig sei. Oben (vgl Kapitel 4.5.5) wurde bereits erwähnt, dass etwa die Sicherheitsbehörden hinsichtlich der Auskunftsbefugnisse des SPG eine Information des Betroffenen gestützt auf § 24 DSG ablehnen. Inwieweit dies mit rechtsstaatlichen Prinzipien und den berührten Grundrechten in Einklang zu bringen ist[490], kann hier dahinstehen. Die Auskunft suchende Stelle (der Urheber, die Sicherheits- bzw Kriminalpolizei, das Gericht, das militärische Organ, etc) ist mit dem Vertragspartner des Access-Providers jedoch regelmäßig nicht vertraglich verbunden. Gegenstand dieser Arbeit sind ausschließlich die vertraglichen Schutzpflichten des Access-Providers gegenüber seinem Kunden. Diese sind im Bestand und in der Reichweite mE völlig unabhängig von den Pflichten Dritter, die ebenfalls auf den Schutz derselben Güter abzielen. Selbst wenn man also zum Ergebnis käme, dass etwa Behörden aufgrund rechtsstaatlicher Erwägungen eine Informationspflicht gegenüber dem Betroffenen trotz fehlender ausdrücklicher Regelung trifft, hat dies keinen Einfluss auf die vertraglichen Pflichten des Access-Providers. Nur er ist mit seinem Kunden durch das vinculum iuris verbunden, das letztlich der Rechtfertigung besonderer Schutzpflichten dient. Der Access-Provider weiß nicht, ob die Auskunft suchende Stelle, seinen Kunden über die Erteilung der Auskunft informiert und kann abgesehen von Auskünften nach der StPO auch nicht damit rechnen. Der Access-Provider muss vielmehr regelmäßig davon ausgehen, dass sein Kunde, wenn er selbst ihn nicht benachrichtigen sollte, über die Erfüllung eines Auskunftsbegehrens nichts erfährt. Dies gilt insbesondere dann, wenn sich wie im Falle der Befugnisausübungen nach dem SPG sogar eine ausdrückliche Stellungnahme der Sicherheitsbehörden vorliegt, wonach diese sich weigern den Betroffenen zu informieren[491]. Auch von einer Information durch den

---

[490] Vgl zu diesen etwa *Raschhofer,* in *Zankl* (Hrsg), Auf dem weg zum Überwachungsstaat (2009) 110ff.

[491] 4148/AB XXIII. GP, 2.

Rechtsschutzbeauftragten (wo vorhanden) darf nicht ohne weiteres ausgegangen werden[492]. In diesen Fällen ist er der einzige, der dann noch in Frage kommt, den Betroffenen durch Benachrichtigung in die Lage zu versetzen seine Rechte wahrzunehmen. Gerade diese Stellung ist es, die für die Annahme einer vertraglichen Schutzpflicht spricht. So spielt auch in anderen Entscheidungen, in denen Verträge um bestimmte Schutz- oder Nebenpflichten ergänzt wurden, die Überlegung, dass einzig der Verpflichtete bestimmte Handlungen bzw Unterlassungen durchführen kann, eine wesentliche Rolle. So ist es etwa in der Autopapiere-Entscheidung[493] offensichtlich, dass sich der OGH auch von der Überlegung leiten ließ, dass einzig der Verkäufer in der Lage war, dem Käufer einen urkundlichen Nachweis des Eigentumsübergangs zu verschaffen[494]. Derartige Sonderstellungen eines Vertragspartners sind mit ein Grund für die Konstruktion bestimmter Neben bzw Schutzpflichten. Für die Vertragshaftung ist es typisch, dass hier umfassendere Sorgfaltspflichten als im Bereich der Deliktshaftung bestehen. Dies wird mit der rechtlichen Sonderbeziehung zwischen den Vertragspartnern gerechtfertigt[495].

Aber auch wenn die Möglichkeit besteht, dass die Auskunft suchende Stelle den Betroffenen informiert, führt dies mE nicht zum Wegfall der Benachrichtigungspflicht. Es gibt auch eine Reihe von Erkenntnissen, in denen eine Neben- bzw Schutzpflicht konstruiert wurde, obwohl sich der Gläubiger dieser Pflicht in der Regel durch enormen Aufwand auch ohne diese Pflicht in einen vergleichbaren Zustand hätte versetzen können. Man denke etwa an die beim Softwarevertrag geschuldete Nebenpflicht des Softwarelieferanten[496], den Besteller in die gelieferte Software einzuführen und einzuschulen. Hier ist davon auszugehen, dass der Besteller auch in der Lage wäre, sich diese Leistung bei einem anderen Experten relativ teuer einzukaufen und somit auch ohne Vertragsergänzung letztlich zum gewünschten Ergebnis käme. Gleiches gilt für die vertragliche Nebenpflicht des Verkäufers zu dem verkauften Gerät eine

---

[492] Zur Frage wie sich eine mögliche Information des Betroffenen durch den Rechtsschutzbeauftragten auswirkt, siehe das sogleich folgende Kapitel unten.

[493] OGH 26.09.1951, 3 Ob 500/51, SZ 24/248; diese Entscheidung widerlegt übrigens die von *Schmidt,* Zur Ökonomie ergänzender Vertragspflichten unter besonderer Berücksichtigung von Konkurrenzschutzgeboten, JA 1978, 597 (600), vertretene These, dass die Judikatur dazu neige im Rahmen ergänzender Vertragsauslegung nur Pflichten entwickeln, die wirtschaftliche Handlungsoptionen begrenzen (zB Konkurrenzschutzgebote), aber niemals Pflichten, die Sachwerte betreffen.

[494] *Graf* geht davon aus, dass, wenn der Vertrag nicht um die Pflicht des Verkäufers ergänzt würde, dem Käufer die Papiere kostenfrei auszuhändigen, letzterem aufgrund der diesbezüglichen Monopolstellung des Verkäufers im Ergebnis wohl ein unangemessenes Entgelt dafür abverlangt worden wäre. Dies sei jedoch als Marktversagen zu qualifizieren, weshalb die Rechtsordnung eingreife: *Graf,* Vertrag und Vernunft (1997) 222ff.

[495] *Koziol,* Delikt, Verletzung von Schuldverhältnissen und Zwischenbereich, JBl 1994, 209 (210).

[496] OGH 29.10.1992, 8 Ob 547/91, SZ 65/144 = ecolex 1993, 85.

Bedienungsanleitung mitzuliefern[497]. Auch hier könnte argumentiert werden, dass sich der Käufer die Bedienungsanleitung auch vom Hersteller oder sonstigen Dritten beschaffen könnte, wenn eine entsprechende Pflicht des Verkäufers nicht vereinbart wurde. Dennoch werden von Judikatur auch hier Nebenpflichten qua ergänzender Vertragsauslegung konstruiert. Daraus folgt, dass die möglichen Pflichten Dritter auf den Bestand und Umfang von Nebenpflichten, die im Rahmen ergänzender Vertragsauslegung konstruiert wurden, nur begrenzt Einfluss haben.

Anderes gilt freilich dann, wenn die Bestimmungen, wonach der Access-Provider Auskunftsbegehren zu erfüllen hat, so wie im Falle der StPO von Bestimmungen flankiert werden, welche die Auskunft suchende Stelle zu einer Information des Betroffenen ausdrücklich verpflichten. In diesen Fällen besteht, wie bereits im vorstehenden Kapitel ausgeführt, keine Benachrichtigungspflicht des Access-Providers.

5.5.6.5. Die mögliche Information durch den Rechtsschutzbeauftragten

Die StPO[498], das MBG[499] und das SPG[500] kennen das Institut des Rechtsschutzbeauftragten. Dieser spielt in allen drei Gesetzen eine ähnliche Rolle. Bestimmte Ermittlungsmaßnahmen können nur ohne Kenntnis des Betroffenen erfolgen, da der Erfolg dieser Maßnahmen davon abhängt, dass eine Information des Betroffenen unterbleibt. Da aber diese Maßnahmen in die Grundrechte – allen voran das Recht auf Achtung der Privatsphäre gem Art 8 EMRK – des Betroffenen eingreifen, tritt eine Rechtsschutzlücke auf. Es bedarf daher geeigneter Vorkehrungen um Missbrauch vorzubeugen[501]. Ohne Rechtsschutzbeauftragten gäbe es jedenfalls für die Dauer der Maßnahmen nur die Behörde, deren Organe zwar zu rechtmäßigem Handeln verpflichtet sind, aber an einer für den Betroffenen übermäßig günstigen Rechtsanwendung naturgemäß kein Interesse haben und den Betroffenen, der mangels Information seine Rechte nicht wahrnehmen kann. Dem Rechtsschutzbeauftragten kommt die Aufgabe zu, diese Rechtsschutzlücke zu schließen und die Interessen des Betroffenen kommissarisch zu wahren[502]. Überdies hat er auch auf die Wahrung der Interessen unbeteiligter Dritter

---

[497] OGH 3.5.1994, 1 Ob 555/94.

[498] Vgl §§ 146 und 147 StPO.

[499] Vgl § 57 MBG.

[500] Vgl §§ 91a ff SPG.

[501] *Handstanger/Okresek*, Sicherheitsverwaltung und MRK, ÖJZ 1995, 251 (251fff).

[502] Vgl dazu *Vogl,* Rechtsschutz und Vollziehung, in *BMI* (Hrsg), Der Rechtsschutzbeauftragte (2004) 19; RV 1708 BlgNR XX. GP, 7.

zu achten[503]. Er wird deshalb auch als „Wächter des Rechtsstaates" bzw als „besonderes Organ der Rechtspflege" bezeichnet[504].

Es stellt sich die Frage, ob und inwieweit die gesetzlich normierten Aufgaben des Rechtsschutzbeauftragten für die Konstruktion einer Benachrichtigungspflicht des Access-Providers von Belang sind. Es könnte argumentiert werden, dass sich eine vertragliche Schutzpflicht erübrige, da die Rechtsordnung die Aufgabe die Interessen des Betroffenen zu schützen bereits dem Rechtsschutzbeauftragten zugeordnet hat. Wozu sollte man den Access-Provider durch eine qua Vertragsergänzung erzeugte Pflicht belasten, wenn doch die Interessen des Betroffenen ohnedies bereits ausreichend berücksichtigt wurden? Dieses Argument hat vor allem wegen der Maxime den Vertragspartner durch ergänzende Pflichten so wenig wie möglich zu belasten in der Tat einiges für sich, vermag aber bei näherer Betrachtung letztlich nicht zu überzeugen:

Hinsichtlich der Auskunfts- und Mitwirkungsbestimmungen in der StPO wurde aufgrund der in den §§ 138 und 139 normierten Pflicht der Staatsanwaltschaft den Betroffenen zu informieren bereits oben eine vertragliche Pflicht des Access-Providers zur Information ausgeschlossen. Zu klären bleibt daher nur mehr die Frage, ob die im SPG und im MBG normierten Aufgaben des Rechtsschutzbeauftragten eine Vertragsergänzung ausschließen. Bezüglich außerhalb dieser drei Gesetze geregelter Auskunftsbefugnisse stellt sich die Frage mangels Zuständigkeit eines Rechtsschutzbeauftragten nicht.

§ 91d Abs 3 SPG bestimmt, dass der Rechtsschutzbeauftragte zur Information der Betroffenen befugt ist, wenn er wahrnimmt, dass durch das Verwenden personenbezogener Daten Rechte von Betroffenen verletzt worden sind, die von dieser Datenverwendung keine Kenntnis haben. Sofern eine Information aus den Gründen des § 26 Abs 2 des DSG 2000 nicht erfolgen kann, ist er zur Erhebung einer Beschwerde an die Datenschutzkommission nach § 90 befugt. In ähnlicher Weise bestimmt § 57 Abs 6 Z 1 MBG, dass der Rechtsschutzbeauftragte, zu einer Information des Betroffenen berechtigt ist, wenn er wahrnimmt, dass durch das Verwenden von Daten Rechte eines Betroffenen verletzt worden sind, der von dieser Datenverwendung keine Kenntnis hat. Z 2 leg cit bestimmt in Ergänzung dazu, dass er eine Beschwerde an die DSK erheben kann, wenn eine Information des Betroffenen nach Z 1 die Sicherung der Einsatzbereitschaft des Bundesheeres oder die Interessen der umfassenden Landesverteidigung gefährden oder erheblich behindern würde[505]. In solchen Fällen darf

---

[503] AB 812 BlgNR XX.GP, 13ff.

[504] *Machacek*, Die Bekämpfung der organisierten Kriminalität in Österreich, ÖJZ 1998, 553 (561).

[505] Vgl *Raschauer/Wessely,* Militärbefugnisgesetz[2] (2007) § 57 Anm 7c.

der Rechtsschutzbeauftragte nur eine Beschwerde einbringen und darf den Betroffenen keinesfalls informieren.

Ob der Betroffene informiert wird, hängt daher sowohl nach dem SPG als auch dem MBG immer zumindest von zwei Umständen ab: Erstens muss der Rechtsschutzbeauftragte zum Ergebnis kommen, es liege eine Rechtsverletzung zu Lasten des Betroffenen vor. Nur für diesen Fall gilt die Befugnis des Rechtsschutzbeauftragten. Hält er die Datenverwendung durch die Sicherheitsbehörden für korrekt, steht ihm nach dem Wortlaut des Gesetzes keine Befugnis zu, den Betroffenen zu informieren. Zweitens muss er die Entscheidung treffen, den Betroffenen zu informieren.

Dies ist für den Betroffenen von Nachteil, weil es sich bei der Frage, ob seine Rechte verletzt wurden, nicht immer um eine eindeutige objektivierbare Tatsachenfrage handelt, sondern oft auch um eine Rechtsfrage. Diese lassen sich naturgemäß je nach Betrachtungswinkel unterschiedlich beantworten. Es werden in der Praxis zwangsläufig Fälle eintreten, in denen der Betroffene, wäre er über die Maßnahme informiert worden, zur Auffassung gelangt, dass er in seinen Rechten verletzt wurde, während der Rechtsschutzbeauftragte aus seiner Sicht nichts zu beanstanden hat. Als Beispiel sei hier etwa eine Überwachungsmaßnahme aus dem in den Medien vieldiskutierten „Terror-Prozess"[506] gegen *Mohammed M.* und *Mona S.* zu nennen. Die im Zuge der Erhebungen gegen die Beschuldigten durchgeführten Überwachungsmaßnahmen wurden vom damaligen zuständigen Rechtsschutzbeauftragten *Dr. Gottfried Strasser* bis zuletzt für korrekt befunden. Er verteidigte das Vorgehen der Kriminalpolizei auch in der Öffentlichkeit als mit der StPO und den Grundrechten der Beschuldigten im Einklang stehend[507]. Diese Auffassung stieß bei einer Reihe von Experten, darunter eine interministerielle Arbeitsgruppe, der Verfassungs- und Strafrechtsexperten angehörten, auf heftige Kritik[508]. Es ist davon auszugehen, dass die Beschuldigten wohl eher die Ansicht der Experten, welche die

---

506 Siehe etwa http://diepresse.com/home/panorama/oesterreich/538703/index.do?_vl_backlink=/home/panorama/oesterreich/index.do (Stand April 2010).

507 http://www.news.at/articles/0810/10/199219/totale-eskalation-wiener-terror-prozess-wuetender-mohamed-m-gericht (Stand April 2010).

508 *BMI/BMJ*, Erweiterung des Ermittlungsinstrumentariums zur Bekämpfung schwerer, organisierter Kriminalitätsformen („Online-Durchsuchung") (2008) FN 30; dort heiß es: "*Die anlässlich des 5. Rechtschutztages des BMI durch den RSB GP iR Dr. Gottfried Strasser vertretene Ansicht, dass ein Eindringen in den Wohnbereich auch zum Zweck der Durchführung einer Überwachung einer Telekommunikation zulässig sei, weil beide Eingriffsmaßnahmen [nämlich Überwachung einer Telekommunikation und optische und akustische Überwachung] Formen der Äußerungsüberwachung im weiteren Sinn darstellten und dem Gesetzesvorbehalt des Art. 8 EMRK – legitimer Zweck, Notwendigkeit in einer demokratischen Gesellschaft, Festlegung im Gesetz – in gleicher Weise genüge getan wurde, ist aus Sicht der Abt. II 3 des BMJ daher mit Entschiedenheit abzulehnen.*"

Maßnahme für unzulässig hielten, geteilt hätten, als die Ansicht des Rechtsschutzbeauftragten. In vielen Fällen hätte der Betroffene wohl auch recht gute Erfolgsaussichten, wenn er einen Rechtsbehelf gegen die Maßnahme einlegen würde. In Fällen, in denen die Maßnahme nach dem Dafürhalten des Rechtsschutzbeauftragten korrekt war und der Betroffene selbst die Maßnahme für unrechtmäßig halten würde, kann letzterer aber kein Rechtsmittel ergreifen, da er vom Rechtsschutzbeauftragten nach dem Wortlaut des § 91d SPG nicht informiert werden darf. Dadurch wird der Betroffene seiner Möglichkeit beraubt seiner Rechtsansicht mittels Rechtsbehelfen zum Durchbruch zu verhelfen. Insofern zeigt sich deutlich, dass der kommissarische Rechtsschutz durch den Rechtsschutzbeauftragten im Vergleich zu einem durch den Betroffenen selbst ausgeübten Rechtsschutz aus Sicht des Letzteren stets ein qualitatives Minus darstellt. Das dadurch entstehende Rechtsschutzdefizit lässt sich einzig durch eine Information des Betroffenen durch seinen Access-Provider bezwingen. Dadurch wird er in die Lage versetzt, seine Rechte selbst wahrzunehmen, seine Möglichkeiten mit einem von ihm gewählten Rechtsbeistand abzuklären und gegebenenfalls Rechtsmittel einzulegen.

Problematisch ist weiters, dass der Rechtsschutzbeauftragte im Falle der Wahrnehmung von Rechtsverletzungen nach dem Wortlaut der Bestimmungen lediglich „befugt" und nicht verpflichtet ist, den Betroffenen zu informieren bzw eine Beschwerde an die DSK zu richten. *Vogl* vertritt dazu die Ansicht, dass sich aus dem Umstand, dass im SPG und im MBG dasselbe Rechtsschutzbedürfnis bestehe wie in der StPO, ergebe, dass auch das SPG und das MBG trotz des in eine andere Richtung weisenden Wortlauts eine Verpflichtung des Rechtsschutzbeauftragten aufstellen[509]. Diese auf ein systematisches Argument gestützte Auffassung ist zumindest problematisch, da eine Interpretation, die „befugt" als „verpflichtet" versteht, eigentlich nicht mehr vom äußerst möglichen Wortsinn des ersteren Begriffes gedeckt ist[510], drückt erstere Bestimmung doch ein Dürfen und letztere ein Müssen aus. Überdies könnte aus dem Mangel einer Informationspflicht im MBG und SPG im Gegensatz zur StPO auch gerade der gegenteilige Schluss gezogen werden. Dem Wortlaut nach wird dem Rechtsschutzbeauftragten durch die Bestimmungen des SPG und des MBG ein Ermessen eingeräumt. Es handelt sich dem Typ nach um ein so genanntes Handlungsermessen, bei welchem die Behörde entscheiden kann, ob sie überhaupt tätig wird[511]. Vom eingeräumten Ermessen muss ein Organ jedoch stets iSd Gesetzes Gebrauch machen

---

509 *Vogl,* Rechtsschutz und Vollziehung in *BMI* (Hrsg), Der Rechtsschutzbeauftragte (2004) 20 mwN; *ders,* Der Rechtsschutzbeauftragte in Österreich (2004) 105; aus den von ihm zitierten Materialien – insbesondere der Bericht des Ausschusses für innere Angelegenheiten, BlgNR 223, XXI. GP, 2 – lassen sich für die heutige Rechtslage keine treffsicheren Schlüsse mehr ziehen.

510 Raschhofer, in *Zankl* (Hrsg), Auf dem Weg zum Überwachungsstaat? (2009) 114.

511 *Walter/Mayer/Kucsko-Stadlmayer,* Bundesverfassungsrecht[10] (2007) Rz 575.

(Art 130 Abs 2 B-VG)[512]. Das Ermessen ist so gesehen immer gebunden, ein völlig willkürliches freies Ermessen ist von Verfassungs wegen unzulässig[513]. Die zu treffende Entscheidung darf nicht auf Willkür beruhen, sondern muss sich aus sachlichen Ableitungen aus im Gesetz vorgegebenen Kriterien ergeben[514]. Da die Behörde ihr Ermessen „im Sinne des Gesetzes" auszuüben hat, muss sich ein solcher dem Gesetz entnehmen lassen. Das Gesetz muss das Organhandeln in einem solchen Maß determinieren, dass der VwGH und der VfGH in der Lage sind, die Übereinstimmung der Rechtsakte des Organs mit dem Gesetz zu überprüfen[515]. Es reicht aus, wenn der ermessensleitende Sinn des Gesetzes aus dem Gesetz erschließbar ist.

Fraglich ist jedoch, ob sich die zu Art 130 Abs 2 B-VG in Judikatur und Literatur angestellten Überlegungen überhaupt auf die Tätigkeit von Rechtsschutzbeauftragten übertragen lassen. In Art 130 B-VG geht es um die gerichtliche Kontrolle des Verwaltungshandelns durch den VwGH, der über die Beschwerden gegen Bescheide der Behörden einschließlich der UVS und deren Säumnis zu entscheiden hat. Die Tätigkeit des Rechtsschutzbeauftragten ist von der Kontrolle durch den VwGH nicht erfasst, seine Entscheidungen sind nicht bekämpfbar. Es ist bereits fraglich, ob man den Rechtsschutzbeauftragten als „Behörde" iSd Art 130 B-VG qualifizieren kann[516]. Nach *Vogl* kommt ihm beispielsweise im Verfahren vor der DSK mangels Verwaltungsorganstellung nicht die Rolle einer Amtspartei, sondern jene einer Formalpartei zu[517]. ME kann an der Eigenschaft der Rechtsschutzbeauftragten im SPG und MBG als Verwaltungsorgan kein Zweifel bestehen. So erfolgte etwa früher[518] die Weisungsfreistellung[519] des Rechtsschutzbeauftragten im Verfassungsrang. Der VfGH meinte in einem Erkenntnis, dass die einfachgesetzlich normierte Weisungsfreiheit des

---

[512] Vgl etwa auch VwGH, 22.6.2006, 2006/21/0109.

[513] *Antoniolli/Koja,* Allgemeines Verwaltungsrecht[3] (1996) 253.

[514] *Adamovich/Funk,* Allgemeines Verwaltungsrecht[3] (1987) 121.

[515] Vgl etwa VwGH 8.7.2004, 2004/07/0032, VwSlg 16405 A/2004.

[516] Zur Frage der Stellung des Rechtsschutzbeauftragten als Verwaltungsorgan vgl etwa *Jabloner,* Verfassungsrechtliche Probleme um die Rechtsschutzbeauftragten, in *Pilgermair* (Hrsg), Festschrift für Herbert Steininger zum 70. Geburtstag (2003) 23 (25ff).

[517] *Vogl,* Der Rechtsschutzbeauftragte n Österreich (2004) 68 mwN.

[518] Durch BGBl I 2/2008 wurde dem Art 20 B-VG ein Abs 2 angefügt, welcher bestimmt, dass durch einfaches Bundesgesetz Organe zur Kontrolle der Wahrung der Gesetzmäßigkeit der Verwaltung von der Bindung an Weisungen der ihnen vorgesetzten Organe freigestellt werden können. Daher ist es möglich, dass seit 1.1.2008 Weisungsfreistellungen von Rechtsschutzbeauftragten (§§ 57 Abs 1 MBG, 91a Abs 1 SPG) im einfachgesetzlichen Rang normiert werden, ohne gegen Art 20 Abs 1 B-VG zu verstoßen.

[519] Vgl zu dieser *Raschhofer*, in *Zankl* (Hrsg) Auf dem Weg zum Überwachungsstaat? (2009) 115ff.

Rechtsschutzbeauftragten im MBG[520] Art 20 Abs 1 B-VG widersprach. Daher war es bis zur Novelle des Art 20 B-VG durch BGBl I 2/2008 nötig, auch den Rechtsschutzbeauftragten im SPG im Verfassungsrang weisungsfrei zu stellen. Das zeigt, dass er zumindest als ein Organ iSd Art 20 B-VG gesehen wird, da sich sonst aus der einfachgesetzlichen Weisungsfreistellung kein Widerspruch zu Art 20 B-VG ergeben hätte. Auch bei Rechtsschutzbeauftragten handelt es sich um Zuständigkeitsbündel und somit um Verwaltungsorgane[521]. Auch der VfGH qualifiziert den Rechtsschutzbeauftragten als Verwaltungsorgan[522].

Würde man annehmen, dass dem Rechtsschutzbeauftragten ungebundenes Ermessen in dem Sinn eingeräumt wird, dass er in seiner Entscheidung völlig frei wäre und sich nicht von vorgegebenen Prinzipien leiten lassen muss, wäre die Bestimmung wohl verfassungswidrig. Wenn sich nicht zumindest der Sinn der Ermessensübung und damit der teleologische Rahmen für die Orientierungskriterien des Organs aus dem Gesetz entnehmen lassen, widerspricht die Bestimmung dem Legalitätsprinzip[523]. Dass der Sinn des Gesetzes die Wahrnehmung von Rechten des Betroffenen ist, die dieser mangels Kenntnis nicht selber wahrnehmen kann, steht wohl unbestreitbar fest. Dass es diesem Sinn eindeutig zuwider laufen würde, wenn der Rechtsschutzbeauftragte im Falle der Wahrnehmung von Rechtsverletzungen willkürlich entscheiden könnte, nichts für den Betroffenen zu unternehmen, liegt auch auf der Hand. Somit ist *Vogl* im Ergebnis zu folgen und festzuhalten, dass die Rechtsschutzbeauftragten nach dem SPG und dem MBG im Falle der Wahrnehmung von Rechtsverletzungen zur Information bzw Beschwerdeeinbringung nicht nur befugt, sondern auch verpflichtet sind.

Insofern entschärft sich das Problem, dass der Rechtsschutzbeauftragte lediglich „befugt" ist. Es bleibt jedoch noch immer das Problem, dass der durch den Rechtsschutzbeauftragten ausgeübte kommissarische Rechtsschutz wie oben beschrieben im Vergleich zu einem persönlich durch den Betroffenen ausgeübten Rechtsschutz ein qualitatives Minus darstellt, weil es auch Fälle geben kann, in denen der Rechtsschutzbeauftragte die letztlich falsche Ansicht vertritt, es liege keine

---

[520] VfGH, 23.1.2004, G 363/02, VfSlg 17.102: der VfGH sprach aus, dass die Weisungsfreistellung im damaligen § 57 Abs 3 MBG mit Blick auf die Gewährleistung eines effizienten Rechtsschutzes zwar konsequent sei, aber schon zufolge der verfassungsrechtlichen Systematik (Art 20 B-VG) einer verfassungsrechtlichen Grundlage bedürfe.

[521] „Organe" sind Zuständigkeitsbündel, wenn diese mit hoheitlichen Befugnissen ausgestattet sind, handelt es sich um Behörden: *Antoniolli/Koja,* Allgemeines Verwaltungsrecht[3] (1996) 331

[522] VfGH 23.1.2004, G 363/02, so im Ergebnis auch *Jabloner,* Verfassungsrechtliche Probleme um die Rechtsschutzbeauftragten, in *Pilgermair* (Hrsg) Festschrift für Herbert Steininger zum 70. Geburtstag (2003) 23 (31).

[523] *Adamovich/Funk,* Österreichisches Verfassungsrecht[3] (1985) 242.

Rechtsverletzung vor. Aus diesem Grund kommt es für den Betroffenen entscheidend darauf an, dass der Access-Provider seine vertragliche Nebenpflicht zur Information erfüllt. Nur diese vermag es jene Rechtsschutzlücke zu schließen, die dadurch entsteht, dass der Rechtsschutzbeauftragte eine für den Betroffenen ungünstige Rechtsansicht vertritt. Nur der Vollständigkeit halber sei hier nochmals erwähnt, dass diese Pflicht nur insoweit besteht, als sich der Access-Provider dadurch nicht dem Risiko einer Straf- bzw Haftbarkeit aussetzt (vgl oben Kapitel 5.5.6).

5.5.7. Die allgemeine Frage nach einer Pflicht des Access-Providers zur Verteidigung der Kundendaten

Es stellt sich die Frage, ob man über den Weg ergänzender Vertragsauslegung auch zu einer Nebenpflicht des Access-Providers kommt, wonach er die Daten seiner Kunden gegenüber der Auskunft suchenden Stelle zu verteidigen hat und wie weit diese Pflicht bejahendenfalls reicht. Unter „Verteidigung" wird im Folgenden in erster Linie die gewissenhafte Überprüfung des von der Auskunft suchenden Stelle an den Access-Provider heran getragenen Auskunfts- bzw Mitwirkungsbegehrens verstanden. Je nach dem Ergebnis dieser Prüfung können darunter weitere Handlungen des Access-Providers fallen: Kommt der Access-Provider zu dem Ergebnis, das Begehren wurde zu Recht an ihn gerichtet, hat er diesem zu entsprechen um sich nicht dem Risiko auszusetzen, sich straf- bzw haftbar zu machen. Sollten die Angaben, auf welche sich die Auskunft suchende Stelle stützt, gemessen an den gesetzlichen Vorgaben unvollständig sein, stellt sich die Frage, inwieweit der Access-Provider darauf drängen muss, dass diese Angaben vervollständigt werden. Sollte er zum Ergebnis gelangen, dass das Auskunftsbegehren unberechtigt ist oder zumindest Zweifel an der Rechtmäßigkeit hegen, wird weiter zu untersuchen sein, inwieweit er sich gegen die Auskunft suchende Stelle stellen muss. Zu klären wird also sein, ob er etwa Rechtsmittel ergreifen muss oder ihn eine Verweigerungspflicht trifft. Soweit er den Kunden über die Beauskunftung informiert und ihn dadurch in die Lage versetzt, seine Rechte selbst wahrzunehmen, scheidet eine Pflicht zur Ergreifung von Rechtsmitteln mE jedenfalls aus. Diesfalls hat sich der Kunde um die Verfolgung seiner Ansprüche zu kümmern. Da, wie oben gezeigt, das Gesetzesrecht bei der ergänzenden Vertragsauslegung eine besondere Rolle spielt, ist in diesem Zusammenhang auf das Kommunikationsgeheimnis sowie § 108 TKG 2003 hinzuweisen, der die unbefugte Mitteilung des Access-Providers über die Tatsache oder den Inhalt des Telekommunikationsverkehrs bestimmter Personen an einen Unberufenen unter Verwaltungsstrafe stellt. Daraus lässt sich die Wertung des Gesetzgebers ableiten, dass der Access-Provider die Daten seiner Kunden zu schützen hat.

Da es bezüglich der Frage einer „Verteidigungspflicht" der Kundendaten in besonderem Maße auf die Beschaffenheit der einzelnen Auskunftsbestimmung ankommt,

werden sich manche Fragen erst im Zusammenhang mit den noch weiter unten zu erörternden Auskunftsbestimmungen klären lassen. Hier können nur allgemeine Aspekte festgehalten werden.

Die Erfüllbarkeit dieser Pflichten zur Verteidigung der Kundendaten hängt in höherem Maße, als das bei den oben erörterten Informationspflichten der Fall ist, von der konkreten Ausgestaltung der Auskunfts- bzw Mitwirkungsbestimmungen ab. Je mehr Informationen die Auskunft suchende Stelle zur Begründung des Auskunftsbegehrens zu liefern hat, desto umfangreicher wird die Entscheidungsbasis des Access-Providers. Je mehr Material ihm zur Verfügung steht, anhand dessen er die Begründetheit des Auskunftsbegehrens überprüfen kann, desto angezeigter scheint es, ihn in die Pflicht zu nehmen. Weiters gibt es Auskunftsbestimmungen die sich ausdrücklich mit der Verantwortlichkeit des Access-Providers auseinandersetzen, so etwa § 98 TKG 2003, der bestimmt, dass (nur) den Betreiber des Notrufdienstes die Verantwortung[524] für die rechtliche Zulässigkeit des Auskunftsbegehrens trifft. Ob dies allerdings auch dann gelten soll, wenn der Access-Provider von der Rechtswidrigkeit des Auskunftsbegehrens in Kenntnis hat, ist zu bezweifeln[525]. Auf diese Frage wird jedoch noch weiter unten im Zusammenhang mit der Bestimmung des § 98 TKG 2003 eingegangen werden. Weiters spielt es eine Rolle, nach welchem Verfahren der Access-Provider Auskunft zu erteilen hat. Soweit Auskunftsbestimmungen wie § 53 Abs 3b SPG bestimmen, dass die Auskunft „unverzüglich" zu erteilen ist oder dies so wie § 98 TKG 2003[526] nahe legen, sind die Möglichkeiten des Access-Providers zur genauen Prüfung von an ihn herangetragenen Auskunftsbegehren sehr begrenzt. Dies ist bei der Entwicklung von Schutzpflichten zu berücksichtigen.

Von den oben analysierten Benachrichtigungspflichten unterscheidet sich die Pflicht die Kundendaten zu verteidigen schon dadurch, dass hier Automatisierungsprozesse von vornherein ausscheiden. Die Automatisierbarkeit der Erfüllung ergänzender Pflichten hat jedoch einen entscheidenden Einfluss auf die damit

---

524 Damit ist vor allem eine primär nach dem TKG 2003 sowie dem DSG 2000 zu beurteilende Verantwortlichkeit angesprochen, vgl *Singer,* in *Stratil* (Hrsg), Telekommunikationsgesetz 2003[3] (2004) Anm 4 zu § 98.

525 *Raschhofer* in *Zankl* (Hrsg), Auf dem Weg zum Überwachungsstaat? (2009) 96.

526 Nach dieser Bestimmung ist die Notwendigkeit der Informationsübermittlung vom Betreiber des Notrufdienstes zu dokumentieren und dem Betreiber unverzüglich, spätestens jedoch innerhalb von 24 Stunden nachzureichen. Der Betreiber darf die Übermittlung nicht von der vorherigen Darlegung der Notwendigkeit abhängig machen. Daraus folgt, dass dem Access-Provider in jenen Fällen, in denen der Betreiber des Notrufdienstes sich dazu entscheidet die Dokumentation nachzureichen, von vorneherein jegliche Kontrollmöglichkeiten genommen werden. Aufgrund der Notsituation wird man die Bestimmung so auslegen müssen, dass der Access-Provider das Auskunftsbegehren dann unverzüglich zu erfüllen hat.

einhergehenden wirtschaftlichen Belastungen[527]. Eine Prüfung kann sinnvollerweise nur durch einen Menschen erfolgen. Da es sich bei Fragen hinsichtlich der Rechtmäßigkeit bzw Begründetheit von Auskunftsbegehren oft um Rechtsfragen handelt, liegt es nahe, diese Aufgabe nur Menschen mit gewissen juristischen Grundkenntnissen auf diesem Gebiet zu übertragen. Wenn man etwa die in Zusammenhang mit dem noch weiter unten näher zu erörternden § 87b Abs 3 UrhG aufgeworfenen komplexen Rechtsfragen betrachtet[528], wird klar, dass diese eigentlich nur von auf den Gebieten des Zivil-, Datenschutz-, Verfassungs- und Europarechts versierten Juristen gelöst werden können. Dies führt auf Seiten des Access-Providers zu einem recht hohen Personalaufwand. Das gilt schon für die reine Überprüfung des Auskunftsbegehrens und noch viel mehr für die Ergreifung von Rechtsbehelfen. Wie wir oben gesehen haben, dürfen die mit ergänzenden Vertragspflichten verbundenen ökonomischen Konsequenzen nicht außer Acht gelassen werden. Da die mit Verteidigungspflichten einhergehenden wirtschaftlichen Belastungen relativ hoch sind, kann hier die allgemeine Feststellung getroffen werden, dass bei der Entwicklung von „Verteidigungspflichten" die Berücksichtigung der wirtschaftlichen Sphäre beim Access-Provider besonders berücksichtigt werden muss.

5.5.8. Die Prüfung des Auskunftsbegehrens

5.5.8.1. Die Frage nach der Rechtmäßigkeit der Speicherung

Der Frage, ob das an den Access-Provider heran getragene Auskunfts- bzw Mitwirkungsbegehren berechtigt ist, ist die Frage, ob er zu dessen Erfüllung überhaupt in der Lage ist, logischerweise vorgelagert. Dieser Zusammenhang ist in dem jüngsten Erkenntnis des OGH in der Sache *LSG gegen Tele 2*[529] deutlich geworden. Die Erfüllung von Auskunftsbegehren setzt meist voraus, dass der Access-Provider bestimmte Daten speichert, die er im Falle eines Auskunftsbegehrens miteinander verknüpfen kann. So kann er einem auf die Identität einer hinter einer bestimmten IP-Adresse stehenden Person gerichteten Auskunftsbegehren nur dann nachkommen, wenn er überhaupt speichert, wann er wem welche IP-Adresse aus seinem Pool zuwies.

Wie bereits (in Kapitel 4.5.7) dargelegt, ist die Speicherung von Verkehrsdaten in Art 6 der EK-Datenschutzrichtlinie und – umsetzend – in § 99 TKG geregelt. Diese Bestimmungen stellen ab dem Zeitpunkt der Verbindungsbeendigung grundsätzlich eine Löschungs- bzw Anonymisierungsverpflichtung auf. Die möglichen vier

---

[527] *Feiler*, in *Zankl* (Hrsg), Auf dem Weg zum Überwachungsstaat? (2009) 77.

[528] OGH 14.7.2009 4 Ob 41/09x, MR 2009, 251.

[529] OGH 14.07.2009, 4 Ob 41/09x, MR 2009, 251.

Ausnahmen (Verarbeitung zu Verrechnungszwecken, zu Marketingzwecken und für Zusatzdienste, Vorratsdatenspeicherung, aufgrund besonderer gesetzlicher Vorschriften) wurden bereits oben ausführlich erläutert. Nur wenn sich der Access-Provider auf eine der vier Ausnahmen stützen kann, ist die Verarbeitung von Verkehrsdaten nach Verbindungsbeendigung ausnahmsweise zulässig.

Was gilt jedoch, wenn ein Auskunftsbegehren zwar faktisch erfüllt werden kann, dies jedoch nur bei Verarbeitung unzulässig gespeicherter Verkehrsdaten möglich ist? Diese Frage wurde durch den OGH in der Entscheidung *LSG gegen Tele 2* eindeutig beantwortet. Wenn die zur Bearbeitung erforderlichen Verkehrsdaten nicht vorhanden sein dürften (und es aber rechtswidrigerweise sind), darf ein Auskunftsbegehren nicht erfüllt werden: „[...] *Damit müssen Ansprüche nach § 87b Abs 3 UrhG derzeit aus gemeinschaftsrechtlichen Gründen am Speicherverbot und der Löschungsverpflichtung nach § 99 Abs 1 TKG 2003 (Art 6 Abs 1 RL 2002/58/EG) scheitern, wenn diese nur durch eine Verarbeitung von Verkehrsdaten erfüllt werden können (Wiebe, Beilage zu MR 2005/4, 12 ff). Es mag zwar zutreffen, dass § 87b Abs 3 UrhG dadurch seine praktische Wirksamkeit verliert, soweit dynamische IP-Adressen verarbeitet werden müssten [...] Das [Scheitern des Auskunftsanspruches, Anm] gilt auch dann, wenn die Beklagte diese Verarbeitung bereits durchgeführt haben sollte. Denn die Zulässigkeit der Weitergabe von Stammdaten kann nicht davon abhängen, ob das dafür erforderliche rechtswidrige Verarbeiten von Verkehrsdaten im Zeitpunkt der Anspruchserhebung oder der darüber ergehenden Entscheidung schon erfolgt war oder nicht.*" Der Access-Provider darf daher einem Auskunftsbegehren in diesen Fällen keinesfalls nachkommen. Dies gilt schon aufgrund der objektiven Rechtslage. Es wird ihn daher auch die vertragliche Pflicht treffen, die Privatsphäre seines Kunden soweit zu schützen, dass er die Erfüllung von Auskunftsbegehren verweigert, denen er nur durch die Verwendung unzulässig verarbeiteter Daten entsprechen könnte. Der Access-Provider wird daher als ersten Schritt immer zu überprüfen haben, ob er die bei ihm vorhandenen Daten auch rechtmäßig speicherte. Verneinendenfalls hat er die Erfüllung zu verweigern.

5.5.8.2. Die Frage nach der Zweckbindung rechtmäßig gespeicherter Daten

Aber selbst wenn der Access-Provider die (Verkehrs-)daten rechtmäßig – etwa zu Verrechnungszwecken – speichert, stellt sich die Frage, inwieweit er diese für die Bearbeitung von Auskunftsbegehren verarbeiten darf, die anderen Zwecken als dem eigentlichen Speicherungszweck dienen[530]. Da es schon jetzt Fälle gibt, in denen der

[530] Vgl etwa *Spindler,* Der Auskunftsanspruch gegen Verletzer und Dritte im Urheberrecht nach neuem recht, ZUM 2008, 640 (646), der für eine Verwertbarkeit von Daten, die zu Verrechnungszwecken gespeichert wurden, auch für urheberrechtliche Auskunftsansprüche eintritt.

Access-Provider völlig legal Verkehrs- und Standortdaten auch nach Beendigung der Verbindung speichern darf (und teilweise sogar muss), stellt sich die Frage schon hinsichtlich der derzeitigen Rechtslage. Dieses Problem wird aber vor allem nach der Umsetzung der Vorratsdatenspeicherungsrichtlinie schlagend werden, da dann Gewissheit bestehen wird, dass jeder Access-Provider die Daten zumindest für sechs Monate auf Vorrat speichert. Er kann dann nicht mehr einwenden, dass er die zur Erfüllung des Auskunftsbegehrens nötigen Daten gar nicht mehr habe. Der aktuelle Umsetzungsentwurf zur VDS-Rl ist sich dieser Problematik wie oben bereits erwähnt (siehe Kapitel 4.5.7.2) in besonderem Maße bewusst. Er ist vom wesentlichen Gedanken getragen, dass (reine) Vorratsdaten auch nur für die in der Vorratsdatenspeicherungsrichtlinie genannten Zwecke verwendet werden sollen. Der Umsetzungsentwurf enthält daher im einzufügenden § 99 Abs 5 Z 2 eine genaue Beschreibung jener Fälle, in denen Verkehrsdaten zu Auskunftszwecken des SPG verarbeitet werden dürfen.

Daten für einen Zweck zu speichern und für einen anderen Zweck zu verarbeiten widerspricht dem grundlegenden datenschutzrechtlichen Prinzip der Zweckbindung[531]. Dazu normiert Art 6 Abs 1 lit c der allgemeinen Datenschutzrichtlinie entsprechend deren 27. Erwägungsgrund, dass personenbezogene Daten den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen (vgl auch § 7 DSG 2000)[532]. Es handelt sich hierbei um einen seit jeher das Datenschutzrecht sowohl auf österreichischer[533] als auch auf europäischer Ebene[534] kennzeichnenden Grundsatz. Art 6 Abs 1 der EK-

---

[531] Daher fordern etwa *Czychowski/Nordemann,* Vorratsdaten und Urheberrecht – Zulässige Nutzung gespeicherter Daten, NJW 2008, 3095 (3097ff), zu Unrecht die Verwertbarkeit von Vorratsdaten zu Zwecken der Auskunft gem § 101 Abs 2 iVm Abs 9 dt UrhG; zutreffend *Hoeren,* Vorratsdaten und Urheberrecht – Keine Nutzung gespeicherter Daten, NJW 2008, 3099 (3101), der eine derartige Verarbeitung strikt ablehnt.

[532] Vgl auch zuletzt VfGH, 15.6.2007, G 147/06 ua, VfSlg 18146, ZfV 2008, 437 (durch automatische Geschwindigkeitsmesssysteme erhobene Daten dürfen ausschließlich zur Feststellung der Überschreitung einer ziffernmäßig festgesetzten Höchstgeschwindigkeit ermittelt und verwendet werden), weiters VfGH 26.1.2006, B1581/03.

[533] § 6 Abs 1 Z 2 und 3 DSG 2000; § 17 Abs 1 DSG 1978; *Dohr/Pollirer/Weiss/Knyrim,* Datenschutzgesetz[2] (6. ErgLf. 2007) § 6 Anm 3; *Duschanek,* Neuerungen und offene Fragen im Datenschutzgesetz 2000, ZfV 2000, 526 (530ff); *Kunnert*, Der Ministerialentwurf für eine DSG-Novelle 2010: Ausgewählte Probleme, jusIT 2009, 102 (103); *Mayer-Schönberger/Zeger/Kronegger,* Auf dem Weg nach Europa: Zur Novellierung des Datenschutzgesetzes, ÖJZ 1998, 244 (248); *Öhlinger,* Auskunftsbefugnisse sowie Auskunfts- und Verschwiegenheitspflichten der Österreichischen Nationalbank, ÖZW 1991, 65 (69); vgl ferner: RV 72 BlgNR XIV. GP, 11: „[...] und die Daten dürfen nur zu dem Zweck verwendet werden, zu dem sie gespeichert wurden."; AB 1036 BlgNR XVI. GP, 2; RV 1613 BlgNR XX. GP, 39; RV 175 BlgNR, XVII. GP, 29.

[534] Art 6 lit b und c der allgemeinen Datenschutz-Rl; Art 5 lit b des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, BGBl 317/1988, EuGH, 8.5.2007, C 73/07, Rz 80ff; vgl auch Generalanwältin *Kokott* in ihrem Schlussantrag vom 18.7.2007 zu C-275/06 in Rz 80: *„Nur die Zwecke der Speicherung*

Datenschutzrichtlinie stellt wie erwähnt eine grundsätzliche Löschungsverpflichtung für Verkehrsdaten nach Beendigung der Verbindung auf, eine Verarbeitung darf dann nur mehr zu ganz bestimmten Zwecken erfolgen. Dennoch wird häufig vertreten, dass etwa zu Betriebszwecken gespeicherte Verkehrsdaten auch für Auskunftszwecke zur Verfügung stehen sollen[535]. Die Normierung von Auskunftspflichten wie beispielsweise § 53 Abs 3a SPG spricht dafür, dass der Gesetzgeber davon ausgeht, dass die dafür notwendigerweise zu verarbeitenden Daten auch für Auskunftszwecke zur Verfügung stehen. Ist diese Auffassung zulässig?

Die Frage, inwieweit ein ursprünglicher Speicherungs- bzw Verarbeitungszweck einer späteren Verarbeitung zu einem nicht kongruenten Auskunftszweck entgegensteht, stellte sich auch im Fall *LSG gegen Tele 2*. Dort bezog der OGH in eindeutiger Weise Stellung:

„[...] Vielmehr ist anzunehmen, dass Art 6 der RI 2002/58/EG und dessen Umsetzung in § 99 TKG 2003 der – im vorliegenden Fall erforderlichen – Verarbeitung von Verkehrsdaten für die Erteilung der hier begehrten Auskunft [gem § 87b Abs 3 UrhG, Anm] entgegensteht. Denn nach Absatz 1 dieser Bestimmung sind Verkehrsdaten, die sich auf Teilnehmer und Nutzer beziehen und vom Betreiber eines öffentlichen Kommunikationsnetzes oder eines öffentlich zugänglichen Kommunikationsdienstes verarbeitet und gespeichert werden, [...] unbeschadet der Absätze 2, 3 und 5 des vorliegenden Artikels und des Artikels 15 Absatz 1 zu löschen oder zu anonymisieren, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden.' Die Absätze 2, 3 und 5 gestatten in weiterer Folge die Verarbeitung (und damit die Speicherung) von Verkehrsdaten für bestimmte Zwecke. Aus diesem Regelungszusammenhang ist abzuleiten, dass eine Verarbeitung von – wenngleich unter Umständen nach den Absätzen 2, 3 und 5 rechtmäßig gespeicherten – Daten für andere Zwecke nicht zulässig ist. Denn die Löschungspflicht hat offenkundig den Zweck, eine unzulässige Nutzung der Daten zu verhindern. Dieser Zweck würde durch die Zulässigkeit der anderweitigen Nutzung rechtmäßig gespeicherter Daten unterlaufen, ohne dass dies durch die Wertung der jeweiligen Ausnahmebestimmungen gedeckt wäre. Zudem verstieße eine solche Auffassung gegen den datenschutzrechtlichen Grundsatz der strikten Zweckbindung,

---

können im Sinne von Art 6 Abs 1 Buchst. b der Richtlinie 95/46 ihre Weitergabe rechtfertigen."

535 *Bär,* Anm zu BVerfG, Beschluss vom 11.3.2008 – 1 BvR 256/08 (Einstweilige Anordnung zur teilweisen Aussetzung der Regelung zur Vorratsdatenspeicherung), MMR 2008, 303 (307); *Jenny,* Eile mit Weile – Vorratsdatenspeicherung auf dem Prüfstand, CR 2008, 282 (283); *Spindler,* Der Auskunftsanspruch gegen Verletzer und Dritte im Urheberrecht nach neuem Recht, ZUM 2008, 640 (646).

wonach Daten, die für einen bestimmten Zweck gespeichert wurden, auch nur für diesen Zweck verarbeitet werden dürfen [...]"[536]

Der OGH hat hier in kaum zu überbietender Deutlichkeit klargestellt, dass auch zulässigerweise gespeicherte Daten nur für jene Zwecke verarbeitet werden dürfen, zu welchen sie gespeichert wurden[537]. Dem OGH ist insbesondere in Bezug auf die Betonung des Zweckbindungsgrundsatzes in aller Entschiedenheit beizupflichten. Er führte weiters aus, dass dies die Verarbeitung von Verkehrsdaten zu Zwecken des Urheberschutzes nicht ausschließe. Die prinzipielle Zulässigkeit der Verwendung von Verkehrsdaten zu Auskunftszwecken findet ihre normative Grundlage in der Ausnahmeklausel des Art 15 der EK-Datenschutzrichtlinie und wurde auch aus gemeinschaftsrechtlicher Perspektive vom EuGH in *Promusicae*[538] festgestellt und in *LSG gegen Tele 2*[539] bestätigt. Mangels ausdrücklicher Vorschrift isd Art 15 EK-Datenschutzrichtlinie, die eine Speicherung für Zwecke der Verfolgung urheberrechtlicher Ansprüche normiert, ist nach Ansicht des OGH die Verarbeitung von Verkehrsdaten für Zwecke des § 87b Abs 3 UrhG jedoch unzulässig. Die Überlegungen des OGH, warum § 87b Abs 3 UrhG keine implizite Speicherverpflichtung enthalte, lassen sich teilweise auch auf die meisten anderen Auskunftsbestimmungen (SPG, MBG, UWG,...) übertragen. Fraglich ist bezüglich dieser Vorschriften etwa, ob sie dem in Art 15 EK-Datenschutzrichtlinie vorgegebenen Kriterium genügen, wonach die Bestimmungen, nach welchen Daten ausnahmsweise aufbewahrt werden dürfen, eine zeitliche Begrenzung vorsehen müssen. Der VfGH vertritt in Bezug auf § 53 Abs 3a SPG die Auffassung, dass auch diese Bestimmung keine Speicherpflicht anordnet. Allerdings hält er eine Verarbeitung von Verkehrsdaten, die rechtmäßigerweise aufbewahrt wurden, für zulässig:

„[...] Gemäß § 99 Abs 2 TKG 2003 dürfen Verkehrsdaten für Zwecke der Verrechnung von Entgelten bis zum Ablauf jener Frist gespeichert werden, innerhalb derer die Rechnung rechtlich angefochten werden oder der Anspruch auf Zahlung geltend gemacht werden kann [...] Der Umfang der verwendeten Verkehrsdaten ist auf das unbedingt notwendige Minimum zu beschränken. Nach diesen Bestimmungen kann es zu einer Speicherung der IP-Adresse beispielsweise zum Zwecke der Verrechnung von Entgelten oder zur Behebung von Störungen (Lösung von Internet-

---

[536] OGH 14.07.2009, 4 Ob 41/09x, MR 2009, 251.

[537] Auch *Zykan,* Zum Verhältnis des Auskunftsanspruchs gem § 87b Abs 3 UrhG zum Datenschutz: OGH 14. 7. 2009, 4 Ob 41/09x – Keine Auskunft über die Identität von Inhabern dynamischer IP-Adressen, jusIT 2009, 206 (207), versteht die Ausführungen des OGH so wie ich.

[538] EuGH 29.1.2008, C 275/06.

[539] EuGH 19.2.2009, C 557/07, MR 2009, 40.

Verbindungsproblemen) kommen. Das SPG idF der Novelle BGBl. I 114/2007 enthält hingegen keine Ermächtigung zur Speicherung von Verkehrsdaten. Somit ist davon auszugehen, dass durch die SPG-Novelle den Betreibern von Telekommunikationsdiensten keine weiter reichenden Speicherverpflichtungen auferlegt wurden, als sie schon bisher bestanden haben. Die hier bekämpften Bestimmungen schaffen Auskunftsverpflichtungen; aus solchen Auskunftsverpflichtungen können jedoch keine zusätzlichen Speicherverpflichtungen abgeleitet werden, sodass diese Auskunftsverpflichtungen nur solche Daten betreffen können, hinsichtlich derer bereits aufgrund der genannten – durch die SPG-Novelle unverändert gebliebenen – Bestimmungen des TKG 2003 die Ermächtigung der Betreiber von Telekommunikationsdiensten zur Speicherung besteht [...]"[540]

In diesem Punkt gibt es daher eine klare Divergenz zwischen OGH und VfGH. Während ersterer eindeutig auf dem Prinzip der Zweckbindung beharrt, kommt es für letzteren hinsichtlich der Zulässigkeit der Verarbeitung nur auf die Rechtmäßigkeit der Speicherung der Daten an. Nach dem TKG etwa für Verrechnungszwecke gespeicherte Verkehrsdaten sollen nach Ansicht des VfGH von Auskunftsverpflichtungen nach dem SPG betroffen sein. Allerdings ist festzuhalten, dass die Ausführungen des VfGH in diesem Punkt nicht zur ratio decidendi gehören. Gegenstand der Entscheidung war der Individualantrag eines Access-Providers[541], mit dem dieser die SPG-Novelle 2007[542] als verfassungswidrig bekämpfte. Der VfGH wies diesen Antrag zurück und begründete dies im Wesentlichen damit, dass es der antragstellenden Gesellschaft an aktueller und unmittelbarer Betroffenheit iSd Art 140 B-VG mangle. Der Access-Provider hatte behauptet, dass die neu geschaffene Norm des § 53 Abs 3a SPG ihn zur Speicherung von Daten in einem Ausmaß von ca 685 Terabyte verpflichten würde. Für die Zurückweisungsentscheidung notwendig war die Auslegung des § 53 Abs 3a SPG nur insoweit, als der VfGH festhielt, dass diese Bestimmung keine Speicherverpflichtung beinhalte. Die weitere Beurteilung, wonach die Sicherheitsbehörden nur auf die anderen nach dem TKG gespeicherten Daten zugreifen können, war für die Zurückweisungsentscheidung nicht notwendig und ist damit obiter dictum. Das trifft zwar auch auf die hier interessierenden Ausführungen des OGH zu, allerdings vermögen letztere mE eher zu überzeugen, vor allem weil sie auch ausdrücklich den Regelungszusammenhang zwischen Art 6 und 15 EK-Datenschutzrichtlinie sowie § 99 TKG und die Teleologie dieser Bestimmungen berücksichtigen. Der OGH ging auf das

---

[540] VfGH 1.7.2009, G 31/08.

[541] T-Mobile Austria GmbH, vgl http://futurezone.orf.at/stories/1618835/ (Stand April 2010).

[542] Bundesgesetzes, mit dem das Sicherheitspolizeigesetz, das Grenzkontrollgesetz und das Polizeikooperationsgesetz geändert werden, BGBl I 114/2007: Mit dieser wurde va § 53 Abs 3a novelliert und der die Stanordermittlung ermöglichende § 53 Abs 3b SPG eingeführt.

Problem, ob rechtmäßig gespeicherte Daten auch für andere Zwecke verwendet werden dürfen, ausführlich und besonders gründlich ein, während der VfGH dieses Problem nur in einem Nebensatz anschnitt und sich der vom OGH berücksichtigen Aspekte vermutlich gar nicht bewusst war. Die Ausführungen des VfGH lassen im Gegensatz zu jenen des OGH jegliches Eingehen auf die europarechtliche Dimension dieses Problems vermissen. Gerade aufgrund dieses Versäumnisses ist jedoch der Begründung des OGH eindeutig der Vorzug zu geben, da sowohl das allgemeine als auch das sektorspezifische Datenschutzrecht im Telekommunikationsbereich der EG das österreichische Datenschutzrecht in dieser Hinsicht in seinen Grundzügen determinieren. Der sich aus der allgemeinen Datenschutzrichtlinie und der EK-Datenschutzrichtlinie ergebende Zweckbindungsgrundsatz wurde nur vom OGH berücksichtigt. Im Ergebnis ist daher grundsätzlich der Auffassung des OGH der Vorzug zu geben. Dies würde allerdings bedeuten, dass die Bestimmungen, die eindeutig zu einer Verarbeitung von Daten führen, die anderen Zwecken als jenen gem den §§ 92ff TKG 2003 dienen (so wie etwa § 53 Abs 3a und 3b SPG oder § 22 Abs 2a MBG), per se unzulässig wären. Auf dieses Problem ist noch weiter unten einzugehen.

Hinsichtlich der Prüfung des Auskunftsbegehrens durch den Access-Provider ist allerdings folgendes vorläufiges Zwischenergebnis festzuhalten: Aus dem Zweckbindungsgrundsatz folgt, dass er Verkehrsdaten für Auskunftszwecke nur verarbeiten darf, soweit bereits den Speicherbestimmungen des TKG oder sonstiger Nebengesetze ein entsprechender Speicherungszweck zu entnehmen ist. Das trifft derzeit mE zunächst auf die Bestimmungen der StPO zu. § 92 Abs 2 TKG 2003 bestimmt, dass die Bestimmungen der StPO durch die Bestimmungen des datenschutzrechtlichen zwölften Abschnitts des TKG unberührt bleiben. Weiters verpflichtet § 94 Abs 2 TKG 2003 den Betreiber, an der Überwachung einer Telekommunikation nach den Bestimmungen der Strafprozessordnung im erforderlichen Ausmaß mitzuwirken. Daraus folgt, dass sämtliche Bestimmungen, die für die Verwendung von Daten durch Access-Provider Beschränkungen vorsehen, unter dem Vorbehalt der Bestimmungen der StPO stehen. Soweit die Verarbeitungszwecke im TKG 2003 eingeschränkt werden, gilt dies nur unter dem Vorbehalt besonderer Bestimmungen der StPO. Letztere genügen mE auch den Anforderungen, die Art 15 Abs 1 EK-Datenschutzrichtlinie an die Vorschriften stellt, durch welche der in Art 5 und 6 leg cit vorgesehene Schutz durchbrochen werden soll. Der in Art 15 EK-Datenschutzrichtlinie in Bezug genommene Art 13 der allgemeinen Datenschutzrichtlinie erlaubt eine Durchbrechung der Löschungsverpflichtung (Art 6 EK-Datenschutzrichtlinie) und der Vertraulichkeit der elektronischen Kommunikation (Art 5 EK-Datenschutzrichtlinie) für den Zweck der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten und für Zwecke der Landesverteidigung.

5.5.8.3. Zweckbindungsgrundsatz und Auskunftsbestimmungen außerhalb der StPO

Etwas anders verhält es sich bei den Auskunftsbestimmungen des SPG (§ 53 Abs 3a und 3b) und des MBG (§ 22 Abs 2a MBG) und sonstiger Auskunftsbefugnisse außerhalb der StPO. Hinsichtlich des SPG sprach der VfGH wie erwähnt aus, dass das SPG dem Access-Provider keine zusätzlichen Speicherverpflichtungen auferlege. Diese Überlegung wird wohl auch für die ganz ähnlich gelagerte Bestimmung des MBG gelten. Da auch das TKG keine Speicherverpflichtungen für die Zwecke sicherheitspolizeilicher Aufgaben bzw Aufgaben der nachrichtendienstlichen Aufklärung oder Abwehr aufstellt, scheinen solche Auskunftsansprüche auf den ersten Blick am oben skizzierten Zweckbindungsgrundsatz zu scheitern[543]. Man könnte behaupten, diese Bestimmungen ermöglichen eine Verarbeitung zu Zwecken, die sich unter keinen der im TKG 2003 aufgezählten Speicherungszwecke subsumieren lassen. Wenn man sich die oben skizzierten Ausführungen des OGH in Erinnerung ruft, warum § 87b Abs 3 UrhG keine Vorschrift iSd Art 15 Abs 1 EK-Datenschutzrichtlinie ist, dann spricht einiges dafür, diese Überlegungen auch auf andere Auskunftsbestimmungen zu übertragen.

Dem Gesetzgeber steht es jedoch frei, den Speicherungszweck für bestimmte Datenkategorien festzulegen, wo immer es ihm angemessen erscheint. Er wird durch Vorgaben der Datenschutzrichtlinien auf europäischer Ebene nicht verpflichtet, dies im unmittelbaren Regelungsumfeld telekommunikationsrechtlicher Bestimmungen zu tun. So untersuchte der OGH in der Sache *LSG gegen Tele 2* wie geschildert die Frage, ob etwa § 87b Abs 3 UrhG den Charakter einer Vorschrift iSd Art 15 Abs 1 EK-Datenschutzrichtlinie habe, was er jedoch letztlich verneinte. Aus dieser Bestimmung ergebe sich keine Speicherverpflichtung. Auch wenn die Bestimmungen des SPG und des MBG keine zusätzlichen Speicherverpflichtungen aufstellen, so ist dennoch möglich und mE geboten, sie so auszulegen, dass sie für aus sonstigen Gründen rechtmäßig gespeicherte Daten den Speicherungszweck erweitern. Diese Bestimmungen zielen eindeutig darauf ab, dass der Access-Provider den Behörden helfen soll, seinen Kunden anhand der bekannt gegebenen Verkehrsdaten (etwa Teilnehmernummer oder IP-Adresse) gegenüber der Behörde zu identifizieren (bzw zu lokalisieren). Insofern unterscheiden sie sich von § 87b Abs 3 UrhG, der nicht eindeutig die Verarbeitung von Verkehrsdaten erwähnt. Auch aus den Materialien zum SPG ergibt sich eindeutig, dass der Gesetzgeber eine Verarbeitung von Verkehrsdaten zu Auskunftszwecken gestatten

---

[543] *Klingenbrunner/Bresich,* Telekommunikationsunternehmen: Beschränkter Rechtsschutz gegen Polizeihandeln, ecolex 2008, 475 (476) lösen das Spannungsverhältnis zwischen TKG und den Auskunftsbestimmungen im SPG, indem sie letztere als lex specialis et posterior zu ersterem sehen. Angesichts der diffizilen Überlegungen des OGH zum Zweckbindungsgrundsatz scheint diese Lösung jedoch etwas zu kurz geraten.

wollte[544]. Ob sich der Gesetzgeber der gemeinschaftsrechtlichen Problematik des Verarbeitens von Verkehrsdaten bewusst war, geht nicht klar aus den Materialien hervor, ist jedoch zu bezweifeln. Dasselbe gilt jedoch für § 87b Abs 3 UrhG und in diesem Fall wertete dies der OGH als Indiz dafür, dass § 87b Abs 3 UrhG keine implizite Speicherverpflichtung enthalte und deshalb keine Vorschrift iSd Art 15 EK-Datenschutzrichtlinie darstelle[545]. Anders als im Falle des § 87b Abs 3 UrhG sprechen die Bestimmungen des SPG und des MBG die Verarbeitung von Verkehrsdaten jedoch ausdrücklich an[546]. Da der Gesetzgeber auch durch diese keine Speicherverpflichtung einführte[547], können die Bestimmungen des SPG und des MBG nur so verstanden werden, dass sie bewirken, dass rechtmäßig gespeicherte Verkehrsdaten auch für die Zwecke sicherheitspolizeilicher Aufgaben bzw Aufgaben der nachrichtendienstlichen Aufklärung oder Abwehr zur Verfügung stehen sollen[548].

Es bleibt also nur noch zu klären, ob diese Bestimmungen den Erfordernissen des Art 15 Abs 1 EK-Datenschutzrichtlinie entsprechen. Es stellt sich die Frage, ob die Zwecke, zu denen Auskünfte nach dem SPG bzw MBG eingeholt werden dürfen, den in Art 15 Abs 1 EK-Datenschutzrichtlinie normierten Zwecken entsprechen. Hinsichtlich der SPG-Befugnisse kommen die Verhütung von Straftaten, sowie der Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen in Betracht, hinsichtlich des MBG die Sicherheit des Staates und die Landesverteidigung. Abgesehen von der Verhütung von Straftaten und der Landesverteidigung sind all diese Zwecke nicht in Art 15 Abs 1 EK-Datenschutzrichtlinie normiert, sondern lediglich in Art 13 Abs 1 der allgemeinen Datenschutzrichtlinie. Art 15 EK-Datenschutzrichtlinie verweist zwar auf Art 13 der allgemeinen Datenschutzrichtlinie, enthält jedoch gleichzeitig selbst einen Katalog von Ausnahmegründen. Insofern drängt sich die Frage auf, inwieweit der Verweis in der EK-Datenschutzrichtlinie sich auch auf die in der allgemeinen Datenschutzrichtlinie angeführten Ausnahmegründe bezieht. Bei systematischer Betrachtungsweise wäre dies

---

[544] RV 272 BlgNR XXIII. GP, 5; zur ursprünglichen Einführung von § 53 Abs 3a SPG durch BGBl I 146/1999 vgl RV 1479 BlgNR XX. GP, 19; hinsichtlich § 22 Abs 2a MBG vgl *Hauer/Keplinger/Kreutner,* Militärbefugnisgesetz (2005) § 22 A 20ff; *Raschauer/Wessely,* Militärbefugnisgesetz[2] (2007) § 22 Anm 5.

[545] Vgl auch *Guggenbichler* in *Ciresa* (Hrsg), Österreichisches Urheberrecht (12. ErgLf. 2009) § 87b Rz 16.

[546] Eine ausdrückliche Bezugnahme auf die Verarbeitung von Verkehrsdaten lassen sowohl die Materialien zur Urheberrechtsnovelle 2003 (BGBl I 32/2003; RV 40 BlgNR XXII. GP, 22) als auch jene zur Urheberrechtsnovelle 2006 (BGBl I 81/2006, RV 1324 BlgNR XXII. GP, 4) vermissen, während bei § 53 Abs 3a SPG schon im Gesetz ausdrücklich die Rede etwa von einer IP-Adresse ist.

[547] Zumindest sieht das der VfGH so, siehe oben.

[548] Eine ähnliche Auffassung wird in Deutschland von manchen etwa hinsichtlich § 101 Abs 9 dt UrhG vertreten: *Spindler,* Der Auskunftsanspruch gegen Verletzer und Dritte im Urheberrecht nach neuem Recht, ZUM 2008, 640 (646); *Jenny,* Eile mit Weile – Vorratsdatenspeicherung auf dem Prüfstand, CR 2008, 282 (283).

eher zu verneinen, da manche Ausnahmegründe in beiden Richtlinien vorkommen, während andere ausschließlich in der EK-Datenschutzrichtlinie (zB Feststellung und Verfolgung des Gebrauchs von elektronischen Kommunikationssystemen) oder in der allgemeinen Datenschutzrichtlinie (Schutz der Rechte anderer) vorkommen. Zumindest hinsichtlich der gemeinsamen Schnittmenge an Ausnahmegründen hätte man sich in Art 15 EK-Datenschutzrichtlinie die Aufzählung konkreter Ausnahmegründe schlicht sparen und einfach auf die allgemeine Datenschutzrichtlinie verweisen können. Überdies ist prinzipiell davon auszugehen, dass die Bestimmungen des sektorspezifischen Datenschutzes der EK-Datenschutzrichtlinie zu den Bestimmungen der allgemeinen Datenschutzrichtlinie die leges speziales sind[549]. Die Generalanwältin *Kokott* argumentierte diesen Umstand in ihrem Schlussantrag zur Rechtssache *Promusicae* sehr präzise[550]. Sie verweist etwa auf die anderen sprachlichen Fassungen der EK-Datenschutzrichtlinie, aus denen recht klar hervorgeht, dass sich der Verweis in Art 15 Abs 1 nur auf die sonstigen Regelungen in Art 13 der allgemeinen Datenschutzrichtlinie, nicht jedoch auf die dort aufgezählten Ausnahmegründe bezieht[551]. Überdies führt sie auch historische Erwägungen an und stellt fest, dass der Rat von einem umfassenden Verweis auf Art 13 der allgemeinen Datenschutzrichtlinie bewusst Abstand genommen habe. Obwohl die Generalanwältin ihre Auffassung gut begründete, griff sie der EuGH in der nachfolgenden Entscheidung nicht auf und überging die an sich sehr überzeugende Argumentation[552]. Somit ist die Rechtsansicht der Generalanwältin als durch die Rechtsprechung des EuGH überholt anzusehen und die in der EK-Datenschutzrichtlinie normierten Verpflichtungen können auch aus den in Art 13 der allgemeinen Datenschutzrichtlinie aufgezählten Gründen durchbrochen werden.

Es spricht noch ein weiterer Aspekt, den der OGH in *LSG gegen Tele 2* unberücksichtigt ließ, dafür, dass die Auskunftsbestimmungen im SPG oder MBG Vorschriften iSd Art 15 Abs 1 Datenschutzrichtlinie darstellen. Der OGH konzentrierte sich in der Entscheidung LSG gegen Tele 2 auf die Frage, ob § 87b Abs 3 UrhG eine

---

549 So bestimmt Art 1 Abs 2 der EK-Datenschutzrichtlinie: *„Die Bestimmungen dieser Richtlinie stellen eine Detaillierung und Ergänzung der Richtlinie 95/46/EG im Hinblick auf die in Absatz 1 genannten Zwecke dar. Darüber hinaus regeln sie den Schutz der berechtigten Interessen von Teilnehmern, bei denen es sich um juristische Personen handelt.*" Dasselbe ergibt sich aus § 92 TKG 2003; vgl auch zur deutschen Rechtslage *Gramlich,* in *Manssen* (Hrsg), Telekommunikations- und Multimediarecht (19. ErgLf. 2007) C § 91 Rz 34ff; *Sieber/Höfinger,* Drittauskunftsansprüche gegen Provider nach § 101a UrhG gegen Internetprovider zur Verfolgung von Urheberrechtsverletzungen, MMR 2004, 575 (582); *Spindler/Dorschel*, Auskunftsansprüche gegen Internet-Service-Provider, CR 2005, 38 (45ff)

550 *Kokott,* Schlussantrag zu C-275/96 vom 18.7.2007, Rz 85ff.

551 Vgl etwa die französische Fassung „[...] *comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE*", oder die englische „[...] *as referred to in Article 13(1) of Directive 95/46/EC*".

552 EuGH 29.1.2008, C-275/06, Rz 53.

Durchbrechung des Löschungsgrundsatzes in Art 6 Abs 1 EK-Datenschutzrichtlinie enthalte und somit eine Speicherpflicht impliziere. Soweit es aber um den Zugriff und die Verarbeitung auf aus anderen Gründen rechtmäßig gespeicherte Daten geht, stellt sich nur die Frage nach der Durchbrechung des Zweckbindungsgrundsatzes. Art 15 Abs 1 EK-Datenschutzrichtlinie erlaubt nicht nur ein ausnahmsweises Abgehen von der in Art 6 leg cit statuierten Löschungspflicht von Verkehrsdaten, sondern auch eine Beschränkung der Rechte und Pflichten gem Art 5 leg cit. Dieser bestimmt, dass die Mitgliedstaaten die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch innerstaatliche Vorschriften sicherzustellen haben. Weiters haben sie jede Form des Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen als die Nutzer, wenn keine Einwilligung der betroffenen Nutzer vorliegt, zu untersagen, es sei denn, dass diese Personen gemäß Artikel 15 Absatz 1 gesetzlich dazu ermächtigt sind. Mit „Überwachen von Nachrichten und der damit verbundenen Verkehrsdaten" kann nur eine Verarbeitung dieser Daten gemeint sein. Was auf Grundlage der Auskunftsbestimmungen in SPG geschieht, ist daher wohl unter die Formulierung „Überwachung von Nachrichten und der damit verbundenen Verkehrsdaten" zu subsumieren. Die dort normierten Auskunftsbefugnisse führen beim Access-Provider zur Verarbeitung von Verkehrsdaten (etwa der Rufnummer oder der IP-Adresse). Diese Form der Überwachung wird durch den Grundsatz der Vertraulichkeit der Information in Art 5 leg cit grundsätzlich ausgeschlossen, jedoch unter den Voraussetzungen des Art 15 Abs 1 leg cit ausnahmsweise zugelassen. Somit ergibt sich aus Art 15 Abs 1 iVm Art 5 Abs 1 leg cit eine weitere Ausnahme, unter welcher Verkehrsdaten verarbeitet werden dürfen. Die Auskunftsbefugnisse in SPG können daher auch als Ausnahmeregelungen betrachtet werden, durch welche die in Art 5 leg cit aufgestellten Verpflichtungen durchbrochen werden. Die Vorschriften des MBG bzw SPG enthalten also genauso wenig wie § 87b Abs 3 UrhG eine implizite Speicheranordnung, aber sie stellen insoweit Vorschriften iSd Art 15 Abs 1 EK-Datenschutzrichtlinie dar, als sie impliziter den Speicherungszweck für aus anderen Gründen rechtmäßig gespeicherte Daten ausweiten. Die Speicherdauer richtet sich nach dem ursprünglichen Zweck, zu dem die Daten gespeichert werden, also etwa dem Verrechnungszweck.

Wenn man sich dieser Lösung nicht anschließen möchte, scheitern alle Auskunftsansprüche außerhalb der StPO am Zweckbindungsgrundsatz. Dies wäre eine unmittelbare Konsequenz aus der Feststellung des OGH, *„dass eine Verarbeitung von – wenngleich unter Umständen nach den Absätzen 2, 3 und 5 [des Art 6 EK-Datenschutzrichtlinie, Anm] rechtmäßig gespeicherten – Daten für andere Zwecke nicht zulässig ist*". Im Ergebnis läge eigentlich eine Antinomie zwischen den §§ 92ff TKG 2003 und den Auskunftsbestimmungen vor. Allein schon deshalb, weil eine derartige

Auslegung sich in der Praxis jedoch nie durchzusetzen vermag, ist es angezeigt, eine Lösung im obigen Sinne zu finden.

5.6. Zwischenergebnis

Den Access-Provider treffen Schutzpflichten hinsichtlich der Privatsphäre des Kunden. Der Begriff Privatsphäre lässt sich nur schwer abgrenzen und wird vor allem über den fehlenden Öffentlichkeitsbezug definiert. Die Privatsphäre zählte bereits vor dem Zivilrechts-Änderungsgesetz 2004 zu den Persönlichkeitsrechten gem § 16 ABGB und genoss somit bereits vor der Einfügung des § 1328a ABGB zivilrechtlichen Schutz. § 1328a ABGB bestätigte die bereits davor gängige Rechtsprechung, dass schuldhafte und rechtswidrige Beeinträchtigungen der Privatsphäre zum Ersatz der daraus erwachsenden Vermögensschäden verpflichten. Neu ist die Ersatzpflicht für immaterielle Schäden in besonders gravierenden Fällen.

Für die Verletzung der Schutzpflichten hat der Access-Provider nach vertraglichen Maßstäben einzustehen, es gelten sohin die Beweislastumkehr gem § 1298 ABGB, er haftet auch für reine Vermögensschäden und er hat für das Verschulden seiner Gehilfen einzustehen. Die Schutzpflichten können auch nach Abwicklung der wechselseitigen vertraglichen Ansprüche, ja selbst nach der erfolgreichen Anfechtung des Vertragsverhältnisses noch Platz greifen, sie bestehen diesfalls unmittelbar aufgrund des Gesetzes („gesetzliches Schuldverhältnis ohne primäre Leistungspflicht"). Bei aufrechten und gültigen Schuldverhältnissen sind sie als Ergänzung des Parteiwillens in ihrer rein vertraglichen Natur anzuerkennen.

Sachlich können die Schutzpflichten durch das einander entgegen gebrachte Vertrauen und die eingeräumten Einwirkungsmöglichkeiten gerechtfertigt werden. Der Access-Provider hat zumindest theoretisch hinsichtlich der Privatsphäre relativ hohe Einwirkungsmöglichkeiten, da er sich aufgrund des bei ihm entstehenden Datenbestandes ein sehr präzises Bild vom Privatleben seines Kunden machen könnte. Dies hat zur Folge, dass bezüglich seiner Pflichten zum Schutz der Privatsphäre des Kunden von einem relativ hohen Maßstab auszugehen ist. Zusätzlich spielt bei der Konstruktion von Schutzpflichten auch die Dauer und die Intensität eines Schuldverhältnisses eine Rolle. Der Umstand, dass Vertragsverhältnisse von Access-Providern regelmäßig auf längere Dauer angelegt werden, ist bei der Entwicklung von Schutzpflichten zu berücksichtigen. Die Verletzung der Schutzpflichten zieht die in Kapitel 3.2.2 dargestellten Konsequenzen nach sich.

Der Inhalt der Schutzpflichten wird – auch bei ungültigen Vertragsverhältnissen – nach den Regeln ergänzender Vertragsauslegung unter

Orientierung am Prinzip von Treu und Glauben bestimmt. Bei der Ermittlung des hypothetischen Parteiwillens sind in ganz besonderem Maße Wertungen zu berücksichtigen, die sich aus der Rechtsordnung ergeben. So lässt sich am besten objektivieren, was „redliche Parteien" vereinbart hätten. Daraus folgt eine besondere Beachtung des datenschutzrechtlichen Prinzips, dass der Betroffene grundsätzlich immer über die ihn betreffenden Datenverwendungen in Kenntnis gesetzt werden soll, damit er seine Rechte effizient wahrnehmen kann.

Die Schutzpflicht, den Kunden über die Erfüllung von Auskunftsbegehren zu informieren, erscheint angesichts der Möglichkeiten derartige Informationsprozesse weitestgehend zu automatisieren zumutbar. Soweit ihm die Information aufgrund gesetzlicher Verbote (vgl etwa § 138 StPO) verwehrt ist oder ihn das Risiko einer Strafbarkeit trifft, erscheint eine Informationspflicht jedoch unzumutbar. Ein weiterer Grund für die Bejahung einer Informationspflicht ist, dass diese vom Provider relativ einfach erfüllt werden kann und deren Erfüllung den Kunden in die Lage versetzt dessen Rechte wahrzunehmen. Im Bereich der StPO ist eine Informationspflicht durch den Access-Provider jedenfalls deshalb zu verneinen, weil die Staatsanwaltschaft eine Benachrichtigungspflicht trifft (§ 138 Abs 5 StPO).

Inwieweit den Access-Provider eine Pflicht zur Verweigerung von Auskunftsbegehren trifft, hängt sehr von der Ausgestaltung der konkreten Norm ab und kann daher im Detail erst im Zusammenhang mit den einzelnen Auskunftsbestimmungen abgehandelt werden (vgl Kapitel 6). Allgemein gilt es jedoch den datenschutzrechtlichen Grundsatz der Zweckbindung zu berücksichtigen, der vor kurzem auch vom OGH in der Entscheidung *LSG gegen Tele2* betont wurde. Daten dürfen prinzipiell nur für jene Zwecke verwendet werden, zu denen sie ursprünglich angelegt wurden. Hinsichtlich der Auskunfts- und Mitwirkungsbestimmungen gilt es § 92 Abs 2 TKG 2003 zu beachten, wonach die Bestimmungen der StPO durch das TKG 2003 unberührt bleiben. Soweit Bestimmungen außerhalb der StPO die Verwendung personenbezogener Daten zu anderen als im TKG 2003 vorgesehenen Zwecken normieren, besteht auf den ersten Blick ein Konflikt mit dem Zweckbindungsgrundsatz, der nicht über die lex-specialis- bzw lex posterior-Regel gelöst werden kann. Allerdings sprechen historische Argumente dafür, dass es sich bei diesen Bestimmungen um Ausnahmebestimmungen iSd Art 15 EK-Datenschutzrichtlinie handelt. Dieser erlaubt ein ausnahmsweises Abgehen von dem in Art 5 leg cit enthaltenen Verbots der Überwachung von (rechtmäßig verarbeiteten) Verkehrsdaten.

6. Die Auskunftsbestimmungen und sonstige damit zusammenhängende Schutzpflichten

6.1. Die Auskunftsbestimmungen im SPG

6.1.1. Der Wortlaut

§ 53 Abs 3a SPG lautet:

Die Sicherheitsbehörden sind berechtigt, von Betreibern öffentlicher Telekommunikationsdienste[553] (§ 92 Abs 3 Z 1 Telekommunikationsgesetz 2003 – TKG 2003, BGBl. I Nr. 70) und sonstigen Diensteanbietern (§ 3 Z 2 E-Commerce-Gesetz – ECG, BGBl. I Nr. 152/2001) Auskunft zu verlangen über

1. Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses,
2. Internetprotokolladresse (IP-Adresse) zu einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung sowie
3. Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war,

wenn bestimmte Tatsachen die Annahme einer konkreten Gefahrensituation rechtfertigen und sie diese Daten als wesentliche Voraussetzung für die Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben benötigen. Die Bezeichnung eines Anschlusses nach Z 1 kann für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder die Abwehr gefährlicher Angriffe auch durch Bezugnahme auf ein von diesem Anschluss geführtes Gespräch durch Bezeichnung eines möglichst genauen Zeitraumes und der passiven Teilnehmernummer erfolgen. Die ersuchte Stelle ist verpflichtet, die Auskunft unverzüglich und kostenlos zu erteilen.

Abs 3b leg cit lautet:

Ist auf Grund bestimmter Tatsachen anzunehmen, dass eine gegenwärtige Gefahr für das Leben oder die Gesundheit eines Menschen besteht, sind die Sicherheitsbehörden zur Hilfeleistung oder Abwehr dieser Gefahr berechtigt, von Betreibern öffentlicher Telekommunikationsdienste Auskunft

- über Standortdaten und
- die internationale Mobilteilnehmerkennung (IMSI) der von dem gefährdeten Menschen mitgeführten Endeinrichtung zu verlangen
- sowie technische Mittel zu ihrer Lokalisierung zum Einsatz zu bringen.

Die Sicherheitsbehörde trifft die Verantwortung für die rechtliche Zulässigkeit des Auskunftsbegehrens, dessen Dokumentation dem Betreiber unverzüglich, spätestens

---

[553] Die in Abs 3a ebenfalls enthaltene Befugnis, auch von Diensteanbietern iSd § 3 Z 2 ECG Auskünfte zu verlangen, kann wegen der Themenstellung dieser Arbeit außer Betracht bleiben. Hier kann es mit einem Hinweis darauf, dass bei wörtlicher Auslegung reine Diensteanbieter iSd ECG jedoch gar nicht in der Lage sind, zu beurteilen, wem eine bestimmte IP-Adresse zugewiesen war, sondern höchstens eine Aussage darüber treffen können, wer diese zu einem bestimmten Zeitpunkt verwendet, sein Bewenden haben. Vgl dazu *Feiler,* in *Zankl* (Hrsg) auf dem Weg zum Überwachungsstaat? (2009) 81ff.

innerhalb von 24 Stunden nachzureichen ist. Die ersuchte Stelle ist verpflichtet, die Auskünfte unverzüglich und gegen Ersatz der Kosten nach § 7 Z 4 der Überwachungskostenverordnung – ÜKVO, BGBl. II Nr. 322/2004, zu erteilen.

6.1.2. Abs 3a

6.1.2.1. Gefahrensituation

Die Ausübung der Befugnis gem § 53 Abs 3a SPG setzt voraus, dass bestimmte Tatsachen die Annahme einer konkreten Gefahrensituation rechtfertigen. Damit ist keine allgemeine Gefahr bzw kein gefährlicher Angriff iSd § 16 Abs 1 SPG[554] gemeint[555], sondern eine bloße Gefahr für ein Rechtsgut, die etwa auch den verwirklicht wäre, wenn jemand seine Selbstmordabsicht äußert. Die Formulierung „wenn bestimmte Tatsachen die Annahme einer Gefahrensituation rechtfertigen" findet sich im SPG auch noch an anderer Stelle, nämlich in § 28a Abs 1 SPG. In den Materialien zu dieser Bestimmung heißt es, die „Aufgabe der Gefahrenerforschung knüpft an eine Situation an, in der es konkrete Anhaltspunkte für das Bestehen einer sicherheitspolizeilich relevanten Gefahr gibt"[556]. Ob eine Gefahr vorliegt, hat sich aus einer objektiven ex-ante-Beurteilung[557] zu ergeben, ein subjektives Belieben des Organs reicht demnach keinesfalls aus[558]. Die Tatsachen (etwa die Selbstmordankündigung) müssen gewiss sein und sie müssen den Verdacht nach rationalen Gesichtspunkten tragen[559].

Neben der Gefahrensituation ist eine weitere Vorraussetzung, dass die Sicherheitsbehörden die begehrten Daten für die Erfüllung ihrer Aufgaben benötigen. Dabei kommen grundsätzlich sämtliche Aufgaben der Sicherheitspolizei nach dem 2. Teil des SPG in Betracht: Die erste allgemeine Hilfeleistungspflicht (§ 19 SPG), die

---

554 Die Definition des gefährlichen Angriffs iSd § 16 Abs 1 Z 1 SPG findet sich in den Absätzen 2 und 3 leg cit. Demnach ist ein gefährlichen Angriff die Bedrohung eines Rechtsgutes durch die rechtswidrige Verwirklichung des Tatbestandes einer gerichtlich strafbaren Handlung, die vorsätzlich begangen und nicht bloß auf Begehren eines Beteiligten verfolgt wird, sofern es sich um einen Straftatbestand nach dem StGB, dem Verbotsgesetz, dem FPG oder dem SMG handelt. Gemäß Abs 3 leg cit ist ein gefährlicher Angriff auch „ein Verhalten, das darauf abzielt und geeignet ist, eine solche Bedrohung vorzubereiten, sofern dieses Verhalten in engem zeitlichen Zusammenhang mit der angestrebten Tatbestandsverwirklichung gesetzt wird".

555 *Hauer/Keplinger,* Sicherheitspolizeigesetz – Polizeiausgabe[10] (2008) § 53 Anm 6.

556 RV 81 BlgNR XXI. GP, 6.

557 *Pürstl/Zirnsack,* Sicherheitspolizeigesetz (2005) § 28a Anm 3.

558 *Hauer,* Sicherheitspolizeigesetz[2] (2001) 252ff.

559 Vgl diesbezüglich auch die Judikatur des VwGH zum Begriff des Verdachts: *„Ein Verdacht kann immer nur auf Grund einer Schlußfolgerung aus Tatsachen entstehen. Ohne Tatsachen – wie weit sie auch vom (vermuteten) eigentlich Tatgeschehen entfernt sein mögen – gibt es keinen Verdacht [...]*", VwGH, 15.3.1989, 88/16/0209

Aufrechterhaltung der öffentlichen Sicherheit (§§ 20ff SPG), die Aufrechterhaltung der öffentlichen Ordnung (§ 27 SPG) sowie der besondere Überwachungsdienst (§ 27a SPG).

6.1.2.2. Die Befugnisse

§ 53 Abs 3a Z 1 SPG

Unter Anschluss iSd dieser Bestimmung ist wohl der Teilnehmeranschluss iSd § 3 Z 20 TKG 2003 zu verstehen[560]. In bestimmten Fällen, nämlich wenn es um die Abwehr gefährlicher Angriffe oder um die erste allgemeine Hilfeleistungspflicht geht, darf der Anschluss auch unter Angabe einer von diesem aus angerufenen Teilnehmernummer und eines möglichst genauen Zeitraums – der nach den Materialien nicht länger als eine Stunde sein darf[561] – bezeichnet werden (§ 53 Abs 3a, 2. Satz SPG). Dabei handelt es sich um die so genannte kleine Rufdatenrückerfassung[562]. Was den Begriff Teilnehmernummer anbelangt, so ist wiederum auf die Definition im TKG 2003 abzustellen. Dieses enthält zwar in § 3 keine eigene Definition, jedoch ist in § 92 Abs 3 Z 3 lit d von Teilnehmernummern und sonstige Kontaktinformation für die Nachricht die Rede. Aus den Materialien ergibt sich[563], dass unter Teilnehmernummern die klassischen Rufnummern zu verstehen sind[564]. Somit kann diese Auskunftspflicht nur die klassische Sprachtelefonie betreffen.

Die Behörde hat also entweder Namen, Teilnehmernummer oder Anschluss zu bezeichnen, und kann auf Grundlage des § 53 Abs 3a Z 1 SPG Auskunft über den dazugehörigen Namen und/oder die dazu gehörige Teilnehmernummer verlangen[565].

---

560 *Wiebe,* Auskunftsverpflichtung der Access-Provider, MR 2005, Beilage 4/05, 18; Nach dieser Bestimmung ist ein Teilnehmeranschluss *„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*", also etwa die Telefonsteckdose.

561 RV 272 BlgNR XXIII. GP, 5; zur Frage der Länge des Zeitraums vergleiche auch *Reindl-Krauskopf/Tipold/Zerbes,* in *Fuchs/Ratz* (Hrsg), Wiener Kommentar zur Strafprozessordnung (2009) § 134 Rz 64.

562 *Reindl-Krauskopf/Tipold/Zerbes,* in *Fuchs/Ratz* (Hrsg) Wiener Kommentar zur Strafprozessordnung (2009) § 134 Rz 62.

563 RV 128 BlgNR XXII. GP, 17: „reine Teilnehmernummer im Telefoniebereich".

564 Vgl auch *Kunnert,* Der sicherheitspolizeiliche Griff nach Telekommunikationsdaten. Möglichkeiten – Grenzen – Kritik, in *Jahnel* (Hrsg), Datenschutzrecht und E-Government: Jahrbuch 2008 (2008) 83 (101).

565 *Pürstl/Zirnsack,* Sicherheitspolizeigesetz (2005) § 53 Anm 35, zur wortgleichen Rechtslage vor der Novelle durch BGBl I 144/2007.

§ 53 Abs 3a Z 2 und 3 SPG

Die in Z 2 und Z 3 genannten Befugnisse wurden durch BGBl I 144/2007 eingefügt. Die IP-Adressen betreffenden Änderungen gehen auf einen Abänderungsantrag[566] der Abgeordneten Parnigoni (SPÖ) und Kößl (ÖVP) zurück, den diese kurz nach Eröffnung der Debatte am 42. Sitzungstag des Nationalrates 2007 um 22.34 Uhr einbrachten. Die Art und Weise, wie diese wesentlichen Änderungen ohne ordentliche Begutachtung nach direkter Vorlage an das Parlament spätnachts beschlossen wurden, führten in der Öffentlichkeit zu heftiger Kritik[567]. Der Abänderungsantrag führte zur Begründung an, dass diese Daten (Stammdaten zu IP-Adressen) *„den Sicherheitsbehörden zur Abwehr gefährlicher Angriffe oder zur Erfüllung der ersten allgemeinen Hilfeleistungspflicht bereits jetzt zugänglich gemacht wurden. Nach den Unterlagen handelt es sich um Abfragen Größenordnungen von etwa 1000 Anfragen pro Jahr.*" Hintergrund dieser neuen Bestimmungen dürfte wohl eine Entscheidung der DSK[568] sein, in welcher diese zum Schluss kam, dass die regelmäßig zur Beauskunftung von IP-Adressen genutzte Rechtsgrundlage des alten § 53 Abs 3a SPG dafür eigentlich keine geeignete Rechtsgrundlage darstelle[569]. Diese Entscheidung wurde mittlerweile höchstgerichtlich bestätigt[570]. Geht man von der Richtigkeit der Angaben im Abänderungsantrag aus, wonach die Befugnis des § 53 Abs 3a alt „etwa 1000 Mal" pro Jahr verwendet wurde, um die mit bestimmten IP-Adressen verknüpften Stammdaten zu erfahren, ist es zu einer Vielzahl von den Betroffenen unbekannten Rechtsverletzungen gekommen.

Fraglich ist, was der Gesetzgeber mit „Nachricht" iSd Z 2 und 3 leg cit bezeichnen wollte. Die diesbezügliche Begrifflichkeit des TKG (§ 92 Abs 3 Z 7 TKG 2003) zu übernehmen, hätte zur Konsequenz, dass alle Datenpakete, die über elektronische Kommunikationsnetze ausgetauscht werden, erfasst wären und zwar unabhängig davon, ob die Kommunikation zwischen zwei Menschen, zwei Maschinen oder Maschinen und Menschen stattfand[571]. Daher wird man vor allem um der Bestimmung keinen

---

[566] AA 89 BlgNR XXIII. GP.

[567] *Chadoian,* Stille Nacht, heimliche Macht – Zur SPG-Novelle 2007 und der Erweiterung sicherheitspolizeilicher Ermittlungsbefugnisse, juridikum 2008, 130; *Lepuschitz/Schindler,* Das österreichische Sicherheitspolizeigesetz (2008) 155; http://futurezone.orf.at/stories/242015/ (Stand April 2010).

[568] DSK 2.10.2007, K 121.279/0017-DSK/2007.

[569] *Feiler,* in *Zankl* (Hrsg), Auf dem Weg zum Überwachungsstaat (2009), 50.

[570] VwGH 27.5.2009, 2007/05/0280.

[571] Vgl § 92 Abs 3 Z 7 TKG 2003, wonach unter "Nachricht" folgendes zu verstehen ist: *„jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet wird. Dies schließt nicht*

verfassungswidrigen Inhalt (Art 18 B-VG) zu unterstellen, wohl zu dem Ergebnis gelangen müssen, dass hier eine restriktive Interpretation angezeigt ist. Nachrichten iSd dieser Bestimmung sollten Gedankenmitteilungen sein, die von Menschen an einen endlichen Kreis anderer Menschen unter Verwendung des Internet Protocol übermittelt wurden[572]. § 53 Abs 3a SPG Z 2 zielt damit auch auf andere elektronische Nachrichten als E-Mails ab. Letzteren werden Absender- und Empfänger-IP-Adresse in der Praxis ohnedies meist als Metainformation angehängt. Zu denken wäre etwa an die Nachrichten in Chatforen. Ist die Sicherheitsbehörde in Kenntnis einer IP-Adresse, wendet sie sich an den Access-Provider und verlangt von diesem gestützt auf Z 3 leg cit Auskunft über Name und Anschrift jener Person, welcher er diese IP-Adresse zum Zeitpunkt der Nachrichtenübermittlung zugeordnet hat.

Fraglich ist, wie die Sicherheitsbehörde die Nachricht, zu der sie den Zeitpunkt ihrer Übermittlung und die dazugehörige IP-Adresse erfahren möchte, gegenüber dem Access-Provider bezeichnen muss. Darf sie die Nachricht etwa unter Angabe eines bestimmten Zeitraums und bestimmter Angaben über den vermuteten Inhalt (zB Wörter wie Bombe, Opernball, Bundesregierung etc) definieren? Würde man die Befugnis so verstehen, hätte das zur Konsequenz, dass sie die Verarbeitung von Inhaltsdaten gestatten würde. Der Access-Provider müsste sämtliche von ihm weitergeleiteten Nachrichten dahingehend durchsuchen, ob sie die fraglichen Schlagwörter enthalten. Dies würde eine Verarbeitung von Inhaltsdaten darstellen. Die Definition des Begriffs „Verarbeiten" gem § 4 Z 9 DSG 2000 umfasst sowohl das Abfragen als auch das Vergleichen personenbezogener Informationen. Auch wenn die abgefragten Daten selbst nur Stammdaten darstellen, so steht aufgrund der Verknüpfung[573] von Inhalts- und Stammdaten in einem solchen Fall das Fernmeldegeheimnis (Art 10a StGG) einer derartigen Beauskunftung entgegen.

Fraglich ist weiters, von welcher IP-Adresse § 53 Abs 3a Z 2 SPG spricht, nahe liegend ist aufgrund der Verwendung des Singulars jedoch, dass nur eine IP-Adresse gemeint sein kann. Eine Nachricht, die unter Verwendung des Internet Protocol verwendet wird, enthält jedoch stets zumindest eine Absender- und eine Empfänger IP-Adresse[574] und kann unter Umständen auch noch IP-Adressen von weiteren Servern enthalten, über welche die Nachricht geleitet wird. Ohne Absender- und Empfänger-IP-Adresse ließe sich das verschickte Datenpaket nicht zustellen. Der Versand einer

---

Informationen ein, die als Teil eines Rundfunkdienstes über ein Kommunikationsnetz an die Öffentlichkeit weitergeleitet werden, soweit die Informationen nicht mit dem identifizierbaren Teilnehmer oder Nutzer, der sie erhält, in Verbindung gebracht werden können."

572 *Feiler,* in *Zankl* (Hrsg), Auf dem Weg zum Überwachungsstaat (2009), 52ff.

573 Vgl zu diesem Problem bereits ausführlich oben Kapitel 4.4.6.

574 RFC 791, Section 3.1. Internet Header Format.

elektronischen Nachricht über das Internet kann sich über einen längeren Zeitraum erstrecken, sodass einer Nachricht auch nicht immer ein bestimmter Zeitpunkt, sondern vielmehr ein bestimmter Zeitraum zugeordnet werden kann. Um die Befugnis nicht ausufernd zu verstehen, erscheint es angezeigt, als IP-Adresse iSd Z 2 leg cit die IP-Adresse des Absenders und als Zeitpunkt, den Zeitpunkt des Versandes zu verstehen[575].

6.1.3. Abs 3b[576]

6.1.3.1. Gefahrensituation

Nach § 53 Abs 3b SPG muss eine Gefahr für das Leben oder die Gesundheit eines Menschen bestehen, eine bloße Gefahr für das Eigentum oder sonstige Rechtsgüter reicht nicht aus, um die Befugnisse in § 53 Abs 3b SPG ausüben zu dürfen.

Die Formulierung „ist aufgrund bestimmter Tatsachen anzunehmen" kommt im SPG mehrmals vor (vgl etwa die §§ 28a, 35, 36 uva SPG). Die zu diesen Bestimmungen geltenden Erwägungen lassen sich auch auf den neuen § 53 Abs 3b SPG übertragen. Voraussetzung für die Ausübung der Befugnis sind konkrete Anhaltspunkte, welche die Annahme einer Gefahr bei einer objektiven ex-ante-Betrachtung rechtfertigen[577]. Zur Frage, wann dies der Fall ist, vgl bereits die obigen Ausführungen zu Abs 3a leg cit. Zu denken wäre etwa an die Meldung eines Beteiligten. So reicht etwa ein Notruf, bei welchem der Anrufer angibt, ein Mensch sei durch eine Lawine verschüttet worden, aus. Der Anruf rechtfertigt die Annahme, dass die Gefahr so wie vom Anrufer angegeben besteht. Der bezüglich der Annahme einer Gefahrensituation anzulegende Maßstab sollte nicht zu streng ausfallen. Vor Missbrauch der Befugnis schützt vor allem der Verhältnismäßigkeitsgrundsatz (§ 29 SPG).

Der Gefahrenbegriff des § 53 Abs 3b SPG darf wie auch jener gem Abs 3a leg cit keinesfalls mit der „allgemeinen Gefahr" oder dem „gefährlichen Angriff" nach § 16 SPG gleichgesetzt werden[578]. Zu diesem Ergebnis führen sowohl die Wort- als auch die systematische Interpretation der Bestimmung. Es gibt Befugnisse (vgl zB § 38a SPG), die auf das Vorliegen eines gefährlichen Angriffs abstellen. Aus der in § 53 Abs 3b SPG gewählten Formulierung – „Gefahr für das Leben oder die Gesundheit" – kann ein weiterer Anwendungsbereich abgeleitet werden. Die Gefahr muss nicht auf einem

---

575 *Feiler,* in *Zankl* (Hrsg), Auf dem Weg zum Überwachungsstaat (2009), 63ff.

576 Die folgenden Ausführungen entsprechen bis zum nächsten Kapitel passagenweise den von mir verfassten Teilen bei *Zankl* (Hrsg), Auf dem Weg zum Überwachungsstaat? (2009) 91ff .

577 *Pürstl/Zirnsack,* SPG (2005) § 36 Anm 1 sowie § 41 Anm 2.

578 *Hauer/Keplinger,* Sicherheitspolizeigesetz – Polizeiausgabe[10] (2008) § 53 Anm 8.

gefährlichen Angriff beruhen, die Ursache bzw der Verursacher der Gefahr sind nicht entscheidend. Auch Suizidenten bzw Selbstmordattentäter fallen in den Anwendungsbereich, obwohl sie selbst es sind, von denen die Gefahr ausgeht. Setzen Eltern etwa den Notruf ab, wonach ihr Kind nach einer Selbstmordankündigung abgetaucht sei, könnte dessen Mobiltelefon nach § 53 Abs 3b SPG geortet werden. Geortet werden dürfen immer nur die gefährdeten Personen, also etwa das Entführungsopfer, nicht jedoch der Entführer[579].

Mangels Abstellen auf die bekannte Formulierung der „allgemeinen Gefahr" wäre eine präzisere Definition begrüßenswert. Aus dem Legalitätsprinzip (Art 18 B–VG) ergibt sich, dass mit steigender Eingriffsintensität auch die Genauigkeit des Tatbestandes zunehmen muss[580]. Auch der EGMR verlangt für Gesetze, welche geheime Ermittlungsmaßnahmen ermöglichen, ein besonders hohes Maß an Genauigkeit[581].

Mit Wegfall der Gefahr darf auch die Befugnis gem § 53 Abs 3b SPG nicht mehr ausgeübt werden. So darf etwa auf Grundlage des § 53 Abs 3b SPG nach der Benachrichtigung über die Freilassung eines Entführungsopfers nicht mehr das beim Entführer zurück gelassene Mobiltelefon geortet werden.

6.1.3.2. Die sicherheitspolizeilichen Aufgaben im Anwendungsbereich des § 53 Abs 3b SPG

Das SPG wird vom Grundsatz der Aufgabenbezogenheit durchzogen (§ 3 SPG), wonach die Ausübung von Befugnissen stets nur zur Erfüllung bestimmter Aufgaben in Frage kommt. Das SPG definiert in § 53 Abs 3b SPG als Aufgaben die „Hilfeleistung oder Abwehr dieser Gefahr." Im ursprünglichen Ministerialentwurf wurde die der Befugnisausübung zugrunde liegende Aufgabe noch folgendermaßen definiert: *„[...] sind die Sicherheitsbehörden zur Abwehr dieser Gefahr darüber hinaus berechtigt [...]"*[582]. Die vom BMJ zur Klarstellung vorgeschlagene Formulierung[583] – *„[...] sind die Sicherheitsbehörden im Rahmen der ersten allgemeinen Hilfeleistungspflicht oder der Abwehr gefährlicher Angriffe darüber hinaus berechtigt [...]"* – wurde bedauerlicherweise nicht übernommen.

---

[579] Der Entführer darf jedoch im Wege der Auskunft über die (Standort)daten einer Nachrichtenübermittlung gem § 135 Abs 2 Z 1 StPO geortet werden.

[580] Vgl etwa VfGH v. 12.12.1985, G 225/85; 29.9.1987, G 139/87.

[581] EGMR, U 2.8.1984, *Malone*, Nr 8691/79, Rz 68; U 26.4.1979, U *Sunday Times*, Nr 13166/87, Rz 49; U 25.03.1998, *Kopp*, 23224/94, Rz 62 ff; U 25.06.1997, *Halford*, 20605/92, Rz 49.

[582] 118 ME BlgNR XXIII. GP, 1.

[583] 13/SN-118/ME BlgNR XXIII. GP, 2, abrufbar unter: http://www.parlinkom.gv.at/PG/DE/XXIII/ME/ME_00118_13/fname_087872.pdf (Stand April 2010).

Fraglich ist, ob dem Umstand, dass hier die Formulierung „Hilfeleistung" und nicht etwa wie in § 53 Abs 3a Satz 2 SPG die Wendung „der Erfüllung der ersten allgemeinen Hilfeleistungspflicht" (§ 19 SPG) verwendet wurde, eine Bedeutung beigemessen werden muss. Andere Bestimmungen des SPG stellen klar, dass unter Hilfeleistung jene iSd § 19 SPG gemeint ist. Dies geschieht etwa durch einen Verweis auf § 19 SPG (etwa § 32 SPG) oder durch die Verwendung der Wortfolge „erste allgemeine Hilfeleistungspflicht" (etwa § 34 SPG). § 53 Abs 3b SPG stellt keinen vergleichbaren Bezug zur allgemeinen Hilfeleistungspflicht gem § 19 SPG her, was mE jedoch zu vernachlässigen ist. Wie erwähnt gilt im SPG der Grundsatz der Aufgabenbezogenheit[584]. Demgemäß sieht § 52 SPG vor, dass personenbezogene Daten nur verwendet werden dürfen, soweit dies zur Erfüllung der ihnen übertragenen Aufgaben erforderlich ist. Dazu zählen die Aufrechterhaltung der öffentlichen Sicherheit (§§ 20 ff SPG), die Aufrechterhaltung der öffentlichen Ordnung (§ 27 SPG), der besondere Überwachungsdienst (§ 27a SPG) und eben die erste allgemeine Hilfeleistungspflicht iSd § 19 SPG. Dieser Aufgabenkatalog im zweiten Teil des SPG ist taxativer Natur[585]. Die Annahme, § 53 Abs 3b SPG wolle eine neue Aufgabe schaffen, wäre systemwidrig.

Auch die Wendung „Abwehr dieser Gefahr" in § 53 Abs 3b SPG führt zu ähnlichen Auslegungsproblemen. Wie oben bereits erwähnt, reicht die für die Befugnisausübung erforderliche Gefahr iSd § 53 Abs 3b SPG weiter als die „allgemeine Gefahr" iSd § 16 SPG. Daraus ist zu schließen, dass die „Abwehr dieser Gefahr" iSd § 53 Abs 3bSPG mehr umfasst, als die „Gefahrenabwehr" iSd §§ 20 ff SPG. Diese Auslegung ist jedoch zweifelhaft, weil die Abwehr einer Gefahr – sofern sie keine Gefahrenabwehr iSd §§ 20 ff SPG bzw erste allgemeine Hilfeleistung iSd § 19 SPG darstellt – nicht zu den oben aufgezählten sicherheitsbehördlichen Aufgaben zählt. Auch hier erscheint es ausgeschlossen, dass der Gesetzgeber in § 53 Abs 3b SPG eine neue Aufgabe schaffen wollte. Deshalb muss die Wendung „Abwehr dieser Gefahr" teleologisch so reduziert werden, dass darunter nur mehr eine Gefahrenabwehr iSd §§ 20 ff SPG zu verstehen ist. So würde die Lokalisierung eines Lawinenopfers etwa zur Erfüllung der ersten allgemeinen Hilfeleistungspflicht und die Lokalisierung eines Entführungsopfers zur Erfüllung der sicherheitspolizeilichen Aufgabe der Gefahrenabwehr erfolgen.

6.1.3.3. Auskunft über Standortdaten und IMSI

Der Begriff „Standortdaten" wird für das SPG nicht näher definiert, es ist diesbezüglich auf die Definition des TKG (§ 92 Abs 3 Z 6) zurückzugreifen. Der Betreiber

---

584 *Giese*, Sicherheitspolizeirecht in *Bachmann* ua (Hrsg), Besonderes Verwaltungsrecht (2004) 13.

585 *Giese*, Sicherheitspolizeirecht in *Bachmann* ua (Hrsg), Besonderes Verwaltungsrecht (2004) 14.

hat auf dieser Grundlage die so genannte Funkzelle (Cell-ID) zu ermitteln, in welcher sich die Endeinrichtung befindet und die geografische Lage dieser Funkzelle bekannt zu geben. So ist die Sicherheitsbehörde in der Lage, die „technischen Mittel zur Lokalisierung" – dh in der Praxis den so genannten IMSI-Catcher – in Position zu bringen, um die gefährdete Person exakt zu lokalisieren (siehe dazu sogleich).

6.1.3.4. Die IMSI und der IMSI-Catcher[586]

Die IMSI (International Mobile Subscriber Identity[587]) ermöglicht eine exakte Identifizierung von Teilnehmern in GSM- und UMTS-Netzen. Jeder SIM (Subscriber Identity Module) ist eine weltweit einzigartige IMSI zugeordnet. IMSIs umfassen 15 Ziffern. Auf eine 3-stellige Länderzahl (Mobile Country Code; MCC) folgen die zweistellige Netzkennzahl (Mobile Network Code; MNC) und anschließend eine 10-stellige Teilnehmerkennung (Mobile Subscriber Identification Number; MSIN). Die Sicherheitspolizei kann auf Grundlage des § 53 Abs 3b SPG Auskunft über die IMSI und die Cell-ID verlangen. Mithilfe dieser Informationen kann sie einen sog IMSI-Catcher in Position bringen und eine exakte Standortfeststellung durchführen[588].

Obwohl das Gesetz an sich technologieneutral ausgestaltet ist, legen die Materialien ein Begriffsverständnis nahe, wonach unter „technischen Einrichtungen zur Lokalisierung gefährdeter Menschen" vor allem sog IMSI-Catcher zu verstehen sein werden. In den EBRV wird unter dem Punkt „finanzielle Auswirkungen" der Aufwand des Ankaufs eines IMSI-Catchers mit etwa € 600.000 beziffert[589].

Der IMSI-Catcher lässt sich auch zur Erhebung der IMSI oder der sog IMEI (International Mobile Equipment Identity) einsetzen[590]. Bei der IMEI handelt es sich um eine jeweils weltweit einzigartige Nummer, die das Endgerät eindeutig identifiziert. Nach den Vorstellungen des Gesetzgebers dient die neu geschaffene Befugnis jedoch einzig der exakten Positionsbestimmung eines Mobiltelefons. IMSI-Catcher ermöglichen überdies eine Inhaltsüberwachung der von den Endgeräten aus geführten Gespräche, da sie sich

---

586 Dieses Kapitel entspricht meinem Beitrag in *Zankl* (Hrsg), Auf dem weg zum Überwachungsstaat? (2009) 102ff.

587 Vgl dazu *Vassilaki*, Telekommunikationsüberwachung – eine Darstellung der aktuellen Rechtsfragen, RDV 2004, 11 (14).

588 Vgl hierzu *Gercke*, Rechtliche Probleme durch den Einsatz des IMSI-Catchers, MMR 2003, 453 (454); *Eckhardt,* Neue Entwicklungen der Telekommunikationsüberwachung, CR 2002, 770 (771).

589 RV 272 BlgNR XXIII. GP 4.

590 *Fox,* Der IMSI-Catcher, DuD 2002, 212 (213).

technisch gesehen dem Endgerät gegenüber als Basisstation bzw Funkzelle ausgeben[591] und aus Sicht des Netzwerks des Access-Providers wie ein Mobiltelefon wirken. Diese Funktionsweise kann auch mit dem Begriff „Man-in-the-middle-Attack" bezeichnet werden[592]. Die zusätzlichen Funktionalitäten des IMSI-Catchers ließen bei manchen Zweifel an der Statthaftigkeit der Novelle aufkommen. So äußerten insbesondere manche oppositionelle Politiker die Befürchtung, dass der seitens des BMI in Wahrheit vor allem angestrebte Zweck die Inhaltsüberwachung sei[593]. Betreiber befürchten zudem Störungen ihrer Dienste, die infolge des Einsatzes eines IMSI-Catchers eintreten könnten[594].

Beim Einsatz eines IMSI-Catchers kommunizieren sämtliche in dessen Einzugsbereich befindlichen Endgeräte wie bei einer Funkzelle nur mehr mit diesem[595]. Die Suche lässt sich auf das jeweilige Netzwerk der gesuchten Person beschränken. Die Ortung durch einen IMSI-Catcher setzt voraus, dass das zu lokalisierende Gerät aktiviert wurde.

6.1.4. Zu Abs 3a und 3b

6.1.4.1. Normativität

Diese Bestimmungen erlauben also in bestimmten Situationen bestimmte Auskünfte von Betreibern öffentlicher Telekommunikationsdienste zu verlangen. Ein Verlangen ist im Gegensatz zu einem Ersuchen, bei dem die Behörde lediglich einen Wunsch äußert, ein normativer Akt[596]. Tatsächlich mangelt es dem in der Praxis verwendeten Formular[597], mit dem Auskunftsansprüche gem § 53 Abs 3a und 3b SPG geltend gemacht werden, oft genau an jenem normativen Charakter. Das ist vor dem Hintergrund des Prinzips des Einsatzes des gelindesten Mittels (Ultima-Ratio-Prinzip;

---

591 *Roggan,* Moderne Telekommunikationsüberwachung: eine kritische Bestandsaufnahme, KritV 2003, 76 (86).

592 *Fox,* Der IMSI-Catcher, DuD 202, 212 (214).

593 http://www.ueberwachungsstaat.at; http://futurezone.orf.at/it/stories/243503/ (Stand 1. 9. 2008); vgl auch die Nachweise bei *Kunnert,* Der sicherheitspolizeiliche Griff nach Telekommunikationsdaten. Möglichkeiten – Grenzen – Kritik, in *Jahnel* (Hrsg), Datenschutzrecht und E-Government: Jahrbuch 2008 (2008) 86 ff.

594 *Fox,* Der IMSI-Catcher, DuD 202, 212 (214).

595 *Vassilaki*, Telekommunikationsüberwachung – eine Darstellung der aktuellen Rechtsfragen, RDV 2004, 11 (14).

596 *Hauer/Keplinger,* Befugnisse der Organe des öffentlichen Sicherheitsdienstes (2007) 144.

597 Abgedruckt beispielsweise bei *Zankl* (Hrsg), Auf dem Weg zum Überwachungsstaat? (2009) 231ff.

§ 28a Abs 3 SPG) und dem Verhältnismäßigkeitsprinzip (§ 29 SPG) auch keineswegs zu beanstanden, sondern eher zu begrüßen. Normativ ist ein verwaltungsbehördlicher Akt nur dann, wenn er rechtsgestaltenden oder rechtsfeststellenden Inhalt aufweist und sein Inhalt bindend ist[598]. Da das Formular nicht als Bescheid bezeichnet wird[599] und es auch keinen normativen Charakter hat, ist es kein Bescheid. Bloße Aufforderungen oder Wünsche, die von Organwaltern ausgesprochen werden, sind auch keine Ausübung unmittelbarer behördlicher Befehlsgewalt und Zwangsgewalt[600]. Das in der Praxis gebräuchliche Formular ist daher als Akt schlichten Verwaltungshandelns zu qualifizieren[601], was, wie noch zu zeigen ist, insbesondere auf die Wahl der zu ergreifenden Rechtsbehelfe Auswirkungen hat.

6.1.4.2. Rechtsschutz

Auskunftsverlangen gem § 53 Abs 3a und 3b SPG sind ihrer Natur nach gegenüber dem Vertragspartner des Access-Providers geheime Maßnahmen, die Sicherheitsbehörden trifft keine positivierte Informationspflicht. Lediglich der Rechtsschutzbeauftragte hat die Möglichkeit, jedoch nicht die Pflicht zur Information (siehe dazu schon oben Kapitel 5.5.6.5). Das wirft mit Blick auf Art 13 EMRK und das rechtsstaatliche Prinzip[602] Zweifel an der Verfassungskonformität dieser Bestimmung auf[603], da es zu Fällen kommen kann, in denen die Rechte des Betroffenen verletzt werden, dieser davon keine Kenntnis erlangt, infolgedessen keine Rechtsbehelfe ergreift und somit dauerhaft beschwert bleibt[604]. Diese Zweifel entstehen insbesondere vor dem Hintergrund der Judikatur des EGMR zu geheimen Überwachungsmaßnahmen, aus der sich ergibt, dass solche nur solange geheim bleiben dürfen, als dies der Zweck der Maßnahme erfordert[605] und in der immer wieder betont wird, dass es zumindest eine

---

598 *Pottacs/Hattenberger,* in *Rill/Schäffer,* Bundesverfassungsrecht 2 (1. Lfg 2001) Rz 11.

599 Was bei Zweifeln hinsichtlich der Normativität Voraussetzung für die Bejahung der Bescheideigenschaft ist, vgl etwa: VwGH, 15.12.1977, 0934/73.

600 ZB VwGH 21.12.1988, 98/17/0011.

601 *Stahov,* in *Zankl* (Hrsg), Auf dem Weg zum Überwachungsstaat? (2009) 108.

602 Vgl dazu VfGH 23.1.2004, G 363/02.

603 Weshalb wie schon mehrfach erwähnt einige (erfolglos) versuchten diese Bestimmung mittels Individualantrag zu bekämpfen: VfGH 1.7.2009, G 29/08; G30/08; G31/08; G35/08; G147/08 ua; vgl auch etwa die Stellungnahme des Verfassungsdienstes des Bundeskanzleramts zum Ministerialentwurf: 15/SN-118/ME XXIII. GP, 2; abrufbar unter: http://www.parlinkom.gv.at/PG/DE/XXIII/ME/ME_00118_15/fname_088025.pdf.

604 Vgl dazu *Raschhofer,* in *Zankl* (Hrsg) Auf dem Weg zum Überwachungsstaat? (2009) 110ff.

605 EGMR U 29.6.2006, *Weber and Saravia*, Nr 54934/00, Rz 135.

effiziente unabhängige Kontrolle geben müsse[606]. Diese Bedenken haben einiges für sich, allerdings muss es aufgrund des Schwerpunkts dieser Abhandlung mit einem Hinweis darauf sein Bewenden haben.

Rechtsschutz durch den Rechtsschutzbeauftragten[607]

Nach § 91c Abs 1 SPG ist der Rechtsschutzbeauftragte über Auskunftsverlangen gem § 53 Abs 3a Z 2 und 3, Abs 3a Satz 2 leg cit sowie § 53 Abs 3b SPG in Kenntnis zu setzen. Im Unterschied zu den Fällen der Ermittlung personenbezogener Daten durch verdeckte Ermittlung (§ 54 Abs 3 SPG) kann eine Information über die wesentlichen Gründe jedoch unterbleiben. Allerdings haben die Sicherheitsbehörden dem Rechtsschutzbeauftragten gem § 91d Abs 1 SPG *„bei der Wahrnehmung seiner Aufgaben jederzeit Einblick in alle erforderlichen Unterlagen und Aufzeichnungen zu gewähren, ihm auf Verlangen Abschriften (Ablichtungen) einzelner Aktenstücke unentgeltlich auszufolgen und alle erforderlichen Auskünfte zu erteilen; insofern kann ihm gegenüber Amtsverschwiegenheit nicht geltend gemacht werden*". Im Falle der Verletzung der Rechte des Betroffenen durch die Verwendung personenbezogener Daten durch die Sicherheitsbehörden darf der Rechtsschutzbeauftragte den Betroffenen informieren, es sei denn, es liegt ein Fall des § 26 Abs 2 DSG 2000 vor. § 26 DSG 2000 sieht ein umfassendes Auskunftsrecht des Betroffenen vor. Das Auskunftsrecht entfällt jedoch gemäß Abs 2 leg cit, „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 entgegen stehen". Als letztere kommen insbesondere die Vorbeugung, Verhinderung oder Verfolgung von Straftaten in Frage.

Für den Fall der Unzulässigkeit der Information des Betroffenen durch den Rechtsschutzbeauftragten ist letzterer zur Beschwerdeerhebung an die DSK befugt. (zur Problematik des Begriffes „befugt" vgl bereits oben Kapitel 6.1.4.2). Er soll die Rechte jener schützen, die ihre Rechte nicht selbst wahrnehmen können. Im Anwendungsbereich des § 53 Abs 3b SPG sind anders als bei Abs 3a leg cit kaum Fälle denkbar, in denen die Voraussetzungen des § 26 Abs 2 DSG 2000 erfüllt sein könnten und damit die Information unzulässig wäre. Selbst wenn dies der Fall sein sollte, darf der

---

[606] EGMR U 28.6.2007, *The Association for European Integration and Human Rights an Ekimdzhiev*, Nr 62540/00, Rz 85ff.

[607] Dieser Abschnitt entspricht im Wesentlichen meinem Beitrag in *Zankl* (Hrsg), Auf dem Weg zum Überwachungsstaat? (2009) 117ff.

Rechtsschutzbeauftragte seine Rechte nach § 91d SPG vollständig wahrnehmen. Er darf gemäß § 91d Abs 1 SPG Einblick in alle erforderlichen Unterlagen und Aufzeichnungen nehmen, sowie Abschriften (Ablichtungen) einzelner Aktenstücke verlangen und alle erforderlichen Auskünfte einholen. Darüber hinaus ist ihm gem § 91d Abs 2 SPG jederzeit Gelegenheit zu geben, die Durchführung der Ermittlungsbefugnisse gem § 53 Abs 3a und 3b SPG zu überwachen und alle Räume zu betreten, in denen Aufnahmen oder sonstige Überwachungsergebnisse aufbewahrt werden.

Wie bereits oben erwähnt, entbindet die Möglichkeit des Rechtsschutzbeauftragten mE den Access-Provider nicht von seiner – qua ergänzender Vertragsauslegung gewonnenen Pflicht – seinen Vertragspartner über die Erfüllung eines Auskunftsbegehrens zu informieren.

Rechtsschutz durch den Access-Provider[608]

Bevor überhaupt geklärt werden kann, ob der Access-Provider die Daten seines Kunden verteidigen muss, ist zunächst zu klären, ob er dies nach der geltenden Rechtslage überhaupt kann. Nach § 90 SPG entscheidet die DSK *„gemäß § 31 des Datenschutzgesetzes 2000 über Beschwerden wegen Verletzung von Rechten durch Verwenden personenbezogener Daten in Angelegenheiten der Sicherheitsverwaltung entgegen den Bestimmungen des Datenschutzgesetzes*". Der verwiesene § 31 DSG 2000 bestimmt, dass die DSK über „Beschwerden von Betroffenen" zu entscheiden hat. Nach der Definition des § 4 Z 3 DSG 2000 ist unter dem Betroffenen jede vom Auftraggeber verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet werden, zu verstehen. Diese Definition umfasst in den hier interessierenden Sachverhalten lediglich den Kunden, nicht jedoch den Access-Provider, weshalb es letzterem an der Aktivlegitimation für Beschwerden gemäß § 90 SPG mangelt.

Für Beschwerdeverfahren vor den UVS lässt sich die Aktivlegitimation des Access-Providers jedoch aus § 87 SPG ableiten. § 87 SPG gibt jedem das einklagbare Recht auf Gesetzmäßigkeit der ihm gegenüber ausgeübten sicherheitspolizeilichen Maßnahmen. Durch die Ausübung von Auskunftsbegehren wird auch der Access-Provider in seinen Rechten beeinträchtigt. Der Eingriff mag sich ihm gegenüber zwar als nicht ganz so intensiv erweisen, wie gegenüber dem Betroffenen, führt bei ihm aber jedenfalls zu einem gewissen Aufwand. Dies anerkennt der Gesetzgeber, soweit er in § 53 Abs 3b SPG einen Kostenersatz vorsieht. Daher kann mE der Access-Provider, der die Auffassung vertritt, ein Auskunftsbegehren sei unrechtmäßig an ihn heran getragen worden, seine Beschwerde auf die Behauptung gründen, er sei in seinem Recht gemäß § 87 SPG

---

[608] Dieser Abschnitt enstpricht im Wesentlichen meinem Beitrag in *Zankl* (Hrsg), Auf dem Weg zum Überwachungsstaat? (2009) 121ff.

verletzt worden. Diese Möglichkeit steht zu Gebote, da § 90 SPG eine Beschwerde an den UVS nur in jenen Fällen ausschließt, in denen eine Beschwerde nach § 31 DSG 2000 zu Gebote steht. Die DSK ist jedoch wie bereits erwähnt nach § 90 SPG ausschließlich zuständig für „Beschwerden gem § 31 DSG", dh Beschwerden des Betroffenen. Im Bereich des öffentlichen Rechts soll ihr eine ausschließliche Zuständigkeit für Datenschutzangelegenheiten zukommen. Gegenstand einer Beschwerde des Providers wäre nicht die Verletzung der Rechte an seinen eigenen personenbezogenen Daten, sondern die mit der Verletzung der Rechte des Betroffenen einher gehende Verletzung seines Rechts gemäß § 87 SPG. Selbst wenn die Befugnisse gemäß § 53 Abs 3a und 3b SPG ohne Einsatz von Befehls- bzw Zwangsgewalt, dh durch schlichtes Polizeihandeln (§ 88 Abs 2 SPG) ausgeübt wurden, ist für Beschwerden des Access-Providers daher nie die DSK zuständig. Für den Provider ist die Maßnahme aus anderen Gründen belastend, vor allem wegen des Aufwandes, der ihm erspart geblieben wäre, wenn die Befugnisausübung in Übereinstimmung mit dem SPG bzw DSG 2000 unterblieben wäre. Deshalb kann er mE eine auf § 87 SPG gestützte Beschwerde vor dem UVS einbringen.

Aus solch einer Beschwerde des Access-Providers ergäbe sich reflexartig auch ein Schutz für seinen Vertragspartner. Würde vor dem UVS ein derartiges Verfahren abgeführt werden, müsste zwangsläufig auch die Frage geklärt werden, ob die Sicherheitsbehörde das Auskunftsverlangen bzw Auskunftsersuchen zu Recht an den Access-Provider richtete. Dafür müssen auch die den Vertragspartner betreffenden datenschutzrechtlichen Implikationen des Falles aufgearbeitet werden. Dies kann in jenen Fällen wichtig sein, in denen er davon Abstand nehmen muss, seinen Vertragspartner über die Erfüllung des Auskunftsbegehrens zu informieren, da er sich sonst einem Strafbarkeitsrisiko aussetzen würde, das ihm selbstverständlich unzumutbar ist.

6.1.4.3. Vertragliche Pflicht zur Ergreifung von Rechtsschutzmaßnahmen?

Fraglich ist, ob, nur weil er eine auch für seinen Vertragspartner günstige Beschwerde an den UVS richten kann, dies auch muss. Eine derartige Verpflichtung wäre so wie seine Informationspflicht eine vertragliche Schutzpflicht. Hier ist nochmals auf die bei der Gewinnung von Vertragspflichten durch ergänzende Vertragsauslegung zu beachtenden Grundsätze zu verweisen (vgl oben Kapitel 5.5.2ff). Insbesondere ist nochmals an das Kriterium der Zumutbarkeit zu erinnern. Während man diese hinsichtlich der bloßen Benachrichtigungspflicht problemlos bejahen kann, ist die Ergreifung von Rechtsmitteln wesentlich komplizierter und damit im Ergebnis mE unzumutbar. Der mit einer Beschwerde an den UVS verbundene Aufwand ist beträchtlich. So wird dies idR Regel wohl dazu führen, dass ein Rechtsanwalt oder zumindest eine rechtskundige Person mit dem Verfassen der Eingabe betraut werden muss, was einen erheblichen Kostenaufwand verursacht. Außerdem wird Access-Provider wohl selten über

einen ausreichenden Kenntnisstand verfügen, um die Erfolgschancen einer derartigen Beschwerde beurteilen zu können. Im Falle des § 53 Abs 3b SPG ist die Notwendigkeit des Auskunftsbegehrens aus Gründen der Nachvollziehbarkeit zwar zu dokumentieren[609]. Daraus wird die Pflicht der Sicherheitsbehörde abgeleitet, dass zumindest der Zweck, dh die zu erfüllende Aufgabe sowie schlagwortartige Angaben über den zugrunde liegenden Sachverhalt anzuführen sind[610]. Die Dokumentation erfolgt in der Praxis mittels des bereits erwähnten Formulars regelmäßig so oberflächlich, dass eine Beurteilung der Rechtmäßigkeit des Auskunftsverlangens nur schwer möglich ist. Die Verpflichtungen, die Vertragspartner im Rahmen ergänzender Vertragsauslegung treffen können, bringen bisweilen sehr beträchtliche wirtschaftliche Auswirkungen mit sich. Man denke etwa an Konkurrenzverbote, die qua ergänzender Vertragsauslegung gewonnen werden. Allerdings haben die von der Judikatur angenommenen Neben- und Schutzpflichten alle gemein, dass ihre Erfüllung bei gewöhnlichem Verlauf dem Gläubiger unmittelbar und garantiert zugute kommt. Der Vorteil, der dem Berechtigten aus einem Konkurrenzverbot erwächst, macht sich unmittelbar bemerkbar. Genau dies wäre jedoch bei der Einbringung einer Beschwerde durch den Access-Provider nicht garantiert, sind die Chancen auf deren Erfolg doch zu ungewiss.

Ein weiterer Grund, der gegen die Annahme einer derartigen Schutzpflicht spricht, ist dass dadurch in Wahrheit das möglicherweise verletzte Rechtsgut, die Privatsphäre, nicht bzw nur unzureichend in den Status quo ante zurückversetzt werden kann (Vgl zu diesem dem Rechtsgut der Privatsphäre eigenen Problem bereits oben, Kapitel 5.4). Der Access-Provider hat abgesehen von der Verweigerung der Erfüllung des Auskunftsbegehrens keine Möglichkeit, die Privatsphäre seines Kunden im Vorhinein zu verteidigen. Er kann die auf § 87 SPG basierte Beschwerde erst nach dem erfolgten Eingriff einbringen.

---

609 RV 272 BlgNR XXIII. GP, 5; Diese Bestimmung ist stark an § 98 TKG 2003 angelehnt. Vgl dazu auch *Kunnert* Der sicherheitspolizeiliche Griff nach Telekommunikationsdaten. Möglichkeiten – Grenzen – Kritik, in *Jahnel* (Hrsg), Datenschutzrecht und E-Government: Jahrbuch 2008 (2008) 130: Er unterscheidet jedoch zwischen § 53 Abs 3b SPG und § 98 TKG 2003, da nur § 98 TKG verlangt, dass die „Notwendigkeit" der Informationsübermittlung zu dokumentieren ist, während gem § 53 Abs 3b SPG lediglich eine „Dokumentation des Auskunftsbegehrens" zu erfolgen hat. Bei Anfragen gem § 53 Abs 3b SPG müsse daher nach dem Gesetzeswortlaut die Erforderlichkeit gegenüber dem Betreiber nicht offengelegt werden. Das wirderspricht mE jedoch den Materialien zur SPG-Novelle, da diese die Parallelität zu § 98 TKG 2003 ausdrücklich betonen und festhalten, dass die Dokumentation der Nachvollziehbarkeit dienen soll.

610 *Klingenbrunner/Bresich,* Telekommunikationsunternehmen: Beschränkter Polizeischutz gegen Poliziehandeln? ecolex 2008, 475 (477).

6.1.4.4. Schutzpflichten im Zusammenhang mit der Dokumentation des Auskunftsbegehrens

Was soll aber gelten, wenn der Access-Provider aufgrund besonderer Umstände zwar massive Zweifel an der Rechtmäßigkeit des Auskunftsbegehrens hegt, aber gleichzeitig befürchten muss, sich durch die Information des Betroffenen der Gefahr einer Strafbarkeit (etwa § 299 StGB, vgl dazu schon oben Kapitel 5.5.6) auszusetzen. Entschließt er sich in diesen Fällen zu einer Verweigerung des Auskunftsbegehrens, riskiert er, dass die Sicherheitsbehörde einen Zwangsakt setzt (§ 50 SPG)[611]. Dies ist ihm, wenn er von der Unrechtmäßigkeit des Auskunftsbegehrens nicht definitiv weiß, keinesfalls zuzumuten, da er seine Erfolgschancen in einem darauf folgenden Beschwerdeverfahren vor dem UVS eben nicht mit Sicherheit beurteilen kann. Ist er aber seinem Vertragspartner in diesen Fällen wirklich zu nichts verpflichtet?

Dies scheint auf den ersten Blick zumindest der Wortlaut des § 53 Abs 3b SPG nahe zu legen, wonach die Sicherheitsbehörde die „Verantwortung für die rechtliche Zulässigkeit des Auskunftsbegehrens" trifft. Fraglich ist, welche Bedeutung dieser Bestimmung zukommen kann. Die Materialien führen dazu aus, dass dieser Teil der Bestimmung an § 98 TKG 2003 angelehnt ist[612]. In der RV zum TKG 2003 heißt es zu letzterer Bestimmung: *„Wenn der Betreiber einem glaubhaften Übermittlungsersuchen entspricht, ist er im Falle eines missbräuchlichen Ersuchens von der Verantwortung befreit."*[613] Nun darf diese Bestimmung getrost als misslungen bezeichnet werden, denn es stellt sich die kaum beantwortbare Frage, was aus ihr abzuleiten ist. Was gilt etwa, wenn – wie im Falle von § 53 Abs 3a SPG – eine derartige Bestimmung fehlt? Wäre daraus e contrario zu schließen, dass dann stets der Access-Provider haftet[614]? Oder lässt sich ihr, was noch eher vertretbar erschiene, entnehmen, dass der Access-Provider nur dort, wo eine derartige Bestimmung fehlt, nach allgemeinen Grundsätzen haftet? Folgt man der Auffassung der Bundesregierung, die diese im Verfahren über den bereits erwähnten Individualantrag eines Access-Providers gegen die Bestimmungen im SPG vertrat, könnte man dies fast annehmen. Der Access-Provider brachte vor, dass er durch die Bestimmungen des § 53 Abs 3a und 3b SPG deshalb betroffen sei, da diese zu Unterlassungs- und Schadenersatzansprüchen seiner Kunden gegen ihn führen könnten. Die Bundesregierung replizierte darauf, dass im Falle des Abs 3b leg cit *„die*

---

611 *Hauer/Keplinger,* Sicherheitspolizeigesetz – Polizeiausgabe[10] (2008) 167.

612 RV 272 BlgNR XXIII. GP, 5.

613 RV 128 BlgNR XXII. GP, 19.

614 Vgl etwa auch die im unter http://portal.wko.at/wk/format_detail.wk?AngID=1&StID=386310&DstID=5000 (stand April 2010) abrufbaren Informationsblatt der WKO vertretene Ansicht, wonach die Frage der zivilrechtlichen Verantwortung nicht abschließend geklärt sei.

Sicherheitsbehörden ebenso wie die Notrufdienste nach § 98 TKG 2003 die Verantwortung für die rechtliche Zulässigkeit des Auskunftsbegehrens treffe[615]*.*" Die Bundesregierung geht also zumindest ihrem Vorbringen in diesem Verfahren nach tatsächlich von einem diesbezüglichen Unterschied zwischen den Abs 3a und 3b leg cit aus. Eine derartige Differenzierung wäre jedoch mit Blick auf Art 2 StGG und Art 7 B-VG kaum sachlich zu rechtfertigen. Wieso sollte der Access-Provider in einem Fall ein Haftungsprivileg genießen und im anderen Fall nicht?

Überdies soll nach den zitierten Materialien der Access-Provider auch im Falle von § 53 Abs 3b und § 98 TKG 2003 nicht schlechthin unverantwortlich für die Erfüllung von Auskunftsbegehren sein, sondern nur dann, wenn er einem „glaubhaften Auskunftsbegehren" entsprach. Weiß der Access-Provider also von der Missbrauchsabsicht der Behörde trifft ihn mE jedenfalls die qua ergänzende Vertragsauslegung gewonnene Schutzpflicht, die Erfüllung des Auskunftsbegehrens zu verweigern. Verletzt er diese Pflicht, können ihm auch die Haftungsprivilegien in § 98 TKG 2003 und § 53 Abs 3b SPG nicht helfen. Unter Rücksichtnahme auf die zitierten Materialien und dem daraus ableitbaren eindeutigen Telos der Bestimmung ist der Wortlaut, soweit er auch in diesen Fällen eine Haftungsbefreiung nahe legt, mE eindeutig teleologisch zu reduzieren.

Ob ein Auskunftsbegehren glaubhaft ist oder nicht, lässt sich nur dann beurteilen, wenn dem Access-Provider zumindest einige Basisinformationen zum jeweiligen Fall vorliegen. Richtet sich die Sicherheitsbehörde an den Access-Provider und zitiert – so wie dies in der Praxis meist der Fall ist – lediglich den Wortlaut der Bestimmungen, kann über die Glaubhaftigkeit eines derartigen Begehrens keine Aussage getroffen werden[616]. Es kann in diesen Fällen, wenn überhaupt, nur überprüft werden, ob sich die Sicherheitsbehörde auf eine dem Grunde nach geeignete Rechtsgrundlage stützt oder nicht. Trifft den Access-Provider daher die vertragliche Schutzpflicht, die Erfüllung des Begehrens von einer umfassenden Information durch die Sicherheitsbehörde abhängig zu machen? Für eine derartige These ließen sich zumindest im Hinblick auf § 53 Abs 3b SPG zwei Argumente vorbringen:

Erstens sprechen die Materialien wie erwähnt davon, dass die Dokumentation des Auskunftsbegehrens aus Gründen der Nachvollziehbarkeit zu erfolgen habe. Diese Nachvollziehbarkeit kann sich sinnvollerweise nur auf den Access-Provider beziehen, weshalb es nicht abwegig erschiene, ihm einen Begründunganspruch

---

[615] VfGH 1. 7. 2009, G 31/08.

[616] Ebenso die WKO in ihrem im Internet veröffentlichten Informationsblatt für ihre Mitglieder. Abrufbar unter http://portal.wko.at/wk/format_detail.wk?AngID=1&StID=386310&DstID=5000 (Stand April 2010).

zuzugestehen[617]. Ein derartiger Begründungsanspruch des Access-Providers würde überdies dem Ziel dienen, Missbrauch vorzubeugen.

Zweitens gilt das Haftungsprivileg in § 53 Abs 3b SPG wie erwähnt nur in jenen Fällen, in denen er einem glaubhaften Auskunftsbegehrens entspricht. Dies legt ebenfalls nahe, dass er auf eine Vervollständigung seines Informationsstandes drängen muss, da er andernfalls die Glaubhaftigkeit des Auskunftsbegehrens unmöglich beurteilen kann.

Die Annahme einer entsprechenden Schutzpflicht würde demnach sowohl mit dem Telos der Bestimmung als auch mit den gezeigten historischen Erwägungen im Einklang stehen. Allerdings steht der klare Wortlaut der Abs 3a und 3b des § 53 SPG dieser Auffassung entgegen. Gem Abs 3a leg cit sind die begehrten Auskünfte „unverzüglich und kostenlos" zu erteilen. Abs 3b leg cit sieht zwar einen Kostenersatz vor, dennoch ist die Auskunft auch nach dieser Bestimmung „unverzüglich" zu erteilen. Zudem bestimmt § 98 TKG 2003, dessen Vorbildwirkung für § 53 Abs 3b SPG die Materialien wie erwähnt betonen, dass der Access-Provider die Erfüllung des Auskunftsbegehrens nicht von der vorherigen Darlegung der Notwendigkeit abhängig machen darf. Da der Access-Provider die Auskünfte unverzüglich zu erteilen hat, scheidet eine vertragliche Schutzpflicht im obigen Sinne mE aus.

Sollte sich aus der Dokumentation erschließen lassen, dass die Behörde unzulässigerweise das SPG als Grundlage für ihr Auskunftsbegehren heranzog und eigentlich eine Anordnung iSd des § 138 StPO erforderlich wäre, ist der Access-Provider zur Verweigerung des Auskunftsbegehrens verpflichtet[618].

6.1.4.5. Pflicht zur Information des Rechtsschutzbeauftragten

In jenen Fällen, in denen der Access-Provider Zweifel an der Rechtmäßigkeit des Auskunftsbegehren hat oder bei Aufwendung der gebotenen Sorgfalt haben muss, ist ihm wie gezeigt die verpflichtende Ergreifung von Rechtsmitteln unzumutbar. Wenn ihn aus Angst vor allfälligen strafrechtlichen Konsequenzen auch keine Schutzpflicht trifft, seinen Vertragspartner zu informieren, kann er seinen Kunden nur dadurch schützen, indem er den Rechtsschutzbeauftragten auf seine Bedenken aufmerksam macht. Dieser kann den geäußerten Bedenken dann unter Inanspruchnahme seiner umfassenden Einsichtsrechte nachgehen und den Betroffenen erforderlichenfalls informieren oder eine Beschwerde bei der DSK einbringen (§ 91d Abs 3 siehe dazu schon

---

[617] *Raschhofer,* in *Zankl* (Hrsg), Auf dem weg zum Überwachungsstaat (2009) 97ff.

[618] *Klingenbrunner/Bresich,* Telekommunikationsunternehmen: Beschränkter Rechtsschutz gegen Polizeihandeln? ecolex 2008, 475 (477), die sich dabei auf § 93 TKG 2003 stützen.

oben). Eine derartige Pflicht scheint durchaus zumutbar, da sie für den Access-Provider nur mit relativ geringem Aufwand verbunden ist. Sie lässt sich nahezu automatisieren. Eine Kurznachricht, in welcher der Fall ausreichend identifiziert und die Bedenken kurz dargelegt werden, liegt wohl noch im Bereich des Zumutbaren. Der Access-Provider muss dabei auch kein Risiko eingehen, wie dies bei der Einbringung einer Beschwerde der Fall wäre. Der Rechtsschutzbeauftragte hat bereits durch die Sicherheitsbehörden über jedes Auskunftsverlangen informiert zu werden, weshalb eine Pflicht zur besonderen Information durch den Access-Provider nur in Ausnahmefällen bestehen kann. Dies wird vor allem dann anzunehmen sein, wenn dem Access-Provider im konkreten Fall Umstände bekannt sind, von denen er annimmt, dass der Rechtsschutzbeauftragte darüber nicht im Bilde ist und diese einen Missbrauch nahe legen.

6.1.4.6. Verweigerungspflicht

Wie bereits erwähnt, hat der Access-Provider die Erfüllung des Auskunftsbegehrens zu verweigern, wenn der dies nur durch Verarbeitung von Daten könnte, die er rechtmäßigerweise gar nicht mehr besitzen dürfte.

6.2. § 98 TKG 2003

6.2.1. Der Wortlaut der Bestimmung

§ 98 TKG 2003 bestimmt:

„Betreiber haben Betreibern von Notrufdiensten auf deren Verlangen Auskünfte über Stammdaten im Sinne von § 92 Abs. 3 Z 3 lit. a bis d sowie über Standortdaten im Sinne des § 92 Abs. 3 Z 6 zu erteilen. In beiden Fällen ist Voraussetzung für die Zulässigkeit der Übermittlung ein Notfall, der nur durch Bekanntgabe dieser Informationen abgewehrt werden kann. Die Notwendigkeit der Informationsübermittlung ist vom Betreiber des Notrufdienstes zu dokumentieren und dem Betreiber unverzüglich, spätestens jedoch innerhalb von 24 Stunden nachzureichen. Der Betreiber darf die Übermittlung nicht von der vorherigen Darlegung der Notwendigkeit abhängig machen. Den Betreiber des Notrufdienstes trifft die Verantwortung für die rechtliche Zulässigkeit des Auskunftsbegehrens."

6.2.2. Die Auskunftsbestimmung im Detail

Nach dieser Bestimmung müssen Access-Provider den Betreibern von Notrufdiensten auf deren Verlangen Auskünfte über die Standortdaten eines Endgerätes

erteilen, sofern dadurch ein Notfall abgewehrt werden kann. Die Betreiber von Notrufdiensten haben die Notwendigkeit der Informationsübermittlung zu dokumentieren und dem Betreiber unverzüglich, jedoch spätestens binnen 24 Stunden nachzureichen. Nach den EBRV ist es unmöglich den Begriff des Notrufdienstes taxativ zu umschrieben[619]. Eine präzise Definition lässt sich den konkreten Materiegesetzen entnehmen. Notrufdienste sind Einrichtungen, denen die Abwehr von Gefahren für Leib, Leben, Gesundheit und Eigentum obliegt, also etwa Rettung, Feuerwehr, Sicherheitspolizei, etc..

Sollte der Access-Provider entgegen § 98 TKG 2003 keine Auskunft über Standortdaten erteilen, begeht er eine Verwaltungsübertretung nach § 109 Abs 3 Z 17 leg cit und ist mit einer Geldstrafe von bis zu 37 000 Euro zu bestrafen.

Aus Sicht des Gesetzgebers schien die Ergänzung der schon zuvor aufgrund § 98 TKG 2003 bestehenden Rechtslage durch § 53 Abs 3b SPG nötig, da Betreiber auch dann zur Bekanntgabe von Standortdaten verpflichtet sein sollen, wenn zuvor kein Notruf abgesetzt wurde. In Praxi treten häufig Fälle auf, in denen bekannt ist, dass eine Person in Gefahr ist, diese jedoch nicht mehr in der Lage war, einen Notruf zu tätigen[620]. Der Gesetzgeber geht offenkundig davon aus, dass ohne Notruf des Gefährdeten keine Auskunft nach § 98 TKG 2003 erteilt werden darf[621]. Dies überzeugt aber nicht, da auch der Wortlaut des § 98 TKG 2003 keinen Notruf der gefährdeten Person, sondern lediglich das Vorliegen eines „Notfalls" voraussetzt[622]. Es ist daher nicht einzusehen, weshalb überhaupt eine neue sicherheitspolizeiliche Befugnis neben § 98 TKG 2003 nötig war. Allerdings gestattet § 53 Abs 3b SPG zusätzlich eine exakte Lokalisierung des Endgerätes der gefährdeten Person und geht in diesem Punkt über die durch § 98 TKG 2003 eröffneten Möglichkeiten hinaus.

---

619 RV 128 BlgNR XXII GP 18.

620 RV 272 BlgNR XXIII. GP 5; Dort heißt es: „Hinkünftig sollen Betreiber auch dann Standortdaten eines Mobiltelefons bekannt geben können, wenn zuvor kein Notruf einer hilfsbedürftigen Person beim Betreiber eines Notrufdienstes eingelangt ist (vgl. § 98 TKG 2003)."; vgl auch *Kunnert,* Der sicherheitspolizeiliche Griff nach Telekommunikationsdaten. Möglichkeiten – Grenzen – Kritik, in *Jahnel* (Hrsg)*,* Datenschutzrecht und E-Government: Jahrbuch 2008 (2008) 128.

621 Davon scheint auch das BMI auszugehen, vgl den Erlass des BMI vom 28. 1. 2008, GZ 94.762/101-GC/08, verfügbar unter: http://portal.wko.at/wk/format_detail.wk?AngID=1&StID=386310&DstID=5000 (Stand 1. 10. 2008)

622 *Raschhofer*, in *Zankl* (Hrsg), Auf dem Weg zum Überwachungsstaat? (2009) 96.

6.2.3. Die Dokumentation der Notwendigkeit

Es gelten insoweit dieselben wie auch schon im Zusammenhang mit § 53 Abs 3b SPG dargestellten Erwägungen (vgl oben Kapitel 6.1.4.4).

6.2.4. Vertragliche Pflicht zur Ergreifung von Rechtsschutzmaßnahmen

Das TKG 2003 kennt keine den §§ 87ff SPG entsprechenden Rechtsschutzinstrumentarien. Die Frage nach einer Pflicht zur Ergreifung bestimmter Rechtsmittel durch den Access-Provider im Nachhinein erübrigt sich somit.

6.2.5. Vertragliche Pflicht zur Verweigerung

Fraglich ist hier ausnahmsweise die Pflicht zur Überprüfung, ob die Daten, die zur Beauskunftung nötig sind, überhaupt zulässigerweise vorhanden sind und ob sie für den angestrebten Zweck verwendet werden dürfen. Selbst wenn dies nicht der Fall sein sollte, darf dies mE nicht ohne weiteres zur Verweigerung des Auskunftsbegehrens führen. Dies liegt daran, dass eine Verweigerung des Auskunftsbegehrens dem Ziel des Schutzes der Privatsphäre dient. Der Access-Provider ist seinem Vertragspartner jedoch nicht nur zum Schutz seiner Privatsphäre verpflichtet, sondern auch zum Schutz seiner sonstigen Güter. § 98 TKG 2003 dient dem Schutz des Lebens und der körperlichen Integrität des Benutzers in Notsituationen. In derartigen Fällen hat der Access-Provider daher zwischen dem Schutz der Privatsphäre und dem Schutz des Lebens bzw der Gesundheit seines Vertragspartners oder mit diesem in Verbindung stehender Personen abzuwägen. Diese Abwägung hat zugunsten des Lebens und der Gesundheit des Vertragspartners des Access-Providers auszugehen. Der Access-Provider ist in diesen Fällen daher mE sogar dann zur Preisgabe der Standortdaten verpflichtet, wenn er sie gar nicht mehr haben dürfte. Er bleibt aber für rechtswidrige Speicherungen von Standortdaten trotzdem voll verantwortlich.

Selbst wenn der Access-Provider an der Rechtmäßigkeit des Auskunftsbegehrens zweifeln sollte, kann ihm – außer in eindeutigen Fällen – eine Verweigerung angesichts der drohenden relativ hohen Verwaltungsstrafe (€ 37.000) nicht zugemutet werden.

Im Ergebnis lässt sich also festhalten, dass es in praxi wohl kaum Fälle geben dürfte, in denen der Access-Provider aufgrund seiner vertraglichen Schutz- und Sorgfaltspflichten zu einer Verweigerung eines Auskunftsbegehrens nach § 98 TKG 2003 verpflichtet ist.

6.3. § 90 Abs 6 TKG 2003

6.3.1. Der Wortlaut der Bestimmung

§ 90 Abs 6 TKG 2003 lautet:

„Betreiber von Kommunikationsdiensten sind verpflichtet, Verwaltungsbehörden auf deren schriftliches und begründetes Verlangen Auskunft über Stammdaten iSv § 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."

Unter Betreibern sind wohl „Betreiber von öffentlichen Kommunikationsdiensten" iSd § 3 Z 1 bzw 3 TKG 2003 und damit Access-Provider im hier verstandenen Sinne gemeint.

Die Materialien zu dieser Bestimmung sind recht knapp gefasst. Dort heißt es lediglich: *„Die Verwaltungsbehörden bedürfen dieser Informationen zur Durchführung von Verwaltungsstrafverfahren*[623]*."* Daraus folgt, dass nur die für die Verfolgung von Verwaltungsübertretungen zuständigen Behörden in Ausübung dieser Funktion berechtigt sind, Auskunftsbegehren nach § 90 Abs 6 TKG 2003 an den Access-Provider zu richten. Private sind auch dann nicht zur Auskunft berechtigt, wenn sie Opfer der Verwaltungsübertretung sein sollten[624]. Die Zuständigkeit der Behörde zur Strafverfolgung ergibt sich aus § 26 VStG bzw Verwaltungsvorschriften, welche die Strafverfolgung anderen Behörden als den Bezirksverwaltungsbehörden zuweisen.

Es dürfen lediglich Stammdaten, also Name, Wohnanschrift, Teilnehmernummer, etc. bekannt gegeben werden. Sofern dazu die andere Datenkategorien zu verarbeiten sind, sind der bereits dargestellte Zusammenhang zwischen den einzelnen Datenkategorien und die sich daraus ergebenden Konsequenzen zu beachten (siehe dazu schon oben Kapitel 4.4.6).

Voraussetzung ist, dass der Betroffene unter dem Verdacht steht, über ein öffentliches Kommunikationsnetz eine Verwaltungsübertretung begangen zu haben. Ausreichend ist also nicht der bloße Verdacht einer Verwaltungsübertretung, sondern es müssen zusätzlich Anhaltspunkte dafür bestehen, dass diese über ein Kommunikationsnetz begangen wurde. Als Beispiel könnte man etwa an die telefonische Anstiftung (§ 7 VStG) zu einer Verwaltungsstraftat denken. Die Formulierung, dass die

---

[623] RV 128 BlgNR XII GP, 17.

[624] *Wiebe,* Auskunftsverpflichtung der Access-Provider, MR 2005, H 4 Beilage 1, 12.

Verwaltungsübertretung *„durch eine über ein öffentliches Telekommunikationsnetz gesetzte Handlung*" begangen worden sein muss, legt nahe, dass die ganze Verwaltungsübertretung über das Kommunikationsnetz begangen worden sein muss. Nicht ausreichend wäre daher, wenn der Verdächtige etwa telefonisch nur ein paar Baumaterialien bestellt, mit denen er in weiterer Folge ohne erforderliche Bewilligung errichtet. Die Straftat muss so beschaffen sein, dass sie zur Gänze über das Kommunikationsnetz begangen werden kann.

Für das an den Access-Provider gerichtete Auskunftsbegehren ist die Schriftform vorgesehen. Zudem normiert § 90 Abs 6 TKG 2003 im Gegensatz zu § 98 leg cit ausdrücklich, dass es begründet werden muss. Zum insoweit recht ähnlich formulierten § 87 b Abs 3 UrhG („ausreichend begründetes Verlangen") wird vertreten, dass dem Provider gegenüber hinreichend konkrete Angaben über die den Verdacht der Rechtsverletzung begründenden Tatsachen zu machen sind, ein Nachweis der konkreten Verletzungshandlung ist nicht nötig[625]. Selbiges wird wohl auch in Bezug auf § 90 Abs 6 TKG 2003 gelten. Ausreichend wäre mE etwa die Bezugnahme auf eine Zeugenaussage, aus der sich ergibt, dass eine bestimmte Verwaltungsstraftat von einem bestimmten Anschluss aus begangen wurde. Wird diese samt Auskunftsbegehren dem Access-Provider zur Kenntnis gebracht, hat er die begehrten Stammdaten herauszugeben.

Die Verletzung der Auskunftspflicht kann wiederum eine Verwaltungsstrafe iSd § 109 Abs 3 Z 13 TKG 2003 darstellen, die mit einer Verwaltungsstrafe von bis zu € 37.000 bedroht ist.

6.3.2. Vertragliche Pflicht zur Ergreifung von Rechtsschutzmaßnahmen

Schon oben im Zusammenhang mit § 98 TKG 2003 wurde ausgeführt, dass das TKG 2003 keine spezifischen Rechtsschutzinstrumentarien kennt. Sofern die Verwaltungsbehörde mit Befehls- oder Zwangsgewalt vorgeht – was aus der Praxis nicht bekannt ist – könnte zwar eine Beschwerde vor dem UVS gem § 67a AVG erwogen werden. Allerdings würde sich ein derartiges Verfahren wenn überhaupt nur reflexhaft günstig auf die Position des Vertragspartners des Access-Providers auswirken – der Kunde wäre keine Partei des Verfahrens – und erscheint ihm aufgrund des relativ großen Aufwandes unzumutbar. Außerdem hat diese erst im Nachhinein erfolgende „Verteidigung" wiederum deshalb wenig Sinn, weil die Vertraulichkeit der Daten zu diesem Zeitpunkt bereits verletzt wurde.

---

[625] *Guggenbichler* in *Ciresa* (Hrsg), Österreichisches Urheberrecht (12. ErgLf. 2009) § 87b UrhG Rz 15.

6.3.3. Verweigerungspflicht

Der Access-Provider hat auch hier wie immer zu überprüfen, ob er die Daten, die er zu Bearbeitung des Auskunftsbegehrens benötigt, zulässigerweise speicherte und verneinendenfalls das Auskunftsbegehren zu verweigern. Soweit er nur den Namen zu einer von der Behörde genannten Teilnehmernummer zu beauskunften hat, werden nur Stammdaten verarbeitet, die er jedenfalls zulässigerweise speichert.

Da hier das Gesetz die Begründungspflicht der Verwaltungsbehörde anders als bei anderen Bestimmungen ausdrücklich erwähnt und auch nicht bestimmt, dass der Access-Provider die begehrte Auskunft unverzüglich zu erteilen hat, erscheint es durchaus vertretbar, dass er auf die Vervollständigung einer zunächst mangelhaften Begründung bestehen kann. Aus seiner Schutzpflicht hinsichtlich der Privatsphäre seines Kunden ergibt sich, dass er dies auch muss. Kann er die Rechtmäßigkeit des Auskunftsbegehrens aufgrund der oberflächlichen Angaben der Behörde nicht beurteilen, hat er daher nicht etwa aus Furcht vor der drohenden Verwaltungsstrafe – die wie dargestellt bis zu € 37.000 betragen kann – ohne weiteres die gewünschten Stammdaten herauszugeben, sondern auf eine Präzisierung der Begründung durch die Behörde hinzuwirken. Solange keine ausreichende Begründung erfolgt, darf er mE mit der Erfüllung des Auskunftsbegehrens zuwarten, ohne sich dem Risiko einer Strafbarkeit auszusetzen. § 109 Abs 3 Z 13 TKG 2003 stellt es unter Strafe, entgegen § 90 nicht die notwendigen Auskünfte oder nicht Auskunft über Stammdaten zu erteilen. Da § 90 Abs 6 TKG 2003 den Access-Provider nur auf ein schriftliches und begründetes Verlangen hin zur Auskunft verpflichtet, kann im Drängen auf eine Vervollständigung keine Verletzung seiner Auskunftspflicht liegen.

Die Verweigerungspflicht trifft ihn nicht bereits bei Zweifeln an der Rechtmäßigkeit des Auskunftsbegehrens, da ihm eine Weigerung dann aufgrund der drohenden Verwaltungsstrafe und der Möglichkeit der Behörde einen Akt unmittelbarer Zwangsgewalt zu setzen unzumutbar erscheint. Eine Verweigerungspflicht kann aber mE bestehen, wenn aus seiner Sicht ausnahmsweise feststeht, dass das Auskunftsbegehren unberechtigt ist. Dies wäre etwa dann der Fall, wenn nach den Angaben der Behörde lediglich eine bloße Vorbereitungshandlung, nicht aber wie vom Gesetz gefordert die gesamte Verwaltungsübertretung über das Telekommunikationsnetz gesetzt wurde.

6.4. § 22 Abs 2a MBG

6.4.1. Der Wortlaut der Bestimmung[626]

„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."

6.4.2. De Befugnis im Detail

Das MBG kennt ähnlich dem SPG Aufgaben (§ 6ff: Wachdienst; § 20ff: nachrichtendienstliche Aufklärung und Abwehr; § 26 militärische Luftraumüberwachung) und Befugnisse, die der Erfüllung dieser Aufgaben dienen. Das MBG folgt in seiner Struktur dem SPG[627]. Es gilt auch hier das Prinzip, dass stets eine Aufgabe bestehen muss, zu deren Erfüllung eine Befugnis ausgeübt wird[628]. Die Befugnis des § 22 Abs 2a SPG darf nur zur nachrichtendienstlichen Aufklärung[629] oder Abwehr[630] erfolgen. Die Befugnis darf nur von militärischen Organen (§ 1 Abs 1 MBG)[631] und von militärischen Dienststellen (§ 1 Abs 2 MBG)[632] ausgeübt werden. Betreiber von

---

626 Abs 2a wurde eingefügt durch BGBl I 103/2002.

627 RV 76 BlgNR XXI. GP, 31; *Funk,* Der unvollendete Rechtsstaat, in *Akyürek/Baumgartner/Jahnel/Lienbacher* (Hrsg), Verfassung in Zeiten des Wandels, Symposion zum 60. Geburtstag von Heinz Schäffer (2002) 199 (211).

628 Vgl *Hauer/Keplinger/Kreutner,* Militärbefugnisgesetz, (2005) 16.

629 Diese dient gem § 20 Abs 1 MBG *„der Beschaffung, Bearbeitung, Auswertung und Darstellung von Informationen über das Ausland oder über internationale Organisationen oder sonstige zwischenstaatliche Einrichtungen betreffend militärische und damit im Zusammenhang stehende sonstige Tatsachen, Vorgänge und Vorhaben.*"

630 Diese dient gem § 20 Abs 2 MBG *„dem militärischen Eigenschutz durch die Beschaffung, Bearbeitung, Auswertung und Darstellung von Informationen über Bestrebungen und Tätigkeiten, die vorsätzliche Angriffe gegen militärische Rechtsgüter zur Beeinträchtigung der militärischen Sicherheit erwarten lassen.*" Zu den Begriffen der nachrichtendienstlichen Aufklärung und Abwehr vergleiche ferner *Wiederin,* Privatsphäre und Überwachungssaat (2003) 152ff.

631 Das sind zum einen Soldaten (Z 1) sowie „Angehörige der Heeresverwaltung, wenn diese Organe ermächtigt sind, Befugnisse nach diesem Bundesgesetz auszuüben, soweit diese Personen mit der Erfüllung von Aufgaben der militärischen Landesverteidigung betraut sind (Z 2).

632 Das sind alle Dienststellen im Vollziehungsbereich des Bundesministers für Landesverteidigung und Sport.

Telekommunikationsdiensten sind Access-Provider im hier verstandenen Sinne (siehe dazu oben Kapitel 4.1).

Die Bestimmung wurde § 53 Abs 3a SPG in seiner alten Fassung nachgebildet[633]. Die zu beauskunftenden Daten entsprechen – auch dem Wortlaut nach – exakt jenen gem § 53 Abs 3a Z 1 SPG. Dort geltende Überlegungen lassen sich aufgrund der Vorbildwirkung[634] der Bestimmung im SPG auch auf die Auskunftsbefugnis im MBG übertragen. Der Anschluss ist entweder anhand der Teilnehmernummer oder anhand des Namens und der Anschrift hinreichend zu individualisieren. So könnte die Behörde etwa die Rufnummer bekannt geben und den zugehörigen Namen samt Anschrift verlangen. Hierbei handelt es sich typischerweise um jene Daten, die auch regelmäßig in Teilnehmerverzeichnissen eingesehen werden können[635]. Da der Gesetzgeber § 53 Abs 3a SPG idF vor BGBl I 114/2007 für keine ausreichende Grundlage zur Ermittlung von IP-Adressen hielt, novellierte er diese Bestimmung. In § 22 Abs 2a MBG fehlen Bestimmungen, welche die Auskunft über eine „IP-Adresse zu einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung" (§ 53 Abs 3a Z 2 SPG) bzw die Auskunft über „Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war" (Z 3 leg cit) erlauben. Somit kann eindeutig gefolgert werden, dass § 22 Abs 2a MBG keine geeignete Rechtsgrundlage für die Beauskunftung von IP-Adressen oder von Stammdaten zu einer der Behörde bekannten IP-Adresse abgibt. § 22 Abs 2a MBG entspricht § 53 Abs 3a SPG in seiner alten Fassung, welcher derlei Auskünfte ebenfalls nicht ermöglichte und daher entsprechend novelliert werden musste. Dieses Ergebnis folgt auch aus der Auslegung des Begriffs „Teilnehmernummer" vor dem Hintergrund der Begriffsbestimmungen im TKG 2003. Dieses verwendet den Begriff Teilnehmernummer in § 92 Abs 3 Z 3 lit d und meint damit nur Teilnehmernummern im klassischen Telefoniebereich und keinesfalls IP-Adressen[636].

Aus dem systematischen Zusammenhang ergibt sich weiters, dass § 22 Abs 2a MBG keine geeignete Grundlage für die so genannte kleine Rufdatenrückerfassung abgibt. Eine solche ermöglicht § 53 Abs 3a SPG, 2. Satz, der bestimmt, dass die Bezeichnung eines Anschlusses nach Z 1 leg cit in bestimmten Fällen auch durch Bezugnahme auf ein von diesem Anschluss geführtes Gespräch durch Bezeichnung eines möglichst genauen Zeitraumes und der passiven Teilnehmernummer erfolgen kann. Da im MBG eine vergleichbare Bestimmung fehlt, lässt sich wegen der

---

633 *Raschauer/Wessely*, Militärbefugnisgesetz[2] (2007) § 22 Anm 5.

634 *Wiederin,* Privatsphäre und Überwachungsstaat (2003) 170.

635 *Reindl-Krauskopf/Tipold/Zerbes,* in *Fuchs/Ratz* (Hrsg) Wiener Kommentar zur Strafprozessordnung (2009) § 134 Rz 61.

636 RV 128 BlgNR XXII. GP, 17.

Vorbildwirkung der Auskunftsbestimmung des SPG folgern, dass der Gesetzgeber den militärischen Organen und Dienststellen keine so weit reichenden Befugnisse einräumen wollte[637].

Das MBG gestattet keinesfalls die Ermittlung von Inhalts- oder Standortdaten[638].

6.4.3. Rechtsschutz

Auch § 22 Abs 2a MBG ist als geheime Maßnahme dem Betroffenen gegenüber konzipiert, eine Verständigungspflicht durch die Behörde besteht nicht. Bedenken die schon im Zusammenhang mit § 53 Abs 3a und 3b SPG erörtert wurden (siehe oben Kapitel 6.1.4.2), bestehen auch hier.

Die militärischen Organe und Dienststellen werden bei der Ausübung ihrer Befugnisse von einem vom Bundesminister für Landesverteidigung gem § 57 Abs 1 MBG ernannten weisungsfreien Rechtsschutzbeauftragten überwacht. Seine Aufgabe ist es, die Rechte der Betroffenen, die von der Ausübung der Befugnisse oft keine Kenntnis erlangen, wahrzunehmen und ein Mindestmaß an faktischer Effizienz des Rechtsschutzes zu wahren[639]. Er ist zur rechtlichen Kontrolle von Maßnahmen der nachrichtendienstlichen Aufklärung und Abwehr befugt. Dem Rechtsschutzbeauftragten sind gem § 57 Abs 4 MBG zur Wahrnehmung seiner Aufgaben jederzeit Einsicht in alle erforderlichen Unterlagen und Aufzeichnungen zu gewähren, auf Verlangen Abschriften oder Kopien einzelner Aktenstücke unentgeltlich auszufolgen und alle erforderlichen Auskünfte zu erteilen. Insofern kann ihm gegenüber Amtsverschwiegenheit nicht geltend gemacht werden. Ausgenommen sind Auskünfte und Unterlagen über die Identität von Personen oder über Quellen, deren Bekannt werden die nationale Sicherheit oder die Sicherheit von Menschen gefährden würde, weiters Abschriften und Kopien, wenn das Bekannt werden der Information die nationale Sicherheit oder die Sicherheit von Menschen gefährden würde. Nimmt der Rechtsschutzbeauftragte im Zuge seiner

---

[637] Vgl auch die Begründung des Abänderungsantrags 658/A, XXI. GP im stenographischen Protokoll der 107. Sitzung des Nationalrates in der XXI. GP auf Seite 223: *„Schließlich soll auch für die militärischen Nachrichtendienste die für die Sicherheitspolizei bereits im Jahr 1999 (§ 53 Abs. 3a SPG) eingeführte Möglichkeit zur Eruierung bestimmter "Stammdaten" von Teilnehmern am öffentlichen Telekommunikationsverkehr eröffnet werden. Auf die Normierung der im polizeilichen Bereich ebenfalls zulässigen Erhebung von "Ermittlungsdaten" kann im Bereich der militärischen Nachrichtendienste verzichtet werden, da bei einem laufenden Angriff gegen militärische Rechtsgüter ohnedies gemäß § 2 Abs. 2 MBG die Sicherheitsexekutive grundsätzlich zur weiteren Veranlassung zuständig ist.*"

[638] *Hauer/Keplinger/Kreutner,* Militärbefugnisgesetz, Linz (2005) § 22 A 20; *Raschauer/Wessely,* Militärbefugnisgesetz[2] (2007) § 22 Anm 5.

[639] VfGH 23.1.2004, G 363/02.

kontrollierenden Tätigkeit wahr, dass durch das Verwenden von Daten Rechte eines Betroffenen verletzt worden sind, der von dieser Datenverwendung keine Kenntnis hat, kann er den Betroffenen informieren. Scheidet diese Möglichkeit aus, weil eine Information des Betroffenen die Sicherung der Einsatzbereitschaft des Bundesheeres oder die Interessen der umfassenden Landesverteidigung gefährden oder erheblich behindern würde, ist er zu Einbringung einer Beschwerde an die DSK gem § 55 MBG befugt. Zur Problematik, dass er nur „befugt", jedoch nicht verpflichtet ist, vgl schon oben Kapitel 6.1.4.2). Wie bereits weiter oben grundlegend ausgeführt, entbindet die mögliche Information des Betroffenen durch den Rechtsschutzbeauftragten den Access-Provider mE nicht von seiner vertraglichen Pflicht zur Information. Anderes kann ausnahmsweise dann gelten, wenn ihm seitens des militärischen Organs bzw der Dienststelle diesbezüglich gegenteilige Instruktionen erteilt wurden.

6.4.4. Vertragliche Pflicht zur Ergreifung von Rechtsschutzmaßnahmen?

Auch der Access-Provider hat ein Recht darauf, dass ihm gegenüber die im MBG vorgesehenen militärischen Maßnahmen nur in den Fällen und der Art gesetzt werden, die gesetzlich vorgesehen sind (§ 53 MBG). Liegen also die Voraussetzungen für eine Befugnisausübung gem § 22 Abs 2a MBG nicht vor und muss der Access-Provider dennoch beauskunften, ist er ähnlich wie im Falle des SPG beschwert und zur Beschwerdeerhebung gem § 54 Abs 2 MBG legitimiert. Eine Beschwerde gem § 55 MBG (wegen Verletzung datenschutzrechtlicher Bestimmungen) scheidet mE aus, weil dazu nur der durch die Datenverwendung Betroffene aktivlegitimiert ist[640]. Fraglich ist die Pflicht einer Beschwerdeeinbringung in jenen Fällen, in denen etwa aufgrund eines drohenden Strafbarkeitsrisikos eine Information des Betroffenen ausscheidet. Der Access-Provider ist zur Beschwerdeeinbringung jedoch aus denselben Gründen nicht verpflichtet, die auch schon im Zusammenhang mit dem SPG angeführt wurden (Kapitel 6.1.4.3). Zum einen ist eine Beschwerde mit erheblichem ihm kaum noch zumutbarem Aufwand verbunden, zum anderen vermag eine im Nachhinein erfolgende Beschwerdeführung die Verletzung der Privatsphäre nicht mehr rückgängig zu machen. Hinzu kommt, dass im Falle des MBG jeglicher Hinweis im Gesetz darauf fehlt, dass der Access-Provider über den Grund des Auskunftsbegehrens in Kenntnis zu setzen ist. Während § 53 Abs 3b SPG wenigstens noch von einer „Dokumentation des Auskunftsbegehrens" spricht, sieht das MBG keinerlei Informationsweitergabe an den Access-Provider vor. Daher kann er sich über die Rechtmäßigkeit der Befugnisausübung und die Erfolgsaussichten einer Beschwerde überhaupt kein Urteil bilden.

---

[640] *Hauer/Keplinger/Kreutner,* Militärbefugnisgesetz (2005) § 55 Anm 3;

6.4.5. Vertragliche Pflicht zur Informationen des Rechtsschutzbeauftragten

Im Falle des SPG wurde für jene Fälle, in denen der Access-Provider aus bestimmten Gründen den Kunden nicht informieren kann, eine Pflicht angenommen, den Rechtsschutzbeauftragten auf Bedenken gegen die Rechtmäßigkeit der Befugnisausübung gesondert hinzuweisen (vgl Kapitel 6.1.4.5). Diese Pflicht wird wohl auch im Bereich des MBG bestehen. Allerdings wird der Access-Provider in praxi aufgrund des Umstandes, dass ihm die Behörde keinerlei Informationen über den Grund des Auskunftsbegehrens zu geben hat, wohl nie Kenntnis von Umständen erlangen, die einen Missbrauch der Befugnis im Besonderen nahe legen. Sollte dies jedoch ausnahmsweise der Fall sein, ergibt sich durch ergänzende Auslegung die vertragliche Pflicht, den Rechtsschutzbeauftragten gesondert auf die Bedenken aufmerksam zu machen, sodass dieser die Rechte des Betroffenen wahren kann.

6.4.6. Pflicht zur Verweigerung der Auskunft

Anders als im Fall des SPG werden im Falle des MBG wohl kaum Fälle eintreten, in welchen der Access-Provider die Erfüllung des Auskunftsbegehrens verweigern könnte. Dies liegt daran, dass er die zur Erfüllung des Begehrens benötigten Daten (Name, Anschrift, Teilnehmernummer) allesamt für die Dauer des Vertragsverhältnisses als Stammdaten zu speichern hat. Es sind also kaum Fälle denkbar, in denen die Bearbeitung des Auskunftsbegehrens nur unter Verwendung unzulässigerweise gespeicherter Daten möglich ist.

6.5. § 87b Abs 3 UrhG[641]

6.5.1. Der Wortlaut der Bestimmung

„Vermittler im Sinn des § 81 Abs. 1a haben dem Verletzten auf dessen schriftliches und ausreichend begründetes Verlangen Auskunft über die Identität des Verletzers (Name und Anschrift) beziehungsweise die zur Feststellung des Verletzers erforderlichen Auskünfte zu geben. In die Begründung sind insbesondere hinreichend

---

641 Im folgenden Kapitel entsprechen Passagen – vor allem jene, die europarechtliche Dimension dieses Problems betreffen – über weite Strecken Teilen meiner Veröffentlichung „Der urheberrechtliche Auskunftsanspruch gem § 87b Abs 3 UrhG gegen Access-Provider", in *Feiler/Raschhofer,* Innovation und internationale Rechtspraxis, Praxisschrift für Wolfgang Zankl (2009) 661ff.

konkretisierte Angaben über die den Verdacht der Rechtsverletzung begründenden Tatsachen aufzunehmen. Der Verletzte hat dem Vermittler die angemessenen Kosten der Auskunftserteilung zu ersetzen."

6.5.2. Allgemeines

Die Bestimmung des § 87b Abs 3 UrhG beruht nach den Vorstellungen des Gesetzgebers auf Art 8 Abs 3 der Rl 2001/29/EG[642] (fortan: Info-Richtlinie)[643]. Der Auskunftsanspruch steht bei jeder Verletzung iSd § 81 UrhG zu[644]. Er richtet sich gegen Vermittler iSd § 81 Abs 1a UrhG.

Der Begriff des Vermittlers entspricht dem Vermittlerbegriff in Art 5 Abs 1 lit a bzw Art 8 Abs 3[645] der Info-Richtlinie. Vermittler sind Betreiber von Diensten der Informationsgesellschaft, die Inhalte in einem Datennetz zwischen Dritten übertragen[646]. Nach dem 59. Erwägungsgrund der Info-Richtlinie sollen die Rechtsinhaber die Möglichkeit haben, eine gerichtliche Anordnung gegen Vermittler zu beantragen, welche die Rechtsverletzung eines Dritten in Bezug auf ein geschütztes Werk oder einen anderen Schutzgegenstand in einem Netz übertragen. In der Rechtsache *LSG gegen Tele 2* hielt der EuGH fest, dass Access-Provider, die den Nutzern nur den Zugang zum Internet verschaffen, ohne selbst weitere Dienste wie File-Sharing anzubieten oder eine rechtliche oder faktische Kontrolle über den genutzten Dienst auszuüben, als Vermittler iSd §§ 87b Abs 3 bzw 81 Abs 1a UrhG gelten. Der EuGH beantwortete die diesbezügliche Vorlagefrage des OGH eindeutig[647]. Somit seht fest, dass Access-Provider grundsätzlich nach § 87b Abs 3 UrhG auskunftspflichtig sind.

Daneben können auch Suchmaschinenbetreiber, Linksetzer und Host-Provider[648] vermittelnde Tätigkeiten ausüben und somit dem Vermittlerbegriff

---

642 Richtlinie 2001/29/EG des Europäischen Parlamentes und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, ABl L 2001/167, 10.

643 RV 40 BlgNR XXII. GP, 23.

644 *Guggenbichler,* in *Ciresa* (Hrsg), Österreichisches Urheberrecht (12. ErgLf 2009) § 87b UrhG Rz 14 mwN.

645 Vgl auch *Neubauer,* Zur Haftung und Auskunftsverpflichtung von Providern – Aktuelles zu Unterlassungs- und Auskunftspflichten in Österreich mit einem Vergleich zur aktuellen Rechtslage in Deutschland im Zivil- und Strafrecht, MR-INT 2008, 25 (27).

646 *Ofner* in *Kucsko,* urheber.recht (2008) 1162; vgl auch 33. Erwägungsgrund der Info-Richtlinie.

647 EuGH 19.2.2009, C-557/07, MR 2009, 40, Rz 46.

648 Vgl dazu *Schanda,* Haftung für Urheberrechtsverletzungen Dritter im digitalen Umfeld, in *Fallenböck/Galla/Stockinger* (Hrsg), Urheberrecht in er digitalen Wirtschaft (2005) 141 (148).

entsprechen[649]. § 81 Abs 1a UrhG verweist auf die §§ 13 bis 17 ECG. Diese regeln die Haftungsprivilegien von Suchmaschinenbetreibern, Linksetzern und Host-Providern[650]. Damit fallen auch die genannten Personengruppen unter den Vermittlerbegriff des § 81 Abs 1a UrhG und § 87b Abs 3 UrhG.

Der Anspruch erfasst den Namen und die Anschrift des mutmaßlichen Verletzers bzw die „zur Feststellung der Identität erforderlichen Auskünfte". Durch letztere Wendung soll dem Auskunftspflichtigen die Einredemöglichkeit genommen werden, dass nicht feststehe, ob der Inhaber einer IP-Adresse die Verletzung auch tatsächlich begangen habe, die Auskunftspflicht jedoch nur die Preisgabe der Identität eines feststehenden Verletzers erfasse[651].

Das Auskunftsbegehren hat in Schriftform zu erfolgen und muss ausreichend begründet sein. Da es Sinn der Bestimmung ist, dem Verletzten die Verfolgung seiner Rechte zu ermöglichen, muss er nur den Verdacht der Verletzung glaubhaft machen, nicht jedoch die Verletzung als solche beweisen. Die Bestimmung soll ihn dazu in die Lage versetzen, den mutmaßlichen Verletzer zu ermitteln und in weiterer Folge die Verletzung zu beweisen[652]. Die Verletzung muss aber nicht für einen Laien offenkundig sein[653]. Der Access-Provider hat nur auf das ausreichend begründete Verlangen hin Auskunft zu erteilen.

In praxi wendet sich der Rechtsinhaber daher zunächst an den Host-Provider, der den Speicherplatz für die jeweilige Verletzung zur Verfügung stellte, um Auskunft darüber zu erlangen, von welcher IP-Adresse aus die Verletzung begangen wurde. Diese IP-Adresse ist einem bestimmten aus der WHOIS-Datenbank[654] ersichtlichen Access-Provider zugeteilt, der sie seinem Kunden für dessen Verbindung zur Verfügung stellte. Manchmal ist der unmittelbare Inhaber der IP-Adresse auch aus dem WHOIS-Register direkt ersichtlich, weshalb keine Auskunft durch einen Access-Provider mehr vonnöten ist. Meist muss sich der Rechtsinhaber jedoch in einem weiteren Schritt an den Access-Provider wenden, um von ihm Namen und Anschrift des mutmaßlichen

---

649 *Dillenz/Gutman,* Praxiskommentar zum Urheberrecht[2] (2004) § 81 Rz 21.

650 Vgl auch *Schanda,* Auskunftsanspruch gegen Access-Provider über die IP-Adressen von Urheberrechtsverletzern, MR 2005 18 (18).

651 RV 1324 der Beilagen XXII. GP, 4.

652 *Guggenbichler,* in *Ciresa* (Hrsg), Österreichisches Urheberrecht (12. ErgLf. 2009) § 87b Rz 15.

653 *Sofokleus/Mosing,* Urheberrechtlicher Auskunftsanspruch gegen Access-Provider: ein „Pyrrhus-Anspruch"?, ÖBl 2008, 268 (269); *Stomper,* Die Folgen der Megasex-Entscheidung – Mitverantwortlichkeit und Auskunftspflicht von Diensteanbietern, RdW 2005 285 (287).

654 ZB unter http://www.ip-adress.com/whois/ (Stand April 2010); vgl *Edthaler/Schmid,* Auskunft über IP-Adressen im Strafverfahren, MR 2008, 220 (220).

Verletzers zu erhalten. Die Erfüllung des an den Access-Provider heran getragenen Auskunftsbegehrens setzt voraus, dass der Access-Provider die Protokollierungen der von ihm hergestellten Verbindungen (sog logfiles) danach durchsucht, welchem Kunden er diese IP-Adresse zum fraglichen Zeitpunkt zur Verfügung stellte[655]. Die Frage, ob und inwieweit dies zulässig ist, war wie bereits oben mehrfach erwähnt Gegenstand des Verfahrens *LSG gegen Tele 2*. Im Zuge dieses Verfahrens trat auch deutlich die europarechtliche Dimension dieses Problems zu Tage. Betroffen sind Bestimmungen der bereits oben ausführlich dargestellten EK-Datenschutzrichtlinie. Darüber hinaus sind die Info-Richtlinie, die Richtlinie 2004/48/EG[656] (fortan: Enforcement-Richtlinie) und die E-Commerce-Richtlinie betroffen. Insbesondere stellte sich die Frage, inwieweit aus dem Gemeinschaftsrecht eine Verpflichtung der Mitgliedstaaten zur Normierung zivilrechtlicher Auskunftsansprüche abgeleitet werden kann. Diese Frage wurde bereits zuvor im Verfahren *Promusicae* durch den EuGH dahin gehend beantwortet, dass es weder eine Pflicht, noch ein gemeinschaftsrechtliches Verbot der Implementierung zivilrechtlicher Auskunftsansprüche zur Verfolgung urheberrechtlicher Rechtspositionen gibt[657]. Die hier interessierenden Bestimmungen der betroffenen Rechtsakte sollen im Folgenden kurz dargestellt werden:

6.5.2.1. Die Info-Richtlinie

Gem Art 8 Abs 1 der Info-Richtlinie müssen die Mitgliedstaaten bei Verletzungen der in dieser Richtlinie festgelegten Rechte und Pflichten angemessene Sanktionen und Rechtsbehelfe vorsehen und alle notwendigen Maßnahmen zu deren Abwendung treffen. Die betreffenden Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. Nach Abs 2 leg cit müssen die Mitgliedstaaten weiters die erforderlichen Maßnahmen treffen, um sicherzustellen, dass Rechtsinhaber, deren Interessen durch Rechtsverletzungen auf dem jeweiligen Hoheitsgebiet des Mitgliedstaates beeinträchtigt werden, Klage auf Schadenersatz erheben und/oder eine gerichtliche Anordnung beantragen können. Nach Abs 3 leg cit haben die Mitgliedstaaten sicherzustellen, dass die Rechtsinhaber gerichtliche Anordnungen gegen Vermittler beantragen können, deren Dienste von einem Dritten zur Verletzung eines Urheberrechts oder verwandter Schutzrechte genutzt werden. Vor der Entscheidung *Promusicae* wurde in der Literatur aus den genannten Bestimmungen teilweise eine Pflicht der Mitgliedstaaten abgeleitet, zivilrechtliche Auskunftsansprüche in ihre Rechtsordnungen

---

655 *Wiebe*, Auskunftsverpflichtung der Access-Provider, Beilage zu MR 2005/4, 11; *Einzinger/Schubert/Schwabl/Wessely/Zykan*, Wer ist 217.204.27.214? MR 2005, 113 (114).

656 Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums, ABl L 2004/157, 45.

657 EuGH 29.1.2008, C 275/06.

aufzunehmen[658]. Allerdings lässt die Richtlinie offen, wie die erwähnten Maßnahmen im Detail ausgestaltet werden müssen. Daher kann der Info-Richtlinie keine Pflicht der Mitgliedstaaten entnommen werden, eine Pflicht zur Auskunft über personenbezogene Daten im Rahmen eines zivilrechtlichen Verfahrens vorzusehen[659]. Einer derartigen Auslegung steht auch Art 9 Abs 1 der Info-Richtlinie entgegen, der vorsieht, dass die Richtlinie Rechtsvorschriften im Bereich des Datenschutzes und des Schutzes der Privatsphäre unberührt lässt.

6.5.2.2. Die Enforcement-Richtlinie[660]

Gemäß Art 1 der Enforcement-Richtlinie regelt diese Maßnahmen, Verfahren und Rechtsbehelfe, die erforderlich sind, um die Durchsetzung der Rechte des geistigen Eigentums sicherzustellen. Nach Art 3 der Enforcement-Richtlinie, haben die Mitgliedstaaten Maßnahmen, Verfahren und Rechtsbehelfe vorzusehen, die zur Durchsetzung der Rechte des geistigen Eigentums, auf die diese Richtlinie abstellt, erforderlich sind. Diese Maßnahmen, Verfahren und Rechtsbehelfe müssen fair und gerecht sein, außerdem dürfen sie nicht unnötig kompliziert oder kostspielig sein und keine unangemessenen Fristen oder ungerechtfertigten Verzögerungen mit sich bringen. Art 8 Abs 1 lit d der Enforcement-Richtlinie bestimmt überdies, dass sichergestellt sein muss, dass die zuständigen Gerichte im Zusammenhang mit einem Verfahren wegen Verletzung eines Rechts des geistigen Eigentums auf einen begründeten und die Verhältnismäßigkeit wahrenden Antrag des Klägers hin anordnen können, dass Auskünfte über den Ursprung und die Vertriebswege von Waren oder Dienstleistungen, die ein Recht des geistigen Eigentums verletzen, von dem Verletzer und/oder jeder anderen Person erteilt werden, die nachweislich für rechtsverletzende Tätigkeiten genutzte Dienstleistungen in gewerblichem Ausmaß erbrachte. Ähnlich wie Art 9 Abs 1 der Info-Richtlinie bestimmt Art 8 Abs 3 lit e der Enforcement-Richtlinie, dass diese Bestimmung unbeschadet anderer gesetzlicher Bestimmungen gilt, die den Schutz der Vertraulichkeit von Informationsquellen oder die Verarbeitung personenbezogener Daten regeln[661]. Nach

---

[658] Nachweise etwa bei: *Spindler,* „Die Tür ist auf" – Europarechtliche Zulässigkeit von Auskunftsansprüchen gegenüber Providern – Urteilsanmerkung zu EuGH „Promusicae/Telefónica", GRUR 2008 574 (576).

[659] EuGH 29.1.2008, C 275/06, Rz 59; Die Auffassung, Art 8 Abs 3 der Info-Richtlinie normiere einen Auskunftsanspruch – zu finden etwa bei *Schanda,* Auskunftspflicht über Inhaber dynamischer IP-Adressen contra Verpflichtung zur Löschung von Verkehrsdaten, MR 2007, 213 (215); *Stomper,* Auskunftsansprüche gegen Internet-Provider nach österreichischem recht, MR-Int 2005, 99 (100) – ist damit überholt.

[660] Vgl dazu etwa *Frey/Rudolph,* EU-Richtlinie zur Durchsetzung der Rechte des geistigen Eigentums, ZUM 2004, 522ff.

[661] Zusätzlich wird das Verhältnis der Enforcement-Richtlinie zu den Bestimmungen des Datenschutzes in Art 2 Abs 3 geregelt, wonach die Datenschutzrichtlinie unberührt bleibt. Aus teleologischen Gründen hat dies auch im Verhältnis zur EK-Datenschutzrichtlinie zu gelten, vgl

Ansicht der Generalanwältin ließe sich unter den Wortlaut der Bestimmung des Art 8 Abs 1 der Enforcement-Richtlinie auch die Offenlegung der Identität von Internetnutzern subsumieren[662]. Der EuGH hielt jedoch eindeutig fest, dass sich auch aus der Bestimmung des Art 8 Abs 1 Enforcement-Richtlinie vor dem Hintergrund des Abs 3 lit e leg cit letztlich keine zwingende Pflicht der Mitgliedstaaten ableiten lässt, eine Auskunftspflicht betreffend personenbezogene Daten im Rahmen eines zivilrechtlichen Verfahrens in ihre Rechtsordnung zu implementieren[663].

6.5.2.3. Die E-Commerce-Richtlinie[664]

Gemäß Art 1 Abs 1 soll die E-Commerce-Richtlinie einen Beitrag zum einwandfreien Funktionieren des Binnenmarktes leisten, indem sie den freien Verkehr von Diensten der Informationsgesellschaft zwischen den Mitgliedstaaten sicherstellt. Gemäß Art 15 der E-Commerce-Richtlinie können die Mitgliedstaaten Anbieter von Diensten der Informationsgesellschaft dazu verpflichten, die zuständigen Behörden unverzüglich über Informationen der Nutzer ihres Dienstes zu unterrichten oder den zuständigen Behörden auf Verlangen Informationen zu übermitteln, anhand derer die Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Speicherung geschlossen haben, ermittelt werden können. Gemäß Art 18 Abs 1 der E-Commerce-Richtlinie müssen die Mitgliedstaaten sicherstellen, dass die nach innerstaatlichem Recht verfügbaren Klagemöglichkeiten im Zusammenhang mit Diensten der Informationsgesellschaft es ermöglichen, dass rasch Maßnahmen, einschließlich vorläufiger Maßnahmen, getroffen werden können, um eine mutmaßliche Rechtsverletzung abzustellen und zu verhindern, dass den Betroffenen weiterer Schaden entsteht. Auch diese Bestimmungen lassen nach Ansicht des EuGH offen, wie die genannten Maßnahmen von den Mitgliedstaaten konkret umzusetzen sind und verpflichten diese wiederum nicht dazu, einen zivilrechtlichen Auskunftsanspruch in ihre Rechtsordnungen zu aufzunehmen[665].

---

dazu Generalanwältin *Kokott*, Schlussantrag vom 18.7.2007 zu Rechtssache C 275/06 vor dem EuGH, Rz 45-47.

662 So Generalanwältin *Kokott*, Schlussantrag vom 18.7.2007 zu Rechtssache C 275/06 vor dem EuGH, Rz 110.

663 EuGH 29.1.2008, C 275/06, Rz 58; überholt ist damit die Ansicht, dass aus Art 8 der Enforcement-Rl ein zwingender Auskunftsanspruch gegenüber Access-Providern abgeleitet werden kann: *Frey/Rudolph,* EU-Richtlinie zur Durchsetzung der Rechte des geistigen Eigentums, ZUM 2004, 522 (525);

664 Vgl dazu *Stomper,* Europäische Union regelt E-Commerce Die EU-Richtlinie über den Elektronischen Geschäftsverkehr im Überblick, SWK 2000, W 59; *Zankl,* Der Entwurf zum E-Commerce-Gesetz, NZ 2001, 325ff.

665 EuGH 29.1.2008, C 275/06, Rz 59.

6.5.2.4. Ergebnis

Weder aus der E-Commerce-Richtlinie, noch aus der Info-Richtlinie oder der Enforcement-Richtlinie ergibt sich eine Verpflichtung der Mitgliedstaaten, im Hinblick auf einen effektiven Schutz des Urheberrechts die Pflicht zur Mitteilung personenbezogener Daten im Rahmen eines zivilrechtlichen Verfahrens vorzusehen. Die Mitgliedstaaten sind jedoch gemeinschaftsrechtlich dazu verpflichtet, sich bei der Umsetzung dieser Richtlinien auf eine Auslegung derselben zu stützen, die es ihnen erlaubt, ein angemessenes Gleichgewicht zwischen den verschiedenen durch die Gemeinschaftsrechtsordnung geschützten Grundrechten sicherzustellen. Bei der Durchführung der Maßnahmen zur Umsetzung dieser Richtlinien haben die Behörden und Gerichte der Mitgliedstaaten nicht nur ihr nationales Recht im Einklang mit diesen Richtlinien auszulegen, sondern auch darauf zu achten, dass sie sich nicht auf eine Auslegung dieser Richtlinien stützen, die mit diesen Grundrechten oder den anderen allgemeinen Grundsätzen des Gemeinschaftsrechts, wie etwa dem Grundsatz der Verhältnismäßigkeit, kollidiert[666].

6.5.3. Richtervorbehalt aufgrund gemeinschaftsrechtlicher Vorgaben?

Jedenfalls bis zur Entscheidung des EuGH in der Rechtssache *LSG* gegen *Tele 2* war die Frage, ob eine gegen Access-Provider gerichtete Auskunftspflicht unter dem Vorbehalt einer richterlichen Genehmigung stehen sollte oder nicht, heftig umstritten[667]. Der Schlussantrag in der Rechtssache *Promusicae* ließ Zweifel daran aufkommen, dass eine Auskunftspflicht gegenüber einem Privaten ohne Prüfung durch ein unabhängiges Gericht dem Gemeinschaftsrecht entspricht[668]. Die Generalanwältin hob die Bindung der Gerichte an Grundrechte und Verfahrensgarantien hervor[669]. Überdies würden sie aufgrund ihrer Unabhängigkeit und Objektivität auch den

---

[666] EuGH 29.1.2008, C 275/06, Rz 71; 19.2.2009, C 557/07, MR 2009, 40, Rz 25ff.

[667] Vgl etwa: *Barbist*, Auskunftspflicht: Streit Provider vs Musikindustrie Reloaded Das EuGH-Urteil in Sachen Promusicae, MR 2007, 415 (417); *Daum*, EuGH zur Auskunftspflicht von Internetserviceprovidern, ecolex 2008, 200; *Haidinger/Schachter*, Urheberrechtlicher Auskunftsanspruch im Spannungsverhältnis zum Datenschutz – Anlassfälle Promusicae und MediaSentry, jusIT 2008, 59 (61); *Neubauer*, Zur Haftung und Auskunftsverpflichtung von Providern Aktuelles zu Unterlassungs- und Auskunftspflichten in Österreich mit einem Vergleich zur aktuellen Rechtslage in Deutschland im Zivil- und Strafrecht, MR-Int 2008, 25 (28).

[668] Generalanwältin *Kokott*, Schlussantrag vom 18.7.2007 zu Rechtssache C 275/06 vor dem EuGH, Rz 113ff.

[669] Vgl auch die Aussendung des Bundeskanzleramtes vom 2.8.2009 zur Entscheidung *Promusicae,* 5ff, abrufbar unter http://www.bka.gv.at/DocView.axd?CobId=36104 (Stand: April 2010).

beschuldigten Nutzer entlastende Umstände erheben. Diese Auffassung ließ den OGH daran zweifeln, dass § 87b Abs 3 UrhG dem Gemeinschaftsrecht entspricht. Die Bestimmung enthält dem Wortlaut nach eine direkte Auskunftspflicht zugunsten geschädigter Rechtsinhaber. Deshalb wendete sich der OGH noch vor Entscheidung des EuGH in der Rechtssache *Promusicae* an letzteren und stellte diesem die Vorlagefrage, ob Art 8 Abs 3 der Enforcement-Richtlinie unter Bedachtnahme auf die Art 6 und 15 der Telekom-Datenschutzrichtlinie dahin auszulegen sei, dass er die Weitergabe personenbezogener Verkehrsdaten an private Dritte zum Zweck der zivilgerichtlichen Verfolgung bescheinigter Verletzungen urheberrechtlicher Ausschlussrechte (Verwertungs- und Werknutzungsrechte) nicht zulasse[670]. Der EuGH entschied wie bereits oben erläutert, dass das Gemeinschaftsrecht kein Verbot enthalte, eine Auskunftspflicht betreffend personenbezogene Verkehrsdaten ohne gerichtliche Zwischenprüfung vorzusehen.

Es bleiben jedoch nach wie vor Zweifel an der Gemeinschaftsrechtskonformität des § 87b Abs 3 UrhG bestehen. Nach der Vorabentscheidung in der Rechtssache *Promusicae* waren bezüglich der Frage des Richtervorbehalts in der Literatur verschiedene Meinungen vorzufinden, die sich allesamt auf die Entscheidung *Promusicae* beriefen[671]. In dieser Hinsicht brachte auch die Entscheidung *LSG* gegen *Tele 2* nichts substanziell Neues[672]. So wird etwa unter Verweis auf die Hervorhebung des Verhältnismäßigkeitsgrundsatzes durch den EuGH vertreten, dass die europäischen datenschutzrechtlichen Bestimmungen (Rl 95/46/EG und Rl 200258/EG) die Weitergabe personengebundener Verkehrsdaten nur an zuständige Behörden erlauben und die unmittelbare Weitergabe an Urheber verbieten[673]. Auf der anderen Seite wird aber aus *LSG* gegen *Tele 2* auch abgeleitet, dass der EuGH § 87b Abs 3 UrhG für gemeinschaftsrechtlich unbedenklich hielt[674]. Nach letzterer Auffassung ist die Frage nach der gemeinschaftsrechtlichen Notwendigkeit eines Richtervorbehaltes eindeutig dahin gehend geklärt, dass aus dem Gemeinschaftsrecht

---

[670] OGH 13.11.2007, 4 Ob 141/07z.

[671] vgl *Neubauer*, Zur Haftung und Auskunftsverpflichtung von Providern – Aktuelles zu Unterlassungs- und Auskunftspflichten in Österreich mit einem Vergleich zur aktuellen Rechtslage in Deutschland im Zivil- und Strafrecht, MR-Int 2008, 25 (28) mwN.

[672] *Büchele,* ÖBl 2010/18 (91); *ders,* Glosse zu EuGH 19.2.2009 Rs C-557/07, *LSG/Tele2,* ÖBl-LS 2009/233 (171); *Zerdick,* Europäisches Datenschutzrecht – neuere Rechtsprechung des EuGH, RDV 2009, 56 (59); vgl auch die Aussendung des BKA zum B des EuGH: BKA 2.8.2009, BKA-VA.C-557/07/0002-V/7/2009, abrufbar unter http://www.austria.gv.at/DocView.axd?CobId=36104 (Stand April 2010).

[673] So *Zerdick,* Europäisches Datenschutzrecht – neuere Rechtsprechung des EuGH, RDV 2009, 56 (59).

[674] *Daum,* Auskunftsanspruch gegenüber Providern – Verpflichtung zur Weitergabe von Nutzerdaten an Dritte, MR 2009, 40 (43).

kein Richtervorbehalt abzuleiten ist. Dass jedoch auch nach der Entscheidung *LSG gegen Tele 2* noch immer Zweifel und Gegenauffassungen bestehen, ist unerfreulich und mE durch die etwas unpräzise Wortwahl des OGH und des EuGH zu erklären. Zwar lässt sich die Absicht des OGH, in dieser Frage endlich Klarheit zu schaffen, aus der Begründung seiner Vorlageentscheidung recht klar herauslesen. Dort meint er: *„Die zweite Vorlagefrage ist daher darauf gerichtet, ob die gemeinschaftsrechtlichen Bestimmungen über den Datenschutz eine Verarbeitung (Speicherung) und direkte Weitergabe personenbezogener Verkehrsdaten über die Benutzung des Internets an die Inhaber geistigen Eigentums zum Zweck der zivilgerichtlichen Verfolgung ihrer Ausschlussrechte (Verwertungs- und Werknutzungsrechte) hindern und Art 8 Abs 3 der Richtlinie 2004/48/EG sowie die in Umsetzung dieser Richtlinie ergangene nationale Bestimmung dementsprechend einschränkend auszulegen sind*[675]." Vor allem aus dem in der Begründung der Entscheidung verwendeten Wort „direkt" kann wohl gefolgert werden, dass der OGH auch wissen wollte, ob das EG-Recht „direkte" Auskunftspflichten (ohne Zwischenschaltung eines Gerichts) zulasse. In der Frage, die dem EuGH letztlich zur Vorabentscheidung vorgelegt wurde, fehlt jedoch das Wort „direkt". Deshalb konnte sich die Antwort des EuGH darauf beschränken, dass das Gemeinschaftsrecht Verpflichtungen zur Weitergabe personenbezogener Daten an private Dritte nicht verbiete. Offen konnte damit jedoch bleiben, ob das Gemeinschaftsrecht es gebiete, dass „private Dritte" ihren Auskunftsanspruch nur vor einem Gericht durchsetzen können, oder eine direkte Beauskunftung durch den Access-Provider möglich sei[676]. So kommt es, dass auch nach der Entscheidung *LSG gegen Tele 2* nach wie vor unterschiedliche Meinungen kursieren. Der OGH sieht es anders und hält die Frage durch die Entscheidung des EuGH für eindeutig geklärt: "*Auf das Gemeinschaftsrecht kann die Notwendigkeit eines Richtervorbehalts seit der im vorliegenden Verfahren ergangenen Vorabentscheidung C-557/07 (LSG/Tele2) allerdings nicht mehr gestützt werden*[677]*.*"

ME können jedoch aus der bloßen Kenntnis des EuGH von § 87b Abs 3 UrhG und dem Umstand, dass er diesen nicht explizit als gegen das Gemeinschaftsrecht verstoßend erachtete, bezüglich der Frage des Richtervorbehaltes keine eindeutigen Schlüsse gezogen werden. Im Vorabentscheidungsverfahren (Art 234 EGV bzw nunmehr Art 267 AEUV) hat der EuGH genau abgegrenzte Kompetenzen. Er muss nicht wie in einem Vertragsverletzungsverfahren über die Konformität innerstaatlichen Rechts mit

---

[675] OGH 13.11.2007, 4Ob141/07z; Hervorhebung durch den Verfasser.

[676] Vgl auch *Neubauer*, Zur Haftung und Auskunftsverpflichtung von Providern Aktuelles zu Unterlassungs- und Auskunftspflichten in Österreich mit einem Vergleich zur aktuellen Rechtslage in Deutschland im Zivil- und Strafrecht, MR-Int 2008, 25 (29), der es bereits vor der Entscheidung des EuGH in der Sache LSG gegen Tele2 für fraglich hielt, ob der EuGH zur Frage des Richtervorbehalts überhaupt Stellung nehmen wird.

[677] OGH 14.07.2009 4 Ob 41/09x, MR 2009, 251.

dem EU/EG-Recht entscheiden, sondern er hat lediglich eine abstrakte Auslegung der unions- bzw gemeinschaftsrechtlichen Norm vorzunehmen[678]. Die Beurteilung der Gemeinschaftsrechtskonformität der mitgliedstaatlichen Norm obliegt dem nationalen Richter[679].

Eine ausdrückliche Klarstellung des EuGH, dass sich aus dem Verhältnismäßigkeitsgrundsatz ergibt, dass Auskunftsansprüche nur gerichtlich durchgesetzt werden können, hätte den angeführten Meinungsstreit einem Ende zuführen können. Es wäre ein leichtes gewesen, sich den in diese Richtung gehenden Ausführungen der Generalanwältin anzuschließen. Eine zwingende gerichtliche Prüfung brächte vor allem den Vorteil mit sich, dass Gerichte wohl besser in der Lage sind, die zur Untermauerung des Auskunftsanspruchs vorgelegten Nachweise zu würdigen. Überdies stellen sich im Zusammenhang mit Auskunftsbegehren von verletzten Rechtsinhabern komplexe Rechtsfragen, deren Lösung nicht unbedingt einem in der Zwickmühle stehenden Access-Provider überlassen werden sollte.[680].

Man könnte die Entscheidung des EuGH jedoch auch so wie der OGH in dem Sinne verstehen, dass für ersteren ein direkter Auskunftsanspruch aus gemeinschaftsrechtlicher Sicht in Ordnung geht. Schließlich erachtet der EuGH die Weitergabe personenbezogener Daten an „private" Dritte als zulässig. Damit könnte gemeint sein, dass „private" Dritte unmittelbar an die Provider herantreten dürfen und keine gerichtliche Kontrolle nötig ist. Unbeschadet der oben angeführten Argumente kann dem Umstand, dass der EuGH § 87b Abs 3 UrhG nicht ausdrücklich als gemeinschaftsrechtswidrig qualifizierte, wohl zumindest eine gewisse Indizwirkung nicht abgesprochen werden. Der EuGH, der das Anlassverfahren *LSG gegen Tele 2* und den Regelungsgehalt des § 87b Abs 3 UrhG kannte, hätte beispielsweise auch in abstracto klarstellen können, dass er einen Richtervorbehalt für notwendig erachtet. Dass er dies unterließ, kann man – auch wenn dieses Verständnis wie gezeigt freilich nicht zwingend ist – gemeinsam mit dem OGH als grünes Licht für unmittelbare Auskunftsansprüche verstehen.

Nach aktueller mE unzutreffender Rechtsprechung des VwGH[681] unterliegen Verkehrsdaten dem Fernmeldegeheimnis. Gegenstand der Auskunft nach

---

678 EuGH 15.7. 1964, Rechtssache 6/64 (*Flaminio Costa v E.N.E.L*), Rz 3.

679 *Fischer/Köck/Karollus,* Europarecht[4] (2002) Rz 1433.

680 *Raschhofer/Steinhofer,* Zwischen Urheber und Kunde: Provider in der Zwickmühle, Die Presse vom 4.10.1009, abrufbar unter http://diepresse.com/home/techscience/internet/512779/index.do?from=simarchiv (Stand April 2010).

681 VwGH 27.5.2009, 2007/05/0280.

§ 87b Abs 3 UrhG sind regelmäßig nur Stammdaten, die zweifellos nicht dem Fernmeldegeheimnis unterliegen. Aus dem Zusammenhang zu den für die Erfüllung des Auskunftsbegehrens verarbeiteten Verkehrsdaten ergibt sich jedoch, dass das Schutzniveau von Art 10a StGG zu beachten und eine derartige Auskunftspflicht daher unter Richtervorbehalt zu stellen ist (vgl dazu auch schon oben Kapitel 4.4.6).

6.5.4. Die Auskunft über Stammdaten unter Verarbeitung von Verkehrsdaten

Der OGH betonte im Fall *LSG gegen Tele 2*, dass ein Auskunftsanspruch, sofern er die Verarbeitung von Verkehrsdaten, voraussetzt, daran scheitern muss, dass nach Art 6 EK-Datenschutzrichtlinie bzw § 99 TKG 2003 Verkehrsdaten unverzüglich nach Verbindungsbeendigung zu löschen sind (siehe dazu schon oben Kapitel 5.5.8). Das gilt auch dann, wenn die Verarbeitung, dh Speicherung unzulässigerweise dennoch erfolgen sollte. Davon sind aufgrund ihrer Qualifikation als Verkehrsdaten[682] zumindest dynamische IP-Adressen betroffen[683]. In Bezug auf statische IP-Adressen hat der Access-Provider bezüglich der Frage, ob er diese speichern soll oder nicht, keine Wahl, da er seinem Kunden die Verwendung einer ganz bestimmten Adresse vertraglich zusicherte. Will er dieser vertraglichen Verpflichtung nachkommen, so muss er speichern, wem er welche IP-Adresse vertraglich zusicherte. Dennoch stünde auch die Verarbeitung einer statischen IP-Adresse für die Auskunftszwecke des § 87b Abs 3 UrhG mit dem ursprünglichen Speicherungszweck nicht im Einklang und wäre daher bei konsequenter Auslegung der am Zweckbindungsgrundsatz orientierten Entscheidung des OGH unzulässig.

In der Praxis wird die Bestimmung des § 87b Abs 3 UrhG den Rechteinhabern zur Verfolgung von über das Internet begangenen Rechtsverletzungen nicht viel bringen. Dieses Ergebnis wird vom OGH ausdrücklich in Kauf genommen.

6.5.5. Vertragliche Pflicht zur Ergreifung von Rechtsschutzmaßnahmen?

Es stehen abgesehen von der Weigerung, die eine gerichtliche Prüfung des Auskunftsbegehrens nach sich zieht, keine Möglichkeiten zur Verfügung, mit denen die

---

682 *Einzinger/Schubert/Schwabl/Wessely/Zykan*, Wer ist 217.204.27.214?, MR 2005, 113 (116); *Wiebe*, Auskunftsverpflichtung der Access-Provider, Beilage zu MR 2005/4, 13 ff.

683 Ebenso *Wiebe,* Auskunftsverpflichtung der Access-Provider – Verpflichtung zur Drittauskunft bei Urheberrechtsverletzungen von Kunden, die an illegalem File-Sharing teilnehmen, MR 2005, H 4 Beilage, 12

Erfüllung eines Auskunftsbegehren verhindert werden könnte. Es kann daher auch keine vertragliche Pflicht zur Ergreifung derartiger Rechtsbehelfe bestehen.

6.5.6. Vertragliche Pflicht zur exakten Prüfung des Auskunftsbegehrens

Der Wortlaut des § 87b Abs 3 UrhG unterscheidet sich von vielen anderen Auskunftsbestimmungen insbesondere dadurch, dass eine Auskunft nur auf ein ausreichend begründetes Begehren zu erteilen ist. Erweist sich die Begründung als mangelhaft, muss bzw darf daher auch keine Auskunft erteilt werden. Daraus ergibt sich die durch ergänzende Vertragsauslegung gewonnene Pflicht des Access-Providers, die Erfüllung des Auskunftsbegehrens jedenfalls so lange zu verweigern, so lange dieses nicht ausreichend begründet wurde. Was als ausreichend zu betrachten ist, hängt von den Umständen im Einzelfall ab. Wie oben bereits ausgeführt, darf die Messlatte keinesfalls so hoch angelegt werden, dass nur im Falle des Nachweises der konkreten Verletzung eine Auskunftspflicht gegeben ist. Dies würde eindeutig dem Telos der Bestimmung widersprechen. Allerdings muss sich aus der Begründung bei objektiver Würdigung der Umstände ein konkreter Verdacht ergeben. Weiters muss das Auskunftsbegehren mE Angaben darüber enthalten, inwiefern die begehrte Auskunft zur Ausforschung des Verletzers führen kann. Dem Begehren sind mE geeignete Bescheinigungsmittel beizulegen. In Betracht käme etwa ein Dokument eines Host-Providers, in welchem dieser bestätigt, dass eine Verletzung von einer Netzwerkschnittstelle mit einer bestimmten IP-Adresse begangen wurde. Aus den vertraglichen Verpflichtungen des Access-Providers seinem Kunden gegenüber ergibt sich, dass er das an ihn heran getragene Auskunftsbegehren zunächst exakt zu prüfen hat. Nur so verstanden macht die Pflicht des Verletzten sein Auskunftsbegehren schriftlich einzubringen und ausreichend zu begründen Sinn. Sollte sich das Auskunftsbegehren als mangelhaft erweisen, hat der Access-Provider auf dessen vollständige Begründung hinzuwirken bzw dessen Erfüllung zu verweigern.

6.5.7. Pflicht zur Verweigerung des Auskunftsbegehrens

Den Access-Provider trifft die Pflicht, die Erfüllung des Auskunftsbegehrens zu verweigern, wenn dies nur unter Verarbeitung von Verkehrsdaten möglich wäre, die nach der Löschungsverpflichtung des § 99 Abs 1 TKG 2003 nicht mehr vorhanden sein dürften. Dies hat der OGH im Fall *LSG gegen Tele 2* ausdrücklich klar gestellt und damit begründet, dass die Zulässigkeit der Weitergabe von Stammdaten nicht davon abhängen kann, ob das dafür erforderliche rechtswidrige Verarbeiten von Verkehrsdaten im Zeitpunkt der Anspruchserhebung oder der darüber ergehenden Entscheidung schon

erfolgt war oder nicht. Da dieses Verhalten schon nach dem positiven Recht geboten ist, bestehen auch keine Schwierigkeiten eine dahin gehende vertragliche Schutzpflicht zu konstruieren.

6.6. § 14a UWG

6.6.1. Der Wortlaut

„(1) *Unternehmer, die Postdienste oder Telekommunikationsdienste anbieten und die im geschäftlichen Verkehr die von ihren Nutzern angegebenen Namen und Anschriften für die Diensteerbringung verarbeiten, haben diese Daten binnen angemessener Frist auf schriftliches Verlangen (Abs. 2) einer der gemäß § 14 Abs. 1 zweiter und dritter Satz klagebefugten Einrichtungen oder des Schutzverbandes gegen unlauteren Wettbewerb bei deren begründetem Verdacht einer unlauteren Geschäftspraktik dieses Nutzers gemäß §§ 1, 1a oder § 2 schriftlich bekanntzugeben. Sie sind nur insoweit zur Auskunft verpflichtet, als diese Daten ohne weitere Nachforschungen verfügbar sind und ein inländisches Postfach oder eine nicht in einem allgemein zugänglichen Teilnehmerverzeichnis eingetragene inländische Rufnummer betreffen.*

(2) Der Auskunftswerber hat bei sonstigem Verlust seines Auskunftsanspruches in seinem Verlangen die Gründe für seinen Verdacht anzugeben und darzulegen, dass er die in Abs. 1 genannten Daten für die Rechtsverfolgung unlauterer Geschäftspraktiken nach §§ 1, 1a oder § 2 benötigt, ausschließlich dafür verwendet und nicht durch allgemein zugängliche Informationsquellen beschaffen kann.

(3) Der Auskunftswerber, ausgenommen die Bundeswettbewerbsbehörde, hat dem zur Auskunft verpflichteten Diensteanbieter die angemessenen Kosten der Auskunftserteilung zu ersetzen. Auch hat er ihn für alle aus der Auskunftserteilung allenfalls erwachsenden Ansprüche seiner Nutzer schadlos zu halten. Eine Kopie seines schriftlichen Verlangens hat er für die Dauer von drei Jahren aufzubewahren."

6.6.2. Hintergrund

Die Bestimmung wurde auf Drängen des BMSK im Zuge der UWG-Novelle 2007[684] in das UWG eingefügt[685]. Zweck der Bestimmung ist es, die

[684] BGBl I 79/2007.

Unterlassungsansprüche der nach § 14 Abs 1 UWG klagebefugten Verbände mit einem Instrument zu flankieren, das die Rechtsdurchsetzung erleichtern soll. In der Praxis scheiterten die Unterlassungsansprüche früher oft daran, dass keine ladungsfähige Anschrift wettbewerbswidrig agierender Mitbewerber bekannt war, da sich diese häufig hinter nicht angemeldeten Handy- oder Geheimtelefonnummern bzw Postfächern versteckten[686]. Bereits im Jahr 2004 gewährte der OGH jedoch einen Auskunftsanspruch gegen einen Access-Provider analog zu § 18 Abs 4 ECG[687]. Der im ECG normierte Auskunftsanspruch betrifft ausschließlich Host-Provider iSd § 16 ECG[688]. Ein Betreiber von Telekommunikationsdiensten ist jedoch nach Ansicht des OGH einem Diensteanbieter nach § 16 ECG insoweit vergleichbar, als beide nur die technischen Vorraussetzungen für das wettbewerbswidrige Verhalten schaffen, jedoch keinen inhaltlichen Einfluss ausüben. Das Fehlen einer § 18 Abs 4 ECG entsprechenden Bestimmung spreche für eine Gesetzeslücke, die es durch Analogie zu schließen gelte. Daher habe ein Telekommunikationsunternehmen, das ein öffentliches Kommunikationsnetz betreibt, den Namen und die Adresse eines Nutzers, der auf Grund einer Vereinbarung über dieses Netz Mehrwertdienste anbietet, 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. Die Entscheidung des OGH wurde von *Zankl*[689] und *Hasberger/Schönhart*[690] mit dem zutreffenden Argument kritisiert, dass § 18 Abs 4 die Auskunftspflicht von Host-Providern regle, Telekommunikationsunternehmen aber gerade keine Host- sondern vielmehr Access-Provider sind[691]. Außerdem scheidet das ECG nach Ansicht *Zankls* deshalb als Analogiebasis aus, weil das ECG gerade keine

---

685 *Majchrzak,* Der Auskunftsanspruch nach § 14a UWG, ÖBl 2008, 180 (180).

686 AB 236 BlgNR XXIII. GP, 2.

687 OGH 16.3.2004 4 Ob 7/04i, ecolex 2004, 854 = wbl 2004, 390 = RdW 2004, 475 = MR 2004, 221 = SZ 2004/33.

688 *Zankl,* E-Commerce-Gesetz (2002) § 18 Rz 283.

689 *Zankl,* Auskunftspflicht für Mehrwertdienste? ecolex 2004, 853 (854).

690 *Hasberger/Schönhart,* Die Haftung von Telekom-Unternehmen für fremdes Fehlverhalten, MR 2004, 297 (300).

691 AM mit dem wenig überzeugenden Argument, dass es bei Mehrwertnummern nicht zwischen Host- und Access-Providern unterschieden werden kann und deshalb gegen Access-Provider ein Auskunftsanspruch bestehen müsse *Plasser,* Lauterkeitsrechtlicher Auskunftsanspruch auch für Mitbewerber nach der UWG-Nov 2007, ÖBl 2008, 183 (184).

Telekommunikationsdienstleistungen regle und die reinen Sprach-Telefonierdienste nicht dem ECG unterliegen[692].

6.6.3. Verpflichtete und Berechtigte

Zur Auskunft verpflichtet sind „Unternehmer, die Postdienste oder Telekommunikationsdienste anbieten". Betroffen sind nicht nur die Post AG, sondern auch alle sonstigen privaten Dienstleister, die Postdienste erbringen. Der Begriff der Unternehmer, die Telekommunikationsdienste erbringen, deckt sich mit dem hier verwendeten Begriff des Access-Providers.

Zur Auskunft berechtigt sind ausschließlich die in § 14 Abs 1 taxativ aufgezählten klagebefugten Einrichtungen[693]. Fraglich ist, ob die bereits erwähnte Entscheidung 4 Ob 7/04i weiterhin maßgeblich ist und sich auch Mitbewerber gestützt auf diese Rechtsprechung mit Auskunftsbegehren an Access-Provider wenden können. Dafür tritt etwa *Plasser* mit dem wenig überzeugenden Argument ein, der Gesetzgeber habe bei der Einfügung von § 14a UWG die Judikatur des OGH übersehen und daher dem Auskunftsanspruch keine bewusste Absage erteilt. Er stützt sich dabei auf eine eher spekulative Auslegung des Berichts des Ausschusses für Wirtschaft und Industrie[694]. Wie jedoch *Majchrzak* überzeugend darzulegen vermag, entschied sich der Gesetzgeber für eine Einschränkung des Auskunftsanspruches auf die wenigen Verbände, um allfälligem Missbrauch und einer übermäßigen Belastung der Auskunftsverpflichteten vorzubeugen[695]. Da die Entscheidung des Gesetzgebers somit bewusst erfolgte, kann von einer Lücke – diese ist grundlegende Vorraussetzung jeglicher analogen Anwendung des § 18 Abs 4 ECG – keine Rede mehr sein. Selbst wenn der Gesetzgeber die Entscheidung 4 Ob 7/04i zum Zeitpunkt der Einfügung von § 14a UWG wie von *Plasser* unterstellt nicht gekannt haben sollte, so erscheint es dennoch äußerst unwahrscheinlich, dass er bei einer Novellierung des UWG die Interessen von Mitbewerbern schlichtweg übersah. Richtigerweise ist daher davon auszugehen, dass durch die Einfügung von § 14a UWG

---

692 RV 817 BlgNR XXI. GP, 18; AA wiederum *Plasser,* Lauterkeitsrechtlicher Auskunftsanspruch auch für Mitbewerber nach der UWG-Nov 2007, ÖBl 2008, 183 (185).

693 Das sind die Bundeskammer für Arbeiter und Angestellte, die Wirtschaftskammer Österreich, die Präsidentenkonferenz der Landwirtschaftskammern Österreichs, der Österreichische Gewerkschaftsbund, die Bundeswettbewerbsbehörde und der Verein für Konsumenteninformation.

694 *Plasser,* Lauterkeitsrechtlicher Auskunftsanspruch auch für Mitbewerber nach der UWG-Nov 2007? ÖBl 2008, 183 (185); ihm zustimmend *Kodek/Leupold,* in *Wiebe/G. Kodek,* UWG, § 14a Rz 9.

695 *Majchrzak,* Der Auskunftsanspruch nach § 14a UWG, ÖBl 2008, 180 (180) mwN; ebenso *Schuhmacher,* Die UWG-Novelle 2007, wbl 2007, 557 (566)

der analogen Anwendung von § 18 Abs 4 ECG iSd der Rechtsprechung des OGH der Boden entzogen wurde.

6.6.4. Begründung des Verdachts

Voraussetzung für den Auskunftsanspruch ist gem § 14a Abs 1 iVm 2, dass der Auskunftswerber gegenüber dem Access-Provider seine Verdachtsgründe schriftlich ausreichend substantiiert. Er muss weiters darlegen, dass er den Namen und die Anschrift für die Rechtsverfolgung unlauterer Geschäftspraktiken nach §§ 1, 1a oder § 2 benötigt, ausschließlich dafür verwendet und nicht durch allgemein zugängliche Informationsquellen beschaffen kann. So wären etwa 0800-Rufnummern oder geografische Rufnummern nicht aus dem von der RTR geführten Verzeichnis ersichtlich[696]. Dem Schriftlichkeitsgebot nach dieser Bestimmung entspricht auch die Übermittlung des Auskunftsbegehrens per Fax, nicht aber die Übermittlung im Wege der elektronischen Post[697]. Dem Wortlaut nach ist Auskunft nur beim Verdacht „unlauterer Geschäftspraktiken" zu erteilen. Diese liegen § 1 Abs 4 Z 2 UWG nur dann vor, wenn die fragliche Handlung unmittelbar mit der Absatzförderung, dem Verkauf oder der Lieferung eines Produkts zusammenhängt. In der Lit wird jedoch vertreten, dass diese Einschränkung nur versehentlich erfolgte und daher auch beim Verdacht auf sonstige unlautere Handlungen iSd § 1 Abs 1 Z 1 Auskunft zu erteilen ist[698].

Ohne die schriftliche Begründung besteht kein Auskunftsanspruch. Nach dem Wortlaut der Bestimmung führt die mangelhafte Begründung des Verdachts zum Verlust des Auskunftsanspruchs. Fraglich ist, ob „Verlust" im Seine eines endgültigen Wegfalls zu verstehen ist oder ob der Verlust des Auskunftsanspruches nur so lange währen soll, so lange die Begründung mangelhaft ist. Dem Zweck, dass nur ausreichend begründeten Auskunftsbegehren nachgekommen werden soll, kann jedenfalls auch Genüge getan werden, indem man „Verlust" im Sinne eines für die Dauer der Mangelhaftigkeit bestehenden Wegfalls des Anspruchs versteht.

Den Auskunftswerber trifft zu Dokumentationszwecken die Pflicht, eine Kopie seines Auskunftsbegehrens über drei Jahre zu verwahren (§ 14a Abs 3 UWG)[699].

---

[696] AB 236 BlgNR XXIII. GP, 2.

[697] AB 236 BlgNR XXIII. GP, 3.

[698] *Majchrzak,* Der Auskunftsanspruch nach § 14a UWG, ÖBl 2008, 180 (180).

[699] AB 236 BlgNR XXIII. GP, 3.

6.6.5. Auskunftsinhalt

Zu beauskunften sind Name und Anschrift jenes Nutzers, der im Verdacht steht, eine unlautere Geschäftspraktik iSd § 1, 1a bzw 2 UWG begangen zu haben. Unter Anschrift ist – soweit möglich – die Zustelladresse iSd § 2 Z 4 bis 6 Zustellgesetz zu verstehen[700]. Der Gesetzgeber hatte dabei Auskünfte zu dem Auskunftswerber bekannten, jedoch nicht in einem allgemein zugänglichen Teilnehmerverzeichnis eingetragenen Rufnummern im Auge. Nicht beauskunftet werden muss daher etwa, wer hinter einer bestimmten Domain steht[701]. Ebenso wenig müssen mE Auskünfte über die Identität von Personen erteilt werden, die hinter einer bestimmten IP-Adresse stehen. Dies ergibt sich schon aus dem Wortlaut der Bestimmung, wonach nur dann eine Auskunftsverpflichtung besteht, wenn „eine nicht in einem allgemein zugänglichen Teilnehmerverzeichnis eingetragene inländische Rufnummer" betroffen ist. Weiters müssen die Daten „ohne weitere Nachforschungen verfügbar" sein. Das Durchsuchen der logfiles wäre jedoch wohl als Nachforschung iSd Bestimmung zu verstehen. Überdies treffen die in 4 Ob 4/09x zu § 87b Abs 3 UrhG angestellten Überlegungen des OGH weitestgehend auch auf § 14a UWG zu. Somit lässt sich festhalten, dass § 14a UWG keine geeignete Rechtsgrundlage darstellt, um die Identität von Personen, denen bestimmte IP-Adressen zu geordnet wurden, zu ermitteln.

Die Auskunft ist binnen angemessener Frist zu erteilen. In der Literatur wird eine Frist von maximal zwei Wochen vorgeschlagen[702], was angesichts der Voraussetzung, dass die Auskunft ohne weitere Nachforschungen möglich sein muss, recht großzügig erscheint.

6.6.6. Kostenersatz und Schadloshaltung

Mit Ausnahme der Bundeswettbewerbsbehörde hat jeder Auskunftswerber dem Access-Provider die „angemessenen" Kosten der Auskunftserteilung zu ersetzen. Dabei ist mangels einschlägiger Rechtsprechung unklar, ob nur tatsächlich entstandene Kosten abgegolten werden müssen, oder generell ein Entgelt zustehen soll[703].

Der Auskunftswerber hat den Access-Provider für alle aus der Auskunftserteilung allenfalls erwachsenden Ansprüche seiner Nutzer schadlos zu halten.

---

[700] AB 236 BlgNR XXIII. GP, 3.

[701] Diesbezüglich bleibt weiterhin § 18 Abs 4 ECG maßgeblich, vgl *Majchrzak/Wiltschek,* Die UWG-Novelle 2007, ÖBl 2008, 4 (13), *Majchrzak*, Der Auskunftsanspruch nach § 14a UWG, ÖBl 2008, 180 (181).

[702] *Kodek/Leupold,* in *Wiebe/G. Kodek,* UWG (2009) § 14a Rz 17.

[703] *Kodek/Leupold,* in *Wiebe/G. Kodek,* UWG (2009) § 14a Rz 25.

Dies gilt nur, soweit der Auskunftsanspruch tatsächlich bestand und die Voraussetzungen des § 14a UWG eingehalten wurden[704]. Der Gesetzgeber geht daher davon aus, dass aus der Erfüllung des Auskunftsbegehrens Schadenersatzansprüche des Nutzers gegen seinen Access-Provider entstehen können. Dies bestätigt die in dieser Arbeit als wesentliches Ergebnis zu Tage geförderte These, dass den Access-Provider vertragliche Schutzpflichten im Hinblick auf die Privatsphäre seines Kunden treffen.

6.6.7. Vertragliche Pflicht zur Überprüfung zur Prüfung des Auskunftsbegehrens?

Nach dem eindeutigen Wortlaut der Materialien soll es keine Pflicht des Access-Providers geben, an ihn gerichtete Auskunftsbegehren inhaltlich oder rechtlich zu überprüfen[705]. Dies irritiert insofern, als der Gesetzgeber aber gleichzeitig davon ausgeht, dass dem Nutzer aus der Erteilung der Auskunft Schadenersatzansprüche gegen den Provider entstehen können. Diese Regelung macht jedoch nur dann einen Sinn, wenn man von bestimmten Pflichten des Access-Providers gegenüber seinem Kunden ausgeht, deren Verletzung diese Ansprüche nach sich zieht. Allerdings ist der Access-Provider nach Stimmen in der Lit wenigstens zur Kontrolle der formalen Voraussetzungen (Schriftlichkeit, Begründungsvollständigkeit) verpflichtet[706]. Unterlässt er die diesbezügliche Kontrolle, stellt dies die Verletzung einer vertraglichen Schutzpflicht dar, die haftungsbegründend ist. Für eine ergänzende Vertragsauslegung ist hier angesichts des eindeutigen Wortlauts der Materialien kein Raum. Es ist daher davon auszugehen, dass abgesehen von der Pflicht zur Kontrolle der Einhaltung der formalen Voraussetzungen keine weitergehende Prüfpflicht besteht.

6.6.8. Vertragliche Pflicht zur Verweigerung

Sollten die formalen Voraussetzungen nicht gegeben sein, besteht eine durch Vertragsergänzung entwickelte Schutzpflicht des Access-Providers, die Erfüllung des Auskunftsbegehrens zu verweigern. Erfüllt er trotz mangelnder formaler Voraussetzungen das Auskunftsbegehren, fehlt es der erfolgenden Datenübermittlung an einer legalen Grundlage, womit er nicht nur gegen Vertragspflichten, sondern auch gegen positives Recht verstößt (§ 8 Abs 1 Z 1 DSG 2000). Weiters wird er die Erfüllung wohl zumindest in jenen Fällen zu verweigern haben, in denen ihm die Missbrauchsabsicht des

---

[704] *Kodek/Leupold,* in *Wiebe/G. Kodek,* UWG (2009) § 14a Rz 27.

[705] AB 236 BlgNR XXIII. GP, 3.

[706] *Kodek/Leupold,* in *Wiebe/G. Kodek,* UWG (2009) § 14a Rz 22.

Auskunftswerbers ausnahmsweise bekannt ist. Da die mangelhafte Begründung des Auskunftsbegehrens wie oben gezeigt zu einem endgültigen Wegfall des Auskunftsanspruchs führt, hat der Access-Provider mE auch in jenen Fällen, in denen er mit Folgeauskunftsbegehren konfrontiert wird, deren Erfüllung zu verweigern.

6.6.9. Vertragliche Pflicht zur Ergreifung von Rechtsschutzmaßnahmen

Abgesehen von der oben erwähnten Möglichkeit, die Erfüllung des Auskunftsbegehrens zu verweigern, was wohl eine Leistungsklage des Auskunftswerbers nach sich ziehen wird[707], stehen dem Access-Provider keine Möglichkeiten bzw Rechtsbehelfe zur Verfügung, mit denen er die Erfüllung des Auskunftsbegehrens behindern könnte. Damit erübrigt sich auch die Frage nach einer allfälligen diesbezüglichen vertraglichen Schutzpflicht.

6.7. § 99 Abs 3 FinStrG

6.7.1. Der Wortlaut der Bestimmung

§ 99 Abs 3 FinStrG 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."

6.7.2. Hintergrund

Vor der Auslagerung der Fernmeldeangelegenheiten in die Telekom Austria AG und die Zulassung diverser anderer Betreiber öffentlicher Telekommunikationsdienste wurde § 120 FinStrG zur Auskunft über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses herangezogen. Diese Bestimmung sieht vor, dass die Finanzstrafbehörde erster Instanz zur Durchführung der Finanzstrafrechtspflege berechtigt ist, mit allen Dienststellen der Gebietskörperschaften einschließlich jener der

---

[707] *Kodek/Leupold,* in *Wiebe/G. Kodek,* UWG (2009) § 14a Rz 23.

Post- und Telegraphenverwaltung unmittelbares Einvernehmen durch Ersuchschreiben zu pflegen. Derartige Ersuchschreiben sind mit möglichster Beschleunigung zu beantworten oder es sind die entgegenstehenden Hindernisse sogleich bekanntzugeben. § 120 FinStrG durchbricht den in Art 20 Abs 3 B-VG geregelten Grundsatz der Amtsverschwiegenheit[708]. Die Post und Telekom Austria AG ist aufgrund § 22 Abs 2 PTSG[709] auch heute noch Adressatin des § 120 FinStrG[710]. Da aber auch von sonstigen Betreibern öffentlicher Kommunikationsdienste die nach § 99 Abs 3 FinStrG zu beauskunftenden Daten für die Zwecke der Strafverfolgung benötigt werden, musste durch Art IV Z 10 des Abgaben-Rechtsmittel-Reformgesetzes[711] eine für alle Betreiber geltende Auskunftsbestimmung eingefügt werden. Sie wurde nach den Materialien § 53 SPG (in seiner damaligen Fassung[712]) nachgebildet[713]. Die Verpflichtung der Access-Provider wird wegen dem öffentlichen Interesse an der Strafverfolgung und der exakten Eingrenzung der zu beauskunftenden Daten als mit den Vorgaben des VfGH zur Indienstnahme Privater[714] vereinbar angesehen[715].

6.7.3. Verpflichtete und Berechtigte

Zur Auskunft verpflichtet sind die „Betreiber öffentlicher Kommunikationsdienste", sohin Access-Provider im hier verstandenen Sinne. Nicht erfasst Diensteanbieter iSd § 3 Z 2 ECG, welche die angeführten Informationen auch gar nicht geben könnten.

---

[708] VwGH 24.9.2002, 2002/16/0133.

[709] Dieser bestimmt: *„Soweit in anderen Bundesgesetzen von der Post- und Telegraphenverwaltung die Rede ist, tritt die Post und Telekom Austria Aktiengesellschaft an deren Stelle*".

[710] VwGH 24.9.2002, 2002/16/0133.

[711] BGBl I 97/2002.

[712] Das BGBl I 97/2002, mit welchem die Auskunftsbestimmung des § 99 Abs 3 FinStrG eingefügt wurde, wurde am 25.6.2002 ausgegeben. Zu diesem Zeitpunkt hatte § 53 Abs 3a SPG folgende Fassung: *„Die Sicherheitsbehörden sind berechtigt, von den Betreibern öffentlicher Telekommunikationsdienste Auskunft über Namen, Anschrift und Teilnehmernummer eines bestimmten Anschlusses zu verlangen, wenn sie diese Daten als wesentliche Voraussetzung für die Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben benötigen. Die Bezeichnung dieses Anschlusses kann für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder die Abwehr gefährlicher Angriffe auch durch Bezugnahme auf ein von diesem Anschluß geführtes Gespräch durch Bezeichnung des Zeitpunktes und der passiven Teilnehmernummer erfolgen. Die ersuchte Stelle ist verpflichtet, die Auskunft unverzüglich und kostenlos zu erteilen.*"

[713] AB 1128 BlgNR XXI. GP, 21.

[714] VfGH 27.2.2003, G 37/02 ua.

[715] *Fellner,* Kommentar zum Finanzstrafgesetz (6. ErgLf 2006) § 99 Rz 12.

Auskunft darf nach dem klaren Wortlaut jede Finanzstrafbehörde für Zwecke des Strafverfahrens verlangen. Das FinStrG unterscheidet zwischen Gerichten, die in den Fällen des § 53 Abs 1 bis 4 FinStrG zuständig sind und den Finanzstrafbehörden. Die im konkreten Fall zuständige Finanzstrafbehörde ergibt sich aus § 58 FinStrG. Aus dem Umstand, dass § 99 Abs 3 lediglich von Finanzstrafbehörden spricht, lässt sich somit ohne Zweifel schließen, dass nur die Finanzstrafbehörden, nicht jedoch die Gerichte zur Auskunft berechtigt sein sollen. Allerdings werden gem § 196 Abs 1 FinStrG auch bei der Aufklärung und Verfolgung gerichtlich strafbarer Finanzvergehen die Finanzstrafbehörden im Dienste der Strafrechtspflege (Art 10 Abs. 1 Z 6 B-VG) tätig. Die in der Strafprozessordnung der Kriminalpolizei zukommenden Aufgaben und Befugnisse haben bei gerichtlich strafbaren Finanzvergehen an Stelle der Kriminalpolizei die Finanzstrafbehörden und ihre Organe wahrzunehmen[716]. Gem § 196 Abs 4 FinStrG stehen den Finanzstrafbehörden auch im Ermittlungsverfahren wegen gerichtlich strafbarer Finanzvergehen der Finanzstrafbehörde die in den § 99 Abs 3 genannten Befugnisse zu.

6.7.4. Voraussetzung

Die einzige Voraussetzung für ein Auskunftsbegehren gem § 99 Abs 3 FinStrG ist, dass die beauskunfteten Daten den Zwecken eines Finanzstrafverfahrens dienen müssen. Diese finale Definition ist weit gefasst und enthält keine Einschränkung auf die Daten eines Beschuldigten. So erlaubt der Wortlaut etwa auch die Beauskunftung von Namen oder Anschriften potenzieller Zeugen, da auch deren Ausforschung den Zwecken des Strafverfahrens dient. Nach dem Wortlaut muss die begehrte Auskunft zur Erreichung des angestrebten Zwecks nicht unerlässlich sein, es reicht aus, wenn sie diesem dient. Allerdings wurde § 99 Abs 3 FinStrG wie erwähnt § 53 Abs 3a SPG in seiner damaligen Fassung nachgebildet. Dieser verlangte, dass die Sicherheitsbehörde die begehrten Daten als wesentliche Voraussetzung für die Erfüllung der ihnen nach dem SPG zukommenden Aufgaben benötigt. Daher wird diese Einschränkung wohl auch für § 99 Abs 3 FinStrG gelten.

6.7.5. Auskunftsinhalt

Da § 99 Abs 3 FinStrG an § 53 Abs 3a SPG idF BGBl I 85/2000 orientiert ist, sind bezüglich des Auskunftsinhalts auch die dazu geltenden Erwägungen zu beachten. § 53 Abs 3a SPG sah damals (so wie § 99 Abs 3 FinStrG heute) lediglich einen

---

[716] *Tannert*, in *Tannert* (Hrsg), Finanzstrafgesetz (34. ErgLf. 2009) § 196 Anm 1.

Anspruch auf Auskunft über Namen, Anschrift und Teilnehmernummer vor. Die damals zu beauskunftenden Daten entsprechen damit im Wesentlichen den nach § 53 Abs 3a Z 1 SPG in der heutigen Fassung zu beauskunftenden Daten. Daher ist an dieser Stelle nur auf die zu dieser Bestimmung obigen Ausführungen zu verweisen (siehe Kapitel 6.1.2.2).

Aus der Entwicklungsgeschichte des § 53 Abs 3a SPG folgt, dass von § 99 Abs 3 FinStrG keinesfalls auch die Auskunft über IP-Adressen bzw über die Identität hinter IP-Adressen stehender Personen erfasst sein kann[717]. Da § 53 Abs 3a SPG in seiner alten Fassung hierfür keine geeignete Rechtsgrundlage bildete[718], mussten durch BGBl I 114/2007 die heutigen Ziffern 2 und 3 eingefügt werden. Die Auskunftsbestimmung im FinStrG, die sich an § 53 Abs 3a SPG in seiner alten Fassung orientiert, wurde hingegen nicht novelliert und gibt daher nach wie vor keine geeignete Rechtsgrundlage für Auskünfte im Zusammenhang mit IP-Adressen ab. Die Auskunftspflicht gem § 99 Abs 3 FinStrG betrifft damit genau wie § 53 Abs 3a Z 1 SPG ausschließlich den Bereich der klassischen Sprachtelefonie.

Aus der Vorbildwirkung des § 53 Abs 3a SPG für § 99 Abs 3 FinStrG kann weiters gefolgert werden, dass letztere Bestimmung es nicht erlaubt, dass der fragliche Anschluss auch durch Bezugnahme auf ein von diesem Anschluss geführtes Gespräch durch Bezeichnung des Zeitpunktes und der passiven Teilnehmernummer (kleine Rufdatenrückerfassung) bezeichnet werden kann. Hätte der Gesetzgeber dies beabsichtigt, hätte er wohl auch den dies bestimmenden zweiten Satz des damaligen § 53 Abs 3a SPG in § 99 Abs 3 FinStrG aufgenommen. Da er dies jedoch unterließ, kann geschlossen werden, dass der Gesetzgeber auf die kleine Rufdatenrückerfassung für Zwecke des Finanzstrafverfahrens verzichten wollte.

6.7.6. Form des Auskunftsersuchens

Im FinStrG ist anders als in anderen Bestimmungen (vgl etwa die obigen Ausführungen zu den §§ 14a UWG, 87b Abs 3, 53 Abs 3b SPG) keine besondere Form vorgesehen, in der das Auskunftsbegehren an den Access-Provider zu richten ist. Vielmehr bestimmt § 99 Abs 3, 2. Satz FinStrG die ersuchte Stelle zur unverzüglichen und kostenlosen Auskunftserteilung. Weder das Gesetz noch die Materialien enthalten einen Hinweis darauf, dass das Auskunftsbegehren gegenüber der ersuchten Stelle zu begründen ist. Aus der Verpflichtung, dem Auskunftsbegehren unverzüglich

---

[717] Dies könnte bei unbedarfter Betrachtungsweise aus dem Begriff „Teilnehmernummer" in § 99 Abs 3 FinStrG abgeleitet werden.

[718] So eindeutig die DSK 20.7.2007, K 121.279/0017-DSK/2007, mittlerweile höchstgerichtlich bestätigt durch VwGH 27.5.2009, 2007/05/0280; ebenso DSK 18.9.2009, K 121.009/0005-DSK/2009.

nachzukommen kann somit geschlossen werden, dass der Gesetzgeber bei Einführung der Bestimmung dem Access-Provider keinerlei Kontrolltätigkeit zuweisen wollte.

6.7.7. Vertragliche Pflicht zur Ergreifung von Rechtsschutzmaßnahmen

Da es sich um eine Auskunft im Rahmen der Strafverfolgung handelt, wird es dem Access-Provider wegen dem eigenen Strafbarkeitsrisiko (§ 299 StGB) in vielen Fällen wohl auch nicht zumutbar sein, seinen Kunden zu informieren. Nach der Rechtsprechung des VwGH gehört § 99 FinStrG dem Verfahrensrecht an, gesonderte Beschwerden gegen entsprechende Verfahrensanordnungen sind daher unzulässig[719]. Gegen das Verfahren betreffende Anordnungen ist, soweit nicht ein Rechtsmittel ausnahmsweise für zulässig erklärt ist, ein abgesondertes Rechtsmittel gem § 152 FinStrG nicht zulässig. Sie können erst mit einem Rechtsmittel gegen die das Verfahren abschließende Entscheidung angefochten werden. Unrechtmäßigkeiten des Auskunftsverlangens können auch im Verfahren zur Erlassung der Zwangsstrafe wegen Verweigerung der Erfüllung des Auskunftsbegehrens geltend gemacht werden[720]. Ein nach Auskunftserteilung durch den Access-Provider eingebrachtes Rechtsmittel vermag die mögliche Verletzung der Privatsphäre seines Kunden nicht mehr rückgängig zu machen. Eine diesbezügliche vertragliche Schutzpflicht ist daher schon aus diesem Grund zu verneinen. Hinzu kommt, dass die Ergreifung eines Rechtsmittels einen dem Access-Provider unzumutbaren Aufwand mit sich brächte und deshalb eine darauf gerichtete Schutzpflicht aus denselben Gründen wie im Zusammenhang mit den anderen Schutzpflichten (vgl Kapitel 6.1ff) regelmäßig zu verneinen ist. Eine Weigerung dem Auskunftsbegehren nachzukommen, die in weiterer Folge die Verhängung einer Zwangsstrafe nach sich zieht, gegen die sich der Access-Provider in einem Verfahren wehren kann, ist mE ebenfalls regelmäßig nicht zumutbar. Da ihm keinerlei Informationen bezüglich des Grundes des Auskunftsbegehrens vorliegen, wird er nur in Ausnahmefällen die Rechtmäßigkeit des Auskunftsbegehrens beurteilen können. Das Risiko einer Zwangsstrafe ist ihm nicht zuzumuten, es sei denn, er weiß definitiv von der Unrechtmäßigkeit des gestellten Auskunftsbegehrens.

Sollte der Access-Provider aufgrund außergewöhnlicher Umstände im konkreten Einzelfall in Kenntnis von Umständen sein, die einen Missbrauch der Bestimmung nahe legen, stellt sich die Frage, ob ihn eine Pflicht zur Information des

---

[719] VwGH 13. 9. 1973, 18/73.

[720] VfGH 20.03.1986, B 410/85, vgl auch *Tannert*, in *Tannert* (Hrsg), Finanzstrafgesetz (34. ErgLf. 2009) § 99 Abs 1 Anm 1.

Rechtsschutzbeauftragten trifft. Das FinStrG kennt jedoch das Institut eines Rechtsschutzbeauftragten nicht. Gem § 195 Abs 1 FinStrG gelten jedoch für Strafverfahren wegen gerichtlich strafbarer Finanzvergehen (§ 53 FinStrG) die Bestimmungen der StPO, soweit in den §§ 195ff FinStrG nichts anderes angeordnet ist. Diese kennt zwar das Institut des Rechtsschutzbeauftragten, allerdings kommt diesem nur jene Aufgaben zu, die in der taxativen Liste des § 147 Abs 1 StPO[721] aufgezählt werden. Die Prüfung und Kontrolle einer Auskunft gem § 99 Abs 3 FinStrG ist von diesem Katalog nicht umfasst. Mangels entsprechender Zuständigkeit des Rechtsschutzbeauftragten erübrigt sich somit auch die Frage einer vertraglichen Pflicht zum Schutz der Kundendaten den Rechtsschutzbeauftragten zu informieren.

6.7.8. Vertragliche Pflicht zur Verweigerung von Auskunftsbegehren

Die gem § 99 Abs 3 FinStrG zu beauskunftenden Daten sind ausnahmslos Stammdaten, die der Access-Provider während aufrechtem Vertragsverhältnis speichern muss. Es sind daher so wie im MBG oder UWG keine Fälle denkbar, in denen die Erfüllung des Auskunftsbegehrens nur unter Verarbeitung unzulässig verarbeiteter (Verkehrs-)Daten möglich ist. Eine vertragliche Verweigerungspflicht aus diesem Grund scheidet daher aus.

Eine sich aus ergänzender Vertragsauslegung ergebende vertragliche Schutzpflicht zur Verweigerung der Erfüllung des Auskunftsbegehrens kann mE wie erwähnt nur ausnahmsweise dann bestehen, wenn der Access-Provider definitiv weiß, dass das an ihn heran getragene Auskunftsbegehren unrechtmäßig ist. In diesen Fällen kann er davon ausgehen, dass eine allfällige Zwangsstrafe jedenfalls nach Durchführung eines Verfahrens wieder aufgehoben wird. Die Inkaufnahme dieses Risikos scheint ihm daher zumutbar. Da er jedoch nie über die Gründe des Auskunftsbegehrens informiert wird, ist ein solcher Fall in praxi kaum denkbar.

---

[721] Vgl dazu *Reindl-Krauskopf,* in *Fuchs/Ratz* (Hrsg), Wiener Kommentar zur StPO (2009) § 147 Rz 4ff.

6.8. § 18 Abs 2 ECG

6.8.1. Der Wortlaut der Bestimmung

„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."

6.8.2. Allgemeines

Die Bestimmung soll im Folgenden nur beleuchtet werden, soweit sie Access-Provider iSd § 13 ECG betrifft. Die auch Host-Provider iSd § 16 ECG betreffende Informationspflicht gem § 18 Abs 2 ECG kann aufgrund der Themenstellung dieser Abhandlung außer Betracht bleiben. Die Abs 3 und 4 des § 18 ECG betreffen Auskunftspflichten der Host-Provider iSd § 16 ECG gegenüber einer Verwaltungsbehörde oder einem privaten Dritten.

Abs 4 leg cit wurde vom OGH jedoch bereits analog auf Betreiber von Telekommunikationsdiensten, sohin auf Access-Provider im hier verstandenen Sinne angewendet[722]. Daher sollen auch die wesentlichen Grundgedanken dieser Rechtsprechung weiter unten analysiert werden.

Die Bestimmung beruht auf Art 15 der E-Commerce-Richtlinie[723], der es den Mitgliedstaaten freistellt, Anbieter von Diensten der Informationsgesellschaft dazu verpflichten, den zuständigen Behörden auf Verlangen Informationen zu übermitteln, anhand derer die Nutzer ihres Dienstes, mit denen sie Vereinbarungen über die Speicherung geschlossen haben, ermittelt werden können (vgl auch den 48. Erwägungsgrund)[724].

---

[722] OGH 16.3.2005, 4Ob7/04i, SZ 2004/33 = RdW 2004/295c = RdW 2004/431; wbl 2004/205 = MR 2004, 221 = ecolex 2004, 853.

[723] *Zankl,* E-Commerce-Gesetz (2002) § 18 Rz 270.

[724] RV 817 BlgNR XXI. GP, 38.

6.8.3. Berechtigte und Verpflichtete

Zur Auskunft verpflichtet sind Diensteanbieter iSd §§ 13- 17 ECG, wobei hier wie erwähnt nur die Verpflichtungen der Access-Provider im oben definierten Sinne (vgl Kapitel 4.1) interessieren. Access-Provider iSd ECG sind Diensteanbieter[725], die lediglich die von einem Nutzer eingegebenen Informationen in einem Kommunikationsnetz übermitteln oder den Zugang zu einem Kommunikationsnetz vermitteln, ohne dabei die weitergegebene Information zu verändern. Normalerweise muss ein Dienst der Informationsgesellschaft die Voraussetzung erfüllen, dass er in der Regel gegen Entgelt erbracht wird. Für die in § 18 ECG statuierten Verpflichtungen von Access-Providern gilt dieses Kriterium wegen § 19 Abs 2 ECG hingegen nicht[726]. Diese Ausnahme könnte Bedeutung etwa im Hinblick auf Unternehmen oder Universitäten erlangen, die zwar keine Betreiber eines öffentlichen Telekommunikationsdienstes iSd § 3 Z 1 TKG 2003 sind, aber da sie ihren Mitarbeitern bzw Studenten unentgeltlich Zugang zu einem Kommunikationsnetz bieten, als Access-Provider iSd § 13 ECG gelten[727].

Umfasst sind nicht schlechthin alle Access-Provider, sondern nur solche, die mit ihren Nutzern Vereinbarungen über die Übermittlung getroffen haben. Diese Einschränkung hat im Bereich der Access-Provider, die Zugang zu einem Kommunikationsnetz vermitteln, kaum Auswirkungen, da diese ihre Dienste wohl kaum ohne vertragliche Grundlage erbringen[728]. Von der Definition des Access-Providers iSd ECG sind jedoch nicht nur Diensteanbieter erfasst, die den Zugang zu einem Kommunikationsnetz vermitteln, sondern auch solche, welche die eingegebenen Informationen lediglich übermitteln[729]. Das müssen nicht zwangsläufig die Vertragspartner der jeweiligen Nutzer sein. Diese Provider sind nach dem klaren Wortlaut des Gesetzes nicht erfasst, weil sie keine Vereinbarung mit den Nutzern über die Übermittlung geschlossen haben[730].

---

[725] Das sind gem § 3 Z 2 ECG natürliche oder juristische Personen oder sonstige rechtsfähige Einrichtungen, die einen in § 3 Z 1 ECG definierten Dienst der Informationsgesellschaft bereitstellen.

[726] Fallenböck/Tillian, Zur Auskunfts- und Mitwirkungspflicht der Internet-Provider, MR 2003, 404 (405).

[727] *Feiler,* in *Zankl* (Hrsg), Auf dem Weg zum Überwachungsstaat? (2009) 83.

[728] Fallenböck/Tillian, Zur Auskunfts- und Mitwirkungspflicht der Internet-Provider, MR 2003, 404 (405ff).

[729] Vgl *Feiler/Boka,* in *Zankl* (Hrsg), Auf dem Weg zum Überwachungsstaat? (2009) 128; vgl ebenfalls den 42. Erwägungsgrund der E-Commerce-Richtlinie.

[730] Diese Ausnahme wurde als nicht nachvollziehbar kritisiert: *Zankl,* E-Commerce-Gesetz (2002) § 18 Rz 278.

Zur Auskunft berechtigt sind lediglich inländische gesetzlich dazu befugte Gerichte. Siehe zu diesem Kriterium sogleich das nächste Kapitel. Verwaltungsbehörden haben ein Auskunftsrecht gem § 18 Abs 3 ECG.

6.8.4. Voraussetzungen

Die begehrten Auskünfte müssen der Ausforschung von Nutzern zur Verhütung, Ermittlung, Aufklärung oder Verfolgung gerichtlich strafbarer Handlungen dienen. Das Gericht kann die Auskunftsbegehren daher nur im Rahmen der Strafverfolgung begehren.

Fraglich ist insbesondere, welche Bedeutung dem Abstellen auf die Voraussetzung einer gesetzlichen Befugnis des Gerichts zukommt. Die Materialien führen dazu aus, dass es sich in der Regel „um eine nur unter besonderen Voraussetzungen zulässige Überwachung des Fernmeldeverkehrs im Sinn der §§ 149a ff StPO[731]" handeln wird[732]. Das mag wohl im Hinblick auf die zur „Ermittlung, Aufklärung oder Verfolgung gerichtlich strafbarer Handlungen" nötigen Auskünfte zutreffen. Im Hinblick auf die in § 18 Abs 2 ECG ebenfalls erwähnte „Verhütung" von Straftaten wird die Befugnis wohl eher im SPG zu suchen sein. Dort finden sich zwar entsprechende Auskunftsbefugnisse (§ 53 Abs 3a und 3b SPG), allerdings sind zu deren Ausübung nicht die Gerichte, sondern ausschließlich die Sicherheitsbehörden ermächtigt. Da Gerichten die Aufgabe der Verhütung von Straftaten nicht zukommt, ist der Anwendungsbereich von § 18 Abs 2 ECG in dieser Hinsicht unklar[733]. Am ehesten würde hier noch die Ermittlungsmaßnahme der Überwachung von Nachrichten bei Geiselnahmen (§ 135 Abs 3 Z 1 StPO) passen, die neben repressiven auch präventive Züge trägt[734]. Allerdings wird diese Maßnahme vom Gericht zwar bewilligt, jedoch von der Staatsanwaltschaft angeordnet (§ 137 StPO).

Die Materialien legen durch ihren Verweis auf die §§ 149a StPO alt die sich bereits aus dem Wortlaut ergebende Auslegung nahe, dass § 18 Abs 2 ECG für sich genommen keine ausreichende gesetzliche Grundlage für Auskünfte zur Ausforschung von Nutzern darstellt. Vielmehr setzt § 18 Abs 2 ECG eine an anderen Stellen normierte Befugnis der Gerichte voraus. Sind die Voraussetzungen der StPO für die Auskunft über die Daten einer Nachrichtenübermittlung nicht erfüllt, kann ein Auskunftsbegehren des

---

[731] Das entspricht der heutigen Auskunft über Daten einer Nachrichtenübermittlung iSd § 134 Z 2 bzw der Überwachung von Nachrichten iSd § 134 Z 3 StPO.

[732] RV 817 BlgNR XXI.GP, 38.

[733] *Zankl,* E-Commerce-Gesetz (2002) § 18 Rz 279.

[734] RV 25 BlgNR XXII. GP, 189.

Gerichts daher nicht allein auf § 18 Abs 2 ECG gestützt werden. Diesfalls würde es an der von § 18 Abs 2 ECG normierten „gesetzlichen Befugnis" fehlen. Damit ist die eigenständige Bedeutung des § 18 Abs 2 ECG jedoch überhaupt zweifelhaft. Deutlich wird dies auch dadurch, dass die heutigen den früheren §§ 149a ff StPO entsprechenden Ermittlungsmaßnahmen nicht mehr aufgrund einer gerichtlichen Anordnung stattfinden. Die Maßnahmen gem den heutigen §§ 135 und 136 StPO werden – mit Ausnahme jener gem § 136 Abs 1 Z 1 StPO – allesamt von der Staatsanwaltschaft aufgrund einer gerichtlichen Bewilligung angeordnet (§ 137 Abs 1 StPO). Dennoch werden die von der Staatsanwaltschaft angeordneten Auskünfte erteilt. Dass nach der neuen StPO das Gericht die Maßnahme nicht anordnet, sondern nur bewilligt und damit die in § 18 Abs 2 ECG normierte Voraussetzung einer gerichtlichen Anordnung nicht erfüllt ist, spielt keine Rolle. Gem § 515 StPO sind Verweise auf Bestimmungen, an deren Stelle mit dem In-Kraft-Treten des Strafprozessreformgesetzes neue Bestimmungen wirksam werden, auf die entsprechenden neuen Bestimmungen zu beziehen.

6.8.5. Auskunftsinhalt

Nach dem Wortlaut der Bestimmung werden die zu erteilenden Auskünfte keineswegs auf jene Nutzer eingeschränkt, die unter dem Verdacht stehen, die zu verhütende, zu ermittelnde, aufzuklärende oder zu verfolgende Straftat zu begehen bzw begangen zu haben. Vielmehr muss die Ermittlung der Identität in irgendeiner Form der Strafverfolgung dienen. Dies würde auch eine Auskunft über Daten einschließen, die nicht zum Verdächtigen führen, sondern nur zu Zeugen oder sonstigen Personen, die der Strafverfolgung dienlich sein könnten. Derartige Auskünfte erlaubt beispielsweise auch § 135 Abs 2 Z 2 StPO[735].

Welche Daten konkret beauskunftet werden müssen, ergibt sich aus den Bestimmungen der StPO, insbesondere jenen zur Auskunft über Daten einer Nachrichtenüberwachung (§ 135 StPO). Sofern dort wie etwa im Falle der Auskunft über Daten einer Nachrichtenübermittlung bei Geiselnahmen (§ 135 Abs 3 Z 1 StPO) eine Beschränkung der Daten auf jene des verdächtigen Nutzers normiert ist, ergeben sich auch aus § 18 Abs 2 ECG keine weitergehenden Befugnisse. Allerdings gibt es in der neuen StPO keine Rechtsgrundlage zur Ermittlung von Stammdaten zu bestimmten Verkehrsdaten wie etwa einer IP-Adresse[736]. Dazu soll nach der mittlerweile überholten

---

[735] *Reindl-Krauskopf/Tipold/Zerbes,* in *Fuchs/Ratz* (Hrsg), Wiener Kommentar zur StPO (2009) § 135 Rz 23ff.

[736] *Reindl-Krauskopf/Tipold/Zerbes,* in *Fuchs/Ratz* (Hrsg), Wiener Kommentar zur StPO (2009) § 134 Rz 36.

Auffassung des OGH[737] § 103 Abs 4 TKG 2003 ermächtigen. Nunmehr soll die Staatsanwaltschaft[738] dazu befugt sein, die Herausgabe der Stammdaten wenn nötig zwangsweise durch Sicherstellung gem § 110 StPO zu verlangen[739]. Dagegen lassen sich jedoch dieselben Argumente einwenden, wie gegen die Auffassung des OGH in 11 Os 57/07z[740], weshalb nach zutreffender Ansicht weder in der StPO noch im TKG 2003 eine Grundlage zur Ermittlung von Stammdaten anhand bekannter Verkehrsdaten vorhanden ist. Daher bildet auch § 18 Abs 2 ECG, dem wie erwähnt nicht der Charakter einer eigenständigen Auskunftsbestimmung zukommt, keine Grundlage zur Beauskunftung von Stammdaten. § 18 Abs 2 ECG enthält keine Speicherverpflichtung im Hinblick auf allfällige an den Access-Provider heranzutragende Auskunftsbegehren[741]. Die Zulässigkeit der Verwendung von Daten richtet sich weiterhin nach den Bestimmungen der §§ 92ff TKG 2003.

Darüber hinaus sind Bestimmungen über die Hausdurchsuchung oder die Sicherstellung zu beachten, allerdings dürfen damit nicht die Regelungen der §§ 134ff StPO umgangen werden[742]. Die Voraussetzungen der nach § 18 Abs 2 ECG zu erteilenden Auskunft ergeben sich aus jenen Bestimmungen der StPO, welche die gesetzliche Befugnis iSd § 18 Abs 2 ECG darstellen.

6.8.6. Form

§ 18 Abs 2 ECG setzt eine gerichtliche Anordnung voraus. Da die meisten gesetzlichen Befugnisse iSd § 18 Abs 2 ECG in der StPO im Vorverfahren jedoch nicht dem Gericht sondern der Staatsanwaltschaft als anordnender Behörde zustehen, stellt sich die Frage, ob auch staatsanwaltschaftliche Anordnungen ausreichend sind[743]. Hier greift mE die Übergangsbestimmung gem § 515 Abs 1, 2. Satz StPO Platz: *„Wird in anderen Bundesgesetzen auf Bestimmungen verwiesen, an deren Stelle mit dem In-Kraft-Treten des Strafprozessreformgesetzes neue Bestimmungen wirksam werden, so*

---

[737] OGH 26.7.2005, 11 Os 57/05z, EvBl 2005/176 = MR 2005, 352 = JBl 2006, 130 = RZ 2006/17.

[738] § 103 Abs 4 TKG 2003 ermächtigt zwar nur Gerichte, allerdings wird diese Ermächtigung wegen § 515 StPO auch auf die Staatsanwaltschaft ausgeweitet.

[739] *Reindl-Krauskopf/Tipold/Zerbes,* in *Fuchs/Ratz* (Hrsg), Wiener Kommentar zur StPO (2009) § 134 Rz 36.

[740] Vgl dazu bereits oben Kapitel 4.4.6.

[741] *Blume/Hammerl,* E-Commerce-Gesetz (2002) § 18 Rz 4.

[742] *Venier/Ebensperger,* in *Brenn* (Hrsg), ECG (2002) 301.

[743] Vgl zu dieser Problematik auch *Edthaler/Schmid,* Auskunft über IP-Adressen im Strafverfahren, MR 2008, 220 (224ff).

sind diese Verweisungen auf die entsprechenden neuen Bestimmungen zu beziehen." § 18 Abs 2 ECG verwies vor dem In-Kraft-Treten des Strafprozessreformgesetzes auf Bestimmungen, die früher gerichtlich anzuordnende Ermittlungsmaßnahmen vorsahen (§§ 149a ff StPO aF). Nachdem diese Bestimmungen seit der StPO-Reform durch BGBl I 19/2004 großteils durch solche ersetzt wurden, die statt einer gerichtlichen nunmehr eine staatsanwaltliche Anordnung vorsehen, bezieht sich § 18 Abs 2 ECG fortan auf diese Bestimmungen[744]. Fraglich ist jedoch, ob der in § 18 Abs 2 ECG enthaltene Verweis auf die Bestimmungen der StPO noch dem verfassungsrechtlichen Bestimmtheitsgebot (Art 18 B-VG) genügt[745].

6.8.7. Vertragliche Pflichten zur Verweigerung bzw zur Ergreifung von Rechtsschutzmaßnahmen im Interesse des Kunden

§ 18 Abs 2 ECG ist wie gezeigt keine Bestimmung, die eine eigenständige Rechtsgrundlage für das Ermitteln der dort erwähnten Informationen darstellt. Daher richten sich auch die Möglichkeiten zur Verweigerung bzw Bekämpfung von Auskunftsbegehren der Gerichte nicht nach den Bestimmungen des ECG, sondern nach den in § 18 Abs 2 ECG angesprochenen Befugnisnormen. Dabei handelt es sich um die Vorschriften der StPO, die noch weiter unten dargestellt werden.

6.9. § 18 Abs 4 ECG analog

6.9.1. Der Wortlaut der Bestimmung

§ 18 Abs 4 ECG lautet: „*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.*"

---

[744] So wird dies etwa im Bezug auf die Beauskunftung von Stammdaten nach § 103 Abs 4 StPO vertreten: *Reindl-Krauskopf/Tipold/Zerbes,* in *Fuchs/Ratz* (Hrsg), Wiener Kommentar zur StPO (2009) § 134 Rz 36.

[745] *Öhlinger*, Verfassungsrecht[7] (2007) Rz 86; *Jerabek,* in *Fuchs/Ratz* (Hrsg), Wiener Kommentar zur StPO (2009) § 515 Rz 1.

6.9.2. Die Entscheidung 4 Ob 7/04i [746]

In 4 Ob 7/04i entschied der OGH, dass Betreiber öffentlicher Kommunikationsdienste in analoger Anwendung des § 18 Abs 4 ECG den Namen und die Adresse eines Nutzers, der auf Grund einer Vereinbarung über dieses Netz Mehrwertdienste anbietet, auf Verlangen dritten Personen zu übermitteln haben, sofern diese ein überwiegendes rechtliches Interesse an der Feststellung der Identität eines Nutzers und eines bestimmten rechtswidrigen Sachverhalts haben sowie überdies glaubhaft machen, dass die Kenntnis dieser Information eine wesentliche Voraussetzung für die Rechtsverfolgung bildet. Hintergrund war die Klage eines Mehrwertdiensteanbieters, der behauptete, dass ein anderer Mehrwertdiensteanbieter, der eine Mehrwertnummer des beklagten Betreibers verwendete, wettbewerbswidrig handle. Er verlangte daher vom Betreiber, dass er ihm die Identität des anderen Mehrwertdiensteanbieters offen legt, damit er diesem gegenüber seine Rechte wahrnehmen kann. Nach Auffassung des OGH gab es in der österreichischen Rechtsordnung keine geeignete Rechtsgrundlage für ein derartiges Auskunftsbegehren. Dies war nach Ansicht des OGH jedoch nicht hinzunehmen, sondern stellte eine planwidrige Gesetzeslücke dar. Auf die mE zutreffende Kritik[747] und die Verteidigung[748] dieser Entscheidung wurde bereits im Zusammenhang mit § 14a UWG (vgl oben Kapitel 6.6.1) ausführlich eingegangen, weshalb es hier mit einem kurzen Hinweis darauf sein Bewenden haben kann.

Die Entscheidung des OGH ist vor allem deshalb problematisch, weil sie die Praxis vor kaum eindeutig beantwortbare Fragen stellt. So ist neben den schwierigen vom Access-Provider im Alleingang zu lösenden Abwägungsfragen – wann liegt etwa ein „überwiegendes Interesse vor? – insbesondere der persönliche Anwendungsbereich der analogen Anwendung des § 18 Abs 4 ECG auf Seiten der Auskunftswerber nicht ganz klar: Im Anlassfall war es ein Mitbewerber, dem der Auskunftsanspruch unter den Voraussetzungen des § 18 Abs 4 ECG zugesprochen wurde. Allerdings spricht nach Auffassung des OGH generell *„der Umstand, dass der Gesetzgeber bei Schaffung des TKG keine dem § 18 Abs 4 ECG vergleichbare Auskunftspflicht [des Access-Providers, Anm] gegenüber Dritten angeordnet hat, [...] für die Annahme einer planwidrigen Gesetzeslücke.*" Daraus wäre mE zu folgern, dass der OGH eine Auskunftspflicht nicht nur Mitbewerbern, sondern allgemein all jenen zugestehen möchte, welche die

---

[746] OGH 16.3.2004 4 Ob 7/04i, ecolex 2004, 854 = wbl 2004, 390 = RdW 2004, 475 = MR 2004, 221 = SZ 2004/33.

[747] *Zankl,* Auskunftspflicht für Mehrwertdienste? ecolex 2004, 853ff; *Hasberger/Schönhart,* Die Haftung von Telekom-Unternehmen für fremdes Fehlverhalten, MR 2004, 297.

[748] *Plasser,* Lauterkeitsrechtlicher Auskunftsanspruch auch für Mitbewerber nach der UWG-Nov 2007, ÖBl 2008, 183; *Kodek/Leupold,* in *Wiebe/G. Kodek,* UWG, § 14a Rz 5ff.

Voraussetzungen eines Auskunftsanspruch gegen einen Host-Provider gem § 18 Abs 4 erfüllen.

Fraglich ist weiters, wie sich diese Entscheidung zur Entscheidung im Fall *LSG gegen Tele 2*[749] verhalten soll. Dort kam der OGH eindeutig zum Ergebnis, dass eine Verarbeitung von Verkehrsdaten zu Auskunftszwecken wegen § 99 Abs 1 TKG bzw Art 6 Abs 1 EK-Datenschutzrichtlinie nur dann zulässig sei, wenn es eine konkrete Ausnahmevorschrift iSd Art 15 EK-Datenschutzrichtlinie gibt. Den Charakter einer Ausnahmevorschrift, welche die Speicherung und Verarbeitung zu Auskunftszwecken zulasse, sprach in concreto selbst § 87b Abs 3 UrhG ab. Eine lediglich analog angewendete Vorschrift wird jedoch noch weniger als Vorschrift iSd Art 15 EK-Datenschutzrichtlinie in Betracht kommen. Es handelt sich zum einen um keine „gesetzlich erlassene Vorschrift" und zum anderen wäre die Verarbeitungs- bzw Speicherungserlaubnis in § 18 Abs 4 ECG analog allenfalls impliziter Natur, was schon im Falle des § 87b Abs 3 UrhG als nicht ausreichend erachtet wurde und durch die Materialien zu § 18 Abs 4 ECG ausgeschlossen wird[750]. Damit steht fest, dass eine analoge Anwendung von § 18 Abs 4 ECG keinesfalls die Verarbeitung von Verkehrsdaten zu Auskunftszwecken decken kann.

In praxi sind jedoch fast ausschließlich Fälle denkbar, in denen dem Auskunftswerber Verkehrdaten (etwa dynamische IP-Adressen) bekannt sind, auf deren Basis er Auskunft vom Access-Provider begehrt. Ist jedoch keine IP-Adresse, sondern eine Rufnummer[751] oder eine statische IP-Adresse bekannt, so könnte vertreten werden, dass aufgrund deren Charakters (auch[752]) als Stammdatum keine Verarbeitung von Verkehrsdaten stattfindet und daher die Namen und Anschrift bekannt gegeben werden können, ohne in Konflikt mit der Entscheidung *LSG gegen Tele 2* zu geraten.

---

[749] OGH 14.7.09, 4 Ob 41/09x.

[750] Vgl RV 817 BlgNR XXI. GP, 39: *„Der Host Provider wird durch diese Regelung auch nicht verpflichtet, diese Daten zu speichern oder aufzubewahren, er hat auch nur die ihm verfügbaren Daten herauszugeben."*

[751] Diesen kommt ein sowohl der Charakter eines Stamm- als auch eines Verkehrsdatums zu: RV 128 BlgNR XXII. GP, 17ff; als was die Rufnummer zu beurteilen ist, hängt somit von den konkreten Umständen ab: *Reindl-Krauskopf/Tipold/Zerbes,* in *Fuchs/Ratz* (Hrsg), Wiener Kommentar zur Strafprozessordnung (2009) § 134 Rz 29.

[752] Die Frage, ob eine statische IP-Adresse ein Stamm- oder Verkehrsdatum darstellt, ist umstritten. Dafür etwa *Einzinger/Schubert/Schwabl/Wessely/Zykan*, Wer ist 217.204.27.214? MR 2005, 113 (116), dagegen etwa *Wiebe*, Auskunftsverpflichtung der Access-Provider, Beilage zu MR 2005/4, 14; diese Frage wurde vom OGH in der Entscheidung *LSG gegen Tele 2* bedauerlicherweise ausdrücklich offen gelassen.

6.9.3. Auskunftsbefugnis

Da schon die Befugnis des § 18 Abs 4 ECG selbst keine Grundlage in der E-Commerce-Richtlinie hat[753], ist bereits diese Auskunftspflicht restriktiv auszulegen[754]. Dies muss jedenfalls auch für die analoge Anwendung des § 18 Abs 4 ECG gelten. Daraus folgt etwa, dass der Nutzer, bezüglich welchem die Offenlegung der Identität verlangt wird, derjenige Nutzer sein muss, der unter dem Verdacht steht, die Rechtsverletzung begangen zu haben, auch wenn der Wortlaut ein weiteres Verständnis erlauben würde[755].

Zur Voraussetzung einer Vereinbarung über die Speicherung bzw – im analogen Anwendungsfall – Übermittlung von Daten mit dem Nutzer vgl die obigen Ausführungen zu § 18 Abs 2 ECG.

Der Auskunftswerber muss folgende Umstände glaubhaft machen:

- ein überwiegendes rechtliches Interesse an der Feststellung der Identität eines Nutzers
- einen bestimmten rechtswidrigen Sachverhalt
- dass die Kenntnis dieser Informationen eine wesentliche Voraussetzung für die Rechtsverfolgung bildet.

Bezüglich der Frage, wann ein Umstand glaubhaft gemacht, dh bescheinigt wurde, wird wohl auf die Lehre und Judikatur zu § 274 ZPO zurück gegriffen werden können[756]. Wichtig ist insbesondere das Kriterium, dass sich aus den vorgelegten Bescheinigungsmitteln für den Access-Provider der zu beweisende Umstand unmittelbar ergibt und keine weiteren aufwändigen Ermittlungen mehr erforderlich sind. So würde mE etwa ein Dokument, dass die rechtswidrige Tätigkeit (etwa Werbung) bescheinigt und eine Telefonnummer des Nutzers enthält, dessen Identität ausgeforscht werden soll, zur Glaubhaftmachung ausreichen. Für die Glaubhaftmachung reicht im Allgemeinen der Nachweis einer überwiegenden Wahrscheinlichkeit der Richtigkeit der zu bescheinigenden angemeldeten Tatsache[757].

---

[753] So auch ausdrücklich die RV 817 BlgNR, XXI. GP, 39.

[754] *Zankl,* E-Commerce-Gesetz (2002) § 18 Rz 283.

[755] *Zankl,* E-Commerce-Gesetz (2002) § 18 Rz 283ff.

[756] Vgl dazu *Klauser/Kodek,* ZPO 16.01 (2008) § 274.

[757] OGH 2.2.2001, 6 Ob 251/00f, SZ 74/27.

Was die Rechtswidrigkeit anbelangt, so sprechen die Materialien davon, dass diese für einen juristischen Laien offenkundig sein muss[758]. Die dagegen vorgebrachte Kritik, dass dies der Wortlaut eben gerade nicht decke, ist zwar richtig[759], aber dennoch sollte mE im Zweifel wegen der vertraglichen Verpflichtungen des Access-Providers gegenüber seinem Kunden eine Auskunftspflicht nur in eindeutigen Fällen bestehen.

Hinsichtlich des überwiegenden Interesses ist wohl auf die zum DSG 2000 vorhandenen Erwägungen zurückzugreifen, auf welche die Materialien auch ausdrücklich verweisen[760]. Schon danach spricht im Zweifel die Vermutung für die Schutzwürdigkeit des Datums[761]. Überdies ergibt sich die Zweifelsregel zugunsten des Schutzes der begehrten Daten auch aus den vertraglichen Schutzpflichten des Access-Providers gegenüber seinem Kunden.

Die Auskunft muss nur wesentliche Voraussetzung, sohin keine conditio sine qua non[762], für die Rechtsverfolgung des Auskunftswerbers sein. Die Glaubhaftmachung dieser Voraussetzung wird regelmäßig nicht besonders schwer fallen.

Die Auskunftsbestimmung des § 18 Abs 4 ECG sieht zwar keine Formpflicht vor, jedoch wird es in der Praxis kaum gelingen, die geforderten Voraussetzungen ohne geeignete Urkunden zu bescheinigen.

6.9.4. Vertragliche Schutzpflichten im Zusammenhang mit § 18 Abs 4 ECG analog

Aufgrund der zahlreichen Voraussetzungen, die der OGH hinsichtlich eines Auskunftsbegehrens gem § 18 Abs 4 ECG analog aufstellte, werden den Access-Provider diesbezüglich genaue Prüfpflichten treffen. Der Access-Provider hat somit das Vorliegen aller oben skizzierten Voraussetzungen exakt zu kontrollieren und bei Nichtvorliegen einer Voraussetzung die Auskunft über Namen und Anschrift jedenfalls zu verweigern. Diese im Rahmen ergänzender Vertragsauslegung gewonnene Schutzpflicht wird bereits durch die Konzeption des § 18 Abs 4 ECG, der grundsätzlich keine Zwischenschaltung eines Richters vorsieht, nahe gelegt. Wer, wenn nicht der Access-Provider soll für die

---

[758] RV 817 BlgNR XXI. GP, 39.

[759] *Zankl,* E-Commerce-Gesetz (2002) § 18 Rz 291.

[760] RV 817 BlgNR XXI. GP, 39.

[761] *Dohr/Pollirer/Weiss,* DSG² (2009) § 8 Anm 9.

[762] *Zankl,* E-Commerce-Gesetz (2002) § 18 Rz 288.

Kontrolle der Voraussetzungen zuständig sein, wenn es nicht zu einer klagsweisen Geltendmachung des Auskunftsanspruchs kommt?

Dabei gilt bezüglich aller drei zu bescheinigenden Voraussetzungen, dass wenn der Access-Provider nicht von der überwiegenden Wahrscheinlichkeit des Vorliegens derselben ausgehen kann, er im Zweifel aufgrund der vertraglichen Schutzpflichten die Herausgabe der begehrten Daten zu verweigern hat[763]. Dies gilt mE auch dann, wenn seitens des Auskunftswerbers eine Klage droht. Die Inkaufnahme dieses Risikos ist hier ausnahmsweise aufgrund der schon fragwürdigen Grundlage der Auskunftspflicht und der guten Aussichtschancen, dass eine Auskunftsverweigerung gerichtlich bestätigt wird, zumutbar. Zudem besteht mE ohnedies eine Informationspflicht gegenüber dem Kunden (vgl dazu oben Kapitel 5.5), sodass er im Falle der anstandslosen Auskunftserteilung eine Klage seines Vertragespartners riskiert. In dieser Situation hat sich der Access-Provider mE im Zweifel für seinen Vertragspartner zu entscheiden.

Der Access-Provider muss im Rahmen seiner Schutzpflichten auch darauf achten, dass es im Zuge der Auskunftserfüllung zu keiner rechtswidrigen Verarbeitung von Verkehrsdaten kommt. Sind die für die Erfüllung erforderlichen Verkehrsdaten nur mehr unzulässigerweise bei ihm vorhanden, hat er wie bei allen anderen Auskunftsansprüchen auch die Herausgabe der begehrten Daten im Einklang mit der Entscheidung *LSG gegen Tele 2* zu verweigern.

6.10. § 7 Abs 6 Zollrechts-Durchführungsgesetz (ZollR-DG)

6.10.1. Der Wortlaut der Bestimmung

§ 7 Abs 6 ZollR-DG lautet: „*Die Zollbehörden sind berechtigt, von den Betreibern öffentlicher Kommunikationsdienste und von Universaldiensten (Abschnitte 3 und 4 des Telekommunikationsgesetzes 2003-TKG 2003, BGBl. I Nr. 70/2003), die einen öffentlichen Telefondienst gemäß § 3 Z 16 TKG 2003 erbringen, Auskunft über Namen, Anschrift und Teilnehmernummer zu verlangen, wenn sie diese Daten als wesentliche Voraussetzung für die Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben benötigen. Die ersuchte Stelle ist verpflichtet, diese Auskunft unverzüglich zu erteilen.*"

---

[763] Vgl auch *Zankl,* E-Commerce-Gesetz (2002) § 18 Rz 291.

6.10.2. Berechtigte und Verpflichtete

Zur Auskunft berechtigt sind die Zollbehörden. Die Organisation sowie die sachliche und örtliche Zuständigkeit der Zollbehörden ergeben sich gem § 6 Abs 2 ZollR-DG aus dem Abgabenverwaltungsorganisationsgesetz (insbesondere den §§ 14 ff).

Zur Auskunft verpflichtet sind nach dem Wortlaut der Bestimmung Betreiber öffentlicher Kommunikationsdienste sowie Betreiber von Universaldiensten. Hier interessieren nur die Pflichten der Betreiber öffentlicher Kommunikationsdienste, dh der Access-Provider im hier verstandenen Sinn. Ein Universaldienst ist ein Mindestangebot an öffentlichen Diensten, zu denen alle Endnutzer unabhängig von ihrem Wohn- oder Geschäftsort zu einem erschwinglichen Preis Zugang haben müssen (§ 26 TKG 2003). Die Erbringung des Universaldienstes ist vom Bundesminister für Verkehr, Innovation und Technologie öffentlich auszuschreiben und nach den Verfahrensvorschriften über die Vergabe von Leistungen zu vergeben. Er kann sich dabei der Regulierungsbehörde bedienen. Die Ausschreibung kann jedoch entfallen, wenn lediglich ein Unternehmen die betrieblichen Voraussetzungen für die Erbringung der Universaldienstleistung erfüllt (§ 30 Abs 1 TKG 2003). Durch die Vorschriften über den Universaldienst soll eine flächendeckende Grundversorgung mit Kommunikationsdiensten sichergestellt werden[764]. Zu den Universaldiensten zählen neben bestimmten Kommunikationsdiensten[765] auch die Erbringung eines betreiberübergreifenden Auskunftsdienstes („Auskunft"), die Erstellung eines betreiberübergreifenden Teilnehmerverzeichnisses („Telefonbuch") sowie die flächendeckende Versorgung mit öffentlichen Sprechstellen an allgemein und jederzeit zugänglichen Standorten („Telefonzellen").

Den zur Auskunft verpflichteten Betreibern steht trotz einer dies unter Verweis auf die Rechtsprechung des VfGH[766] fordernden Stellungnahme des BMJ[767] zum

---

[764] Vgl Erwägungsgrund 4 der Richtlinie 2002/22/EG des Europäischen Parlamentes und des Rates vom 7. März 2002 über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten (Universaldienstrichtlinie), ABl L 2002/108, 51; *Schmelz/Stratil,* Das neue Telekommunikationsgesetz, ecolex 1998, 267 (269); *Lichtenberger/Ruhle,* Das novellierte TKG – Basis für wirksamen Wettbewerb auf den österreichischen Kommunikationsmärkten? ecolex 2003, 812 (814ff).

[765] Die meisten Universaldienstleistungen werden in Österreich von der Telekom austria AG erbracht. Zur Kritik daran vgl *Ruhle/Lichtenberger/Kittl,* Erste Erfahrungen mit dem TKG 2003 in Österreich, MR 2005, 63 (78).

[766] VfGH 27.3.2003, G 37/02 ua.

[767] 8/SN-129 ME BlgNR XXII. GP, abrufbar unter: http://www.parlinkom.gv.at/PG/DE/XXII/ME/ME_00129_08/fname_000000.pdf (Stand April 2010).

Ministerialentwurf[768] kein Kostenersatz zu. Die Materialien gehen davon aus, dass diese Auskunftsbefugnis die Betreiber nur geringfügig belasten wird[769].

6.10.3. Voraussetzungen

Einzige Voraussetzung für das Auskunftsverlangen ist, dass die Zollbehörde die Auskunft über Namen, Anschrift und Teilnehmernummer für die Erfüllung der ihr nach dem ZollR-DG übertragenen Aufgaben benötigt. Die Aufgaben der Zollverwaltung werden unter anderem in einer demonstrativen Liste in § 6 ZollR-DG angeführt. Weitere Aufgaben ergeben sich etwa aus den §§ 16ff (Zollaufsicht). Die Aufgaben der Zollorgane können, sofern den Anordnungen der Organe keine Folge geleistet wird, mit Zwangsgewalt durchgesetzt werden (§ 35 Abs 1 ZollR-DG).

Die finale Beschreibung der Voraussetzung enthält keinerlei Einschränkung auf bestimmte Personen, deren Daten ermittelt werden. So ist wird nach dem Wortlaut der Bestimmung etwa in keiner Weise vorausgesetzt, dass die gewünschten Daten zu einer Person führen, die eine Zollzuwiderhandlung (§ 4 Abs 2 Z 14 ZollR-DG) begangen hat.

6.10.4. Auskunftsinhalt

Die Bestimmung wurde nach den Materialien bewusst dem § 53 Abs 3a SPG in seiner Fassung vor der Novelle durch BGBl I 114/2007 nachgebildet, bleibt aber hinter diesem zurück[770]. In welchem Punkt die Auskunftsbefugnis gem § 7 Abs 6 ZollR-DG hinter § 53 Abs 3a SPG zurück bleiben soll, sagen die Materialien nicht ausdrücklich.

Die zu beauskunftenden Daten gleichen exakt jenen, die auch nach § 53 Abs 3a SPG zu beauskunften sind. Es ist daher auf die dortigen Ausführungen zu verweisen (vgl oben Kapitel 6.1). Ähnlich wie im Falle des § 99 Abs 3 FinStrG, der ebenfalls nach dem Vorbild der Bestimmung aus dem SPG geschaffen wurde, wird man daraus wohl zwei wesentliche Schlüsse ziehen können (vgl dazu bereits oben Kapitel 6.7.5 im Detail):

Zum einen sieht § 7 Abs 6 ZollR-DG keine Möglichkeit vor, dass die Bezeichnung des Anschlusses auch durch Bezugnahme auf ein von diesem Anschluss geführtes Gespräch durch Bezeichnung eines möglichst genauen Zeitraumes und der

---

[768] ME 129 BlgNR XXII. GP.

[769] RV 405 BlgNR XXII. GP, 7.

[770] RV 405 BlgNR XXII. GP, 7.

passiven Teilnehmernummer erfolgen kann. Daraus ist zu folgern, dass die Auskunftsbefugnis im ZollR-DG keine kleine Rufdatenrückerfassung ermöglicht. Dies wird durch die Materialien, die ausdrücklich betonen, dass § 7 Abs 6 ZollR-DG hinter der Auskunftsbestimmung im SPG zurück bleiben soll, bestätigt.

Zum anderen ist aus der Entwicklungsgeschichte des § 53 Abs 3a SPG abzuleiten, dass die Auskunftsbefugnis im ZollR-DG keine Auskunft über IP-Adressen bzw über zu bestimmten IP-Adressen gehörenden Stammdaten erlaubt. Das ZollR-DG kennt keine Befugnisse, die den durch BGBl I 114/2007 in § 53 Abs 3a z 2 und 3 SPG eingefügten entsprechen. Die Auskunftsbestimmung im ZollR-DG betrifft daher nur den Bereich der klassischen Sprachtelefonie.

6.10.5. Form des Auskunftsbegehrens

Das ZollR-DG bindet das Auskunftsbegehren anders als andere Bestimmungen an keinerlei Formvorschriften. Vielmehr ist die Auskunft unverzüglich zu erteilen. Dies unterstreicht den Willen des Gesetzgebers, dass der Access-Provider keine Gelegenheit haben soll, die Rechtmäßigkeit des Auskunftsbegehrens zu überprüfen.

6.10.6. Vertragliche Pflicht zur Ergreifung von Rechtsschutzmaßnahmen

Prinzipiell kann gem Art 243 des Zollkodex[771] jede Person einen Rechtsbehelf gegen Entscheidungen der Zollbehörden auf dem Gebiet des Zollrechts einlegen, die sie unmittelbar und persönlich betreffen. Ergänzend dazu bestimmt § 85a Abs 1 ZollR-DG, dass im Rahmen des Geltungsbereichs des § 2 Abs 1 und 2 ZollR-DG als Rechtsbehelf gegen Entscheidungen der Zollbehörden (Z 1) und wegen der Behauptung einer Rechtsverletzung durch Ausübung unmittelbarer Befehls- oder Zwangsgewalt durch ein Zollorgan (Z 2) die Berufung zusteht.

Fraglich ist bereits, ob dem Access-Provider hier überhaupt ein Rechtsbehelf zukommt. Durch die Einschränkung der Möglichkeit der Einbringung von Rechtbehelfen auf jene Personen, die durch die Entscheidungen unmittelbar und persönlich betroffen sind, sollen Rechtsmittel zur Wahrnehmung Dritter ausgeschlossen werden[772]. Unter Betroffenheit verstehen manche aber auch eine rein wirtschaftliche

---

[771] VO 2913/92/EWG des Rates vom 12. Oktober 1992 zur Festlegung des Zollkodex der Gemeinschaften, Amtsblatt L 1992/302, 1.

[772] *Alexander* in *Witte* (Hrsg), Zollkodex[2] (1998) Art 243 Rz 2.

Betroffenheit[773], die sogar durch die Materialien, wenn auch nur in „geringfügigem" Maße zugestanden wird. Selbst wenn man letzterer Auffassung folgt und eine Rechtsmittelegitimation des Access-Providers bejaht, so scheidet eine vertragliche Schutzpflicht zur Ergreifung von Rechtsschutzmaßnahmen mE aus Zumutbarkeitsgründen aus. In den Fällen, in welchen der Access-Provider seinen Vertragspartner nicht über die Erfüllung eines Auskunftsbegehrens informieren kann, muss er mE auch kein Rechtsmittel zu seinen Gunsten gegen das Auskunftsverlangen einbringen. Nach dem Wortlaut des § 7 Abs 6 ZollR-DG sind dem Access-Provider gegenüber keinerlei Gründe für die Stellung des Auskunftsbegehrens zu benennen. Er hat das unbegründete Begehren vielmehr unverzüglich zu erfüllen. Damit wird er kaum in der Lage sein, die Rechtmäßigkeit des an ihn heran getragenen Auskunftsbegehrens zu beurteilen, weshalb die Ergreifung eines Rechtsmittels aus seiner Perspektive ein zu hohes Risiko darstellt und ihm somit nicht zugemutet werden kann.

6.10.7. Vertragliche Pflicht zur Verweigerung des Auskunftsbegehrens

Da § 7 Abs 6 ZollR-DG ähnlich wie § 99 Abs 3 FinStrG oder § 22 Abs 2a MBG keinesfalls zur Verarbeitung von (reinen) Verkehrsdaten führen wird, sind in praxi keine Fälle denkbar, in welchen die zur Bearbeitung des Auskunftsbegehrens nötigen Daten nicht mehr vorhanden sein dürfen. Zur Erfüllung der nach § 7 Abs 6 ZollR-DG müssen lediglich Stammdaten verarbeitet werden. Eine Verweigerung aus dem Grund, dass die Erfüllung des Auskunftsbegehrens zu einer unrechtmäßigen Verarbeitung von Verkehrsdaten führen würde, scheidet somit aus.

Eine vertragliche Pflicht zur Verweigerung der Erfüllung der Auskunft besteht mE nur in jenen in praxi kaum denkbaren Extremfällen, in denen dem Access-Provider die Unrechtmäßigkeit des an ihn heran getragenen Auskunftsbegehrens definitiv bekannt ist.

---

[773] *Stiehle* in *Schwarz/Wockenfoth* (Begründer), Zollrecht 1/3[3] (13. ErgLf. 1997) Art 243 Rz 9; eine unmittelbare Betroffenheit bei bloß wirtschaftlicher oder ideeller Betroffenheit hingegen ausschließend *Alexander* in *Witte* (Hrsg), Zollkodex[2] (1998) Art 243 Rz 8.

6.11. Auskunft über Daten einer Nachrichtenübermittlung (§ 134 Z 2 StPO) und Überwachung von Nachrichten (§ 134 Z 3 StPO)

6.11.1. Legaldefinition der Auskunft über Daten einer Nachrichtenübermittlung

§ 134 Z 2 StPO definiert die Auskunft über Daten einer Nachrichtenübermittlung als *„die Erteilung einer Auskunft über Verkehrsdaten (§ 92 Abs. 3 Z 4 TKG), Zugangsdaten (§ 92 Abs. 3 Z 4a TKG) und Standortdaten (§ 92 Abs. 3 Z 6 TKG) eines Telekommunikationsdienstes oder eines Dienstes der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes).*"

6.11.2. Auskunftsinhalt

Zu beauskunften sind Verkehrs-, Zugangs- und Standortdaten (zu diesen Begriffen vgl bereits oben Kapitel 4.4). Es dürfen auch die Standortdaten eines Endgeräts zu Zeitpunkten bekannt gegeben werden, zu denen keine Kommunikation geführt wird bzw wurde[774]. Der Wortlaut der Bestimmung umfasst jedoch nicht auch die Beauskunftung von Stammdaten.

Stammdaten werden jedoch in der Praxis regelmäßig auf Anordnung der Staatsanwaltschaft formlos gem § 103 Abs 4 TKG 2003 bekannt gegeben. Dabei wird unzulässigerweise ausgeblendet, dass bei der Beauskunftung von Stammdaten Verkehrsdaten verarbeitet werden müssen.

Da § 135 Abs 2 iVm § 134 Z 2 StPO keine geeignete Rechtsgrundlage für die Beauskunftung von Stammdaten darstellt, wird in der Praxis § 110 StPO (Sicherstellung) herangezogen, wenn die Stammdaten zwangsweise ermittelt werden sollen[775]. Dies ist mE ebenfalls keine befriedigende Lösung, weil dabei – genau wie bei den formlosen Auskunftsbegehren nach § 103 Abs 4 TKG 2003 – der oben dargestellte Zusammenhang zwischen den Datenkategorien (vgl Kapitel 4.4.6) ignoriert wird[776]. Die Sicherstellung ist von der Staatsanwaltschaft anzuordnen und von der Kriminalpolizei

---

[774] RV 25 BlgNR XXII. GP, 187; *Reindl-Krauskopf/Tipold/Zerbes* in *Fuchs/Ratz* (Hrsg), Wiener Kommentar zur Strafprozessordnung (2009) § 134 Rz 35.

[775] *Reindl-Krauskopf/Tipold/Zerbes* in *Fuchs/Ratz* (Hrsg), Wiener Kommentar zur Strafprozessordnung (2009) § 134 Rz 36.

[776] Vgl auch *Hasberger,* Die providerinterne Auswertung von Verkehrsdaten und Datenschutz, MR 2010, 23 (23ff).

durchzuführen, während die Auskunft über Verkehrsdaten gem § 137 StPO nur aufgrund einer gerichtlichen Bewilligung von der Staatsanwaltschaft angeordnet werden kann. Verkehrsdaten sind somit verfahrensrechtlich wesentlich besser geschützt, weil ihre Preisgabe zusätzlich die Prüfung durch ein unabhängiges weisungsfreies Gericht erfordert. Sofern für die Beauskunftung von Stammdaten Verkehrsdaten verarbeitet werden müssen, wäre daher mE das höhere durch § 137 StPO vorgegebene Schutzniveau einzuhalten. Da die StPO keine eigene Bestimmung zur Beauskunftung von Stammdaten enthält, liegt mE eine planwidrige Lücke vor. Das Gesetz erscheint gemessen an seiner eigenen Absicht und immanenten Teleologie, ergänzungsbedürftig[777]. Der OGH verneinte dies jedoch in der Vergangenheit mit der Begründung, dass der Vorgang der Erhebung der Stammdaten des Inhabers eines bestimmten Teilnehmeranschlusses schon vor der StPO-Novelle 2004 bekannt war und von der strafgerichtlichen Praxis als außerhalb der Regeln für die Telekommunikationsüberwachung stehend angesehen wurde. Das legislatorische Schweigen zwinge somit zur Annahme, der Gesetzgeber habe diesen Vorgang nicht den einschränkenden Bedingungen der Überwachung einer Telekommunikation unterwerfen wollen, zumal es sich um die am Wenigsten eingriffsintensive Maßnahme handle[778]. Allerdings war dem Gesetzgeber zum Zeitpunkt der Entstehung der Novelle noch nicht bekannt, wie der EuGH die Beauskunftung von Stammdaten vor dem Hintergrund der EK-Datenschutzrichtlinie beurteilt. Nach dessen Judikatur ist die Auskunft über Stammdaten, wenn dafür Verkehrsdaten verarbeitet werden müssen, eine nur in den Ausnahmefällen des Art 15 EK-Datenschutzrichtlinie zulässige Verarbeitung von Verkehrsdaten. Der einfache Weg, alleine auf die Bekanntgabe von Stammdaten abzustellen, ist somit gemeinschaftsrechtlich nicht mehr gangbar[779]. Diese Klarstellungen durch die Judikatur des EuGH konnte der Gesetzgeber damals nicht im Auge haben, weshalb sich die Entscheidung des Gesetzgebers, die Auskunft über Stammdaten keiner Regelung zuzuführen, aus heutiger Perspektive als lückenhaft erweist. Die Lücke ist mE durch eine analoge Anwendung der Verfahrensvorschriften hinsichtlich der Auskunft über Daten einer Nachrichtenübermittlung auch auf Fälle der Beauskunftung von Stammdaten zu schließen.

---

[777] OGH 23.3.1976 4 Ob 313/76, SZ 49/45 = EvBl 1976/263 = ÖBl 1976, 113 = JBl 1976, 490 = GRURInt 1977, 211.

[778] OGH 26.7.2005, 11 Os 57/05z, EvBl. 2005/176 = MR 2005, 352 = JBl 2006, 130 = RZ 2006/17.

[779] OGH 14.7.2009 4 Ob 41/09x.

6.11.3. Voraussetzungen der Auskunft über Daten einer Nachrichtenübermittlung[780]

§ 135 Abs 2 StPO regelt drei Tatbestände, in denen die Auskunft über Daten einer Nachrichtenübermittlung zulässig sein soll. Die in § 135 Abs 2 Z 2 StPO geregelte Ermittlungsmaßnahme setzt die Zustimmung des Inhabers der technischen Einrichtung, die Ziel oder Ursprung einer Übertragung von Nachrichten war oder sein wird, voraus, während die in Z 1 und 3 leg cit geregelten Tatbestände auf dieses Erfordernis verzichten.

Wenn der Inhaber der technischen Einrichtung, die Ziel oder Ursprung einer Nachrichtenübertragung war oder sein wird, der Auskunft über Daten der Nachrichtenübermittlung ausdrücklich zustimmt, ist diese bereits zulässig, wenn zu erwarten ist, dass dadurch die Aufklärung einer mit mehr als sechs Monaten Freiheitsstrafe bedrohten Vorsatztat gefördert werden kann (§ 135 Abs 2 Z 2 StPO).

Ansonsten ist die Auskunft über Daten einer Nachrichtenübermittlung zulässig,

- wenn und solange der dringende Verdacht besteht, dass eine von der Auskunft betroffene Person eine andere entführt oder sich sonst ihrer bemächtigt hat, und sich die Auskunft auf Daten einer solchen Nachricht beschränkt, von der anzunehmen ist, dass sie zur Zeit der Freiheitsentziehung vom Beschuldigten übermittelt, empfangen oder gesendet wird (§ 135 Abs 2 Z 1 StPO) oder
- wenn zu erwarten ist, dass dadurch die Aufklärung einer mit mehr als einem Jahr Freiheitsstrafe bedrohten Vorsatztat gefördert werden kann und aufgrund bestimmter Tatsachen anzunehmen ist, dass dadurch Daten des Beschuldigten ermittelt werden können (§ 135 Abs 2 Z 3 StPO)[781].

Ein dringender Tatverdacht wird nur dann vorliegen, wenn die Verdachtsmomente stärker sind als die entlastenden Umstände[782]. Eine Beweisregel, worauf sich der dringende Tatverdacht zu gründen hat, ist dem Gesetz fremd[783]. Der

---

[780] Dieses Kapitel ist teilweise angelehnt an meinen Beitrag in *Zankl* (Hrsg), Auf dem weg zum Überwachungsstaat? (2009), 192ff.

[781] § 135 Abs 2 Z 3 ermöglicht wie Abs 3 Z 4 die Ermittlung von Standortdaten des Beschuldigten: *Reindl-Krauskopf/Tipold/Zerbes* in *Fuchs/Ratz* (Hrsg), Wiener Kommentar zur Strafprozessordnung (2009) § 134 Rz 63.

[782] *Schmidt,* Die Grundrechtskonformität der Überwachung einer Telekommunikation, Diss Wien (2003) 75 mwN.

[783] OGH 23.10.2000, 13 Os 127/00; *Reindl-Krauskopf/Tipold/Zerbes* in *Fuchs/Ratz* (Hrsg), Wiener Kommentar zur StPO (2009) § 135 Rz 37, meinen, dass der Grad des Verdachts in

dringende Tatverdacht ist ein höherer Grad von Wahrscheinlichkeit, dass der Beschuldigte die ihm angelastete Straftat begangen hat. "Verdacht" ist mehr als eine bloße Vermutung. Es ist die Kenntnis von Tatsachen, aus denen nach der Lebenserfahrung auf die Begehung eines Vergehens oder Verbrechens geschlossen werden kann[784]. „Förderung der Aufklärung" iSd § 135 Abs 2 Z 2 und 3 StPO bedeutet die Erhebung des Sachverhalts und die Ermittlung aller zur Überführung aber auch zur Entlastung und Verteidigung des Verdächtigen geeigneten Beweismittel[785].

6.11.4. Legaldefinitionen im Zusammenhang mit der Überwachung von Nachrichten

In § 134 Z 3 StPO wird die Überwachung von Nachrichten definiert als *„das Ermitteln des Inhalts von Nachrichten (§ 92 Abs. 3 Z 7 TKG), die über ein Kommunikationsnetz (§ 3 Z 11 TKG) oder einen Dienst der Informationsgesellschaft (§ 1 Abs 1 Z 2 des Notifikationsgesetzes) ausgetauscht oder weitergeleitet werden."*

§ 134 Z 5 StPO definiert das Ergebnis der Nachrichtenüberwachung als Inhalt übertragener Nachrichten.

6.11.5. Zum Begriff der Nachrichtenüberwachung[786]

Die Überwachung von Nachrichten ist die Ermittlung des Inhalts von Nachrichten, die über ein Kommunikationsnetz oder einen Dienst der Informationsgesellschaft ausgetauscht oder weitergeleitet werden. Der Begriff „Nachricht" wird im TKG 2003 legaldefiniert (siehe auch oben Kapitel 4.4.4). Gem § 92 Z 7 TKG 2003 versteht man unter „Nachricht jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet wird." Hinsichtlich des Nachrichtenbegriffs gilt es auch die Begriffsdefinitionen der EK-Datenschutz-RL zu beachten[787].

---

etwa jenem entspricht, der zur Verhängung der Untersuchungshaft erforderlich ist; *Fuchs,* Grundsatzgedanken und Zweckrationalität in der aktuellen kriminalpolitischen Diskussion, in FS-*Platzgummer* (1995) 425 (434) verlangt, dass Gegenstand des Verdachts sämtliche objektiven und subjektiven Merkmale sein müssen; kritisch zum Begriff des dringenden Tatverdachts *Aichinger,* Neue Fahndungsmethoden zur Bekämpfung organisierter Kriminalität, Diss Wien (1997) 76 ff

784 OGH 15.4.1997, 11 Os 54/97.

785 *Fabrizy,* StPO[10] (2008) § 135 Rz 8.

786 Dieses Kapitel ist teilweise angelehnt an meinen Beitrag in *Zankl,* Auf dem Weg zum Überwachungsstaat? (2009) 193ff.

787 EBRV 128 BlgNR XXII. GP 17.

Die Definition des Nachrichtenbegriffs in der StPO bzw im TKG 2003 setzt nicht notwendigerweise einen bewussten menschlichen Denkvorgang[788] oder eine menschliche Tätigkeit bzw einen menschlichen Empfänger oder Absender[789] voraus. Jedes über einen öffentlichen Kommunikationsdienst ausgetauschte Bit ist Nachricht iSd § 92 Z 7 TKG 2003 und damit iSd § 134 Z 3 StPO. Informationen, die ohne bewusste Handlung des Nutzers eines Endgerätes an einen Server automatisch übermittelt oder von diesem empfangen werden, sind ebenso erfasst wie ein Telefonat oder die Versendung einer E-Mail. Wenn also etwa ein Musikabspielprogramm automatisch im Internet nach CD-Covers zu den auf dem Endgerät gespeicherten Titeln sucht, stellen die automatisch generierte Anfrage und die an das Endgerät übermittelten Bilddateien unter die Überwachungsbefugnis fallende Nachrichten dar.

Keine Nachricht iSd StPO liegt vor, wenn Informationen lediglich abgespeichert oder verarbeitet werden, ohne sie über einen öffentlichen Kommunikationsdienst oder Dienst der Informationsgesellschaft auszutauschen bzw weiterzuleiten. Wird also etwa der Plan eines Terroranschlages als Textdatei auf einem Rechner gespeichert bzw lediglich über ein internes Netzwerk übermittelt, liegt keine Nachricht iSd § 134 Z 3 StPO vor. Wird diese Textdatei in weiterer Folge per E-Mail an einen Mittäter geschickt, darf der Inhalt der Nachricht gem § 135 Abs 3 StPO unter Einhaltung der Bestimmungen der §§ 137 ff StPO ermittelt werden. Vor dem Absenden und nach dem Empfang der Nachricht durch den Empfänger liegt kein Kommunikationsvorgang vor[790]. Das Abspeichern einer empfangenen Nachricht liegt bereits außerhalb des Kommunikationsvorgangs. Informationen, die außerhalb des Kommunikationsvorgangs liegen, können durch Sicherstellung (§ 110 StPO) erlangt werden[791]. Sollen die Daten beim Anbieter des Kommunikationsdienstes oder Dienstes der Informationsgesellschaft erlangt werden, sind die Verfahrensbestimmungen zur Überwachung von Nachrichten einzuhalten, weil der Kommunikationsvorgang dann noch nicht beendet ist[792]. Dies gilt auch dann, wenn die Daten beim Anbieter des

---

788 So auch *Feiler* in *Zankl* (Hrsg), Auf dem Weg zum Überwachungsstaat? (2009) 52ff.

789 *Zanger/Schöll,* Telekommunikationsgesetz[2] (2004) § 92 Rz 32.

790 Vgl auch die Ausführungen des deutschen BVerfG zur reichweite des Fernmeldegeheimnisses: BVerfG 16.6.2009, 2 BvR 902/06, Rz 45; vgl dazu *Klein,* Offen und (deshalb) einfach – Zur Sicherstellung und Beschlagnahme von E-Mails beim Provider, NJW 2009, 2996ff.

791 *Reindl-Krauskopf/Tipold/Zerbes* in *Fuchs/Ratz* (Hrsg), Wiener Kommentar zur StPO (2009) § 134 Rz 50; vgl zur alten Rechtslage ebenso OGH 15.2.2007, 15 Os 20/06i.

792 Anderes wird zur teilweise vergleichbaren deutschen Rechtslage vertreten: BGH 31. 3. 2009, 1 StR 76/09, NJW 2009, 1828 = NStZ 2009, 397; *Graf* in *Graf* (Hrsg), Beck'scher Online.Kommentar zur StPO (2009) § 100a Rz 28.

Kommunikationsdienstes oder Dienstes der Informationsgesellschaft zu einem Zeitpunkt erlangt werden sollen, zu welchem sie bereits abgerufen wurden[793].

Eine Nachricht liegt auch dann vor, wenn die Information nicht über ein Kommunikationsnetz, sondern über einen Dienst der Informationsgesellschaft[794] ausgetauscht oder weitergeleitet wird. Die ausdrückliche Aufnahme von Diensten der Informationsgesellschaft war nötig, da die Definition des Kommunikationsdienstes in § 3 Z 9 TKG 2003 diese ausschließt[795].

Die Befugnis umfasst das Mithören, Aufzeichnen, Abfangen (vgl § 149a StPO alt) oder sonstige Ermitteln des Inhalts von Bild-, Ton- und Textnachrichten, ohne dass es dabei auf die Art der Übertragung ankäme. Die Bestimmungen der StPO enthalten keine Einschränkungen hinsichtlich der zur Durchführung der Überwachung verwendeten Technologie. Die Befugnis des § 135 Abs 3 StPO wurde bewusst technologieneutral ausgestaltet[796]. Aus § 136 Abs 2 StPO lässt sich jedoch erschließen, dass diese Befugnis nicht auch zum Eindringen in Wohnungen oder bestimmte andere durch das Hausrecht geschützte Räumlichkeiten ermächtigt[797]. Dies ist nur im Rahmen der optischen oder akustischen Überwachung von Personen unter den Voraussetzungen des § 136 Abs 2 StPO erlaubt.

6.11.6. Voraussetzungen der Nachrichtenüberwachung[798]

Die Überwachung von Nachrichten ist auf Grund des Verweises von § 135 Abs 3 Z 1 StPO auf § 135 Abs 2 Z 1 StPO in Fällen der Entführung oder Geiselnahme zulässig. Überdies ist sie in den Fällen des § 135 Abs 2 Z 2 StPO zulässig, wenn der Inhaber[799] jener technischen Einrichtung, die Ziel oder Ursprung der

---

793 *Reindl-Krauskopf/Tipold/Zerbes* in *Fuchs/Ratz* (Hrsg), Wiener Kommentar zur StPO (2009) § 134 Rz 53; aA *Zerbes,* Das Urteil des deutschen Bundesverfassungsgerichts zur Online-Durchsuchung und Online-Überwachung, ÖJZ 2008, 834 (837)

794 § 1 Abs 1 Z 2 1. Satz NotifG definiert als Dienst der Informationsgesellschaft „jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung"

795 *Reindl-Krauskopf/Tipold/Zerbes* in *Fuchs/Ratz* (Hrsg), Wiener Kommentar zur StPO (2009) § 134 Rz 44.

796 *Pilnacek/Pleischl,* Das neue Vorverfahren (2005) Rz 584; EBRV 25 BlgNR XXII. GP 186.

797 Ebenso *BMJ/BMI,* Erweiterung des Ermittlungsinstrumentariums zur Bekämpfung schwerer, organisierter und terroristischer Kriminalitätsformen („Online-Durchsuchung") (2008) 25.

798 Dieses Kapitel wurde teilweise angelehnt an meinen Beitrag in *Zankl* (Hrsg), Auf dem weg zum Überwachungsstaat? (2009) 195ff.

799 Zur Frage der Inhaberschaft vgl *Reindl-Krauskopf/Tipold/Zerbes* in *Fuchs/Ratz* (Hrsg), Wiener Kommentar zur StPO (2009) § 135 Rz 27ff.

Nachrichtenübermittlung ist (§ 135 Abs 3 Z 2 iVm § 135 Abs 2 Z 2 StPO), ausdrücklich zustimmt. Diesfalls muss die aufklärende Straftat mit einer Freiheitsstrafe von mindestens sechs Monaten bedroht sein.

Ansonsten ist die Überwachung von Nachrichten zulässig,

- wenn dies zur Aufklärung einer mit mehr als einem Jahr Freiheitsstrafe bedrohten Vorsatztat erforderlich erscheint oder die Aufklärung oder Verhinderung von im Rahmen einer kriminellen oder terroristischen Vereinigung oder einer kriminellen Organisation (§§ 278 bis 278b StGB) begangenen oder geplanten strafbaren Handlungen ansonsten wesentlich erschwert wäre und entweder

  - der Inhaber der technischen Einrichtung, die Ursprung oder Ziele einer Nachrichtenübertragung war oder sein wird, einer der bezeichneten Straftat dringend verdächtig[800] ist (§ 135 Abs 3 Z 3 lit a StPO) , oder
  - aufgrund bestimmter Tatsachen zu erwarten ist, dass eine der Tat dringend verdächtige Person die technische Einrichtung benützen oder mit ihr eine Verbindung herstellen werde (§ 135 Abs 3 Z 3 lit b StPO) oder

- wenn auf Grund bestimmter Tatsachen zu erwarten ist, dass dadurch der Aufenthalt eines flüchtigen oder abwesenden Beschuldigten, der einer mit mehr als einem Jahr Freiheitsstrafe bedrohten Vorsatztat dringend verdächtig ist, ermittelt werden kann (§ 135 Abs 3 Z 4 StPO).

Während die Überwachung gem § 135 Abs 3 Z 3 StPO zur Aufklärung der Straftaten „erforderlich" erscheinen oder die Aufklärung der Straftaten „wesentlich erschwert" sein muss, wird in § 135 Abs 3 Z 2 StPO lediglich gefordert, dass die Aufklärung der Straftat „zu erwarten" ist. Diese unterschiedlichen Formulierungen legen in den Fällen des § 135 Abs 3 Z 3 StPO eine strengere Prüfung der Notwendigkeit der Maßnahme hinsichtlich der Aufklärung bzw Verhinderung der Straftat nahe. Die Maßnahme gem § 135 Abs 3 Z 2 StPO muss zur Aufklärung nicht unbedingt erforderlich, sondern nur verhältnismäßig sein. Dabei ist insbesondere auch die Anzahl der durch die Überwachung betroffenen unbeteiligten Personen zu beachten[801]. Die Überwachung von Nachrichten zu Aufklärungszwecken gem § 135 Abs 3 Z 3 muss hingegen zur Aufklärung nötig sein, dh es dürfen keine Ermittlungsalternativen bestehen, mittels derer dieselben Ergebnisse erzielt werden könnten. Die Überwachung von Nachrichten bei Organisationsdelikten nimmt gewissermaßen eine Mittelstellung ein. Die Aufklärung muss ohne Durchführung der Maßnahme wesentlich erschwert sein, was bedeutet, dass sie

---

[800] Zum dringenden Tatverdacht vgl bereits die obigen Ausführungen zu § 135 Abs 2 Z 1.

[801] *Reindl-Krauskopf/Tipold/Zerbes* in *Fuchs/Ratz* (Hrsg), Wiener Kommentar zur StPO (2009) § 135 Rz 25.

bereits dann zum Einsatz kommen kann, wenn bestehende Ermittlungsalternativen zu einem beträchtlichen Aufwand bzw zu erheblichen zeitlichen Verzögerungen führen würden.

6.11.7. Verfahren[802]

Die Ermittlungsmaßnahmen der Auskunft über Daten einer Nachrichtenübermittlung bzw Nachrichtenüberwachung bedürfen gem § 137 Abs 1 StPO einer Anordnung durch die Staatsanwaltschaft und einer Bewilligung durch das Gericht. Zunächst hat also die Staatsanwaltschaft die gerichtliche Bewilligung gem § 101 Abs 2 StPO zu beantragen. Aufgrund der Bewilligung kann sie dann eine Anordnung gem § 138 Abs 1 StPO an die Kriminalpolizei erlassen, die nicht mit der an den Access-Provider ergehende Anordnung gem § 138 Abs 3 StPO („Betreiberanordnung") zu verwechseln ist. Die Auskunft über Daten einer Nachrichtenübermittlung darf auch für einen vergangenen Zeitraum angeordnet werden, die Überwachung von Nachrichten hingegen nur für zukünftige Zeiträume (§ 137 Abs 3 StPO)[803]. Allerdings vertritt *Reindl-Krauskopf* unter Verweis auf die Schutzrichtung und den Wortlaut des § 135 Abs 3 StPO die Auffassung, dass auch auf Inhaltsdaten aus der Vergangenheit zugegriffen werden darf[804].

Anordnungen (§ 101 Abs 2 StPO) und Bewilligungen (§ 105 StPO) von Maßnahmen nach den §§ 135 Abs 2 und 3 haben gem § 138 Abs 1 StPO zu enthalten:

- die Bezeichnung des Verfahrens
- den Namen des Beschuldigten
- die Tat, deren der Beschuldigte verdächtig ist samt gesetzlicher Bezeichnung
- die Tatsachen, aus denen sich die Erforderlichkeit und Verhältnismäßigkeit ergibt[805]
- die Namen oder sonstigen Identifizierungsmerkmale des Inhabers der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von

---

802 Dieses Kapitel ist teilweise angelehnt an meinem Beitrag in *Zankl* (Hrsg), Auf dem Weg zum Überwachungsstaat? (2009) 204ff.

803 *Fabrizy,* StPO[10] (2008) § 138 Rz 3.

804 *Reindl-Krauskopf* in *Fuchs/Ratz* (Hrsg), Wiener Kommentar zur StPO (2009) §§ 137, 138 Rz 24.

805 Dabei ist der Maßstab, der an die Begründung des Tatverdachts und der Verhältnismäßigkeit anzulegen ist, umso strenger, je weiter der Grundrechtseingriff geht und je mehr unbeteiligte Personen von der Maßnahme betroffen sind: *Reindl-Krauskopf* in *Fuchs/Ratz* (Hrsg), Wiener Kommentar zur Strafprozessordnung (2009) §§ 137, 138 Rz 28.

Nachrichten war oder sein wird, oder der Person, deren Überwachung angeordnet wird,

- die für die Durchführung der Ermittlungsmaßnahme in Aussicht genommenen Örtlichkeiten,
- die Art der Nachrichtenübertragung, die technische Einrichtung und das Endgerät oder die Art der voraussichtlich für die optische und akustische Überwachung zu verwendenden technischen Mittel,
- den Zeitpunkt des Beginns und der Beendigung der Überwachung,

Anbieter iSd § 92 Abs 3 Z 1 TKG 2003[806], dh Access-Provider im hier verstandenen Sinne, und sonstige Dienstanbieter (§§ 13, 16 und 18 Abs 2 Z 3 ECG 2003) sind gem § 138 Abs 2 StPO verpflichtet, Auskunft über Daten einer Nachrichtenübermittlung zu erteilen und an einer Überwachung von Nachrichten mitzuwirken. Hier interessieren nur die Pflichten der Access-Provider. Die mitwirkungsverpflichteten Anbieter sind Adressaten einer gesonderten Anordnung der Staatsanwaltschaft („Betreiberanordnung"[807]), die oben genannte Anordnung gem § 138 Abs 1 StPO geht an die Kriminalpolizei (§ 102 Abs 1 StPO). Die Betreiberanordnung hat auch die gerichtliche Bewilligung anzuführen. Dies wird so ausgelegt, dass der Anordnung keinesfalls die gesamte gerichtliche Bewilligung beizulegen ist, sondern vielmehr nur das Datum und die Geschäftszahl der Bewilligung anzuführen ist. Die Betreiberanordnung hat somit nur jene Angaben zu enthalten, die für die technische Durchführung der Ermittlungsmaßnahme nötig sind[808]. Da Betreiberanordnungen notfalls mit Zwangsmitteln gem § 93 StPO durchgesetzt werden können, ergibt sich auch § 83 Abs 3 StPO, dass diese zu eigenen Handen iSd § 21 Abs 3 ZustellG zuzustellen sind.

Die Ergebnisse einer Ermittlungsmaßnahme sind durch die Staatsanwaltschaft zu prüfen und in Bild- oder Schriftform zu übertragen. Nur die für das weitere Verfahren bedeutsamen und als Beweismittel verwendbaren Teile (§§ 140, 144, 157 Abs 2 StPO) sind zu den Akten zu nehmen (§ 138 Abs 4 StPO).

Gem § 138 Abs 5 StPO hat die Staatsanwaltschaft nach Beendigung einer Ermittlungsmaßnahme nach den §§ 135 Abs 2 und 3 ihre Anordnung und deren gerichtliche Bewilligung dem Beschuldigten und den von der Durchführung der

---

806 § 138 Abs 2 StPO idF des BGBl I 19/2004 verweist – vermutlich auf Grund eines Redaktionsversehens – auf § 92 Abs 1 Z 3 TKG 2003. Die Definition des Begriffs „Anbieter" befindet sich in § 92 Abs 3 Z 1 TKG 2003.

807 *Reindl-Krauskopf* in *Fuchs/Ratz* (Hrsg), Wiener Kommentar zur Strafprozessordnung (2009) §§ 137, 138 Rz 41.

808 *Reindl-Krauskopf* in *Fuchs/Ratz* (Hrsg), Wiener Kommentar zur Strafprozessordnung (2009) §§ 137, 138 Rz 15.

Ermittlungsmaßnahme Betroffenen unverzüglich zuzustellen. Die Zustellung kann jedoch aufgeschoben werden, solange durch sie der Zweck dieses oder eines anderen Verfahrens gefährdet wäre (vgl § 50 Satz 2 StPO). Dabei gilt es jedoch die Verhältnismäßigkeit (vgl § 5 StPO) sowie die sich aus grundrechtlichen Überlegungen ergebenden Schranken zu beachten. Wenn die Ermittlungsmaßnahme später begonnen oder früher beendet wurde, als zu den in § 138 Abs 1 Z 4 StPO genannten Zeitpunkten, ist auch der Zeitraum der tatsächlichen Durchführung mitzuteilen.

§ 139 StPO regelt die Einsichtnahme bzw das Anhören der durch die Ermittlungsmaßnahme erlangten Ergebnisse durch den Beschuldigten bzw sonstige Betroffene. § 140 bestimmt, unter welchen Voraussetzungen bei sonstiger Nichtigkeit die Ergebnisse im weiteren Verfahren als Beweismittel verwendet werden dürfen.

Die Anordnung, Genehmigung, Bewilligung und Durchführung der Nachrichtenüberwachung bzw der Auskunft über Daten einer Nachrichtenübermittlung obliegt gem § 146 StPO zu bestellenden Rechtsschutzbeauftragten nur, wenn diese Maßnahmen gegen Personen gerichtet sind, die gemäß § 157 Abs 1 Z 2 bis 4 StPO berechtigt sind, die Aussage zu verweigern (§ 147 Abs 1 Z 5 StPO).

Schließlich ist noch auf die jedem gem § 106 StPO zustehende Möglichkeit eines Einspruches hinzuweisen. Der Einspruch an das Gericht steht im Ermittlungsverfahren jeder Person zu, die behauptet, durch die Staatsanwaltschaft oder Kriminalpolizei in einem subjektiven Recht verletzt zu sein, weil (1) ihr die Ausübung eines Rechtes nach diesem Gesetz verweigert oder (2) eine Ermittlungs- oder Zwangsmaßnahme unter Verletzung von Bestimmungen dieses Gesetzes[809] angeordnet oder durchgeführt wurde. Gemäß § 106 Abs 1 letzter Satz StPO liegt eine Verletzung eines subjektiven Rechts nicht vor, „soweit das Gesetz von einer bindenden Regelung des Verhaltens von Staatsanwaltschaft oder Kriminalpolizei absieht und von diesem Ermessen iSd Gesetzes Gebrauch gemacht wurde“[810]. Diese an Art 130 B-VG angelehnte Bestimmung wird etwa hinsichtlich der Dauer der angeordneten Überwachungsmaßnahme beachtlich sein.

---

[809] Prüfungsgegenstand ist ausschließlich die StPO: vgl *Pilnacek/Pleischl,* Das neue Vorverfahren (2005) Rz 433; zur Abgrenzung zur Beschwerde gem § 88 SPG vgl *Ennöckl,* Der Rechtschutz gegen sicherheitsbehördliche Maßnahmen, JBl 2008, 409 (417ff); *Klingenbrunner/Bresich,* Telekommunikationsunternehmen: Beschränkter Rechtsschutz gegen Polizeihandeln, ecolex 2008, 475 (476).

[810] Zur Kritik vgl *Luef-Kölbll/Hammerschick/Soyer/Stangl,* Zum Strafprozessreformgesetz, JSt 2009, 9 (14).

6.11.8. Rechtsbehelfe der Access-Provider

Access-Provider haben gem § 106 StPO das Recht auf eine Beschwerde gegen die Anordnung der Staatsanwaltschaft gem § 138 Abs 3 StPO („Betreiberanordnung")[811]. Aus dem Konzept der StPO ergibt sich aber, dass dem Access-Provider weder gegen die gerichtliche Bewilligung, noch gegen die Anordnung der Staatsanwaltschaft gem § 138 Abs 1 StPO ein Rechtsmittel zusteht. Aus der Anordnung durch die Staatsanwaltschaft gem § 138 Abs 1 StPO, deren Adressatin nicht der Provider, sondern die Kriminalpolizei ist (§ 102 StPO), erwachsen dem Access-Provider keine unmittelbaren Verpflichtungen. Diese bekommt er in aller Regel nicht zu Gesicht.

Gegen die gerichtliche Bewilligung stünde gem § 87 Abs 1 StPO nur dann das Rechtsmittel der Beschwerde zu, wenn dem Access-Provider durch den Beschluss unmittelbar Pflichten entstünden oder er hiedurch von einem Zwangsmittel betroffen wäre[812]. Die gerichtliche Bewilligung verpflichtet den Access-Provider jedoch zu nichts, sie ist lediglich Grundlage der Anordnung der Staatsanwaltschaft gem § 138 Abs 1 StPO, deren Adressatin wie erwähnt die Kriminalpolizei ist. Sie wird ihm wie oben gezeigt nach dem Konzept der StPO auch nicht vollinhaltlich übermittelt, vielmehr erfährt er lediglich deren Entscheidungsdatum und Geschäftszahl. Die verpflichtende Wirkung ergibt sich erst aus der an ihn gerichteten Betreiberanordnung gem § 138 Abs 3 StPO, weshalb ihm nur gegen diese ein Einspruch gem § 106 StPO offen steht.

Der Betreiber kann seine Beschwerde darauf stützen, dass die Anordnung der Staatsanwaltschaft gem § 138 Abs 3 StPO ihn in seinem subjektiven Recht verletzt, weil die Ermittlungsmaßnahme unter Verletzung der Bestimmungen der StPO durchgeführt wurde (§ 106 Abs 1 Z 2 StPO). Beschwerden über die Verletzung subjektiver Rechte gem § 106 Abs 1 Z 2 StPO sind auch nach Beendigung des Ermittlungsverfahrens nicht als gegenstandslos zu betrachten (§ 107 Abs 1 StPO e contrario). § 106 StPO soll sicherstellen, dass die in der StPO vorgesehenen Ermittlungsmaßnahmen nur in den vom Gesetz festgelegten Fällen und nur in der vom Gesetz vorgeschriebenen Weise ausgeübt werden sollen[813]. In den Materialien[814] und in

---

811 RV 25 BlgNR XXII. GP, 191; ebenso *Pilnacek/Pleischl,* Das neue Vorverfahren (2005) Rz 604.

812 So zutreffend *Klingenbrunner/Bresich,* Telekommunikationsunternehmen: Beschränkter Rechtsschutz gegen Polizeihandeln? ecolex 2008, 475 (476); *Reindl-Krauskopf* in *Fuchs/Ratz* (Hrsg), Wiener Kommentar zur Strafprozessordnung (2009) §§ 137, 138 Rz 20ff; aA *Tipold,* ebenda, § 87 Rz 16.

813 *E. Fuchs*, Rechtsschutz im Ermittlungsverfahren, ÖJZ 2007, 895 (896); RV 25 BlgNR XXII. GP, 142.

814 RV 25 BlgNR XXII. GP, 142.

der Literatur[815] wird klargestellt, dass das Gericht ausschließlich die Einhaltung der StPO zu überprüfen hat. Dabei ist aber erkennbar nur eine Klarstellung dahingehend gemeint, dass die Prüfung der Einhaltung der Bestimmungen des SPG und der Richtlinienverordnung[816] weiterhin gem § 88 SPG den UVS[817] vorbehalten bleiben soll[818]. Die gerichtliche Zuständigkeit zur Prüfung der Einhaltung datenschutzrechtlicher Bestimmungen, die mit der StPO im Zusammenhang stehen und auf welche die StPO (etwa in § 134 StPO) auch verweist, bleibt dadurch unberührt. Verletzungen der §§ 92ff TKG 2003, die mit Auskünften über Daten einer Nachrichtenübermittlung bzw mit einer Nachrichtenüberwachung im Zusammenhang stehen, dürfen vom Gericht geprüft werden. Eine Zuständigkeit der DSK kommt nur in Frage, soweit die staatsanwaltlichen Anordnungen bzw gerichtlichen Bewilligungen überschritten wurden und das Handeln der Kriminalpolizei darin keine Deckung mehr findet[819]. Die gerichtliche Prüfung im Einspruchsverfahren hat aufgrund einer ex-ante Überprüfung zu geschehen[820]. Fraglich ist, ob dem Einspruch aufschiebende Wirkung zukommt. Obwohl das Gesetz eine derartige Wirkung nicht erwähnt, ist diese jedoch aus einem Größenschluss abzuleiten: Wenn sogar Beschwerden an das OLG gegen die gerichtliche Entscheidung erster Instanz gem § 107 Abs 3 StPO die aufschiebende Wirkung zukommt, wird dies wohl auch für den Einspruch selbst gelten. Wenn Rechtsmittel an das Gericht zweiter Instanz die Durchführung der Maßnahme aufschieben, muss dies mE noch vielmehr für die Dauer des erstinstanzlichen Verfahrens gelten.

Der Einspruch ist bei der Staatsanwaltschaft schriftlich, per Telefax, oder im elektronischen Rechtsverkehr einzubringen oder mündlich zu Protokoll zu geben (§ 84 Abs 2 StPO). Im Einspruch sollte der Access-Provider die angegriffene Maßnahme bezeichnen und im Einzelnen darlegen, weshalb er sich in seinen Rechten verletzt fühlt, dh weshalb die Ermittlungsmaßnahme unter Verletzung von Bestimmungen der StPO

---

815 *Fabrizy,* StPO[10] (2008) § 106 Rz 3.

816 Verordnung des Bundesministers für Inneres, mit der Richtlinien für das Einschreiten der Organe des öffentlichen Sicherheitsdienstes erlassen werden (Richtlinien-Verordnung – RLV), Stammfassung BGBl 266/1993.

817 Nach Ansicht des UVS ist diese Abgrenzung nicht möglich. Die durch die StPO-Reform geschaffene Kompetenzsplitterung verstößt nach Auffassung des UVS gegen Art 83 Abs 2 B-VG, weshalb er im Oktober 2009 einen auf Art 140 Abs 1 iVm Art 129a Abs 3 und Art 89 Abs 2 B-VG gestützten Antrag auf Gesetzesprüfung beim VfGH einbrachte (anhängig unter G 259/09); vgl dazu *Helm,* Anfechtung der §§ 106 f StPO durch den UVS , UVSaktuell 2009, 148ff; ebenfalls zu den Abgrenzungsproblemen *Venier,* Der zahnlose Rechtsschutz der StPO am Beispiel der Hausdurchsuchung, JSt 2009, 156 (159).

818 Zur Abgrenzung vgl *Ennöckl,* Der Rechtschutz gegen sicherheitsbehördliche Maßnahmen, JBl 2008, 409 (417ff).

819 *Kunnert*, Der Ministerialentwurf für eine DSG-Novelle 2010: Ausgewählte Probleme, jusIT 2009, 102 (104); vgl auch *Venier*, Das neue Ermittlungsverfahren: Eine Reform und ihre Mängel, ÖJZ 2009, 591 (593).

820 JAB 406 BlgNR XXII. GP 16.

angeordnet wurde. Zusätzlich hat sie ein bestimmtes Begehren zu enthalten, wie der Rechtsverletzung abgeholfen werden soll. Sie kann sich aber auch auf das Begehren beschränken, festzustellen, dass eine Rechtsverletzung stattfand[821]. Zunächst hat die Staatsanwaltschaft die Möglichkeit dem Einspruch zu entsprechen und so der Rechtsverletzung abzuhelfen. Tut sie dies nicht, oder verlangt der Einspruchswerber dies, hat die Staatsanwaltschaft den Einspruch direkt an das Gericht zur Entscheidung weiterzuleiten. Stellungnahmen der Staatsanwaltschaft und der Kriminalpolizei hat das Gericht dem Einspruchswerber zur Äußerung binnen einer festzusetzenden, sieben Tage nicht übersteigenden Frist zuzustellen (§ 106 Abs 4 StPO).

Unzulässige Einsprüche und solche, denen die Staatsanwaltschaft bereits entsprochen hat, sind vom Gericht zurückzuweisen (§ 107 Abs 1 StPO). Wenn nötig, kann das überprüfende Gericht auch eine mündliche Verhandlung anberaumen und Beweise aufnehmen. Durch die Entscheidung des Gerichts darf sich die Position des Access-Providers nicht verschlechtern[822]. Gegen die Entscheidung des Gerichts steht dann noch ein Rechtsmittel an das OLG offen. Das Oberlandesgericht kann die Behandlung einer Beschwerde ablehnen, es sei denn, dass die Entscheidung von der Lösung einer Rechtsfrage abhängt, der grundsätzliche Bedeutung zukommt, insbesondere weil das Gericht von der Rechtsprechung des Oberlandesgerichts oder des Obersten Gerichtshofs abweicht, eine solche Rechtsprechung fehlt oder die zu lösende Rechtsfrage in der bisherigen Rechtsprechung nicht einheitlich beantwortet wird (§ 107 Abs 3 StPO).

6.11.9. Vertragliche Pflicht zur Ergreifung von Rechtsbehelfen

Nur weil der Access-Provider einen auf § 106 Abs 1 Z 2 StPO gestützten Einspruch gegen die Betreiberanordnung gem § 138 Abs 3 StPO einbringen kann, heißt das noch nicht, dass er dazu auch vertraglich verpflichtet ist.

Der Access-Provider hat im Bereich der Überwachungsmaßnahmen der StPO die Möglichkeit, durch das Rechtsmittel des Einspruchs die Daten des Kunden dauerhaft zu schützen. In der Regel ist es ihnen verwehrt, ihre Kunden über die Auskünfte bzw die Mitwirkung nach den Bestimmungen der §§ 135ff StPO zu informieren. Der Access-Provider hat anders als bei anderen Auskunftsbefugnissen wie etwa im SPG die Möglichkeit, durch die Einbringung eines Rechtsbehelfs mit aufschiebender Wirkung die Verletzung der Privatsphäre seines Kunden endgültig hintanzuhalten, bevor sie

---

821 *Fabrizy,* StPO[10] (2008) § 106 Rz 7; RV 25 BlgNR XXII. GP, 143.

822 *E. Fuchs,* Rechtsschutz im Ermittlungsverfahren, ÖJZ 2007, 895 (900).

eintritt. Das bei anderen Auskunftspflichten gültige Argument (vgl etwa oben Kapitel 6.1.4.3), dass eine vertragliche Pflicht zur Ergreifung von Rechtsschutzmaßnahmen die bereits eingetretene Rechtsgutverletzung nicht mehr rückgängig machen kann, greift hier also nicht.

Die Pflicht zur Einbringung eines Einspruchs wird jedoch regelmäßig aus Zumutbarkeitserwägungen nicht bejaht werden können. Das liegt wiederum daran, dass der Betreiberanordnung nach hM weder die gerichtliche Bewilligung der Maßnahme noch die an die Staatsanwaltschaft gerichtete Anordnung gem § 138 Abs 1 StPO beizulegen sind und der Access-Provider daher kaum eine Möglichkeit hat, die Rechtmäßigkeit der Ermittlungsmaßnahme zu beurteilen. Die an ihn ergehende Betreiberanordnung enthält anders als die Anordnung gem § 138 Abs 1 StPO keine Begründung der Maßnahme, sondern lediglich die zur technischen Umsetzung erforderlichen Angaben[823]. Die Einbringung eines Einspruchs setzt wenigstens die Angabe voraus, weshalb bei der Anordnung einer Maßnahme die Bestimmungen der StPO verletzt wurden, sofern der Rechtsbehelf zum gewünschten Ergebnis führen soll. Da dem Access-Provider die hierfür erforderlichen Informationen regelmäßig fehlen, ist eine Pflicht zur Ergreifung von Rechtsmitteln in den meisten Fällen wohl zu verneinen.

Sollten dem Access-Provider aufgrund eher unwahrscheinlicher Umstände jedoch Informationen über die Gründe der Ermittlungsmaßnahme zukommen, ist er mE zur Überprüfung der Einhaltung der gesetzlichen Vorgaben vertraglich verpflichtet. Sollte also etwa der Betreiberanordnung ausnahmsweise die Anordnung gem § 138 Abs 1 StPO beigelegt werden, ist er mE zur Prüfung verpflichtet, ob die dort angeführte rechtliche Begründung zutrifft. Stellt er etwa fest, dass das Anlassdelikt nicht den gesetzlich erforderten Strafrahmen aufweist, ist er zur Einbringung eines Einspruchs verpflichtet, in welchem er diese Bedenken kurz anzuführen hat.

Weiters wird eine vertragliche Verpflichtung zur Einbringung eines Einspruchs gem § 106 StPO mE dann bestehen, wenn der Access-Provider aus den Umständen die Verletzung von Bestimmungen der StPO erschließen kann. So wird er etwa dann tätig werden müssen, wenn er seit vergleichsweise außergewöhnlich langer Dauer die technischen Einrichtungen außergewöhnlich vieler unbeteiligter Personen zu überwachen hat. Diesfalls liegt der Verdacht der Unverhältnismäßigkeit nahe, weshalb die Maßnahme gegen die StPO (§ 5 StPO) verstößt, was durch den Access-Provider mittels einfachem Schriftsatz geltend zu machen wäre. Er hätte hierfür lediglich die Anordnungen zu bezeichnen und seine Bedenken im Hinblick auf die Verhältnismäßigkeit

---

[823] *Reindl-Krauskopf* in *Fuchs/Ratz* (Hrsg), Wiener Kommentar zur Strafprozessordnung (2009) §§ 137, 138 Rz 15.

anzuführen, weshalb ihm diese Maßnahme, die sonst keinerlei Kosten verursacht, auch zumutbar erscheint.

6.11.10. Vertragliche Pflicht zur Verweigerung der Mitwirkung

Dem Access-Provider drohen im Falle der Weigerung der Mitwirkung Zwangsmaßnahmen und Beugestrafen von bis zu € 10.000. Daher ist bei der Entwicklung von Vertragspflichten zur Verweigerung der Mitwirkung qua ergänzender Vertragsauslegung äußerste Vorsicht geboten. Dennoch gibt es mE Fälle, in denen der Access-Provider seinem Kunden verpflichtet ist, die Mitwirkung an der Maßnahme gegenüber der Kriminalpolizei bzw Staatsanwaltschaft zu verweigern. Dies ist vor allem dann der Fall, wenn er die zur Mitwirkung erforderlichen Daten nicht mehr haben dürfte. Die Daten, auf die im Rahmen der Auskunft über Daten einer Nachrichtenübermittlung zugegriffen werden soll, müssen rechtmäßig gespeichert worden sein[824]. Werden etwa Verkehrsdaten aus der Vergangenheit von ihm verlangt, so hat er die Auskunft zu verweigern, wenn er die gewünschten Daten zwar hat, jedoch legalerweise nicht mehr haben dürfte. Sofern er also etwa gem § 99 Abs 1 TKG 2003 zur Löschung der begehrten Verkehrsdaten verpflichtet gewesen wäre, hat er die Auskunft über diese Daten zu verweigern.

ME ist er weiters zur Verweigerung verpflichtet, wenn die Betreiberanordnung die formalen durch § 138 Abs 3 StPO vorgegebenen Kriterien nicht erfüllt. So hätte er mit der Mitwirkung etwa dann zuzuwarten, wenn die Anordnung die zugrunde liegende gerichtliche Bewilligung nicht anführt.

In derart eindeutigen Fällen ist dem Access-Provider die Verweigerung der Mitwirkung deshalb zuzumuten, weil er letztlich keine Zwangsmaßnahmen bzw Beugestrafen zu befürchten hat. Wenn er nachweisen kann, dass er unter Berücksichtigung der datenschutzrechtlichen Bestimmungen des TKG 2003 (§§ 92ff) gar nicht in der Lage ist, die gewünschte Auskunft zu erteilen, bekommt er spätestens in einem Verfahren über seinen Einspruch gem § 106 StPO Recht.

6.12. Zwischenergebnis

Die einzelnen Auskunftsbestimmungen, die sich an Access-Provider richten, sind höchst unterschiedlich ausgestaltet. Sie dienen unterschiedlichen Zwecken – vom

---

[824] RV 25 BlgNR XXII. GP, 190; *Fabrizy,* StPO[10] (2008) § 138 Rz 4.

Schutz der Urheber oder Mitbewerber bis zur Strafverfolgung oder Landesverteidigung. Die Auskunftsbestimmungen weisen dem Access-Provider unterschiedliche Rollen zu. Im Falle des § 53 Abs 3a SPG wird er etwa von den Sicherheitsbehörden in Pflicht genommen, die ihm gegenüber schon dem Wortlaut der Bestimmung nach keinerlei Begründung anzugeben haben. In derartigen Fällen sind die Prüfpflichten des Access-Providers auf ein Minimum reduziert. Andere Bestimmungen wie § 87b Abs 3 UrhG, der bestimmt, dass der Access-Provider nur auf ein schriftliches und ausreichend begründetes Verlangen hin Auskunft zu erteilen hat, legen hingegen eine eingehende Prüfung des Auskunftsbegehrens nahe. Dabei fällt auf, dass den Staat als Auskunftswerber (SPG, MBG, StPO, etc) gegenüber dem Access-Provider regelmäßig weniger Informationspflichten treffen als Private (UrhG, UWG).

Zusammenfassend lässt sich festhalten, dass die Auskunftsbegehren, die auf den ersten Blick auf sehr ähnliche Daten abzielen, im Detail recht unterschiedlich ausgestaltet sind. Manche ermöglichen beispielsweise nur den Zugriff auf Namen, Anschrift und Teilnehmernummer (FinStrG, MBG, etc), während andere (§ 53 Abs 3a Z 2 und 3 SPG) auch die Auskunft über IP-Adressen gestatten. Teilweise scheint der Gesetzgeber an mögliche Haftungen des Access-Providers gegenüber seinem Kunden zumindest in Ansätzen zu denken (§ 53 Abs 3b SPG), die meisten Regelungen blenden diese Problematik jedoch aus. In diesen Fällen ist der Rechtsanwender in besonderem Maße gefordert, den Bestand und Umfang der Schutzpflichten des Access-Providers zu erforschen.

Soweit sich die Auskunft auf IP-Adressen bzw auf mit IP-Adressen verknüpften Daten bezieht, sind die Vorgaben auf europäischer Ebene, insbesondere die EK-Datenschutzrichtlinie, zu beachten. IP-Adressen sind Verkehrsdaten, die gemäß Art 6 EK-Datenschutzrichtlinie nach Verbindungsbeendigung grundsätzlich – Ausnahmen bestehen etwa zu Verrechungszwecken – unverzüglich löschen sind. Davon kann aufgrund von Ausnahmebestimmungen iSd Art 15 EK-Datenschutzrichtlinie abgegangen werden. Der OGH entschied in der Sache *LSG gegen Tele 2*, dass § 87b Abs 3 UrhG, der keine ausdrückliche Speicheranordnung trifft, keine Bestimmung iSd Art 15 EK-Datenschutzrichtlinie sei. Den Access-Provider trifft die Prüfpflicht, ob die für die Erfüllung des Auskunftsbegehrens erforderlichen (Verkehrs-)Daten bei ihm noch zulässigerweise vorhanden sind. Verneinendenfalls hat er die Erfüllung zu verweigern.

Soweit sich die Auskunft wie etwa im Falle des MBG oder UWG nur auf Stammdaten bezieht, ohne dass hierfür Verkehrsdaten verarbeitet werden müssen, entfällt eine derartige Prüfpflicht, weil Stammdaten stets zulässigerweise gespeichert werden dürfen.

Erweist sich ein Auskunftsbegehren als unvollständig oder sonst mangelhaft, trifft den Access-Provider in manchen Fällen die vertragliche Schutzpflicht,

auf die Vervollständigung des Auskunftsbegehrens zu drängen. Die gilt insbesondere in jenen Fällen, in denen er nur auf ein „schriftliches und begründetes" Verlangen hin Auskunft zu erteilen hat (vgl etwa §§ 90 Abs 6 TKG 2003, 87b Abs 3 UrhG) und ihn diese Pflicht nicht „unverzüglich" trifft.

Soweit der Access-Provider seinen Vertragspartner über die Auskunftserteilung informieren kann und dies auch tut, trifft ihn schon deshalb keine Pflicht, für seinen Kunden Rechtsmittel zu ergreifen. In jenen Fällen, in denen ihm dies verweigert ist (etwa bei Auskunftsbegehren nach der StPO) stellt sich die Frage nach einer Pflicht, sich mittels Rechtbehelfen gegen das Auskunftsbegehren zu stellen. Obwohl es manche Auskunftsbestimmungen erlauben würden, dass der Access-Provider vor Auskunftserteilung gegen das Auskunftsbegehren ein Rechtsmittel mit zT auch aufschiebender Wirkung einbringen kann, ist ihm dies mE in keinem Fall zumutbar. In den meisten Fällen – wie etwa im SPG – könnte er die Rechtsbehelfe jedoch ohnedies nur im Nachhinein und somit erst nach der bereits erfolgten Beeinträchtigung der Privatsphäre einbringen. Dieses Argument und die wirtschaftliche Unzumutbarkeit sprechen daher im Ergebnis eindeutig gegen eine derartige Schutzpflicht.

7. Resümee

Die Rechtsordnung beinhaltet eine Reihe von Bestimmungen, die Access-Provider zur Auskunft bzw Mitwirkung verpflichten. Die in dieser Arbeit abgehandelten Bestimmungen haben gemein, dass sie auf die Ermittlung personenbezogener Daten abzielen und somit einen Eingriff in die Privatsphäre des Kunden des Access-Providers darstellen. Der Schutz der Privatsphäre ergibt sich zum einen aus gesetzlichen Bestimmungen, die vor allem im TKG 2003 und im DSG 2000 zu finden sind. Zum anderen ist der Access-Provider seinem Kunden überdies auch vertraglich zur Wahrung seiner Privatsphäre verpflichtet.

Das TKG 2003 unterscheidet in Anlehnung an die EK-Datenschutzrichtlinie zwischen verschiedenen Datenkategorien, für die jeweils unterschiedliche Schutzbestimmungen bestehen. So ist die Vertraulichkeit des Inhalts von Nachrichten besonders gut geschützt und ein Eingriff nur *„aufgrund eines richterlichen Befehls in Gemäßheit bestehender Gesetze*" zulässig (Art 10a StGG). Verkehrsdaten wie etwa IP-Adressen genießen nach einem (mE zutreffenden) Teil der Lehre und Rechtsprechung zwar nicht einen ganz so hohen Schutz, werden vom TKG aber stärker geschützt, als bloße Stammdaten wie etwa Name und Anschrift einer Person. Wird im Zuge der Erfüllung eines Auskunftsbegehrens zwischen Daten unterschiedlich hoher Schutzkategorien ein Zusammenhang hergestellt, sind mE stets die Bestimmungen der jeweils höheren Schutzkategorie zu beachten. Ist beispielsweise der Inhalt einer Nachricht bekannt (Inhaltsdaten) und soll der Name des Senders (Stammdaten) vom Access-Provider bekannt gegeben werden, ist ein richterlicher Befehl nötig, obwohl nur ein Stammdatum beauskunftet wurde. Dies ergibt sich aus teleologischen Erwägungen zu der Bestimmung, die das höher bewertete Datum schützt. Im genannten Beispiel wird durch die Auskunft bekannt, wer eine Nachricht mit bestimmtem Inhalt verschickte – eine Information die das Fernmeldegeheimnis mE auch schützen will.

Die Bestimmungen des TKG 2003 zum Datenschutz beruhen weitestgehend auf der EK-Datenschutzrichtlinie und präzisieren die aus dem allgemeinen Datenschutzrecht bekannten Grundsätze auf dem Sektor der elektronischen Kommunikation. Zwei wichtige Prinzipien des Datenschutzrechts sind etwa der Grundsatz, dass jeder grundsätzlich über die ihn betreffenden Datenverwendungen umfassend im Bilde sein soll oder das Zweckbindungsprinzip. Nach Letzterem dürfen Daten nur für jene Zwecke verwendet werden, zu denen sie ursprünglich angelegt wurden. Diese Prinzipien sind bei der Entwicklung vertraglicher Schutzpflichten des Access-Providers zu beachten.

Die vorliegende Arbeit hat einige Auslegungsschwierigkeiten aufgezeigt und einer Lösung zuzuführen versucht, die sich bei der Interpretation von Bestimmungen des

TKG 2003 oder aus dem Regelungszusammenhang zu Auskunftsbestimmungen ergeben. So sind die für die meisten Auskunftsbegehren benötigten Verkehrsdaten in der Mehrzahl der Fälle unmittelbar nach Verbindungsbeendigung zu löschen oder zu anonymisieren, es sei denn, sie werden für Verrechnungszwecke benötigt. Ausnahmebestimmungen sind möglich, müssen jedoch, um als Ausnahmebestimmungen iSd Art 15 EK-Datenschutzrichtlinie zu gelten, nach der aktuellen Entscheidung des OGH in der Sache *LSG gegen Tele 2* eine ausdrückliche Speicheranordnung treffen. Die vorliegende Arbeit zeigt etwa, weshalb Auskunftsbestimmungen wie jene des SPG, die keine ausdrückliche Speicheranordnung treffen, dennoch als Ausnahmebestimmungen iSd Art 15 EK-Datenschutzrichtlinie gelten können und somit nicht leer laufen.

Die den Access-Provider treffenden Schutzpflichten hinsichtlich der Privatsphäre seines Kunden lassen sich mittels ergänzender Vertragsauslegung unter Orientierung am Prinzip von Treu und Glauben konstruieren. Dabei wurden die erkennbaren Wertungen des Gesetz- bzw Richtliniengebers auf dem Gebiet des Datenschutzrechts berücksichtigt und der Vertragsergänzung zugrunde gelegt. Eine der wichtigsten in dieser Arbeit entwickelten vertraglichen Pflichten ist wohl die Benachrichtigungspflicht des Access-Providers. Soweit es ihm nicht verboten ist oder er das Risiko eingeht, sich straf- bzw haftbar zu machen, hat er seinen Kunden über die Erfüllung eines Auskunftsbegehrens zu informieren. Die Informationspflicht bringt für den Access-Provider keinen hohen Aufwand mit sich und ist daher wirtschaftlich zu rechtfertigen. Sie ergibt sich zudem aus einer – soweit ersichtlich – bislang noch nie erwogenen Auslegung des § 96 Abs 3 TKG 2003. Die Informationspflicht entfällt dort, wo den Auskunftswerber eine eindeutige Pflicht zur Information des Betroffenen trifft wie in der StPO. Sie entspricht dem erwähnten Prinzip, dass der Betroffene stets über die ihn betreffenden Datenverwendungen Bescheid wissen soll um seine Rechte wahrnehmen zu können. Eine Pflicht, sich im Interesse des Kunden gegen Auskunftsbegehren mittels Rechtsbehelfen zur Wehr zu setzen, trifft den Access-Provider aus Zumutbarkeitsgründen nicht. Je nachdem, wie die Begründungspflichten des Auskunftswerbers dem Gesetz nach beschaffen sind, sehen auch die Prüfpflichten des Access-Providers hinsichtlich des Auskunftsbegehrens unterschiedlich aus. Soweit das Gesetz eine Begründung des Auskunftsbegehrens verlangt, hat der Access-Provider das Auskunftsbegehren auf dessen Vollständigkeit zu prüfen und die Auskunft bzw Mitwirkung nötigenfalls zu verweigern. Weiters bestehen Verweigerungspflichten in jenen Fällen, in denen der Access-Provider die zur Auskunftserfüllung erforderlichen Daten zwar de facto noch vorrätig hat, sie aufgrund der Bestimmungen des TKG 2003 jedoch bereits hätte löschen müssen.

Die gezeigten Schutzpflichten werden vom Access-Provider geschuldet wie jede andere vertragliche Pflicht. Diese Arbeit brachte das Ergebnis, dass für das Institut der positiven Vertragsverletzungen und dazu geltende Sonderregelungen im Gefüge des

ABGB kein Platz ist. Das Institut der positiven Vertragsverletzung geht auf eine Erfindung des deutschen Juristen *Hermann Staub* zu Beginn des vergangenen Jahrhunderts zurück, der eine Lücke im BGB vermutete und diese mittels Analogie schloss. Wie gezeigt werden konnte, besteht diese Lücke weder im BGB und noch weniger im ABGB, weshalb die Verletzung von Schutzpflichten unter das positive Schadenersatz- und Leistungsstörungsrecht subsumiert werden kann. Die Schutzpflichten können stets nur auf eine endgültige (Unmöglichkeit) oder vorübergehende Art (Verzug) verletzt werden. Daher stehen bei Schutzpflichtverletzungen mE entgegen der hM grundsätzlich die in den §§ 918ff ABGB statuierten Rechtsbehelfe zu. Das gilt insbesondere auch für Rücktrittsrechte. Diese können jedoch ausnahmsweise ausscheiden, sofern sich deren Ausübung gemessen an der Schwere der Schutzpflichtverletzung als missbräuchlich erweist (§ 1295 ABGB). Die Schutzpflichten (etwa zur Benachrichtigung) können mE auch gesondert eingeklagt werden, sofern sie ausreichend bestimmt und fällig sind. Sofern die Verletzung der Schutzpflichten zu Vermögensschäden führt, ist der Access-Provider zu deren Ersatz verpflichtet. Die Prüfung von Ersatzansprüchen kann jedoch in einigen Fällen – etwa wenn die im Vermögen des Kunden eingetretene Vermögensminderung die Folge einer gegen ihn verhängten Strafe darstellt – ergeben, dass kein Rechtswidrigkeitszusammenhang vorliegt. Bei besonders erheblichen Verletzungen der Privatsphäre besteht gem § 1328a ABGB auch ein Anspruch auf den Ersatz des dadurch erlittenen immateriellen Schadens.

Für die Zukunft bleibt mit Spannung die Umsetzung der Vorratsdatenspeicherungsrichtlinie zu erwarten. Der aktuelle vom Ludwig Boltzmann Institut für Menschenrechte im Auftrag des BMVIT erarbeitete Umsetzungsentwurf ist zu begrüßen, da er die Interessen der Access-Provider und der Betroffenen bestmöglich schützt und miteinander in Ausgleich bringt. Er ist vom Grundgedanken getragen, dass jene Daten, die künftig auf Vorrat zu speichern sind, auch nur für die in der Vorratsdatenspeicherungsrichtlinie genannten Zwecke zur Verfügung stehen sollen. Daten, die künftig als Vorratsdaten zu speichern und nach dem Umsetzungsentwurf auch als solche zu kennzeichnen sind, dürfen daher nicht für Auskunftsbegehren außerhalb der StPO verwendet werden. Die einzige Ausnahme betrifft Standortdaten gefährdeter Personen. Sollte die Richtlinie tatsächlich in dieser Weise umgesetzt werden, wird sich die Situation der Auskunftswerber im Bezug auf die meisten Auskunftsbestimmungen nicht verändern, da ihnen ein Zugriff auf die Vorratsdaten verwehrt bleiben wird.

Literaturverzeichnis

Aichinger, Neue Fahndungsmethoden zur Bekämpfung organisierter Kriminalität, Diss Wien (1997)

Ballerstedt, Zur Haftung für culpa in contrahendo bei Geschäftsabschluss durch Stellvertreter, AcP 1950/51, 501

Bar, Vertrauenshaftung ohne Vertrauen – Zur Prospekthaftung bei der Publikums-KG in der Rechtsprechung des BGH, ZGR 1983, 476

Bar, "nachwirkende" Vertragspflichten, AcP 1979, 452

Bär, Anm zu BVerfG, Beschluss vom 11.3.2008 – 1 BvR 256/08 (Einstweilige Anordnung zur teilweisen Aussetzung der Regelung zur Vorratsdatenspeicherung), MMR 2008, 303

Barbist, Auskunftspflicht: Streit Provider vs Musikindustrie Realoaded – Das EuGH Urteil in Sachen Promusicae, MR 2007, 415

Barta, Zivilrecht, Wien (2000)

Bauer/Reimer (Hrsg), Handbuch Datenschutzrecht, Wien (2009)

Bergauer, Auskunftspflicht der Access-Provider: Zwei kontroverse Beschlüsse des OLG Wien, RdW 2005, 467

Berka, Lehrbuch Grundrechte, Wien (2000)

Berka, Medienfreiheit und Persönlichkeitsschutz, Wien (1982)

Blomeyer, Allgemeines Schuldrecht[3], Berlin (1964)

Blume/Hammerl, Kommentar zum E-Commerce-Gesetz, Wien (2002)

BMI (Hrsg), Der Rechtsschutzbeauftragte in Österreich, Wien (2004)

Böhm, Die "Altlastensanierung" als Problem der ergänzenden Vertragsauslegung bzw des Wegfalls der Geschäftsgrundlage (II), ÖZW 1990, 104

Brenn, E-Commerce-Gesetz, Wien (2002)

Bresich/Pesta, Haftung für offenes WLAN? RdW 2007, 647

Büchner/Ehmer/Geppert/Kerkhoff/Piepenbrock/Schütz/Schuster, Beck'scher TKG Kommentar, München (2000)

Burkert, Die Konvention des Europarats zum Datenschutz, CR 1988, 751

Bydlinski F., Juristische Methodenlehre und Rechtsbegriff, Wien (1982)

Bydlinski F., Juristische Methodenlehre und Rechtsbegriff[2], Wien (1991)

Bydlinski F., Vertragliche Sorgfaltspflichten zugunsten Dritter, JBl 1960, 359

Bydlinski F., Bemerkungen über Grundrechte und Privatrecht, ÖZöffR 1962/63, 423

Bydlinski F., Probleme der Schadensverursachung: nach deutschem und österreichischem Recht, Stuttgart (1964)

Bydlinksi P., Grundzüge des Privatrechts[2], Wien (1994)

Canaris, Die Feststellung von Lücken im Gesetz, Berlin (1964)

Canaris, Ansprüche wegen "positiver Vertragsverletzung" und "Schutzwirkung für Dritte" bei nichtigen Verträgen, JZ 1965, 475

Chadioan, Stille Nacht, heimliche Macht Zur SPG-Novelle 2007 und der Erweiterung sicherheitspolizeilicher Ermittlungsbefugnisse, juridikum 2008, 130

Crome, System des Deutschen Bürgerlichen Rechts, Tübingen (1902)

Czychowski, Auskunftsansprüche ggü Internetzugangsprovidern "vor" dem 2. Korb und "nach" der Enforcement-Richtlinie der EU, MMR 2004, 517

Czychowski/Nordemann, Vorratsdaten und Urheberrecht – Zulässige Nutzung gespeicherter Daten, NJW 2008, 3095

Damjanovic/Holoubek/Kassai/Lehofer/Urbanitsch, Handbuch des Telekommunikationsrechts, Wien (2006)

Daum, EuGH zur Auskunftspflicht von Internetserviceprovidern, ecolex 2008, 200

Dernburg, Über das Rücktrittsrecht des Käufers bei positiven Vertragsverletzungen, JZ 1903, 1

Dohr/Weiss/Pollirer/Knyrim, Datenschutzrecht[2], Wien (2002) Loseblattausgabe

Dölle, Außergesetzliche Schuldpflichten, ZgesStW 1943, 67

Dullinger, Kommentar zu OGH 4. 3. 1986, 14 Ob 12/86, ZAS 1987, 93

Duschanek, Neuerungen und offene Fragen im Datenschutzgesetz 2000, ZfV 2000, 526

Eckhardt, Neue Entwicklungen der Telekommunikationsüberwachung, CR 2002, 770

Edthaler/Schmidt, Auskunft über IP-Adressen im Strafverfahren, MR 2008, 220

Ehrlich, Über Lücken im Rechte, JBl 1988, 447

Ehrenzweig, Das Recht der Schuldverhältnisse[6], Wien (1920)

Ehrenzweig/Mayerhofer, Das Recht der Schuldverhältnisse[3], Wien (1986)

Enneccerus/Lehmann, Lehrbuch des Bürgerlichen Rechts II, Marburg (1932)

Enneccerus/Nipperdey, Lehrbuch des Bürgerlichen Rechts I/1[14], Tübingen (1952)

Ennöckl, Der Rechtsschutz gegen sicherheitsbehördliche Maßnahmen, JBl 2008, 409

Ermacora, Handbuch der Grundfreiheiten und Menschenrechte, Wien (1963)

Esser, Schuldrecht, Karlsruhe (1949)

Esser/Schmidt, Schuldrecht I/1[7], Heidelberg (1992)

Esser/Schmidt, Schuldrecht I/2[7], Heidelberg (1993)

Faivre, Der Telekommunikationsvertrag, Bern (2005)

Fallenböck, Der Einsatz von Location Based Services – eine erste Analyse rechtlicher Problemfelder, MR 2002, 182

Feiel, Datenspeicherung auf Vorrat und Grundrechtskonformität, jusIT 2008, 97

Fellner, Finanzstrafgesetz, Enns (1995)

Flora, Auskunfts- und Überwachungspflichten im neuen Strafverfahren, ÖJZ 2008, 35

Fox, Der IMSI-Catcher, DuD 2002, 212

Freitag, Schlechterfüllung und Schlechterbringung – Zur Systematik der "positiven Vertragsverletzung", Breslau (1932)

Frey/Rudolph, EU-Richtlinie zur Durchsetzung der Rechte des geistigen Eigentums, ZUM 2004, 522

Fromm/Nordemann, Urheberrecht[9], Stuttgart (1998)

Frost, "Vorvertragliche" und vertragliche Schutzpflichten, Berlin (1981)

Frowein/Peukert, EMRK-Kommentar[2], Kehl am Rhein (1996)

Frowein/Peukert, EMRK-Kommentar[3], Kehl am Rhein (2009)

Fuchs E., Rechtsschutz im Ermittlungsverfahren, ÖJZ 2007, 895

Fuchs H., Grundsatzgedanken und Zweckrationalität in der aktuellen kriminalpolitischen Diskussion, in *Fuchs H./Brandstetter* (Hrsg), FS Platzgummer, Wien (1995) 425

Fuchs H./Ratz, Wiener Kommentar zur StPO, Wien (2002)

Funk, Der unvollendete Rechtsstaat, in *Akyürek/Baumgartner/Jahnel/Lienbacher* (Hrsg), Verfassung in Zeiten des Wandels, Symposion zum 60. Geburtstag von Heinz Schäffer, Wien (2002) 199

Funk/Krejci/Schwarz, Zur Registrierung von Ferngesprächsdaten durch den Dienstgeber, RdA 1984, 285

Gercke, Rechtliche Probleme durch den Einsatz des IMSI-Catchers, MMR 2003, 453

Gerhardt, Die Haftungsfreizeichnung innerhalb des gesetzlichen Schuldverhältnisses, JZ 1970, 535

Gerhardt, Der Haftungsmaßstab im gesetzlichen Schuldverhältnis (Positive Vertragsverletzung, culpa in contrahendo), JuS 1970, 597

Gernhuber, Handbuch des Schuldrechts VIII, Tübingen (1989)

Gitter/Schnabel, Die Richtlinie zur Vorratsspeicherung und ihre Umsetzung in das nationale Recht, MMR 2007, 411

Glöckner, Die Positive Vertragsverletzung: die Geburt eines Rechtsinstituts, Frankfurt a.M. (2006)

Goldmann/Lilienthal, Das Bürgerliche Gesetzbuch systematisch dargestellt I[2], Berlin (1903)

Grabenwarter, Die Europäische Menschenrechtskonvention[3], München (2008)

Graf, Vertrag und Vernunft, Wien (1997)

Gschnitzer, Schuldrecht. Besonderer Teil und Schadenersatz, Wien (1963)

Gschnitzer/Faistenberger, Österreichisches Schuldrecht, Allgemeiner Teil[2], Wien (1991)

Güldner, Die Beweislast für Verschulden bei der Haftung für positive Vertragsverletzung, Verschulden beim Vertragsabschluss und nachvertragliches Verschulden, Düsseldorf (1965)

Haedicke, Informationsbefugnisse des Schutzrechtsinhabers im Spiegel der EG-Richtlinie zur Durchsetzung der Rechte des geistigen Eigentums, in *Ohly/Bodewig/Dreier/Götting/Haedicke/Lehmann* (Hrsg), Perspektiven des Geistigen Eigentums und Wettbewerbsrecht, FS Gerhard Schricker, München (2005) 15

Hahn, AGB in TK-Dienstleistungsverträgen, MMR 1999, 586

Haidinger/Schachter, Urheberrechtlicher Auskunftsanspruch im Spannungsverhältnis zum Datenschutz – Anlassfälle Promusicae und MediaSentry, jusIT 2008, 59

Handstanger/Okresek, Sicherheitsverwaltung und MRK – Rechtsprechung der Organe der MRK zum Handeln der Sicherheitspolizei, ÖJZ 1995, 251

Hasberger, Zum Kostenersatz für die Telekommunikationsüberwachung, MR 2008, 58

Hasberger, Die providerinterne Auswertung von Verkehrsdaten und Datenschutz, MR 2010, 23

Hasberger/Schönhart, Die Haftung von Telekom-Unternehmen für fremdes Fehlverhalten, MR 2004, 297

Hasenöhrl, Das österreichische Obligationenrecht[2], Wien (1892)

Hauer, Sicherheitspoliziegesetz[2], Wien (2001)

Hauer/Keplinger/Kreutner, Militärbefugnisgesetz, Linz (2005)

Hauer/Keplinger, Befugnisse der Organe des öffentlichen Sicherheitsdienstes, Wien (2007)

Hauer/Keplinger, Sicherheitspolizeigesetz – Polizeiausgabe[10], Wien (2008)

Heck, Zur Entstehungsgeschichte des § 276, AcP 1933, 259

Hellmich, Location Based Services – Datenschutzrechtliche Anforderungen, MMR 2002, 152

Helm, Anfechtung der §§ 106 f StPO durch den UVS Wien, UVSaktuell 2009, 148

Helmich, Schadenersatz bei Eingriffen in die Privatsphäre, ecolex 2003, 888

Himmelschein, Erfüllungszwang und Lehre von den positiven Vertragsverletzungen, AcP 1932, 308

Hinteregger, Der Schutz der Privatsphäre durch das österreichische Schadenersatzrecht – de lege lata et de lege ferenda, in *Koziol/Spier* (Hrsg), Liber Amicorum Pierre Widmer, Wien (2003) 143

Hochher, Auskunftspflichten im Abgaben- und im Finanzstrafverfahren, FJ 1999, 289

Hoeren, Vorratsdaten und Urheberrecht – Keine Nutzung gespeicherter Daten, NJW 2008, 3099

Honsell, Aktuelle Probleme der Sachmängelhaftung, JBl 1989, 205

Kopf/Kathrein, 1811-2011: 200 Jahre ABGB – SPG-Novelle: Auskunft über Teilnehmer- und Standortdaten, ÖJZ 2008/5

Jahnel, Datenschutz im Internet, ecolex 2001, 84

Jenny, Eile mit Weile – Vorratsdatenspeicherung auf dem Prüfstand, CR 2008, 282

Kahlert, Urheberrecht kontra Datenschutz, ELR 2008, 282

Karner/Koziol, Der Ersatz ideellen Schadens im österreichischen Recht und seine Reform, 15. ÖJT Band II/1, Wien (2003)

Kassai, Der Einsatz von Location Based Services – eine erste Analyse rechtlicher Problemfelder, MR 2004, 433

Kerschner, Probleme der Sachmängelhaftung. Oder: Das ABGB ist tot – Es lebe das BGB! JBl 1989, 541

Kerschner, Wegfall der Geschäftsgrundlage bei unwiderruflichen Sozialleistungen, wbl 1988, 211

Klang/Gschnitzer, ABGB IV/2^2, Wien (1978)

Klang/Gschnitzer, Kommentar zum Allgemeinen Bürgerlichen Gesetzbuch^2 IV/1, Wien (1968)

Klauser/Kodek, ZPO 16.01, Wien (Online-Kommentar, Stand April 2010)

Klein, Offen und (deshalb) einfach – Zur Sicherstellung und Beschlagnahme von E-Mails beim Provider, NJW 2009, 2996

Klingenbrunner, Telekommunikationsunternehmen: Beschränkter Rechtsschutz gegen Polizeihandeln? ecolex 2008, 475

Klug, Juristische Logik^3, Berlin (1966)

Köpcke, Typen der positiven Vertragsverletzung, Stuttgart (1965)

Kosta/Dumortier, The Data Retention Directive an the Principles of European data protection legislation, MR-Int 2007, 130

Koziol, Delikt, Verletzung von Schuldverhältnissen und Zwischenbereich, JBl 1994, 209

Koziol, Österreichisches Haftpflichtrecht I^3, Wien (1997)

Koziol, Österreichisches Haftpflichtrecht II, Wien (1975)

Koziol, Österreichisches Haftpflichtrecht II^2, Wien (1984)

Kreß, Lehrbuch des Allgemeinen Schuldrechts, München (1929)

Krückmann, Unmöglichkeit und Unmöglichkeitsprozess, AcP 1907, 1

Kucsko, Urheber.recht, Wien (2008)

Kuderna, Die Zustimmung zur Übermittlung von Daten, RdA 1992, 412

Kunnert, Der sicherheitspolizeiliche Griff nach Telekommunikationsdaten. Möglichkeiten – Grenzen – Kritik, in *Jahnel* (Hrsg), Datenschutzrecht und E-Government: Jahrbuch 2008, Wien (2008) 83

Kunnert, Der Ministerialentwurf für eine DSG-Novelle 2010: Ausgewählte Probleme, jusIT 2009, 102

Lachmayer, Demokratischer Überwachungsstaat im rechtsstaatlichen Spannungsfeld, juridikum 2006, 30

Laga/Sehrschön, E-Commerce-Gesetz, Wien (2002)

Lange, Wörterbuch zur inneren Sicherheit, Wiesbaden (2006)

Larenz, Lehrbuch des Schuldrechts I, München (1953)

Larenz, Lehrbuch des Schuldrechts I[13], München (1982)

Larenz, Culpa in contrahendo, Verkehrssicherungspflicht und "sozialer Kontakt", MDR 1954, 515

Larenz, Methodenlehre der Rechtswissenschaft[5], Berlin (1983)

Lehmann, Die positiven Vertragsverletzungen, AcP 1905, 60

Lenhoff, Positive und negative Vertragsverletzungen gegenseitiger Verträge, ZBl 1917, 385

Leonhard, Allgemeines Schuldrecht des BGB, München (1929)

Lepuschitz/Schindler, Das österreichische Sicherheitspolizeigesetz[5], Wien (2008)

Lichtenberger/Ruhle, Das novellierte TKG – Basis für wirksamen Wettbewerb auf den österreichischen Kommunikationsmärkten? ecolex 2003, 812

Luef-Kölbl/Hammerschick/Soyer/Stangl, Zum Strafprozessreformgesetz, JSt 2009, 9

Lust, Telekommunikationsrecht im Überblick, Wien (2004)

Machcek, Der Rechtsschutzbeauftragte nach der StPO: Weisungsfreier Sachwalter des Rechtsschutzes oder weisungsgebunden eine Horrorvision, AnwBl 2004, 90

Machacek, Die Bekämpfung der organisierten Kriminalität in Österreich, ÖJZ 1998, 553

Maier, Strafrecht – Kriegsrecht – Ausnahmezustand? Der Rechtsstaat vor der Hausforderung des Terrorismus, JRP 2006, 27

Majchrzak, Der Auskunftsanspruch nach § 14a UWG, ÖBl 2008, 180

Majchrzak/Wiltschek, Die UWG-Novelle 2007, ÖBl 2008, 4

Manssen, Telekommunikations- und Multimediarecht, Berlin (2008)

Marhold, Kommentar zu OGH 24. 10. 1978, 4 Ob 91/78, ZAS 1979, 177

Matzka/Koschy, Datenschutzrecht für die Praxis, Wien (1986)

Mayer, Willensmängel im öffentlichen Recht, ecolex 1992, 812

Mayer-Maly, Das Rechtsverhältnis zwischen Arbeitnehmern, in Tomandl (Hrsg), Innerbetriebliche Arbeitnehmerkonflikte aus rechtlicher Sicht, Wien (1977) 59

Mayer-Maly, Die Bedeutung des faktischen Parteiwillens für den hypothetischen, in *Jakobs/Knobbe-Keuk/Picker/Wilhelm* (Hrsg), FS zum 70. Geburtstag von Werner Flume, Köln (1978) 621

Mayer-Schönberger/Brandl, Datenschutzgesetz, Wien (2006)

Mayer-Schönberger/Zeger/Kronegger, Auf dem Weg nach Europa: Zur Novellierung des Datenschutzgesetzes, ÖJZ 1998, 244

McGuire, Beweismittelvorlage und Auskunftsanspruch nach der Richtlinie 2004/48/EG zur Durchsetzung der Rechte des geistigen Eigentums, GRURInt 2005, 15

Medicus, Grenzen der Haftung für culpa in contrahendo, JuS 1965, 209

Meinhard, Schadenersatz bei Verletzung der Privatsphäre, RZ 2004, 33

Meinhof, Die Dialektik von Revolution und Konterrevolution, in *Internationales Komitee zur Verteidigung politischer Gefangener in Westeuropa* (Hrsg), Letzte Texte von Ulrike (1976) 57

Merkel, Die Rechteinheit des österreichischen Staates. Eine staatsrechtliche Untersuchung auf Grund der Lehre von der lex posterior, AöR 1918, 56

Mommsen, Beiträge zum Obligationenrecht, 1. Abtheilung, Die Unmöglichkeit der Leistung in ihrem Einfluß auf obligatorische Verhältnisse, Braunschweig (1853)

Mondel, Die Regelungsschwerpunkte des E-Commerce-Gesetzes, Diss Wien (2002)

Müller, Die Haftung des Stellvertreters bei culpa in contrahendo und positiver Vertragsverletzung, NJW 1969, 2169

Neubauer, Zur Haftung und Auskunftsverpflichtung von Providern – Aktuelles zu Unterlassungs- und Auskunftspflichten in Österreich mit einem Vergleich zur aktuellen Rechtslage in Deutschland im Zivil-und Strafrecht, MR-Int 2008, 25

Nordemann/Dustmann, To Peer Or Not To Peer – Urheberrechtliche und datenschutzrechtliche Fragen der Bekämpfung der Internet-Piraterie, CR 2004, 380

Oertmann, Das Recht der Schuldverhältnisse[2], Berlin (1906)

Öhlinger, Auslegung öffentlichen Rechts, JBl 1971, 284

Öhlinger, Auskunftsbefugnisse sowie Auskunfts- und Verschwiegenheitspflichten der Österreichischen Nationalbank, ÖJZ 1991, 65

Otto/Seitlinger, Die "Spitzelrichtlinie", MR 2006, 227

Parschalak/Otto/Weber/Zuser, Telekommunikationsrecht, Wien (2006)

Pfarl, Gefunden! LBS im Mobilfunknetzbereich, ecolex 2005, 569

Picker, Vertragliche und deliktische Schadenshaftung, JZ 1987, 1041

Pilnacek/Pleischl, Das neue Vorverfahren, Wien (2005)

Pisko, Die subjektiven Voraussetzungen des Rücktrittsrechts nach § 918 ABGB, JBl 1920, 241

Pisko, Lehrbuch des österreichischen Handelsrechts, Wien (1923)

Plasser, Lauterkeitsrechtlicher Auskunftsanspruch auch für Mitbewerber nach der UWG-Nov 2007, ÖBl 2008, 183

Pletzer, Recht auf kein Kind? – Überlegungen anlässlich der jüngsten Entscheidung des OGH zu "wrongful birth", JBl 2008, 183

Pracher, Datenschutz in der Telekommunikation, in *Forgó/Feldner/Witzmann/Dieplinger* (Hrsg) Probleme des Informationsrechts, Wien (2003)

Pürstl/Zirnsack, Sicherheitspolizeigesetz, Wien (2005)

Raape, Die Beweislast bei positiver Vertragsverletzung, AcP 1942, 217

Rabel, Das Recht des Warenkaufs, Berlin (1936)

Raschauer/Wessely, Militärbefugnisgesetz, Wien (2007)

Reindl, Die nachträgliche Offenlegung von Vermittlungsdaten des Telefonverkehrs im Strafverfahren („Rufdatenrückrfassung"), JBl 1999, 791

Reischauer, Das Persönlichkeitsrecht auf Achtung des Fernsprechgeheinisses (§ 16 ABGB) und seine Bedeutung für das Dienstverhältnis, RdA 1973, 207

Rill/Schäffer, Bundesverfassungsrecht, Wien, Loseblattausgabe

Raschhofer, Der urheberrechtliche Auskunftsanspruch gemäß § 87b Abs 3 UrhG gegen Access-Provider, in *Feiler/Raschhofer* (Hrsg), Innovation und internationale Rechtspraxis, Praxisschrift für Wolfgang Zankl (2009) 661

Rebmann/Säcker, Münchener Kommentar zum Bürgerlichen Gesetzbuch II^2, München (1985)

Rebmann/Säcker, Münchener Kommentar zum Bürgerlichen Gesetzbuch II^3, München (1994)

Roggan, Moderne Telekommunikationsüberwachung: eine kritische Bestandsaufnahme, KritV 2003, 76

Rohlack, Das Verhältnis der positiven Forderungsverletzung und culpa in contrahendo zur Sachmängelhaftung beim Kauf- und Werkvertrag, Baden-Baden, 1997

Ruhle/Lichtenberger/Kittl, Erste Erfahrungen mit dem TKG 2003 in Österreich. Eine Analyse der Gesetzesanwendung durch die Regulierungsbehörde, MR 2005, 63

Rummel, Vertragsauslegung nach der Verkehrssitte, Wien (1972)

Rummel, Verkehrssitten und Vertragsauslegung, JBl 1972, 66

Ruppe, Geheimnisschutz im Wirtschaftsleben, Wien (1980)

Säcker/Rixecker, Münchener Kommentar zum Bürgerlichen Gesetzbuch I[5], München (2006)

Schack, Der Schutzzweck als Mittel der Haftungsbegrenzung im Vertragsrecht, JZ 1986, 305

Schäfer/Ott, Lehrbuch der ökomomischen Analyse des Zivilrechts[4], Berlin (2005)

Schanda, Haftung für Urheberrechtsverletzungen Dritter im digitalen Umfeld, in *Fallenböck/Galla/Stockinger* (Hrsg), Urheberrecht in der Digitalen Wirtschaft, Wien (2005) 141

Schanda, Auskunftsanspruch gegen Access-Provider über die IP-Adressen von Urheberrechtsverletzern, MR 2005, 18

Schanda, Auskunftspflicht über Inhaber dynamischer IP-Adressen contra Verpflichtung zur Löschung von Verkehrsdaten, MR 2007, 213

Schermaier, Bona Fides in Roman Contract law, in *Zimmermann/Whittacker* (Hrsg), Good faith in European contract law, Cambridge (2000) 63

Schlechtriem, Schuldrecht[2], Tübingen (1994)

Schlechtriem, Schuldrecht[5], Tübingen (2003)

Schlesinger, Die Lehre von den positiven Vertragsverletzungen und ihr Einfluss auf das österreichische Recht, ZBl 1926, 401

Schlesinger, Das Wesen der positiven Vertragsverletzungen, ZBl 1926, 732

Schmelz/Stratil, Das neue Telekommunikationsgesetz, ecolex 1998, 267

Schmidt, Die Grundrechtskonformität der Überwachung einer Telekommunikation, Diss Wien (2003)

Schmidt, Zur Ökonomie ergänzender Vertragspflichten unter besonderer Berücksichtigung von Konkurrenzschutzgeboten, JA 1978, 597

Schmölzer, Rückwirkende Überprüfung von Vermittlungsdaten im Fernmeldeverkehr, JBl 1997, 211

Schneider, Verträge über Internet Access, München (2001)

Schöndorf, Über den Entwurf einer Novelle zum österreichischen ABGB, Archiv für Bürgerliches Recht 1913, 120

Schrammel, Gewährleistung für schlechte Dienste, in *Fischer-Cermak/Kletecka/Schauer/Zankl* (Hrsg), Festschrift zum 65. Geburtstag von Rudolf Welser (2004) 585

Schrey/Meister, Beschränkte Verwendbarkeit von Standortdaten – Hemmschuh für den M-Commerce, K&R 2002, 177

Schumacher, Die UWG-Novelle 2007, wbl 2007, 557

Schwarz/Wockenfoth, Zollrecht, Köln (1997)

Sieber/Höfinger, Drittauskunftsansprüche gegen Provider nach § 101a UrhG gegen Internetprovider zur Verfolgung von Urheberrechtsverletzungen, MMR 2004, 575

Simonetos, Das Recht der Leistungsstörungen, Stuttgart (1938)

Sofokleus/Mosing, Urheberrechtlicher Auskunftsanspruch gegen Access-Provider: ein "Pyrrhus-Anspruch"?, ÖBl 2008, 268

Spindler, Der Auskunftsanspruch gegen Verletzer und Dritte im Urheberrecht nach neuem Recht, ZUM 2004, 640

Spindler/Dorschel, Auskunftsansprüche gegen Internet-Service-Provider, CR 2005, 38

Statistik Austria, Europäische Erhebungen über den IKT-Einsatz in Haushalten 2002-2009, erstellt am: 31.08.2009, abrufbar unter: http://www.statistik.at/web_de/statistiken/informationsgesellschaft/ikt-einsatz_in_haushalten/index.html (Stand April 2010).

Staub, Die positiven Vertragsverletzungen[2], Berlin (1913)

Staub/Koenige, Kommentar zum HGB[12], Berlin (1926)

Stefula, Haftung des Erfüllungsgehilfen nach vertraglichen Grundsätzen? RZ 2001, 216

Stoll, Die Lehre von den Leistungsstörungen, Tübingen (1936)

Stoll, Abschied von der Lehre der positiven Vertragsverletzungen, AcP 1932, 257

Stomper, Zur Auskunftspflicht von Internet Providern, MR 2005, 118

Strasser G., Zur Gewährleistung von Rechtsschutz im Strafverfahren, ÖJZ 2006, 155

Strasser R., Der immaterielle Schaden im österreichischen Recht, Wien (1964)

Stürner, Der Anspruch auf Erfüllung von Treue- und Sorgfaltspflichten, JZ 1976, 389

Tannert, Finanzstrafgesetz, Wien (1974) Loseblattausgabe

Thanner/Vogl, Sicherheitspolizeigesetz[4], Wien (2010)

Thiele, Leistungsstörung und Schutzpflichtverletzung, JZ 1967, 649

Thienel/Schulev-Steindl, Verwaltungsverfahrensrecht[5], Wien (2009)

Tomandl (Hrsg), Innerbetriebliche Arbeitnehmerkonflikte aus rechtlicher Sicht, Wien (1977)

Triffterer/Rosbaud/Hinterhofer (Hrsg), Salzburger Kommentar zum StGB, Wien (1992) Loseblattausgabe

Vassilaki, Telekommunikationsüberwachung – eine Darstellung der aktuellen Rechtsfragen, RDV 2004, 11

Venier, Der zahnlose Rechtsschutz der StPO am Beispiel der Hausdurchsuchung, JSt 2009, 156

Venier, Das neue Ermittlungsverfahren: Eine Reform und ihre Mängel, ÖJZ 2009, 591

Vogl, Rechtsschutz und Vollziehung, in *BMI* (Hrsg), Der Rechtsschutzbeauftragte in Österreich, Wien (2004)

Vogl, Der Rechtsschutzbeauftragte in Österreich, Wien (2004)

Walter Ausforschung von Musikanbietern in Filesharing-Netzen – Providerauskunft – Datenschutz, MR 2009, 251

Walter/Mayer/Kucsko-Stadlmayer, Bundesverfassungsrecht[10], Wien (2007)

Welser, Bürgerliches Recht II[13], Wien (2007)

Wendt, Unterlassungen und Versäumnisse im Bürgerlichen Recht, AcP 1902, 1

Wessely, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht? ÖJZ 1999, 491

Wessely, Wohin soll ich mich wenden? Wege und Irrwege des datenschutzrechtlichen Rechtsschutzes im Sicherheitspolizei- und Militärbefugnisrecht, juridikum 2006, 51

Westhelle, Nichterfüllung und positive Vertragsverletzung, Köln (1978)

Westphal, Die neue EG-Richtlinie zur Vorratsdatenspeicherung, EuZW 2006, 555

Westphal, Die Richtlinie zur Vorratsdatenspeicherung von Verkehrsdaten – Neues aus Brüssel zum Verhältnis von Sicherheit und Datenschutz in der Informationsgesellschaft, juridikum 2006, 34

Westpahlen/Grote/Pohle, Der Telefondienstvertrag, Heidelberg (2001)

Wiebe, Auskunftsverpflichtung der Access-Provider, MR 2005, Beilage zu 4/05

Wiebe/Kodek, UWG, Wien (2009)

Wiederin, Einführung in das Sicherheitspolizeirecht, Wien (1998)

Wiederin, Privatsphäre und Überwachungsstaat, Wien (2003)

Wilburg, Elemente des Schadenersatzrechts, Marburg a.d. Lahn (1941)

Wittwe, Zollkodex, München (1998)

Wittwer, Die positive Vertrags- oder Forderungsverletzung, ÖJZ 2004, 161

Zanger/Schöll, Kommentar zum TKG 2003[2], Wien (2004)

Zankl, Bürgerliches Recht[5], Wien (2010)

Zankl, Der Entwurf zum E-Commerce-Gesetz, NZ 2001, 325

Zankl, E-Commerce-Gesetz in Sicht, AnwBl 2001, 459

Zankl, E-Commerce-Gesetz, Wien (2002)

Zankl, Auskunftspflicht für Mehrwertdienste? ecolex 2004, 853

Zankl, Online-Privilegien für Unterlassungsansprüche? ecolex 2004, 361

Zankl, Qualifikation und Dauer von Mobilfunkverträgen, ecolex 2005, 29

Zankl (Hrsg), Auf dem Weg zum Überwachungsstaat? Wien (2009)

Zeiller, Commentar über das allgemeine bürgerliche Gesetzbuch für die gesammten deutschen Erbländer der oesterreichischen Monarchie, Wien (1811)

Zeller, Der Schutz von Verkehrsdaten bei der Mobilkommunikation, Diss Wien, 2006

Zerbes, Das Urteil des deutschen Bundesverfassungsgerichts zur Online-Durchsuchug und Online-Überwachung, ÖJZ 2008, 834

Zitelmann, Nichterfüllung und Schlechterfüllung, in Festgabe der Bonner juristischen Fakultät für Paul Krüger zum Doktor-Jubiläum, Berlin (1911) 265

Zykan, Zum Verhältnis des Auskunftsanspruchs gem § 87b Abs 3 UrhG zum Datenschutz: OGH 14. 7. 2009, 4 Ob 41/09x – Keine Auskunft über die Identität von Inhabern dynamischer IP-Adressen, jusIT 2009, 206