Die strafrechtliche Verantwortlichkeit des Providers für User-Videos

Das Urteil des Mailänder Bezirksgerichts in Strafsachen vom 24.02.2010 gegen Google-Manager aus der Sicht des österreichischen Strafrechts

Diplomarbeit

aus Strafrecht und Strafverfahrensrecht

zur Erlangung des akademischen Grades

einer Magistra

der Rechtswissenschaften an der

Paris-Lodron Universität Salzburg

eingereicht von

Katrin Niederacher

0520116

Betreuer

Univ.-Prof. Dr. Otto Lagodny

Salzburg, Juni 2011

Inhaltsverzeichnis

Literaturverzeichnis IV

Internetquellen VII

Entscheidungsverzeichnis IX

Rechtsquellenverzeichnis X

Abkürzungsverzeichnis XII

Einleitung 1

1. Teil: Allgemeine Grundlagen – Der Provider 5

A. Arten von Providern 6

I. Access-Provider 6

II. Host-Provider 7

III. Content-Provider 7

IV. Domain-Name-Service-Provider 7

B. Provider-Art von Google 8

2. Teil: Urteil des Mailänder Bezirksgericht gegen Google-Manager 9

A. Sachverhalt 9

B. Urteilsbegründung 11

C. Schuldsprüche 12

3. Teil: Materielles Strafrecht 13

A. Österreichische Strafgewalt 13

B. Strafbarkeit der Google-Manager 16

I. Strafbarkeit nach italienischem Recht 16

1. Strafbarkeit nach dem italienischen StGB 16

2. Strafbarkeit nach italienischem Datenschutzrecht 16

II. Strafbarkeit nach österreichischem Recht 17

1. Strafbarkeit nach dem StGB 17

a) Wegen Körperverletzung nach § 83 17

b) Wegen Quälens wehrloser Personen nach § 92 18

c) Wegen strafbarer Handlungen gegen die Ehre §§ 111 ff 19

aa) Üble Nachrede, § 111 19

bb) Beleidigung, § 115 21

(1) Unmittelbarer Täterschaft 22

(2) Beteiligung 22

d) Zwischenresümee 24

e) Begehung durch Unterlassung 26

aa) Kontrollmöglichkeit: Host-Provider 26

bb) Voraussetzungen: Unechte Unterlassungsdelikte 27

2. Strafbarkeit der Google-Manager nach dem VbVG 30

3. Strafbarkeit der Google-Manager nach dem DSG 2000 31

a) Personenbezogene Daten 32

b) Tathandlung 33

c) Schutzwürdiges Geheimhaltungsinteresse des Betroffenen 34

d) Unrechtmäßige Bereicherung 35

aa) Bereicherung ... 35

bb) Unrechtmäßigkeit der Bereicherung ... 35

e) Schädigungsvorsatz nach § 1 Abs 1 DSG 2000 ... 37

f) Anwendung von österreichischem Datenschutzrecht ... 38

g) Zwischenergebnis ... 39

4. Strafbarkeit der Google-Manager nach dem TKG 2003 ... 40

a) Verletzung von Rechten der Benützer, § 108 ... 40

b) Kommunikationsgeheimnis § 93 ... 41

5. Strafbarkeit der Google-Manager nach dem MedienG ... 43

a) Üble Nachrede, Beschimpfung, Verspottung und Verleumdung ... 43

b) Medien ... 44

c) Anwendbarkeit MedienG auf ausländische Medien ... 45

d) Medieninhaber ... 45

III. Resümee: Verantwortlichkeit des Providers ... 47

Abschließende Überlegungen ... 51

Anhang: ausgewählte Gesetzesstellen ... 54

Verbandsverantwortlichkeitsgesetz ... 54

Datenschutzgesetz 2000 ... 55

Telekommunikationsgesetz 2003 ... 59

Mediengesetz ... 60

Literaturverzeichnis

Bachner-Foregger, Strafgesetzbuch, 22. Auflage 2009, Manz, Wien

Berka, Lehrbuch Verfassungsrecht, Grundzüge des österreichischen Verfassungsrechts für das juristische Studium, 2. Auflage 2008, Springer, Wien, New York

Bertl/Schwaighofer, Österreichisches Strafrecht Besonderer Teil I, 11. Auflage 2010, Springer, Wien, New York

Burgstaller/Fabrizy, §§ 82-87 in: *Höpfel/Ratz* (Hrsg), Wiener Kommentar zum Strafgesetzbuch, 2. Auflage, Band 2, 36. Lfg (2002), Manz Wien

Daum, Providerauskunft und Urheberrecht – der Gesetzgeber ist am Zug!, MR 2009, S. 247-251

Fabrizy, Strafgesetzbuch, Kurzkommentar, 10. Auflage 2010, Manz, Wien

Fabrizy, §§ 12-14 in: *Höpfel/Ratz* (Hrsg), Wiener Kommentar zum Strafgesetzbuch, 2. Auflage, Band 1, 11. Lfg (2000), Manz Wien

Finke, Die strafrechtliche Verantwortung von Internet-Providern, Köhler-Druck, 1998, Tübingen

Foregger, §§ 111-117 in: *Höpfel/Ratz* (Hrsg), Wiener Kommentar zum Strafgesetzbuch, 2. Auflage, Band 3, 1. Lfg (1999), Manz Wien

Fuchs, Österreichisches Strafrecht Allgemeiner Teil I, 7. Auflage 2008, Springer, Wien

Hasberger/*Semrau-Deutsch*, Host-Provider als Richter?, ecolex 2005, S. 197-199

Höhne, Medienrechtliche Ordnungsvorschriften für Online-Medien, in: *Berka* (Hrsg), Medien im Web, Manz 2009, S. 1-7

Höpfel/Kathrein, §§ 61-67 in: *Höpfel/Ratz* (Hrsg), Wiener Kommentar zum Strafgesetzbuch, 2. Auflage, Band 2, 21. Lfg (2011),Manz Wien

Jahnel, Datenschutz im Internet, ecolex 2001, S. 84-89

Kaufmann/*Tritscher*, TKG 2003 – der neue Rechtsrahmen für „elektronische Kommunikation“ (Teil 1), MR 4/2003, S. 273-208

Kienapfel/*Höpfel*, Strafrecht Allgemeiner Teil, 13. Auflage 2009, Manz Wien

Kienapfel/Schmoller, Studienbuch Strafrecht Besonderer Teil II, 1. Auflage 2003, Manz Wien

Kienapfel/Schroll, Studienbuch Strafrecht Besonderer Teil I, 1. Auflage 2003, Manz Wien

Kienapfel/Schroll, Strafrecht Besonderer Teil I, 5. neu bearbeitete Auflage 2005, Manz Wien

Krammer, Der Einzug des Internet-Zeitalters in das Mediengesetz, GesRZ 2005, S. 186-193

Lambauer, §§ 111 ff in: *Triffterer*/*Rosbaud*/*Hinterhofer* (Hrsg), Salzburger Kommentar zum Strafgesetzbuch, Band 3, 20. Lfg. (2009), LexisNexis, Wien

Lagodny, Die Herausforderungen des Internet an das Strafrecht, in: *Gruber* (Hrsg), Die rechtliche Dimension des Internet, Manz Wien 2001, S. 51-68

Lehofer, Das Telekommunikationsgesetz 2003 – Der Übergang vom alten zum neuen Telekommunikationsrecht, ÖJZ 2003/48, S. 781-788

Lewisch, Strafrecht Besonderer Teil I, 2. Auflage 1999, WUV Wien

Messner, § 83 in: *Triffterer*/*Rosbaud*/*Hinterhofer* (Hrsg), Salzburger Kommentar zum Strafgesetzbuch, Band 2, 18. Lfg. (2008), LexisNexis, Wien

Michel/*Wessely*, Strafrecht Allgemeiner Teil, 1. Auflage 1999, Manz Wien

Plöckinger, Zur Zuständigkeit österreichischer Gerichte bei Straftaten im Internet, ÖJZ 2001, S. 789-804

Rosenthal, Internet-Provider-Haftung – ein Sonderfall? in: *Jung* (Hrsg), Aktuelle Entwicklungen im Haftungsrecht, Edition Weblaw/Schulthess, Bern, Zürich, Basel, Genf, 2007, S. 149-206

Reindl-Krauskopf, Computerstrafrecht im Überblick, 2. Auflage 2009, facultas.wuv, Wien

Schmölzer/*Mayer-Schönberger*, Das Telekommunikationsgesetz 1997 – Ausgewählte rechtliche Probleme, ÖJZ 1998, S. 378-387

Schwaighofer, §§ 62-67 in: *Triffterer*/*Rosbaud*/*Hinterhofer* (Hrsg), Salzburger Kommentar zum Strafgesetzbuch, Band 2, 7. Lfg. (2002), LexisNexis, Wien

Schwarzenegger, Der räumliche Geltungsbereich des Strafrechts im Internet – Die Verfolgung von grenzüberschreitender Internetkriminalität in der Schweiz im Vergleich mit Deutschland und Österreich, ZStrR 2000, Band 118, S. 109-130

Thiele, Unbefugte Bildaufnahme und ihre Verbreitung im Internet – Braucht Österreich einen eigenen Paparazzi-Paragrafen?, RZ 2007, S. 2-14

Zanger, Telekommunikationsgesetz 2003, LexisNexis 2003, Wien

Internetquellen

Geist, Die Zuständigkeit bei Internetdelikten,
http://www.it-academy.cc/article/399/Die+Zustaendigkeit+bei+Internet Delikten.html
(Stand: 6.4.2010; 14:30h)

Glossar von Fischer-Lehmann Consulting GmbH
http://www.fischer-lehmann.ch/Web/web/glossar.htm#I
(Stand: 29.3.2011; 11:00h)

Impressum von Google Inc
http://www.google.at/intl/de/impressum.html
(Stand 25.1.2011; 19:30h)

Monti, Erstes Urteil im italienischen Strafverfahren gegen Google-Führungskräfte
http://www.unwatched.org/node/1721
(Stand 24.5.2010; 17:35h)

Nutzungsbedingungen von Google Inc
http://www.google.com/accounts/TOS
(Stand 1.6.2011; 20:30h)

Peters, Google Video: Die Hintergründe des Mailänder Strafurteils
http://www.telemedicus.info/article/1716.Google-Video-Die-Hintergruende-des-Mailaender-Strafurteils.html
(Stand 9.5.2010 13:48h)

Rat für Kriminalitätsverhütung in Schleswig-Holstein, Happy Slapping und mehr…
https://www.datenschutzzentrum.de/schule/happy-slapping.pdf
(Stand: 24.03.2011; 16:30h)

Schmidbauer, Internet4jurists.at
http://www.internet4jurists.at/urh-marken/immaterial.htm
(Stand 31.01.2011; 17:15h)

Standorte von Google Inc
http://www.google.at/corporate/address.html
(Stand 25.1.2011; 20:00h)

Entscheidungsverzeichnis

Österreichische Rechtsprechung

Entscheidung zum MedienG
OLG Wien 14.11.2007, 18 Bs 259/07f, MR 2007, S. 308-309

Entscheidung zum MedienG
OGH 24.1.2006, 4 Ob 226/05x, MR 2006, S. 148-150

Entscheidung zur Haftung von Host-Providern
OGH 6.7.2004, 4 Ob 66/04s; ecolex 2004, 799

Italienische Rechtsprechung

Urteil des Mailänder Bezirksgerichts 1972/2010, 24.02.2010 (italienisch),
http://speciali.espresso.repubblica.it//pdf/Motivazioni_sentenza_Google.pdf
(Stand: 19.04.2010; 14:35h)

Rechtsquellenverzeichnis

Rechtsquellen des Europarates

Cybercrime Konvention des Europarates

http://conventions.coe.int/Treaty/en/Treaties/html/185.htm

Rechtsquellen des Europäischen Parlaments und des Rates

Datenschutzrichtlinie für elektronische Kommunikation (TKG 2003)

Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABL L 201 vom 31.7.2002, S. 37-47

EC-RL

Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8 Juni 2000 über bestimmte rechtliche Aspekte der Dienst der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr"), ABL L 178/1 vom 17.7.2000, S. 1-15

EG-Datenschutzrichtlinie

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 1995 L 281 vom 23.11.1995, S. 31-50

Frequenzentscheidung (TKG 2003)

Entscheidung 676/2002/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen Rechtsrahmen für die Funkfrequenzpolitik in der Europäischen Gemeinschaft, ABL L 108 vom 24.4.2001, S. 1-6

Genehmigungsrichtlinie (TKG 2003)

Richtlinie 2002/20/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über die Genehmigung elektronischer Kommunikationsnetze und –dienste, ABL L 108 vom 24.4.2002, S. 21-32

Rahmenrichtlinie (TKG 2003)

Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und –dienste, ABL L108 vom 24.4.2002, S. 33-50

Universaldienstrichtlinie (TKG 2003)

Richtlinie 2002/22/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und –diensten, ABL L 108 vom 24.4.2002, S. 51-77

Zugangsrichtlinie (TKG 2003)

Richtlinie 2002/19/ EG des Europäischen Parlaments und des Rates vom 7. März 2002 über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung, ABL L108 vom 24.4.2002, S. 7 -20

Abkürzungsverzeichnis

Abb	Abbildung
ABGB	Allgemeines Bürgerliches Gesetzbuch
ABL	Amtsblatt (EU)
Abs	Absatz
AGB	Allgemeine Geschäftsbedingungen
Art	Artikel
AT	Allgemeiner Teil
BGBl	Bundesgesetzblatt
BT	Besonderer Teil
B-VG	Bundes-Verfassungsgesetz
bzw	beziehungsweise
dh	das heißt
DSG 2000	Datenschutzgesetz 2000
ECG	E-Commerce-Gesetz
EC-RL	E-Commerce-Richtline; 2000/31/EG
EG	Europäische Gemeinschaft
etc	et cetera
EU	Europäische Union
ev	eventuell(e)
ff	fortfolgende
FG	Fernmeldegesetz
gem	gemäß

GesRZ	Der Gesellschafter, Zeitschrift für Gesellschafts- und Unternehmensrecht
GmbH	Gesellschaft mit beschränkter Haftung
Hrsg	Herausgeber
idR	in der Regel
Inc	Incorporate
insb	insbesondere
IP	Internetprotokoll
iS	im Sinne
iSd	im Sinne des
iVm	in Verbindung mit
lit	Litera
Kap	Kapitel
Lfg	Lieferung
MedienG	Mediengesetz
MR	Medien & Recht, Zeitschrift für Medien- und Kommunikationsrecht
Nr	Nummer
OGH	Oberster Gerichtshof
OLG	Oberlandesgericht
ÖJZ	Österreichische Juristen-Zeitung
PC	Personal Computer
RL	Richtlinie
Rz	Randziffer
RZ	Richterzeitung

S	Seite
SbgK	Salzburger Kommentar zum Strafgesetzbuch
StGB	Strafgesetzbuch
StGG	Staatsgrundgesetz
StrAnpG 1974	Strafrechtsanpassungsgesetz 1974
TKG 1997	Telekommunikationsgesetz 1997
TKG 2003	Telekommunikationsgesetz 2003
ua	unter anderem
UrhG-Nov 1996	Urheberrechtsgesetz-Novelle 1996
uU	unter Umständen
usw	und so weiter
va	vor allem
VbVG	Verbandsverantwortlichkeitsgesetz
Vorbem	Vorbemerkungen
WK	Wiener Kommentar zum Strafgesetzbuch
Z	Ziffer
zB	zum Beispiel
ZStrR	Schweizerische Zeitschrift für Strafrecht
zT	zum Teil

Einleitung

Ein am Down-Syndrom erkrankter Junge wurde von Jugendlichen geschlagen, mit Gegenständen beworfen und beschimpft. Das Ganze wurde gefilmt und auf eine Videoplattform im Internet hochgeladen und auf „Google Video Italy“ veröffentlicht. Für dieses User-Video wurden Ende Februar 2010 drei Top-Manager von Google in Italien wegen fahrlässiger Datenverwendung nach Art 167 des italienischen Datenschutzgesetzes[1] zu bedingten Freiheitsstrafen verurteilt, da sie die Privatsphäre des Opfers massiv verletzt hätten, denn nach italienischem Datenschutzrecht bedarf es zur Veröffentlichung von personenbezogenen Daten der Einwilligung des Betroffenen. Das Mailänder Gericht sah in der konkreten Darstellung des am Down-Syndrom erkrankten Jugendlichen eine Veröffentlichung von besonders sensiblen personenbezogenen Gesundheitsdaten. Für deren Veröffentlichung hätte nach Ansicht des Gerichts zumindest eine ausdrückliche Erlaubnis der Eltern vorliegen müssen, die aber fehlte.

Aufgrund der Weite und Unübersichtlichkeit des Internets ist es oftmals schwierig, den einzelnen Täter auszuforschen. Ein einmal in das Internet eingespeister Inhalt ist binnen weniger Sekunden nahezu weltweit an jedem Computer abrufbar, der eine Verbindung zum Internet hat. Problematisch erweist sich auch, dass das Internet über keinerlei zentrale Verwaltung verfügt, die einmal „online“ gestellten Daten werden daher auch keiner Kontrolle unterworfen. Durch diese Unübersichtlichkeit ist das Internet für den einzelnen Staat auch schwer zu überwachen. Straftaten sind daher schwierig zu verhindern. Auch für den einzelnen Provider, also der Internetdienstanbieter, ist eine Überwachung seines Speichers schwierig, denn aufgrund der enormen Menge an Daten, die tagtäglich von den einzelnen Nutzern auf dessen Speichermedien abgelegt werden, ist es schier unmöglich, jede einzelne Datei zu kontrollieren, vor allem wenn man an große Provider wie zB Google denkt, die Millionen von Nutzern haben. Daher erscheint

[1] Codice in materia di protezione die dati personale *(„Gesetz zum Schutz personenbezogener Daten“)*, decrete legislativo 30 giugno 2003, n 196 *(„gesetzliche Verordnung vom 30. Juni 2003, Nr 196“),* pubblicato sulla GU n. 174 del 29-7-2003 *(„veröffentlicht im Amtsblatt Nr 174 vom 29.7.2003“).*

es auch fraglich, ob dem Provider eine solche Kontrolle überhaupt zumutbar ist. Eine weitere Schwierigkeit ist die Möglichkeit der Anonymisierung durch zB Verschlüsselungsprogramme und andere Software, die die Ermittlung des jeweiligen Urhebers erheblich erschweren und zT sogar unmöglich machen. Daher wird überlegt, wie der einzelne Provider in die Pflicht genommen werden kann, um der Kriminalität entgegenzuwirken. Eine weitere Schwierigkeit bei Internetdelikten bereitet zT die Anknüpfung an nationales Recht. Straftaten im Internet können von überall auf der Welt begangen werden und strafrechtlich relevante Inhalte können auch überall auf der Welt in das Internet hochgeladen werden. Wiederum können daher die strafrechtlich relevanten Inhalte weltweit abgerufen werden.

Vor dem Hintergrund der rasanten technischen Weiterentwicklung gibt es kein einheitliches Computerstrafrecht. Die verschiedenen Kriminalitätsaspekte werden in unterschiedlichen Regelungen gefasst. Die Tatbestände finden sich im Kernstrafrecht, also dem StGB, ebenso wie in den Nebengesetzen, zB dem Datenschutzgesetz 2000. In Österreich gibt es das Telekommunikationsgesetz 2003 (TKG 2003), das am 20. August 2003 in Kraft getreten ist. Dieses Gesetz regelt nunmehr – im Gegensatz zu seinem Vorgänger, dem TKG 1997 – die für das Internet maßgebenden Rechtsfragen. Jedoch müssen für die Festlegung, für welche Arten von Inhalten sich der Provider verantworten muss, auch weiterhin Bestimmungen des österreichischen Strafrechts herangezogen werden, da auch im TKG 2003 keine expliziten Regelungen zur strafrechtlichen Verantwortlichkeit der Provider zu finden sind. Die Strafbestimmung des TKG 2003 sanktioniert zwar die Verletzung von Rechten der Benutzer (§ 108 TKG 2003), allerdings findet sich hier auch keine detaillierte Regelung zur strafrechtlichen Verantwortlichkeit. Es stellt sich daher die Frage, nach welcher Rechtsvorschrift ein Sachverhalt, wie der oben dargestellte, zu beurteilen ist.

Auch europarechtliche Normen, wie die E-Commerce-Richtline (EC-RL), sind für eine Beurteilung der Frage der Verantwortlichkeit des Providers von Relevanz, da Österreich Mitglied der EU ist. Die EC-RL wurde durch das E-Commerce-Gesetz (ECG) umgesetzt. Das ECG nennt den betreffenden Gesetzesabschnitt „Verantwortlichkeit von Dienstanbietern“, regelt aber in den einzelnen Paragraphen den Ausschluss der Verantwortlichkeit; auch inhaltlich stellt dieser Gesetzestext jeweils darauf ab, dass der

Dienstanbieter „nicht verantwortlich“ ist, sofern er bestimmte Vorgaben beachtet, daher sind die Vorschriften des ECG nicht haftungsbegründend, sondern haftungsbeschränkend.[2] Weiters enthält das ECG lediglich einen Verwaltungsstraftatbestand; das Verwaltungsstrafrecht ist jedoch nicht Thema dieser Arbeit. Daher kann das ECG bei der vorliegenden Arbeit unberücksichtigt bleiben, denn in dieser Arbeit soll die gerichtliche Verantwortlichkeit des Providers behandelt werden.

Auch andere europarechtliche Normen wurden in innerstaatliches Recht umgesetzt, va im TKG 2003 und auch im Datenschutzgesetz 2000 (DSG 2000), die ebenfalls für diese Arbeit von Relevanz erscheinen.

Der § 51 DSG 2000 ist das Gegenstück zum Art 167 des italienischen Datenschutzgesetzes, nach welchem im Februar 2010 die Manager von Google zu bedingten Freiheitsstrafen verurteilt wurden, daher wird auch hier gezielt Augenmerk auf das Datenschutzrecht gelegt werden.

Es stellt sich nun die Frage, ob sich die Führungskräfte eines Providers in Österreich zu verantworten hätten, würde sich ein ähnlicher Fall wie der in Italien hierzulande ereignen. Weiters ist festzustellen, wie sehr sich der einzelne Provider für fremdes Fehlverhalten verantworten muss. Weiters ist zu prüfen, inwieweit dem Provider fremde Inhalte zuzurechnen sind, wenn er doch lediglich Speicherplatz zur Verfügung stellt.

Keine Rolle bei dieser Arbeit spielt das Verhalten der Jugendlichen, die den am Down-Syndrom erkrankten Jungen misshandelt und gedemütigt haben, auch wenn sie uU das eine oder andere strafrechtlich relevante Verhalten gesetzt haben. Das Thema „Happy Slapping“[3] soll daher hier in dieser Arbeit vollständig ausgeklammert werden. Es soll lediglich untersucht werden, inwieweit sich der Provider und dessen Führungskräfte für fremdes Fehlverhalten zu verantworten haben.

Im ersten Teil dieser Arbeit erfolgt eine kurze Auflistung der Arten des Providers und in welchen Formen diese in Erscheinung treten. Aufgrund der weiten Verbreitung des

---

[2] *Reindl-Krauskopf*, Computerstrafrecht[2], S. 106.

[3] Als „**Happy Slapping**“ *(engl.: „Fröhliches Schlagen“)* wird ein grundloser Angriff auf meist unbekannte Personen bezeichnet. Dieser Trend begann etwa 2004 in England. Jugendliche greifen, meist in der Überzahl, willkürlich Passanten an und nehmen ihre Gewalttaten mit einem Foto-Handy auf. Diese Aufnahmen werden anschließend im Internet veröffentlicht oder anderweitig verbreitet. Siehe *Rat für Kriminalitätsverhütung in Schleswig-Holstein*, Happy Slapping und mehr…, https://www.datenschutzzentrum.de/schule/happy-slapping.pdf (Stand: 24.03.2011).

Internets wird auf eine Erklärung der Funktionsweise verzichtet. Im zweiten Teil wird der Sachverhalt des italienischen Urteils, das zu Beginn schon erwähnt wurde, kurz dargestellt. Im dritten Teil dieser Arbeit soll dann auf das materielle österreichische Recht eingegangen und somit untersucht werden, wie der italienische Fall in Österreich zu behandeln wäre. Dabei beschäftige ich mich mit der Anknüpfung an österreichisches Recht (internationales Strafrecht) und untersuche vergleichbare österreichische Tatbestände im Strafgesetzbuch, also dem Kernstrafrecht, und ebenso in den Nebenstrafgesetzen, zB dem Verbandsverantwortlichkeitsgesetz.

1. Teil

Allgemeine Grundlagen – Der Provider

Da das Internet mittlerweile einen hohen Beliebtheitsgrad erlangt hat und auch enorm weit verbreitet ist, wird bei dieser Arbeit auf einen umfassenden Überblick über die Funktionsweise und die Entwicklung des Internets ebenso wie auf dessen Entwicklung und Geschichte verzichtet. Lediglich sollte festgehalten werden, dass eine grenzenlose Kommunikation, die nahezu zeitgleich vor sich gehen kann, durch das Internet ermöglicht wird.[4]

Wie bereits in der Einleitung erwähnt, weist das Internet eine dezentrale Struktur auf. Dh, dass die einzelnen PCs der Nutzer über Server verbunden sind und diese Server wiederum untereinander in Verbindung stehen. Ist eine Verbindung zB unterbrochen und kann daher auf diesem Wege die Information nicht transportiert werden, dann wird automatisch eine andere Verbindung genutzt. Aufgrund dieser dezentralen Struktur ist eine Überwachung extrem schwierig zu bewältigen.

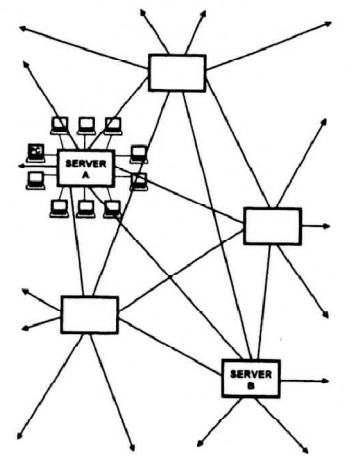

Abb 1: Dezentrale Struktur des Internets[5]

[4] *Geist*, Die Zuständigkeit bei Internetdelikten, http://www.it-academy.cc/article/399/Die+Zustaendigkeit+bei+InternetDelikten.html (Stand: 6.4.2010).

[5] Grafik aus: *Lagodny* in: *Gruber* (Hrsg), Dimensionen, S. 52.

Ebenso ist die Anonymität im Internet sehr hoch. Dies wird vor allem durch verschiedene Software und Verschlüsselungsprogramme erreicht. Auch werden die Grenzen der einzelnen Staaten durch das Internet irrelevant, was sich als problematisch für eine Anknüpfung an nationales Recht erweisen kann. Nun stellt sich die Frage der Verantwortlichkeit der Internet-Provider für die Handlungen ihrer Kunden und anderer Benutzer des Internets.

Der Provider (Internet-Service-Provider) wird auch Internetdienstanbieter oder Internetdienstleister genannt. Provider sind daher Anbieter von Diensten, Inhalten oder technischen Leistungen, die für die Nutzung bzw den Betrieb von Inhalten oder Diensten im Internet notwendig sind.[6]

A. Arten von Providern

Es gibt verschiedene Erscheinungsformen des Internet-Providers. Die Unterscheidung erfolgt aufgrund der verschiedenen Dienste, die der jeweilige Provider zur Verfügung stellt.

I. Access-Provider

Access-Provider sind Anbieter, die lediglich den Zugang zum Internet anbieten. Sie transportieren auch Informationen eines Nutzers über ein Kommunikationsnetz, wählen diese Information weder aus noch verändern sie sie; es kann auch zu kurzfristigen automatischen Zwischenspeicherungen kommen, die aus technischen Gründen notwendig sind.[7]

---

[6] Glossar von Fischer-Lehmann Consulting GmbH http://www.fischer-lehmann.ch/Web/web/glossar.htm#I (Stand: 29.3.2011).

[7] *Reindl-Krauskopf*, Computerstrafrecht[2], S. 104.

II. Host-Provider

Host-Provider stellen ihre Serverstruktur für das Bereithalten von Inhalten zur Verfügung,[8] bieten also auch sonstige Dienste, wie vor allem Speicherplatz für Kunden, an. Sie speichern fremde Inhalte auf ihren Servern ab und halten sie zur Abfrage für andere User bereit.[9]

III. Content-Provider

Ein Content-Provider bietet neben dem Internet-Zugang auch eigene redaktionell aufgearbeitete Beiträge und Inhalte an.

IV. Domain-Name-Service-Provider

Der Domain-Name-Service-Provider ist jener Provider, der sicherstellt, dass die Domain-Namen einer bestimmten „Endung" (sprich: Top-Level-Domain) im Internet für Internet-Adressen verwendet werden können.[10]

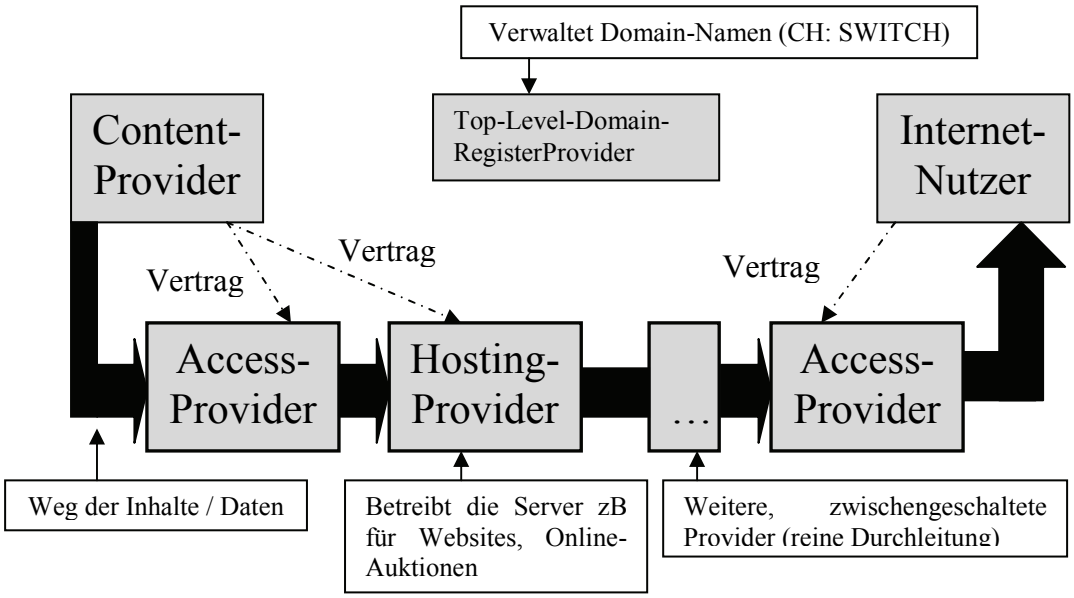

Abb 2: Die Grafik zeigt das Verhältnis und die Position der verschiedenen Provider mit Bezug auf den Datenfluss im Internet.[11]

---

8 *Rosenthal* in: *Jung*, Entwicklungen, S. 155, Rz 11.

9 *Reindl-Krauskopf*, Computerstrafrecht[2], S. 104.

10 *Rosenthal* in: *Jung*, Entwicklungen, S. 155, Rz 11.

11 Grafik aus: *Rosenthal* in: *Jung*, Entwicklungen, S. 156, Rz 11.

Zwar erfüllt ein Provider idR mehrere der oben genannten Aufgaben, jedoch ist für die Frage der strafrechtlichen Verantwortung stets entscheidend, welche Funktion er in concreto erfüllt hat.[12]

Die Provider (Access- und Host-Provider) sind im Gegensatz zum Content-Provider einem besonderen, schwer kontrollierbaren Haftungsrisiko für fremde Inhalte ausgesetzt, wissen sie doch idR nicht, um welche Inhalte es sich handelt. Darüber hinaus verändern sich die Inhalte sehr rasch. Daher muss ein Kompromiss gefunden werden zwischen den wirtschaftlichen Interessen und der Bedeutung der Provider für Dienste der Informationsgesellschaft einerseits und dem Rechtsgüterschutz durch Strafrecht anderseits.[13]

B. Provider-Art von Google

Bei Google handelt es sich um einen Host-Provider. Google stellt nämlich seine Serverstruktur den Kunden zur Verfügung und hier vor allem Speicherplatz, wie zB bei „Google Video“ oder „Google Mail“. Google ist aber auch Content Provider, da es auch eigene Inhalte zum Abruf bereitstellt, zB „Google Maps“ und der gleichen.

Die anderen Erscheinungsformen des Providers, also Access-Provider, Backbone-Provider und Domain-Name-Service-Provider, kommen für Google nicht in Frage, da Google nicht den Zugang zum Internet vermittelt und auch nicht die „Endungen“ einer Internet-Adresse überprüft.

In dem dieser Arbeit zu Grunde liegenden Fall tritt Google als Host-Provider in Erscheinung, da es sich um ein User-Video handelt, das auf den Speichermedien von Google abgelegt wurde.

---

[12] *Reindl-Krauskopf*, Computerstrafrecht[2], S. 104.

[13] *Reindl-Krauskopf*, Computerstrafrecht[2], S. 105.

2. Teil

Urteil des Mailänder Bezirksgericht gegen Google-Manager

A. Sachverhalt[14]

Auf der Videoplattform von „Google Video Italy“ wurde ein User-Video veröffentlicht, in dem zu sehen war, wie ein am Down-Syndrom erkrankter Junge von anderen Jugendlichen brutal misshandelt und gedemütigt wurde, denn der Junge wurde weiters beschimpft und mit Gegenständen beworfen. Dies wurde gefilmt und das Video wurde dann am 8. September 2006 auf „Google Video Italy“ hochgeladen. Veröffentlicht wurde dieses in der Rubrik „Funny Videos“.

Angeklagte im erstinstanzlichen Verfahren vor dem Mailänder Bezirksgericht in der Zusammensetzung als Einzelrichter waren

D. (Erster Vizepräsident für Firmenentwicklung und oberster Rechtsberater des Unternehmens; damaliger Chef von „Google Italy“),

R. (Mitglied der Beratung der Administration von Google Italien GmbH; Finanzchef),

F. (verantwortlich für den Datenschutz in Europa) und

A. (verantwortlich für das Projekt „Google Video“ in Europa).

Wie aus der Anklage hervorgeht, handelte es sich bei den vier Angeklagten um hohe Manager von Google. Privatbeteiligte am Verfahren waren die **Organisation Vivi Down**[15] und die **Ombudsperson der Stadt Mailand**.

Kurz nach der Veröffentlichung des Videos rangierte es auf dem ersten Platz der unterhaltsamsten Videos und hatte 5.500 Aufrufe bis zu seiner Entfernung über zwei

---

[14] *Peters*, Google Video: Die Hintergründe des Mailänder Strafurteils, http://www.telemedicus.info/article/1716.Google-Video-Die-Hintergruende-des-Mailaender-Strafurteils.html (Stand 9.5.2010) und italienisches Urteil des „Tribunale Ordinario di Milano“ *(Bezirksgericht von Mailand)*, 1972/2010, 24.02.2010 http://speciali.espresso.repubblica.it//pdf/Motivazioni_sentenza_Google.pdf (Stand: 19.04.2010).

[15] **Vivi Down**, eine soziale Non Profit Organisation, hat zum Ziel die Sicherung der Gesundheit von Menschen mit Down-Syndrom sowie die Bereitstellung von medizinischen Untersuchungen und die Förderung der wissenschaftlichen Forschung.

Monate später. Weiters war es auf Platz 29 der „Top 100“ Downloads.[16] Am 6. November 2006 gingen aus Nutzerkreisen bei Google entsprechende Hinweise auf das Video ein. Eine Nutzerin verlangte die Löschung des Clips. Einen weiteren Tag später, am 7. November 2006, verlangte schließlich auch die Polizei die Löschung des Videos. Noch am selben Tag wurde es von Google entfernt.[17]

Die Staatsanwaltschaft Mailand erhob Anklage gegen vier Google-Manager, **D.**, **R.**, **F.** und **A.**, wegen Verleumdung. **D.**, **R.** und **F.** waren weiters wegen rechtswidriger Datenverarbeitung angeklagt. Die Staatsanwaltschaft war der Meinung, dass Google organisatorische Vorkehrungen hätte treffen müssen, um eine Veröffentlichung solcher Videos zu verhindern. Allerdings verdiene Google mit jedem Klick Geld und sei deshalb nicht daran interessiert, Videos, die zwar rechtsverletzend sind, aber oft aufgerufen werden, zu verhindern bzw zu entfernen. Eine Reaktion von Google sei nur auf Druck der Presse erfolgt, nicht aber aus Kooperationsbereitschaft.[18] Die Staatsanwaltschaft argumentierte weiters, dass im italienischen Recht ein Rechtsgrundsatz existiere, der besagt: Einen Umstand nicht zu verhindern bedeutet, ihn mit zu verantworten. Das Datenschutzgesetz setzt die Einholung einer Ermächtigung voraus, bevor personenbezogene Daten verarbeitet werden dürfen; online veröffentlichte Videos sind als persönliche Daten zu betrachten und somit hatten die Führungskräfte von Google die Verpflichtung zu überprüfen, ob jeder User, der das Video veröffentlicht hat, zuvor die präventive Einverständniserklärung der abgebildeten Personen eingeholt hat und durch die Versäumung dieses Schrittes haben sie gegen das Datenschutzgesetz verstoßen und zudem haben sie die Beleidigung des Gewaltopfers zugelassen, indem sie das Video nicht vorabkontrolliert haben. Allerdings wurde dieser Anklagepunkt abgelehnt, da eine Vorabkontrolle nicht zumutbar sei.[19]

---

16 Italienisches Urteil des „Tribunale Ordinario di Milano“ S. 13.

17 *Peters*, Google Video: Die Hintergründe des Mailänder Strafurteils, http://www.telemedicus.info/article/1716.Google-Video-Die-Hintergruende-des-Mailaender-Strafurteils.html (Stand 9.5.2010).

18 *Peters*, Google Video: Die Hintergründe des Mailänder Strafurteils, http://www.telemedicus.info/article/1716.Google-Video-Die-Hintergruende-des-Mailaender-Strafurteils.html (Stand 9.5.2010).

19 *Monti*, Erstes Urteil im italienischen Strafverfahren gegen Google-Führungskräfte http://www.unwatched.org/node/1721 (Stand 24.5.2010).

B. Urteilsbegründung

Die vier Google-Manager waren wegen Verleumdung angeklagt, da im Video ein Satz gefallen ist, in dem die Organisation Vivi Down explizit beleidigt wurde. Richter *Oscar Magi* sprach alle vier Angeklagten im ersten Anklagepunkt – Verleumdung – frei. *„Das geltende italienische Recht sehe keine Pflicht zur inhaltlichen Vorabkontrolle von Videos hinsichtlich ehrverletzender Äußerungen vor“,*[20] hieß es in der Urteilsbegründung. Daher könne auch keine Zuwiderhandlung der Angeklagten gegen eine solche Pflicht angenommen werden, obwohl die Staatsanwaltschaft zuvor von einer solchen Verpflichtung zur präventiven inhaltlichen Vorabkontrolle ausgegangen war. Nach Richter *Magi* könnten sich nach derzeitiger Rechtslage jedoch alleine die Uploader des Videos der Verleumdung strafbar gemacht haben.[21]

Durch die Veröffentlichung des besagten Videos habe Google jedoch gegen das italienische Datenschutzrecht verstoßen, denn bei der Veröffentlichung von personenbezogenen Daten bedürfe es nämlich der Zustimmung des Betroffenen.[22] Bei der Darstellung des am Down-Syndrom erkrankten Jungen handle es sich um eine Veröffentlichung besonders sensibler personenbezogener Gesundheitsdaten. Für eine Veröffentlichung dieser hätte die ausdrückliche Erlaubnis der Eltern vorliegen müssen. Google habe es verabsäumt, und zwar in fahrlässiger Weise, sich des Vorliegens einer solchen Erlaubnis zu vergewissern bzw Google habe hierfür nicht die notwendigen Vorkehrungen getroffen. Zwar versichern die User in den Nutzungsbedingungen, dass nur legales Material auf die Plattform geladen wird, aber eine bloße Zustimmung in den AGBs sei vor dem Hintergrund des italienischen Datenschutzrechts nicht ausreichend.[23] Es bedürfe demnach zum einen einer ausdrücklichen datenschutzrechtlichen Belehrung und zum anderen müsste auch eine ausdrückliche Erklärung darüber erfolgen, dass dem

---

[20] *Peters*, Google Video: Die Hintergründe des Mailänder Strafurteils, http://www.telemedicus.info/article/1716.Google-Video-Die-Hintergruende-des-Mailaender-Strafurteils.html (Stand 9.5.2010).

[21] *Peters*, Google Video: Die Hintergründe des Mailänder Strafurteils, http://www.telemedicus.info/article/1716.Google-Video-Die-Hintergruende-des-Mailaender-Strafurteils.html (Stand 9.5.2010).

[22] *Peters*, Google Video: Die Hintergründe des Mailänder Strafurteils, http://www.telemedicus.info/article/1716.Google-Video-Die-Hintergruende-des-Mailaender-Strafurteils.html (Stand 9.5.2010).

[23] *Peters*, Google Video: Die Hintergründe des Mailänder Strafurteils, http://www.telemedicus.info/article/1716.Google-Video-Die-Hintergruende-des-Mailaender-Strafurteils.html (Stand 9.5.2010).

Nutzer beim Upload die Zustimmung aller im Video auftretenden Personen zur Veröffentlichung ihrer personenbezogenen Daten vorliege.[24]

Weiters ist es nach italienischem Recht tatbestandsmäßig notwendig, dass mit Gewinnerzielungsabsicht gehandelt wurde.[25] Nach Ansicht des Gerichts habe Google indirekt über Werbeschaltungen Geld verdienen wollen. Google bestreitet das allerdings, aber im fraglichen Zeitraum gab es auf „Google Italy" mehrere Anzeigenkampagnen von großen Mode- und Kosmetikmarken.[26] Des Weiteren sei dem behinderten Jungen auch ein Schaden durch das unrechtmäßige Verarbeiten von Daten bei „Google Italy" zugefügt worden, daher sei auch das letzte Tatbestandsmerkmal der italienischen Datenschutzvorschrift erfüllt.[27]

C. Schuldsprüche

Die drei Angeklagten **D. F.** und **R.** wurden wegen fahrlässiger rechtswidriger Datenverarbeitung nach Art 167 des italienischen Datenschutzgesetzes jeweils zu einer bedingten Haftstrafe von sechs Monaten verurteilt. Nach italienischem Recht haften nämlich die verantwortlichen Führungskräfte strafrechtlich für Verfehlungen ihres Unternehmens.

A. wurde freigesprochen.

---

[24] *Peters*, Google Video: Die Hintergründe des Mailänder Strafurteils, http://www.telemedicus.info/article/1716.Google-Video-Die-Hintergruende-des-Mailaender-Strafurteils.html (Stand 9.5.2010).

[25] *Peters*, Google Video: Die Hintergründe des Mailänder Strafurteils, http://www.telemedicus.info/article/1716.Google-Video-Die-Hintergruende-des-Mailaender-Strafurteils.html (Stand 9.5.2010).

[26] *Peters*, Google Video: Die Hintergründe des Mailänder Strafurteils, http://www.telemedicus.info/article/1716.Google-Video-Die-Hintergruende-des-Mailaender-Strafurteils.html (Stand 9.5.2010).

[27] *Peters*, Google Video: Die Hintergründe des Mailänder Strafurteils, http://www.telemedicus.info/article/1716.Google-Video-Die-Hintergruende-des-Mailaender-Strafurteils.html (Stand 9.5.2010).

3. Teil

Materielles Strafrecht

A. Österreichische Strafgewalt

Einmal ins Internet eingespeiste Daten sind von beinahe jedem Ort der Erde aus abrufbar, sodass eine räumliche Beschränkung auf das Territorium eines bestimmten Staates kaum möglich ist.[28] Multimediale Inhalte können mit geringem Aufwand und universaler Wirkung verbreitet werden. Einmal auf einem Web- oder Newsserver abgespeichert, stehen diese digitalisierten Informationen gleichzeitig auf allen angeschlossenen Rechnern zum Abruf bereit, können also von Nutzern in fast allen Ländern der Welt gelesen, betrachtet, angehört und auch auf die eigene Festplatte herunterkopiert werden.[29] Verschiedene Fälle von Internetkriminalität in jüngster Vergangenheit zeigen, wie irrelevant nationalstaatliche Grenzen für die Täter von Internetdelikten geworden sind.[30]

Daher stellt sich die Frage, ob österreichisches Recht überhaupt auf für im Internet begangene Straftaten anwendbar ist. Zu beantworten ist diese Frage mit den **§§ 62 ff StGB**, die das **internationale Strafrecht** regeln.

Das internationale Strafrecht erlangt aufgrund der Mobilität des modernen Menschen und der Vernetztheit der Welt immer mehr an Bedeutung.[31] Durch das internationale Strafrecht wird der räumliche und persönliche Bereich umschrieben, für den sich das österreichische Strafrecht materielle Geltung beimisst,[32] also der internationale Anwendungsbereich des österreichischen Strafrechts. Es geht daher darum, welche strafbaren Handlungen von österreichischen Gerichten zu verfolgen sind (inländische

---

28 *Plöckinger*, Zuständigkeit, ÖJZ 2001, 799.

29 *Schwarzenegger*, Geltungsbereich, ZStrR 2000, 109.

30 *Schwarzenegger*, Geltungsbereich, ZStrR 2000, 110.

31 *Kienapfel/Höpfel,* AT[13] E 12 Rz 1.

32 *Höpfel/Kathrein,* WK[2] Vorbem §§ 62-67 Rz 1; ebenso: *Michel/Wessely,* AT S. 5; so auch: *Bachner-Foregger*, StGB[22] § 62: Mit dem irreführenden Namen „internationales Strafrecht" bezeichnet man die Strafanwendungsnormen, die bestimmen, nach welchen nationalen Strafbestimmungen eine Ausländertat oder eine Auslandstat zu behandeln ist.

Gerichtsbarkeit). Es handelt sich dabei um österreichisches Recht; auch eine Verurteilung erfolgt immer nach österreichischem materiellem Strafrecht.[33] Die §§ 62 ff StGB enthalten reines Strafanwendungsrecht, bestimmen also nur, wann österreichische Strafgesetze gelten.[34] Meist werden mit dem „Internationalen Strafrecht" die sogenannten Strafanwendungsnormen in Verbindung gebracht, also jene Bestimmungen, die die Anwendung der innerstaatlichen Gesetze auf Straftaten mit internationalem Bezug regeln („Internationales Strafrecht im engeren Sinn").[35] Früher wurde die überwiegende Auffassung vertreten, dass die Staaten aufgrund ihrer Souveränität frei sind, ihre eigene Strafrechtsordnung auf internationale Sachverhalte aller Art für anwendbar zu erklären. Nunmehr ist nach herrschender Auffassung diese Normsetzungsbefugnis durch das Völkerrecht beschränkt: Ein Staat darf nur solche Straftaten seinen eigenen Strafgesetzen unterwerfen, die wenigstens einen losen Anknüpfungspunkt zu diesem Staat aufweisen; andernfalls wird das allgemeine völkerrechtliche Verbot des Rechtsmissbrauchs verletzt. Welche Anknüpfungspunkte ein Staat wählt, bleibt zwar ihm überlassen, doch muss er dabei auf die Interessen anderer Staaten an der Wahrung ihrer Rechtsordnung und dabei auf den Schutz ihrer Staatsangehörigen Rücksicht nehmen.[36]

Für die Internetkriminalität scheint eine Begrenzung des räumlichen Geltungsbereiches notwendig, da der Erfolg aller im Wege des Internets begangenen Handlungen auf der ganzen Welt eintritt. Daher reichen die Bestimmungen der §§ 62 bis 67 StGB prinzipiell aus, um eine Verfolgung der „Cyber-Kriminalität" zu gewährleisten.[37]

---

[33] *Michel/Wessely,* AT S. 5.

[34] *Schwaighofer*, SbgK Vorbem §§ 62-66 Rz 4; ebenso: *Fuchs,* AT I^7 Kap 5 Rz 20; demnach bestimmt das österreichische Strafanwendungsrecht, ob ein Verhalten, das den Tatbestand eines österreichischen Strafgesetzes erfüllt, auch dann von österreichischen Gerichten nach österreichischem Recht bestraft wird, wenn es im Ausland oder sonst mit Beziehung zum Ausland begangen worden ist; das österreichische Recht wird dabei ohne Rücksicht darauf verwendet, ob auch ein anderer Staat die Tat verfolgt oder nicht.

[35] *Schwaighofer,* SbgK Vorbem §§ 62-66 Rz 1.

[36] *Schwaighofer,* SbgK Vorbem §§ 62-66 Rz 2; so auch *Fuchs,* AT I^7 Kap 5 Rz 11: Jeder Staat darf nur dann strafen, wenn die Tat eine Beziehung zum Inland aufweist (völkerrechtlicher Anknüpfungspunkt).

[37] *Höpfel/Kathrein,* WK^2 § 67 Rz 13.

Die Anknüpfung stellt sich als nicht sehr problematisch dar, da angenommen wird, dass der im Video dargestellte misshandelte Junge die österreichische Staatsbürgerschaft besitzt und sich der Vorfall auch im Inland ereignet hat und die Täter ebenfalls Österreicher waren, die das Video dann auch in Österreich ins Internet hochgeladen haben.

Zum Inland im Sinne des internationalen Strafrechts gehören herkömmlicherweise diejenigen Räume, innerhalb derer das staatliche Strafrecht seine Aufgabe hat, den Rechtsfrieden zu begründen und zu erhalten. Gem Art 3 Abs 1 B-VG umfasst das Bundesgebiet die Summe der Gebiete der Bundesländer. Inland im strafrechtlichen Sinn umfasst somit das gesamte österreichische Staatsgebiet einschließlich der Seen und Flüsse, den Luftraum über dem Bundesgebiet sowie das Erdinnere.[38] Demnach ist Ausland jeder Ort, der nicht zum Bundesgebiet gehört, also nicht „Inland" ist, ob dieses Gebiet unter fremder oder gar keiner Staatsgewalt steht, ist belanglos.[39]

Daraus lässt sich schließen, dass österreichisches, materielles Strafrecht für anwendbar erklärt werden kann.

[38] *Höpfel/Kathrein,* WK² § 62 Rz 5.

[39] *Höpfel/Kathrein*, WK² § 62 Rz 8; so auch: *Fabrizy*, StGB [10] § 64 Rz 1.

B. Strafbarkeit der Google-Manager

I. Strafbarkeit nach italienischem Recht

1. Strafbarkeit nach dem italienischen StGB

Die Google-Manager waren nach Art 595 des italienischen StGB auch wegen des Vorwurfes der Verleumdung angeklagt, da im Video die Organisation Vivi Down namentlich in einer beleidigenden Weise, die ihre Reputation schädigt, genannt wurde, allerdings wurden die Angeklagten von Richter *Oscar Magi* freigesprochen, denn *„Das geltende italienische Recht sehe keine Pflicht zur inhaltlichen Vorabkontrolle von Videos hinsichtlich ehrverletzender Äußerungen vor“,*[40] hieß es in der Urteilsbegründung und daher könne auch keine Zuwiderhandlung der Angeklagten gegen eine solche Pflicht angenommen werden. Alleine die Uploader des Videos könnten sich nach *Magi* wegen Verleumdung strafbar gemacht haben.[41]

2. Strafbarkeit nach italienischem Datenschutzrecht

Drei der vier angeklagten Mitarbeiter von Google wurden in dem Urteil wegen der rechtswidrigen Verwendung personenbezogener Daten nach Art 167 des italienischen Datenschutzgesetzes verurteilt – genauer, wegen sensibler Daten über den Gesundheitszustand einer Person. Google habe es auch fahrlässig unterlassen, sich von der Existenz einer Einwilligung zur Veröffentlichung zu vergewissern. Ein weiteres Merkmal des Tatbestandes war die Gewinnerzielungsabsicht. Da das besagte Video häufig angesehen wurde und auch zum fraglichen Zeitraum mehrere Werbekampagnen vor allem von großen Kosmetikfirmen stattfanden, habe Google daher indirekt mit den Werbeschaltungen an dem Video Geld verdient und somit auch das Tatbestandsmerkmal der Gewinnerzielungsabsicht erfüllt.[42]

---

[40] *Peters*, Google Video: Die Hintergründe des Mailänder Strafurteils, http://www.telemedicus.info/article/1716.Google-Video-Die-Hintergruende-des-Mailaender-Strafurteils.html (Stand 9.5.2010).

[41] *Peters*, Google Video: Die Hintergründe des Mailänder Strafurteils, http://www.telemedicus.info/article/1716.Google-Video-Die-Hintergruende-des-Mailaender-Strafurteils.html (Stand 9.5.2010).

[42] *Peters*, Google Video: Die Hintergründe des Mailänder Strafurteils, http://www.telemedicus.info/article/1716.Google-Video-Die-Hintergruende-des-Mailaender-Strafurteils.html (Stand 9.5.2010).

II. Strafbarkeit nach österreichischem Recht

1. Strafbarkeit nach dem StGB

Aus dem oben dargestellten Sachverhalt[43] ergibt sich, dass folgende unter Strafe gestellte Delikte des österreichischen Strafgesetzbuches in Frage kommen könnten, und zwar **§ 83 Körperverletzung**, da der am Down-Syndrom erkrankten Jungen geschlagen wurde.

Des Weiteren kommt **§ 92 Quälen oder Vernachlässigen unmündiger, jüngerer oder wehrloser Personen** in Betracht, da sich der Junge aufgrund seiner Beeinträchtigung nicht wehren konnte.

Auch die Delikte des **vierten Abschnitts, strafbare Handlungen gegen die Ehre (§§ 111 ff)**, können in Frage kommen, weil auch Beleidigungen gegenüber dem am Down-Syndrom erkrankten Jungen gefallen sind und auch die Organisation „Vivi Down“ in der Filmsequenz namentlich erwähnt wird.

a) Wegen Körperverletzung nach § 83

Aus dem Sachverhalt geht hervor, dass der beeinträchtigte Junge geschlagen und auch mit Gegenständen beworfen wurde. Fraglich ist nun, ob der am Down-Syndrom erkrankte Jugendliche eine Körperverletzung[44] oder eine Gesundheitsschädigung[45] davongetragen hat.

---

[43] Siehe S. 8 ff.

[44] Der Ausdruck „**Verletzung am Körper**“ weist primär auf eine Substanzbeeinträchtigung hin und umfasst daher nach allgemeiner Ansicht nicht ganz unerhebliche Eingriffe in die **körperliche Integrität.** *Burgstaller/Fabrizy,* WK^2 § 83 Rz 6: ua sind Eingriffe in die körperliche Integrität: Schwellungen, Prellungen, Brüche und auch sog innere Verletzungen, etc; so auch: *Kienapfel/Schroll*, BT I^5 § 83 Rz 6: der Begriff Verletzung am Körper umfasst alle nicht ganz unerheblichen Eingriffe in die körperliche Integrität, welche über bloße körperliche Misshandlungen hinausgehen und gemeinhin als Wunden, Schwellungen, Verstauchungen, Verrenkungen, Brüche und sonstige Läsionen bezeichnet werden; ebenso: *Lewisch*, BT I^2 S. 23 und S. 24; siehe auch: *Bertl/Schwaighofer*, BT I^9 § 83 Rz 1; *Bachner-Foregger,* StGB^{22} § 83; Körperverletzung ist die Zufügung von Wunden oder zumindest ausgedehnteren Blutunterlaufungen; *Fabrizy*, StGB ^{10} § 83 Rz 2; *Messner,* SbgK § 83 Rz 46 ff.

[45] Bei der **Schädigung an der Gesundheit** geht es primär um eine Funktionsstörung. *Burgstaller/Fabrizy,* WK^2 § 83 Rz 6.

§ 83 Abs 1 besagt, dass derjenige zu bestrafen ist, der einen anderen am Körper verletzt oder an der Gesundheit schädigt, und **Abs 2** stellt auch eine Misshandlung unter Strafe, wenn dabei eine fahrlässige Verletzung oder Schädigung der Gesundheit die Folge ist. Der § 83 schützt daher die körperliche Unversehrtheit.[46] Die herrschende Meinung will vom Schutzzweck auch die Gesundheit des Menschen umfasst wissen.[47] Somit zählen sowohl die körperliche Unversehrtheit als auch die Gesundheit des Menschen zu den geschützten Rechtsgütern des § 83.

Eingriffe in sonstiges Wohlbefinden schützt § 83 nicht. So werden körperliche Misshandlungen, die nicht die Schwelle einer Körperverletzung oder Gesundheitsschädigung erreichen, nicht als Delikte gegen Leib und Leben, sondern allenfalls als Delikte gegen die Ehre eingeordnet.[48]

Aus dem Sachverhalt, der sich am an dem Vorfall, der dem italienischen Urteil zu Grunde liegt, orientiert, lassen sich keine Anhaltspunkte ableiten, die auf eine Verletzung am Körper oder eine Gesundheitsschädigung schließen lassen würden, daher ist das Delikt der Körperverletzung nach § 83 nicht verwirklicht.

Daher kann auch festgehalten werden, dass keine Strafbarkeit des Providers nach dieser Vorschrift gegeben ist.

b) Wegen Quälens wehrloser Personen nach § 92

Da den Managern von Google weder die Fürsorge noch die Obhut für den am Down-Syndrom erkrankten Jungen zukommen, scheidet diese Delikt für eine mögliche Strafbarkeit des Providers aus.

---

[46] *Kienapfel/Schroll*, BT I[5] Vorbem §§ 83 ff Rz 3; *Lewisch*, BT I[2] S. 23: § 83 Abs 1 pönalisiert die vorsätzliche Herbeiführung entweder einer Körperverletzung oder einer Gesundheitsschädigung; *Burgstaller/Fabrizy,* WK[2] § 83 Rz 3; *Messner,* SbgK § 83 Rz 7.

[47] *Messner,* SbgK § 83 Rz 7; ebenso: *Burgstaller/Fabrizy,* WK[2] § 83 Rz 3.

[48] *Burgstaller/Fabrizy,* WK[2] § 83 Rz 7; M*essner,* SbgK § 83 Rz 8; ebenso: *Kienapfel/Schroll*, BT I[5] § 83 Rz 15: körperliche Misshandlungen werden wegen ihres ehrverletzenden Charakters in erster Linie als Beleidigungen eingestuft; vgl § 115 Abs 1 3. Fall.

c) Wegen strafbarer Handlungen gegen die Ehre §§ 111 ff

Strafbare Handlungen gegen die Ehre kommen deshalb in Frage, da der beeinträchtigte Junge in der Videosequenz beschimpft und auch die Organisation „Vivi Down“ im fraglichen Video namentlich genannt wurde.[49]

Beleidigungsfähig ist grundsätzlich jeder Mensch – auch ein Kind oder Geisteskranker.[50] Bei Beleidigungen von Geisteskranken muss das Opfer allerdings den beleidigenden Charakter einer Tathandlung als solchen zumindest in Umrissen erkennen können.[51]

Aus dem oben dargestellten Sachverhalt lassen sich keine Anhaltspunkte erkennen, dass der am Down-Syndrom erkrankte Junge den beleidigenden Charakter nicht hätte erkennen können, und somit darf angenommen werden, dass dieser Junge auch beleidigungsfähig ist.

Problematisch stellt sich allerdings die Situation bei der Beleidigung der Organisation Vivi Down dar, denn das österreichische Strafgesetz stellt bei der Beleidigungsfähigkeit auf einen Menschen ab. Die Tatbilder der strafbaren Handlungen gegen die Ehre beziehen sich lediglich auf physische Einzelpersonen und die im § 116 genannten Einzelkollektive als Objekte.[52] Allerdings wird dort keine Organisation genannt, unter die Vivi Down fallen würde.

Daher ist nach dem StGB Vivi Down nicht beleidigungsfähig und deshalb scheidet eine Strafbarkeit der Manager von Google wegen der Beleidigung der Ehre der Organisation Vivi Down aus.

aa) Üble Nachrede, § 111

Beim Delikt des § 111 wird das Rechtsgut Ehre im Wege einer „Nachrede“, das ist die Zuschreibung ehrenrühriger Charakter- oder Verhaltensmängel (Schmähung), somit in

---

[49] Siehe 8 ff.

[50] *Lambauer,* SbgK Vorbem §§ 111 ff Rz 18; *Foregger,* WK^2 §§ 111-117 Rz 1: Nach § 16 ABGB hat jeder Mensch angeborene, schon durch Vernunft einleuchtende Rechte, und § 17 ABGB bestimmt: „Was den angeborenen natürlichen Rechten angemessen ist, dieses wird solange als bestehend angenommen, als gesetzmäßige Beschränkungen dieser Rechte nicht bewiesen wird“.

[51] *Lambauer,* SbgK Vorbem §§ 111 ff Rz 19; so auch: *Foregger,* WK^2 §§ 111-117 Rz 10.

[52] *Foregger,* WK^2 §§ 111-117 Rz 23.

einer ganz besonders diffamierenden und niederträchtigen Weise beeinträchtigt.[53] Keine Schmähungen sind dagegen bloße Unhöflichkeiten und Belästigungen.[54] Wenn der Täter allerdings – ohne Rücksicht auf die von ihm verwendete Wortwahl – den anderen bloß kränken will, dann handelt es sich in erster Linie um das Delikt nach § 115.[55]

Aus dem Sachverhalt gehen keine Anhaltspunkte hervor, die eine besonders diffamierende oder niederträchtige Weise belegen, es geht lediglich hervor, dass die Jugendlichen den am Down-Syndrom erkrankten Jungen beschimpft haben und daher auch nicht auf einen uU verächtlichen Charakter oder eine allgemeine nichtswürdige Einstellung des beeinträchtigten Jungen abgestellt haben. Es kann angenommen werden, dass es den Jugendlichen bei ihren Beleidigungen darauf ankam, den am Down-Syndrom erkrankten Jungen zu kränken und zu beleidigen. Damit § 111 in Frage käme, müsste sich der Vorwurf auf ein einigermaßen konkretisiertes Verhalten beziehen.[56] Die Jugendlichen beleidigen den am Down-Syndrom erkrankten Jungen ganz allgemein wegen seiner Behinderung und wollten diesen in erster Linie kränken und bloßstellen. Es werden dem beeinträchtigten Jungen keine Charakter- oder Verhaltensmängel unterstellt, denn eine körperliche bzw geistige Beeinträchtigung kann nicht als Charakter- bzw Verhaltensmangel gewertet werden, auch wenn der Junge aufgrund seiner Beeinträchtigung beleidigt und beschimpft wird. Er hat sich ja weder ehrenrührig benommen noch ein von der Gesellschaft verpöntes Verhalten an den Tag gelegt. Daher ist meines Erachtens eine Strafbarkeit nach § 111 nicht gegeben, denn die Beeinträchtigung ist einfach eine Tatsache und es wird dem Jungen nicht unterstellt, er habe sich ehrenrührig oder unmoralisch verhalten.

Somit wurde weder die erste Alternative einer möglichen Tathandlung, nämlich das Zeihen einer verächtlichen Eigenschaft oder Gesinnung, verwirklicht noch die zweite Alternative, nämlich das Beschuldigen eines anderen eines unehrenhaften oder gegen die guten Sitten verstoßenden Verhaltens.

---

[53] *Kienapfel/Schroll,* Studienbuch BT I[1] § 111; ebenso: *Kienapfel/Schroll,* BT I[5] § 111 Rz 3; *„Das geschützte Rechtsgut ist das Recht eines jeden Menschen auf achtungsvolle Behandlung und Begegnung und wird durch die üble Nachrede als Sammelbegriff für diffamierende Vorwürfe eines Charaktermangels bzw eines gegen die guten Sitten verstoßenden Verhaltens verletzt.“, Lambauer*, SbgK § 111 Rz 10.

[54] *Lambauer,* SbgK § 111 Rz 20.

[55] *Foregger,* WK[2] § 111 Rz 3.

[56] *Lambauer,* SbgK § 111 Rz 26.

Von § 111 wird die objektive Ehre geschützt. Bloße Unhöflichkeiten oder Belästigungen fallen nicht unter den Straftatbestand dieses Paragraphen – diese werden von § 115 erfasst. Daher wurde der Straftatbestand nach § 111 nicht erfüllt und deshalb ist auch eine Strafbarkeit der Google-Manager nach dieser Vorschrift nicht gegeben.

bb) Beleidigung, § 115

§ 115 verpönt Verhaltensweisen, die zwar nicht geeignet sind, die objektive Ehre[57] zu mindern, aber ihren Träger gleichwohl in der öffentlichen Meinung oder in der Meinung mehrerer herabzusetzen.[58] Die Beleidigung ist nur dann gerichtlich strafbar, wenn sie öffentlich[59] oder vor mehreren Leuten begangen wird.[60]

Im oben dargestellten Fall[61] darf angenommen werden, dass eine Mindestpublizität gegeben ist, denn die Jugendlichen haben die Beschimpfungen und die Misshandlung des am Down-Syndrom erkrankten Jungen gefilmt und anschließend auf der Internetplattform „Google Video Italy“ veröffentlicht, sodass das Video von einer Vielzahl von Menschen abgerufen werden konnte.

Die Tathandlung kann in Worten, Bildern, Gesten, Spucken und sonstigen ehrenkränkenden Kundgebungen bestehen.[62] Wesentlich ist bei der Beschimpfung (und auch bei der Verspottung) der Bedeutungsgehalt der Äußerung. Nur dann, wenn hierdurch eine Missachtung ausgedrückt werden sollte, kommt Strafbarkeit in Betracht.[63]

Aus dem Sachverhalt geht zwar der genaue Wortlaut, den die anderen Jugendlichen gegenüber dem beeinträchtigten Jungen gebraucht haben, nicht hervor, allerdings wird man annehmen dürfen, dass es sich dabei um eine in einer Beleidigung ausgedrückte

---

57 *Foregger,* WK² § 115 Rz 1: Objektive Ehre: Darunter wird die Übereinstimmung des Verhaltens eines Menschen mit den an ihn gestellten sittlichen und sozialen Forderungen in der Meinung seiner Umwelt verstanden.

58 *Foregger*, WK² § 115 Rz 2.

59 **Öffentlich** ist eine Beleidigung dann, wenn sie unmittelbar von einem größeren Personenkreis wahrgenommen werden kann. vgl § 69 StGB.

60 *Lambauer,* SbgK § 115 Rz 7.

61 Siehe S. 8.

62 *Lambauer,* SbgK § 115 Rz 11.

63 *Lambauer,* SbgK § 115 Rz 16.

Missachtung des anderen handelt. Ebenso wird eine Verspottung angenommen werden dürfen, denn das Wesen der Verspottung besteht darin, dass der Täter einen anderen lächerlich macht oder als minderwertig verhöhnt.[64] Die **Verspottung** richtet sich gegen wirkliche, angebliche oder vermeintliche Unzulänglichkeiten des Beleidigten, mögen diese unmittelbar in seiner Person oder in seinen Lebensumständen gelegen sein, unter anderem ist es Ziel der Verspottung, den Verspotteten lächerlich zu machen und ihn in den Augen anderer herabzusetzen, ohne dass freilich seiner Ehrenhaftigkeit zu nahe getreten wird.[65]

Aus dem Sachverhalt geht hervor, dass der beeinträchtigte Junge beschimpft wurde. Es kann daher angenommen werden, dass eine Verspottung stattgefunden hat.

(1) Unmittelbarer Täterschaft

Unmittelbarer Täter (= Ausführungstäter) ist, wer eine dem Wortlaut des Tatbestandes entsprechende Ausführungshandlung setzt, dessen Verhalten also der Schilderung der Tathandlung durch das Tatbild entspricht.[66]

Unmittelbare Täter sind die Jugendlichen. Für eine unmittelbare Täterschaft des Providers lassen sich aus dem Sachverhalt keine Anhaltspunkte ableiten.

(2) Beteiligung

Bestimmungstäter ist, wer einen anderen zur Ausführung einer strafbaren Handlung veranlasst, also wer dafür ursächlich ist, dass sich ein anderer zur Ausführung einer strafbaren Handlung entschließt. Bestimmung iS des § 12 zweiter Fall ist somit das Veranlassen der Tatbegehung durch Erweckung des Tatenschlusses.[67]

Im Sachverhalt lassen sich auch keine Anhaltspunkte finden, die eine Bestimmungstäterschaft der Google-Manager indizieren würde, denn es ist nicht ersichtlich, dass diese in irgendeiner Weise auf die Jugendlichen eingewirkt hätten, um

---

64 *Lambauer*, SbgK § 115 Rz 24.

65 *Kienapfel/Schroll,* Studienbuch BT I[1] § 115; ebenso: *Foregger,* WK[2] § 115 Rz 11.

66 *Fabrizy,* WK[2] § 12 Rz 18; ebenso: *Kienapfel/Höpfel*, AT[13] E 3 Rz 3.

67 *Fabrizy,* WK[2] § 12 Rz 42.

zu erreichen, dass der beeinträchtigte Junge beleidigt worden wäre. Demnach scheidet die Bestimmungstäterschaft aus.

Die **Beitragstäterschaft** (§ 12 dritter Fall) ist eine Generalklausel für jede Mitwirkung an der Tat, die nicht unmittelbare Täterschaft oder Bestimmungstäterschaft ist.[68] Beitragstäter ist, wer eine andere für den Tatablauf kausale Handlung setzt, der Beitrag zur Ausführung der Tat kann physisch oder psychisch sein. Letzteres etwa durch Erteilung von Ratschlägen oder Bestärken im Tatentschluss.[69]

Es stellt sich nun die Frage, ob der beeinträchtigte Junge dennoch beleidigt und das Video gemacht worden wäre, wenn Google nicht die Möglichkeit zur Veröffentlichung solcher „Happy-Slapping"-Videos bieten würde. Daher ist zu überlegen, ob die Manager einen Beitrag zur Tat geleistet haben, indem sie Speicherplatz zur Verfügung gestellt haben.

Es kommt eine mögliche fahrlässige Beteiligung der Google-Manager in Frage. Längere Zeit war eine fahrlässige Beteiligung umstritten, jedoch wird diese nun von der herrschenden Lehre und der Rechtsprechung bejaht.[70] Voraussetzung ist allerdings, dass der Beteiligte gegen eine ihn selbst treffende deliktstypische objektive Sorgfaltspflicht verstoßen und auch subjektiv sorgfaltswidrig gehandelt hat.[71]

Allerdings wird man bei diesem Fall die objektive Zurechnung des Erfolges ausschließen können. Zwar ist der Adäquanzzusammenhang gegeben, denn es liegt innerhalb der allgemeinen Lebenserfahrung, dass das Bereitstellen von Speicherplatz auch zu einem Missbrauch führen kann und auf diesen zB beleidigende Videos geladen werden, weiters ist auch hier der Erfolgseintritt vorhersehbar. Allerdings ist der Risikozusammenhang nicht gegeben, denn es ist per se nicht rechtswidrig, seinen Nutzern Speicherplatz zur Verfügung zu stellen.

Daher kann die objektive Zurechnung verneint werden und die Google-Manager sind nicht nach § 115 strafbar.

---

68 *Fabrizy,* WK² § 12 Rz 81.

69 *Fabrizy,* WK² § 12 Rz 82.

70 *Fabrizy*, WK² § 12 Rz 106; ebenso: *Kienapfel*, AT E 3 Rz 34, E 5 Rz 1 und 28.

71 *Fabrizy*, WK² § 12 Rz 107.

Auch das körperliche Misshandeln ist eine mögliche Tathandlung des § 115. Misshandlung am Körper ist jedes Einwirken auf den Körper eines anderen, das dessen Wohlbefinden nicht unerheblich beeinträchtigt.[72] Aus dem Sachverhalt[73] geht hervor, dass der am Down-Syndrom erkrankte Junge von den anderen auch geschlagen und mit Gegenständen beworfen wurde.

Wiederum sind die unmittelbaren Täter die Jugendlichen, eine Bestimmungstäterschaft der Google-Manager kann ausgeschlossen werden, da keine Indizien im Sachverhalt sind, dass diese auf die Jugendlichen in irgendeiner Weise eingewirkt hätten, damit jene den beeinträchtigten Jungen misshandeln. Eine Täterschaft durch einen sonstigen Beitrag kann weiters ausgeschlossen werden, da auch hier keine objektive Zurechnung des Erfolgs möglich ist, da der Risikozusammenhang nicht gegeben ist, denn das Bereitstellen von Speicherplatz ist, wie schon erwähnt, an sich nicht rechtswidrig.

d) Zwischenresümee

Zusammenfassend lässt sich demnach festhalten, dass es keine Strafbarkeit der Google-Manager nach dem StGB gibt, da sich bei keinem der oben dargestellten Delikte auch nur eine Beteiligung dieser an einer möglicherweise von den Jugendlichen begangenen unter Strafe gestellten Handlungen hätte feststellen lassen, und schon erst recht kann keine unmittelbare Täterschaft angenommen werden kann, da sich hierfür keine Indizien aus dem Sachverhalt ergeben.

Für das Delikt der Körperverletzung nach § 83 lassen sich keine Anhaltspunkte im Sachverhalt finden, der dem Mailänder Strafurteil zu Grunde liegt, die darauf schließen ließen, dass der beeinträchtigte Junge eine Körperverletzung bzw Schädigung an der Gesundheit davongetragen hätte.

Wie bereits oben dargestellt, ergibt sich nach § 92 – Quälen oder Vernachlässigen unmündiger, jüngerer oder wehrloser Personen – keine Strafbarkeit für die Manager von

---

[72] *Lambauer,* SbgK § 115 Rz 28.

[73] Siehe S. 8 ff.

Google, da diese keine Fürsorge- bzw Obsorgeverpflichtung gegenüber dem am Down-Syndrom erkrankten Jungen trifft.

Aus dem Sachverhalt lässt sich weder eine Strafbarkeit nach § 111 1. Alternative (Schmähung) ableiten, da die Beleidigungen in keiner besonders diffamierenden oder niederträchtigen Weise erfolgt sind, denn es ging den Jugendlichen vermutlich bloß um die Kränkung des beeinträchtigten Jungen und weiters ist eine körperliche bzw geistige Beeinträchtigung kein ehrenrühriger Charakter- bzw Verhaltensmangel, noch lässt sich eine Strafbarkeit nach der 2. Alternative (eine Person eines unehrenhaften oder gegen die guten Sitten verstoßenden Verhaltens beschuldigen) ableiten, denn eine Beeinträchtigung verstößt nicht gegen die guten Sitten bzw ist kein unehrenhaftes Verhalten. Die Jugendlichen konfrontieren den beeinträchtigen Jungen mit der Tatsache seiner Behinderung und unterstellen diesem jedoch keinen Verhaltens- oder Charaktermangel. Daher hat es sich vermutlich um bloße Unhöflichkeiten bzw Belästigungen seitens der Jugendlichen gehandelt. Denn den Jugendlichen kam es nicht auf ihren Wortlaut an, als sie den Jugendlichen beschimpft haben. Vielmehr ging es ihnen darum, den am Down-Syndrom erkrankten Jungen zu demütigen und bloßzustellen. Somit wurde auch der Straftatbestand nach § 111 nicht erfüllt.

Jedoch ist das Delikt der Beleidigung nach § 115 vollendet, allerdings kann eine Beteiligung der Manager an diesem Delikt ausgeschlossen werden, da der Erfolg nicht objektiv zugerechnet werden kann, denn das Zur-Verfügung-Stellen von Speicherplatz ist per se nicht strafbar und somit auch kein Verstoß gegen den Schutzzweck einer Norm. Des Weiteren würde es meines Erachtens auch zu weit führen, wenn man den Provider alleine für das Bereitstellen von Speicherplatz zur Verantwortung ziehen würde.

Daher lässt sich abschließend festhalten, dass es keine Strafbarkeit der Google-Manager nach dem StGB für das User-Video gibt.

e) Begehung durch Unterlassung

Das einzige Delikt des StGB, das verwirklicht wurde, ist die **Beleidigung nach § 115**. Allerdings wurde eine Strafbarkeit der Google-Manager wegen Beteiligung durch sonstigen Beitrag ausgeschlossen, da der Erfolg objektiv nicht zurechenbar war.

Nun ist zu prüfen, ob bei diesem Delikt auch eine Begehung durch Unterlassung möglich ist.

aa) Kontrollmöglichkeit: Host-Provider

Bei Google handelt es sich in dem dieser Arbeit zu Grunde liegenden Fall um einen Host-Provider.[74]

Der Host-Provider stellt seinen Kunden Speicherplatz auf seinem Server zur Verfügung und seine Kunden können auch strafrechtlich relevante Inhalte auf den Speichermedien des Providers ablegen. Fraglich ist nun, ob sich der Provider auch für diese Inhalte verantworten muss, auch wenn sie gar nicht seiner Kontrolle unterliegen. Da es mittlerweile eine Vielzahl von Internetusern gibt, ist es für einen Provider nahezu unmöglich, jede einzelne Webpage auf ihren Inhalt zu prüfen. Derzeit besteht auch keine gesetzliche Verpflichtung, dass ein Provider die auf seinem Server abgespeicherten Daten überprüft.

Erlangt der Provider jedoch Kenntnis von strafrechtlich relevanten Inhalten, egal auf welche Weise – sei es durch Zufall, bei einer Prüfung oder aufgrund von Hinweisen – so ist er verpflichtet, zu reagieren und die strafrechtlich relevanten Inhalte zu sperren.[75] Wird vom Provider keine Kenntnis von den strafrechtlich relevanten Inhalten erlangt, so kann auch eine Begehung durch Unterlassung in Frage kommen, denn eine Begehung durch aktives Tun wird man ausscheiden können, da das bloße Zur-Verfügung-Stellen von Speicherplatz für seine Kunden nicht strafbar ist, auch wenn dadurch strafbare Inhalte verbreitet werden.

Das österreichische Strafrecht kennt zwei Arten von Unterlassungsdelikten, nämlich die echten und die unechten Unterlassungsdelikte. Bei den echten Unterlassungsdelikten

---

[74] Siehe S. 7.

[75] Vgl Art 15 EC-RL; § 16 ECG.

(auch schlichte Unterlassungsdelikte) steht die Nichtvornahme des gebotenen Tuns unter Strafe.[76] Unechte Unterlassungsdelikte sind Delikte, bei denen das Gesetz die Herbeiführung eines Erfolgs durch Nichtvornahme eines gebotenen Tuns mit Strafe bedroht.[77]

Bei § 115 handelt es sich um ein unechtes Unterlassungsdelikt, da dieses ein Erfolgsdelikt ist.

bb) Voraussetzungen: Unechte Unterlassungsdelikte

Erforderlich für eine Begehung durch Unterlassung ist, dass den Provider eine Garantenstellung nach § 2 trifft.

> *„Bedroht das Gesetz die Herbeiführung eines Erfolges mit Strafe, so ist auch strafbar, wer es unterläßt, ihn abzuwenden, obwohl er zufolge einer ihn im besonderen treffenden Verpflichtung durch die Rechtsordnung dazu verhalten ist und die Unterlassung der Erfolgsabwendung einer Verwirklichung des gesetzlichen Tatbildes durch ein Tun gleichzuhalten ist.“*

Daraus folgt, dass eine Garantenstellung nur aufgrund von Rechtspflichten begründet werden kann. Diese ergeben sich entweder unmittelbar aus einem Gesetz oder werden aus der Rechtsordnung abgeleitet und die Garantenstellung muss den Täter persönlich treffen. Daher sind die Entstehungsgründe für eine Garantenstellung eine Rechtsvorschrift, eine enge natürliche Verbundenheit, eine freiwillige Pflichtübernahme, eine Gefahrengemeinschaft, gefahrbegründendes Vorverhalten sowie die Überwachung von Gefahrenquellen[78] (Garantenstellung aus allgemeinen Sicherungspflichten).

Da keine der oben dargestellten Rechtsvorschriften den Provider in die Pflicht nimmt und auch keine Kontrolle der Inhalte verlangt wird, wird man auch eine **Garantenstellung aufgrund einer Rechtsvorschrift** ausschließen können.

---

[76] *Kienapfel/Höpfel,* AT[13] Z 28 Rz 1.
[77] *Kienapfel/Höpfel,* AT[13] Z 28 Rz 9.
[78] *Kienapfel/Höpfel,* AT[13] Z 30 Rz 6.

Ebenso wird man dem Provider keine **Garantenstellung aufgrund enger natürlicher Verbundenheit** unterstellen können, denn eine natürliche Verbundenheit begründet nur dann eine Garantenstellung iSd § 2, wenn sie eng ist und eine rechtliche (insb durch zumindest faktische Übernahme einer Beschützerfunktion konkretisierte) und nicht bloß sittlich-moralische Grundlage besitzt.[79]

Auch eine **Garantenstellung aus Gefahrengemeinschaft** kann man für den Provider ausschließen, denn diese würde begründet, wenn sich mehrere Personen zu dem Zweck verbunden haben, durch ihren Zusammenschluss die Chancen zur Bewältigung eines gefährlichen Unternehmens zu erhöhen.[80] Grundsätzlich kann allerdings nicht angenommen werden, dass das Internet eine gefährliche Unternehmung darstellt.

Eine **Garantenstellung aus freiwilliger Pflichtübernahme** entsteht üblicherweise durch einen Vertrag. Zwar wird meist ein Vertrag zwischen dem einzelnen User und dem Host-Provider geschlossen werden, jedoch wird in keinem dieser Verträge vorgesehen sein, dass der Provider bei Unkenntnis der Inhalte auch eine Rechtmäßigkeit dieser garantieren wird, denn der Provider hat ja auch nicht die (technischen) Möglichkeiten, die einzelnen Inhalte eines jeden zu kontrollieren.

Weiters können auch andere Benutzer an die Inhalte, die auf den Speichermedien des jeweiligen Providers liegen, gelangen und mit diesen „Dritten“ besteht überhaupt kein Vertragsverhältnis und aus diesem Grund wird auch keine Garantenstellung aus freiwilliger Pflichtübernahme gegeben sein.

Die **Garantenstellung aus Ingerenz**, also aus vorangegangenem gefahrbegründendem Tun, entsteht durch die nahe „adäquate“ Gefahr des einen Schadenseintritt auslösenden vorangegangenen Tuns.[81]

Daher stellt sich nun die Frage, ob das Zur-Verfügung-Stellen von Speicherplatz als objektiv pflichtwidriges Verhalten gilt und eine Gefahr für fremde Rechtsgüter darstellt.

Eine solche Verantwortlichkeit wäre zu bejahen, wenn es rechtlich und tatsächlich möglich wäre, die Inhalte der Internet-Angebote auf strafbares Material zu durchsuchen und der Provider zu einer solchen Kontrolle verpflichtet wäre. Durch den Betrieb von

---

79 *Kienapfel/Höpfel,* AT[13] Z 30 Rz 12.

80 *Kienapfel/Höpfel,* AT[13] Z 30 Rz 16.

81 *Finke*, Verantwortung, S. 125.

Rechnern im Internet kann zwar eine nahe und adäquate Gefahr für eine Verbreitung von strafrechtlich relevanten Inhalten entstehen, dieser Betrieb ist aber per se nicht rechtswidrig.[82]

Daher wird man dem Host-Provider keine Garantenstellung zusprechen können, wenn er lediglich Speicher zur Verfügung stellt.

Eine **Garantenstellung aus einer allgemeinen Sicherungspflicht** kann unabhängig von einem Vorverhalten für von bestimmten Sachen ausgehenden Gefahren bestehen. Allerdings wird man auch hier dem Provider keine generelle Garantenstellung für sämtliche über seinen Dienst verbreitete und transportierte Inhalte anlasten können. Eine solche Art der Garantenstellung wäre nämlich nur dann gegeben, wenn der Provider Kenntnis erlangt hätte, dass über ihn strafrechtlich relevante Inhalte verbreitet werden, und der Provider trotz Kenntnis untätig bliebe.

Zusammenfassend ist somit festzuhalten, dass den Host-Provider keine Garantenstellung trifft, solange er keine Kenntnis von den strafrechtlich relevanten Inhalten auf seinen Speichermedien hat. Eine Garantenstellung trifft ihn erst, wenn er, egal aus welchem Grund auch immer, sei es Zufall, Hinweise oder Kontrolle, Kenntnis von den Inhalten erlangt und dennoch untätig bleibt und diese nicht sperrt und bzw oder löscht.

Daher ist auch eine Strafbarkeit der Google-Manager wegen Begehung durch Unterlassung an der Beteiligung nach § 115 nicht gegeben.

---

[82] *Finke*, Verantwortung, S. 125.

2. Strafbarkeit der Google-Manager nach dem VbVG

Das Verbandsverantwortlichkeitsgesetz (VbVG) kann möglicherweise bei der Frage der Verantwortlichkeit des Providers zum Tragen kommen, wenn die Führungskräfte des Internetdienstanbieters zur Verantwortung gezogen werden sollen. Im Urteil des Mailänder Bezirksgerichts in Strafsachen wurden Manager von Google Ende Februar 2010 wegen eines User-Videos auf „Google Video Italy" verurteilt.

Das Verbandsverantwortlichkeitsgesetz regelt, *„unter welchen Voraussetzungen Verbände für Straftaten verantwortlich sind",*[83] Verbände iSd VbVG sind unter anderem juristische Personen.[84] Somit fällt der Provider Google unter die Anwendung des VbVG, da Google als „Google Inc" auftritt, und auch im Impressum festgehalten wird, dass Google eine registrierte Gesellschaft ist.[85]

Allerdings ist eine Strafbarkeit nach dem StGB Voraussetzung für eine Strafbarkeit nach dem VbVG. Die Strafbarkeit der Google-Manager nach dem StGB wurde allerdings ausgeschlossen.[86] Daher ist auch keine Anwendbarkeit des VbVG gegeben.

Es wäre zwar denkbar, die Manager für die Handlungen der Jugendlichen nach dem VbVG zur Verantwortung zu ziehen, denn in § 3 Abs 3 VbVG ist die *Verantwortlichkeit für eine Tat von Mitarbeitern* verankert. Allerdings ergeben sich aus dem Sachverhalt keine Anhaltspunkte, dass die Jugendlichen, die für das User-Video und auch die Misshandlungen verantwortlich waren, Mitarbeiter von Google sind, da sich keine Indizien für ein arbeitnehmerähnliches Verhältnis oder ein sonstiges Dienstverhältnis ergeben, und daher scheidet auch hier die Verantwortlichkeit des Verbandes aus.

Zusammenfassend kann somit festgestellt werden, dass eine Anwendbarkeit des Verantwortlichkeit VbVG nicht gegeben ist.

---

[83] Vgl § 1 Abs 1 VbVG; siehe Anhang S. 52.

[84] Vgl § 1 Abs 2 VbVG; siehe Anhang S. 52.

[85] Impressum von Google Inc http://www.google.at/intl/de/impressum.html (Stand 25.1.2011).

[86] Siehe S. 23.

3. Strafbarkeit der Google-Manager nach dem DSG 2000

Der **§ 51 DSG 2000** stellt die **Datenverwendung in Gewinn- oder Schädigungsabsicht** unter Strafe und lautet:

> *„Wer mit dem Vorsatz, sich oder einen Dritten dadurch unrechtmäßig zu bereichern, oder mit der Absicht, einen anderen dadurch in seinem von § 1 Abs. 1 gewährleisteten Anspruch zu schädigen, personenbezogene Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat, selbst benützt, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat, ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.“*

Für den Datenschutz im Internet sind die rechtlichen Bestimmungen des DSG 2000 maßgebend. Im DSG 2000, das am 1.1.2000 in Kraft trat, wurde die EG-Datenschutzrichtlinie[87] in österreichisches Recht umgesetzt. Das DSG 2000 möchte den Gefahren entgegenwirken, die von den nahezu unbegrenzten Möglichkeiten der Speicherung und Verarbeitung von Daten in elektronischen Datenverarbeitungsanlagen oder anderen Datensammlungen ausgehen.[88]

Im DSG 2000 wurde sowohl eine gerichtliche Strafbarkeit als auch eine verwaltungsstrafrechtliche Bestimmung verankert. Allerdings ist das Verwaltungsstrafrecht nicht Thema dieser Arbeit.

Durch die DSG-Novelle 2010[89] wurde aus dem bisherigen Ermächtigungsdelikt des § 51 DSG 2000 ein Offizialdelikt.

---

87 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 1995 L 281 vom 23.11.1995.

88 *Berka*, Verfassungsrecht, Rz 1407.

89 BGBl I Nr 133/2009.

Aus dem Sachverhalt[90] geht hervor, dass eine Verurteilung auch stattgefunden hat, weil der im Video dargestellte Junge am Down-Syndrom erkrankt ist und es sich – nach italienischem Recht – um sensible personenbezogene Daten handelt.

Der § 51 des DSG 2000 ist das österreichische Pendant zu Art 167 des italienischen Datenschutzgesetzes, nach dem im Februar 2010 die Verurteilung der Google-Manager in Mailand erfolgte.

Die Tathandlung des § 51 DSG 2000 kann in einer **Nutzung**, einem **Zugänglich-Machen** oder **Veröffentlichen** von personenbezogenen Daten, die einem aufgrund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich gemacht wurden, bestehen.

a) Personenbezogene Daten

Nach § 4 Abs 1 Z 1 DSG 2000 sind personenbezogene Daten Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist. Das DSG 2000 bezieht sich ausschließlich auf die Verarbeitung personenbezogener Daten. „Sensible Daten“, also besonders schutzwürdige Daten, sind Daten natürlicher Personen über ihre rassische oder ethnische Herkunft, politische Meinung und auch über ihre Gesundheit.[91]

Das Video gibt Auskunft über die Gesundheit des am Down-Syndrom erkrankten Jungen, da im Video Angaben über seine körperliche bzw geistige Beeinträchtigung gemacht werden. Es handelt sich daher um personenbezogene, sensible Daten.

Weiters kann man auch davon ausgehen, dass dem Provider die Daten aufgrund seiner berufsmäßigen Beschäftigung zumindest zugänglich gemacht wurden, in dem seine User die Daten auf den Host des Providers abspeichern.

---

[90] Siehe S. 8 ff.

[91] Vgl § 4 Abs 1 Z 2 DSG 2000.

b) Tathandlung

Der Provider hat die Tathandlung der Veröffentlichung verwirklicht, indem das Video auf seiner Website veröffentlicht wurde.

Bei dem Delikt der Datenverwendung in Gewinn- oder Schädigungsabsicht nach § 51 DSG 2000 reicht ein bedingter Vorsatz aus.[92] Diesen könnte man dadurch annehmen, indem Google in seinen Nutzungsbedingungen[93] erklärt, dass *„Google die Daten nicht auf ihre Rechtmäßigkeit überprüft"*. Wenn Google es daher unterlässt, die Daten zu überprüfen, muss davon ausgegangen werden, dass Google es zumindest für möglich halten muss, dass die Speicherkapazitäten auch missbräuchlich zB zur Speicherung von rechtswidrigen Daten, unter anderem sensibler personenbezogener Daten, verwendet werden. Die Vergangenheit hat ja auch gezeigt, dass ständig rechtswidriges Material auf Websites im Internet kursiert, Google muss sich dessen auch bewusst sein und versucht sich relativ einfach durch solche Passagen in den Nutzungsbedingungen aus der Verantwortung zu stehlen.

Durch die unterlassene Kontrolle der User-Daten könnte daher ein zumindest bedingter Vorsatz des Providers nach der Strafbestimmung des § 51 DSG 2000 angenommen werden, denn der Provider muss damit rechnen, dass auf seinem Speicher auch rechtswidrige Daten abgelegt werden, die uU gegen das Datenschutzrecht verstoßen. Allerdings besagt § 93 TKG 2003, dass die „*Inhaltsdaten dem Kommunikationsgeheimnis*"[94] unterliegen.

Auf der einen Seite ergibt sich daher möglicherweise eine Strafbarkeit des Providers, weil dieser es unterlässt, die Daten zu überprüfen, und auf der anderen Seite kann dieser sich gerade deshalb strafbar machen, wenn der Provider die Inhaltsdaten seiner User kontrolliert. Nach dem TKG 2003 ist daher aus Gründen des Schutzes des

---

92 § 7 Abs 1 iVm § 5 Abs 1 2. Halbsatz StGB: *„Wenn das Gesetz nichts anderes bestimmt, ist nur vorsätzliches Handeln strafbar"* und *„…dazu genügt es, daß der Täter diese Verwirklichung ernstlich für möglich hält und sich damit abfindet"* = bedingter Vorsatz (dolus eventualis).

Nach Art 1 Abs 1 StrAnpG 1974 sind nämlich *„die Bestimmungen des Allgemeinen Teils des StGB auch auf Taten anzuwenden, die in anderen auf Gesetzesstufe stehenden, als Bundesrecht geltenden Rechtsvorschriften mit gerichtlicher Strafe bedroht werden."*

93 Nutzungsbedingungen von Google http://www.google.com/accounts/TOS (Stand 1.6.2011).

94 Näheres zum Kommunikationsgeheimnis nach § 93 TKG 2003 siehe S. 41.

Kommunikationsgeheimnisses eine Vorabkontrolle der auf den Servern abgespeicherten Daten nur mit einem triftigen Grund zulässig.

Es stellt sich nun die Frage, ob der Provider die Daten überhaupt kontrollieren darf, denn ohne diese Möglichkeit wäre ein Vorsatz nach § 51 DSG 2000 nicht möglich.

Da der § 93 TKG 2003 eine Legaldefinition des Kommunikationsgeheimnisses nach Art 10a StGG enthält, ergibt sich eine sehr eingeschränkte Möglichkeit der Haftenden, die übermittelten Inhalte auf gesetzwidrige Inhalte zu kontrollieren. Meines Erachtens ist es daher für den Provider erst dann möglich, die User-Daten einer Kontrolle zu unterziehen, wenn ein triftiger Grund dafür vorliegt oder der Benutzer seine Einwilligung zu einer Überprüfung der Daten gibt. Eine Vorabkontrolle ohne diese Einwilligung bzw. ohne triftigen Grund würde deshalb einen Verstoß gegen das Kommunikationsgeheimnis bedeuten.

Daher kann man auch den bedingten Vorsatz bei § 51 DSG 2000 nicht auf Grund der unterlassenen Kontrolle annehmen, denn der Provider darf nicht ohne Weiteres die Daten seiner User kontrollieren.

c) Schutzwürdiges Geheimhaltungsinteresse des Betroffenen

§ 51 DSG 2000 pönalisiert die Nutzung, das Zugänglichmachen oder Veröffentlichen der personenbezogen Daten, wenn *„der Betroffenen an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat“*. § 9 DSG 2000 enthält eine taxative Aufzählung, wann dieses schutzwürdige Geheimhaltungsinteresse bei der Verwendung[95] von sensiblen Daten des Betroffenen[96] nicht verletzt wird.[97] Allerdings kommt kein Aufzählungspunkt in Frage, der eine Verwendung erlauben würde, da zB der Betroffene die Daten nicht selbst veröffentlicht hat (Z 1) und auch keine Zustimmung des Betroffenen nach Z 6 vorlag.

Daher wurde das schutzwürdige Geheimhaltungsinteresse des Betroffenen verletzt.

---

[95] § 4 Z 8 DSG 2000: *Verwenden von Daten: jede Handhabung von Daten, also sowohl das Verarbeiten (Z 9) als auch das Übermitteln (Z12)*.

[96] § 4 Z 3 DSG 2000: *„Betroffener“: jede vom Auftraggeber (Z4) verschiedene natürliche Person …, deren Daten verwendet (Z8) werden“*.

[97] Siehe § 9 DSG 2000; Anhang S. 55.

d) Unrechtmäßige Bereicherung

§ 51 DSG 2000 verlangt zudem als erweiterten Vorsatz einen Bereicherungsvorsatz:

„Wer mit dem Vorsatz, sich oder einen Dritten dadurch unrechtmäßig zu bereichern, …, personenbezogene Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung … zugänglich geworden sind … veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat…“

Bei diesem erweiterten Vorsatz ist daher – über den Vorsatz zB der Veröffentlichung der Daten hinaus – ein Bereicherungsvorsatz notwendig, dh, dass durch die Verwendung der Daten das eigene Vermögen oder das Vermögen eines Dritten vermehrt wird.

aa) Bereicherung

Bei der Bereicherungskomponente ist zu prüfen, ob der Täter eine Vermögensvermehrung bewirken wollte.[98] Aus dem Sachverhalt[99] geht hervor, dass auf *„Google Video“* Werbeinserate von großen Kosmetikfirmen geschalten waren, wodurch Google bei jedem Aufruf der Seite Geld bekam. Daher wird man annehmen können, dass Google eine Vermehrung des eigenen Vermögens bewirken wollte und daher auch der Bereicherungsvorsatz gegeben ist. Dabei handelt es sich um eine mittelbare Bereicherung, denn Google verdiente indirekt bei jedem „Klick“.

bb) Unrechtmäßigkeit der Bereicherung

Die vom Täter gewollte Bereicherung ist unrechtmäßig, wenn der Bereicherte keinen Anspruch auf die Vermehrung des Vermögens hat.[100]

---

98 *Kienapfel/Schmoller*, BT II § 133 Rz 88.

99 Siehe S. 8 ff.

100 *Kienapfel/Schmoller*, BT II § 133 Rz 88.

Zulässigkeit der Datenverwendung

Das DSG 2000 sieht für die Beantwortung der Frage, ob eine konkrete Datenverwendung zulässig ist, eine zweistufige Zulässigkeitsprüfung vor: Zunächst ist der Zweck der Datenverarbeitung anhand der Berechtigung des Auftraggebers[101] zu überprüfen. In einem weiteren Schritt ist zu ermitteln, ob schutzwürdige Geheimhaltungsinteressen verletzt werden, wobei zwischen „sensiblen" und „nicht-sensiblen" Daten zu unterscheiden ist.[102]

Nach den allgemeinen Grundsätzen des § 7 Abs 1 DSG 2000 dürfen Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden. Sie müssen für den Zweck der Datenanwendung wesentlich sein und dürfen darüber nicht hinaus gehen.[103]

Die Daten wurden von den Jugendlichen selbst durch das Filmen des Jungen gesammelt. Aus dem Sachverhalt gehen keine Indizien hervor, dass diese dazu eine Berechtigung gehabt hätten, ganz im Gegenteil, denn das Misshandeln und Beleidigen eines beeinträchtigten Menschen kann keinesfalls rechtmäßig sein. Auch kann dieses Filmen keinesfalls unter § 7 Abs 1 DSG 2000 fallen, der besagt, dass diese Daten nur für eindeutige und rechtmäßige Zwecke ermittelt werden dürfen. Das Misshandeln und Filmen wird nie ein rechtmäßiger Zweck zur Datenermittlung sein. Daher kann von keiner Berechtigung der Auftraggeber gesprochen werden.

Bei der Darstellung des am Down-Syndrom erkrankten Jungen handelt es sich um sensible personenbezogene Daten und auch seine schutzwürdigen Geheimhaltungsinteressen[104] wurden durch die Veröffentlichung verletzt. Daher war die Datenverwendung unrechtmäßig.

Eine Unrechtmäßigkeit der Bereicherung selbst ist nicht gegeben, da diese auf der Werbung basiert und nicht auf der Verwendung der Daten selbst. Daher ist dieses Tatbestandsmerkmal nicht erfüllt, da diese Art der Werbung als solche rechtmäßig ist.

---

[101] § 4 Abs 1 Z 4: *„Auftraggeber ist jede natürliche oder juristische Person oder Personengemeinschaft, die die Entscheidung getroffen hat, Daten für einen bestimmten Zweck zu verarbeiten"*.

[102] *Jahnel*, Datenschutz, ecolex 2001, 86.

[103] *Jahnel*, Datenschutz, ecolex 2001, 86.

[104] Vgl § 9 DSG 2000.

Der Tatbestand des § 51 DSG 2000 mit der Variante unrechtmäßige Bereicherung wurde vom Provider nicht erfüllt und daher ist dieser nach österreichischem Recht auch nicht strafbar.

e) Schädigungsvorsatz nach § 1 Abs 1 DSG 2000

Weiters pönalisiert § 51 DSG 2000 eine Schädigung des Betroffenen in seinem Grundrecht auf Datenschutz:

„Wer ... mit der Absicht, einen anderen dadurch in seinem von § 1 Abs. 1 gewährleisteten Anspruch zu schädigen, personenbezogene Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung ... zugänglich geworden sind ... veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat…“

Hierbei handelt es sich um einen erweiterten Vorsatz als Alternative zum Bereicherungsvorsatz.

Nach § 1 Abs 1 DSG 2000 hat jedermann einen grundrechtlichen Anspruch auf Geheimhaltung der ihn betreffenden personenbezogen Daten, soweit daran ein schutzwürdiges Interesse, besonders im Hinblick auf Achtung seines Privat- und Familienlebens, besteht.[105] Dieses Recht kann nur mit Zustimmung des Betroffenen oder zur Wahrung überwiegender berechtigter Interessen eines anderen eingeschränkt werden. Dem Grundrecht auf Datenschutz wird auch eine unmittelbare Drittwirkung zuerkannt.[106] Dieses Grundrecht ist nach § 1 Abs 5 DSG 2000 „auf dem Zivilrechtsweg“ geltend zu machen, soweit Rechtsträger, die in Formen des Privatrechts eingerichtet sind, tätig werden. Es steht somit fest, dass der Verfassungsgesetzgeber mit dieser Formulierung eine Drittwirkung begründen wollte, dh angeordnet hat, dass der hier verankerte Geheimhaltungsanspruch auch von privaten Rechtssubjekten beachtet werden muss. Bei dieser Geltungsanordnung handelt es sich zugleich um die Anordnung einer unmittelbaren Drittwirkung.[107]

---

[105] *Berka*, Verfassungsrecht, Rz 1264.
[106] *Jahnel*, Datenschutz, ecolex 2001, 85.
[107] *Berka*, Verfassungsrecht, Rz 1264.

Eine Absicht zur Schädigung im Grundrecht auf Datenschutz wird man Google nicht unterstellen können, denn *„der Täter handelt absichtlich, wenn es ihm darauf ankommt, den Umstand oder Erfolg zu verwirklichen, für den das Gesetz absichtliches Handeln voraussetzt.*[108] Google hat es zwar in Kauf genommen, dass auch rechtswidrige Daten auf dem Host abgelegt und auch sensible Daten veröffentlicht werden, allerdings kann hier von keiner Absicht gesprochen werden. Google kam es nicht darauf an, den am Down-Syndrom erkrankten Jungen in seinem Grundrecht auf Datenschutz zu schädigen. Daher ist eine Strafbarkeit des Providers nach dieser Variante – absichtliche Schädigung des Grundrechts auf Datenschutz – nicht gegeben.

f) Anwendung von österreichischem Datenschutzrecht

Grundsätzlich ist das DSG 2000 auf jede Datenverarbeitung in Österreich anzuwenden. Eine Durchbrechung des Territorialitätsprinzips besteht aber zu Gunsten des Sitzstaates innerhalb der EU. Dies bedeutet, dass auf eine Datenverarbeitung in Österreich dann das Recht des Sitzstaates (eines anderen EU-Staates) anzuwenden ist, wenn Daten in Österreich für einen Auftraggeber des privaten Bereichs aus einem anderen EU-Staat verarbeitet werden, ohne dass der Auftraggeber eine feste Betriebsstätte in Österreich hat.[109]

Im Prinzip existiert kein Auftraggeber, da die Jugendlichen die Daten selbst – durch das Filmen des Jungen – gesammelt und veröffentlicht haben.

Wäre Google Auftraggeber für die Datenanwendung, dann wäre – nach dem Prinzip des Sitzstaates – deutsches Datenschutzrecht anzuwenden, denn die von Österreich nächstgelegene Niederlassung befindet sich in München.[110] Es wird angenommen, dass der geschädigte Junge die österreichische Staatsbürgerschaft besitzt und der Vorfall sich im Inland ereignet hat, daher kommt österreichisches Datenschutzrecht, nämlich das DSG 2000, zur Anwendung.

---

[108] Siehe § 5 Abs 2 StGB.

[109] *Jahnel*, Datenschutz, ecolex 2001, 86.

[110] Standorte von Google Inc http://www.google.at/corporate/address.html (25.1.2011).

g) Zwischenergebnis

Der Provider ist nach § 51 DSG 2000 nicht strafbar. Google hat zwar sensible personenbezogene Daten, nämliche solche, die über den Gesundheitszustand des Betroffenen (Erkrankung am Down-Syndrom) Aufschluss geben, veröffentlicht. Das schutzwürdige Geheimhaltungsinteresse des beeinträchtigten Jungen wurde weiters durch diese Veröffentlichung verletzt. Dass der Provider zumindest einen bedingten Vorsatz hatte, weil dieser damit hätte rechnen müssen, dass es auch zu einem Verstoß nach dem DSG 2000 kommen kann, wenn Google die Daten nicht auf die Rechtmäßigkeit kontrolliert, kann nicht angenommen werden, da nach dem TKG 2003 eine solche Kontrolle nicht zulässig ist. Eine Vorabkontrolle würde nach § 93 TKG 2003 einen Verstoß gegen das Kommunikationsgeheimnis nach sich ziehen.

Weiters hat Google den erweiterten Vorsatz, nämlich jenen der unrechtmäßigen Bereicherung, ebenfalls nicht erfüllt, auch wenn auf der Website Werbeinserate geschalten waren und Google somit indirekt an der Veröffentlichung des Videos verdient hat. Das Schalten von Inseraten ist per se nicht rechtswidrig.

Somit ist der Provider nach § 51 DSG 2000 nicht strafbar.

4. Strafbarkeit der Google-Manager nach dem TKG 2003

Das TKG 2003 (Telekommunikationsgesetz 2003) enthält sowohl eine gerichtliche Strafbestimmung als auch einen Verwaltungsstraftatbestand. Letzter kann jedoch in der vorliegenden Arbeit unberücksichtigt bleiben.

a) Verletzung von Rechten der Benützer, § 108

§ 108 TKG 2003lautet:

(1) Eine im § 93 Abs 2 bezeichnete Person, die

1. unbefugt über die Tatsache oder den Inhalt des Telekommunikationsverkehrs bestimmter Personen einem Unberufenen Mitteilung macht oder ihm Gelegenheit gibt, Tatsachen, auf die sich die Pflicht zur Geheimhaltung erstreckt, selbst wahrzunehmen,

2. eine Nachricht fälscht, unrichtig wiedergibt, verändert, unterdrückt, unrichtig vermittelt oder unbefugt dem Empfangsberechtigten vorenthält,

ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu drei Monaten oder mit Geldstrafe bis zu 180 Tagessätzen zu bestrafen.

(2) Der Täter ist nur auf Antrag des Verletzten zu verfolgen.

Das TKG 2003 setzt den EU-Rechtsrahmen für elektronische Kommunikationsnetze und Kommunikationsdienste in österreichisches Recht um.[111] Der Regulierungsrahmen besteht aus der Rahmenrichtlinie,[112] der Genehmigungsrichtlinie,[113] der

[111] *Lehofer*, Telekommunikationsgesetz, ÖJZ 2003/48, 781.

[112] Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und –dienste, ABL 2002 L108 vom 24.4.2002.

[113] Richtlinie 2002/20/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über die Genehmigung elektronischer Kommunikationsnetze und –dienste, ABL 2002 L108 vom 24.4.2002.

Zugangsrichtlinie,[114] der Universaldienstrichtlinie,[115] der Datenschutzrichtlinie für elektronische Kommunikation[116] und der Frequenzentscheidung[117].[118]

Der Gesetzgeber hat den Anwendungsbereich gegenüber dem TKG 1997 massiv erweitert.[119] Vom Anwendungsbereich sind nunmehr grundsätzlich alle elektronischen Kommunikationsnetze und –dienste erfasst.[120] Obwohl das Wort „Internet" im neuen Gesetz nicht vorkommt, regelt der Rechtsakt nunmehr im Unterschied zum TKG 1997 alle dafür maßgebenden Rechtsfragen.[121]

Die Strafbestimmung des § 108 TKG 2003 richtet sich gegen eine im § 93 Abs 2 2003 bezeichnete Person. § 93 TKG 2003 regelt das Kommunikationsgeheimnis.

b) Kommunikationsgeheimnis § 93

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

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

…

[114] Richtlinie 2002/19/ EG des Europäischen Parlaments und des Rates vom 7. März 2002 über den Zugang zu elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung, ABL 2002 L108 vom 24.4.2002.

[115] Richtlinie 2002/22/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und –diensten, ABL 2002 L108 vom 24.4.2002.

[116] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABL L 201 vom 31.7.2002.

[117] Entscheidung 676/2002/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen Rechtsrahmen für die Funkfrequenzpolitik in der Europäischen Gemeinschaft, ABL 2002 L108 vom 24.4.2002.

[118] *Kaufmann/Tritscher*, TKG 2003, MR 2003, 273.

[119] *Kaufmann/Tritscher*, TKG 2003, MR 2003, 273.

[120] *Lehofer*, ÖJZ 2003/48, 781.

[121] *Zanger*, Telekommunikationsgesetz 2003, S III.

Der § 93 TKG 2003 enthält nunmehr eine Legaldefinition des Kommunikationsgeheimnisses nach Art 10a StGG, nicht nur präziser als bisher, sondern auch weiter und umfassender festgemacht. Daraus ergibt sich eine sehr eingeschränkte Möglichkeit der Haftenden, die übermittelten Inhalte auf gesetzwidrige Inhalte zu kontrollieren.[122]

Google ist zwar der Betreiber eines Kommunikationsnetzes, allerdings aus Gründen des Schutzes des Kommunikationsgeheimnisses ist eine Vorabkontrolle der auf den Servern abgespeicherten Daten nur mit einem triftigen Grund zulässig.

Des Weiteren sanktioniert § 108 TKG 2003 die *Verletzung von Rechten der Benützer* und der am Down-Syndrom erkrankte Junge ist kein Benützer des Kommunikationsnetzes von Google, denn dieser steht in keinem Verhältnis zu Google. Einzig und allein die Jugendlichen, die den beeinträchtigten Jungen misshandelt und beschimpft haben, sind Benützer des Kommunikationsnetzes von Google.

Weiters hat Google keinem Unbefugten über den Inhalt des Telekommunikationsverkehrs eine Mitteilung gemacht, da die Jugendlichen ja das Video auf den Google-Servern abgelegt und auch einer Veröffentlichung des Videos in den Nutzungsbedingungen zugestimmt hatten. Zudem handelte es sich bei dem User-Video um keine *„Tatsache, auf die sich die Geheimhaltung erstreckt“,*[123] da es ja von den Jugendlichen gewollt war, dass das Video veröffentlicht wird.

Daher ist eine Strafbarkeit der Google-Manager nach dem TKG 2003 nicht gegeben.

---

[122] *Schmölzer/Mayer-Schönberger*, Telekommunikationsgesetz 1997, ÖJZ 1998,382.

[123] Vgl § 108 Abs 1 Z 1 2. Halbsatz TKG 2003.

5. Strafbarkeit der Google-Manager nach dem MedienG

Auch eine Anwendung des Mediengesetzes (MedienG) ist zu prüfen; vor allem in Hinsicht auf „üble Nachrede“, „Beschimpfung“, „Beleidigung“ und „Verspottung“, da in der Videosequenz der beeinträchtigte Junge und eine italienische Organisation namens „Vivi Down“ namentlich genannt und auch beschimpft und beleidigt wurden.[124]

a) Üble Nachrede, Beschimpfung, Verspottung und Verleumdung

§ 6 Abs 1 MedienG lautet:

(1) Wird in einem Medium der objektive Tatbestand der üblen Nachrede, der Beschimpfung, der Verspottung oder Verleumdung hergestellt, so hat der Betroffene gegen den Medieninhaber Anspruch auf Entschädigung der erlittenen Kränkung. ...

Weiters ist nach § 7 MedienG ebenfalls ein Entschädigungsanspruch gegeben, wenn *„durch das Medium der höchstpersönlichen Lebensbereich eines Menschen in einer Weise erörtert oder dargestellt wird, die geeignet ist, ihn in der Öffentlichkeit bloßzustellen“*.

Wie bereits oben[125] dargestellt, wurde der am Down-Syndrom erkrankte Junge in der Videosequenz beschimpft, misshandelt und mit Gegenständen beworfen, daher wurde der objektive Tatbestand der Beleidigung gem § 115 StGB erfüllt. Ein Anspruch auf Entschädigung der erlittenen Kränkung ist nach § 6 MedienG möglich. Ebenso ist ein Anspruch nach § 7 MedienG gegeben, da auch in den höchstpersönlichen Lebensbereich eingegriffen wurde, weil er aufgrund seiner körperlichen und geistigen Beeinträchtigung verspottet wurde und es sich dabei um einen höchstpersönlichen Lebensbereich handelt und er durch diese Verspottung in der Öffentlichkeit bloßgestellt wurde.

---

[124] Siehe S. 8 ff.

[125] Siehe Sachverhalt S. 8 und Beleidigung § 115 StGB S. 20.

Gem § 8 MedienG kann man den *„Anspruch auf einen Entschädigungsbetrag ... vom Betroffenen im Strafverfahren, an dem der Medieninhaber als Beschuldigter oder nach § 41 Abs 6 beteiligt ist ... geltend machen“.*

Weiters besagt § 28 MedienG, dass *„die strafrechtliche Verantwortlichkeit für Medieninhaltsdelikte sich ... nach den allgemeinen Strafgesetzen bestimmt“*, und nach § 41 Abs 1 gelten *„für Strafverfahren eines Medieninhaltsdelikts ... die Bestimmungen der Strafprozessordnung 1975.“* Daraus folgt, dass es sich bei Delikten nach dem MedienG um **gerichtliches Strafrecht** handelt.

Seit der Mediengesetznovelle 2005 ist das MedienG nun auch auf den Online-Bereich anzuwenden, denn ein Hauptanliegen der Mediengesetznovelle 2005 war es insbesondere, mit den Ordnungsvorschriften im Online-Bereich mit der Situation gleichzuziehen, die für den Offline-Bereich ganz zweifelsfrei bestand.[126]

b) Medien

Homepages, bzw allgemeiner Websites, stellen Medien iSd § 1 Abs 1 Z 1 MedienG dar;[127] und zwar unter der Voraussetzung, dass sich die gegenständliche Internetseite an einen größeren Personenkreis richtet. Medium ist nämlich nicht das „Netz“ an sich, auch nicht eine der technischen Einrichtungen (Computer, Server, und der gleichen), sondern der konkrete über dieses vermittelte Dienst, insb die einzelne Homepage.[128] Nach dem MedienG sind ausdrücklich Websites erfasst. Nach Auffassung des Gesetzgebers ist allein die fortdauernde Abrufbarkeit entscheidend und nicht das Ausmaß sowie der Intervall der Updates, damit Websites den periodischen Medien zuzurechnen sind.[129] Auch der OGH definiert in einer Entscheidung[130] eine Website medienrechtlich als ein „*periodisches elektronisches Medium*“.

---

[126] *Höhne* in: *Berka*, Medien, S. 1.

[127] So auch: *Höhne* in: *Berka*, Medien, S. 2.

[128] *Krammer*, Mediengesetz, GesRZ 2005, 187.

[129] *Krammer*, Mediengesetz; GesRZ 2005, 187.

[130] OGH 24.1.2006, 4 Ob 226705x = MR 2006,148.

Daraus ergibt sich, dass die Website von Google ein Medium iSd § 1 Abs 1 Z 1 MedienG ist, denn es ist wohl unbestritten, dass diese an einen größeren Personenkreis gerichtet ist.

c) Anwendbarkeit MedienG auf ausländische Medien

Als problematisch für eine Anwendbarkeit des MedienG könnte sich erweisen, dass Google keinen Sitz in Österreich hat.[131] Allerdings ist das MedienG nach § 51 auch auf ein ausländisches Medium, das nur einen Sitz im Ausland hat, anwendbar, wenn das Medium im Inland verbreitet wurde, empfangen oder abgerufen werden konnte (Z 1) und der Verletzte bzw Betroffene Österreicher war (Z 2). Weiters muss es sich um Delikte handeln, die in Z 3 genannt wurden, zB Ehrverletzungen.

Der nächstgelegene Sitz von Google ist in München,[132] allerdings ist auf die Website von Google auch von Österreich aus ein Zugriff möglich und diese kann im Inland abgerufen werden und auch wird angenommen, dass es sich bei dem am Down-Syndrom erkrankten Jungen um einen Österreicher handelt. Des Weiteren – wie weiter oben[133] in dieser Arbeit bereits festgestellt – handelt es sich bei den strafbaren Handlungen gegen diesen Jugendlichen unter anderem auch um Delikte gegen die Ehre. Somit ist das MedienG auch auf Google anwendbar.

d) Medieninhaber

Medieninhaber ist, wer sonst im Falle eines elektronischen Mediums dessen inhaltliche Gestaltung besorgt und dessen Ausstrahlung, Abrufbarkeit oder Verbreitung entweder besorgt oder veranlasst.[134] Maßgebliches Moment ist stets die Besorgung der inhaltlichen Gestaltung des jeweiligen Online-Angebots, weshalb – so die erläuternden Bemerkungen verdeutlichend – Access- und Service-Provider als Medieninhaber ausscheiden, solange sie nicht zugleich als Content-Provider fingieren, dh selbst Inhalte

---

131 Standorte von Google Inc http://www.google.at/corporate/address.html (Stand 25.1.2011).

132 Standorte von Google Inc http://www.google.at/corporate/address.html (Stand 25.1.2011).

133 Siehe S. 19.

134 Vgl § 1 Abs 1 Z 8 lit c MedienG.

in Netz stellen.[135] Dies geht auch aus einer Entscheidung des OLG Wien[136] hervor, begründet wird dies damit, dass es dem Access- bzw Service-Provider an der Möglichkeit der inhaltlichen Gestaltung des Mediums als Medieninhaber mangelt.

Daher wird Google für das Video eines Users nicht als Medieninhaber in Betracht kommen, da Google nur Speicherplatz auf seinem Host zu Verfügung stellt, nicht aber für den Inhalt verantwortlich ist und diesen daher im Vorhinein nicht beeinflussen kann.

Zusammenfassend lässt sich somit feststellen, dass die Websites von Google zwar ein Medium iSd § 1 Abs 1 Z 1 MedienG sind, und auch, dass das MedienG auf Google als ausländisches Medium Anwendung findet, allerdings ist Google im Falle eines User-Videos, das lediglich auf seinem Host abgespeichert wurde, kein Medieninhaber iS von Abs 1 Z 8 lit c MedienG.

Daher ist keine Strafbarkeit nach dem MedienG gegeben.

[135] *Krammer*, Mediengesetz, GesRZ 2005, 188.

[136] OLG Wien 14.11.2007, 18 Bs 259/07f = MR 2007, 308.

III. Resümee: Verantwortlichkeit des Providers

Zusammenfassend lässt sich nun festhalten, dass die Manager von Google nicht nach dem österreichischen **StGB** strafbar gemacht werden können, da das Delikt der Körperverletzung nach § 83 nicht verwirklicht wurde.

Da den Managern von Google weder die Fürsorge noch die Obhut für den am Down-Syndrom erkrankten Jungen zukommen, scheidet auch § 92 StGB, Quälen oder Vernachlässigen unmündiger, jüngerer oder wehrloser Personen, für eine mögliche Strafbarkeit des Providers aus.

Weiters haben sich die Manager auch nicht wegen der Delikte gegen die Ehre nach §§ 111 ff StGB strafbar gemacht. Denn für eine Beteiligung durch einen sonstigen Beitrag (§ 12 dritter Fall) ist der Erfolg nicht objektiv zurechenbar, denn das Bereitstellen von Speicherplatz ist per se nicht rechtswidrig.

Für Google als Verband ist keine Verantwortlichkeit nach dem **VbVG** gegeben, denn für die Anwendbarkeit des VbVG ist eine Strafbarkeit des StGB Voraussetzung und diese konnte ja ausgeschlossen werden.

Ebenso ist auch eine Strafbarkeit für Google nach dem **MedienG** nicht gegeben, da Google kein Medieninhaber iSd § 1 Abs 1 Z 8 lit c MedienG ist, denn Google ist nicht für die inhaltliche Gestaltung des User-Videos verantwortlich und weiters ist auch unter anderem der Service-Provider nach einer Entscheidung des OLG Wien (18 Bs 259/07f) kein Medieninhaber iSd MedienG.

Das **TKG 2003** ist zwar auch auf den Online-Bereich anzuwenden, allerdings ergibt sich aus der Strafbestimmung des § 108 TKG 2003 keine Verantwortlichkeit für Google für den dieser Arbeit zu Grunde liegenden Fall, da dieser Paragraph die Verletzung von Rechten der Benützer des Telekommunikationsverkehrs sanktioniert und der beeinträchtigte Jugendliche nicht Benützer des Kommunikationsnetzes von Google war. Eine Vorabkontrolle seitens Google der auf den Servern gespeicherten Daten wäre auch aufgrund des Kommunikationsgeheimnisses des § 93 TKG 2003 nicht zulässig gewesen, daher liegt auch kein Verstoß gegen das TKG 2003 vor und Google ist daher nach dem TKG 2003 nicht strafbar.

Des Weiteren ist Google nach **§ 51 DSG 2000** nicht strafbar. Diese Bestimmung ist das Gegenstück zum Art 167 des italienischen Datenschutzrechts. Eine Verantwortlichkeit des Providers ist deshalb nicht gegeben, da Google zwar sensible personenbezogene Daten veröffentlicht hat, jedoch mangelt es am Bereicherungsvorsatz, da die Bereicherung an sich nicht unrechtmäßig war, denn das Schalten von Werbeinseraten ist per se nicht rechtswidrig.

Bei der Veröffentlichung kann man dem Provider auch keinen bedingten Vorsatz unterstellen, denn dadurch, dass dieser die auf seinem Host gespeicherten Daten keiner Kontrolle auf Rechtmäßigkeit unterzieht – wie auch aus den Nutzungsbedingungen von Google hervorgeht – muss Google zwar damit rechnen, dass auch rechtswidrige Daten auf den Speichermedien abgelegt werden, die dann auf „Google Video" veröffentlicht werden, was wiederum Google billigend durch diese unterbliebene Kontrolle in Kauf nimmt, allerdings darf der Provider nicht einfach so die User-Daten überprüfen. Eine Kontrolle würde einen Verstoß nach dem TKG 2003 nach sich ziehen. Denn § 93 TKG 2003 besagt, dass zum Schutz des Kommunikationsgeheimnisses eine Kontrolle nur mit einem triftigen Grunde – oder der Einwilligung der Benützer – zulässig ist. Beides ist nicht der Fall.

Zudem wurde der Provider durch das Video auch nicht unrechtmäßig bereichert. Tatsache ist, dass es durch die Schaltung von Werbeinseraten auf den Websites von Google zu einem Zuwachs des Vermögens von Google gekommen ist, denn der Provider hat mit jedem Klick Geld verdient. Unrechtmäßig deshalb nicht, da zwar keine Zulässigkeit der Datenverwendung gegeben war, allerdings ist das Schalten von Werbeinseraten per se nicht rechtswidrig. Die Daten wurden ja von den Jugendlichen und nicht von Google gesammelt.

Daher ist der Provider auch nach dem österreichischen Datenschutzrecht wegen eines User-Videos nicht strafbar.

Bei der Variante des § 51 DSG 2000 *„Schädigung im Grundrecht auf Datenschutz"* nach § 1 Abs 1 DSG 2000 fordert das Gesetz Absicht, die aber dem Provider nicht unterstellt werden kann, denn Google hat es zwar billigend in Kauf genommen, dass auch rechtswidrigen Daten auf der Website veröffentlicht werden, aber man kann

Google nicht unterstellen, dass es dem Provider darauf ankam, den beeinträchtigten Jungen durch die Veröffentlichung in seinem Grundrecht auf Datenschutz zu schädigen.

Das E-Commerce-Gesetz (**ECG**), das die E-Commerce-Richtlinie (2000/31/EG)[137] der EU in innerstaatliches Recht umgesetzt, findet bei dieser Arbeit keine Berücksichtigung, da ein Provider nach diesem Gesetz lediglich wegen einer Verwaltungsübertretung zur Verantwortung gezogen werden kann. Das Verwaltungsstrafrecht ist nicht Thema dieser Arbeit, daher kann hier auf eine weitere Prüfung einer ev Verantwortlichkeit des Providers verzichtet werden.

Die **Cybercrime Konvention** des Europarates[138] ist auf den dieser Arbeit zu Grunde liegenden Fall nicht anwendbar, da diese in vier Titel gegliedert ist und keiner der vier greifen würde, denn der erste Titel befasst sich mit „Straftaten gegen die Vertraulichkeit und Verfügbarkeit von Daten“, also zB Hacking, der zweite Titel regelt computerbezogene Straftaten, wie Datenfälschen oder Betrug usw, im dritten Titel werden die inhaltsbezogenen Straftaten geregelt, derzeit nur Kinderpornographie, und der vierte regelt Urheberrechtsverletzungen.

Weiters sind aber auch noch Ansprüche nach dem **Urheberrecht** denkbar. Allerdings sind Ansprüche nach dem Urhebergesetz auf dem Zivilrechtsweg geltend zu machen und in dieser Arbeit soll der strafrechtliche Aspekt der Verantwortlichkeit dargestellt werden. Zu diesem Thema nur so viel: § 78 UrhG-Nov 1996 (Urheberrechtsgesetz-Novelle 1996) normiert das Recht am eigenen Bild. § 78 schützt zwar gegen Persönlichkeitsinteressen verletzende Veröffentlichungen von Bildnissen, aber nach herrschender Meinung nicht gegen die unbefugte Bildaufnahme an sich.[139] Dabei genügt es, dass die Person des Abgebildeten erkennbar ist. Die Veröffentlichung von Bildern mit Personen ohne Zustimmung der Abgebildeten ist aber nicht gänzlich untersagt, sondern hängt davon ab, ob dadurch "berechtigte Interessen" des Abgebildeten tangiert werden, dabei kommt es auch auf den Zusammenhang der

[137] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8 Juni 2000 über bestimmte rechtliche Aspekte der Dienst der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“), ABL. L 178/1 vom 17.7.2000.

[138] Cybercrime Konvention des Europarates http://conventions.coe.int/Treaty/en/Treaties/html/185.htm.

[139] *Thiele*, Bildaufnahme, RZ 2007,4.

Veröffentlichung an. Die Veröffentlichung ist etwa dann zulässig, wenn die Abbildung nicht in einem negativen Konnex erfolgt und auch nicht mit kommerziellen Absichten.[140] § 78 Abs 3 UrhG-Nov 1996 dient dazu, dass die Aufklärung und Verfolgbarkeit von Online-Eingriffen in Urheberrechte durch Einräumung eines Auskunftsanspruches an den in seinen Urheberrechten Verletzten über die Identität des Verletzers gegenüber dem Vermittler (Provider) ermöglicht wird. Allerdings, in einem Urteil des OGH vom 14.07.09 (4 Ob 41/09x) hat der OGH keine rechtmäßige Möglichkeit zur Beauskunftung des Inhabers einer dynamischen IP-Adresse, unter der urheberrechtlich geschützte Inhalte rechtswidrig öffentlich zur Verfügung gestellt wurden.[141]

[140] *Schmidbauer*, Internet4jurists.at http://www.internet4jurists.at/urh-marken/immaterial.htm (Stand 31.01.2011).

[141] *Daum*, Providerauskunft, MR 2009, 247.

Abschließende Überlegungen

Das internationale Strafrecht gewinnt wegen der komplexen Struktur des Internets immer mehr an Bedeutung. Nationalstaatliche Grenzen verlieren aufgrund der globalen Vernetzung an Gewicht. Bei dem vorliegenden Fall hat sich die Anknüpfung an materielles österreichisches Strafrecht als nicht sehr problematisch erwiesen, da angenommen wurde, dass der am Down-Syndrom erkrankte Jugendliche die österreichische Staatsbürgerschaft besitzt und der Tatort bei allen Delikten im Inland gelegen war. Bei anderen Delikten als jenen, die dieser Arbeit zu Grunde liegen, scheint allerdings für die Internetkriminalität eine Begrenzung des räumlichen Geltungsbereichs notwendig, da der Erfolg aller im Wege des Internets begangenen Handlungen auf der ganzen Welt eintritt.[142]

Hier ist der Gesetzgeber gefordert, denn die derzeitige Rechtslage erleichtert die Beantwortung der Frage nach einer Verantwortlichkeit des Providers keineswegs. So liegt das Risiko einer Fehleinschätzung ausschließlich bei dem Host-Provider, wenn es um die Frage geht, ob es sich um rechtswidrige Inhalte handelt, die sich auf dem Server befinden. Denn der Host-Provider hat zwei Möglichkeiten, wenn der Verdacht auf solche Inhalte besteht: Er kann tätig werden und die Information sperren und sich daher der Gefahr einer eventuellen Haftung aus Vertragsverletzung aussetzen, wenn er zu Unrecht sperrt. Bleibt der Provider allerdings untätig, so drohen ihm uU strafrechtliche oder zivilrechtliche Konsequenzen.[143] Allerdings wurde die Haftung für Host-Provider für fremdes Fehlverhalten durch den OGH deutlich eingeschränkt. Denn der Host-Provider muss nur dann tätig werden, wenn die beanstandeten Inhalte als Rechtsverletzungen zu qualifizieren und diese auch für einen juristischen Laien ohne weitere Nachforschungen offenkundig sind.[144] Damit wird verhindert, dass der Host quasi als Richter tätig werden muss, wenn fremde Inhalte verwaltet werden.[145] Weiters darf der Provider auch auf Grund des Kommunikationsgeheimnisses, das im TKG 2003

---

[142] *Höpfel/Kathrein*, WK [2] § 67 Rz 13.

[143] *Hasberger/Semrau-Deutsch*, Host-Provider, ecolex 2005, 197.

[144] OGH 6.7.2004, 4 Ob 66/04s = ecolex 2004, 799.

[145] *Hasberger/Semrau-Deutsch*, Host-Provider, ecolex 2005, 199.

verankert ist, die User-Daten nicht ohne triftigen Grund kontrollieren, was aber eindeutig im Widerspruch zu der Strafbarkeit nach dem DSG 2000 steht, denn durch die unterbliebene Vorabkontrolle könnte man dem Provider einen bedingten Vorsatz unterstellen, sodass dieser nach dem DSG 2000 für den dieser Arbeit zu Grunde liegenden Fall zur Verantwortung gezogen werden könnte. Allerdings erscheint es mir nahezu unmöglich, dass der Provider alle Daten, die tagtäglich auf seinen Speichermedien abgelegt werden, einer eingehenden Kontrolle auf Rechtmäßigkeit unterziehen kann, man bedenke nur, wie viele User ein derart großer Provider, wie Google es ist, hat. Meines Erachtens ist es daher weder möglich noch für den Provider zumutbar, dass dieser zu einer umfassenden Kontrolle verpflichtet wird, zum einen aufgrund der enormen Datenmenge und zum anderen: Kann auch ein juristischer Laie die Rechtmäßigkeit aller Inhalte zweifelsfrei erkennen? Weiters ist auch ist eine allgemeine Überwachungspflicht nach der EC-RL nicht gewünscht und nach dem TKG 2003 uU sogar ein Verstoß gegen das Kommunikationsgeheimnis.

Auch wird es immer notwendiger, dass die Staatengemeinschaft im Hinblick auf die Internetkriminalität in enger Zusammenarbeit miteinander steht. Dies erscheint allerdings wiederum schwierig, denn nicht in jedem Staat gibt es die selben Wertvorstellungen, sodass zB die Verbreitung von nationalsozialistischem Gedankengut über das Internet in Österreich strafbar ist, wohingegen in den USA dies nicht der Fall ist, dort wird diese Verbreitung von der Meinungsäußerungsfreiheit geschützt.

Entweder wird man zu mehr Toleranz gezwungen, weil man Dinge einfach nicht so verfolgen kann, wie man es nach der eigenen Rechtsordnung gerne haben möchte. Denn man ist gezwungen, das Urteil anderer Rechtsordnungen hinzunehmen. Oder man wird sich letztlich weltweit einigen müssen, welche Dinge man verbietet und welche man erlaubt.[146]

Vor allem die Entwicklung von Gesetzen, die es ermöglichen, den Provider besser in die Pflicht zu nehmen, wäre meines Erachtens notwendig, denn wie aus dem in dieser Arbeit vorgelegten Fall ersichtlich ist, reicht die derzeitige Gesetzeslage in Österreich nicht aus. Allerdings ist es meiner Meinung nach auch nicht zielführend, wenn dem Internetdienstanbieter jegliche Verfehlungen seiner User zugerechnet werden können.

---

[146] *Lagodny* in: *Gruber* (Hrsg), Dimensionen, S. 61.

Zusätzlich ist auch zu beachten, solange die Provider, wie im oben dargelegten Fall, Geld an der Veröffentlichung von User-Videos verdienen (durch die Schaltung von Werbeinseraten) und auch umso mehr Geld bekommen, je beliebter das Video bei den anderen Nutzern ist, desto geringer wird das Interesse der jeweiligen Internetdienstanbieter sein, mit den Strafverfolgungsbehörden zusammenzuarbeiten und sich somit die Gelder für die Werbeschaltungen entgehen zu lassen.

Es wird sich zeigen, wie die Gesetzgeber auf die neuen Möglichkeiten, die durch das Internet geschaffen werden, in Zukunft reagieren.

Anhang

(ausgewählte Gesetzesstellen)

Verbandsverantwortlichkeitsgesetz (VbVG)

Artikel 1, 1. Abschnitt

Anwendungsbereich und Begriffsbestimmungen

Verbände

§ 1. (1) Dieses Bundesgesetz regelt, unter welchen Voraussetzungen Verbände für Straftaten verantwortlich sind und wie sie sanktioniert werden, sowie das Verfahren, nach dem die Verantwortlichkeit festgestellt und Sanktionen auferlegt werden. Straftat im Sinne dieses Gesetzes ist eine nach einem Bundes- oder Landesgesetz mit gerichtlicher Strafe bedrohte Handlung; auf Finanzvergehen ist dieses Bundesgesetz jedoch nur insoweit anzuwenden, als dies im Finanzstrafgesetz, BGBl. Nr. 129/1958, vorgesehen ist.

(2) Verbände im Sinne dieses Gesetzes sind juristische Personen sowie eingetragene Personengesellschaften und Europäische wirtschaftliche Interessenvereinigungen.

(3) Keine Verbände im Sinne dieses Gesetzes sind

1. die Verlassenschaft;
2. Bund, Länder, Gemeinden und andere juristische Personen, soweit sie in Vollziehung der Gesetze handeln;
3. anerkannte Kirchen, Religionsgesellschaften und religiöse Bekenntnisgemeinschaften, soweit sie seelsorgerisch tätig sind.

2. Abschnitt,

Verbandsverantwortlichkeit – Materiellrechtliche Bestimmungen

Verantwortlichkeit

§ 3. (1) Ein Verband ist unter den weiteren Voraussetzungen des Abs. 2 oder des Abs. 3 für eine Straftat verantwortlich, wenn

1. die Tat zu seinen Gunsten begangen worden ist oder
2. durch die Tat Pflichten verletzt worden sind, die den Verband treffen.

(2) Für Straftaten eines Entscheidungsträgers ist der Verband verantwortlich, wenn der Entscheidungsträger als solcher die Tat rechtswidrig und schuldhaft begangen hat.

(3) Für Straftaten von Mitarbeitern ist der Verband verantwortlich, wenn

1. Mitarbeiter den Sachverhalt, der dem gesetzlichen Tatbild entspricht, rechtswidrig verwirklicht haben; der Verband ist für eine Straftat, die vorsätzliches Handeln voraussetzt, nur verantwortlich, wenn ein Mitarbeiter vorsätzlich gehandelt hat; für eine Straftat, die fahrlässiges Handeln voraussetzt, nur, wenn Mitarbeiter die nach den Umständen gebotene Sorgfalt außer acht gelassen haben; und
2. die Begehung der Tat dadurch ermöglicht oder wesentlich erleichtert wurde, dass Entscheidungsträger die nach den Umständen gebotene und zumutbare Sorgfalt außer acht gelassen haben, insbesondere indem sie wesentliche technische, organisatorische oder personelle Maßnahmen zur Verhinderung solcher Taten unterlassen haben

(4) Die Verantwortlichkeit eines Verbandes für eine Tat und die Strafbarkeit von Entscheidungsträgern oder Mitarbeitern wegen derselben Tat schließen einander nicht aus.

Datenschutzgesetz 2000 (DSG 2000)

Artikel 1

(Verfassungsbestimmung)

Grundrecht auf Datenschutz

§ 1. (1) Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.

(2) Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBl. Nr. 210/1958, genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.

(3) Jedermann hat, soweit ihn betreffende personenbezogene Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, dh ohne Automationsunterstützung geführten Dateien bestimmt sind, nach Maßgabe gesetzlicher Bestimmungen

1. das Recht auf Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden;
2. das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten.

(4) Beschränkungen der Rechte nach Abs. 3 sind nur unter den in Abs. 2 genannten Voraussetzungen zulässig.

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

Artikel 2

1. Abschnitt

Allgemeines, Definitionen

§ 4. Im Sinne der folgenden Bestimmungen dieses Bundesgesetzes bedeuten die Begriffe:

1. „Daten“ („personenbezogene Daten“): Angaben über Betroffene (Z 3), deren Identität bestimmt oder bestimmbar ist; „nur indirekt personenbezogen“ sind Daten für einen Auftraggeber (Z 4), Dienstleister (Z 5) oder Empfänger einer Übermittlung (Z 12) dann, wenn der Personenbezug der Daten derart ist, daß dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann;
2. „sensible Daten“ („besonders schutzwürdige Daten“): Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben;
3. „Betroffener“: jede vom Auftraggeber (Z 4) verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet (Z 8) werden;

4. Auftraggeber: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten zu verwenden (Z 8), unabhängig davon, ob sie die Daten selbst verwenden (Z 8) oder damit einen Dienstleister (Z 5) beauftragen. Sie gelten auch dann als Auftraggeber, wenn der mit der Herstellung eines Werkes beauftragte Dienstleister (Z 5) die Entscheidung trifft, zu diesem Zweck Daten zu verwenden (Z 8), es sei denn dies wurde ihm ausdrücklich untersagt oder der Beauftragte hat auf Grund von Rechtsvorschriften oder Verhaltensregeln über die Verwendung eigenverantwortlich zu entscheiden;
5. Dienstleister: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie Daten nur zur Herstellung eines ihnen aufgetragenen Werkes verwenden (Z 8);
6. „Datei“: strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind;
7. „Datenanwendung“: die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte (Z 8), die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen (automationsunterstützte Datenanwendung);
8. Verwenden von Daten: jede Art der Handhabung von Daten, also sowohl das Verarbeiten (Z 9) als auch das Übermitteln (Z 12) von Daten;
9. Verarbeiten von Daten: das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen (Z 11), Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten mit Ausnahme des Übermittelns (Z 12) von Daten;
10. (Anm.: aufgehoben durch BGBl. I Nr. 133/2009)
11. Überlassen von Daten: die Weitergabe von Daten zwischen Auftraggeber und Dienstleister im Rahmen des Auftragsverhältnisses (Z 5);
12. Übermitteln von Daten: die Weitergabe von Daten an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das Veröffentlichen von Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers;
13. „Informationsverbundsystem“: die gemeinsame Verarbeitung von Daten in einer Datenanwendung durch mehrere Auftraggeber und die gemeinsame Benützung der Daten in der Art, daß jeder Auftraggeber auch auf jene Daten im System Zugriff hat, die von den anderen Auftraggebern dem System zur Verfügung gestellt wurden;
14. „Zustimmung“: 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;
15. „Niederlassung“: jede durch feste Einrichtungen an einem bestimmten Ort räumlich und funktional abgegrenzte Organisationseinheit mit oder ohne Rechtspersönlichkeit, die am Ort ihrer Einrichtung auch tatsächlich Tätigkeiten ausübt.

2. Abschnitt, Verwendung von Daten, Grundsätze

§ 6. (1) Daten dürfen nur

1. nach Treu und Glauben und auf rechtmäßige Weise verwendet werden;
2. für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden; die Weiterverwendung für wissenschaftliche oder statistische Zwecke ist nach Maßgabe der §§ 46 und 47 zulässig;
3. soweit sie für den Zweck der Datenanwendung wesentlich sind, verwendet werden und über diesen Zweck nicht hinausgehen;
4. so verwendet werden, daß sie im Hinblick auf den Verwendungszweck im Ergebnis sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind;
5. solange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist; eine längere Aufbewahrungsdauer kann sich aus besonderen gesetzlichen, insbesondere archivrechtlichen Vorschriften ergeben.

(2) Der Auftraggeber trägt bei jeder seiner Datenanwendungen die Verantwortung für die Einhaltung der in Abs. 1 genannten Grundsätze; dies gilt auch dann, wenn er für die Datenanwendung Dienstleister heranzieht.

(3) Der Auftraggeber einer diesem Bundesgesetz unterliegenden Datenanwendung hat, wenn er nicht im Gebiet der Europäischen Union niedergelassen ist, einen in Österreich ansässigen Vertreter zu benennen, der unbeschadet der Möglichkeit eines Vorgehens gegen den Auftraggeber selbst namens des Auftraggebers verantwortlich gemacht werden kann.

(4) Zur näheren Festlegung dessen, was in einzelnen Bereichen als Verwendung von Daten nach Treu und Glauben anzusehen ist, können für den privaten Bereich die gesetzlichen Interessenvertretungen, sonstige Berufsverbände und vergleichbare Einrichtungen Verhaltensregeln ausarbeiten. Solche Verhaltensregeln dürfen nur veröffentlicht werden, nachdem sie dem Bundeskanzler zur Begutachtung vorgelegt wurden und dieser ihre Übereinstimmung mit den Bestimmungen dieses Bundesgesetzes begutachtet und als gegeben erachtet hat.

Zulässigkeit der Verwendung von Daten

§ 7. (1) Daten dürfen nur verarbeitet werden, soweit Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sind und die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzen.

(2) Daten dürfen nur übermittelt werden, wenn

1. sie aus einer gemäß Abs. 1 zulässigen Datenanwendung stammen und
2. der Empfänger dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis - soweit diese nicht außer Zweifel steht - im Hinblick auf den Übermittlungszweck glaubhaft gemacht hat und
3. durch Zweck und Inhalt der Übermittlung die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt werden.

Die Zulässigkeit einer Datenverwendung setzt voraus, daß die dadurch verursachten Eingriffe in das Grundrecht auf Datenschutz nur im erforderlichen Ausmaß und mit den gelindesten zur Verfügung stehenden Mitteln erfolgen und daß die Grundsätze des § 6 eingehalten werden.

Schutzwürdige Geheimhaltungsinteressen bei Verwendung sensibler Daten

§ 9. Schutzwürdige Geheimhaltungsinteressen werden bei der Verwendung sensibler Daten ausschließlich dann nicht verletzt, wenn

1. der Betroffene die Daten offenkundig selbst öffentlich gemacht hat oder
2. die Daten in nur indirekt personenbezogener Form verwendet werden oder
3. sich die Ermächtigung oder Verpflichtung zur Verwendung aus gesetzlichen Vorschriften ergibt, soweit diese der Wahrung eines wichtigen öffentlichen Interesses dienen, oder
4. die Verwendung durch Auftraggeber des öffentlichen Bereichs in Erfüllung ihrer Verpflichtung zur Amtshilfe geschieht oder
5. Daten verwendet werden, die ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand haben, oder
6. der Betroffene seine Zustimmung zur Verwendung der Daten ausdrücklich erteilt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt, oder
7. die Verarbeitung oder Übermittlung zur Wahrung lebenswichtiger Interessen des Betroffenen notwendig ist und seine Zustimmung nicht rechtzeitig eingeholt werden kann oder
8. die Verwendung der Daten zur Wahrung lebenswichtiger Interessen eines anderen notwendig ist oder
9. die Verwendung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder

10. Daten für private Zwecke gemäß § 45 oder für wissenschaftliche Forschung oder Statistik gemäß § 46, zur Benachrichtigung oder Befragung des Betroffenen gemäß § 47 oder im Katastrophenfall gemäß § 48a verwendet werden oder
11. die Verwendung erforderlich ist, um den Rechten und Pflichten des Auftraggebers auf dem Gebiet des Arbeits- oder Dienstrechts Rechnung zu tragen, und sie nach besonderen Rechtsvorschriften zulässig ist, wobei die dem Betriebsrat nach dem Arbeitsverfassungsgesetz zustehenden Befugnisse im Hinblick auf die Datenverwendung unberührt bleiben, oder
12. die Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder -behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist, und die Verwendung dieser Daten durch ärztliches Personal oder sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder
13. nicht auf Gewinn gerichtete Vereinigungen mit politischem, philosophischem, religiösem oder gewerkschaftlichem Tätigkeitszweck Daten, die Rückschlüsse auf die politische Meinung oder weltanschauliche Überzeugung natürlicher Personen zulassen, im Rahmen ihrer erlaubten Tätigkeit verarbeiten und es sich hiebei um Daten von Mitgliedern, Förderern oder sonstigen Personen handelt, die regelmäßig ihr Interesse für den Tätigkeitszweck der Vereinigung bekundet haben; diese Daten dürfen, sofern sich aus gesetzlichen Vorschriften nichts anderes ergibt, nur mit Zustimmung der Betroffenen an Dritte weitergegeben werden.

10. Abschnitt

Strafbestimmungen

Datenverwendung in Gewinn- oder Schädigungsabsicht

§ 51. Wer mit dem Vorsatz, sich oder einen Dritten dadurch unrechtmäßig zu bereichern, oder mit der Absicht, einen anderen dadurch in seinem von § 1 Abs. 1 gewährleisteten Anspruch zu schädigen, personenbezogene Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat, selbst benützt, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat, ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.

Telekommunikationsgesetz 2003 (TKG 2003)

Kommunikationsgeheimnis

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

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

…

13. Abschnitt

Strafbestimmungen

Verletzung von Rechten der Benützer

§ 108 (1) Eine im § 93 Abs 2 bezeichnete Person, die

1. unbefugt über die Tatsache oder den Inhalt des Telekommunikationsverkehrs bestimmter Personen einem Unberufenen Mitteilung macht oder ihm Gelegenheit gibt, Tatsachen, auf die sich die Pflicht zur Geheimhaltung erstreckt, selbst wahrzunehmen,
2. eine Nachricht fälscht, unrichtig wiedergibt, verändert, unterdrückt, unrichtig vermittelt oder unbefugt dem Empfangsberechtigten vorenthält,

ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu drei Monaten oder mit Geldstrafe bis zu 180 Tagessätzen zu bestrafen.

(2) Der Täter ist nur auf Antrag des Verletzten zu verfolgen.

Mediengesetz (MedienG)

Erster Abschnitt

Begriffsbestimmungen

§ 1. (1) Im Sinn der Bestimmungen dieses Bundesgesetzes ist

1. "Medium": jedes Mittel zur Verbreitung von Mitteilungen oder Darbietungen mit gedanklichem Inhalt in Wort, Schrift, Ton oder Bild an einen größeren Personenkreis im Wege der Massenherstellung oder der Massenverbreitung;

1a. "Medieninhalte": Mitteilungen oder Darbietungen mit gedanklichem Inhalt in Wort, Schrift, Ton oder Bild, die in einem Medium enthalten sind;

2. "periodisches Medium": ein periodisches Medienwerk oder ein periodisches elektronisches Medium;

3. Massenherstellungsverfahren in Medienstücken vervielfältigter Träger von Mitteilungen oder Darbietungen mit gedanklichem Inhalt;

4. "Druckwerk": ein Medienwerk, durch das Mitteilungen oder Darbietungen ausschließlich in Schrift oder in Standbildern verbreitet werden;

5. "periodisches Medienwerk oder Druckwerk": ein Medienwerk oder Druckwerk, das unter demselben Namen in fortlaufenden Nummern wenigstens viermal im Kalenderjahr in gleichen oder ungleichen Abständen erscheint und dessen einzelne Nummern, mag auch jede ein in sich abgeschlossenes Ganzes bilden, durch ihren Inhalt im Zusammenhang stehen;

5a. "periodisches elektronisches Medium": ein Medium, das auf elektronischem Wege

   a) ausgestrahlt wird (Rundfunkprogramm) oder

   b) abrufbar ist (Website) oder

   c) wenigstens vier Mal im Kalenderjahr in vergleichbarer Gestaltung verbreitet wird (wiederkehrendes elektronisches Medium);

6. "Medienunternehmen": ein Unternehmen, in dem die inhaltliche Gestaltung des Mediums besorgt wird sowie

   a) seine Herstellung und Verbreitung oder

   b) seine Ausstrahlung oder Abrufbarkeit

   entweder besorgt oder veranlasst werden;

7. "Mediendienst": ein Unternehmen, das Medienunternehmen wiederkehrend mit Beiträgen in Wort, Schrift, Ton oder Bild versorgt;

8. "Medieninhaber": wer

   a) ein Medienunternehmen oder einen Mediendienst betreibt oder

   b) sonst die inhaltliche Gestaltung eines Medienwerks besorgt und dessen Herstellung und Verbreitung entweder besorgt oder veranlasst oder

   c) sonst im Fall eines elektronischen Mediums dessen inhaltliche Gestaltung besorgt und dessen Ausstrahlung, Abrufbarkeit oder Verbreitung entweder besorgt oder veranlasst oder

   d) sonst die inhaltliche Gestaltung eines Mediums zum Zweck der nachfolgenden Ausstrahlung, Abrufbarkeit oder Verbreitung besorgt;

9. "Herausgeber": wer die grundlegende Richtung des periodischen Mediums bestimmt;

10. "Hersteller": wer die Massenherstellung von Medienwerken besorgt;

11. "Medienmitarbeiter": wer in einem Medienunternehmen oder Mediendienst an der inhaltlichen Gestaltung eines Mediums oder der Mitteilungen des Mediendienstes journalistisch mitwirkt, sofern er als Angestellter des Medienunternehmens oder Mediendienstes oder als freier Mitarbeiter diese journalistische Tätigkeit ständig und nicht bloß als wirtschaftlich unbedeutende Nebenbeschäftigung ausübt;

12. "Medieninhaltsdelikt": eine durch den Inhalt eines Mediums begangene, mit gerichtlicher Strafe bedrohte Handlung, die in einer an einen größeren Personenkreis gerichteten Mitteilung oder Darbietung besteht.

(2) Zu den Medienwerken gehören auch die in Medienstücken vervielfältigten Mitteilungen der Mediendienste. Im übrigen gelten die Mitteilungen der Mediendienste ohne Rücksicht auf die technische Form, in der sie geliefert werden, als Medien.

Üble Nachrede, Beschimpfung, Verspottung und Verleumdung

§ 6. (1) Wird in einem Medium der objektive Tatbestand der üblen Nachrede, der Beschimpfung, der Verspottung oder der Verleumdung hergestellt, so hat der Betroffene gegen den Medieninhaber Anspruch auf eine Entschädigung für die erlittene Kränkung. Die Höhe des Entschädigungsbetrages ist nach Maßgabe des Umfangs und der Auswirkungen der Veröffentlichung, insbesondere auch der Art und des Ausmaßes der Verbreitung des Mediums, zu bestimmen; auf die Wahrung der wirtschaftlichen Existenz des Medieninhabers ist Bedacht zu nehmen. Der Entschädigungsbetrag darf 20 000 Euro, bei einer Verleumdung oder bei besonders schwerwiegenden Auswirkungen einer üblen Nachrede 50 000 Euro nicht übersteigen.

…

Verletzung des höchstpersönlichen Lebensbereiches

§ 7. (1) Wird in einem Medium der höchstpersönliche Lebensbereich eines Menschen in einer Weise erörtert oder dargestellt, die geeignet ist, ihn in der Öffentlichkeit bloßzustellen, so hat der Betroffene gegen den Medieninhaber Anspruch auf eine Entschädigung für die erlittene Kränkung. Der Entschädigungsbetrag darf 20 000 Euro nicht übersteigen; im übrigen ist § 6 Abs. 1 zweiter Satz anzuwenden.

…

Gemeinsame Bestimmungen

§ 8. (1) Den Anspruch auf einen Entschädigungsbetrag nach den §§ 6, 7, 7a, 7b oder 7c kann der Betroffene in dem Strafverfahren, an dem der Medieninhaber als Beschuldigter oder nach dem § 41 Abs. 6 beteiligt ist, bis zum Schluß der Hauptverhandlung oder Verhandlung geltend machen. Kommt es nicht zu einem solchen Strafverfahren, so kann der Anspruch mit einem selbständigen Antrag geltend gemacht werden.

…

Ergänzende Verfahrensbestimmungen

§ 41. (1) Für Strafverfahren wegen eines Medieninhaltsdeliktes und für selbstständige Verfahren (§§ 8a, 33 Abs. 2, 34 Abs. 3) gelten, soweit in diesem Bundesgesetz nichts Anderes bestimmt ist, die Bestimmungen der Strafprozessordnung 1975.

…

(6) In den im Abs. 1 bezeichneten Verfahren ist der Medieninhaber zur Hauptverhandlung zu laden. Er hat die Rechte des Angeklagten; insbesondere steht ihm das Recht zu, alle Verteidigungsmittel wie der Angeklagte vorzubringen und das Urteil in der Hauptsache anzufechten. Doch werden das Verfahren und die Urteilsfällung durch sein Nichterscheinen nicht gehemmt; auch kann er gegen ein in seiner Abwesenheit gefälltes Urteil keinen Einspruch erheben.

…

Neunter Abschnitt

Geltungsbereich

§ 50. Die §§ 1, 23, 28 bis 42, 43 Abs. 4, 47 Abs. 1 und 2, 48, 49, im Falle der Z 3 dieser Bestimmung auch § 43b Abs. 1, 2 und 7 sowie im Falle der Z 4 dieser Bestimmung auch § 25 Abs. 5, nicht aber die anderen Bestimmungen dieses Bundesgesetzes, sind auch anzuwenden auf

1. die Medien ausländischer Medienunternehmen, es sei denn, dass das Medium zur Gänze oder nahezu ausschließlich im Inland verbreitet wird;
2. von einem fremden Staat herausgegebene oder verlegte Medienwerke und Medienwerke, die von einer in Österreich akkreditierten oder mitakkreditierten Mission, einer in Österreich errichteten konsularischen Vertretung oder einer über- oder zwischenstaatlichen Einrichtung, der Österreich angehört oder mit der es offizielle Beziehungen unterhält, herausgegeben oder verlegt werden; Gleiches gilt für von den genannten Stellen oder Einrichtungen verbreitete wiederkehrende elektronische Medien sowie für Websites dieser Stellen oder Einrichtungen;
3. Medienwerke oder wiederkehrende elektronische Medien oder Websites, die vom Nationalrat, Bundesrat, von der Bundesversammlung oder einem Landtag oder die von einer Behörde in Erfüllung von Aufgaben der Hoheitsverwaltung oder der Gerichtsbarkeit herausgegeben oder verlegt werden, im Fall wiederkehrender elektronischer Medien oder Websites verbreitet oder abrufbar gehalten werden und als amtlich erkennbar sind, sowie als amtlich erkennbare Teile von Medienwerken, sofern die angeführten Voraussetzungen nur auf diese zutreffen;
4. Schülerzeitungen sowie Medien, die im Verkehr, im häuslichen, geselligen, kulturellen, wissenschaftlichen oder religiösen Leben, im Vereinsleben, im Wirtschaftsleben im Rahmen der Tätigkeit eines Amtes oder einer Interessenvertretung oder bei einer anderen vergleichbaren Betätigung als Hilfsmittel dienen.

§ 51. Auf Mitteilungen oder Darbietungen in einem Medium, dessen Medieninhaber seinen Sitz im Ausland hat (ausländisches Medium), sind über § 50 Z 1 hinaus die §§ 6 bis 21, 23 sowie 28 bis 42 anzuwenden,

1. wenn das Medium im Inland verbreitet worden ist, empfangen oder abgerufen werden konnte,
2. soweit der Verletzte oder Betroffene zur Zeit der Verbreitung Österreicher war oder einen Wohnsitz oder Aufenthalt im Inland hatte oder sonst schwerwiegende österreichische Interessen verletzt worden sind und
3. soweit durch die Mitteilung oder Darbietung eines der folgenden Rechtsgüter verletzt worden ist:
   a. Ehre und wirtschaftlicher Ruf,
   b. Privat- und Geheimsphäre,
   c. sexuelle Integrität und Selbstbestimmung,
   d. Sicherheit des Staates oder
   e. öffentlicher Friede.