Sonderdruck aus:

Recht aktuell
Weiterbildungsveranstaltung der Juristischen Fakultät an der Universität Basel

Tagungsband Recht aktuell 2006
Bern: Edition Weblaw 2006
Herausgeber: Peter Jung

Aktuelle Entwicklungen im Haftungsrecht

DAVID ROSENTHAL

Internet-Provider-Haftung – ein Sonderfall?

www.weblaw.ch
edition

Beitragsübersicht Tagungsband Recht aktuell 2006
Aktuelle Entwicklungen im Haftpflichtrecht

Prof. Dr. Peter Jung

Herausgeber Tagungsband Recht aktuell 2006. Ordinarius für Privatrecht, Universität Basel.

Vorwort des Herausgebers

Prof. Dr. Thomas Kadner Graziano

Ordinarius für Privatrecht an der Universität Genf, Direktor «Certificat de Droit Transnational»

Entwicklungstendenzen im schweizerischen ausservertraglichen Haftungs- und Schadensrecht

PD Dr. iur. Peter Loser

Rechtsanwalt. Mitglied der Direktion der St.Galler Kantonalbank.

Die Vertrauenshaftung in der Praxis

Dr. iur. Hans-Peter Egli

Bezirksrichter, Vorsitzender des Arbeitsgerichts Zürich.

Der besondere Haftungsmassstab von Art. 321e OR

Prof. Dr. Walter Fellmann

Rechtsanwalt und Notar in Luzern; nebenamtlicher Ordinarius an der Universität Luzern.

Haftung für fehlerhafte Rechtsberatung und Prozessführung

Markus Schmid

Advokat, Dietrich Greuter Schmid, Basel.

Aspekte und Thesen der Arzthaftung

Prof. Dr. Lukas Handschin

Titularprofessor für Privatrecht, Universität Basel. Rechtsanwalt Schumacher Baur Hürlimann, Zürich.

Die Verantwortlichkeit der Gesellschaftsorgane – auch für die Richtigkeit der Bilanz?

Prof. Dr. Hanspeter Dietzi

Deputy Group General Counsel UBS AG, Basel/ Zürich; Titularprofessor, Universität Basel.

Haftungsfälle im Zusammenhang mit Bankdienstleistungen

David Rosenthal

Konsulent für Informations- und Telekommunikationsrecht, Homburger Rechtsanwälte, Zürich.

Internet-Provider-Haftung – ein Sonderfall?

Dr. iur. Philippe Spitz

Advokat, LL.M., Basel/Zürich, Lehrbeauftragter an der Universität Basel.

Haftung für Wettbewerbshandlungen

Prof. Dr. Thomas Sutter-Somm

Ordinarius für Zivil- und Zivilprozessrecht, Dekan Jur. Fakultät, Universität Basel.

Der Haftpflichtprozess im Lichte der neuesten Tendenzen der Vereinheitlichung des schweizerischen Zivilprozessrechts

Prof. Dr. Franz Hasenböhler

Rechtskonsulent KPMG Legal; em. Ordinarius für Privatrecht an der Universität Basel.

Haftungsfragen im Lichte der revidierten Versicherungsgesetzgebung

Peter Jung (Hrsg.), Tagungsband Recht aktuell 2006 (Aktuelle Entwicklungen im Haftpflichtrecht):

Internet-Provider-Haftung – ein Sonderfall?

David Rosenthal [dro]

Die Haftung von Access- und Hosting-Providern wirft zahlreiche Fragen auf, die durch unrealistische Vorstellungen über die Rolle und Eingriffsmöglichkeiten solcher Provider zu einer erheblichen Rechtsunsicherheit geführt haben. Für das Strafrecht wird diese nun durch die Schaffung eines Providerstrafrechts möglicherweise geklärt, auch wenn der Vorentwurf noch einiger Korrekturen bedarf. Klärungsbedarf besteht auch im Bereich der zivilrechtlichen Verantwortlichkeit. Zwar wäre schon mit den bestehenden Gesetzen eine sachgerechte Lösung – einschliesslich einer Enthaftung der Access-Provider – möglich, doch gibt die bisherige Diskussion und Rechtsentwicklung wenig Anlass zur Hoffnung. Die Erkenntnis, dass Dienstleistungen von Internet-Providern zwar missbraucht werden können, sie aber letztlich harmlose Alltagshandlungen sind und die Sorgfaltspflichten der Provider dementsprechend ausfallen müssen, hat sich zumindest im Bereich der zivilrechtlichen Haftung noch nicht etabliert.

Inhaltsübersicht

I. Einleitung

A. Aktualität damals und heute

[Rz 1] In jedem Berufs- und Branchenzweig stellen sich mancherlei Fragen zur straf- und zivilrechtlichen Verantwortlichkeit seiner Akteure. Das ist an sich nichts Ungewöhnliches und erregt im Normalfall auch nicht das Interesse eines breiteren Publikums. Das ist im Falle der Internet-Provider[1] allerdings nicht so: Die öffentliche Diskussion um die Verantwortlichkeit dieser Branche ist so alt wie die Branche selbst. Sie hat freilich nichts mit der Frage zu tun, ob ein Internet-Provider – welche konkrete Rolle er auch hat – seinen Vertragspflichten gegenüber seinen Kunden

nachkommt. Es geht nicht um Ausfälle von Internet-Zugängen, ebensowenig um Sabotage- oder Hacker-Angriffe, noch um vergessene Backups. Zu reden gibt nur eines: Die Verantwortlichkeit der Internet-Provider für die Handlungen ihrer Kunden und anderer Benutzer des Internets.

[Rz 2] In der Schweiz setzte die Diskussion im Sommer 1998 erstmals richtig ein[2]. Ausgelöst wurde sie von einem Schreiben der damaligen Bundespolizei an die «Internet Service Provider in der Schweiz». Die grossen und kleinen Anbieter von Internet-Zugängen wurden darauf aufmerksam gemacht, dass unter einer Reihe konkret aufgeführter Internet-Adressen Inhalte angeboten wurden, die eindeutig das Verbot der Rassendiskriminierung verletzten. Diese Angebote lagen notabene nicht auf den Servern der angeschriebenen Provider. Der einzige Tatbeitrag der Provider bestand darin, Zugang zum Internet zu verschaffen, über welches wiederum auf die fraglichen Websites zugegriffen werden konnte. Sollten die Provider den Zugang über ihre Systeme zu diesen Adressen nicht sperren, wie auch immer dies zu bewerkstelligen wäre, stünde «mit dem durch Sie gegebenenfalls ermöglichten Zugang zu den entsprechenden Sites eine strafbare Gehilfenschaft» zu den genannten Delikten in Frage, wurde den Providern beschieden[3]. Verwiesen wurde dabei auf den als «Telekiosk»-Fall bekannten BGE 121 IV 109, in welchem der damalige Generaldirektor der Telecom PTT strafrechtlich zur Verantwortung gezogen wurde, weil das von ihm geführte Unternehmen mit seiner Telekominfrastruktur kostenpflichtige Telefonsex-Angebote Dritter ohne die erforderlichen Jugendschutzmassnahmen ermöglichte. Der Brief der Bundespolizei an die Provider sollte den für eine Strafbarkeit erforderlichen Vorsatz schaffen.

[Rz 3] Zu einer Verurteilung eines Internet-Providers kam es damals bekanntlich nicht. Statt dessen begannen die inzwischen unter öffentlichen Druck geratenen Strafverfolgungsbehörden mit den Internet-Providern zusammenzuarbeiten, um im Rahmen der technischen Möglichkeiten zumindest gegen jene Internet-Straftäter vorgehen zu können, die aus oder in der Schweiz agierten[4].

[Rz 4] Seither flammt die Diskussion um die Verantwortlichkeit der Provider immer wieder auf, allerdings mit anderen Akzenten. Ein Beispiel vom November 2005 ist ein Schreiben der Schweizer Vertretung der International Federation of Producers of Phonograms and Videograms (IFPI), das an verschiedene Internet-Zugangsanbieter versandt wurde, deren Kunden[5] angeblich ohne Erlaubnis fremde Musikstücke im Internet über Tauschbörsen angeboten haben sollen. Die IFPI bat in ihren Schreiben die Internet-Provider nicht nur darum, die Identitäten dieser Kunden preiszugeben – was diesen, wie die IFPI hätte wissen müssen, aufgrund des Datenschutzgesetzes und Fernmeldegeheimnisses verboten ist. Die IFPI drohte den Internet-Providern implizit auch mit Strafverfolgung und zivilrechtlichen Ansprüchen, sollten sie den fraglichen Kunden weiterhin erlauben, ihre Internet-Zugänge für das illegale Anbieten von Musik im Internet zu nutzen. Man wies darauf hin, «dass die Mitwirkung an von einem Dritten begangenen Verletzungen von Urheber- und verwandten Schutzrechten als Gehilfenschaft ebenfalls strafbar und schadenersatzpflichtig ist, sobald Sie trotz Kenntnis von den Rechtsverletzungen beziehungsweise des entsprechenden Verdachtes diese weiterhin durch die fortgesetzte Zurverfügungstellung Ihrer technischen Infrastruktur ermöglichten», schrieb die IFPI[6]. Adressen ihrer Kunden geben Provider wie Bluewin der IFPI ohnehin nicht bekannt, leiten die Warnungen der IFPI aber inzwischen auch nicht mehr weiter[7]. Nichtsdestotrotz verdeutlichen die Aktivitäten der IFPI, dass die Diskussion der straf- und zivilrechtlichen Verantwortlichkeit der Internet-Provider nach wie vor aktuell ist. Inwiefern sie praktische Relevanz hat, ist allerdings eine andere Frage, auf die noch einzugehen sein wird[8].

B. Politischer Kontext

[Rz 5] Die in der Schweiz seit Jahren geführte Diskussion kann nur verstehen, wer auch den politischen Kontext kennt. Dieser geht zurück auf die Anfänge der Internet-Euphorie ab Mitte der 90er-Jahre. Das Internet wurde damals in der Öffentlichkeit nicht als allzwecktaugliches Arbeits- und Unterhaltungsinstrument empfunden und schon gar nicht nüchtern als Telekommunikationsnetz betrachtet, was es in den Jahrzehnten zuvor immer schon gewesen war. Gesehen wurde es vor allem als Plattform für die unkontrollierte Informationsverbreitung, die dadurch auffiel, dass sie für die Verbreitung verbotener, ungewollter oder gefährlicher Inhalte benutzt wurde. Es war die Zeit, in der das Internet für Websites mit Neonazi-Parolen, Pornographie und Anleitungen zum Selberbau von Nagelbomben bekannt wurde. Da sich diese Phänomene im Internet scheinbar «grenzenlos» ausbreiten konnten, war es den an die Landesgrenzen gebundenen Strafverfolgungsbehörden damals scheinbar nicht möglich, dagegen anzukommen. Überdies herrschte die Auffassung, dass Strafverfolger bezüglich neuer Technologien, wie das damalige World Wide Web eine war, nicht über das nötige Know-how für eine effektive Strafverfolgung verfügten.

[Rz 6] So stellte sich bald ein Ohnmachtsgefühl ein. Straftäter konnten das Internet scheinbar frei für ihre Zwecke nutzen, ohne dass die nationalen Strafverfolgungsbehörden dem auch nur ansatzweise beikommen konnten. In den USA konnten Neonazis ihre Rassismusparolen im Schutz der Meinungsäusserungsfreiheit auf ihren Websites frei verbreiten (man erinnere sich an die vielzitierte «Zündel»-Website). Die Folge war absehbar: Wenn schon nicht die Urheber der Cyberspace-Straftaten zu ermitteln oder zu fassen waren, hiess es, sollten wenigstens jene zur Verantwortung gezogen werden, die (damals) mit dem Betrieb der erforderlichen Infrastruktur gutes Geld verdienten – die Internet-Provider. Weil letztlich das Internet nichts anderes ist als ein Netz von zusammengeschalteten Netzwerken und jedes dieser Teilnetze von einem real existierenden Provider betrieben wird, lag es nahe, den Internet-Providern die Daumenschrauben anzusetzen. So wurde in Deutschland (zum Schluss allerdings erfolglos) der Chef des deutschen Ablegers eines der damals grossen Internet-Provider angeklagt, weil er den Zugang zu gewissen illegalen Inhalten auf einem Server der Muttergesellschaft in den USA nicht verhindert hatte[9]. In der Schweiz fürchteten sich die Organe hiesiger Zugangsprovider derweil erklärtermassen davor, für irgendwelche strafbaren Inhalte irgendwo im Internet stellvertretend verantwortlich gemacht zu werden, weil sie als einzige aller an der Datenübertragung zum Benutzer irgendwie beteiligter Personen in der Schweiz ansässig waren und damit der hiesigen Strafhoheit unterstanden.

[Rz 7] Weil es damals einerseits um öffentlichkeitswirksame Delikte wie Kinderpornographie oder Rassismus ging, die Internet-Provider vom Internet-Boom andererseits aber finanziell profitierten, hatten sie in der Öffentlichkeit immer wieder ein Legitimierungsproblem. Nichtsdestotrotz gab es (nicht nur in der Schweiz) erhebliche Proteste seitens der Provider sowie anderer Kreise, die kein «zensuriertes» Internet wollten, in welchem jeder Internet-Zugriff wie in Ländern wie China zuerst einen Provider-Filter durchlaufen müsste. Pikanterweise hatte die Musikindustrie eine solche Filterpflicht schon sehr früh verlangt. Demnach hätten Provider jeden Austausch von Musikdateien technisch unterbinden müssen, es sei denn, er stamme aus einer legalen Quelle. Dazu kam es – richtigerweise – nie, denn in der Öffentlichkeit ist mittlerweile ebenso erkannt worden, dass sich die Probleme des Internets durch eine Kriminalisierung der Internet-Zugangsprovider nicht lösen würden und ebenso nicht dadurch, ihnen die Verantwortung für jene Dinge zu übertragen, die auf ihren Datennetzen transportiert werden. Solche Regulierungsversuche hatte es im Übrigen schon im 19. Jahrhundert gegeben, als der Telegraph die Welt, wie heute das Internet, erobert hatte. Auch damals scheiterten solche Regulierungsversuche[10].

[Rz 8] In der Europäischen Union wurde im Jahre 2000 im Rahmen der so genannten E-Commerce-Richtlinie 2000/31/EG[11] («ECRL») das Prinzip festgeschrieben, dass Internet-Zugangsanbieter und andere reine «Durchleitungsanbieter» für die Inhalte der von ihnen übermittelten Informationen nicht verantwortlich gemacht werden können[12]. Auch jene Provider, auf deren Rechnern fremde Inhalte gespeichert würden, wurden von einer Verantwortlichkeit ausgenommen, zumindest solange, als ihnen die rechtswidrige Tätigkeit nicht bekannt ist[13]. Sobald sie dies aber ist, muss er sie entfernen oder den Zugang zu ihr sperren, wobei allerdings keine Pflicht besteht, die übermittelten oder gespeicherten Informationen zu überwachen oder aktiv nach rechtswidrigen Inhalten zu forschen[14].

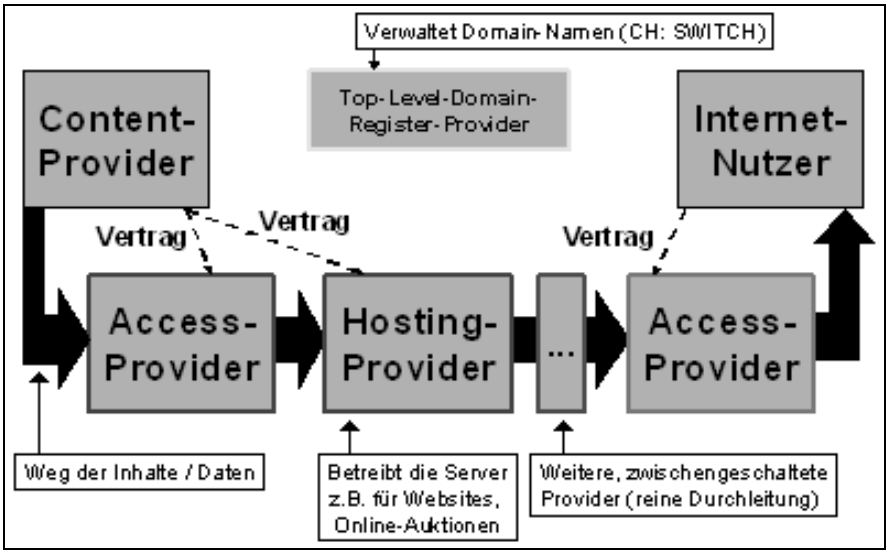
[Rz 9] In der Schweiz fehlen solche Bestimmungen, was im Jahre 2000 zu einer ständerätlichen Motion unter dem Titel «Netzwerkkriminalität» geführt hat[15]. Diese wurde zwar offen formuliert, zielte jedoch darauf ab, in der Schweiz eine ähnliche Bestimmung wie in der bereits erwähnten E-Commerce-Richtlinie zu schaffen und somit letztlich für eine Klarstellung der (nicht weit zu fassenden) Verantwortlichkeit der Provider zu sorgen – im Gegensatz zur EU aber stets mit Fokus auf das Strafrecht. Die Motion wurde 2001 in beiden Räten angenommen und in der Folge wurde von einer Expertengruppe ein Bericht ausgearbeitet, der im Juni 2003 dem Bundesrat vorgelegt und daraufhin veröffentlicht wurde («Expertenbericht»)[16]. Im Dezember 2004 erschien schliesslich ein Bericht des Bundesrates und zur Vernehmlassung ein Vorentwurf über eine neue Regelung der strafrechtlichen Verantwortlichkeit der Provider und die Kompetenzen des Bundes bei der Verfolgung strafbarer Handlungen mittels elektronischer Kommunikationsnetze («Bericht zum Vorentwurf» und «Vorentwurf»)[17]. Der (weiter hinten erörterte) Vorentwurf lehnt sich stark an den Expertenbericht an[18].

II. Verantwortlichkeit im Strafrecht

A. Ein Expertenstreit

[Rz 10] Die strafrechtliche Verantwortlichkeit der Internet-Provider ist in der Schweiz seit je her umstritten. Ohne die diesbezügliche Diskussion im Einzelnen darlegen zu wollen[19], dreht sie sich im Wesentlichen um die Frage der Anwendbarkeit und Anwendung des Medienstrafrechts (Art. 27 StGB, Art. 322bis StGB) auf Internet-Provider, sowie um die Anwendung der allgemeinen Regeln des Strafrechts, insbesondere über die Gehilfenschaft, auf Internet-Provider.

[Rz 11] Dabei ist es wichtig, die verschiedenen Erscheinungsformen des Internet-Providings auseinanderzuhalten. Typischerweise unterschieden wird dabei zwischen den Anbietern, die lediglich den Zugang ins Internet anbieten (so genannte Access-Provider), und denjenigen, die ihre Server-Infrastruktur für das Bereithalten von Inhalten zur Verfügung stellen (so genannte Hosting-Provider). Immer wieder ist auch vom «Content-Provider» die Rede, doch ist dieser Begriff insofern irreführend, als dass damit lediglich diejenige Person gemeint ist, von welcher der fragliche Inhalt stammt (also beispielsweise der Verfasser bzw. Urheber einer Website). Hingegen wird kaum vom Domain-Name-Service-Provider gesprochen, also jenem Provider, der sicherstellt, dass die Domain-Namen einer bestimmten «Endung» (sprich: Top-Level-Domain) im Internet für Internet-Adressen verwendet werden können. In der Diskussion der Provider-Verantwortlichkeit landläufig nicht unterschieden wird auch zwischen dem Access-Provider des Abrufers einer Information und dem Access-Provider, der es einem Straftäter überhaupt erst möglich macht, seinen eigenen Server mit strafbaren Inhalten ans Internet anzuschliessen. Die folgende Grafik zeigt das Verhältnis und die Position der verschiedenen Provider mit Bezug auf den Datenfluss im Internet.



[Rz 12] Ausgehend von den beiden Formen des Access-Providers und des Hosting-Providers wurde auf verschiedene Weise versucht, die Strafbarkeit zu begründen oder aber abzulehnen. Das Bundesamt für Justiz und in der Folge das damalige Bundesamt für Polizeiwesen vertrat in einem vielzitierten Gutachten[20] bzw. Positionspapier[21] gegenüber den Providern eine sehr restriktive Haltung und sah im Wesentlichen auch eine Strafbarkeit des reinen Access-Providers (des Internet-Nutzers) für gegeben, sollten bekannte strafbare Inhalte nicht gesperrt werden[22]. Dem widersprach mehr oder weniger ausnahmslos die damalige Schweizer Lehre als auch ein prominentes, von einem Provider-Interessensverband in Auftrag gegebenes Gegengutachten («VIT-Gutachten»), welches eine Strafbarkeit der Access-Provider ablehnt[23].

[Rz 13] Zusätzlich kompliziert wurde die Diskussion durch den höchstrichterlichen Entscheid BGE 125 IV 206 aus dem Jahre 1999, der den Grundsatz in Frage stellt, wonach, was sich medial veröffentlichen lässt und sich in der Veröffentlichung erschöpft, ein Mediendelikt ist, auf welches das Medienstrafrecht zur Anwendung komme. Das Bundesgericht verwies in seiner Entscheidung ausdrücklich auf harte Pornographie (Art. 197 Ziff. 3 StGB), Gewaltdarstellungen (Art. 135 StGB) und das Leugnen von Völkermord (Art. 261bis Abs. 4 StGB), welche nicht zu den Mediendelikten zu zählen sind.

[Rz 14] Während die Frage der territorialen Anwendbarkeit des Strafrechts auf Internet-Provider für vergleichsweise wenig Gesprächsstoff sorgte[24], wurde um so mehr darüber diskutiert, wie Internet-Provider im Falle einer Strafbarkeit mit deren praktischen Konsequenzen umgehen sollten: Welche Art Hinweise würden genügen, um zumindest einen Eventualvorsatz eines Internet-Providers zu begründen? Welche technischen Eingriffsmöglichkeiten seien für einen Access-Provider

möglich und zumutbar? Darf der Umstand, dass sich ein Internet-Provider ernsthaft mit der Bekämpfung von Straftaten im Internet auseinandersetzt, diesem letztlich ein höheres Strafbarkeitsrisiko eintragen, im Gegensatz zu einem Provider, der sich um Hinweise nicht kümmert?

[Rz 15] Während in der öffentlichen Diskussion immer der Standpunkt vertreten wurde, eine Sperrung von Internet-Angeboten sei für einen Access-Provider nicht zumutbar, zeigten einzelne Provider, die um Strafverfolgung fürchteten, dass solche Sperrungen nichtsdestotrotz möglich waren. Das tatsächliche Problem war (und ist) jedoch nicht, ob es technische Möglichkeiten gibt, mit denen ein Access-Provider den Zugriff auf bestimmte Websites, Server, IP-Adressen oder Domain-Namen verhindern kann – er kann es tun[25]. Das tatsächliche Problem sind, abgesehen von der Problematik des Missbrauchspotentials[26], die Skalierbarkeit und die Nebenwirkungen. Wird ein Access-Provider dazu verpflichtet, den Zugang zu fünf rassistischen Websites zu sperren, folgen bald 50, 500 und 500´000 illegale Angebote im Internet, die er ebenfalls sperren soll, weil auch sie entsprechende Gesetzesbestimmungen verletzen. Es ist nicht zu erwarten, das die Regeln, die für eine Strafbarkeit des Providers im Falle der Verletzung des Verbots der Rassendiskriminierung sorgen, im Falle anderer Delikte nicht ebenso oder ähnlich anwendbar sind, – und an Delikten fehlt es im Internet wie in der «realen» Welt beileibe nicht. Im Bereich der zivilrechtlichen Haftung stellt ist dieses Ausuferungspotential noch sehr viel grösser, weil der Katalog der möglichen unerlaubten Handlungen gegenüber den auch strafbaren Handlungen sehr viel weiter geht.

[Rz 16] Die Nebenwirkungen von Sperrungen sind ebenfalls nicht zu unterschätzen: Zwar gibt es heute technische Verfahren, mit denen beispielsweise für die Mehrheit der Internet-Benutzer der Zugriff auf bestimmte Domain-Namen verunmöglicht werden kann. Damit sind aber auch allfällige legale und erwünschte Angebote unter diesen Domain-Namen nicht mehr nutzbar. Dieser «Kollateralschaden» kann je nach Art der Sperrung unterschiedlich gross ausfallen und wirkt um so gewichtiger, als jene Content-Provider, deren Angebote gesperrt werden sollen, erfahrungsgemäss die ersten sein werden, die ihre Angebote unter neuen, von den Sperren noch nicht erfassten Adressen neu lancieren, die legitimen, von den Sperren miterfassten Angebote und Aktivitäten hingegen durch diese weiterhin beeinträchtigt werden. Aus diesen und weiteren Gründen hat sich inzwischen denn auch international die Ansicht durchgesetzt, dass es nicht sein kann, den Access-Provider stellvertretend für jene unerwünschten Erscheinungen verantwortlich zu machen, die das Internet zwangsläufig mit sich bringt und auf die auch ein Access-Provider keinen wirklichen Einfluss hat[27].

B. Begrenzter Leidensdruck – und kaum Praxis

[Rz 17] In der Schweiz hielt sich der alltägliche Leidensdruck sowohl der Strafverfolger als auch der Internet-Provider ungeachtet der oben erwähnten Diskussion bisher in engen Grenzen. Dies wiederspiegelt sich in der Tatsache, dass es, anders als etwa in Deutschland, bisher kaum zu Praxis im Bereich der Verantwortlichkeit von Providern gekommen ist. Die wenigen tatsächlich existierenden Fälle beschränken sich auf strafrechtliche Aspekte.

[Rz 18] Der vielzitierte Bundesgerichtsentscheid BGE 121 IV 109 («Telekiosk») ist in diesem Zusammenhang sicherlich der wichtigste Entscheid, auch wenn regelmässig darauf hingewiesen wird, dass seine Feststellungen nicht unbesehen auf Internet-Provider übertragen werden können[28]. Jedenfalls hat das Bundesgericht nach der hier vertretenen Ansicht das fortgesetzte Zurverfügungstellen einer für eine Straftat benutzten Telekommunikationseinrichtung richtigerweise als aktives Tun[29] und nicht als Unterlassen qualifiziert: So kann ein Provider beispielsweise nicht mit einem Autovermieter verglichen werden, der seinem Kunden ein Fahrzeug überlässt und nach dessen Übergabe einstweilen keine weitere Leistung zu erbringen hat. Ein Hosting-Provider ist – um beim Verkehr zu bleiben – vielmehr mit einem Limousinenservice zu vergleichen, der seinem Kunden sein Fahrzeug mitsamt Fahrer überlässt: Befördert der Fahrer seinen Gast auch dann noch weiter, wenn dieser eine Bank ausraubt, wird dem mit Wissen und Willen freiwillig weiterarbeitenden Fahrer zweifellos nicht eine Unterlassungstat vorgeworfen, sondern ein aktives Fördern des Haupttäters bei dessen Raubzügen. Auch die Arbeit des Hosting-Providers beschränkt sich nicht auf das initiale Bereitstellen des Servers. Seine Haupttätigkeit liegt im aktiven Aufrechterhalten des Server-Betriebs und der darauf befindlichen Website seines Kunden, was sich auch schon an den regelmässigen Gebühren zeigt, die Hosting-Provider für ihre Dienstleistungen verlangen.

[Rz 19] Ob die Streitfrage einer Strafbarkeit für aktives Tun oder durch Unterlassen von praktischer Relevanz ist, darf freilich bezweifelt werden, da sie letztlich dieselben Wertungsfragen aufwirft[30]: Schafft ein Internet-Provider ein gesellschaftlich unerwünschtes Risiko[31]? Welche Sorgfaltspflichten werden von ihm erwartet? Erstere Frage ist zwar umstritten, muss aber m.E. mindestens beim Access-Provider mit einem Nein beantwortet werden: Wenn die heutige Gesellschaft das Internet wünscht, woran die Entwicklung der vergangenen Jahre wohl kaum Zweifel lässt, kann es nicht angehen, dass diejenigen, deren einzige Aufgabe darin besteht, eben jener Gesellschaft diese Infrastruktur

bereitzustellen, von derselben Gesellschaft deswegen als Gefahr betrachtet werden. Der Internet-Provider ist ein wertneutraler Dienstleistungserbringer. Der Strafgerichtspräsident Basel-Stadt im Entscheid «Lyrics Server» vom 31. Januar 2003 hat dies treffend formuliert[32]: «Das Zurverfügungstellen eines Internetzugangs ist dem Anschliessen eines Telefons ans Telefonnetz vergleichbar. Auch über das Telefon werden die verschiedensten Delikte begangen, ohne dass jemand auf die Idee kommen würde, das Zurverfügungstellen des Telefonanschlusses als gefährlich zu bezeichnen. In der Zurverfügungstellung des Internetzugangs kann deshalb unter keinen Umständen die Schaffung eines <unerlaubten> Risikos für strafrechtlich geschützte Rechtsgüter gesehen werden, die eine strafrechtliche Haftung aus Ingerenz rechtfertigen würde»[33].

[Rz 20] Vertreter anderer Behörden haben die strafrechtliche Verantwortlichkeit von Internet-Access-Providern anders beurteilt. So hat die Eidg. Spielbankenkommission im November 2000 über 200 Provider aufgefordert, den Zugriff auf 591 illegale Spielbanken zu sperren, dies gestützt auf Art. 5 des Spielbankengesetzes[34]. Auf Proteste der Provider hin kamen beide Seiten ins Gespräch, und die Behörde erklärte den Vollzug der in ihrem ursprünglichen Schreiben geforderten Massnahmen als aufgeschoben.

[Rz 21] Für Aufsehen sorgte auch die Affäre «Appel au peuple», in welcher eine Waadtländer Untersuchungsrichterin zahlreiche Internet-Access-Provider der Schweiz, gestützt auf eine besondere Bestimmung des dortigen Prozessrechts, mit einer Sperrverfügung betreffend ehrverletzender Websites bedachte, letztlich aber scheiterte[35]. Immerhin ging das zuständige Gericht davon aus, dass eine Strafbarkeit der Access-Provider grundsätzlich möglich sei. Es sind allerdings keine Weiterungen in diesem Fall bekannt; die fraglichen Websites sind im Übrigen weiterhin abrufbar.

[Rz 22] Die andere Streitfrage, der Umfang der Sorgfaltspflichten eines Internet-Providers, stellte sich in der Praxis bisher nicht. In den wenigen beurteilten Fällen wussten die Provider nach Ansicht der Gerichte genau, was sie taten – und sie billigten es auch. Zu erwähnen ist etwa die «Mailbox»-Entscheidung des Zürcher Obergerichts vom 7. Dezember 1998. Sie betraf ein elektronisches Schwarzes Brett (ein so genanntes Bulletin-Board- oder Mailbox-System), das für Computerbenutzer nicht über das Internet zugänglich war, sondern über spezielle Einwahlnummern für Modems. Das System diente als für jedermann offene Online-Tauschbörse (damals war der Austausch von Musikdateien allerdings noch kein Thema). Wer etwas beziehen wollte, musste für je drei Dateien eine eigene Datei beisteuern. 1995 wurden im Rahmen einer Polizeiaktion auf dem Rechner des Systems auch rund 1´000 pornographische Dateien ermittelt; der Betreiber – ein Student – wurde wegen der Inhalte der von ihm unterhaltenen Tauschbörse schliesslich zu 600 Franken Busse verurteilt. Das Gericht ging davon aus, er habe bewusst jede Alterskontrolle unterlassen und so Jugendlichen ungehinderten Zugang zu pornographischem Material geboten. Dieses Material wurde zwar von Dritten in der Tauschbörse deponiert, vom Betreiber aber in entsprechende Unterverzeichnisse verschoben, womit für die Richter erwiesen war, dass der Betreiber über die fraglichen Inhalte im Bilde war und sie billigte.

[Rz 23] Von einem vorsätzlichem Handeln ging auch das Strafgericht Basel-Landschaft aus, als es mit (nicht veröffentlichtem) Entscheid vom 16. Dezember 1999 einen Internet-Hosting-Provider zu einer Busse von 300 Franken wegen Gehilfenschaft zur Datenbeschädigung verurteilte. Der Provider hatte einem Italiener die Benutzung seines Servers erlaubt, was dieser wiederum zur Verbreitung einer Anleitung zum Virenbau benutzte. Den Umstand, dass solche Inhalte gemäss den Vertragsbestimmungen von Providern nicht erlaubt sind, liess das Gericht nicht gelten, ebensowenig das Argument, die Vireninformationen dienten der Virenbekämpfung, nicht der Datenbeschädigung: Der Provider sei ein Fachmann (auch in Sachen Viren) gewesen und habe gewusst, was sich über seinen Server abspielte. Damit habe er in Kauf genommen, dass die Anleitung auch für unzulässige Zwecke benutzt werden konnte.

[Rz 24] Zu erwähnen ist an dieser Stelle, dass ein Grund für das Fehlen von Praxis in diesem Bereich wohl darin zu suchen ist, dass Internet-Provider in der Schweiz in der Bekämpfung der Netzwerkkriminalität mit den Behörden gut kooperieren. Die in diesem Bereich aktiven Strafverfolgungsbehörden stellen der hiesigen Provider-Branche denn auch im Grossen und Ganzen ein sehr gutes Zeugnis aus; die Zusammenarbeit klappt gut, auch wenn die Provider ihrerseits an bestimmte gesetzliche Rahmenbedingungen, wie das Fernmeldegeheimnis, gebunden sind.

[Rz 25] Immerhin bestehen mit dem Bundesgesetz über die Überwachung des Post- und Fernmeldeverkehrs (BÜPF[36]) und einer entsprechenden Verordnung und Ausführungsvorschriften seit einigen Jahren relative klare Regeln für die Frage der Überwachung von Internet-Aktivitäten (auch wenn in der Praxis die Tarifansätze in diesem Bereich immer wieder für Gesprächsstoff sorgen). So sieht beispielsweise Art. 15 BÜPF vor, dass Internet-Provider bestimmte Randdaten der Internet-Nutzung ihrer Kunden während sechs Monaten aufbewahren müssen, um diese auch noch rückwirkend identifizieren zu können. In diesem Zusammenhang hält Art. 14 Abs. 4 BÜPF im Sinne einer Internet-«Sondervorschrift»

wiederum fest, dass, wenn «eine Straftat über das Internet begangen» wird, eine Internet-Anbieterin verpflichtet ist, der zuständigen Behörde «alle Angaben zu machen, die eine Identifikation des Urhebers oder der Urheberin ermöglichen.» Eine richterliche Genehmigung ist in diesem Fall nicht erforderlich. Dabei hat die Rekurskommission UVEK im Jahre 2004 entschieden, dass diese Regelung auch für dynamische Internet-Adressen gilt, also auch auf jene Internet-Nutzer anwendbar ist, die keinen festen Internet-Zugang haben, sondern sich via Telefonanschluss ins Internet einwählen[37]. Diese Bestimmung gibt den Strafverfolgungsbehörden ein relativ wirksames Instrument in die Hand, mögliche Internet-Straftäter in der Schweiz zu ermitteln, auch wenn diese zunächst scheinbar anonym im Internet auftreten (zum Beispiel als Benutzer von Internet-Tauschbörsen). In der Regel genügt eine IP-Adresse und eine genaue Angabe von Datum und Zeit ihrer Nutzung, um anhand der von den verschiedenen Providern geführten Adress- und Verbindungsprotokolle den betreffenden Abonnenten zu ermitteln.

[Rz 26] Bei der Identifikation von Internet-Benutzern für (reine) zivilrechtliche Ansprüche hilft dieses Verfahren allerdings nicht weiter. Hier sind Anspruchsberechtigte auf den Goodwill der Provider angewiesen, soweit sich diese in ihren allgemeinen Geschäftsbedingungen überhaupt das Recht vorbehalten, Kundendaten gegenüber Dritten mit schutzwürdigen Interessen offenzulegen.

C. Providerstrafrecht de lege ferenda

1. Vorschlag des Expertenberichts

[Rz 27] Der in der Folge der Motion «Netzwerkkriminalität» entstandene Expertenbericht[38] kam ob der zahlreichen Diskussionen und unterschiedlichen Standpunkte zum Schluss, dass keine klare, ausdrückliche Regelung der Verantwortlichkeit im Zusammenhang mit Internet-Inhalten besteht. Darum sei eine eindeutige Regelung im Gesetz angezeigt, so die Experten[39]. Sie erarbeiteten einen Vorschlag mit den folgenden Zielen[40]:

- Der Autor und der Content-Provider für von ihnen ausgehende illegale Inhalte sollen strafrechtlich voll verantwortlich sein;
- Der Hosting-Provider soll beschränkt haften, d.h. im Wesentlichen nur, wenn er die mögliche und zumutbare Verhinderung der Nutzung deliktischer Informationen wider besseres Wissen unterlässt oder von Dritten erhaltene Hinweise auf solche Informationen nicht an die Strafverfolgungsbehörden weiterleitet. In diesem Rahmen strafrechtlich belangt werden können soll der Hosting-Provider, «der sich in der Schweiz befindet», auch wenn sich die Täterschaft im Ausland aufhält;
- Der Access-Provider soll für im Netz zirkulierende deliktische Inhalte nicht strafrechtlich verantwortlich sein.

[Rz 28] Der Expertenbericht beschäftigte sich ausserdem mit Fragen der Strafverfolgung im Falle von strafbaren Internet-Inhalten. Auf diesen Themenkomplex wird hier nicht weiter eingegangen.

2. Vorentwurf des Bundesrates

[Rz 29] Gestützt auf den Expertenbericht legte der Bundesrat im Oktober 2004 einen Bericht und Vorentwürfe über die Änderung des Strafgesetzbuches über die strafrechtliche Verantwortlichkeit der Provider und die Kompetenzen des Bundes bei der Verfolgung strafbarer Handlungen mittels elektronischer Kommunikationsnetze vor[41]. Der Vorentwurf nimmt die Grundidee des Expertenvorschlags auf, liefert aber einen eigenen Entwurf für eine Regelung:

(neuer Titel) 6. Strafbarkeit in elektronischen Kommunikationsnetzen und in Medien
Artikel 27 VE-StGB
Strafbarkeit in elektronischen Kommunikationsnetzen

1 Wird eine strafbare Handlung mittels Übertragung, Bereitstellen oder Bereithalten von Informationen in einem elektronischen Kommunikationsnetz begangen, so gelten die allgemeinen Bestimmungen dieses Gesetzes über Täterschaft und Teilnahme. Vorbehalten bleiben die nachfolgenden Bestimmungen:

[2] Ist der Täter Autor oder Redaktor im Sinne von Artikel 27bis, so richtet sich die Strafbarkeit nach dieser Bestimmung.

[3] Wer fremde Informationen zur Nutzung in einem elektronischen Kommunikationsnetz automatisiert bereithält, macht sich unter den Voraussetzungen von Artikel 322bis Ziffer 1 strafbar. Das Bereithalten eines Verzeichnisses, in welches fremde Informationen automatisiert aufgenommen werden, gilt als Bereithalten fremder Informationen.

[4] Wer lediglich den Zugang zu einem elektronischen Kommunikationsnetz vermittelt, ist nicht strafbar. Eine automatische und kurzzeitige Speicherung fremder Informationen infolge Nutzerabfrage gilt als Zugangsvermittlung.

Artikel 322bis VE-StGB
Nichtverhindern strafbarer Handlungen in elektronischen Kommunikationsnetzen und in Medien

1. Wer in einem elektronischen Kommunikationsnetz fremde Informationen automatisiert bereithält, mittels deren, wie er sicher weiss, eine strafbare Handlung begangen wird, und es unterlässt, die Nutzung dieser Informationen zu verhindern, obwohl es ihm technisch möglich und zumutbar ist, wird mit Gefängnis oder Busse bestraft.
   Wer in einem elektronischen Kommunikationsnetz fremde Informationen automatisiert bereithält, mittels deren eine strafbare Handlung begangen wird, und es unterlässt, von Dritten an ihn gerichtete und bei ihm eingegangene Hinweise auf solche Informationen an die Strafverfolgungsbehörden weiterzuleiten, wird mit Gefängnis oder Busse bestraft.
   Handelt es sich bei der strafbaren Handlung um ein Antragsdelikt, so wird die Tat nur verfolgt, wenn ein Antrag auf Verfolgung der strafbaren Handlung vorliegt.
   Ob mittels einer Information eine strafbare Handlung begangen wird, beurteilt sich nach schweizerischem Recht.
   Informationen im Sinne der Absätze 1 und 2 werden ungeachtet schweizerischer Strafhoheit gelöscht.

2. Wer als Verantwortlicher nach Artikel 27bis Absätze 2 und 3 eine Veröffentlichung, durch die eine strafbare Handlung begangen wird, vorsätzlich nicht verhindert, wird mit Gefängnis oder Busse bestraft. Handelt der Täter fahrlässig, so ist die Strafe Haft oder Busse.

[Rz 30] Der Vorentwurf sollte neben dem geltenden Medienstrafrecht eine parallele Regelung für Provider schaffen, gewissermassen ein Providerstrafrecht.

3. Keine Strafbarkeit für Access-Provider

[Rz 31] Der Vorentwurf sieht über einen neuen Art. 27 VE-StGB im allgemeinen Teil des StGB zunächst eine Sonderregelung vor, wonach eine Strafbarkeit reiner Access-Provider vollständig ausgeschlossen wird. Damit ist die allenthalben diskutierte Pflicht zur Sperrung von Websites mit strafbaren Inhalten oder die Filterung solcher vom Tisch. Dies gilt auch für Forderungen, wonach die Übertragung von unzulässigen Inhalten (z.B. Raubkopien) über das Internet generell zu unterbinden sei. Immerhin ist darauf hinzuweisen, dass in der EU im Zusammenhang mit der so genannten Durchsetzungsrichtlinie 2004/48/EG[42] ein Auskunftsanspruch von Rechteinhabern gegenüber Raubkopierern einerseits wie auch andererseits gegenüber Dritten, darunter auch Internet-Providern, vorgesehen ist.

[Rz 32] Eine Frage bleibt beim Entwurf für ein Providerstrafrecht allerdings offen: Fällt auch der Access-Provider des Straftäters unter diese Regelung? Ist also auch jener straffrei, der einem Straftäter zur Vornahme seiner Delikte den Zugang zu einem elektronischen Kommunikationsnetz vermittelt? Diese Frage wird auch in der internationalen Diskussion kaum erörtert, weil der Begriff des Access-Providers nicht danach differenziert wird, ob dieser mit dem Täter in direkter vertraglicher Beziehung steht und erst die Erfüllung dieses Vertrags die Straftat ermöglicht oder aber, ob es sich um einen Access-Provider eines beliebigen Internet-Benutzers handelt. Im Falle des Access-Providers des Täters wäre es wohl angezeigt, eine vergleichbare Regelung wie im Falle eines Hosting-Providers anzuwenden, die allerdings darauf Rücksicht nehmen muss, dass der Access-Provider nicht in derselben Weise in die Verbreitung strafbarer Informationen eingreifen kann wie der Hosting-Provider, über dessen Server die Verbreitung erfolgt[43].

4. Hosting-Provider strafbar nur nach Sonderdeliktsnorm

[Rz 33] Hosting-Provider werden in ihrer diesbezüglichen Funktion ebenfalls von einer Stafbarkeit nach den allgemeinen Regeln ausgenommen, mit Ausnahme im Falle der im neuen Art. 322bis VE-StGB definierten Sonderdelikte für Hosting-Provider. Mit anderen Worten sollen Hosting-Provider nicht mehr als Gehilfen der Haupttäter (d.h. der Content-Provider) haften sondern nach einer Sondernorm im Rahmen von dort definierten (echten) Unterlassungstatbeständen. Faktisch wird ihre Strafbarkeit gegenüber der heutigen Situation eingeschränkt[44].

[Rz 34] Damit stellt sich im Übrigen auch die Frage der Akzessorietät zur Haupttat nicht mehr. Der Haupttäter braucht nach dem Konzept des Art. 322bis VE-StGB ohnehin nicht mehr verfolgt werden, damit der Provider strafrechtlich zur Verantwortung gezogen werden kann. Auch wenn nach den allgemeinen Regeln des Strafrechts eine bestimmte Tat in der Schweiz strafrechtlich nicht verfolgt werden könnte (etwa weil es an einer Strafhoheit für die Schweiz fehlt[45]), würde der Hosting-Provider im Rahmen der in Art. 322bis VE-StGB definierten Delikte strafrechtlich belangt werden können, da die fraglichen Informationen ungeachtet der allgemeinen Grundsätze einer schweizerischen Strafhoheit nach schweizerischem Recht beurteilt werden sollen.

[Rz 35] Der wohl unbeabsichtigte Nachteil einer solchen Lösung liegt darin, dass die Strafbarkeit eines Providers selbst dann bestehen würde, wenn das fragliche Internet-Angebot keinen Bezug zur Schweiz hat, sich ja möglicherweise nicht einmal auf einem Server in der Schweiz befinden muss, wenn der rechtliche Sitz des Providers als Anknüpfungskriterium für eine Strafhoheit genügen würde. Schwierigkeiten mit unvorhersehbaren Konsequenzen ergeben sich auch im Bereich von Delikten, die Immaterialgüterrechte betreffen, da diese nach hiesiger Auffassung dem Recht des Staates unterstehen müssen, für den deren Schutz beansprucht wird[46].

[Rz 36] Die Folge ist, dass insbesondere international tätige Hosting-Provider aus den USA, die einen Standort für ihr internationales oder Europageschäft suchen, nicht mehr ohne zusätzliches Risiko die Schweiz als Standort wählen könnten. Eine Lösungsmöglichkeit wäre die Ergänzung der Bestimmung durch einen Vorbehalt, dass eine Strafbarkeit nur im Falle von Informationen gegeben sein kann, die (auch) speziell auf eine Nutzung in der Schweiz ausgerichtet sind. Damit könnte eine hiesige Strafbarkeit eines in der Schweiz domizilierten Betreibers einer Internet-Auktionsplattform für den chinesischen Markt ausgeschlossen werden (wie sie nach Art. 322bis VE-StGB jedoch denkbar wäre).

[Rz 37] Der Vorentwurf stellt bezüglich Strafbarkeit von Hosting-Providern – grob gesagt – vier Regeln auf:

a) Regel 1: Regelung gilt nur für das Bereithalten fremder Informationen

[Rz 38] Nach der ersten Regel gilt der Ausschluss der Strafbarkeit des Providers nach den allgemeinen Regeln des Strafgesetzbuches nur soweit der Hosting-Provider fremde strafbare Informationen bereithält. Die Schwierigkeit der vorgeschlagenen Formulierung besteht darin, dass nicht nur auf die Fremdheit der Information abgestellt wird (was an sich genügen würde), sondern zusätzlich nur jene Provider von der herkömmlichen Strafbarkeit ausgenommen werden, welche diese Informationen «automatisiert» bereithalten. Obwohl diese Voraussetzung auf den ersten Blick einleuchten mag, wirft sie auf den zweiten Blick Fragen auf: Führt dieses Kriterium dazu, dass all jene Hosting-Provider von einer Haftungsbeschränkung ausgenommen wären, die von sich aus – ohne Rechtspflicht – automatisierte Inhaltskontrollen durchführen (z.B. durch eine Suche nach bestimmten, heiklen Stichwörtern) und die ihnen verdächtig erscheinenden Inhalte manuell auf offensichtliche Regelverstösse kontrollieren? Würde dieser Umstand dazu führen, dass nicht mehr von einem «automatisierten» Bereithalten gesprochen werden kann (was abzulehnen ist), würden verantwortungsbewusste Hosting-Provider benachteiligt, wogegen jene Hosting-Provider, die sich um die Inhalte auf ihren Servern überhaupt nicht kümmern wollen deswegen ein geringeres Strafbarkeitsrisiko eingehen. Dies kann nicht die Absicht des Gesetzgebers sein.

[Rz 39] Deshalb sollte das Kriterium des «automatisierten» Bereithaltens ersatzlos gestrichen werden. Oder es sollte zumindest klargestellt werden, dass es das Entgegennehmen der fremden Information ist, das automatisiert ablaufen muss (die diesbezüglichen Ausführungen im Expertenbericht sind technisch nicht korrekt[47]). Über den Begriff der

«Fremdheit» der Information sind jene Hosting-Provider, die sich die Inhalte zum Beispiel im Rahmen einer vorgängigen, redaktionellen Kontrolle zu eigen gemacht haben und damit auch Content-Provider sind, bereits von einer Haftungsprivilegierung ausgeschlossen.

[Rz 40] Klarheit sollte in der einen oder anderen Weise auch über die Behandlung von elektronischen Marktplätzen, die Angebote von Dritten in ihre Datenbanken bzw. in ihre Handelsplattformen aufnehmen, geschaffen werden[48]. Die Betreiber dieser Infrastrukturen werden – im Gegensatz zu Suchmaschinen – nicht ausdrücklich erwähnt, fallen aber, soweit es nur um den Betrieb der Handelsinfrastruktur geht, richtigerweise ebenfalls unter den Begriff des Hosting-Providers[49]. Die Betreiber von solchen Online-Marktplätzen bieten zwar eine äusserlich einheitlich gestaltete Umgebung an, doch der Inhalt der Kauf- und Verkaufsangebote stammt letztlich von Dritten und zielt auf einen Kaufvertrag mit einem anderen Dritten; der Betreiber der Plattform stellt lediglich die Infrastruktur hierfür zur Verfügung, ist also selbst nicht Partei der Transaktion (aber immerhin meist mit einer vom Transaktionsvolumen abhängigen Gebühr daran beteiligt). Wie die Expertenkommission schon für klassische Suchmaschinen erkannt hat[50], wäre auch der Betrieb von Online-Marktplätzen nicht mehr möglich, wenn von einer Kontrollpflicht der verzeichneten Angebote ausgegangen werden müsste, zumal bei bekannteren Marktplätzen Dritte jeden Tag Hunderte von neuen Produkteangeboten aufschalten (im Vergleich dazu: Für die Zahl von rund 300 neuen Domain-Namen pro Tag in der Schweiz hat der Gesetzgeber eine Kontrollpflicht eines Domain-Namen-Providers bereits ausdrücklich verneint[51]).

b) Regel 2: Nichtverhindern der Inhalte wider besseren Wissens strafbar

[Rz 41] Der Vorentwurf sieht vor, dass ein Hosting-Provider strafbar wird, wenn er den Zugang zu fremder Information auf seiner Infrastruktur im Rahmen des technisch Möglichen und Zumutbaren nicht sperrt oder die Information entfernt, sobald er «sicher weiss», dass damit eine strafbare Handlung begangen wird.

[Rz 42] Mit dieser Regelung sollte, so die Idee, die Strafbarkeit des Hosting-Providers auf jene Fälle beschränkt werden, in denen ein Provider mit direktem Vorsatz handelt bzw. nicht handelt. Doch die zahlreichen Reaktionen auf die Formulierung des Vorentwurfs zeigen, dass dieses Begriffsverständnis keineswegs klar ist und der Begriff des «sicheren Wissens» letztlich mehr Fragen aufwirft, als er löst – vor allem dann, wenn «sicheres Wissen» nicht erst dann vorliegen soll, wenn dem Provider der Entscheid einer zuständigen richterlichen Behörde vorliegt, welche den konkreten Fall beurteilt hat. Letztlich wird es bei dieser Formulierung um jene Fälle gehen, in denen der Provider wider besseren Wissens um das Vorliegen einer Straftat nichts tut, um die Verbreitung der Inhalte zu verhindern.

[Rz 43] Ein solches Verständnis löst freilich nicht die Frage, welche Sorgfaltspflichten ein Hosting-Provider hat, um ein solches Wissen zu erlangen, sollte eine solche Sorgfaltspflicht überhaupt bestehen. Muss der Provider eine interne oder externe Rechtsabteilung unterhalten, um Hinweise auf fragwürdige Inhalte und Zufallsfunde zu beurteilen? Die Antwort muss ein klares Nein sein. Es kann nicht die Aufgabe eines Providers sein, dessen Rolle die Bereitstellung einer technischen Infrastruktur ist, auch noch über die rechtliche Zulässigkeit von Internet-Inhalten zu befinden. Zudem wird aus strafrechtlicher Sicht das Verschulden einer Person ohnehin nach deren subjektivem Wissen und Willen beurteilt. Es ist in diesem Zusammenhang allerdings nicht ganz klar, wie sich das Unternehmensstrafrecht[52] auf solche Fälle auswirkt. So könnte argumentiert werden, dass im Falle eines Providers zwar kein Organ und auch kein Mitarbeiter strafrechtlich verantwortlich werden, stattdessen aber das Unternehmen bestraft wird, wenn es wegen mangelhafter Organisation nicht möglich ist, diejenige natürliche Person zu ermitteln, die sich mit dem fraglichen Inhalt und der Würdigung eines Hinweises auseinandergesetzt hat, wenn davon ausgegangen wird, dass ein eingegangener Hinweis klar und eindeutig war.

[Rz 44] Die eigentliche Problematik der Bestimmung von Art. 322bis VE-StGB liegt jedoch an einem anderen Punkt: Derjenige Provider, der tatsächlich eine Rechtsabteilung hat oder einen Inhalt einer juristischen Prüfung unterzieht, geht dadurch ein Strafbarkeitsrisiko ein, das er ansonsten nicht hätte. Wiederum setzt der Vorentwurf also den falschen Anreiz: Es wird derjenige durch eine Haftungsprivilegierung belohnt, der den «Kopf in den Sand steckt» und derjenige einem Strafbarkeitsrisiko ausgesetzt, der sich bemüht hat, einen umstrittenen Inhalt auf seine Rechtmässigkeit zu überprüfen, ihm der Richter aber nicht glaubt, wenn er im Prozess behauptet, er habe einen bestimmten Inhalt nicht als strafbar erachtet. Der vorsichtige Provider wird somit auch in Zweifelsfällen eine Sperrung veranlassen, was sicherlich nicht Sinn der Sache sein kann. Eine solche Sperrung kann überdies zu einer zivilrechtlichen Verantwortlichkeit des Providers aus Verletzung des Hosting-Vertrags mit seinem Kunden führen[53].

[Rz 45] Das Problem wird dadurch noch verschärft, dass in der Praxis die von der Öffentlichkeit diskutierten Delikte wie (Kinder-)Pornographie oder Rassendiskriminierung eine untergeordnete Rolle spielen. Viel häufiger sind Hinweise auf betrügerische Aktivitäten oder Verletzungen geistigen Eigentums. In diesen Fällen ist der Entscheid über die Frage der Widerrechtlichkeit eines Inhalts oder einer Handlung noch viel schwieriger und den Hosting-Providern oft nicht zuzumuten. Dieser Entscheid ist nur entsprechend geschulten Behörden oder privaten Rechtsexperten und nur in Zusammenarbeit mit den Rechteinhabern möglich. Die hierfür nötigen Ermittlungs- und Abklärungsarbeiten können einem Provider jedoch kaum sinnvollerweise übertragen werden, auch wenn er über eine eigene Rechtsabteilung verfügen sollte. Die Beurteilung von Straftaten – und darum geht es hier letztlich – ist nicht die Aufgabe eines Hosting-Providers.

[Rz 46] In diesem Zusammenhang ist vertreten worden, dass «sicheres Wissen» nur erlangen kann, wer einen Hinweis aus «zuverlässiger Quelle» erhält[54]. Dieses Argument verkennt die Wirkungsweise von Art. 322bis VE-StGB: Entgegen dem Vorschlag einer Minderheit der Expertenkommission ist das Vorliegen eines Hinweises aus einer zuverlässigen Quelle keine Voraussetzung der Strafbarkeit. Denn Art. 322bis VE-StGB verlangt lediglich ein sicheres Wissen des Providers (bzw. des fraglichen Organs). Das erfordert eine rechtliche Qualifikation des Sachverhalts seitens des Providers und nicht etwa seitens einer Behörde. Sicheres Wissen kann der Provider in diesem Sinne auch ohne jeglichen Hinweis erlangen, etwa wenn er zufälligerweise auf kinderpornographische Inhalte stösst. Liegt ein Hinweis vor, der einen Sachverhalt ausreichend klar und glaubwürdig dargelegt und ist die darin vertretene rechtliche Qualifikation dieses Sachverhalts ebenfalls schlüssig und glaubwürdig, so mag das ebenfalls dazu führen, dass der Provider von einer Straftat ausgeht. Zwingend ist dieser Schluss aber nicht. Richtig ist wohl nur, dass je höher die Zuverlässigkeit der Quelle ist, je eher ein Gericht annehmen wird, dass ein Provider sicheres Wissen hatte – vor allem dann, wenn er selbst nicht in der Lage war, eine juristische Einschätzung vorzunehmen. Wenn jedoch ein Provider über einen eigenen Rechtsdienst mit entsprechendem Know-how verfügt, wird er möglicherweise selbst den Hinweis einer an sich zuverlässigen Quelle kritisch hinterfragen, möglicherweise zu einer anderen Beurteilung kommen und somit nach Art. 322bis VE-StGB mangels direktem Vorsatz nicht mehr strafbar sein.

[Rz 47] Hinzu kommt, dass selbst der Begriff der zuverlässigen Quelle nicht viel weiterhilft. Als zuverlässige Quelle gelten im Allgemeinen die Strafverfolgungsbehörden, die einen Provider im Zuge ihrer Ermittlungen über auf seinem Server befindliche Inhalte aufklären. Sie sind jedoch im Provider-Alltag die Ausnahme. Häufig sind Mitteilungen irgendwelcher Internet-Benutzer oder eigene Kunden, die auf bestimmte, ihnen problematisch erscheinende Inhalte stossen und die Beschwerdestelle des Providers informieren, die aber in vielen Fällen entweder keine klare Beurteilung zulassen (weil Informationen fehlen), nicht von einem Kunden des Providers stammen (und somit ausserhalb seiner Wirkungssphäre liegen) oder klarerweise kein strafrechtlich relevantes Delikt darstellen. Eine weitere Kategorie von Hinweisen stammt von den durch einen Inhalt verletzten Personen bzw. deren Rechtsvertretern, die mit entsprechenden Abmahnschreiben an die Provider gelangen. Letztere pauschal ebenfalls als «zuverlässige Quelle» zu bezeichnen, dürfte sicherlich nicht richtig sein, denn letztlich handelt es sich um die Behauptung einer Partei, die im Rahmen einer Abmahnung (von etwaigen standesrechtlichen Pflichten des Verfassers abgesehen) gegenüber dem Provider weder der Objektivität noch der Vollständigkeit und Wahrheit verpflichtet ist. Es wird wesentlich darauf ankommen, wie qualifiziert der Hinweis bzw. die Anspruchsberechtigung des Dritten dokumentiert ist und wie offensichtlich die strafrechtliche Relevanz der behaupteten Drittrechtsverletzung vor diesem Hintergrund erscheint[55].

[Rz 48] Vor dem Hintergrund all dieser Überlegungen stellt sich somit die Frage, ob das äussert subjektive Element des «sicheren Wissens» tatsächlich ein geeignetes Element zur Anknüpfung einer Sperrpflicht eines Hosting-Providers darstellt. Nach der hier vertretenen Ansicht wäre eine objektive Anknüpfung nicht nur «gerechter», sondern auch praktischer: So könnte das Vorliegen sicheren Wissens beim Provider verzichtet und stattdessen verlangt werden, dass dem Provider eine Mitteilung einer zuständigen Behörde vorliegt, die ihrerseits erklärt, über «sicheren Wissens» bezüglich der Strafbarkeit zu verfügen[56]. So wäre die «heisse Kartoffel» dort, wo sie hingehört: Es käme nicht mehr auf die rechtliche Qualifikation des Providers an, sondern jene einer Behörde, zu deren Aufgabe die vorläufige Beurteilung eines Sachverhalts gehört und deren sie auch wesentlich besser gewachsen ist als ein Provider, dessen Hauptgeschäft der Betrieb einer technischen Infrastruktur ist. Dem Missbrauch wäre dadurch wenigstens teilweise vorgebeugt, dass sich die Behörde schriftlich darauf festlegen müsste, dass im konkreten Fall «sicher» eine Straftat vorliegt, was sie aus Haftungsgründen nur tun wird, wenn sie tatsächlich dieser Überzeugung ist.

[Rz 49] Beachtung verdient schliesslich das Wissen um den Inhalt, mittels welchem eine strafbare Handlung begangen wird. Selbst wenn die juristische Qualifikation der damit begangenen Straftat keine Zweifel offenlässt, setzt die Strafbarkeit des Providers immer auch voraus, dass er um den fraglichen Inhalt und dessen Lokalisierung im konkreten Einzelfall weiss. Hat der Provider viele Inhalte auf seinem System, kann es freilich ein erhebliches praktisches Problem

bereiten, die fraglichen Inhalte zu ermitteln, wenn diesbezüglich keine spezifischen Hinweise vorliegen oder die Inhalte sich verändern oder verschieben. Richtigerweise kann sich eine Strafbarkeit des Providers nach Art. 322bis VE-StGB nur bezüglich eines konkreten, bereits lokalisierten Einzelinhalts ergeben. Das Wissen darum, dass sich ein bestimmter Inhalt irgendwo auf dem System befindet, darf aber nicht genügen. Gesetzgebungstechnisch kann dies über das vorgesehene Kriterium der «Zumutbarkeit» einer Massnahme zur Verhinderung der Nutzung erfasst werden (das «sichere Wissen» bezieht sich auf das Begehen der Straftat), doch lässt der Vorentwurf diesen heiklen Punkt letztlich offen. Sinnvoll wäre daher festzuhalten, dass der Provider nicht nur sicheres Wissen bezüglich der Strafbarkeit hat, sondern auch konkrete Kenntnis der Information im Einzelfall.

[Rz 50] Wie weitgehende Massnahmen einem Hosting-Provider von der Praxis im Ausland bezüglich der Lokalisierung unerlaubter Angebote zugemutet werden, zeigt allerdings ein Entscheid des BGH[57]. Er hatte eine Unterlassungsklage gegen die Betreiberin einer grossen Internet-Auktionsplattform zu beurteilen, über deren Plattform auch gefälschte Rolex-Uhren vertrieben wurden. Der BGH hielt fest, dass es in der Vergangenheit zu mehreren klar erkennbaren Markenverletzungen gekommen sei. Die Betreiberin müsse diese Fälle zum Anlass nehmen, Angebote von Rolex-Uhren einer besonderen Prüfung zu unterziehen, befand der BGH[58]. Eine solche Konsequenz ginge im Falle von Art. 322bis VE-StGB zweifellos zu weit, würde doch durch die Hintertür eine Pflicht des Hosting-Providers zur Überwachung der Inhalte der eigenen Kunden eingeführt. Eine solche trifft den Hosting-Provider aber nicht, wie auch der Bericht zum Vorentwurf explizit festhält[59].

c) Regel 3: Nichtweiterleiten von Hinweisen auf Straftaten eigener Kunden strafbar

[Rz 51] Der Vorentwurf des Bundesrates sieht in Ergänzung zur limitierten Sperrpflicht in Art. 322bis VE-StGB eine Pflicht zur Weiterleitung von Hinweisen auf Straftaten eigener Kunden vor. Der Gedanke hinter dieser Regelung ist, dass jener Provider, der sich nicht mit Hinweisen auseinandersetzen will bzw. solche ignoriert und somit auch bei klarer Rechtslage keinen direkten Vorsatz hat, wenigstens den Strafverfolgungsbehörden die Verfolgung der Straftat ermöglichen soll.

[Rz 52] Was in der Theorie sinnvoll und nachvollziehbar erscheint (jedenfalls sinnvoller als eine von den Providern finanzierte und privat geführte gemeinsame Meldestelle, wie dies teilweise im Ausland vorgesehen ist), ist in der Praxis jedoch untauglich und wird sowohl von Providern als auch von Strafverfolgern abgelehnt. Hauptgrund ist die mangelnde Effektivität und die kontraproduktiven Folgen der Massnahme. Die Pflicht zur Weiterleitung von Hinweisen soll offenbar für sämtliche, bei einem Provider eingehenden Hinweise gelten, gleichgültig ihrer Herkunft, und gleichgültig, welche Art von Straftat sie betreffen[60]. Dies wird zahlenmässig dazu führen, dass die zuständigen Behörden damit rechnen müssen, von Schweizer Providern jeden Tag Hunderte von Hinweisen zu erhalten. Der Bundesrat geht in seinem Begleitbericht selbst davon aus, dass «ein vorsichtiger Hosting-Provider sämtliche eingehenden Hinweise an die Strafverfolgungsbehörden weiterleiten wird»[61]. Gedient ist damit freilich niemandem, schon gar nicht der Bekämpfung der Netzwerkkriminalität: Die Strafverfolgungsbehörden müssten ihre Kapazitäten im Wesentlichen damit vergeuden, aus der Flut der Beschwerden jene wenigen Hinweise herauszufiltern, denen sich in Anbetracht der beschränkten Mittel tatsächlich nachzugehen lohnt und bei denen eine Strafverfolgung in der Schweiz auch tatsächlich möglich ist.

[Rz 53] Wie die praktische Erfahrung der Vergangenheit zeigt, besteht denn auch überhaupt keine Notwendigkeit, die Provider unter Strafandrohung zur Weiterleitung von Hinweisen zu verpflichten. Das Problem der Netzwerkkriminalität besteht nicht darin, dass die Behörden nicht rechtzeitig von Delikten im Internet erfahren – hierzu genügen die bestehenden Kanäle, inklusive der sehr erfolgreich operierenden Koordinationsstelle für Internet-Kriminalität KOBIK, die ein Meldeformular für Online-Hinweise betreibt[62]. Das Problem besteht bei in der Schweiz verübten Delikten darin, bei den (in der Regel kantonalen) zuständigen Stellen über genügend Ressourcen zu verfügen, welche die Hinweise rasch genug auswerten und – in Kooperation mit dem fraglichen Provider – die nötigen Massnahmen zur Sicherung der Beweise und zur Verfolgung der Straftäter einleiten können. An Hinweisen fehlt es nicht, ebensowenig an der Kooperationsbereitschaft der Internet-Provider.

[Rz 54] Hinzu kommt, dass die Weiterleitungspflicht viele Fragen offenlässt. Müssen jegliche Hinweise weitergeleitet werden oder nur solche, die über einen bestimmten Kanal beim Provider eintreffen? Müssen die Hinweise in einem speziellen Format weitergeleitet werden und wer trägt hierfür die Kosten – oder genügt es, alle eingehenden E-Mails unverändert weiterzuleiten? Wem müssen die E-Mails weitergeleitet werden – einer Stelle des Bundes oder aber den

Kantonen, die in den meisten Fällen zuständig sein werden? Müssen alle Hinweise auf irgendwelche möglicherweise strafbaren Inhalte weitergeleitet werden oder nur solche, die in qualifizierter Form auf eine Straftat hinweisen? Muss der Provider die Hinweise auf ihre Plausibilität überprüfen? Antworten darauf gibt es bisher keine.

[Rz 55] Unklar ist auch, wie sich eine Weiterleitungspflicht auf das Verhältnis zum eigenen Kunden auswirken würde, würde die vorgeschlagene Regelung doch den Hosting-Provider faktisch dazu verpflichten, im Falle eines Hinweises durch einen Dritten – auch wenn dieser falsch ist – seine eigenen Kunden bei den Strafverfolgungsbehörden zu «denunzieren».

[Rz 56] Besonders paradox wird die Situation im Falle von konzerninternen Hosting-Providern. Zu denken ist etwa an einen Konzern, der seine Informatik-Aktivitäten an eine eigene Tochtergesellschaft ausgelagert hat, die für eine Konzerngesellschaft eine Website betreibt und damit ein Hosting-Provider wäre[63]. Würde dieses interne Service-Center zum Beispiel das Abmahnschreiben eines Konkurrenten zugesandt erhalten, wonach die Aussagen auf der Website des Konzerns einen (auch strafbaren) Verstoss gegen die Preisbekanntgabeverordnung darstellen, so müsste sich der Konzern quasi selbst «anzeigen». Leitet das Service-Center das Abmahnschreiben des Konkurrenten nicht an die Strafverfolgungsbehörden weiter, könnte es je nach Fortgang des Verfahrens wegen Verstosses gegen Art. 322bis VE-StGB zur Verantwortung gezogen werden. Das wäre eine absurde Situation.

d) Regel 4: Grundsätzlich sind alle strafbaren Handlungen erfasst

[Rz 57] Bei alledem ist zu beachten, dass Art. 322bis VE-StGB nicht zwischen Delikten verschiedener Schwere unterscheidet. Eine Strafbarkeit des Providers soll zwar im Falle von Antragsdelikten ausgeschlossen werden, falls kein Antrag auf Verfolgung der Handlung erfolgt. Diese scheinbare Einschränkung ist jedoch in Wirklichkeit keine: Der Provider wird regelmässig lange vor Ablauf der üblicherweise geltenden Antragsfrist von drei Monaten[64] über eine Sperrung einer Information bzw. Weiterleitung eines Hinweises entscheiden müssen. Wartet er einen etwaigen Antrag ab, wird er strafbar, sollte sich der Verletzte doch noch zu einem Antrag durchringen, weil damit die Voraussetzungen seiner Strafbarkeit rückwirkend erfüllt sind. Eine sinnvolle Beschränkung des für eine Strafbarkeit des Providers in Frage kommenden Deliktskatalogs erscheint daher unumgänglich.

5. Starke Resonanz auf Vorentwurf, weiteres Vorgehen

[Rz 58] Der Vorentwurf hatte eine aussergewöhnlich starke Resonanz: Mit rund 100 Vernehmlassungseingaben lag die Vorlage nur wenig unter der Anzahl Stellungnahmen zum Vorentwurf für eine Revision des allgemeinen Teils des Strafgesetzbuches. Im Grundsatz wurde dabei der Handlungsbedarf bestätigt und eine Sonderregelung der Providerverantwortlichkeit begrüsst. Die Stellungnahmen fielen teilweise sehr unterschiedlich aus. Auch Extrempositionen fehlten nicht: Der Branchenverband «Swiss Interactive Media and Software Association» (SIMSA)[65] verlangte neben der Straflosigkeit der Access-Provider zusätzlich auch eine vollständige Straflosigkeit der Hosting-Provider, da sie wie die Access-Provider eine unabdingbare Funktion beim Austausch von Informationen über elektronische Kommunikationsnetze wahrnehmen würden[66]. Stattdessen wurde vorgeschlagen, Domain-Namen-Registrare (wie z.B. die SWITCH) in die Pflicht zu nehmen[67].

[Rz 59] Zum Zeitpunkt dieses Beitrags waren die Vernehmlassungsergebnisse noch nicht offiziell bekannt. Diverse Vernehmlasser äusserten sich allerdings schon öffentlich oder inoffiziell im Vorfeld zu ihrer Position zum Vorentwurf. Während in der Vernehmlassung zahlreiche Stimmen die Straflosigkeit der Access-Provider begrüssten, wurden die beiden Sonderdelikte für Hosting-Provider deutlich als zu weit gefasst und unpraktikabel kritisiert. Es wurde die Beschränkung auf ausgewählte Straftaten verlangt (z.B. Offizialdelikte), ebenso die Beschränkung auf Fälle, in denen die Strafverfolgungsbehörden einen Provider auf die Strafbarkeit eines Angebots hinweisen. Die Weiterleitungspflicht wurde aus den vorgängig bereits genannten Gründen als kontraproduktiv und angesichts der guten Kooperation zwischen Providern und Strafverfolgungsbehörden auch als unnötig gewertet.

[Rz 60] Eine weitere Hauptkritik richtete sich gegen den Umstand, dass der Bundesrat bewusst von einer Regelung der zivilrechtlichen Verantwortlichkeit von Providern absah und nur einen Vorschlag für eine strafrechtliche Regelung vorbrachte. Der Expertenbericht bestätigte auch in diesem Bereich einen Handlungsbedarf aufgrund einer unklaren Rechtslage[68], auch wenn die Motion «Netzwerkkriminalität» die Prioritäten unstreitig im Bereich des Strafrechts setzte.

[Rz 61] Ob das Gesetzgebungsprojekt für ein Providerstrafrecht nach dem Vorentwurf weiter verfolgt wird und falls ja, in welcher Weise, war zum Zeitpunkt dieses Beitrags noch nicht klar. Ein Entscheid des Bundesrates wird im ersten Halbjahr 2006 erwartet. Wird das Projekt fortgesetzt, wäre mit neuen Regelungen jedoch nicht vor 2009 zu rechnen.

III. Verantwortlichkeit im Zivilrecht

A. Ausgangslage

1. Beseitigungs- und Unterlassungsansprüche dominieren

[Rz 62] Die zivilrechtliche Verantwortlichkeit der Access- und Hosting-Provider ist in der Schweiz bisher weitgehend ungeklärt. Praxis fehlt, und auch in der Lehre wurde diese Fragestellung bisher kaum diskutiert[69]. Die Ursache dafür dürfte zum einen darin liegen, dass die Diskussion um die Verantwortlichkeit von Providern über viele Jahre eine strafrechtliche war. Anlass der Diskussion waren vor allem abstrakte Gefährdungsdelikte, die zwar eine strafrechtliche aber keine zivilrechtliche Seite hatten und sich somit die Frage nach einer zivilrechtlichen Haftung nie stellte.

[Rz 63] Das hat sich inzwischen geändert. Im Internet stellen Verletzungen privater Rechtsgüter den Regelfall dar, wobei die Verletzung von Immaterialgüterrechten, unlauteres Verhalten (z.B. Spamming), Vermögensdelikte (z.B. Betrug, Sabotageakte und Hacking) und die Verletzung von Persönlichkeitsrechten dominieren. Dabei geht es den Verletzten in der Mehrheit der Fälle lediglich darum, eine weitere Verletzung zu unterbinden. Schadenersatzforderungen sind selten. Entsprechend dürfte die Motivation im zivilrechtlichen Vorgehen gegen Provider auch nicht in deren «deep pockets» zur Befriedigung von finanziellen Ausfällen liegen, wie vielleicht vermutet werden könnte, sondern in der Tatsache, dass der Hosting- oder Access-Provider des Verletzers diesem bezüglich der Tat am nächsten steht und über ein Vorgehen gegen seinen Provider der Verletzer am einfachsten zumindest vorläufig «gestoppt» werden kann.

[Rz 64] Die zivilrechtliche Haftung des Providers wird mit anderen Worten primär als Druckmittel für Beseitigungs- und Unterlassungsansprüche ins Feld geführt (inwieweit solche auch gegenüber einem Access-Provider bestehen, sei an dieser Stelle nicht erörtert). Das erklärt auch, warum die Frage der zivilrechtlichen Sorgfaltspflicht eines Providers in der Lehre und Praxis bisher kaum eine nähere Erörterung erfuhr: Geht es um Beseitigungs- und Unterlassungsansprüche, kommt es nicht auf ein Verschulden an, und würde ein Access- oder Hosting-Provider umgehend aktiv, wenn er auf eine bestimmte unerlaubte Handlung eines Kunden aufmerksam gemacht worden ist, wäre das für eine Schadenersatzpflicht erforderliche Verschulden mangels einer Kontroll- und Überwachungspflicht ohnehin nicht nachzuweisen.

[Rz 65] In solchen Fällen stellt sich primär die Frage, welche technisch möglichen und zumutbaren Möglichkeiten ein Access- und Hosting-Provider hat, um eine an sich unbestrittene Rechtsverletzung auch in Zukunft zu verhindern bzw. nicht mehr weiter zu unterstützen. In der Schweiz ist auch diese Frage im Zusammenhang mit zivilrechtlichen Rechtsverletzungen bisher nicht erörtert worden; den Normalfall des Beseitigungsanspruchs – eine bereits bestehende Website mit einzelnen, klar identifizierten Seiten mit rechtswidrigem Inhalt – kann ein Hosting-Provider durch einfaches Löschen der bezeichneten Dateien vom Server bewältigen.

[Rz 66] Weitaus problematischer wird es, wenn sich ein Provider mit einem Unterlassungsanspruch bezüglich eines zukünftigen, noch nicht bestehenden unerlaubten Inhalts konfrontiert sieht. Einen solchen Fall hatte der deutsche Bundesgerichtshof im bereits erwähnten Entscheid «Rolex v. ricardo.de» zu beurteilen. Der BGH kam zum Schluss, dass die Betreiberin eines Online-Marktplatzes Angebote für Rolex-Uhren «einer besonderen Prüfung» zu unterziehen habe, weil es auf ihrer Plattform in der Vergangenheit bereits zu «klar erkennbaren Markenverletzungen» bezüglich solcher Uhren gekommen ist[70]. Welche technischen Möglichkeiten die Betreiberin hierfür hat, war strittig und blieb letztlich offen. Der BGH wies jedoch auf die Möglichkeit einer Software hin, die Verdachtsfälle anhand niedriger Preise und Wörter wie «Nachbildung» oder «Replika» ermitteln könne. Verallgemeinert würde dies bedeuten, dass, wenn erst einmal aufgrund einer konkreten Rechtsverletzung ein Unterlassungsanspruch gegeben ist, sich gestützt darauf, nach Ansicht des BGH, auch eine Pflicht begründen lässt, mit geeigneten Massnahmen, wie etwa ein vorgezogenes Filterverfahren, jede weitere solche Rechtsverletzung zu verhindern.

[Rz 67] Dieser Entscheid des BGH geht klar zu weit, denn in letzter Konsequenz führt er zu genau jener allgemeinen Kontroll- und Überwachungspflicht eines Hosting-Providers, die heute aus Gründen der Zumutbarkeit, Praktikabilität und Kosten rundweg abgelehnt wird. Art. 15 der E-Commerce-Richtlinie hält diesbezüglich für die EU sogar ausdrücklich fest, dass Providern keine allgemeine Verpflichtung auferlegt werden darf, «die von ihnen übermittelten oder gespeicherten Information zu überwachen oder aktiv nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen». Diese Lösung scheint offenbar auch nach Ansicht des Bundesrates eine sachgerechte Lösung zu sein[71]. Zwar enthält die E-Commerce-Richtlinie bezüglich des Haftungsprivilegs für Hosting-Provider einen Vorbehalt im Falle von Unterlassungs- und Beseitigungsansprüchen[72], doch kann sich jener Vorbehalt richtigerweise nur auf einen konkreten, bereits identifizierten Sachverhalt beziehen und nicht auf eine unbestimmte Anzahl von Verletzungen, die lediglich nach ihrer Art bestimmt sind, wie aus dem BGH-Urteil geschlossen werden könnte. Alles andere hätte zur Konsequenz, dass eine Pflicht des Hosting-Providers zur laufenden Überwachung sämtlicher Aktivitäten seiner Kunden gewissermassen durch die Hintertüre wieder eingeführt wird, denn anders liesse sich dem Anspruch des BGH nicht beikommen. Hier besteht eine akute Ausuferungsgefahr auf dem Buckel der Hosting-Provider: Wenn die Betreiberin der Auktionsplattform im vorgängig erwähnten Fall des BGH eine Überwachungspflicht betreffend Rolex-Uhren trifft, lässt sich eine solche letztlich auch für jede andere Marke begründen, von welcher Fälschungen im Umlauf sind. Der gesamte Kontrollaufwand des Providers würde ins Unermessliche steigen, ohne dass dieser unzumutbare Gesamtaufwand dem einzelnen Markeninhaber entgegengehalten werden könnte, weil der jeweilige, die einzelne Marke betreffende Einzelaufwand für sich betrachtet nicht unzumutbar erscheinen mag.

[Rz 68] Vernünftigerweise kann sich daher auch ein Beseitigungs- und Unterlassungsanspruch nur auf einen konkreten Einzelfall einer unerlaubten Handlung beziehen und nicht auf Wiederholungstaten. Schaltet der Verletzer im besagten Online-Marktplatz, dessen Rolex-Angebot von der Betreiberin entfernt worden ist, einen Monat später ein neues Angebot für eine gefälschte Rolex-Uhr auf, so muss richtigerweise verlangt werden, dass der Rechteinhaber hiegegen erneut einschreitet und Beseitigung dieses einen Angebots verlangt. Ein Verstoss gegen einen Unterlassungsanspruch liegt erst dann vor, wenn der Provider ein gesperrtes Angebot wieder entsperrt bzw. die Sperre bezüglich dieses Angebots nicht mehr weiter aufrechterhält. Eine Neubuchung des Angebots durch den Verletzer, selbst mit identischem Inhalt und durch die identische Person, wäre nicht mehr erfasst, zumindest dann nicht, wenn der Provider solche Angebote zunächst automatisiert entgegennimmt.

[Rz 69] Der Umstand, dass Hosting-Provider aus eigenem Antrieb teilweise gewisse Filtermechanismen einsetzen, ändert an der Frage der Zumutbarkeit im Übrigen nichts. Denn letztlich geht es um die Frage der Sorgfaltspflicht eines Hosting-Providers bei der Durchführung seiner Dienstleistung. Deren Verletzung ist es auch, die den Hosting-Provider haften lässt, sollte er im Rahmen der Beseitigung bzw. Verhinderung einer Rechtsverletzung nicht die erforderliche Sorgfalt walten lassen. Ist nun ein Hosting-Provider von sich aus sorgfältiger als es ein vernünftiger Hosting-Provider üblicherweise ist, darf ihm daraus nicht eine weitergehendere, zivilrechtliche Haftung erwachsen. Erforderlich ist auch hier ein objektiver Sorgfaltsmassstab.

2. Gesetzgeberischer Handlungsbedarf?

[Rz 70] Der Bundesrat hat es in seinem Bericht zum Vorentwurf klar abgelehnt, die zivilrechtliche Verantwortlichkeit einer vergleichbaren Regelung wie im Strafrecht zu unterziehen oder sie sonstwie zu klären: Mit einer zivilrechtlichen Haftungsbeschränkung würde das Verhalten von Providern im Zusammenhang mit unerlaubten Angeboten in bisher nicht gekanntem Ausmass «entschuldigt», heisst es im Bericht[73]. Diese Aussage ist verfehlt: Es geht keineswegs um eine Entschuldigung, denn sie würde eine generelle «Schuld» der Provider an Netzwerkdelikten voraussetzen. Dass eine solche nicht gegeben ist, ist unbestritten und mit ein Grund, warum die strafrechtliche Haftung von Access-Providern nicht nur eingeschränkt, sondern vollständig ausgeschlossen wird.

[Rz 71] Wenn mit Verweis auf Rechtsunsicherheit im strafrechtlichen Bereich zu Recht eine entsprechende Klärung der strafrechtlichen Verantwortlichkeit gefordert wird, so gilt dies auch für die zivilrechtliche Verantwortlichkeit. Sie geht in den meisten Fällen Hand in Hand mit der Frage der Strafbarkeit und stellt sich im privatrechtlichen Bereich sogar noch vordringlicher, da eine zivilrechtliche Haftung keinen Vorsatz erfordert und somit häufiger greift. Wenn der Bericht zum Vorentwurf[74] eine zivilrechtliche Haftungsregelung für Provider mit dem Hinweis ablehnt, der Gesetzgeber habe sich anders als im Strafrecht gegen ein Medienzivilrecht ausgesprochen, so ist das nicht korrekt. Das Recht auf Gegendarstellung in Art. 28g ZGB wurde zu eben dem Zweck eingeführt, zivilrechtliche Prozesse im Medienbereich zu

vermeiden. Ähnliche Regelungen sind auch für Provider denkbar und im Ausland bereits Realität[75]. Das Datenschutzrecht enthält genauso Haftungsprivilegien für Medien wie das Urheberrecht[76]. Auch die Haftung von Domain-Namen-Providern hat der Gesetzgeber faktisch bereits beschränkt[77].

[Rz 72] Das andere Argument des Berichts zum Vorentwurf, das Zivilrecht sei weder lückenhaft noch unklar, geht ebenfalls am Ziel vorbei. Das Zivilrecht ist deshalb lückenhaft, weil es zur Verantwortlichkeit von Providern (unbestrittenermassen) keine Ausführungen macht, obwohl solche geboten wären. Weil dem so ist, kommen – wie dies auch im Strafrecht beim Fehlen einer Sonderregelung der Fall ist – die herkömmlichen Regeln über die Gehilfenschaft zur Anwendung. Der Grund für die Notwendigkeit einer Klarstellung im Strafrecht ist derselbe; hier wie dort geht es darum festzuhalten, welches Verhalten von Access- und Hosting-Providern erwartet wird. Wenn der Gesetzgeber mit dem vorliegenden Revisionsentwurf klar zum Ausdruck bringt, dass er diese Frage nicht einzelnen Richtern überlassen will, ist nicht ersichtlich, warum er diese Frage nur für das Strafrecht beantworten sollte, nicht aber für das Zivilrecht bzw. worin der Unterschied liegen soll – die Rechtsunsicherheit besteht in beiden Bereichen in gleicher Weise (im strafrechtlichen Bereich ist das Haftungsrisiko des Providers de lege lata sogar geringer als im zivilrechtlichen Bereich[78]). Dementsprechend wurde die Frage in anderen Rechtsordnungen für beide Bereiche parallel geregelt[79]. Wird im Gegensatz dazu ein Schweigen des hiesigen Gesetzgebers bezüglich einer Haftungssonderregelung für Provider als «qualifiziert» interpretiert (wofür die Materialien bisher sprechen), muss damit gerechnet werden, dass eine Revision, die für eine Haftungsbeschränkung nur im Strafgesetzbuch sorgt, dahingehend interpretiert wird, dass der Gesetzgeber im Bereich der zivilrechtlichen Sorgfaltspflichten der Provider von einem höheren Standard ausgehen möchte als im Strafrecht. Dies kann nicht im Sinne des Gesetzgebers sein.

[Rz 73] Die Problematik liegt somit nicht darin, dass aufgrund der bestehenden gesetzlichen Grundlage eine sachgerechte Verantwortlichkeit von Providern nicht möglich wäre. Es wäre auch auf Basis des bestehenden schweizerischen Zivil- wie auch Strafrechts durchaus möglich gewesen, die Verantwortlichkeit von Access-Providern für ihre Durchleitung von Daten auszuschliessen[80]. Es wäre aufgrund der bestehenden Gesetzeslage ebenso möglich gewesen, die Haftung von Hosting-Providern durch Auslegung der entsprechenden Gesetzesbestimmungen dahingehend einzuschränken, dass diese nur im Falle vorausgehender, konkreter und qualifizierter Hinweise eintreten kann[81]. Doch die konkret geführte Diskussion dieser Themen hat aufgrund der Internet-Euphorie von Anfang an am erforderlichen Realitätsbezug gelitten und drängte den Provider allzu rasch in die Rolle des Sündenbocks und Richters in einer Person. Erst dies hat zu einer Rechtsunsicherheit geführt, die zum Teil durch wenig vorausschauende Urteile im In- und Ausland noch verstärkt worden ist.

[Rz 74] Wie wichtig Rechtssicherheit für Internet-Provider ist, hat der Gesetzgeber im Bereich der Domain-Namen, wo eine ähnliche Diskussion ebenfalls stattgefunden hatte, bereits erkannt und bestätigt: Die Adressierungselementeverordnung[82] hält heute ausdrücklich fest, dass die Betreiberin des Domain-Namen-Registers nicht überprüfen muss, ob ein bei ihr angemeldeter Domain-Name Markenrechte verletzt (Art. 14f Abs. 2 AEFV). Damit ist nicht nur ihre strafrechtliche, sondern auch ihre zivilrechtliche Haftung im Fall einer Registrierung eines Markenrechte verletzenden Domain-Namens ausgeschlossen. Der Verletzte hat sich an den Domain-Namen-Inhaber zu wenden.

[Rz 75] Eine solche, über den vom Vorentwurf adressierten strafrechtlichen Bereich hinaus gehende Rechtssicherheit gilt es nun auch für Provider von anderen Dienstleistungen als Domain-Namen herzustellen. Zumindest aber sollte auf die eine oder andere Weise klarzustellen, dass für Provider im Bereich des Zivilrechts zweifellos keine strengeren Sorgfaltspflichten bestehen als im Strafrecht. Dass es bisher zu keinen relevanten Praxisentscheiden über die zivilrechtliche Verantwortlichkeit von Access- und Hosting-Providern gekommen ist und daher der Leidensdruck auf allen Seiten nicht sehr gross erscheinen mag, steht zu dieser Forderung nicht im Widerspruch. Ist es doch die Rechtsunsicherheit, welche einerseits Verletzte dazu bewegt, an sich berechtigte Ansprüche gegenüber Providern nicht durchzusetzen und andererseits Provider dazu veranlasst, Druckversuchen von tatsächlich oder vermeintlich verletzten Personen zum Nachteil ihrer Kundschaft nachzugeben, ohne dass dazu eine Rechtspflicht bestünde. Solche Auswirkungen einer Rechtsunsicherheit können zweifellos nicht im Sinne des Gesetzgebers sein. Seine Aufgabe ist es, möglichst klare Verhaltensrichtlinien und Verantwortlichkeiten zu definieren. Bei Lichte betrachtet ist der Handlungsbedarf im Strafrecht denn auch nicht markant anders zu beurteilen als im Zivilrecht. Ein Provider wird die Folgen einer zivilrechtlichen Verantwortlichkeit für eine unerlaubte Handlung jedenfalls kaum als weniger schwerwiegend betrachten als die strafrechtlichen, die letztlich (vorwiegend) einzelne Verantwortliche treffen[83]. Ganz im Gegenteil: Nicht nur die Höhe etwaiger finanzieller Verbindlichkeiten, sondern auch die Wahrscheinlichkeit deren Eintritts ist aufgrund des im Zivilrecht fehlenden Vorsatzerfordernisses höher.

B. Voraussetzung der Haftung für Schadenersatz

[Rz 76] Die nachfolgenden Ausführungen behandeln einige ausgewählte Aspekte der zivilrechtlichen Haftung eines Access- oder Hosting-Providers. Wie schon im heute geltenden Strafrecht bestehen die grössten Unsicherheiten im Bereich der Verantwortlichkeit von Access-Providern. Folgende Darstellung soll den hiesigen Stand der Verantwortlichkeit von Internet-Providern im Vergleich verdeutlichen:

Providertyp	OR 41	StGB	VE-StGB
Access (für Nutzer)	?	?	x
Access (für Verletzer)	?	?	x
Hosting (für Verletzer)	✓✓✓	✓✓	✓

[Rz 77] Soll ein Provider für einen durch ein rechtswidriges Angebot im Internet entstandenen Schaden haften, liefert regelmässig Art. 41 OR die entsprechende Anspruchsgrundlage (allenfalls in Verbindung mit entsprechenden Spezialgesetzen, wie das Urheberrechtsgesetz). Die «Providerhaftung» ist somit eine Verschuldenshaftung, die nach den klassischen Voraussetzungen (Schaden, Kausalzusammenhang, Widerrechtlichkeit, Verschulden) beurteilt wird.

[Rz 78] Immer wieder diskutiert wird die Frage, ob sich ein Access- oder Hosting-Provider einer Verantwortlichkeit als Gehilfe durch positives Tun (im Sinne einer fortgesetzten Bereitstellung seiner Infrastruktur) aussetzt (wie hier vertreten) oder aber eine Unterlassungstat begeht, indem er gegen bestimmte Aktivitäten nicht einschreitet[84]. Diese Frage soll an dieser Stelle nicht weiter erörtert werden, da sie primär dogmatischer Natur ist und in der Regel keine Auswirkungen auf das Ergebnis der Beurteilung der Verantwortlichkeit des Providers hat. Entscheidend ist letztlich in beiden Fällen der Sorgfaltsmassstab, nach welchem das Verhalten eines Providers beurteilt wird[85]. In technischer Hinsicht ist darauf hinzuweisen, dass sich die Dienstleistung eines Providers allerdings nicht darin erschöpft, zu Beginn der Vertragsbeziehung mit dem Kunden eine Handlung vorzunehmen (z.B. Bereitstellung von Speicherplatz für eine Website, Bereitstellen einer Einwählnummer), sondern laufende Aktivitäten erforderlich sind, um seine Dienstleistung aufrecht zu erhalten[86].

1. Widerrechtlichkeit

[Rz 79] Das Kriterium der Widerrechtlichkeit eines bestimmten Verhaltens bereitet im Zusammenhang mit der Beurteilung der zivilrechtlichen Verantwortlichkeit eines Acccess- und Hosting-Providers für einen Fremdinhalt in der Regel keine Schwierigkeiten. Ein schädigendes Verhalten ist widerrechtlich, wenn gegen eine Norm verstossen wird, welche ein absolutes Recht des Geschädigten schützt (so genanntes Erfolgsunrecht) oder wenn eine besondere Schutznorm verletzt wird, deren Zweck im Schutz von Schäden der eingetretenen Art besteht (so genanntes Verhaltensunrecht)[87]. Relevante Verhaltensnormen finden sich in der gesamten Rechtsordnung, einschliesslich des Strafrechts[88].

[Rz 80] Im Bereich der Provider-Haftung ergibt sich die Widerrechtlichkeit in den klassischen Fällen der Verletzung von geistigem Eigentum, der Persönlichkeitsverletzungen, des unlauteren Wettbewerbs oder der Vermögensdelikte (wie Betrug) aus den einschlägigen Schutznormen der entsprechenden Spezialgesetze (wie das Urheberrechtsgesetz[89], das Markenschutzgesetz[90], das Bundesgesetz gegen den unlauteren Wettbewerb[91] oder das Datenschutzgesetz[92]), dem Persönlichkeitsschutz gemäss Art. 28 ff. ZGB und dem Strafgesetzbuch, insbesondere dem Vermögensstrafrecht (z.B. Art. 146 StGB) (wobei nachfolgend zusammenfassend jeweils immer nur von einer «unerlaubten Handlung» die Rede sein wird, die ein Verletzer bzw. Schädiger begeht).

[Rz 81] In einzelnen Fällen sind Schwierigkeiten in der Herleitung einer Widerrechtlichkeit natürlich denkbar. Sie können sich im Bereich des Geistigen Eigentums zum Beispiel dort ergeben, wo die Monopolrechte eines Rechteinhabers durch die entsprechenden Gesetze beschränkt werden oder vertragliche Grenzen bestehen, so etwa im Fall von Downloads raubkopierter Inhalte aus dem Internet (im Rahmen von Art. 19 Abs. 1 URG zulässig) oder im Fall der Verwendung urheberrechtlich geschützter Werke, die durch das Zitatrecht (Art. 25 URG) geschützt werden.

[Rz 82] Hinzuweisen ist ferner darauf, dass nach bundesgerichtlicher Rechtsprechung im Fall einer Konstruktion einer (unechten) Unterlassungstat eine Verletzung allein des Gefahrensatzes, sollten die Aktivitäten eines Internet-Providers überhaupt als Schaffung einer Gefahrenquelle qualifiziert werden, für sich noch keine Rechtswidrigkeit begründet[93]; es muss auch eine entsprechende Schutznorm bzw. ein absolutes Recht verletzt werden.

[Rz 83] Als besondere Schutznorm erscheint, de lege ferenda, auch der vom Bundesrat in seinem Vorentwurf vorgeschlagene Art. 322bis VE-StGB, der den Provider bei «sicherem Wissen» zur Verhinderung eines strafbaren Internet-Angebots bzw. zur Weiterleitung von Hinweisen an die Behörden verpflichtet. Aus heutiger Sicht dürfte diese Schutznorm für zivilrechtliche Schadenersatzansprüche jedoch von beschränkter praktischer Relevanz sein[94]: Zur Annahme der Rechtswidrigkeit durch Nichtverhinderung eines strafbaren Internet-Angebots gestützt auf einen solchen Art. 322bis VE-StGB müsste auch das subjektive Tatbestandselement des «sicheren Wissens» erfüllt sein, was eine Haftung für fahrlässiges Verhalten faktisch ausschliesst. Diese Hürde wird ein Geschädigter bei der Durchsetzung von Schadenersatzansprüchen allerdings in jenen Fällen umgehen können, indem sich eine Ersatzpflicht des Providers bereits aus der Teilnahme des Providers an der unerlaubten Handlung des Kunden des Providers ergibt, denn der in Art. 27 VE-StGB vorgeschlagene Ausschluss der Regeln der Teilnahme im Falle eines Hosting-Providers gilt für das Zivilrecht nicht[95].

2. Verschulden

[Rz 84] In den meisten Fällen wird sich die Schadenshaftung des Providers für rechtswidrige Internet-Inhalte an der Frage des Verschuldens des Providers entscheiden. Dies ist auch im Strafrecht so[96]. Die Erleichterung für den Geschädigten im Zivilrecht besteht darin, dass fahrlässiges Verhalten genügt[97]. Die zivilrechtliche Haftung kann somit erheblich weiter gehen als die strafrechtliche.

[Rz 85] Verschulden setzt voraus, dass der Schädiger – hier also der Provider – die mögliche Verursachung einer Schädigung eines Dritten durch sein Verhalten erkennt oder erkennen kann[98]. Umstritten ist, ob der Schädiger neben der Möglichkeit des Schadens auch die Rechtswidrigkeit des herbeigeführten Erfolges bzw. seines Verhaltens voraussehen können muss[99]. Dies wird dort von entscheidender Bedeutung sein, wo ein Provider die Rechtswidrigkeit der Verwendung eines Internet-Inhalts weder aus dem Inhalt selbst noch den ihm vorliegenden Informationen mit der erforderlichen Gewissheit erkennen kann. Dies kann zum Beispiel der Fall sein, wenn ein Dritter behauptet, der Inhalt einer Website oder die Tätigkeit eines Kunden des Providers verletze seine Urheberrechte.

[Rz 86] In der bisherigen strafrechtlichen Praxis zur Verantwortlichkeit von Hosting-Providern[100] gingen die Gerichte aufgrund der Fakten jeweils von einem vorsätzlichen Handeln des Providers aus: Es konnte nach Überzeugung der Richter nachgewiesen werden, dass sie wussten, worum es ging und zumindest in Kauf nahmen, dass ihr Handeln – das Bereithalten der rechtswidrigen Inhalte – eine Ursache für den Erfolg setzen würde. Ist ein Bewusstsein der Rechtswidrigkeit nicht erforderlich und entfällt somit auch das Element der Missbilligung[101], ist – leider – abzusehen, dass (auch) die Zivilgerichte in Fällen klarer, dem Provider bekannter Rechtsverletzungen mit absehbarer Schadensfolge durch seine eigenen Kunden von vorsätzlichem Handeln ausgehen werden.

[Rz 87] Dies ist deshalb nicht sachgerecht, weil ein kommerzieller Provider ungeachtet der Polemik der öffentlichen Diskussion um deren Haftung in aller Regel nicht will, dass durch sein Verhalten einem Dritten Schaden entsteht, weil er damit letztlich gegen seine eigenen kommerziellen Interessen handelt: Zwar wird immer wieder ins Feld geführt, ein Hosting-Provider, der rechtswidrige fremde Inhalte bereithält, verdiene an diesen Inhalten, sei deshalb an ihnen interessiert und nehme damit letztlich auch den durch sie verursachten Schadenin Kauf. Diese Argumentation verkennt aber, dass ein kommerzieller Hosting-Provider im heutigen, hart umkämpften Markt angesichts tiefer Margen nur dann profitiert, wenn ihm sein Kunde keine besonderen Umstände verursacht und seine Kundschaft grundsätzlich auch keine unerlaubten Angebote betreibt. Ein kommerzieller Provider wird die Umtriebe, die ihm durch rechtswidrige Angebote eines

seiner Kunden immer entstehen werden, diesem Verursacher in der Praxis aus praktischen Gründen so gut wie nie überwälzen können. Überdies schaden rechtswidrige Angebote dem Ruf des Providers, was sich wiederum negativ auf seine Konkurrenzfähigkeit und Attraktivität ausübt. Das ist denn auch der Grund, warum heute gerade grössere Hosting-Provider Geldbeträge in die freiwillige Bekämpfung von unerlaubten Angeboten, die die potentiellen Einnahmen aus der Unterstützung solcher Angebote bei weitem übersteigen[102].

[Rz 88] Daraus ergibt sich, dass nur unter aussergewöhnlichen Umständen angenommen werden, dass ein kommerziell tätiger Provider die Schädigung eines Dritten durch sein fortgesetztes Zurverfügungstellen seiner Infrastruktur bzw. Nichteinschreiten tatsächlich will und somit vorsätzlich handelt.

[Rz 89] Handelt der Provider nicht vorsätzlich, stellt sich als nächstes die Frage, ob zumindest Fahrlässigkeit vorliegt. Eine solche liegt vor, wenn der Provider die rechtswidrige Schädigung durch die Verletzung einer Sorgfaltspflicht verursacht hat, der Provider es also an der unter den gegebenen Umständen erforderlichen Sorgfalt hat mangeln lassen[103].

[Rz 90] Im Zusammenhang mit der Begründung der Fahrlässigkeit eines Access- wie auch Hosting-Providers wird häufig mit dem Gefahrensatz argumentiert[104]: Es wird vertreten, dass der Provider durch sein Tun – zum Beispiel das Bereitstellen eines Internet-Zugangs oder von Speicherplatz für eine Website – einen gefährlichen Zustand geschaffen hat und er deshalb die nötigen Schutzmassnahmen treffen muss – zum Beispiel die Sperrung bestimmter Inhalte – damit sich die geschaffene Gefahr nicht verwirklicht. Tut er dies nicht, verletzt er seine Sorgfaltspflicht und handelt schuldhaft[105].

[Rz 91] Diese Begründung ist abzulehnen, denn sie geht davon aus, dass die Tätigkeit eines Access- oder Hosting-Providers an sich bereits eine gefährliche Situation schafft, indem aus der Tatsache des Erfolgseintritts auf das Vorbestehen einer Gefahrenquelle geschlossen wird. Dies aber verkennt die Realität: Die Access- und Hosting-Dienstleistungen von kommerziellen Internet-Providern sind genausowenig eine Gefahrenquelle wie das Bereitstellen eines Telefonanschlusses oder das Vermieten eines Schaufensters oder Ladenlokals[106]: Es sind vollkommen alltägliche, gesellschaftlich akzeptierte und erwünschte, rechtlich zulässige und tatunspezifische Dienstleistungen, bei denen ein Missbrauch für unzulässige Zwecke zwar nicht ausgeschlossen werden kann (und in diesem Fall auch ohne bewusste Mitwirkung des Providers möglich ist[107]), die aber (heute) in der weitaus überwiegenden Mehrheit der Fälle rechtmässig eingesetzt werden[108].

[Rz 92] Auch wenn der Gefahrensatz mangels Gefährlichkeit des Access- und Hosting-Providings in aller Regel nicht zur Begründung einer Sorgfaltspflichtverletzung eines Providers herangezogen werden kann, bleibt eine solche selbstverständlich möglich. Der Gefahrensatz ist lediglich eine von mehreren Methoden, um eine Sorgfaltspflichtverletzung zu begründen.

[Rz 93] Konkret wird sich daher die Frage stellen, ob eine Schädigung nach der «branchenüblichen» Sorgfalt vorauszusehen und zu verhindern gewesen wäre. Dabei wird vorliegend aufgrund der Praxiserfahrung davon ausgegangen, dass hierzulande kommerzielle Access- und Hosting-Provider üblicherweise gewissenhaft handeln, ihre Dienstleistung grundsätzlich nicht gefährlich ist und von ihnen keine juristische, sondern primär eine technische und wirtschaftliche Expertise erwartet wird oder erwartet werden kann[109]. Hinzuweisen ist in diesem Zusammenhang allerdings darauf, dass im Fall einer juristischen Person bzw. einer Kollektivgesellschaft ein schuldhaftes Verhalten vorliegt, wenn eines ihrer Organe bzw. ein Gesellschafter schuldhaft gehandelt hat[110]. Da ungeachtet eines objektivierten Fahrlässigkeitsbegriffs auch die Erfahrung einer Person berücksichtigt werden muss[111], kann sich das gerade für grössere Provider mit juristischem Know-how negativ auswirken. Dies darf allerdings nicht dazu führen, dass einem Provider, der zur Erkennung und Verhinderung rechtswidriger Angebote freiwillig mehr unternimmt als erforderlich wäre, eben diese Vorsichtsmassnahmen zum Vorwurf gemacht werden[112].

[Rz 94] Welche Sorgfalt von einem Access- oder Hosting-Provider verlangt werden kann, ist in der Schweiz bisher nicht gerichtlich geklärt. Zudem ist nur wenig dazu publiziert worden, und manches, das publiziert worden ist, ist praxisfern, unverhältnismässig und nach wie vor von der falschen Vorstellung geprägt, die Dienstleistungen eines Internet-Providers stelle grundsätzlich eine Gefahr dar. Da die Frage der Sorgfaltspflicht regelmässig die für eine Haftung eines Internet-Providers entscheidende Frage ist, wirkt diese Rechtsunsicherheit entsprechend schwer.

[Rz 95] Eine generelle Kontrollpflicht des Providers, also die Pflicht, von sich aus nach möglichen Schädigungen zu forschen – selbst stichprobenweise – ist rundweg abzulehnen. Dies ist einerseits die Folge der Erkenntnis, dass ein solches Forschen uferlos, unpraktikabel, die Dienstleistungen verteuert und somit weder zumutbar noch verhältnismässig ist[113] (selbst wenn dies mit der raschen Entwicklung der Technik und Leistungsfähigkeit der Computersysteme technisch zusehends einfacher wird[114]), andererseits die Konsequenz der Tatsache, dass die Dienstleistungen eines Access- oder Hosting-Providers nicht per se als gefährlich betrachtet werden können. Daran ändert auch die Tatsache, dass Missbräuche solcher Dienstleistung vorkommen können und in der Vergangenheit möglicherweise schon vorgekommen sind, nichts. In der hiesigen Literatur wird denn auch für den zivilrechtlichen Bereich eine präventive Kontrollpflicht selbst beim Hosting-Provider abgelehnt, wenn auch mit verständlichen, aber nicht immer sachgerechten Einschränkungen[115].

[Rz 96] In der Praxis stellt sich die Frage der Sorgfaltspflicht regelmässig (erst) dann, wenn der Provider einen externen Hinweis auf eine mögliche Schädigung erhält, sei es durch unbeteiligte Dritte, sei es durch einen behördlichen Hinweis, sei es durch eine Abmahnung mit oder ohne Unterlassungserklärung. Anders als im Strafrecht wird dem Provider in einem solchen Fall ein bewusstes Wegschauen nichts nütze. Umgekehrt darf von einem Provider, der freiwillig Massnahmen ergriffen hat, um unerlaubte Handlungen im Kreise seiner Kunden selbst zu erkennen (bzw. zu verhindern)[116], nicht ein höheres Mass an Sorgfalt abverlangt werden[117]. Er würde für sein überdurchschnittliches Verhalten bestraft; überdies würde dies den Grundsatz eines objektivierten Verschuldensbegriffs zuwiderlaufen. Solche freiwilligen Massnahmen dürfen auch nicht ohne weiteres als Eingeständnis dafür gewertet werden, dass weniger weitgehende Massnahmen im Sinne der Sorgfaltspflicht nicht genügt hätten[118]; eine solche Tendenz ist in der Diskussion freilich zu beobachten.

[Rz 97] Auch im Falle von «externen» Hinweisen ist zu differenzieren, und viele werden letztlich – wenigstens im Sinne der branchenüblichen Sorgfaltspflicht – zu keinen weiteren Schritten führen. Einen durchschnittlich grossen, kommerziellen Provider können jeden Tat zahlreiche Hinweise auf mögliche oder angebliche unerlaubte Handlungen erreichen (die keineswegs nicht nur Handlungen seiner eigenen Kunden betreffen müssen, sondern sich auf irgendwelche Delikte im Internet beziehen können, einschliesslich der Zustellung von E-Mails mit unerlaubtem Inhalt). Einerseits kann ein Provider schon aufgrund der Menge und oftmals geringen Qualität nicht allen Hinweisen nachgehen, zumal sein Geschäftszweck nicht das Überprüfen von Hinweisen ist, andererseits kann er selbst dort, wo er aufgrund eines Hinweises erkennen konnte, dass sein Verhalten zu einer rechtswidrigen Schädigung beitragen kann, unterschiedlich reagieren. Die Sperrung eines bestimmten Angebots oder eines Internet-Zugangs ist nur eine von mehreren Möglichkeiten. Im Einzelfall mag beispielsweise bereits eine Ermahnung des eigenen Kunden angemessen sein. Selbst die Nichtbeachtung eines klaren Hinweises muss keine Unsorgfalt begründen, wenn der Provider etwa aufgrund früherer Erfahrungen oder der Umstände des Falles darauf vertrauen darf, dass die vom Hinweisgeber befürchtete Schädigung nicht eintreten wird.

[Rz 98] Wie in solchen Fällen üblich, sind pauschale Rezepte nicht möglich. Wesentlich ist zunächst die Herkunft, Art und Qualität des Hinweises. Ist ein Hinweis auf eine rechtswidrige Aktivität eines seiner Kunden zu ungenau, kann diese zwar zu einem Schaden führen, doch kann dem Provider daraus kein Vorwurf gemacht werden, weil ihm die zur Beurteilung des Falls und für ein Einschreiten erforderlichen Angaben fehlten. Der folgende Fragenkatalog kann für die Beurteilung eines Hinweises unter dem Aspekt der «branchenüblichen» Sorgfaltspflicht Anhaltspunkte liefern.

- Stammt der Hinweis von einer Behörde oder einer geschädigten oder sonstwie berechtigten Person oder deren Vertreter? Im Fall von Hinweisen unbeteiligter Dritter wird normalerweise davon ausgegangen, dass diese nicht als Hinweise einer zuverlässigen, ernst zu nehmenden Quelle gelten und deren Nichtbeachtung durch einen Provider somit auch keine Sorgfaltspflichtverletzung begründet[119]. Dies gilt insbesondere auch für anonyme Hinweise.

- Ist der Hinweis substanziiert und glaubhaft? Selbst wenn eine berechtigte Person darauf hinweist, dass ein bestimmter Sachverhalt sie schädigt oder schädigen wird, kann von einem Provider nur dann ein Handeln erwartet werden, wenn dieser Hinweis über die nötigen Details und Belege verfügt, welche die Verletzung nicht nur hinreichend konkretisiert, sondern auch glaubhaft macht und zwar sowohl für einen in Rechtsfragen erfahrenen als auch unerfahrenen Provider. Nicht genügend ist eine blosse, unbelegte Behauptung, wenn sich deren Glaubhaftigkeit nicht bereits aus dem entsprechenden Angebot ergibt (wie dies im Strafrecht z.B. bei einem klar kinderpornographischen Inhalt der Fall wäre). Im Fall einer Markenverletzung würde dies beispielsweise die Beilage entsprechender Registerauszüge erfordern.

- Bezieht sich der Hinweis auf einen konkreten, nachgewiesenen und aktuellen Einzelfall? Ein Provider kann, wenn überhaupt, nur gegen aktuelle, ihm konkret bekannte, unerlaubte Handlungen bzw. Angebote einschreiten. Wenn – wie eingangs erwähnt – die IFPI einen Access-Provider darüber informiert, dass ein bestimmter Kunde in der Vergangenheit angeblich Raubkopien im Internet angeboten hat, dann darf das für den Access-Provider keine Konsequenzen haben: Die einzigen behaupteten, konkreten Taten liegen in der Vergangenheit und dauern nicht mehr an. Die Wahrscheinlichkeit, dass ein bestimmter Kunde auch in Zukunft wieder Raubkopien im Internet anbieten wird, genügt nicht, dass ein Provider dessen Zugang sperren muss. Es kann vom Provider nicht erwartet werden, dass er auf den allgemeinen Hinweis einer berechtigten Person hin bei gewissen seiner Kunden deren Verhalten im Internet überwacht und es gegebenenfalls unterbindet. Selbst im Strafrecht besteht die Möglichkeit einer Überwachung nur unter sehr restriktiven Bedingungen und nur im Falle bestimmter, schwerer Straftaten[120]. Der Hinweis muss somit derart konkret und aktuell sein, dass der Provider den fraglichen Inhalt sofort auffinden bzw. eine gegenwärtig noch anhaltende Aktivität (z.B. ein laufender Sabotageangriff) sofort erkennen und unterbinden kann. Im Fall einer Internet-Seite wäre hierzu beispielsweise die Angabe deren genauen Adresse und im Fall eines unerlaubten Angebots auf einer Online-Auktionsplattform deren vom System zugewiesene Identifikationsnummer. Ändert sich diese Nummer oder die Adresse, weil der Schädiger seinen Inhalt bzw. sein Angebot entfernt und später neu plaziert, ist normalerweise ein neuer Hinweis erforderlich. Liegt also eine unerlaubte Handlung in der Vergangenheit, wird ein Hosting- oder Access-Provider bei Wiederholung der Tat in der Regel auch dann kein Verschulden treffen, wenn er auf die vergangene Handlung aufmerksam gemacht worden ist.

- Ist die geltend gemachte Rechtsverletzung offenkundig? Ungeachtet der umstrittenen Frage, inwieweit das Verschulden die Frage der Rechtswidrigkeit einschliesst, scheidet eine Sorgfaltspflichtverletzung eines Providers richtigerweise aus, wenn die behauptete Rechtsverletzung nicht offenkundig ist[121]. Offenkundig muss sie wiederum sowohl für den juristischen Laien als auch den Fachmann sein. Letzteres ist deswegen wichtig, weil ein juristischer Laie ein bestimmtes Internet-Angebot als offenkundig unzulässig erachten mag, ein Fachmann dieses aber aufgrund seines umfassenderen Wissens um die Rechtslage vertretbarerweise als zulässig erachten kann. Zu beachten ist auch, dass es die Rechtsverletzung ist, die im konkreten Fall offenkundig sein muss. Ein Hinweis ist somit ungenügend, wenn er darlegt, dass eine bestimmte Handlung gegenwärtig stattfindet oder konkret und aktuell droht. Der Hinweis muss auch zeigen, warum die Handlung offenkundig eine Verletzung geltenden Rechts darstellt. Dies verlangt keine ausführliche Darlegung der rechtlichen Argumente, wohl aber allgemeinverständliche, auch für den juristischen Laien nachvollziehbare Ausführungen, weshalb die geltend gemachte Schädigung geltendes, anwendbares Recht verletzt und daher eine unerlaubte Handlung darstellt[122]. Es kann von einem Provider, der in der Regel keinen näheren Bezug zur Streitsache hat und deren Hintergründe auch nicht kennt, nicht verlangt werden, entsprechende Recherchen und rechtliche Abklärungen zu treffen. Dies wäre bei der Vielzahl der Hinweise, die ein Provider regelmässig erhält, unzumutbar und unpraktikabel.

  Von einem Provider kann letztlich nur erwartet werden, dort ohne richterliche Anweisung tätig zu werden, wo es sich um eine offenkundig unerlaubte Handlung handelt und ihm der Hinweisgeber die für diese Erkenntnis nötigen Angaben geliefert hat. Weder kann vom Provider verlangt werden, dass er selbst forscht, noch dass er im Zweifelsfall gegen seine eigenen Kunden und für einen Dritten entscheiden muss, welcher eine ihn schädigende Handlung behauptet, aber nicht darlegen kann, warum diese rechtswidrig sein soll.

[Rz 99] Dieser Fragenkatalog ist nicht dahingehend zu verstehen, dass ein Provider sämtliche Hinweise bezüglich sämtlicher aufgeführter Kriterien überprüfen muss. Stammt der Hinweis beispielsweise nicht aus einer qualifizierten Quelle oder ist er schon auf den ersten Blick zu wenig konkret, braucht er ihm nicht weiter nachzugehen. Tut er es allerdings doch und erhärtet sich im Laufe seiner Nachforschungen der Vorwurf, kann er die so gewonnenen Erkenntnisse unter Umständen nicht mehr ignorieren: Haben seine eigenen, freiwilligen Nachforschungen in einem solchen Fall die schlechte Qualität des Hinweises wettgemacht, kann dies – falls der Provider seine Erkenntnisse in der Folge keine angemessenen Massnahmen ergreift – ein Verschulden begründen, das nicht bestanden hätte, wenn der Hinweis ignoriert worden wäre. An das Wissen des Providers im Falle von Eigenrecherchen und «Zufallsfunden» ist freilich derselbe Standard anzusetzen wie im Falle eines externen Hinweises: So kommt eine Sorgfaltspflichtverletzung auch bei selbst entdeckten unerlaubten Handlungen nur im Falle einer offenkundigen Rechtsverletzung und nur bezüglich des dem Provider konkret bekannten Einzelfalls in Frage. Erfährt der Access-Provider zufälligerweise, dass ein Kunde seinen Internet-Zugang benutzt hat, um unerlaubterweise einen Inhalt von einer Website herunterzuladen, so handelt er selbstverständlich nicht unsorgfältig, wenn er den Internet-Zugang dieses Kunden nicht sperrt. Es wäre von ihm auch im Falle eines Hinweises nicht erwartet worden.

[Rz 100] Erfüllt ein Hinweis (bzw. das Ergebnis einer Eigenrecherche) die genannten Kriterien, wertet ein Provider einen Hinweis auf eine aktuelle oder bevorstehende Schädigung als berechtigt und hält er dementsprechend die beschriebene Entwicklung für möglich, stellt sich – wie bereits dargelegt – die Frage, auf welche Weise der Provider reagieren soll, damit ihn kein Verschulden trifft. Auch hier kommt es selbstverständlich auf die Umstände an. Folgende Fragen verdeutlichen dies:

- Wie hoch ist das Gefährdungs- bzw. Schädigungspotenzial? Zunächst bestimmen Art und Qualität des Hinweises, welches Gefährdungs- und Schädigungspotenzial der Provider aus den dargelegten Umständen erkennen kann. Dieses wird wiederum die erforderliche Reaktion des Providers bestimmen. So ist in der Lehre anerkannt, dass sorgfältiges Handeln nicht bedeutet, dass jede Verletzung eines Rechtsguts vermieden werden muss. Es sind die Verhältnisse im Einzelfall zu berücksichtigen[123]. Ist die Wahrscheinlichkeit einer Gefährdung gering, kann es durchaus vertretbar sein, auf einen entsprechenden Hinweis nicht zu reagieren oder den betreffenden Kunden über den ihn betreffenden Hinweis in Kenntnis zu setzen[124] bzw. ihn zu ermahnen. Die Erfahrungen im Zusammenhang mit früheren bzw. ähnlichen Fällen des betroffenen Providers oder anderer Provider sind hierbei ebenfalls zu berücksichtigen.

  Eine wesentliche Rolle bei der Prüfung eines Hinweises und ebenso bei dessen Beachtung spielt ferner die Art und Schwere der Rechtsgutsverletzung, auf welche ein Provider aufmerksam gemacht wird. Wirft ein Hinweisgeber einem Kunden des Providers vor, dessen private Website verbreite seit Wochen ehrverletzende Aussagen über ihn im Internet, ist das Schädigungspotenzial zweifellos geringer als im Fall der Website eines Kunden des Providers, über welche dieser seit kurzem einen schwunghaften, gewerbsmässigen Handel mit raubkopierter Software betreibt. Im ersteren Fall darf vermutet werden, dass die private, unbekannte Website nur sehr gering frequentiert ist. Zudem dauert die Verletzung schon seit einiger Zeit an, und es kann ihr – falls die Äusserungen tatsächlich ehrverletzend sind – durch eine Richtigstellung entgegengetreten werden. Im Fall der raubkopierten Software droht finanzieller Schaden nicht nur durch deren Bezug über die Website, sondern auch durch deren Weiterverbreitung an anderen Stellen im Internet. Zudem verfügen die Schädiger in solchen Fällen erfahrungsgemäss nicht über die Mittel, um den verursachten Schaden wiedergutzumachen, soweit dieser sich überhaupt ermitteln lässt. Daher wird die Sorgfaltspflicht eines Providers hier ein rascheres, umfassendes Einschreiten verlangen.

- Wird das Fernmeldegeheimnis oder der Datenschutz tangiert? Die Dienstleistungen eines Access- oder Hosting-Providers werden regelmässig nicht nur vom Datenschutzgesetz erfasst, sondern unterliegen[125] ebenso dem Fernmeldegeheimnis[126]. Zwar gilt das Fernmeldegeheimnis nicht unbedingt gegenüber dem Provider selbst, doch hat der Gesetzgeber mit dieser Bestimmung zum Ausdruck gebracht, dass der Inhalt privater Fernmeldekommunikation (im Gegensatz zum Inhalt einer von jedermann öffentlich abrufbaren Website) nicht der Überwachung durch den Provider unterliegen soll, es sei denn, dies ist zur Erbringung seiner Dienstleistung (z.B. im Rahmen eines Virenfilters) nötig oder gesetzlich vorgesehen (z.B. im Rahmen der behördlichen Überwachung des Fernmeldeverkehrs[127]).

  Gleiches ergibt sich aus dem Datenschutzgesetz, nach welchem der Provider nur dann in die private Kommunikation seiner Kunden eingreifen darf, wenn sich dies durch ein überwiegendes öffentliches oder privates Interesse oder aufgrund gesetzlicher Vorschriften rechtfertigt (oder dies mit den Kunden vereinbart wurde). Aus diesem Grund handelt ein Access-Provider grundsätzlich nicht unsorgfältig, wenn er sich weigert, im privaten Kommunikationsverkehr seiner Kunden (wozu auch der Zugriff des Kunden des Access-Providers auf eine Website zählt) nach bestimmten unerlaubten Aktivitäten zu forschen und diese gegebenenfalls auch zu sperren.

- Unterliegt der Provider einer Leistungspflicht? Normalerweise wird ein Internet-Provider die fortgesetzte Unterstützung einer Rechtsverletzung nicht dadurch rechtfertigen können, vertraglich zur Erbringung dieser Leistung verpflichtet gewesen zu sein. Umgekehrt wird den Provider nicht nur gegenüber einem durch ihn möglicherweise Geschädigten eine Sorgfaltspflicht treffen, sondern auch gegenüber seinem eigenen Kunden, gegen welchen er Massnahmen ergreifen soll. Zwar kann sich ein Provider den dafür nötigen rechtlichen Spielraum durch Ausgestaltung seiner Vertragsbedingungen schaffen, was auch regelmässig getan wird. Dies

ändert jedoch nichts an den berechtigten Interessen seines Kunden, dass ihm sein Provider weiterhin die vereinbarten Leistungen erbringt. Ein vernünftig handelnder Provider wird daher aufgrund der ihm zur Verfügung stehenden Informationen versuchen, eine Lösung zu finden, die beiden Interessen – jener des angeblich Geschädigten und jener seines Kunden und angeblichen Schädigers – angemessen Rechnung trägt.

Eine solche Abwägung der Interessen bedeutet keine Abkehr von einem objektivierten Fahrlässigkeitsbegriff, da hier nicht die subjektive Entschuldbarkeit des Providers zur Diskussion steht, sondern ein Interessensgegensatz Dritter, dessen tatsächliche Berechtigung der Provider typischerweise nicht abschliessend beurteilen kann (und soll) – es steht unter Umständen die Aussage des Hinweisgebers gegenüber der Aussage des angeblichen Schädigers und Kunden des Providers. In dieser Situation kann es von Bedeutung sein, ob der Provider dem angeblichen Schädiger lediglich einen «Gratis»-Service zukommen lässt und der Schädiger damit rechnen muss, dass dieser jederzeit beendet wird oder aber, ob der Provider für den angeblichen Schädiger eine komplexe und teure E-Commerce-Lösung betreibt, auf dessen Verfügbarkeit sein Kunde vertraut und grundsätzlich auch vertrauen darf. Verhält sich ein Provider im letzteren Fall gegenüber Vorwürfen einer rechtswidrigen Schädigung als Ergebnis einer Interessensabwägung sehr viel zurückhaltender beim Ergreifen etwaiger Massnahmen als gegenüber einem Benutzer einer Gratisdienstleistung, handelt er nicht fahrlässig.

Ähnliches gilt auch dort, wo ein Provider einem Kontrahierungszwang unterliegt. Im noch geltenden Fernmelderecht unterliegen Internet-Provider als solche noch keinem Kontrahierungszwang. Inskünftig ist dies allerdings denkbar[128]. Für einen Access- und Hosting-Provider kann sich auch aus einer allfälligen Marktbeherrschung ein Kontrahierungszwang ergeben[129]. Zwar kann ein Provider auch im Falle eines Kontrohierungszwangs Kunden ablehnen, die seine Dienstleistungen für unerlaubte Handlungen nutzen. Sein Spielraum ist jedoch deutlich enger, was sich entsprechend auf seine Sorgfaltspflichten auswirkt.

- Wer ist der Schädiger und wie reagiert dieser auf die Vorwürfe? Die Person des (angeblichen) Schädigers spielt nicht nur für die Glaubwürdigkeit des Hinweises eine Rolle, sie ist auch bezüglich der Prognose des Providers relevant, wie wahrscheinlich sich eine bestimmte Schädigung einstellen wird bzw. welche Massnahmen ein Provider ergreifen muss.

  Handelt es sich beim angeblichen Schädiger zum Beispiel um ein dem Provider bekanntes, an sich «rechtschaffenes» Unternehmen, verhält sich der Provider nicht unsorgfältig, wenn er seinen Kunden zunächst anspricht und ihm Zeit zur Reaktion gewährt. Kontert dieser Kunde auf den Hinweis und legt auf ebenso glaubwürdige Weise dar, dass die angebliche Rechtsverletzung bzw. Schädigung nicht besteht, wird sich der Provider nicht schuldhaft verhalten, wenn er diesen Kunden weiterhin versorgt und den Hinweisgeber auf den Rechtsweg verweist. Mit anderen Worten: Verliert der Hinweis eines Dritten aufgrund neuer Erkenntnisse seine Glaubwürdigkeit, handelt der Provider nicht fahrlässig, wenn er diesem nicht mehr Folge leistet.

  Handelt es sich beim angeblichen Schädiger jedoch um eine Person, die die Dienstleistungen des Providers als anonymer Kunde nutzt, wird es insbesondere vom Gefährdungs- und Schadenspotenzial abhängen, ob der Provider auf den glaubwürdigen Hinweis hin vorsorglich eingreifen und beispielsweise einen Inhalt sperren muss oder ob Zeit bleibt, dem angeblichen Schädiger zumindest eine kurze Frist zur Stellungnahme zu gewähren.

- Was sind die Auswirkungen eines Eingreifens? Es gibt für einen Provider verschiedene technische Möglichkeiten, ein bestimmtes Internet-Angebot bzw. eine bestimmte Handlung im Internet zu unterbinden. Sie wirken mehr oder weniger breit und sind mehr oder weniger zuverlässig. Grundsätzlich hat der Provider nur, aber immerhin eine der Situation angemessene Massnahme einzusetzen. Ist eine bestimmte Seite einer Website vom Server des Providers zu entfernen, genügt es nicht, lediglich entsprechende Links auf die Seite zu löschen, sofern die Seite weiterhin direkt angewählt werden kann oder im Verzeichnislisting erscheint. Umgekehrt wäre es unverhältnismässig und durch die Sorgfaltspflicht des Providers letztlich nicht zu begründen, wenn statt der einzelnen Seite die gesamte Website nicht mehr abrufbar wäre.

  Solche Diskussionen wurden vor allem im Zusammenhang mit der Sperrung bestimmter Internet-Angebote durch Access-Provider diskutiert. Zwar haben sich die diesbezüglichen Mechanismen etwas weiterentwickelt, doch stellt sich – ohne dies hier weiter erörtern zu können[130] – nach wie vor das Problem, dass eine Sperrung unerlaubter Angebote auch zur Blockierung legitimer Angebote und anderen Nebenwirkungen führen kann. Hier wird wiederum eine Interessensabwägung erforderlich sein und zwar einerseits unter Berücksichtigung der Interessen

der Anbieter und Benutzer der legitimen Dienstleistungen und andererseits mit Blick auf die Wirksamkeit der Sperr- und Blockiermassnahmen. Dabei stehen nicht die Möglichkeiten zur Umgehung dieser Massnahmen im Vordergrund[131], sondern der Umstand, dass solche Sperren typischerweise laufend geändert werden müssen, um die entsprechend veränderten Angebote weiterhin zu erfassen. Erscheint eine Massnahme aus solchen Gründen als nicht wirkungsvoll, kann einem Provider, unter dem Titel des Verschuldens keinen Vorwurf gemacht werden, wenn er sie nicht einsetzt.

[Rz 101] Zusammengefasst bedeutet dies, dass ein Access Provider in aller Regel auch dann keine Sorgfaltspflichtverletzung begeht, wenn er auf einen konkreten und glaubhaften Hinweis hin den Zugang seiner Kunden zu einem bestimmten Internet-Angebot nicht sperrt. Hingegen wird in der Regel ein für eine Schadenersatzhaftung hinreichendes Verschulden eines Hosting-Providers vorliegen, wenn der Provider trotz eines konkreten und glaubhaften Hinweises aus qualifizierter Quelle, trotz einer offenkundigen Rechtsverletzung und trotz eines im Vergleich zu den Interessen des Kunden des Providers überwiegenden Gefährdungs- und Schädigungspotenzials den öffentlichen Zugriff auf einen bestimmten, auf der Infrastruktur des Providers bereitgehaltenen Inhalts (nach angemessenen Abklärungen, allenfalls auch nachdem dem Kunden eine Möglichkeit zur Stellungnahme gewährt wurde) nicht sperrt, obwohl ihm dies möglich und zumutbar war.

3. Teilnahme, Kausalzusammenhang

[Rz 102] Ein Provider wird in der Mehrheit der Fälle zwar nur in untergeordneter Funktion an einer bestimmten Schädigungshandlung mitwirken und nimmt dadurch – nach der hier vertretenen Ansicht – in der Regel die Rolle eines Gehilfen ein[132]. Durch Einbezug des Gehilfen in Art. 50 Abs. 1 OR hat der Gesetzgeber allerdings verdeutlicht, dass der Provider auch für seine blosse mittelbare Verursachung eines Erfolgs und Schadens einer unerlaubten Handlung schadenersatzpflichtig sein soll. Die für den Geschädigten entscheidende Frage ist somit, in welchem Umfang er den Provider beanspruchen kann.

[Rz 103] Hierzu wird in Art. 50 Abs. 1 OR festgehalten, dass solidarische Haftung gegenüber dem Geschädigten entsteht, wenn mehrere einen Schaden gemeinsam verschulden, sei es als Anstifter, Urheber oder Gehilfen. Ungeachtet des deutschen Wortlauts der Bestimmung, setzt Solidarität nach Art. 50 Abs. 1 OR nicht nur ein gemeinsames Verschulden sondern auch eine gemeinsame Verursachung voraus[133].

[Rz 104] Bei einem Hosting-Provider wird in der Praxis unbestritten sein, dass er durch das Bereithalten der Inhalte des Schädigers an den Erfolg bzw. Schaden einen Kausalbeitrag leistet. Daran ändert sich auch dann nichts, wenn mehrere Hosting-Provider parallel tätig sind. Umstrittener ist die Frage eines Kausalbeitrags bezüglich Access-Provider[134]: Wird davon ausgegangen, dass auch sie adäquat kausal zum Erfolg bzw. zur Schadensverursachung beitragen (mindestens im Sinne einer Teilursache), kann der Kreis der gemeinsamen – und damit der potenziell solidarisch haftenden – Verursacher auch auf sämtliche Access-Provider ausgedehnt werden[135]. Ist ein Angebot im Internet erst einmal öffentlich abrufbar, bietet systembedingt grundsätzlich jeder Access-Provider seinen Kunden einen Zugang hierzu an und kann so zum Mitverursacher des Erfolgs bzw. Schadens werden.

[Rz 105] Die zweite Voraussetzung von Art. 50 Abs. 1 OR, das gemeinsame Verschulden, setzt keine Absprache zwischen dem Provider und dem Schädiger voraus; es genügt, wenn sich der Provider seines Zusammenwirkens mit dem Schädiger und dessen pflichtwidrigen Verhaltens bewusst ist oder sein konnte[136]. Im Verhältnis zwischen Provider und hauptverantwortlichem Schädiger wird das gemeinsame Verschulden regelmässig vorliegen, vorausgesetzt natürlich, den Provider trifft überhaupt ein Verschulden: Es ist kaum vorstellbar, dass sich ein Hosting- oder Access-Provider, der von einem konkreten, rechtswidrigen Inhalt Kenntnis hat, nicht auch seines Zusammenwirkens mit dem hauptverantwortlichen Schädiger bewusst ist oder es ihm bewusst sein konnte. Damit aber haftet dieser Provider mit dem Schädiger solidarisch für den gesamten Schaden.

[Rz 106] Somit braucht die Frage der Anwendbarkeit von Art. 51 Abs. 1 OR (unechte Solidarität[137]) zur Begründung der Solidarität zwischen dem hauptverantwortlichen Schädiger und einem Provider als seinem Gehilfen auf ein solches Verhältnis nicht geprüft zu werden. Die Frage stellt sich allenfalls dann, wenn ein und derselbe Schädiger bezüglich desselben unerlaubten Inhalts mit mehreren verschiedenen Hosting-Providern zusammenwirkt, die voneinander jedoch nichts wissen. In einem solchen Fall wäre es unbillig, wenn der eine, schuldhaft handelnde Hosting-Provider nicht nur für den durch seine Mitwirkung entstandenen Schaden solidarisch mit dem hauptverantwortlichen Schädiger haften müsste,

sondern gleich auch für jenen Schaden, der durch die Mitwirkung der anderen Hosting-Provider entstanden ist (der sich freilich unter Umständen nicht auseinanderhalten lässt). Die Lösung liegt in solchen Fällen allerdings nicht in der Annahme einer unechten Solidarität unter den Hosting-Providern (unecht deshalb, weil sie im Verhältnis untereinander kein gemeinsames Verschulden trifft), sondern in der Annahme unterschiedlicher Schäden (Art. 51 OR gilt nur dort, wo eine Haftung mehrerer für «denselben» Schaden zur Diskussion steht).

[Rz 107] Etwas problematischer wird es, wenn nicht nur der Kausalbeitrag eines Hosting-Providers, sondern auch jener eines Access-Providers als rechtlich relevante (Teil-)Ursache eines Erfolgs bzw. Schadens betrachtet wird. Dies führt regelmässig zu einer Vielzahl von Beteiligten, die als Teilverursacher im Verhältnis zum Geschädigten grundsätzlich immer für den ganzen Schaden haften[138]. Dies würde bedeuten, dass sich ein Geschädigter nicht mehr an den hauptverantwortlichen Schädiger und auch nicht mehr an dessen Hosting-Provider halten müsste, sondern praktisch einen beliebigen der unzähligen Access-Provider im Markt belangen könnte, sofern dieser Zugang zum fraglichen, unerlaubten Angebot bietet und ihn auch ein Verschulden trifft. Dieser würde als Teilverursacher solidarisch für den gesamten Schaden haften.

[Rz 108] Das erscheint, angesichts des äusserst geringen Kausalbeitrags eines einzelnen Access-Providers, kein sachgerechtes Ergebnis. In der Lehre ist denn auch in anderem Zusammenhang erkannt worden, dass sich das Prinzip der Solidarhaftung bei Schadensverursachungen durch eine unbestimmte, grosse Zahl von Handelnden nicht aufrechterhalten lässt[139]. Anders als etwa im Fall der Teilnahme an einer Demonstration, bei welcher aus Billigkeitsgründen jeder Teilnehmer für jeden Schaden haftet, stellt die Beteiligung einzelner Access-Provider keine irgendwie geartete «psychische Mitverursachung»[140] dar, mit welcher eine Solidarhaftung begründet werden kann. Die Mitwirkung von Access-Providern am weltweiten Internet ist mit der Mitwirkung eines Demonstranten an einer Demonstration jedenfalls nicht zu vergleichen.

[Rz 109] Auch hierfür gibt es vernünftige Lösungsansätze. In der Literatur wurde vorgeschlagen, die Mitwirkung eines Access-Providers als Fall einer blossen Begünstigung eines Erfolgs einer unerlaubten Handlung nach Art. 50 Abs. 3 OR zu qualifizieren[141]. Dies wäre dann gegeben, wenn gezeigt werden kann, dass der Access-Provider durch seine Aktivität einen bereits eingetretenen Erfolg lediglich perpetuiert, der Access-Provider also erst nach vollendeter Tat auftritt. In diesem Fall haftet der Access-Provider zwar ebenfalls aber nur dann und nur soweit, als durch seine eigene Beteiligung ein Schaden verursacht worden ist. Diesen Nachweis zu erbringen, wird freilich sehr schwer sein, selbst beim Vorliegen von Logbüchern, die die Quelle der Zugriffe[142] auf einen bestimmten Inhalt dokumentieren (worüber typischerweise bestenfalls der fragliche Hosting-Provider, kaum aber der Access-Provider verfügt). In der Praxis dürfte Art. 50 Abs. 3 OR allerdings kaum zur Anwendung kommen: Entweder ist die Mitwirkung eines Access-Providers nötig, dass ein Erfolg überhaupt eintreten kann (z.B. indem die Möglichkeit zur Kenntnisnahme eines rufschädigenden Inhalts überhaupt erst geschaffen wird), oder aber die fragliche Tat erschöpft sich nicht in einer einmaligen Handlung, sondern stellt einen «Dauerdelikt» dar.

[Rz 110] Denkbar ist auch die Anwendung von in der Kausalitätslehre in anderem, aber vergleichbaren Zusammenhang bereits diskutierten Lösungsansätzen, wie beispielsweise eine Aufteilung der Haftung nach Marktanteilen[143] oder eine nach der realen Beteiligung abgestufte Haftung[144]. Es stellt sich jedoch die grundlegendere Frage, ob die Handlung eines Access-Providers überhaupt noch als adäquater Kausalbeitrag zu berücksichtigen ist. Nach der hier vertretenen Ansicht ist dies nicht der Fall: Zwar kann nicht in Abrede gestellt werden, dass ohne Access-Provider niemand Zugang zu rechtswidrigen Inhalten im Internet erlangen kann und somit dort, wo die tatsächliche oder mögliche Kenntnisnahme eine Voraussetzung für den Taterfolg ist, grundsätzlich natürliche Kausalität besteht. Stellt sich jedoch die Frage, ob ein Internet-Zugang, den ein bestimmter Access-Provider dem Publikum (aber nicht dem Schädiger) zur Verfügung stellt, den Eintritt des Erfolgs wesentlich begünstigt, wie dies zur Annahme der Adäquanz erforderlich ist[145], muss dies verneint werden: Der Access-Provider stellt lediglich eine alltägliche, harmlose Infrastruktur zur Verfügung.

[Rz 111] Der Access-Provider ist zu vergleichen mit einer Telefongesellschaft, die selbst dann, wenn sie nebst all den anderen, von ihren Kunden getätigten Anrufen auch Anrufe an Rufnummern im Netz einer anderen Telefongesellschaft weiterverbindet, die für rechtswidrige Angebote genutzt werden, dieser Kausalbeitrag aber nicht über die erforderliche Adäquanz verfügt. Der Fall des Access-Providers ist auch vergleichbar mit dem des Betreibers eines öffentlichen Verkehrsnetzes, das vom Publikum auch dazu benutzt werden kann, eine Ausstellung rechtswidriger Inhalte zu besuchen.

Auch hier käme niemand auf die Idee, den betreffenden Verkehrsbetrieb als adäquat kausale Mitursache für den Taterfolg der Ausstellungsbetreiber zu betrachten, selbst wenn unzweifelhaft ist, dass ein Teil des Publikums die Ausstellung ohne öffentliche Verkehrsverbindungen nicht besucht hätte.

[Rz 112] Würde der Kausalbeitrag eines Access-Providers, der dem Publikum einen Internet-Zugang verschafft, als adäquat und damit rechtlich relevant betrachtet werden, müsste dies folgerichtig auch für eine ganze Reihe weiterer Provider gelten. Der Access-Provider begünstigt den Eintritt des Erfolges nicht mehr oder weniger, als jene Fernmeldedienstanbieter, die dem fraglichen Access-Provider die Datenleitungen und Infrastruktur auf der «letzten Meile» zur Verfügung stellen, damit dieser seinen Internet-Zugangsdienst erbringen bzw. seine Kunden mit den Zugangssystemen des Access-Providers Kontakt aufnehmen können. Der einzige Unterschied besteht darin, dass nur der Access-Provider nach Aussen in Erscheinung tritt und nur der Access-Provider von den genannten Fernmeldedienstanbietern den Zugriffsversuch eines Kunden auf ein bestimmtes Angebot erkennen und auch sperren kann. Die Betrachtung lässt sich auch auf die dem Access-Provider nachgelagerten, oft zahlreichen, weiteren Internet-Provider ausdehnen, also auf die Betreiber der «Überlandstrecken»[146] und «Knotenpunkte»[147] im Internet, die den Zugang auf bestimmte Angebote theoretisch ebenfalls sperren könnten. Dabei wird klar, dass sich der Kausalbeitrag eines Access-Providers von den Kausalbeiträgen all dieser anderen Provider im Grunde nicht unterscheidet und deshalb auch nicht einzusehen ist, warum derjenige eines Access-Providers adäquat sein soll, diejenigen aller anderen Provider jedoch unbestrittenermassen nicht.

[Rz 113] Zusammenfassend ergibt dies, dass ein Access-Provider, der lediglich dem Publikum einen Zugang ins Internet anbietet, zivilrechtlich schon deshalb für rechtswidrige Angebote im Internet nicht haftet, weil sein Kausalbeitrag zum Taterfolg bzw. Schaden nicht die erforderliche Adäquanz aufweist. Anders ist es hingegen beim Hosting-Provider: Dieser wird, soweit die anderen Voraussetzungen, insbesondere das Verschulden, gegeben sind, solidarisch für den gesamten Schaden haften, den das von ihm bereitgehaltene, rechtswidrige Angebot des hauptverantwortlichen Schädigers (d.h. seines Kunden) verursacht.

[Rz 114] Insbesondere für einen Hosting-Provider kann somit ein schadenträchtiges, rechtswidriges Angebot eines Kunden ein erhebliches, wirtschaftliches Risiko darstellen. Ein vom Geschädigten in Anspruch genommener Provider mag zwar gestützt auf einen Vertrag mit dem hauptverantwortlichen Schädiger (wo vorhanden) oder kraft Gesetz auf diesen Regress nehmen, doch wird erfahrungsgemäss der Schädiger selten über das erforderliche Haftungssubstrat verfügen oder aber aus rechtlichen und praktischen Gründen überhaupt nicht zu belangen sein, wofür bereits sprechen wird, dass der Geschädigte nicht ihn, sondern den Provider belangt hat. Dem Provider wird es überdies ohne Unterstützung des Schädigers regelmässig nicht leicht fallen, einen Prozess hinsichtlich Tatsachen, die nicht sein eigenes Verhalten als Provider betreffen, zu führen.

IV. Fazit

[Rz 115] Ist die Internet-Provider-Haftung ein Sonderfall? Die Antwort darauf fällt nicht schwer: Sie ist es leider. Dies liegt nicht daran, dass die bestehenden, allgemeinen Bestimmungen des Straf- und Zivilrechts keine sachgerechten Lösungen bezüglich der Verantwortlichkeit der verschiedenen Kategorien von Internet-Providern zulassen würden. Sie tun es und zwar auch im Bereich des Zivilrechts, wie vorstehend aufgezeigt.

[Rz 116] Der Sonderfall der Provider-Haftung besteht darin, dass der Internet-Provider in der öffentlichen Diskussion, in der Praxis, in der Lehre und teilweise auch vom Gesetzgeber zum Sonderfall gemacht wurde. Die Internet-Provider-Haftung ist ein politisches Thema geworden, und es herrscht eine allgemeine Tendenz, den Internet-Provider unter dem Vorwand der straf- und zivilrechtlichen Verantwortlichkeit zu einem Sündenbock und Richter wider Willen zu machen: Sündenbock deshalb, weil die Haftung des Providers regelmässig damit begründet wird, dass sich die «wahren» Täter wegen der Internationalität, der vermeintlichen Anonymität und der Offenheit des Internets nicht fassen lassen und daher auf die Provider ausgewichen werden muss[148]. Richter deshalb, weil jeweils der betreffende Hosting-Provider selbst beurteilen soll, ob ein angeblich unerlaubter Inhalt es tatsächlich ist und der betreffende Hosting-Provider im Fall einer ungerechtfertigt unterlassenen Sperrung damit rechnen muss, straf- und/oder zivilrechtlich zur Verantwortung gezogen zu werden.

[Rz 117] Nun mag man einwenden, dass das Tätigwerden in jeder Branche gewisse Haftungsrisiken mit sich bringt. Das ist zwar richtig, verkennt aber eine Besonderheit im Zusammenhang mit der hier diskutierten Internet-Provider-Haftung: Bei dieser handelt es sich nicht, wie etwa bei der Arzt- oder Anwaltshaftung, um die Verantwortlichkeit für eine korrekte,

sorgfältige Erbringung derjenigen Leistungen, die die Kunden eines Providers von ihm erwarten und für die sie ihn bezahlen. Es handelt sich auch nicht um eine Haftung des Providers für ein von ihm erwecktes Vertrauen. Statt dessen handelt es sich um die Haftung des Internet-Providers gegenüber beliebigen Dritten, mit welchen der fragliche Access- oder Hosting-Provider keinerlei Beziehung unterhält und auch nicht unterhalten will.

[Rz 118] Die Erkenntnis, dass ein Provider in der Tat eine völlig alltägliche und grundsätzlich harmlose technische Dienstleistung erbringt und daher seine Haftung für im Internet begangene Delikte die absolute Ausnahme sein muss und die Sorgfaltspflichten eines Providers dementsprechend zurückhaltend zu definieren sind, setzt sich erst allmählich durch. Bis dies endgültig der Fall ist, wird sowohl im Straf- als auch im Zivilrecht eine unnötige Rechtsunsicherheit bestehen. Im Strafrecht scheint sie allgemein anerkannt zu sein, ebenso der gesetzgeberische Handlungsbedarf; im Zivilrecht betrifft die Rechtsunsicherheit vor allem die Frage der Sorgfaltspflicht und der Rahmen, in welchem Umfang gegen einen Provider Unterlassungsansprüche möglich sein sollen – der «Rolex v. Ricardo.de»-Entscheid des BGH hat hier jedenfalls die falschen Zeichen gesetzt.

[Rz 119] Diese Rechtsunsicherheit stellt nicht nur ein unnötiges Risiko für die einzelnen Provider dar. Sie birgt auch ein Missbrauchspotenzial: je grösser die Rechtsunsicherheit ist, desto besser kann das Haftungs-Risiko eines Providers dazu benutzt werden, diesen unter Druck zu setzen. Dies wird heute von (privaten) Dritten ausgenutzt, um missliebige Inhalte anderer im Internet zu unterbinden, auch wenn diese möglicherweise zulässig sind und der Provider für diese möglicherweise gar nicht verantwortlich ist. Ist das Risiko einer Haftung nicht abwegig, richtet sich die Forderung nicht gegen einen wichtigen Kunden und birgt sie auch keine Ausuferungsgefahr, wird ein kommerziell denkender Hosting-Provider – wie die praktische Erfahrung zeigt – dem auf ihn von einem angeblich Verletzten ausgeübten Druck nicht selten nachgeben und sich damit Ärger ersparen. So gesehen, nutzt Rechtssicherheit in diesem Bereich keineswegs nur den Providern sondern auch ihren Kunden und ganz generell den Internet-Nutzern.

[Rz 120] Rechtssicherheit für Internet-Provider zu schaffen bedeutet denn auch nicht nur Enthaftung. Sie ist zweifellos eine wichtige Komponente einer Sonderregelung und in Fällen, wie dem Access-Provider (des Publikums), auch ohne Vorbehalt angezeigt. Sie kann überdies bei anderen Kategorien von Providern unter Umständen auch als positiven Anreiz für erwünschte Verhaltensweisen eingesetzt werden (anstatt, wie im Vorentwurf für ein Providerstrafrecht, mit Strafdrohungen zu arbeiten).

[Rz 121] Eine Sonderregelung bietet jedoch auch die Chance, neben der Allokation von Verantwortlichkeiten spezifische Verfahren zu schaffen, mit denen sich Haftungsfälle von vorneweg vermeiden lassen. Ein Beispiel einer solchen Alternative zu einem gerichtlichen Vorgehen ist das Gegendarstellungsrecht nach Art. 28g ZGB. Auch im Bereich von Internet-Delikten sind spezielle Verfahren denkbar, die den Interessen aller Beteiligter – Verletzter, Verletzer und Provider – besser dienen können als eine spezifische Regelung nur der Haftpflicht. Wichtig ist jedoch, dass solche Verfahren dafür sorgen, dass der Provider primär als neutraler Dritter auftritt und die Auseinandersetzung zwischen dem angeblich Verletzten und dem angeblichen Verletzer direkt und nicht über den Provider ausgefochten wird. Letzterer sollte nicht eine Rolle oder eine Verantwortung übernehmen müssen, für die er als «blosser» Betreiber einer technischen Infrastruktur an sich nicht geschaffen ist.

1 Zum Begriff siehe hinten Rz 11.

2 David Rosenthal, Bundespolizei bekämpft Rassismus im Internet, Ein Schnellschuss sorgt für Kopfschütteln, in: NZZ, 31. Juli 1998, Nr. 175, S. 78.

3 Abrufbar unter http://seegras.discordia.ch/Essays/BUPO-Brief.txt und http://normative.zusammenhaenge.at/faelle/ch/bupo-webzensur.html.

4 David Rosenthal, Kooperation statt Konfrontation, Gesinnungswandel bei der Bundespolizei, in: NZZ, 14. August 1998, Nr. 186, S. 57.

5 Zwar konnte die IFPI die Internet-Adressen (so genannte IP-Adressen) der fraglichen Personen aufzeichnen, nicht jedoch deren Identität eruieren. Die IP-Adressen geben jedoch an, welchen Provider diese Personen benutzen, um ins Internet zu gelangen. Der Provider kann anhand dieser Angaben wiederum den Kunden ermitteln.

6 Musterschreiben sind abrufbar unter www.netzpolitik.org/2005/briefe-der-ifpi-schweiz-an-die-provider.

7 Philip Wegmüller, Kriminalisierte Kunden, in: Facts 01/2006.

8 Siehe hinten Rz 101.

9 Der Fall «Compuserve». Zu weiteren Infos siehe etwa www.digital-law.net/somm; das Urteil des Landgerichts München I vom 17. November 1999 ist abrufbar unter www.netlaw.de/urteile/lgm_12.htm.

10 Tom Standage, Das Viktorianische Internet, St. Gallen/Zürich, 1999, S. 118. So wurden gemäss dieser Quelle damals Vorschriften eingeführt, welche die telegraphische Übermittlung von Ergebnissen von Pferderennen untersagten, weil Betrüger auf diese Weise versucht hatten, der konventionellen Übermittlung der Rennergebnisse an die Buchmacher zuvorzukommen. Nach der Einführung dieser Vorschriften setzten die Betrüger stattdessen Geheimcodes ein, um die damaligen «Internet-Provider», die Telegraphisten in den Telegraphenämter, zu täuschen.

11 Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt.

12 Art. 12 ECRL.

13 Art. 14 ECRL.

14 Art. 15 ECRL.

15 Motion 00.3714 von Ständerat Thomas Pfisterer: «1. Der Bundesrat wird eingeladen, zum Schutz des Internet im Interesse von Bevölkerung und Wirtschaft in erster priorität rasch eine rechtssichere, praktikable, international möglichst harmonisierte Regelung im Strafrecht, eventuall in einzelnen weiteren Bestimmungen zu beantragen. 2. Er soll nötigenfalls unerlässliche weitere Rechtsänderungen beantragen (spätere Priorität).»

16 Bericht der Expertenkommission «Netzwerkkriminalität», Bern 2003/2004 («Expertenbericht»).

17 Der Vorentwurf des Bundesrates und der erläuternde Bericht vom Oktober 2004 sowie die Medienmitteilung sind abrufbar unter www.ejpd.admin.ch/ejpd/de/home/dokumentation/mi/2004/2004-12-10.html und www.ejpd.admin.ch/ejpd/de/home/themen/kriminalitaet/ref_gesetzgebung/ref_netzwerkkriminalitaet.html.

18 Siehe hinten Rz 27 und Rz 29.

19 Vgl. die Übersicht im Expertenbericht, S. 59 ff., sowie, statt vieler, Grace Schild Trappe, Strafrechtliche Verantwortlichkeit der Internet Service Provider (ISP), in: Jusletter 6. November 2000, und Marcel A. Niggli/Chrisitan Schwarzenegger, Strafbare Handlungen im Internet, in: SJZ 98 (2002), S. 61-73.

20 Gutachten des Bundesamts für Justiz vom 24. Dezember 1998, VPB 64.75.

21 Positionspapier des Bundesamts für Polizei vom 15. Mai 2000.

22 Vgl. hierzu David Rosenthal, Sollen Provider für illegale Inhalte haften? Positionspapier der Bundespolizei wirft Fragen auf, in: NZZ, 19. Mai 2000, Nr. 116, S. 80.

23 Marcel A. Niggli/Franz Riklin/Günter Stratenwerth, Die strafrechtliche Verantwortlichkeit von Internet-Providern, Ein Gutachten zuhanden des Verbands Inside Telecom (VIT) vom 2. Oktober 2000 («VIT-Gutachten»), abgedruckt in: Medialex Sonderausgabe, Bern 2000.

24 Vgl. etwa Christian Schwarzenegger, Der räumliche Geltungsbereich des Strafrechts im Internet, in: ZStrR 118 (2000), 109 ff.

25 Vgl. etwa Maximilian Dornseif, Government mandated blocking of foreign Web content, in: In: Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.) Security, E-Learning, E-Services: Proceedings of the 17. DFN-Arbeitstagung über Kommunikationsnetze, Düsseldorf 2003, ISBN 3-88579-373-3.

26 Siehe hinten Rz 119.

27 Vgl. die Diskussion um Sperrverfügungen der Bezirksregierung Düsseldorf vom Februar 2002, so etwa unter www.ccc.de/censorship/, www.david-gegen-goliath.org/Materialsammlung.pdf, www.heise.de/newsticker/meldung/35483 sowie www.brd.nrw.de/BezRegDdorf/hierarchie/themen/Sicherheit_und_Ordnung/Medienmissbrauch/index.php.

28 VIT-Gutachten, S. 23 f.

29 Womit noch nichts gesagt sein soll über die Qualifikation dieses aktiven Tuns als strafrechtliche relevante Gehilfenschaft oder bloss «harmlose Gehilfenschaft», wie sie im Falle zumindest eines Access-Providers zweifellos zu Recht vertreten wird (vgl. VIT-Gutachten, S. 24 und S. 25 f. sowie den «Antilopenfleisch-Fall» in BGE 119 IV 289, in welchem erste Ansätze zur Beschränkung des Tatbestands der Gehilfenschaft im Falle von alltäglichen Handlungen erarbeitet wurden).

30 Gleiches gilt auch für die zivilrechtliche Haftung.

31 Falls nein, so wird dies in einer nicht-strafbaren «harmlosen» Gehilfenschaft resultieren oder aber es fehlt an der für die Begründung eines unechten Unterlassungsdelikts notwendigen Garantenstellung durch Schaffung einer Gefahr.

32 Abgedruckt in Sic! 2003, S. 960-964 sowie Jurius, Urteil des Strafgerichtspräsidenten Basel-Stadt zu «lyrics.ch», in: Jusletter 8. September 2003.

33 Erw. 3b.

34 SR 935.52; diese Bestimmung hat folgenden Wortlaut: «Die telekommunikationsgestützte Durchführung von Glücksspielen, insbesondere mittels Internet, ist verboten.»

35 Tribunal d´accusation du Canton de Vaud, Arrêt du 2 avril 2003; vgl. auch Christian Schwarzenegger, Sperrverfügungen gegen Access-Provider – Über die rechtliche Zulässigkeit polizeilicher Gefahrenabwehr durch Sperranordnungen im Internet, in: Oliver Arter/Florian S. Jörg (Hrsg.), Internet-Recht und Electronic Commerce Law, 3. Tagungsband, Bern 2003, S. 249 ff.

36 SR 780.1.

37 Entscheidung vom 27. April 2004.

38 Siehe vorne Rz 9.

39 Expertenbericht, S. 144.

40 Expertenbericht, S. 144 f.

41 Siehe vorne Rz 9.

42 Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates zur Durchsetzung der Rechte des geistigen Eigentums.

43 Eine typische Konstellation wäre, dass der Täter auf seinem Computer (z.B. ein PC) eine Website mit einem illegalen Inhalt betreibt (was technisch keinen grösseren Aufwand mit sich bringt), dieser Computer über einen DSL- oder Kabel-Internet-Zugang eines Access Providers ständig mit dem Internet verbunden ist und die Website so von anderen Internet-Benutzern jederzeit abgerufen werden kann. Der Access-Provider kann in solchen Fällen mit gewissem Aufwand eine Weiterverbreitung der Internet-Inhalte etwa dadurch unterbinden, dass er alle externe Zugriffe auf Webserver seines Kunden blockiert, will er den Zugang nicht ganz kündigen.

44 David Rosenthal, Netzwerkkriminalität: Straflosigkeit für Access-Provider, in: Medialex 1/2005, S. 7f.

45 Vgl. Expertenbericht, S. 60 f. und S. 68 ff.

46 Art. 110 Abs. 1 IPRG (SR 291).

47 Der Expertenbericht hält auf S. 102 fest, ein Hosting-Provider müsse nach der Einräumung des Speicherplatzes auf seinem Server nichts mehr weiteres tun, damit sein Kunde diesen für sein Angebot nutzen könne. Richtig ist, dass der Betrieb eines Servers eine Daueraufgabe ist; Speicherkapazitäten müssen verwaltet, die Sicherheit des System aufrecht erhalten werden. Dies umfasst auch zahlreiche Arbeiten, die nicht automatisiert stattfinden. Was jedoch zutrifft ist, dass der Hosting-Provider bei diesen Arbeit sich nicht inhaltlich mit den einzelnen Angeboten seiner Kunden auseinandersetzt, sondern wie ein Hauswart nur die technische Infrastruktur unterhält.

48 Zum Beispiel Internet-Auktionsplattformen wie eBay oder Ricardo.

49 Die Frage hat sich auch bezüglich Art. 14 ECRL gestellt. Gemäss der Kommission erfasst der Begriff nicht nur das traditionelle Hosten von fremden Websites, sondern auch ähnliche Dienstleistungen (vgl. Schreiben der Europäischen Kommission vom 14. Februar 2003). Vgl. hierzu auch das Urteil (I ZR 304/01) des BGH vom 11. März 2004 i.S. «Rolex v. ricardo.de» in: Jusletter 27. September 2004.

50 Expertenbericht, S. 103.

51 Vgl. Art. 14f Abs. 2 AEFV (SR 784.104).

52 Art. 100quater f. StGB.

53 Art. 322bis VE-StGB würde die Rechtfertigung einer Seite nur zulassen, wenn der Provider sicheres Wissen bezüglich der Strafbarkeit hätte, was der Provider im Prozess mit einem Kunden zu beweisen hätte. Provider werden also weiterhin gut beraten sein, in ihren Vertragsbedingungen sich das Recht einräumen zu lassen, auch in Zweifelsfällen unerlaubter Inhalte Angebote sperren zu dürfen.

54 Expertenbericht, S. 117.

55 Siehe hinten Rz 98.

56 Die Formulierung könnte folgendermassen lauten: «... bereithält, von der er im Einzelfall konkrete Kenntnis hat und mittels welcher, wie ihm von einer zuständigen Behörde für diesen Fall schriftlich mitgeteilt worden ist, eine strafbare Handlung begangen wird, ...».

57 Urteil (I ZR 304/01) des BGH vom 11. März 2004 i.S. «Rolex v. ricardo.de» in: Jusletter 27. September 2004.

58 Erw. 2 (b)(bb)(2).

59 Bericht zum Vorentwurf, S. 12.

60 Siehe hinten Rz 54.

61 Bericht zum Vorentwurf, S. 17.

62 Zugänglich unter www.cybercrime.ch; siehe auch Philipp Kronig/Eva Bollmann, Die nationale Koordinationsstelle zur Bekämpfung der Internetkriminalität – ein Porträt, in: Schweizerische Anwaltsrevue, 2/2006, S. 51-54; Eva Bollmann, Die Bekämpfung der Internetkriminalität in der Schweiz – die nationale Koordinationsstelle KOBIK, in: Jusletter 8. November 2004.

63 Sofern im Konzernverbund die dargestellten Informationen tatsächlich als «fremd» qualifiziert werden.

64 Art. 29 StGB.

65 Homepage: www.simsa.ch.

66 Schreiben der Simsa vom 1. April 2205 i.S. Netzwerkkriminalität: Vernehmlassung zur Revision des Strafgesetzbuches, S. 3.

67 Ebd., S. 5.

68 Expertenbericht, S. 86 ff.

69 Vgl. etwa Robert G. Briner, Zivil- und strafrechtliche Verantwortung der Internet Provider, in: Schweizerische Anwaltsrevue, 2/2006, S. 51; Patrick Rohn, Zivilrechtliche Verantwortlichkeit der Internet Provider nach schweizerischem Recht, Diss. Zürich 2004; Rolf H. Weber, E-Commerce und Recht, Rechtliche Rahmenbedingungen elektronischer Geschäftsformen, Zürich 2001, S. 507 ff. und S. 515 ff.; einen Überblick für das deutsche Recht gibt Thomas Hoeren, Skriptum zum Internetrecht, Fassung vom Januar 2006; das Skriptum wird regelmässig aktualisiert (vgl. www.uni-muenster.de/Jura.itm/hoeren/).

70 Urteil (I ZR 304/01) des BGH vom 11. März 2004 i.S. «Rolex v. ricardo.de», in: Jusletter 27. September 2004, Erw. 2(b)(bb)(2).

71 Bericht zum Vorentwurf, S. 12.

72 Art. 14 Abs. 3 ECRL.

73 Bericht zum Vorentwurf, S. 12, Absatz 2.

74 Bericht zum Vorentwurf, S. 11 f.

75 So zum Beispiel mit dem Digital Millennium Copyright Act (DMCA) in den USA, der für Provider seit 1998 einen «safe harbor» gegen Klagen wegen Urheberrechtsverletzungen statuiert, solange sich dieser an gewisse Regeln hält.

76 Vgl. z.B. Art. 13 Abs. 2 Bst. d DSG (SR 235.1); Art. 28 URG (SR 231.1).

77 Art. 14f Abs. 2 AEFV (SR 784.104); siehe nachfolgend Rz 74.

78 Siehe hinten Rz 84.

79 Z.B. im Rahmen der bereits erwähnten E-Commerce-Richtlinie (ECRL).

80 Für das Zivilrecht siehe die Ausführungen hinten Rz 98 ff. und Rz 107 ff..

81 Siehe hinten Rz 84 ff.

82 SR 784.104.

83 Immerhin ist seit der Einführung von Art. 100quater StGB auch eine subsidiäre Strafbarkeit des Providers im Falle eines Verbrechens oder Vergehens möglich, wenn die für die Straftat verantwortliche natürliche Person im Betrieb des Providers sich aufgrund von Organisationsmängeln nicht ermitteln lässt.

84 Vgl. zuletzt etwa Briner, a.a.O., S. 48, der offenbar von einer (echten oder unechten?) Unterlassungstat ausgeht.

85 Vgl. nachfolgend Rz 92; gl. M. offenbar Rohn, a.a.O., Fn. 901, S. 198.

[86] Vgl. vorne Rz 18 und Fussnote 47.

[87] Heinz Rey, Ausservertragliches Haftpflichtrecht, Zürich 2003, N 672.

[88] Rey, a.a.O, N 697; Karl Oftinger/Emil W. Stark, Schweizerisches Haftpflichtrecht, Erster Band: Allgemeiner Teil, §4, N 42, S. 182.

[89] URG, SR 231.1.

[90] MSchG, SR 232.11.

[91] UWG, SR 241.

[92] DSG, SR 235.1.

[93] BGE 124 III 297 S. 300; vgl. auch Oftinger/Stark, a.a.O., §4 N44, S. 182f.

[94] Von gewissen Sonderfällen ausgenommen, etwa wenn eine Anknüpfung an das schweizerische Recht durch das IPRG nicht möglich ist und daher die diesbezügliche Sonderregelung von Art. 322bis VE-StGB hilfreich sein kann.

[95] Siehe nachfolgend Rz 102 ff.

[96] Siehe vorne Rz 22.

[97] Im Falle der Verletzung von Immaterialgüterrechten kann sich auch die Frage des Gewinnherausgabeanspruchs stellen. Hier ist umstritten, ob ein Verschulden vorliegen muss (vgl. Andri Hess-Blumer, Teilnahmehandlungen im Immaterialgüterrecht unter zivilrechtlichen Aspekten, in: Sic! 2003, S. 104, m.w.H.).

[98] Oftinger/Stark, a.a.O., § 5, N 16, S. 193

[99] Vgl. Oftinger/Stark, a.a.O, § 5, N 16, S. 193.

[100] Siehe vorne Rz 22 f.

[101] Oftinger/Stark, a.a.O, § 5, N 45, S. 200.

[102] So beschäftigt zum Beispiel eBay nach eigenen Angaben in Deutschland ein 100-köpfiges «Sicherheitsteam», das einschreitet, wenn gemäss den Nutzungsbestimmungen unzulässige Waren verkauft werden sollen oder es «Anzeichen für andere unseriöse Aktivitäten» von Benutzern der Plattform gebe (Quelle: Pressemitteilung von eBay Deutschland vom 12. November 2004, abrufbar unter www.ebay.de).

[103] Rey, a.a.O., N 843; Oftinger/Stark, a.a.O., § 5, N 51, S. 202.

[104] Vgl. etwa Rohn, a.a.O., S. 199, m.w.H., und S. 246 f., m.w.H.; Briner, a.a.O., S. 48f.

[105] Zum Gefahrensatz vgl. Rey, a.a.O., N 866 ff.

[106] So auch das Entscheid des Strafgerichtspräsidenten Basel-Stadt vom 31. Januar 2003 («Lyrics Server»), abgedruckt in: Sic! 2003, S. 960-964 sowie Jurius, Urteil des Strafgerichtspräsidenten Basel-Stadt zu «lyrics.ch», in: Jusletter 8. September 2003.

[107] Dementsprechend unspezifisch ist der Tatbeitrag.

[108] Für das Strafrecht vgl. VIT-Gutachten, S. 24 und S. 25 f. zur «harmlosen Gehilfenschaft» sowie BGE 119 IV 289 («Antilopenfleisch»).

[109] Somit scheidet ein diesbezügliches Übernahmeverschulden nach der hier vertretenen Auffassung aus.

[110] Oftinger/Stark, a.a.O., § 5, N 41f., S. 199.

[111] Rey, a.a.O., N 847, m.W.H.

[112] Vgl. etwa BGE 121 III 358 S. 362.

[113] Das gilt notabene auch für Stichprobenkontrollen, die nach der hier vertretenen Ansicht eine reine Ressourcenverschwendung sind: Die überwiegende Mehrheit der Inhalte sind rechtmässiger Natur oder aber dergestalt, dass ein Provider ohne spezifische Hinweise und Zusatzwissen von sich aus gar nicht erkennen könnte, dass sie Rechte Dritter verletzen. Somit ist die Chance, auf im Rahmen von zufälligen Stichprobenkontrollen auf einen erkennbar rechtswidrigen Inhalt zu stossen noch bevor eine entsprechend qualifizierter Beschwerde eingeht, beinahe null. Mit gezielteren Stichproben könnte die Trefferquote wohl erhöht werden, doch würde dies wiederum voraussetzen, dass eine Vorausscheidung von heiklen Inhalten bzw. Kunden stattfinden müsste, was wiederum mit einem zumutbarem Aufwand für einen (in der Regel hochautomatisierten) Provider-Betrieb normalerweise nicht möglich ist. Ist die Dienstleistung eines Providers so gestaltet, dass eine vorgängige Benutzerregistrierung erforderlich ist, wird ein Provider allenfalls ein Benutzerkonto sperren können, das für missbräuchliche Aktivitäten verwendet wurde. Es wird

von einem Provider jedoch nicht verlangt werden können, dass er eine Neuregistrierung derselben Person (unter Einrichtung eines neuen Benutzerkontos) verhindert, weil dies wiederum voraussetzen würde, dass er seine Kunden sicher und zuverlässig identifiziert. Dies muss eine freiwillige Massnahme bleiben. Sie darf daher für die Bestimmung der Sorgfaltspflicht nicht relevant sein.

114 So setzen die Strafverfolgungsbehörden bereits heute Systeme ein, die das Internet automatisiert nach bekannter Kinderpornographie absuchen können.

115 Vgl. etwa Rohn, a.a.O., S. 204 ff., m.w.H., der mit Verweis auf BGE 126 III 161 S. 168 (in welchem Entscheid es um eine Druckerei ging) immerhin dann periodische Stichproben für geboten hält, wenn etwa infolge vorgängiger Rechtsverletzungen durch den selben Anbieter eine erhöhte Verletzungswahrscheinlichkeit besteht. Dies ist aus den bereits genannten Gründen gegen eine präventive Kontrolle bzw. Stichprobenkontrolle abzulehnen. Erhält ein Provider hingegen Hinweise, hat er diese nach branchenüblicher Sorgfalt zu prüfen (periodische Stichprobenkontrollen umfasst dies allerdings nicht). Dieses System funktioniert hinreichend rasch und zuverlässig.

116 Z.B. durch den Einsatz von Programmen, die öffentliche Inhalte der Kunden automatisiert auf bestimmte, heikle Stichworte und andere Anzeichen für unseriöse Aktivitäten untersuchen und im Falle von Treffern diese dafür dem «Abuse»-Team des Providers zur manuellen Kontrolle weiterleiten. Solche Methoden werden vor allem von grösseren Providern eingesetzt, die aufgrund der Art ihrer Dienstleistung eine erhöhte Missbrauchsanfälligkeit aufweisen (wie z.B. Online-Versteigerungsplattformen).

117 Siehe hierzu nachfolgend die Ausführungen im Zusammenhang mit Eigenrecherchen unter Rz 99.

118 Rey, a.a.O., N 877, m.w.H.

119 In der Literatur wird darauf hingewiesen, dass eine Nachrpüfungspflicht in Bezug auf jeden Hinweis von privater Seite ein weites Betätigungsfeld für Querulanten eröffnen würde und das Erfordernis einer Hinweisberechtigung unbeteiligte Personen von Hinweisen abhalte, was wiederum eine effektivere Verfolgung von ernsthaften Hinweisen betroffener Personen ermögliche (Rohn, a.a.O., S. 251; Weber, a.a.O, S. 508 f.).

120 Festgelegt durch das BÜPF (siehe vorne Rz 25).

121 So auch Rohn, a.a.O., S. 202, m.w.H., und S. 250.

122 Stellt ein Internet-Angebot auf dem Server eines Hosting-Providers beispielsweise lediglich eine Vertragsverletzung zwischen dem Kunden des Providers und einem Dritten dar, so wäre dies für einen Provider irrelevant, da er hierfür nicht einzustehen bräuchte. Verletzt das Internet-Angebot aber beispielsweise zugleich auch eine Bestimmung des Gesetzes gegen den unlauteren Wettbewerb oder liegt eine strafbare Handlung vor, so wird die diesbezügliche Schädigung für den Provider relevant, weil sie (auch) zur unerlaubten Handlung wird.

123 Oftinger/Stark, a.a.O., § 5, N 60, S. 204.

124 Was sich möglicherweise bereits im Sinne einer vertraglichen Nebenpflicht des Providers gegenüber seinem Kunden ergeben kann, falls der Hinweis ernsthafter Natur ist.

125 Im Falle des Hosting-Providers dies deshalb, weil er seinen Kunden nicht nur Speicherplatz zur Verfügung stellt, sondern ebenfalls mittels einer eigenen Internet-Anbindung sorgt, dass diese Inhalte an die nachfragenden Internet-Benutzer übermittelt werden.

126 Art. 43 FMG (SR 784.10).

127 Art. 44 FMG (SR 784.10).

128 Eine Möglichkeit hierzu wäre die Erweiterung des Katalogs der Grundversorgungsdienste um einen Internet-Breitbandzugang, soweit diese Pflicht nicht bloss auf die Bereitstellung eines Anschlusspunktes für entsprechende Dienstleistungen beschränkt wird, sodass der eigentliche Internet-Zugangsdienst über einen beliebigen Access-Provider bezogen werden kann.

129 So etwa aus Art. 7 KG (SR 251).

130 Siehe vorne Rz 15; Rohn, a.a.O., S. 212 ff. m.w.H., und S. 252 ff., m.w.H.

131 Solche Möglichkeiten bestehen in den meisten Fällen, doch ist das breitere Publikum in aller Regel nicht in der Lage oder bereit, sie einzusetzen, weshalb sie für die Beurteilung der Sorgfaltspflicht eines Providers meist unerheblich sind.

132 Zum Begriff: Rey, a.a.O., N 1435b, m.w.H.; zur Teilnahme im Immaterialgüterrecht: Andri Blumer-Hess, a.a.O., S. 95 ff., demzufolge es der überwiegenden Lehre und einhelliger Rechtssprechung

entspricht, dass auch in denjenigen Bereichen, in denen spezialgesetzliche Bestimmungen zur Teilnahme vorhanden sind, die Teilnahmebestimmungen keine unabhängig von einer unmittelbaren Verletzungshandlung losgelöste Gefährdungstatbestände statuieren (S. 98, m.w.H.).

[133] Rey, a.a.O., N 1427.

[134] Was umstritten ist, vgl. nachfolgend Rz 107.

[135] Zur solidarischen Haftung durch gemeinsame Verursachung vgl. Vito Roberto, Schweizerisches Haftpflichtrecht, Zürich 2002, N 161, S. 47; Rey, a.a.O., N 631 ff.

[136] BGE 115 II 42 S. 45; Rey, a.a.O., N 1436.

[137] BGE 130 III 591 S. 603 m.w.H.

[138] Rey, a.a.O., N 633.

[139] Roberto, a.a.O., N 162, m.w.H.

[140] Rey, a.a.O., N 627.

[141] Rohn, a.a.O., S. 245 f.

[142] D.h. die verschiedenen Access-Provider (zu ermitteln anhand der benutzten IP-Adresse), über welche die Zugriffe erfolgt sind.

[143] Rey, a.a.O., N 624, m.w.H.; Roberto, a.a.O., N 174 f., S. 51.

[144] Roberto, a.a.O., N 162, S. 47, m.w.H.

[145] Vgl. z.B. BGE 123 III 110 S. 112; Roberto, a.a.O., N 179, S. 52.

[146] Hierzu gehören etwa die Betreiber von «Backbones», also Datenstrecken, über welche verschiedene Provider ihre Netze untereinander verbinden oder die sie zur Übertragung ihres Internet-Verkehrs über grössere Distanzen nutzen.

[147] Hierzu gehören die Betreiber von «Peering Points», also Provider, deren Dienstleistung darin besteht, verschiedene Providernetze an einer Stelle physisch miteinander zu verbinden.

[148] Ähnlich auch Robert G. Briner/Clara Ann Gordon, Den Sack schlagen, den Esel meinen, in: NZZ 29. Juli 2005, Nr. 175, S. 11, die im Zusammenhang mit dem bundesrätlichen Vorentwurf für ein Providerstrafrecht betonen, es erscheine «unverhältnismässig, den Internet-Service-Provider strafrechtlich zur Verantwortung zu ziehen, weil seine Dienstleistungen von Dritten missbraucht werden.».

Erschienen in Peter Jung (Hrsg.), Tagungsband Recht aktuell 2006 (Aktuelle Entwicklungen im Haftpflichtrecht)

Zitiervorschlag David Rosenthal, Internet-Provider-Haftung – ein Sonderfall?, in: Peter Jung (Hrsg.), Tagungsband Recht aktuell 2006 (Aktuelle Entwicklungen im Haftpflichtrecht), Bern: Edition Weblaw 2006

dro David Rosenthal studierte an der Universität Basel, wo er seit 1999 Lehrbeauftragter für Informatik- und Telekommunikationsrecht ist. Er war zunächst als Software-Entwickler tätig, führte dann ein Pressebüro für Informationstechnologie, verfasste zahlreiche Publikationen und hält regelmässig Vorträge. Er war u.a. Mitglied der Eidg. Rekurskommission für das Fernmelde- und Postwesen. Seit 2001 ist er Konsulent für Informations- und Telekommunikationsrecht der Wirtschaftskanzlei Homburger in Zürich.

Der vorliegende Beitrag basiert auf einem Vortrag des Autors im Rahmen der Tagung «Recht Aktuell» der Juristischen Fakultät der Universität Basel vom 3. Februar 2006 in Basel.