Haftung eines Internet Service Providers in der Schweiz

Autoren:

Amir Guindehi
Buchholzstr. 143
8053 Zürich

D-ELEK

Markus Roth
Niederweg 1d
8907 Wettswil

D-ELEK

ETH Zürich
Professur für Privatrecht
Prof Urs Ch. Nef

Zürich, den Dienstag, 13. Juni 2000

Inhaltsverzeichnis

Literaturverzeichnis

BJ 1 Internet, Neues Medium – neue Fragen ans Recht, Bericht einer interdepartementalen Arbeitsgruppe zu strafrechtlichen, datenschutzrechtlichen und urheberrechtlichen Fragen rund um Internet, Bundesamt für Justiz, Bern, Mai 1996

PMF 1 Zürcher Porno-Mailbox-Fall: Fehlende Zuganskontrolle, Copyright © 1997, 1998 Insider Communications, Rosenthal & Partner, Basel, http://www.insider.ch/ipd/recht/kapitel2/rch3002.htm

ZHOL 1 Bundesgerichtsurteile betreffend Internet-Provider, (öffentliche Beratung vom 5. April 2000 im Fall 1A.104/1999 und Urteil 1P.703/1999 vom 28. Februar 2000), http://www.zhol.ch/pubs/news/lokalzhol/2000_04_05_14_04_rdzh_141208.asp

Abkürzungsverzeichnis

BJ	Bundesamt für Justiz
DSG	Datenschutzgesetz
ISP	Internet Service Providers
MP3	Kurzformel für Audio-Dateiformat: MPEG 2,5 Audio Layer III
SDA	Schweizerische Depechenagentur
StGB	Strafgesetzbuch
URG	Urheberrechtsgesetz
WCT	WIPO Copyright Treaty
WIPO	World Intellectual Property Organization
WPPT	WIPO Performance and Phonograms Treaty
ZHOL	Zürich Online

1. Problemstellung

Im Rahmen der MTU-Veranstaltung des Sommersemesters 2000 erhielten wir die Aufgabe, eine Seminararbeit zur Rechtslage der Haftung des Internet Service Providers, im Weiteren ISP genannt, zu erarbeiten

Im Zentrum der Arbeit stehen Fragen über die Haftung des ISP im Zusammenhang mit Datenschutz, Strafrecht, Urheberrecht, Zensurpflicht und Meinungsfreiheit. Als Arbeitsgrundlage und Inspiration wurde auf dem Bericht einer interdepartementalten Arbeitsgruppe des Bundesamtes für Justiz aus dem Mai 1996 aufgebaut [BJ 1].

Im diesem Bericht gibt der Bund 11 Empfehlungen an den ISP ab, welche wir aus der Sicht der ISP kommentieren werden.

„Es versteht sich, dass die vorstehend aufgeworfenen Fragen lediglich einen kleinen Teilaspekt der mit der rasanten Entwicklung des Internet verbundenen Rechtsprobleme bilden. Die globale Ausdehnung dieses Mediums, seine technischen Möglichkeiten, die geschätzte Teilnehmerzahl von weltweit ca. 40 Mio. Sowie das Fehlen eines verantwortlichen, individualisierbaren Betreibers bergen naheliegenderweise auch erhebliche Missbrauchsmöglichkeiten, die in jüngster Zeit auch in den Medien vermehrt thematisiert werden.“[1]

Die 40 Mio. Teilnehmer, die im Bericht erwähnt werden, sind in der Zwischenzeit rasant angewachsen, so dass wir heute von mehreren 100 Mio. Teilnehmern ausgehen können. Im Bericht wurden auch folgende Einschränkungen gemacht:

„Die mit Internet verbundenen Rechtsfragen sind ausserordentlich vielfältig und komplex. Hinzu kommt, dass dieses Medium durch eine rasante technische Entwicklung gekennzeichnet ist, deren weiteren Verlauf sich heute kaum absehen lässt. Entsprechend kann der vorliegende Bericht nicht über eine vorläufige Standortbestimmung hinausgehen; seine Empfehlungen sind als ein Versuch zu verstehen, ein provisorisches und noch unvollständiges Instrumentarium gegen den Missbrauch von Internet zu schaffen.“[2]

[1] BJ 1, Seite 3.
[2] BJ 1, Seite 4.

2. Strafrechtiliche Aspekte

2.1 Gesetzesgrundlagen

Nach Studium von [BJ 1] und StGB fanden wir folgende Delikte, die durch Gesetzesartikel im StGB direkt geregelt oder am Rande tangiert werden.

2.1.1 Computerdelikte

StGB Art. 143	Unbefugte Datenbeschaffung
StGB Art. 143bis	Unbefugtes Eindringen in ein Datenverarbeitungssystem
StGB Art. 144bis	Datenbeschädigung
StGB Art. 147	Betrügerischer Missbrauch einer Datenverarbeitungsanlage
StGB Art. 150 Abs. 4	Erschleichen einer Dienstleistung durch die Benutzung von Internet oder eines anderen Netzwerkes.

2.1.2 Gedankenäusserungsdelikte

StGB Art. 135	Tatbestände der Gewaltdarstellung (sog. Brutalos)
StGB Art. 197	Pornographie
StGB Art. 261bis	Rassendiskriminierung
StGB Art. 173 ff.	Ehrverletzung
StGB Art. 320 und 321	Geheimnisverletzung
StGB Art. 259	Öffentliche Aufforderung zu Verbrechen oder Gewalttätigkeit
StGB Art. 144bis Ziff. 2	Datenbeschädigung, wie etwa die Anleitung zur Herstellung von Computerviren

2.2 Empfehlungen des Bundes

2.2.1 Empfehlung 1 – Sperrung von rechtswidrigen Netzinhalten

„Verfügt der Provider aufgrund eigener Erkenntnis oder durch Dritte über konkrete Hinweise, die den Verdacht begründen, dass bestimmte Netzinhalte rechtswidrig sein könnte, so soll er im Hinblick auf eine allenfalls notwendige Sperrung umgehend Abklärungen treffen oder treffen lassen. Hat der Provider sichere Kenntnis von rechtswidrigen, namentlich strafrechtlich relevanten Netzinhalten, so soll er unverzüglich die technisch möglichen und zumutbaren Massnahmen ergreifen, um den Zugriff auf diese Netzinhalte zu sperren.“[3]

[3] BJ 1, Seite 17.

2.2.2 Empfehlung 2 – Zentrale Stelle

„Der Branche wird die Schaffung einer zentralen Stelle empfohlen, welche Hinweise von Providern, deren Kunden und Dritten über rechtswidrige Netzinhalte entgegennimmt und auswertet. Diese Stelle soll als Dienstleistungs- und Informationsdrehscheibe die angeschlossenen Providers mit aktuellen Informationen über zu sperrende Netzinhalte versorgen und die Branchenangehörigen in fachlicher und technischer Hinsicht unterstützen.“[4]

2.2.3 Empfehlung 3 - Netzzugang

„Dem Provider wird empfohlen, Abonnementsverträge grundsätzlich nur mit solchen natürlichen Personen abzuschliessen, die urteilsfähig und mündig sind. Dem Abonnenten soll zudem der Netzzugang ausschliesslich mittels Benutzeridentifikation und Passwort (pin-code) ermöglicht werden.“[5]

2.2.4 Empfehlung 4 – Vorbehalt im Abonnementsvertrag

„Der Provider soll sich im Abonnementsvertrag das Recht vorbehalten, den Anschluss bei Verdacht vorsorglich zu sperren und das Vertagsverhältnis einseitig aufzulösen, sofern der Kunde rechtswidrige Inhalte von seinem Anschluss aus verbreitet oder auf seinem Anschluss abrufbar hält.“[6]

2.2.5 Empfehlung 5 – Aufforderung zur Mitteilung

„Der Kunde soll im Abonnementsvertrag nachdrücklich aufgefordert werden, ihm zur Kenntnis gelangende rechtswidrige Netzinhalte und andere rechtswidrige Internet-Verwendungen unverzüglich dem Provider und/oder der zentralen Stelle (vgl. Empfehlung 2) mitzuteilen“[7]

2.2.6 Empfehlung 6 – Erscheinungsformen von harter Pornografie

„Der Provider soll sich des Umstandes bewusst sein, dass strafbare Gewaltdarstellungen I.S. von Artikel 135 StGB sich nicht in filmischen oder Photographischen Darstellungen erschöpfen, sondern auch in anderen Gegenständen oder Vorführungen, insbesondere in Computerspielen, einthalten sein können, und dass auch das Anpreisen oder Anbieten von Gewaltdarstellungen eine strafbare Handlung ist. Gleiches gilt auch für Darstellungen harter Pornographie i.S. von Artikel 197 Ziffer 3 StGB.“[8]

[4] BJ 1, Seite 18.
[5] BJ 1, Seite 19.
[6] BJ 1, Seite 19.
[7] BJ 1, Seite 19.
[8] BJ 1, Seite 20.

2.3 Kommentar zu den Empfehlungen des Bundes

2.3.1. Zu Empfehlung 1

Auszugehen ist von der Rechtslage, wie sie im Urteil des Bundesgerichts im Fall Rosenberg festgelegt worden ist.

Danach macht sich ein Provider nur dann strafbar, wenn er konkrete Kenntnisse über strafrechtliche Handlungen hat, welche mittels den von ihm zur Verfügung gestellten Anlagen begangen werden und er dagegen nichts unternimmt. Diesfalls macht er sich der Gehilfenschaft zum in Frage stehenden Delikt schuldig. Klar ist, dass Gehilfenschaft grundsätzlich nur bei Verbrechen und Vergehen im Sinne des Strafgesetzbuches strafbar ist, nicht jedoch bei Übertretungen (Art. 104 StGB).

Eine Pflicht des Providers, präventiv eine Kontrolle der über seine Anlagen verbreiteten bzw. zur Verfügung gestellten Inhalte durchzuführen, sofern dies überhaupt technisch durchführbar sein sollte, besteht dagegen klarerweise nicht.

Die Sperrung soll nicht bloss bei den bisher im Zentrum des Interesses stehenden Delikten der Pornographie, Gewaltdarstellung, Rassismus etc. erfolgen.
Erfasst werden nun plötzlich alle strafrechtlich relevanten Inhalte, insbesondere auch solche, die Gegenstand von sogenannten Übertretungen, wie z.B. die Verletzung der Pflicht zur Preisbekanntgabe an Konsumenten oder die Verletzung der Ausverkaufsvorschriften gemäss Art. 25 und 26 des Bundesgesetzes gegen den unlauteren Wettbewerb, darstellen.

Von Gesetzes wegen ist jedoch bei sogenannten Übertretungen, welche von Dritten begangen werden, eine strafrechtliche Verantwortlichkeit der Provider und damit eine Pflicht zur Ergreifung von Massnahmen zur Verhinderung solcher Verhaltensweisen grundsätzlich nicht gegeben.

Unter "rechtswidrig" werden aber auch Verhaltensweisen verstanden, welche strafrechtlich gar nicht relevant sind. Hier ist nun überhaupt nicht ersichtlich, weshalb der Provider einschreiten soll. In diesen Fällen verlangt die Rechtsordnung von den nicht direkt beteiligten Privaten keine Massnahmen. Für die Beseitigung der Rechtswidrigkeit sind allein die zuständigen Behörden im Rahmen von Verwaltungsverfahren oder die direkt betroffenen Privaten durch zivilrechtliche Klage zuständig.

Fazit des oben genannten ist, dass die Empfehlung 1 bezüglich der Sperrung rechtswidriger Netzinhalte zu weit gefasst ist.

2.3.2. Zu Empfehlung 2 und 5

Bei der vorstehend in geschilderten Rechtslage führt die Empfehlung zur Schaffung einer zentralen Stelle, welche die Provider über zu sperrende Inhalte informiert, zu einer Erhöhung des Risikos der Strafbarkeit der Provider.

Durch das Weiterleiten der Kenntnisse über strafbares Verhalten bzw. Inhalte durch die zentrale Stelle an andere Provider wird auch bei diesen die Grundvoraussetzung der Strafbarkeit geschaffen.

Diese Empfehlung ist in Anbetracht der möglichen Konsequenzen für die Provider in der gegenwärtigen Situation deshalb nicht verantwortbar, weil keine klaren Richtlinien in bezug auf das Verhalten gegenüber möglicherweise strafbaren Inhalten im Internet bestehen.

Zudem ist es bei den heutigen Marktverhältnissen, bei denen viele neue Provider entstehen und ebensoviele wieder vom Markt verschwinden, kaum möglich, jeweils alle (es dürften heute wohl bereits über 100 sein) zu informieren. Diejenigen, welche von der zentralen Stelle informiert bzw. in Kenntnis gesetzt werden, werden somit vor denjenigen, die nichts wissen, klar benachteiligt.

Es stellt sich das kaum lösbare Problem, wie sich ein Provider zu verhalten hat, wenn die strafrechtliche Relevanz von Netzinhalten zwar als möglich, aber nicht als erwiesen anzusehen ist.

Jedenfalls kann dem Provider nicht empfohlen werden, in dieser Situation das betreffende Material vorsorglich einmal zu entfernen bzw. zu sperren. Denn er riskiert damit, sollte sich diese Massnahme nachträglich als nicht gerechtfertigt herausstellen, dafür seitens des Inhaltanbieters haftbar gemacht zu werden.

Aufgrund des Urteils des Bundesgerichtes im Fall Rosenberg wird andererseits davon ausgegangen, dass der Provider sich nicht auf den Standpunkt stellen kann, er habe nichts vorzukehren, bis eine Verurteilung des eigentlichen Täters erfolgt sei, und er damit absolute Gewissheit über die Strafbarkeit des in Frage stehenden Materials hat. Denn ist ihm die Beurteilung von bestimmtem Material selbst nicht möglich, hat er jedoch genügend konkrete Hinweise bezüglich der strafrechtlichen Relevanz erhalten, so hat der Provider die nähere Abklärung unter Einbezug der Strafbehörden vorzunehmen. Dies alles ist für den Provider immer mit erheblichem Aufwand verbunden.

Dass durch eine zentrale private Stelle den Providern in diesem Punkt wesentliche Unterstützung geboten werden kann, ist nicht anzunehmen, sind doch die regelmässig solche Stellen führenden Rechtsanwälte keine Hellseher bzw. häufig nicht in der Lage, eine verbindliche Auskunft über die Frage, ob ein bestimmter Inhalt strafbar ist der nicht, zu geben.

Die Wirksamkeit einer solchen zentralen Stelle auf privater Basis wäre nicht zuletzt auch deshalb fraglich, weil aufgrund der kantonalen Strafrechtshoheit nicht mit einer in der gesamten Schweiz einheitlichen Verfolgungspraxis zu rechnen ist und es als ausgeschlossen erscheint, dass eine zentrale private Stelle dem immer genügend wird Rechnung tragen können.

Durch die Information aller angeschlossenen Provider durch die zentrale Stelle besteht daher die Gefahr, dass der einzelne Provider mit einer Flut von Informationen über eventuell rechtswidrige Inhalte konfrontiert wird und schlichtweg überfordert ist, diese Informationen hinreichend und rechtzeitig zu prüfen und die entsprechenden Massnahmen zu seinem Schutz zu treffen.

Zudem wäre ein solcher Provider gegenüber einem der Informationsstelle nicht angeschlossenen und somit nicht informierten Provider klar benachteiligt.

Auch ist zu beachten, dass sich die Empfehlung nicht nur auf die im Bericht als Beispiel genannte, auch für einen Laien relativ leicht zu beurteilende harte Pornographie bezieht, sondern auf alle strafrechtlichen Tatbestände.

Aber selbst im Pornographie-Artikel von StGB 197 ist in Ziffer 5 vorgesehen, dass Gegenstände oder Vorführungen, welche an und für sich unter das Verbot fallen würden, dann nicht pornographisch sind, wenn sie einen schutzwürdigen kulturellen oder wissenschaftlichen Wert haben. Die Beurteilung, ob diese Voraussetzungen vorliegen, kann sich anerkanntermassen als äusserst schwierig herausstellen.

Durch die empfohlene Einführung einer zentralen Stelle droht somit die Gefahr, dass die Provider freiwillig und unbesehen eine Verantwortung auf sich nehmen, der sie gar nicht gerecht werden können.

Zudem werden die sich der Empfehlung bzw. einem entsprechenden Ehrenkodex unterwerfenden Provider gegenüber solchen, die dies nicht tun (und dies werden wohl insbesondere die grossen, weltweit tätigen und gut beratenen sein) krass benachteiligt, erhöht sich doch ihre Verantwortung und damit das Strafbarkeits- und Haftungsrisiko.

Andererseits ist in diesem Zusammenhang festzuhalten, dass sich heute private Internet-Nutzer vor ungewollten Inhalten selber schützen können, durch Softwareprodukte wie etwa CyberPatrol, Surfwatch etc.

Es stellen sich jedoch noch weitere grundsätzliche Fragen, welche zu klären sind.

In der bisherigen Diskussion um die Entfernung/Sperrung von strafrechtlich relevantem Material durch Provider stand unter Bezugnahme auf das Rosenberg-Urteil des Bundesgerichts die Frage im Vordergrund, ob und unter welchen Voraussetzungen ein Provider entsprechende Massnahmen treffen muss, um seine eigene Strafbarkeit als Gehilfe auszuschliessen.

Eine ganz andere und in ihren Auswirkungen allenfalls verheerende Sache ist es jedoch, wenn die Provider durch Einrichtung einer eigenen zentralen Meldestelle sich dem Kampf für ein von strafrechtlich relevantem Material freies Internet verschreiben und, unabhängig von der Frage einer eigenen Strafbarkeit, solches Material entfernen bzw. sperren und dazu auch noch ihre Kunden auffordern, ihrerseits ebenfalls entsprechende Meldungen an den Provider oder die zentrale Stelle zu richten, wie dies die Empfehlung 5 vorsieht.

Durch Einrichtung einer privaten zentralen Stelle in bezug auf strafrechtlich relevante Inhalte oder der gegenseitigen Informationspflicht unter den Providern verbunden mit einer Löschungspflicht für alle Provider wird im Ergebnis eine Strafverfolgung auf privater Basis eingeführt.

Ob dies wirtschaftlich für die Provider überhaupt tragbar ist, wäre erst noch zu prüfen.

Die Einrichtung einer privaten zentralen Stelle ist aber schon deshalb höchst bedenklich, weil dadurch die im Rahmen der behördlichen Strafverfolgung vorgesehenen rechtsstaatlichen Sicherungen nicht mehr gewährleistet sind. Grundsätzlich muss die Durchsetzung des Strafrechts auch im Internet den zuständigen staatlichen Behörden vorbehalten bleiben. Private Initiativen sollten sich daher höchstens als flankierende Massnahmen in die staatliche Strafverfolgung integrieren.

Es will auch nicht einleuchten, weshalb die Provider sich entsprechend den Empfehlungen des Bundes in der Unterdrückung von rechtswidrigem Material im Internet engagieren und gewissermassen die staatliche Strafverfolgung substituieren sollen, wenn sich daraus für die Provider im wesentlichen nur Nachteile ergeben.

Dass die staatliche Strafverfolgung wegen der Internationalität des Internet der zumeist im Ausland sitzenden Täter nicht habhaft zu werden vermag, darf keine Begründung dafür sein, sich quasi stellvertretend an die geographisch zwar am nächsten gelegenen, mit den in Frage stehenden Delikten jedoch in aller Regel am wenigsten in Berührung stehenden Provider (diese sind zumeist weder Täter noch Konsumenten der strafrechtlichen Inhalte) zu halten.

Statt den im Bericht des Bundes vorgezeichneten Weg eines zweistufigen Verfahrens, wonach zuerst ein Selbstregulierungssystem der Branche zu prüfen sei, um danach bei einem allfälligen Versagen desselben ein staatliches Aufsichts- und Kontrolldispositiv einzurichten, müsste in erster Linie nach Wegen gesucht werden, wie die Effizienz der staatlichen Strafverfolgung erhöht werden könnte.

In den Empfehlungen sind jedoch zu den sich im Zusammenhang mit der Errichtung eines privaten Informations- und Kontrollsystems stellenden Fragen keine näheren Angaben gemacht, was als Mangel zu betrachten ist.

Es besteht die Gefahr, dass auf privater Basis, aus der unbegründeten Befürchtung vor eventuellen Massnahmen des
Bundes heraus und im Hinblick auf die teilweise sensationslüsterne Presse in unkoordinierter Weise und aufgrund der Bundesempfehlungen in eine falsche Richtung vorgeprellt wird.

Weiter ist zu berücksichtigen, dass eine allfällige Koordination der Provider und deren Informationstätigkeit in erster Linie mit den kantonalen Strafbehörden zu erfolgen hätte und nicht mit dem Bund, welcher in bezug auf die Strafverfolgung nur über punktuelle und im hier interessierenden Zusammenhang nicht im Vordergrund stehende Zuständigkeiten verfügt.

Insgesamt ist festzuhalten, dass weder die Voraussetzungen, noch die Rahmenbedingungen, noch die (auch wirtschaftlichen) Folgen einer auf der gegenseitigen Information der Provider unter sich oder auf den entsprechenden Mitteilungen von Kunden oder von Dritten beruhende und über eine zentrale private
Stelle koordinierte Repressionspolitik gegen die als strafrechtlich bedenklich erachteten Inhalte des Internet genügend geklärt sind. Es fehlt bisher insbesondere auch jede nähere Koordination mit den zuständigen Strafverfolgungsbehörden. Die genannte Empfehlung ist somit verfrüht, nicht durchdacht und sollte widerrufen werden.

2.3.3. Zu Empfehlung 3

Der Sinn der Empfehlung, Abonnementsverträge der Provider nur mit urteilsfähigen Mündigen abzuschliessen, ist nicht ersichtlich.

Um für den Jugendschutz den Zugang zu weicher Pornographie für Jugendliche unter 16 Jahren zu verhindern, ist die Massnahme untauglich. Denn der gesetzliche Jugendschutz gilt gerade auch dort, wo ein Internet-Anschluss nicht auf einen Jugendlichen lautet, sondern auf dessen Eltern, eine Schule oder sonst einen Dritten.

In seinem Rosenberg-Urteil, wo es um den Zugang Jugendlicher zu Pornographie über 156-Telefonnummern ging, hat das Bundesgericht verlangt, dass durch entsprechende Massnahmen (Passwörter; Identifikation etc.) der Zugang zu den entsprechenden Nummern bzw. Angeboten wirksam verhindert wird. Klarerweise völlig unerheblich war, ob der benutze Telefon-Anschluss auf einen Jugendlichen lautete oder auf jemand anderen.

Der Jugendschutz hat somit auch im Internet bei den einzelnen pornographischen Angeboten und nicht beim Zugang (Anschluss) zum Internet anzusetzen.

Es ist nämlich nicht der Access-Provider, sondern der Anbieter von pornographischen Inhalten, welcher verpflichtet ist, die Angebote gegen den Zugriff Jugendlicher zu sichern.

Nur wenn ein Provider konkrete Kenntnis hat, - und nur dann - dass ein pornographisches Angebot mit weicher Pornographie Jugendlichen unter 16 Jahren über ihn zugänglich ist, muss er im Rahmen seiner Möglichkeiten dagegen einschreiten, notfalls das Angebot sperren, will er dem Risiko einer Verurteilung analog dem Fall Rosenberg wegen Gehilfenschaft zur Pornographie entgehen.

Diese Vorgehensweise wurde auch in einem Gerichtsurteil am Zürcher Obergericht im Dezember 1998 [PMF 1] gefordert, bei dem ein Zürcher ETH-Student, Besitzer einer Mailbox ohne Zugangskontrolle, zu einer Busse verurteilt wurde. Trotz Hinweisen auf pornographisches Material, hat der Student C. mit der Begründung, dass Daten frei seien, dieses nicht gesperrt. Nach Auffassung des Gerichts hätte Student C. spätestens nach Kenntnisnahme des illegalen Materials, dieses entfernen und eine Alterskontrolle einführen, oder falls dies technisch nicht realisierbar wäre, die ganze Mailbox einstellen müssen.

2.3.4. Zu Empfehlung 4

Die Empfehlung ist dahingehend zu erweitern, dass auf Verdacht hin eine Sperrung auch möglich ist, wenn es sich um von Dritten verbreitete bzw. abrufbar gehaltene Inhalte handelt, ansonsten der Provider damit rechnen muss, von seinen Kunden im Falle, dass sich der Verdacht nicht bewahrheitet, für die ungerechtfertigte Sperrung haftbar gemacht zu werden.

3. Datenschutzrechtliche Aspekte

3.1 Gesetzesgrundlagen

DSG Art. 7 Abs. 1 Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden

3.2 Empfehlungen des Bundes

3.2.1 Empfehlung 7 – Information über Datenschutz-Risiken

„Der Provider soll seinen Kunden über die datenschutzrechtlichen Risiken, die sich aus dem Benutzen des Netzes sowie der Inanspruchnahme von Diensten ergeben können, ausreichend informieren sowie ihn auf Massnahmen und Produkte zu Gewährleistung der Vertraulichkeit, Richtigkeit und Verfügbarkeit von Personendaten (z.B. Chiffrierungs- und Verschlüsselungstechniken) hinweisen.“[9]

3.2.2 Empfehlung 8 – Bearbeitung von Personendaten

Der Provider soll ausschliesslich diejenigen Personendaten seiner Kunden bearbeiten, die er zur Erfüllung seiner Dienstleistung benötigt. Die bearbeiteten Daten sind durch technische und organisatorische Massnahmen ausschliesslich dem Personal zugänglich zu machen, das sie zur Aufgabenerfüllung benötigt. Die Daten sollen zu keinem anderen Zweck verwendet werden als demjenigen, der bei der Datenbeschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Dritten dürfen sie nur zugänglich gemacht werden, sofern der Kunde einverstanden ist, bzw. eine qualifizierte Pflicht zur Bekanntgabe besteht.

3.2.3 Empfehlung 9 – Persönlichkeitsprofile/ Personendaten

Der Provider soll keine Persönlichkeitsprofile seiner Kunden erstellen und auch deren Namen, Adressen und Telefonnummern nicht einem Netzzugriff zur Verfügung stellen, es sei denn, die betroffene Person habe eingewilligt, oder es liege eine Rechtfertigung durch Gesetz oder ein überwiegendes öffentliches oder privates Interesse vor.

[9] BJ 1, Seite 21.

3.3 Kommentar zu den Empfehlungen des Bundes

3.3.1. Zu Empfehlung 7

Diese Empfehlung ist insofern problematisch, als nicht präzisiert wird, wie weit die Informationspflicht des Providers geht bzw. was als ausreichende Information über die datenschutzrechtlichen Risiken sowie über die entsprechenden Massnahmen und Produkte zu deren Eingrenzung anzusehen ist.

Sofern die Information allgemein gehalten wird, dürfte sie für den Kunden wohl wenig Nutzen bringen, da sie bereits allgemein Bekanntes wiederholen würde.

Eine detailliertere Information und Abklärung über Risiken und zu treffende Massnahmen stellt demgegenüber typischerweise Gegenstand eines entsprechenden Beratungsauftrages mit dem Kunden dar. Ein solcher kann aber nicht einseitig durch den Provider herbeigeführt werden und auch nicht durch den Bund mittels Empfehlung vorgegeben werden.

3.3.1. Zu Empfehlung 8

„Lausanne (sda) Ohne Genehmigung des Richters darf gemäss Bundesgericht vom Provider über den E-Mail-Verkehr keine Auskunftserteilung an die Strafverfolgungsbehörden erfolgen. In einem weiteren Entscheid hat es die Hausdurchsuchung bei einem Provider abgesegnet.

In seiner öffentlichen Sitzung von Mittwoch kam das Bundesgericht zum Schluss, dass Angaben über den Absender oder den Zeitpunkt der Versendung eines E-Mails unter das Fernmeldegeheimnis fallen. Damit würden für die Auskunftserteilung die gleichen Voraussetzungen gelten wie bei einer Telefonabhörung“[10]

Der Internet-Provider Swiss Online weigerte sich, den Absender und Sendezeitpunkt eines E-Mails weiterzugeben, da eine gesetzliche Grundlage und eine richterliche Genehmigung fehle. Auch Randdaten unterliegen dem Fernmeldegeheimnis. Das Bundesgericht liess in der Folge keine Zweifel offen, dass der E-Mail Verkehr unter den umfassenden Begriff des Fernmeldeverkehrs einzuordnen sei. Für den Eingriff in die Geheimsphäre der Betroffenen sei deshalb eine richterliche Genehmigung einzuholen.

[10] ZHOL 1 Seite 1.

4. Urheberrechtliche Aspekte

4.1 Gesetzesgrundlage

URG Art. 1	Der Schutz des URG gilt für Urheber von Werken der Literatur und Kunst (Urheberrecht), ausübende Künstler, Hersteller von Ton- und Tonbildträgern sowie für Sendeunternehmen (verwandte Schutzrechte).
URG Art. 2 Abs. 2	Urheberrechtsschutz geniessen Werke der Literatur und Kunst wie etwa, Texte jeglicher Art, Werke der Musik, Werke der bildenden Kunst, Werke mit wissenschaftlichem oder technischem Inhalt, visuelle oder audiovisuelle Werke, Computerprogramme.
URG Art. 2 Abs. 1	Die obgenannten Werke sind aber nur urheberrechtlich geschützt, falls sie zum Bereich der Literatur und Kunst gehören, das Ergebnis einer geistigen Schöpfung sind und einen individuellen Charakter haben; d.h. das Merkmal der Individualität bzw. der Originalität erfüllen
URG Art. 3	Ein Werk zweiter Hand liegt vor, falls ein bereits vorhandenes Werk (ursprüngliches Werk) so bearbeitet wird, dass sein individueller Charakter erkennbar bleibt.
URG Art. 4	Sammlungen (Art. 4 URG) sind geschützt, sofern es sich bezüglich Auswahl oder Anordnung um geistige Schöpfungen mit individuellem Charakter handelt.
URG Art. 35 und 36	Die Hersteller von Ton- und Bildträgern und Sendeunternehmer sind durch das URG geschützt.
URG Art. 29	Der Urheberrechtsschutz erlischt in der Schweiz 70 Jahre nach dem Tod des Urhebers (Nach der Berner Übereinkunft sind Werke mindestens bis 50 Jahre nach dem Tod des Urhebers geschützt. Somit kann die Einspeisung eines Werkes auf eine Datenautobahn in einem Land mit niedriger Schutzfrist durchaus gesetzeskonform sind, das Kopieren in der Schweiz aber unter den Verbotsanspruch des Urhebers fallen, da das Werk hier aufgrund der Inländerbehandlung noch geschützt ist). Für Computerprogramme gilt eine Schutzdauer von 50 Jahren, welche ebenfalls mit dem Tod des Urhebers zu laufen beginnt.

4.2 Empfehlungen des Bundes

4.2.1 Empfehlung 10 – Sperrung bei Urheberrechtsverletzung

Die Empfehlung 1 ist auch dann zu beachten, wenn der Provider Kenntnis hat, dass bestimmte Netzinhalte gegen Urheberrechte oder verwandte Schutzrechte verstossen.

4.2.2 Empfehlung 11 – Klauseln im Abonnementsvertrag

Der Provider soll im Abonnementsvertrag auf die Pflicht zur Beachtung der Urheberrechte und der verwandten Schutzrechte hinweisen und sich das Recht vorbehalten, bei entsprechendem Verdacht den Anschluss vorsorglich zu sperren und bei Verletzungen das Vertragsverhältnis einseitig aufzulösen.

4.3 Kommentar zu den Empfehlungen des Bundes

Die Empfehlung 11 ist dahingehend zu erweitern, dass auf Verdacht hin eine Sperrung auch möglich ist, wenn es sich um von Dritten verbreitete bzw. abrufbar gehaltene Inhalte handelt, ansonsten der Provider damit rechnen muss, von seinen Kunden im Falle, dass sich der Verdacht nicht bewahrheitet, für die ungerechtfertigte Sperrung haftbar gemacht zu werden.

Gemäss URG stellt bereits der Upload auf den Server eine urheberrechtlich relevante Vervielfältigung dar, der nur mit Zustimmung des Inhabers der Urheberrechte erlaubt ist. Denn das URG weist dem Berechtigten vor allem das Recht zu, ein Werk „anderswo wahrnehmbar zu machen“, sowie Kopien des Werkes anzubieten, zu veräussern oder sonstwie zu verbreiten. Ohne Belang ist der Zweck der Veröffentlichung, der Schutz des URG greift unabhängig von der Motivation des Rechtsverletzers ein. Dies wird auch durch das internationale Urheberrecht gestützt. Die von der World Intellectual Property Organzation (WIPO) akzeptiereten neuen Verträge WIPO Copyright Treaty (WCT) und dem WIPO Performance and Phonograms Treaty (WPPT) sprechen von einem so genanntetn „making available right“. Dies besagt, dass auch die Verfügbarmachung urheberrechtlich geschützter Werke in der Weise, dass Angehörige der Öffentlichkeit an oder zu einem individuell von ihnen gewählten Ort oder Zeitpunkt auf geschützte Werke zugreifen können, erlaubnispflichtig ist. Die Schweiz hat die WIPO-Abkommen zwar unterschrieben, eine Umsetzung ins schweizerische Recht ist jedoch nicht vor 2002 zu erwarten.