Rainer KNYRIM

Cyber-Anarchie versus Old-Economy–Rechtsstaat

Inhaltsübersicht

1. Einleitung

Der Gesetzgeber in Österreich hat in den letzten Jahren verschiedene Maßnahmen getroffen, um neue Rechtsbereiche des IT-Rechts zu regulieren, etwa durch das neue Datenschutzgesetz 2000, das E-Commerce-Gesetz, das Telekommunikationsgesetz 2003. Diese neuen Gesetze sind in der Rechtstheorie viel versprechend, die praktische Durchsetzung erfüllt diese Erwartungen aber nicht. Zuständige Behörden reagieren zunächst nicht oder sehr spät auf Anzeigen. Beamte und Richter sind mit den neuen Materien immer wieder überfordert, in vielen Bereichen fehlt ausreichend geschultes Personal.[1] Dieser Beitrag im ersten „Jahrbuch Datenschutzrecht" soll einen Rückblick auf Fälle aus der anwaltlichen Praxis der letzten Jahre sowie einen Ausblick auf mögliche weitere Rechtsprobleme in der Zukunft – Stichwort Web 2.0 – geben. Der Beitrag beschränkt sich dabei nicht auf Datenschutzrecht sondern greift Fälle auf, die „Querschnittsmaterien" zwischen mehreren Rechtsgebieten beinhalten. Da es ein Praxisbericht ist, erhebt dieser Beitrag keinen Anspruch auf Wissenschaftlichkeit.

1 Siehe dazu auch *Kissling*, Cybertäter kommen ungeschoren davon, Computerwelt online vom 29.11.2004.

2. Fall 1: Internetserviceprovider vs. Betreiber eines Pyramidenspiels/Spam

Ein Betreiber eines Pyramidenspiels im Salzburgerland fiel deshalb auf, weil Internet-User eines Internetserviceproviders sich untereinander massenhaft Spam-Mails zu dessen Pyramidenspiel-Webseite zusandten und sich Kunden des Internetserviceproviders bei diesem über die Spammails beschwerten.

Da der Internetserviceprovider zu diesem Zeitpunkt gerade eine Werbekampagne gegen Spammer führte, beauftragte er seinen Rechtsvertreter, „aus allen Rohen zu schießen", um auszuprobieren, was die entsprechenden Gesetze in Österreich „bewirken" (bei dem Internetserviceprovider handelte es sich um die deutsche Tochtergesellschaft eines der weltweit größten Internetserviceprovider).

Das Pyramidenspiel funktionierte so, dass auf einer Website zum Mitspielen aufgerufen wurde und Mitspieler jeweils weitere Mitspieler suchen mussten (Pyramiden „aufbauen" mussten). Als Mindestverdienst wurden dabei über EUR 80.000,-- innerhalb von vier bis sechs Wochen in Aussicht gestellt. Nach einer schriftlichen Abmahnung durch den Rechtsvertreter des Internetserviceproviders im Juli 2003 „schoss" der Rechtsvertreter des Internetserviceproviders dann tatsächlich mit allen erdenklichen rechtlichen Möglichkeiten auf den Betreiber dieses Pyramidenspiels, der sich in seiner Antwort im Recht wähnte und sein Angebot als legales „Multi Level Marketing" bezeichnete:

- Es wurde eine Anzeige bei der zuständigen Staatsanwaltschaft eingebracht, die mehrere mögliche Rechtsgrundlagen anregte, unter anderem neben Betrug, Ketten- oder Pyramidenspiel[2], Störung der Funktionsfähigkeit eines Computersystems[3], Datenverwendung in Gewinn- oder Schädigungsabsicht[4] und über Ersuchen der Staatsanwaltschaft Hamburg auch noch § 6c deutsches UWG, der progressive Kundenwerbung verbietet.
- Bei der zuständigen Fernmeldebehörde wurde eine Anzeige wegen verbotenem Spamming nach § 107 TKG 2003 eingebracht, der Sanktionsrahmen beträgt dabei bekanntlich immerhin bis EUR 37.000,-- Geldstrafe.
- Schließlich wurde bei der zuständigen Bezirkshauptmannschaft eine Anzeige nach mehreren Rechtsgrundlagen eingebracht, nämlich nach E-Commerce-Gesetz wegen unklarer Angaben zu dem Gewinnspiel auf der Webseite[5] und wegen Nichtlöschung rechtswidriger Inhalte.[6] Der Sanktionsrahmen beträgt dabei allerdings bloß maximal EUR 3.000, -- Geldstrafe. Weiters wurde nach DSG 2000 ein Verstoß gegen die DVR-Meldepflicht angezeigt, da der Betreiber des Pyramidenspiels keinerlei DVR-Meldung hatte und die Datenanwendung vermutlich meldepflichtig war.[7] Der Sanktionsrahmen beträgt dabei maximal EUR 9.445, --, weiters können der Verfall der Daten und der Datenträger ausgesprochen werden. Schließlich beinhaltete die Anzeige an die zuständige Bezirkshauptmannschaft auch noch das Fehlen der Gewerbeberechtigung nach der Gewerbeordnung.
- Weiters wurde eine Anzeige[8] bei der Datenschutzkommission eingebracht, in der die Unzulässigkeit der sehr umfangreichen Verwendung von E-Mail-Kontaktadressen gerügt wurde, die der Betreiber des Pyramidenspiels als Teil des Spiels auf CD-ROMs anbot und zu denen er den Mitspielern empfahl, die dortigen E-Mail-Adressen zu kontaktieren, um sie für das Spiel anzuwerben.[9] Diese Anzeige wurde verbunden mit einem Ersuchen um Einbringung einer Strafanzeige oder einer zivilgerichtlichen Klage durch die Datenschutzkommission.[10]

Insgesamt wurden somit bei vier verschiedenen zuständigen Stellen Anzeigen eingebracht, gestützt auf 12 als Sanktionsmechanismen denkbare Normen aus sechs verschiedenen Gesetzen (darunter eines der BRD) die allesamt (auch) die Aufgabe haben, die „New Economy" zu schützen. Dies erfolgte zeitgleich im Juli 2003. Die Hoffnung, dass im schnellen „Internetzeitalter" auch die zuständigen Behörden rasch reagieren, wurde zu Nichte gemacht, denn einen ganzen Sommer lang geschah zunächst einfach nichts. Erst als im Herbst 2003 der Rechtsvertreter des Internetserviceproviders der Strafanzeige bei der Staatsanwaltschaft „nachtelefonierte", gelangte er zu einer örtlichen Polizeistelle, der er riet, die Adresse des Betreibers des Pyramidenspiels aufzusuchen, die dieser – was ungewöhnlich ist – erfreulicherweise im vollständigen Wortlaut auf der Webseite des Pyramidenspiels angegeben hatte, um dort vorhandene Computer zu beschlagnahmen. Tatsächlich war die Webseite am nächsten Tag offline, die Polizeibeamten hatten tatsächlich den Computer beschlagnahmt und dieser dürfte der Server der Webseite gewesen sein. Es zeigte sich somit, dass keiner der Anträge nach den verschiedensten neuen Normen aus dem IT-Bereich dazu führte, dass umgehend das Weiterlaufen des Pyramidenspiels im Internet beseitigt wurde, sondern dass die „gute alte Polizeiarbeit" letztlich das Problem durch Beschlagnahme des Beweisgegenstandes faktisch löste.

Die vom Internetserviceprovider dennoch bewusst fortgeführten Anzeigen ließen in der Folge an Skurrilität kaum zu wünschen übrig: Nachdem sich der Rechtsvertreter des Internetserviceproviders bei der zuständigen Bezirkshauptmannschaft über Wochen hin von Sachbearbeiter zu Sachbearbeiter durchtelefonierte und sich einer nach dem anderen für die Rechtsmaterien Datenschutzgesetz und E-Commerce-Gesetz für unzuständig erklärte, drohte er dem Bezirkshauptmann im Dezember 2003 schriftlich einen Devolutionsantrag an. In seinem Antwortschreiben nannte der Bezirkshauptmann dann Sachbearbeiter, bei denen es sich um jene handelte, die bereits mehrfach vorher ihre negative Zuständigkeit bekannt gegeben hatten und mit der Materie vom Bezirkshauptmann nun doch erstmalig in ihrer Laufbahn „zwangsbeglückt" wurden. Gerade zu humoristisch war die Frage des für die Anzeige nach Datenschutzgesetz nun als zuständig nominierten Sachbearbeiters an den Rechtsvertreter, was er denn nun tun solle, der Rechtsvertreter solle ihm in dieser Materie weiterhelfen. Spätestens

2 § 168a StGB.
3 § 126b StGB (wegen der Aufforderung zum Spammen, die dem Spiel immanent war).
4 § 51 DSG 2000.
5 § 6 Abs 1 E-Commerce-Gesetz.
6 § 16 Abs 1 Z 2 E-Commerce-Gesetz.
7 § 52 Abs 2 DSG 2000, zuständig ist ebenfalls die Bezirksverwaltungsbehörde.
8 § 30 Abs 1 DSG 2000 diente als Rechtsgrundlage, siehe dazu näher *Knyrim*, Praxishandbuch Datenschutzrecht (2003), 233f.
9 Nach eigener Aussage hatte er diese CD-ROMs, die rund 1 Mio E-Mail-Adressen enthielten, bei ebay ersteigert.
10 Diese Möglichkeit steht der Datenschutzkommission nach § 30 Abs 6 DSG 2000 zu.

in diesem Moment zeigte sich, dass die Idee, die Kompetenz zur Verhängung der Verwaltungsstrafen im Datenschutzrecht auf die Bezirksverwaltungsbehörden auszulagern, jene war, die dem Datenschutzrecht in Österreich ganz offensichtlich am wenigsten zum Durchbruch verholfen hat. Dabei ist den Beamten und Vertragsbediensteten der Bezirksverwaltungsbehörden kein Vorwurf zu machen, sondern dem Gesetzgeber, der höchst komplexe Materien wie etwa das Datenschutzgesetz oder das E-Commerce-Gesetz auf Stellen auslagert, die mit diesen noch nie zu tun hatten sowie der Verwaltung, die diesen dann nicht die notwendigen Schulungen in dieser Materie zuteil werden lässt.

Nach einem Urgenzschreiben antwortete Anfang 2004 auch die Datenschutzkommission und teilte mit, dass sie ihrerseits bei der Bezirkshauptmannschaft eine Anzeige eingebracht habe und eine Verfolgung bei dieser urgiert habe und ihr eine sofortige Bearbeitung zugesagt wurde. Die Datenschutzkommission führte sogar aus, dass, was den „Handel" mit den E-Mail-Adressen betreffe, soweit die Adressen nicht von einer der in § 17 Abs 2 DSG 2000 aufgezeigten Ausnahmen erfasst seien, dies einen weiteren Verstoß gegen die Registrierungspflicht bedeuten könne. Möglicherweise sei, so die DSK in ihrem Schreiben, sogar der gerichtliche Straftatbestand der Datenverwendung in Gewinn- oder Schädigungsabsicht[11] erfüllt. Die Datenschutzkommission teilte jedoch mit, dass sie mangels Zuständigkeit zur Strafverfolgung diesbezüglich nicht weiter tätig werden könne und ihr auch ein Einschreiten nach § 30 DSG 2000 nicht möglich sei (was sie bereits in einem Schreiben im September 2003 mitgeteilt hatte). Erfreulicherweise hatte die Datenschutzkommission in diesem Fall sogar auf Anregung des Rechtsvertreters hin selbst Anzeige bei der zuständigen Bezirkshauptmannschaft eingebracht. Im Endeffekt ging sie jedoch nicht weiter nach § 30 DSG 2000 vor. Leider ist festzustellen, dass die Datenschutzkommission Betroffene regelmäßig auf den Zivilrechtsweg verweist und nicht aktiver selbst im Rahmen ihrer Möglichkeiten vorgeht. So gab es bis 2007 „gerüchteweise" erst ein einziges Zivilverfahren, in dem sich die Datenschutzkommission als Privatbeteiligte angeschlossen hatte. Eine zivilgerichtliche Klage, die die Datenschutzkommission nach § 30 Abs 6 Z 4 DSG 2000 selbst bei schwerwiegenden Verstößen durch Auftraggeber des privaten Bereichs eingebracht hätte, ist dem Autor bislang nicht bekannt. Auch hier trifft der Vorwurf aber auch wieder die öffentliche Verwaltung, die die Geschäftsstelle der DSK seit Jahren mit einem im internationalen Vergleich geradezu peinlich niedrigen Personalstand ausstattet.[12]

Die Hoffnung, dass das zuständige Fernmeldebüro den Strafrahmen von EUR 37.000,--[13] wegen unzulässigen Spammings rasch ausschöpfen würde, wurde ebenfalls zerstört: Aufgrund mehrfacher telefonischer Nachfragen erfuhr der Rechtsvertreter des Internetserviceproviders, dass das Fernmeldebüro an akutem Personalmangel litt, da ein Jurist gekündigt hatte und ein anderer sich in längerem Krankenstand befinde. Einige Monate später wurde dem Rechtsvertreter die erfreuliche Nachricht am Telefon überbracht, dass „in wenigen Monaten" wieder ein Jurist verfügbar sei, der sich um die Anzeige kümmern werde. Tatsächlich teilte das Fernmeldebüro dann im November 2004, also 16 Monate (!) nach Einbringung der Anzeige mit, dass tatsächlich gegen den Beschuldigten aufgrund der Anzeige ein Verwaltungsstrafverfahren eingeleitet worden sei. Wie weit dieses gediehen sei, wollte man jedoch nicht beauskunften und berief sich darauf, dass der Internetserviceprovider im Verfahren nach § 107 TKG 2003 keine Parteistellung genieße und ihm daher Auskünfte über den Verlauf und den Ausgang des Verfahrens nicht erteilt werden könnten. Der Ausgang des Verfahrens vor der Fernmeldebehörde wird somit ewig ungewiss bleiben, ebenso der Ausgang der Anzeigen bei der zuständigen Bezirkshauptmannschaft, die im Laufe der Bearbeitung ebenfalls auf das Argument der mangelnden Parteistellung und den daher zu wahrenden Datenschutz einschwenkte.

11 § 51 Abs 1 DSG 2000.

12 Siehe dazu die Statistik im Jahresbericht der Datenschutzkommission 2007, online unter www.dsk.gv.at.

13 § 109 Abs 3 Z 20 TKG 2003.

Das Argument der mangelnden Parteistellung ist für Anzeiger äußerst frustrierend und der Rechtsentwicklung und Rechtssicherheit im „Cyberspace" sicherlich nicht förderlich, wenn diejenigen Privatpersonen, die es auf sich nehmen, auf ihre Kosten und Mühen Anzeigen einzubringen, um dem Recht zum Durchbruch zu verhelfen, am Schluss keinerlei Informationen darüber erhalten, ob und wie ihre Anzeige erledigt wurde. Es wäre sehr erfreulich, wenn man – in Anlehnung an § 30 Abs 7 DSG 2000 – auch für Anzeigen nach § 52 DSG 2000, E-Commerce-Gesetz und § 107 TKG 2003 gesetzlich festhält, dass der Anzeiger zumindest über die Art und Weise der Erledigung seiner Anzeige informiert wird, wenn ihm schon keine Parteienstellung zuerkannt wird. Anzumerken ist, dass eine der häufigsten an den Autor dieses Beitrags gestellten Fragen ist, „wie denn die Strafpraxis im Datenschutzrecht sei", und niemand darüber Auskunft geben kann, da es keinerlei statistisches Material zu geben scheint. Nicht einmal die Datenschutzkommission selbst wird mehr von den Bezirksverwaltungsbehörden über Anzeigen und deren Erledigungen informiert, was diametral entgegengesetzt zur Datenschutzpolitik vieler anderer europäischer Länder ist, wo die verhängten Strafen der Datenschutzbehörden aus generalpräventiven Überlegungen umgehend „publikumswirksam" in den Medien veröffentlicht werden.[14]

Nachdem versucht wurde, dem zuständigem Bezirksgericht im Strafverfahren seitens des anzeigenden Internetserviceproviders im Rahmen einer Rechtshilfeeinvernahme in Deutschland und umfangreicher Schriftsätze die verschiedenen, oben zitierten Tatbestände des Strafgesetzbuches zur Computerkriminalität[15] verständlich zu machen, verurteilte das Bezirksgericht den Betreiber des Pyramidenspiels schließlich im April 2005 wegen des Vergehens des Ketten- bzw Pyramidenspiels nach § 168a Abs 1 und 2 StGB zu 50 Tagessätzen à EUR 3,--, also in Summe zu EUR 150,--. Der Verurteilte berief gegen das Urteil, die zweite Instanz bestätigte das Urteil der ersten Instanz im März 2006. EUR 150,-- Geldstrafe blieben somit das einzig bekannte Ergebnis nach knapp drei Jahren Verfahren in diesem „Cyberkrieg". Der Krieg ging verloren, weil die vermeintlichen scharfen Schwerter, die der Gesetzgeber geschmiedet hatte, am „Schlachtfeld" nicht aus ihren Scheiden gezogen wurden. Oder lag es daran, dass es sich nicht um Schwerter, sondern um Hightech-Waffen in einem Technologiekrieg handelt, die zu komplex zu bedienen sind?

14 So etwa in England oder Spanien, wo die Strafen der Datenschutzbehörden so publiziert werden, dass sogar in deutschsprachigen Medien über diese berichtet wird, regelmäßig etwa auf www.heise.de, gelegentlich sogar auf www.futurezone.orf.at.

15 Siehe jüngst *Bergauer*, Computerwürmer und Gemeingefährdungsdelikte im Strafrecht, jusIT 2008, 2.

3. Fall 2: Mobilfunkbetreiber vs. Privatdetektiv

In diesem Fall „zapfte" ein österreichischer Privatdetektiv die Standortkennungen (Cell-ID) der Sendemasten (Base Stations) eines österreichischen Mobilfunkbetreibers an, um damit Standortbestimmungen zu machen. Er bot gewerblich die Ortung von Mobiltelefonen, die er mit einem speziell konfigurierten Zusatzstecker adaptierte, über eine von ihm betriebene Onlineplattform an. Unter anderem bewarb er mittels Spammail die österreichischen Rechtsanwälte, denen er sein System etwa zur „Beweissicherung" in Scheidungsverfahren empfahl. Wie sich der Autor dieses Beitrages selbst nach einem „Testkauf" überzeugen konnte, funktionierte das Ortungsystem erstaunlich präzise, in Wien etwa auf rund 150 Meter, Überland auf wenige Kilometer genau. Das Orten wurde so durchgeführt, dass an das vorher präparierte und bei der zu überwachenden Person deponierten Handy (etwa im Kofferraum versteckt oder unter dem Auto befestigt – eine „Montagenleitung" dafür war dem Geräte beigepackt) – eine SMS gesandt wurde, die die vom Handy gerade empfangene Cell-ID auslas und per SMS an das System des Detektivs zurücksandte, wo diese Cell-ID mit einer vorher durch das „Abfahren" Österreichs erstellten elektronischen Karte der Cell-ID verglichen wurde und so der aktuelle Standort des Geräts binnen weniger Sekunden auf der Internetplattform des Detektivs mit einem vorher von ihm vergebenen Passwort abgerufen werden konnte. Man konnte mit dem System ganze Bewegungsprofile der überwachten Person erstellen. Überdies konnte man mittels SMS das durch den Zusatzstecker adaptierte Gerät so steuern, dass dieses unbemerkt Anrufe von selbst annahm und man damit auch abhören konnte. Der Detektiv konnte das System ausschließlich deswegen betreiben, weil er das Netz eines Mobilfunkbetreibers verwendete, um aus diesem ständig die Cell-IDs „abzusaugen". Nach einer erfolglosen Abmahnung im Frühjahr 2004 erhielt der Rechtsvertreter der Mobilfunkbetreiberin den Auftrag, wegen sittenwidriger Ausbeutung fremder Leistung mit Klage und Antrag auf einstweilige Verfügung am Handelsgericht Wien gegen den Privatdetektiv vorzugehen.

Trotz des Versuches, durch längere vorbereitende Schriftsätze dem Gericht die Mobilfunktechnologie und das System der Ausbeutung der Leistungen des Mobilfunkbetreibers durch den Detektiv zu erklären, schloss sich das Handelsgericht Wien den sehr plakativen und vereinfachten Darstellungen des gegnerischen Anwaltes an, die inhaltlich unzutreffend waren, aber für einen technischen Laien sehr nachvollziehbar klangen und wies den Antrag auf einstweilige Verfügung ab. Dies im Wesentlichen mit der Begründung, dass der beklagte Privatdetektiv nicht die Daten der klagenden Mobilfunkbetreiberin übernehme, um ihr im eigenen Segment der Mobiltelefonie Konkurrenz zu machen, sondern dieser vielmehr ein Zusatzprodukt anbiete, welches geeignet sei, eine andere Dienstleistung als die der Mobiltelefonie anzubieten. Im Vergleich setze beispielsweise „auch ein Anrufbeantworter voraus, dass das Telefon und die Telefonleitung funktionieren, auch hier liegt noch keine Ausbeutung fremder Leistung vor, ebenso wenig wie beim Tunen eines Markenfahrzeugs".[16]

Die Berufungsentscheidung des OLG Wien vom März 2005 gab dem Mobilfunkbetreiber recht, das Berufungsgericht hatte ein besseres Verständnis für den technisch durchwegs schwierigen Sachverhalt und führte aus, dass die Rechtsrüge zutreffend geltend mache, dass die Vorgangsweise des Beklagten als sittenwidrig im Sinne des § 1 UWG zu beurteilen sei. Der Privatdetektiv führte das Verfahren bis zum Obersten Gerichtshof weiter, dieser gab dem Berufungsgericht Recht und hielt fest, dass die Ausbeutung von fremden Daten zu Geschäftszwecken ohne Bezahlung eines entsprechenden Entgelts sowie ohne eigenen Schaffensvorgang unzulässig sei.[17] Dieser Fall zeigte deutlich, wie schwer es für ein „allgemeines" Gericht ist, einen in der Mobilfunk- und IT-Technologie gleichzeitig angesiedelten Fall technisch richtig zu erfassen und dies über die Instanzen zu absolut konträren rechtlichen Beurteilungen des technischen Sachverhalts führen kann.

16 HG Wien 18 Cg 71/04m v. 18.8.2004.

4. Fall 3: Berufsvertretung vs Domaingrabber

Eine Berufsvertretung wollte bei Einführung der so genannten IDN-Domains im März 2004 eine Domain registrieren, die ihren Namen, jedoch mit dem Umlaut „ä" geschrieben, enthielt. Die Registrierung schlug fehl, denn ein deutscher Domaingrabber erhielt diese Domain zugeteilt. Die Berufsvertretung klagte auf Unterlassung der Aufrechterhaltung der Domainregistrierung und Übertragung oder Löschung der Domainregistrierung beim Handelsgericht Wien im Jahr 2004. Geltend gemacht wurde eine sittenwidrige Behinderung durch Domaingrabbing (§ 1 UWG), eine Irreführung durch den Domainnamen (§ 2 UWG)[18] und Verletzung von Namensrechten (§ 43 ABGB). Der OGH konnte zwei Jahre später darüber entscheiden: Er gab der Berufsvertretung aufgrund von § 43 ABGB recht, die Entscheidung wurde bereits in der Literatur besprochen.[19]

Zum Übertragungs- und Löschungsbegehren[20] führte der OGH in dieser Entscheidung aus: „Die Kläger begehren weiters, den Beklagten schuldig zu erkennen, die Domain auf den Erstkläger zu übertragen. Ihr Anspruch muss schon daran scheitern, dass sie die Voraussetzungen für eine Herausgabe und damit einen Übertragungsanspruch nicht behauptet haben." Im Ergebnis erhielt die Berufsvertretung zwar inhaltlich nach einer ausführlichen Begründung durch den OGH Recht, erhielt die Domain jedoch nicht übertragen. Die Domain wurde entsprechend dem Urteil des OGH vom Beklagten jedoch wieder zur Registrierung freigegeben und die Berufsvertretung versuchte zum zweiten Mal, die Domain zu registrieren. Wieder kam ihr jedoch ein Domaingrabber – diesmal mit Hilfe eines österreichischen Domaincatchers – zuvor und registrierte diese über eine „Briefkastenfirma" mit Adresse „M... Holding Inc., First Floor ... Building, 00000, Port Villa, VU".[21] Da die Schlichtungsstelle für nic.at, wo die Domain registriert war, nicht verpflichtend war, hätte eine neuerliche Klage unter Umständen in Vanuatu zugestellt werden müssen. Sicherheitshalber wurde zunächst wieder bei nic.at der „Wartestatus" beantragt und statt einer Klagseinbringung zunächst

17 4 Ob 113/05d vom 15.9.2005, siehe etwa kurier.at „Detektiv darf keine Handys orten" vom 1.12.2005.

18 In der jeweils damals gültigen Fassung des UWG.

19 OGH 24.2.2006, 4 Ob 165/05a, siehe etwa ecolex 2006/287 = MR 2006, 215 = wbl 2006/132 = RdW 2006/468.

20 Zum Löschungsanspruch siehe jüngst wieder OGH 2.10.2007, 17 Ob 13/07x, EvBl 2008/028 = jusIT 2008, 14 = ÖBl 2008/16.

21 VU steht für die Republik Vanuatu in der Südsee.

ein Brief an nic.at geschrieben, mit dem Hinweis, dass die Registrierung nicht den nic.at Geschäftsbedingungen entspreche und entgegen den Geschäftsbedingungen von nic.at die Domain offensichtlich nicht gutgläubig registriert wurde, da die Entscheidung des OGH zum Sachverhalt bereits hinreichend publiziert worden war. Nic.at widerrief erfreulicherweise das Vertragsverhältnis mit dem Domaininhaber nach einem erfolglosen Zustellversuch und die Domain wurde einer Neuvergabe zugeführt. Die Berufsvertretung wollte diesmal kein Risiko eingehen und beauftragte ihrerseits jenen österreichischen Domaincatcher, der bei der vorigen Registrierung die Domain „geschnappt" hatte. Diesem Domaincatcher gelang es jedoch diesmal nicht, die Domain zu erhalten. Auch der dritte Anlauf, die Domain zu registrieren scheiterte erneut und die Domain wurde wieder auf einen Domaincatcher aus Deutschland registriert. Um sich weitere Kosten zu ersparen (mittlerweile waren zwei Rechtsanwaltskanzleien in dem Verfahren tätig gewesen), dürfte sich die Berufsvertretung letztlich außergerichtlich mit dem deutschen Domaincatcher geeinigt haben, der diese beim letzten Anlauf „registriert". Dieser Fall zeigte, dass technisch versierte Personen im Internet die Oberhand behalten und auch jahrelanges Prozessieren bis zum Obersten Gerichtshof und eine gute rechtliche Ausgangslage erfolglos gegen dieses technische Können sein können. Es bleibt daher zu überlegen, ob diese Situation durch eine gesetzliche Stärkung des rechtmäßigen Domain(nicht)inhabers auf Vollzugs- und Sanktionsseite verbessert werden könnte.

5. Zwischenbilanz: Betroffene Rechtsbereiche im „Cyberspace"

Die oben angeführten Fälle waren einige durchwegs typische Beispiele, die zeigen, dass im „Cyberspace" sehr rasch und einfach Rechtsverletzungen gesetzt werden, die, wenn überhaupt, nur durch sehr langwierige und kostspielige, teilweise frustrierende Prozesse und Verwaltungsverfahren korrigiert werden können. Ein Rechtsrahmen ist zwar vorhanden, führt aber nicht zum gewünschten, raschen und durchschlagenden Erfolg in der Praxis. Typische Rechtsbereiche sind:

- Sittenwidriges Verhalten (§ 1 UWG Ausbeuten fremder Leistungen, Domaingrabbing).
- Verletzung von Namensrechten (§ 43 ABGB) durch Domaingrabbing.
- Spamming (§ 107 TKG).
- Illegale Datenverwendung (§§ 51 und 52 Abs 1 DSG 2000).
- Verstoß gegen DVR-Meldepflichten (§ 52 Abs 2 DSG 2000).
- Betrug, illegale Geschäftsmodelle, Computerkriminalität (StGB, insbesondere die „Computerstraftatbestände").
- E-Commerce-Gesetz-Verstöße (Kennzeichnung, Haftung für Inhalt).
- Fehlende Gewerbeberechtigung nach der Gewerbeordnung.

6. Weitere Problemfelder und Fälle im „Web 2.0"

Mit dem „Web 2.0", dem Internet der „Communities", wo nicht mehr wie im „Web 1.0" überwiegend Unternehmen mit Verbrauchern korrespondieren, sondern in User-Plattformen Nutzer in unterschiedlichsten Zusammensetzungen

miteinander in Verbindung treten, zeigen sich weitere Problemfelder, die den Kampf des „Old-Economy-Rechtsstaates" gegen den „Cyberspace" noch verkomplizieren.

Zu bemerken ist etwa, dass sich Urheberrechtsverstöße mittlerweile nicht nur massenhaft im Bereich von Musik und Film bewegen, sondern dass in Web 2.0-Anwendungen wie etwa der virtuellen 3D-Welt „Second Life" auch Urheberrechtsverstöße im Bereich Architektur, Design,[22] ebenso Missbrauch von Namensrechten und Markennamen stark zunehmen.[23] Auch der Missbrauch von Bildrechten wird weiter forciert, etwa dadurch, dass Nutzer in ihre persönlichen Profile zB auf „flickr.com" oder „facebook.com" wahllos Bilder aus dem Internet kopieren und auf ihren Profilen verwenden. Taucht man in die neuen Web 2.0-Welten ein, ist man geradezu an die „rechtsfröhlichen Zeiten" des Beginn des Internets im ersten großen Hype vor rund 10 Jahren erinnert, als das Internet von manchen bewusst als rechtsfreier Raum propagiert wurde. Auch das Web 2.0 scheint bei den Usern wieder den Eindruck zu erwecken, dass in diesem alles erlaubt ist.

Ein Problem, das gerade in dem Community-Gedanken des Web 2.0 verstärkt auftritt ist, dass dieser von Einzelpersonen dazu missbraucht wird, andere Personen oder Personengruppen gezielt in ein schlechtes Licht zu rücken und herabzuwürdigen, wobei ebenfalls nicht Rücksicht genommen wird, ob damit vielleicht Straftatbestände wie etwa Verleumdung verwirklicht werden. Dies ist umso bedenklicher, als viele User verstärkt der Ansicht sein dürften, dass das, was im Internet etwa auf wikipedia.com oder wikpedia.de zu finden ist, den Anspruch auf absolute Richtigkeit hat. Dieses Phänomen wurde bereits unter dem Schlagwort „Wikiality" bekannt, einer Zusammensetzung der Wörter „Wikipedia" und „Reality", das die von den Inhalten von Wikipedia geschaffene Scheinrealität und Scheinrichtigkeit bezeichnet.[24] Ein Beispiel für die „Verleumdung" ganzer

22 Etwa das Kopieren ganzer Gebäude der realen Welt und von Designgegenständen zum kommerziellen Verkauf als Ausstattungsgegenstände in dieser virtuellen Welt.

23 Die für die virtuellen Welten kopierten, aus der realen Welt nachgebauten Gegenstände werden unter den Originalnamen und Marken im Verkauf angeboten. Markennamen werden verstärkt als Suchwörter für Produkte und Dienstleistungen aller Art missbraucht. Gibt man etwa im Suchfeld von „Second Life" den Markennamen „Nike" ein, erhält man als Suchtreffer Angebote für Onlineglücksspiel und Online-Pornografie in Second Life.

24 Der Autor dieses Beitrages konnte sich von diesem Phänomen überzeugen, dem teils auch die „Redakteure" von Wikipedia selbst verfallen zu sein scheinen: Ende 2006 fand sich auf wikipedia.de unter dem Titel „Bundesgesetz über den Schutz personenbezogener Daten" ein kurzer Beitrag über das österreichische Datenschutzgesetz von einem Benutzer mit Namen „McMer", der von sich aus angab, dass er deutsche Firmen hinsichtlich ihrer Datenverarbeitung berate. Sein Beitrag enthielt bereits im allerersten Absatz zwei „Halbrichtigkeiten", nämlich dass personenbezogene Daten in Österreich ohne vorherige Zustimmung des Betroffenen nicht weitergegeben werden dürfen (was, wenn man § 8 Abs 1 DSG 2000 liest, nicht stimmt) und dass weiters die Datenschutzkommission durch das DSG 2000 gegründet wurde (was ebenfalls nicht korrekt ist, da die Datenschutzkommission bereits mit dem DSG 1978 eingerichtet wurde). Der Autor dieses Beitrages machte sich die Mühe, einen Arbeitstag lang diesen Artikel in wikipedia.de umfangreich zu überarbeiten. Nachdem er diesen auf wikipedia.de online gestellt hatte, wurde dieser als „Sabotageakt" von einem anderen User wieder gelöscht (dieser User bezeichnete sich in seinem

Berufsstände und einzelner Vertreter desselben war etwa eine von einem österreichischen Verein betriebene Webseite, die der Webseite wikipedia.de täuschend ähnlich sah und auch einen ähnlichen Namen hatte. In deren Bloßstellungen waren österreichische Richter, Rechtsanwälte und Staatsanwälte enthalten und es wurde aufgerufen, weitere negative Berichte unter Namensnennung der betroffenen Person auf dieser Community-Seite online zu stellen.[25] Ein Strafverfahren gegen die Hauptakteure, die hinter dieser Webseite standen, wurde relativ rasch eingeleitet, zunächst bestand allerdings das Problem, dass eine derartige Menge an Staatsanwälten und Richtern verschiedener Gerichte vor allem in Ostösterreich mit negativen Artikeln „bloßgestellt" wurden, dass erst eine Staatsanwaltschaft in Westösterreich gefunden werden musste, die unbefangen war, weil auf der Webseite nicht erwähnt. Die Hauptakteure der Webseite hatte sich überdies eines Domainregistrierung- Anonymisierungsdienstes aus den USA bedient, der erst nach detaillierter schriftlicher Schilderung der Verleumdungshandlungen und Hinweis auf die Strafbarkeit des Sachverhalts den Namen des registrierenden Vereins bzw der registrierenden Person herausgab.

Ein anderer Fall ging für die Betroffenen eher unerfreulich aus und zeigte erneut, wie alleine gelassen Unternehmen teilweise mit ihren Problemen bleiben: Eine radikale englische Tierschutzorganisation betrieb eine europaweite Kampagne gegen Pharmaunternehmen, die angeblich Tierversuche bei einer bestimmten Tierversuchsfirma in Großbritannien durchführen. Die Tierschutzorganisation führte in Wien einen „Aktionstag" durch, bei dem sie unter anderem vor verschiedenen Pharmaunternehmen demonstrierten, teilweise an den Privatadressen der Geschäftsführer der Unternehmen Flugzettel in die Briefkästen und Autos verteilte, in denen die Nachbarschaft darüber informiert wurde, dass sie mit einem „Tiermörder" zusammenlebe, zumindest in ein Büro wurde auch von mehreren Aktivisten unter der Vorgabe, ein Botendienst zu sein, eingedrungen und dort eine „Demonstration" in den Büroräumen (unter Anwesenheit einer einzigen Freitagnachmittagssekretärin) abgehalten und von dieser Aktion Fotos geschossen. Die Fotos der Innenräume wurden mit Namensnennung des Unternehmens danach auf einer Tierschutz-Community-Webseite als „Erfolgsstory" über die Demonstration publiziert. Dies mit dem unrichtigen Zitat der anwesenden Sekretärin, dass diese ihre Arbeit in dem Unternehmen hasse und ohnehin soeben ihren Job gekündigt habe. Da diese Sekretärin nach der „Demonstration" sofort die Polizei gerufen hatte, gelangte der Sachverhalt zu einer polizeilichen Aufnahme. Da es sich, wie aus der Webseite der Tierschutzorganisation zu entnehmen war, um eine europaweit konzertierte Aktion handelte, befasste sich in der Folge das Landesamt für Verfassungsschutz und Terrorismusbekämpfung mit dem Fall, allerdings für das betroffene Unternehmen ohne sichtlichen Erfolg. Weder unterstützte das Landesamt dabei, den unrichtigen Text von der Webseite der Tierschutzorganisation zu entfernen, noch konnte es verhindern, dass wenige

eigenen Profil auf wikipedia.de als Spezialist unter anderem für historische Seeschifffahrt) und erst nach einer kurzen, aber heftigen Diskussion mit diesem über die Qualität und Richtigkeit des ersten und des überarbeiteten Artikel wurde der überarbeitete Artikel online gestellt.

25 Es wurde etwa vorgeschlagen für Richter folgende Informationen aufzunehmen „ist Mitglied beim Verein XXX, bei der Burschenschaft XYZ ... ist Obmann des Vereins „Richter für Demokratie" mit Sitz in Nordkorea, ist verheiratet, lebt in Scheidung, hat 5 uneheliche Kinder, ...".

Wochen später ein zweites Mal in das Büro eingedrungen wurde und diesmal ein Demonstrant Mineralwasser in den Server des Unternehmens leerte. Dieser Vorfall fand sich wenige Stunden später wieder im Internet, dennoch erhielt der Rechtsvertreter des Pharmaunternehmens vom Landesamt die Auskunft, dass man keinerlei Informationen über den Stand der Ermittlungen mitteilen könne, denn die Sache sei geheim, man sei der Geheimdienst. Dies trotz des Hinweises, dass von einem Geheimnis wohl kaum gesprochen werden könne, wenn die Aktion vollständig im Internet nachzulesen sei. Somit blieb auch diesem Unternehmen – wie so vielen Unternehmen – keine andere Möglichkeit, als auf eigene Kosten und Mühen gegen die Tierschutzorganisation vorzugehen. Als kostengünstigster und raschester Weg erwies sich, die Haftung des Internetproviders anzusprechen. Es handelte sich dabei um einen niederländischen Internetprovider, der erfreulicherweise sogar ein eigenes Formular für das Ansprechen seiner Haftung auf seine Serviceseiten bereit stellte und nach Onlineeingabe des Sachverhaltes binnen sehr kurzer Frist reagierte und bekannt gab, dass er die „Beschwerde" an den Betreiber der Webseite der Tierschutzorganisation weitergegeben habe. Tatsächlich wurden daraufhin binnen weniger Stunden von der Tierschutzorganisation die Innenaufnahmen gegen Straßenansichten des Pharmaunternehmen ausgetauscht und der Bericht über die „Demonstration" im Büro und die falsche Aussage der Sekretärin wurden offline gestellt und durch eine allgemeine Androhung ersetzt, dass man wieder kommen werde.

Es zeigt sich somit, dass gerade der Community-Gedanke des Web 2.0 es Einzelpersonen leichter macht, die vermeintlich richtige Realität zu ihren Gunsten oder zu Lasten anderer zu verändern. Durch die immer weiter stattfindende Verschmelzung von Realität und Fiktion wird für andere User immer schwerer, Richtiges von Falschem zu unterscheiden. Und für Betroffene wird es immer schwieriger, mit den Rechtsbehelfen der „Old-Economy" gegen diese Probleme des Cyberspace vorzugehen. Dies vor allem in der notwendigen Geschwindigkeit des Internets.

Datenschutzrecht ist dabei ein Teil davon, der immer wichtiger wird, da er mittlerweile nicht mehr nur dem „Drittschutz" dient (dem Schutz davor, dass Dritte unzulässigerweise oder unrichtige Daten über einen verarbeiten) sondern auch dem „Selbstschutz", da ein weiteres, immer häufiger auftretendes Problem ist, dass Internetuser unter ihrem Namen in Communities des Web 2.0 Informationen über sich preisgeben oder Kommentare schreiben,[26] die für sie später dann – etwa bei der Arbeitssuche – schädlich sein können.[27] Da das vermeintlich schnelle und kurzlebige Internet aber durch die Internet-Suchmaschinen[28] ein erstaunlich langes „Gedächtnis" hat und derartige, in unüberlegten Sekunden onlinegestellte Texte womöglich jahrelang nachzulesen sind, ist gerade die Ausübung der Widerspruchs- und Löschungsrechte bei der Verwendung eigener Daten ein immer stärker werdendes Thema. Exemplarisch dafür war die kürzlich erfolgte telefonische Anfrage an den Autor dieses Artikels, ob dieser nicht Google klagen könne, da bei der Eingabe des Namens des Anrufers ein drei

26 etwa in Blogs, Onlinetagebüchern, Kommentarseiten oder Diskussionsforen.

27 Dieses Thema war Inhalt einer großen Podiumsdiskussion mit dem Titel „Das Ende der Privatheit" des von der Wirtschaftskammer Salzburg in Kooperation mit der Universität Salzburg im Rahmen der IRIS 2008 veranstalteten UBIT-Zukunftsforum 2008 am 21. Februar 2008.

28 Siehe dazu *Weichert*, Datenschutz bei Suchmaschinen, MuRInt 2007, 188.

Jahre alter, polemischer Kommentar von diesem selbst auf einer Webseite für eine bestimmte Sportart gefunden wurde, der nach Inhalt und Ausdrucksweise für den Betroffenen selbst sehr schädlich war. Der Anrufer, der gerade auf der Suche nach einem neuen Job in der IT-Branche war, fürchtete, dass potentielle Arbeitgeber rasch auf diesen von ihm selbst verfassten Kommentar stoßen würden und ihn daher nicht einmal zu Bewerbungsgesprächen einladen würden. Die Vision, den ersten diesbezüglichen Musterprozess eines Österreichers gegen Google als Privatperson zu führen, stieß den Anrufer ab und er nahm den Rat an, sich zuerst mit dem Betreiber der Webseite dieser Sportart, auf der der Originaltext gepostet war, wegen einer Löschung desselben in Verbindung zu setzen.[29]

Wenn der Community-Gedanke des Web 2.0 längerfristig ohne Schaden für den Betroffenen funktionieren soll, sind die Unternehmen daher aufgefordert, nicht nur selbst die Daten der User zu schützen, sondern auch die User davor zu schützen, dass sie sich nicht selbst schädigen. Ein Bemühen um den Datenschutz wird sich dabei aber nicht bloß darauf reduzieren lassen können, dass man die gesetzlichen Bestimmungen einhält.[30] Vielmehr wird es Aufgabe sein, durch technische Maßnahmen und durch die Strukturierung die Communities so zu gestalten, dass User dort sich nicht selbst schaden können und Inhalte dort von den Usern auch wieder selbst gelöscht werden können.[31]

Selbstverständlich ist aber auch, dass das Unternehmen die Daten Dritten gegenüber möglichst schützt. Als Negativbeispiel eines Web 2.0-Unternehmens, das sämtliche Haftung für Datenschutz abgeben zu versucht, sei an dieser Stelle die Firma Linden Lab genannt, Betreiberin der virtuellen Welt „Second Life"[32] in deren AGB es in Punkt 6.1. heißt: „Linden Lab will not give any of your personal information to any third party without your express approval except: ... to comply with tax and other explicable law; ... to law enforcement or other appropriate third parties in connection with criminal investigations and other investigations of fraud; or as otherwise necessary to protect Linden Lab, its agents and other users of the service. Linden Lab does not guarantee the security of any of your private transmissions against any authorized or unlawful interception or access

29 Selbst wenn der Text dort gelöscht ist, kann er aber noch lange als Screenshot im Cache von Google verfügbar sein.

30 Zitat aus den AGB von parship.at, einer Online-„Partnervermittlungsbörse": „parship.at geht mit dem Thema Sicherheit höchst verantwortungsvoll um und verpflichtet sich deshalb, die gesetzlichen Bestimmungen zum Datenschutz unbedingt einzuhalten". Diese Angabe ist für parship.at aber eigentlich nicht zutreffend, denn tatsächlich hat parship.at sich offensichtlich Gedanken gemacht, wie es die User der Plattform vor sich selbst schützen könnte und codiert deren Namen bzw gewählten Usernamen automatisch mit einer Buchstaben- und Zahlenkombination.

31 Die beliebte Online-Community www.facebook.com etwa bestimmt in ihrer Privacy Policy (nach amerikanischem Recht), dass die Daten, die der User dort eingibt, nicht diesem gehören, sondern dem Betreiber der Webseite, der diese in jeglicher Form weiterverwenden darf. Laut einem Bericht eines Rechtsanwaltes (Simon Mc Garr im Interview mit siliconrepublic.com am 11.2.2008) ist dies grob EU-datenschutzwidrig und es scheint überdies so zu sein, dass es den Usern überhaupt nicht möglich ist, ihre von ihnen selbst eingegebenen Daten auf dieser Webseite auch wieder endgültig zu löschen. Es ist davon auszugehen, dass sich viele tausende europäische User bereits auf dieses, nach europäischem Datenschutzrecht zumindest äußerst bedenkliche Modell eingelassen haben.

32 www.secondlife.com

by third parties. Linden Lab can (and you authorize Linden Lab to) disclose any information about you to private entities, law enforcement agencies or government officials, as Linden Lab in its sole discretion, believes necessary or appropriate to investigate or resolve possible problems or inquiries or as otherwise required by law". Diese Klausel ist geradezu eine Generalvollmacht an den Betreiber der Community, Daten ohne große „Hemmungen" an wen auch immer herauszugeben.[33]

7. Ergebnis

Die Beispiele in diesem Beitrag zeigen, dass der Gesetzgeber zwar bemüht ist, den „Old-Economy-Rechtsstaat" durch „moderne" Normen zu bereichern, die auch den „Cyberspace" regeln sollen, dass in der Praxis die Umsetzung und Anwendung dieser Bestimmungen jedoch verbesserungswürdig sind. Verbesserungswürdig sind etwa die Zuständigkeitsverteilungen bei der Sanktionierung dieser „modernen" Normen, etwa die Zentralisierung der Vollziehung der Straftatbestände des Datenschutzrechtes oder E-Commerce-Gesetzes bei spezialisierten Stellen, anstatt diese auf unzählige Bezirksverwaltungsbehörden zu zerstreuen,[34] wo sich Personen mit nicht ausreichender Schulung und Kenntnis der Materie damit „herumschlagen" müssen. Ebenso verbesserungsfähig ist die Ausstattung der zuständigen Stellen mit geschultem Fachpersonal, etwa der Datenschutzkommission, die seit Jahren unter akutem Personalmangel leidet und immer mehr zum peinlichen personellen Schlusslicht unter den europäischen Datenschutzbehörden wird.[35] Unbedingt verbessert werden muss auch der Rechtsschutz bei den typischerweise internationalen Sachverhalten im Internet. Dazu müssten eine verbesserte Zusammenarbeit zwischen den Gerichten und Strafverfolgungsbehörden in diesem Bereich stattfinden sowie einfachere, klare und effizientere Zuständigkeiten geschaffen werden. Dies, was natürlich ein schwieriges Unterfangen ist, auf globaler Ebene.

Wenn nicht, wird der „Cyberspace" immer mehr zur „Cyberanarchie" werden, die mit dem Old-Economy-Rechtsstaat nicht mehr geregelt werden kann, was

33 Passend dazu heißt es in Punkt 5.3. der AGB von Linden Lab „you understand and agree that Linden Lab has the right but not the obligation, to remove any content (including your content) in whole or in part at any time for any reason or no reason, with or without notice and with no liability of any kind." Die „Generalklausel" zur Datenweitergabe wird somit auch noch ergänzt um die Zustimmung, dass sämtliche oder Teile der Daten jederzeit ohne Vorankündigung und ohne jegliche Haftung irgendeiner Art von der Plattform entfernt werden können. Dies, obwohl mittlerweile angeblich auf dieser Webseite Millionen von „Linden-Dollar" umgesetzt werden, die in echte Dollar gewechselt werden können. Es zeigt sich hier das Problem, dass eine Community einerseits als bloßes Online-„Spiel" abgetan wird, andererseits dort „virtuelle" Besitztümer geschaffen werden, die in reales Geld umgewechselt werden können. Hier jegliche Haftung sowohl zivilrechtlicher Natur als auch für Datenschutz und Datensicherheit auszuschließen, ist wohl nicht der richtige Weg für die Zukunft des Web 2.0.

34 Oder, wie der mittlerweile gekippte Entwurf der Verfassungsreform aus 2007 vorsah, auf Landesverwaltungsgerichte zu zersplittern.

35 Siehe etwa dazu erneut die „Mahnung" im Datenschutzbericht 2007 der Datenschutzkommission, online unter www.dsk.gv.at.

aber sinnvolle gewerbliche Tätigkeit in diesem nicht mehr möglich macht und somit wirschaftsschädlich ist.

8. Abschließendes Fallbeispiel

Nachstehendes, letztes Beispiel soll zeigen, wie kompliziert die Sachverhalte im Web 2.0 noch werden können:

Ein Second Life-Avatar,[36] der dort auf „German Island" lebt, in Google Earth[37] aber in Burundi lokalisiert werden kann, behauptet in einem youtube-Video,[38] dass ein bestimmter ebay-User,[39] dessen reales Haus er auf Google Earth in Kasachstan lokalisiert haben will, mit einem gehackten Avatar eines Minderjährigen auf ebay.fr einen virtuellen iPod[40] durch Versteigerungsmanipulation billig „ergaunert" habe, mit dem er dann von einem Studenten aus Kolumbien über eine ftp-Plattform einer amerikanischen Universität illegal gekaufte Lieder von itunes[41] in der Bar eines virtuellen Nachtlokals Namens „Paris Hilton", das im virtuellen Wien angesiedelt ist, abspielt.

Könnte der bloßgestellte User den Avatar auf Verleumdung klagen? Wo? Dürfte der Avatar zum Wahrheitsbeweis die Herausgabe aller notwendigen Userdaten von Google und Second Life verlangen? Könnte Paris Hilton auf Verletzung ihrer Namensrechte klagen? Wen? Wo? Wäre das Abspielen der illegalen Lieder auf dem „ergaunerten" iPod in einer virtuellen Welt eine öffentliche Aufführung, für die Urheberrechtsabgaben zu zahlen ist? Wäre es eine Urheberrechtsverletzung? Wo muss das virtuelle Nachtlokal seine Eintrittsgelder versteuern? Usw, usw.[42]

Viele spannende Fragen also, zu denen Juristen beweisen werden müssen, dass es keine unlösbaren Rechtsprobleme gibt, auch nicht für den „Old-Economy-Rechtsstaat" im „Cyberspace".

36 www.secondlife.com.
37 www.earth.google.com.
38 www.youtube.com.
39 www.ebay.com.
40 www.apple.com/itunes.
41 www.apple.com/itunes.
42 Siehe schon Output 2007/07, 18.