

Neuere Tendenzen im brasilianischen Internetrecht

Arne Rathjen, Rechtsanwalt

E-Mail:netlaw@rathjenra.com

I. Einführung / Allgemeines

Die traditionell guten deutsch-brasilianischen Beziehungen haben sich laut amtlichen Quellen in jüngerer Zeit zu einer „strategischen Partnerschaft“ ausgeweitet.

Insbesondere seit den frühen neunziger Jahren sind die diplomatischen Kontakte erheblich vertieft worden. Brasilien ist daher nach wie vor einer der bevorzugten deutschen Investitionsstandorte, und es wird aktuell mehr deutsches Kapital in Brasilien investiert als z. B. in den USA. Diese erfreulichen Faktoren werden ergänzt durch die (jedenfalls in Brasilien) seit einem Jahr optimistisch stimmende Wirtschaftslage. Von Wachstumsraten wie etwa 5,2 % p.a. (2004) träumt man in Deutschland nur noch. Interessant in diesem Kontext ist auch, dass etwa die Exporte Brasiliens mittlerweile zu 55 % aus industriellen Fertigprodukten bestehen. Größter Handelspartner Brasiliens ist aktuell die EU mit einem Anteil von ~ 25 %.

Vor diesem Hintergrund ist logischerweise der E-Commerce (gerade im B2B-Sektor, also der elektronische Geschäftsverkehr zwischen Unternehmen) von Interesse. Es lohnt sich daher, einen Blick auf die Entwicklung des Internetrechts in Brasilien zu werfen.

Zunächst einige Daten. Guter (oder nicht so guter) brasilianischer Tradition zufolge wird dieser Bereich massiv staatlich gefördert, heute zumeist durch die Gewährung von Steuervergünstigungen. Die Gesamtzahl der in Brasilien ansässigen Softwareunternehmen wird aktuell mit ca. 2800 angegeben (Mexiko: 700, Argentinien 300). Ca. 60 % der Softwareunternehmen Lateinamerikas befinden sich dort. Die Entwicklung diverser Internetdienstleistungen stellt in jedem Fall eine strategisch herausragende Komponente dar.

Nachdem zunächst durch die in den achtziger Jahren bestehende „Marktreserve“ der Hauptanteil von Softwareunternehmen in brasilianischen Händen lag, ist nunmehr die Mehrzahl der dort ansässigen Unternehmen in Allianzen mit den jeweiligen globalen

Marktführern eingebunden (Microsoft, Oracle und IBM). Eine anschauliche Fallstudie für die (wachsende) Bedeutung des E-Commerce in Brasilien ist Dell, mit einer 1999 in Rio Grande do Sul gegründeten Filiale. Wie bekannt hat Dell den Zwischenhandel weitgehend abgeschafft und vertreibt seine Produkte, sei es an Konsumenten, sei es an Unternehmen, vorwiegend über das Internet. In diesem Kontext wurde die vergleichsweise schwache Telekommunikations- Infrastruktur in Brasilien als Hindernis bewertet.

Auch im Unternehmenssektor ist die Bewertung und Ausstattung der brasilianischen Unternehmen im internationalen Vergleich eher unterdurchschnittlich. Behindernd wirkt sich in diesem Kontext auch die regional strukturierte Besteuerung aus. Wichtiger für die Standortentscheidung als etwa Steuervergünstigungen war u.a. die hohe Qualität des Ausbildungsstandes der Arbeiter, insbesondere im Süden des Landes. Generell ist Brasilien mit Computer – und Telekommunikationsprodukten eher unterversorgt, wobei der Markt seit Mitte der neunziger Jahre regelrecht explodiert ist und ein Ende nicht abzusehen. Das Wachstum des Technologiesektors wurde für 2004 mit ca. 9 % beziffert. Das Potential bleibt hoch, zumal wenn man bedenkt, dass sich einige der in den neunziger Jahren initiierten Privatisierungen noch nicht voll ausgewirkt haben. In Brasilien gibt es zur Zeit ca. 22 Millionen Internetnutzer, so dass Brasilien damit weltweit an zehnter Stelle steht (in absoluten Zahlen gerechnet), allerdings erst an zweiundsiebzigster, wenn man die Bevölkerungszahl berücksichtigt. Die Zahl der Internet – Hosts ist mit ca. 3, 5 Mio. recht hoch – damit liegt Brasilien, wieder in absoluten Zahlen gerechnet, an siebter Stelle weltweit.

Marktperspektiven ergeben sich u.a. aus der vergleichsweise geringen Verbreitungsdichte.

II. Gesetzliche Grundlagen

Die Fülle der Verordnungen, Erlasse, Richtlinien, Gesetze usf., welche sich mit der Materie „Internet“ beschäftigen, ist erheblich. Es kann hier nur ein Überblick gegeben werden, zumal es sich bei einer Vielzahl von Normen lediglich um Verwaltungsvorschriften handelt, welche die (interne) Nutzung des Internet im Bereich der Verwaltung, Justiz und Gesetzgebung regeln.

Ein Überblick:

1. Lei nº 10.077, de 30/12/2004 (DOU de 31/12/2004), in Verbindung mit Lei nº 8.248, de 23/10/1991, Lei nº 8.387, de 30/12/1991, Lei nº 10.176, de 11/01/2001, welches die öffentlichrechtlichen Rahmenbedingungen für den Informatiksektor reguliert.
2. Portaria nº 614, de 01/12/2004 (DOU de 08/12/2004), welche die Rede BrasilNano installiert, mit dem Ziel gezielter Förderung der Nanotechnologie
3. Das Lei nº 10.973, de 02/12/2004 (DOU de 03/12/2004) befaßt sich mit der Förderung von Forschung und Entwicklung.

4. Resolução nº 397, de 18/10/2004 (DOU de 19/10/2004): Regelt den Einsatz digitaler Signaturen im Superior Tribunal de Justiça.
5. Decreto nº 5.244, de 14/10/2004 (DOU de 15/10/2004): Regelt Aufbau und Organisation des Conselho Nacional de Combate à Pirataria e Delitos contra a Propriedade Industrial
6. Resolução nº 287, de 14/04/2004, welches sich mit der Verwendung von E-Mails und ähnlichen Übertragungsmodi (als proessuale Handlungsform) im Zuständigkeitsbereich des STF befaßt.
7. Das Decreto nº 4.928, de 23/12/2003 (DOU de 24/12/2003) schafft eine Reihe von Steuervergünstigungen für innovative Forschungsvorhaben.
8. Decreto nº 4.829, de 03/09/2003 (DOU de 04/09/2003), welches das CGIBr, Comité Gestor da Internet no Brasil, installiert, vgl. auch Decreto nº 4.776, de 10/07/2003 (DOU de 11/07/2003), im Falle des Rede Brasil de Tecnologia - RBT
9. Lei nº 10.664, de 22/04/2003 (DOU de 23/04/2003): Diverse Änderungen der Informatikgesetzgebung (insbesondere Lei nos 8.248 / 91).
10. Digitale Signatur / Zertifizierungsstellen: Decreto nº 4.414, de 07/10/2002 (DOU de 08/10/2002), vgl. auch Decreto nº 3.996, de 31/10/2001.
11. Lei nº 10.176, de 11/01/2001: Diverse Änderungen der Informatikgesetzgebung
12. Lei nº 9.610, de 19/02/1998: Das neue Urheberrechtsgesetz, sowie die weiteren Ausführungsdekrete Decreto nº 2.894, de 22/12/1998, Decreto de 13/03/2001
13. Lei nº 9.609, de 19/02/1998: „LEI DE SOFTWARE“, befaßt sich mit dem Schutz von Computerprogrammen, sowie Decreto nº 2.556, de 20/04/1998

III. Ausgewählte Rechtsfragen

1. Strafrechtliche Aspekte, Cybercrime, Produktpiraterie

Die geradezu unglaubliche Entwicklung des E-Commerce und die noch unglaublicheren Erwartungen, die an ihn geknüpft wurden (teils nicht unberechtigt), haben mutmaßlich ein Thema in den früheren Jahren des WWW aus dem Blickfeld geraten lassen: Es ist die Sicherheitsproblematik.

Man verbringt heute (fast) mehr Zeit mit der Nachinstallation von Sicherheits-Updates, Virenschutzprogrammen, ausgefeilten Sicherheitssystemen und anderem mehr als mit der eigentlichen Arbeit und droht in einem anarchistischen Chaos aus Virenpest, Malware,

Spyware, bösartigen Javascript-Codes, Hackerangriffen, staatlichem Abhörwahn. Datenplündererei und Spam unterzugehen.

Die ursprünglich vorhandenen Produktivitätsvorteile drohen wieder zu verschwinden.

Deutlich sichtbar hat sich die Sicherheitslage seit ca. 2000 für Internetnutzer jeglicher Couleur (wie auch im allgemeinen) kontinuierlich und dramatisch verschlechtert. Es scheint, als habe der Fuchs die Aufsicht über den Hühnerstall erhalten und freue sich, wenn die Hühnchen ein wenig hüpfen.

Deutlich sichtbar ist die Verseuchung durch Computerviren, Würmer und anderes, allerdings auch die Heimsuchung durch mittlerweile kommerziell betriebene Hackereinsätze organisierter Banden, schließlich und endlich aber auch die lawinenartige Überflutung der E-Mail-Postfächer mit Spam, extrem angestiegen, während die Thematik 1999 noch eher theoretischen Charakter hatte. Ca. 80 % des E-Mail-Verkehrs entfällt mittlerweile auf Spam, wobei die Art der Versendung sicherlich Rückschlüsse zulässt auf die Qualität der Produkte bzw. die Seriösität der Anbieter. Es gibt relativ wenig Spam-Versender und sie scheinen auch bekannt zu sein, allerdings sind sie technisch hochgerüstet und verstreuen über sog. Bot-Netze in millionenfacher Zahl (bezogen auf eine „Kampagne“) E-Müll, wobei sich die Täter gleich massenweise in ungeschützte PCs einloggen, um von dort aus Müllmails mit falscher Absenderadresse weiterzuverschicken.

Mittlerweile wird bereits Politmüll über sog. Bot-Netze mit Hilfe von Würmern dem Publikum nahegebracht. Die Industriespionage dürfte mittlerweile epidemische Ausmaße angenommen haben, zumal staatlich gefördert, wie auch die illegale Datenverwertung zu kommerziellen Zwecken unter Umgehung sämtlicher Datenschutzbestimmungen. Die größte Bedrohung für die Datensicherheit, so stand in den Mitteilen der Bundesrechtsanwaltskammer (!) zu lesen, geht nunmehr von – sog. Sicherheitsbehörden aus. Man ist als Anwalt genötigt, Mandanten darauf hinzuweisen, dass der Aspekt der Vertraulichkeit eine Illusion schafft, die unter heutigen Bedingungen gefährliche Konsequenzen haben kann. Man ist von Gesetzes wegen verpflichtet, sie darauf hinzuweisen, dass im Zweifel alle Daten abgezogen werden, die sich irgendwie verwerten lassen.

Ein interessantes rechtspolitisches Problem, bzw. auch technisches, ist der virtuelle Bankraub sowie artverwandte Delikte. Die Zeit kunstvoll inszenierter Coups wie etwa im Falle des Commerzbank – Raubs in Berlin-Zehlendorf (man hatte unter der Bank einen Tunnel gegraben, so dass nicht auffiel, dass die Täter längst verschwunden waren, als die Polizei zugriff....) scheint vorbei. Viel besser erscheint es, einfach den Bankrechner zu übernehmen und sich bei Bedarf Geld überweisen zu lassen. Hier gibt es ein undefinierbares Dunkelfeld. Hinzu treten dann noch sog. Denial-of-Service-Attacken (Überflutung von Websites mittels automatisierter Massenanfragen) und ähnliche Sabotageakte aus unterschiedlichsten, teils politischen Motiven oder aber das Blockieren von Websites aus Verdeckungsabsicht oder aber in der Meinung, Zensor spielen zu müssen. Ein mittlerweile kontraproduktives Szenario. Der Chaos Computer Club sah dann auch schon vor Kurzem das Ende des E-Mail-Verkehrs heranziehen. In Brasilien wird dieses „universo sombrio da pirataria e fraude“ als Entwicklungshindernis angesehen – wohl zu Recht. Hinzu tritt die an diese Zustände nicht angepasste Gesetzeslage. Der Gesetzgeber – nicht nur in Brasilien – ist weit hinter der tatsächlichen Entwicklung zurückgeblieben und hat etwa die Bedeutung des E-Commerce

sowie der Notwendigkeit funktionierender Sicherheitssysteme nicht erkannt. Ergebnis ist das explosionsartige Ansteigen der computergestützten Kriminalität.

Brasilien ist nach Expertenmeinung einer der von computergestützten Straftaten am meisten heimgesuchte Ort der Welt (Folha Online 19.11.2002) und in dieser Hinsicht Weltspitzenreiter. Hacker hatten bereits die Site des Obersten Gerichtshofs übernommen. Ein Grüppchen namens „Resistência 500“ hatte die Site geknackt und ein Protestschreiben hinterlegt, das den Nutzern der Gerichts-Website unaufgefordert entgegenflatterte. Doch damit nicht genug. Es wurde bekannt, dass auch die Site des Präsidenten der Republik Ziel von Attacken gewesen war. Dann kam das Parlament an die Reihe. Schließlich kam es zu – zunächst nicht erklärbaren – mysteriösen Veränderungen der Sites diverser Ministerien, in denen despektierliche statements über eine Reihe von führenden Politikern auftauchten.

Wen wundert es, wenn der durch brasilianische Kriminelle weltweit angerichtete Schaden auf ca. 45 Milliarden USD geschätzt wird und Brasilien zum maior laboratório do cibercrime em todo o mundo befördert wurde (Folha online, 2002). Besonders beliebt, wie aus Statistiken und Fallmaterial ersichtlich, ist die Nutzung illegal erworbener Kreditkartendaten. Jüngst wurde bekannt, dass fast die gesamten nordamerikanischen Datenbestände einiger Kreditkartenunternehmen in die Hand von Datendieben gelangt waren. Das Comité Gestor da Internet meldete für 2002 und 2003 einen diesbezüglichen Zuwachs an registrierten kreditkartenbezogenen Delikten um 275 %.

Für 2004 ging man von ca. 5000 „ataques e golpes“ pro Monat innerhalb des brasilianischen Internets aus, zumeist Phishing – Attacken mit geklonten Bankseiten, die dem arglosen Nutzer zugespielt werden, um ihn dann zur Preisgabe von Konto – und Kreditkartendaten zu bewegen (Folha Online, Februar 2004).

Die Reaktion des Gesetzgebers fiel bisher eher mäßig aus. Zivilrechtlich bleibt der Rückgriff auf die Generalklausel des Art. 186 CC. Strafgesetze, die sich explizit mit Computerkriminalität befassen, gibt es in Brasilien nicht (oder bisher nicht, entsprechende Vorhaben sind auf den Weg gebracht worden), so dass man gewissermaßen kreative Lösungsansätze bemühen musste, etwa den Rückgriff auf das Gesetz Nr. 9296 / 96. Dieses behandelt eigentlich den Schutz des Post – und Fernmeldegeheimnisses im weiteren Sinne. Art. 10 stellt das nicht durch Gerichtsbeschluss gedeckte Abhören / Mitschneiden von verschiedenen Typen des Datenverkehrs unter Strafe. Dieses Gesetz wurde in mehreren Fällen zur Aburteilung von Hackern herangezogen, wie im übrigen der CP für Delikte allgemeiner Art, etwa im Falle von Phishing (Betrug) oder aber das Lei complementar Nr. 105/2001, welches den strafrechtlichen Schutz des Bankgeheimnisses gewährleistet.

Im Zentrum des Interesses stand auch der Identitätsdiebstahl. Wie anderorts auch hat sich die Hackerszene – einst eher belächelt – zu einem Phänomen organisierter Bandenkriminalität gewandelt. Naheliegende Ziele sind primär Banken und Kreditkartenfirmen, die im Jahre 2004 den Diebstahl von x Millionen Datensätzen zu beklagen hatten (Dunkelziffer ?).

Das Projecto de Lei 84 / 99 sieht folgende Lösungsansätze vor: Der Einbruch in Datenverarbeitungssysteme ohne Zugangsberechtigung wird mit einer Höchststrafe von 2 Jahren im Falle der Bereicherungsabsicht belegt. Das zitierte Phishing führt nach dem

Entwurf zu einer Maximalstrafe von 6 Jahren Freiheitsstrafe. In den USA etwa ist das strafrechtliche Risiko bei einem Höchstwert von 15 Jahren Freiheitsstrafe angesiedelt.

Gesetz geworden ist das Projekt bisher nicht.

So war es dann eine Labsal, folgende Nachricht zu lesen:

Brazilian police arrest 85 in crackdown on hackers

Summary:

The raid - dubbed Operation Pegasus - was carried out by 410 federal police officers in seven states. Brazilian police arrested 85 people on Thursday accused of stealing more than \$33 million by hacking into the online bank accounts of unwitting Internet users, authorities said. The raid - dubbed Operation Pegasus - was carried out by 410 federal police officers in seven states, making it one of the biggest crackdowns on electronic crime in Brazil. In all, 105 arrest warrants were issued after a four-month investigation found that the suspects had pocketed about 80 million reais in the scam. While most Brazilians do not have computers at home, studies show that those who do are among the most avid Internet users in the world, especially when it comes to private banking. Brazil is also quickly gaining a reputation as a hotbed for computer hackers. Last month, a Brazilian research group called the Computer Emergency Response Team published a study showing that online fraud complaints in the country shot up 1,300 percent in the second quarter, jumping to 7,942 from just 562 a year earlier.

Source: Reuters
[08/26/2005]

2. Zivilrechtliche und prozessuale Fragen, Haftungstatbestände

Die Problematik des elektronisch durchgeführten Vertragsschlusses ist aufgrund der weiten Verbreitung des E-Commerce und seiner steigenden Bedeutung gerade im B2B – Verkehr (zwischen Unternehmen) bereits mehr oder minder ausdiskutiert, hier besteht eine durchaus beachtliche (weltweite) Rechtsvereinheitlichung. Brasilien weist insoweit keine so großen Besonderheiten auf. Man ging sogar so weit, den Einsatz von elektronischen Medien im Bereich der notariellen Beurkundung und öffentlicher Register zu diskutieren. Auch ist man im Vergleich zu Deutschland teils recht weit gelangt, da z. B. prozessuale Willenserklärungen elektronisch abgegeben werden können (per E-Mail etwa). Auch ist das elektronische Handelsregistersystem weit ausgebaut. Die Verwendung des Fax in diesem Kontext wurde bereits durch Gesetz Nr. 8245 / 91 geregelt. Der Staat Rio de Janeiro bot seit langem den aus hiesiger Sicht hochinteressanten Service an, registrierten Benutzern die Möglichkeit zu geben, sich auf dem Gerichtsserver einzuloggen und auf diesem Wege prozessual gültige Erklärungen abzugeben. In Deutschland wurden diese Dinge bereits deshalb nicht ernsthaft diskutiert, weil die technische Ausstattung nicht vorhanden war / ist. Zumindest wäre erforderlich, Gerichtsserver mit einschlägigen Funktionen auszustatten und dann die (u. U. signierten) elektronischen Dokumente gedruckt an die Spruchkörper

weiterzuleiten. Allerdings gab es bereits bei der Protokollierung durch Computer statt per Hand oder Diktat große Schwierigkeiten.

Die Resolution 287/04 des Supremo Tribunal Federal sei aufgrund ihres für hiesige Verhältnisse geradezu revolutionären Gehalts im Wortlaut wiedergegeben:

RESOLUÇÃO Nº 287, DE 14 DE ABRIL DE 2004.

Institui o e-STF, sistema que permite o uso de correio eletrônico para a prática de atos processuais, no âmbito do Supremo Tribunal Federal.

O PRESIDENTE DO SUPREMO TRIBUNAL FEDERAL, no uso das atribuições que lhe confere o art. 13, XVII, combinado com o art. 363, I, do Regimento Interno, e tendo em vista o decidido na Sessão Administrativa do dia 25 de março de 2004, Processo Administrativo nº 285.293, assim como o disposto na Lei 9.800, de 26 de maio de 1999,

RESOLVE:

Art. 1º Fica instituído no âmbito do Supremo Tribunal Federal o e-STF, sistema de transmissão de dados e imagens, tipo correio eletrônico, para a prática de atos processuais, nos termos e condições previstos na Lei 9.800, de 26 de maio de 1999.

Art. 2º O acesso ao e-STF dá-se por meio da página do Supremo Tribunal Federal na internet, endereço eletrônico www.stf.gov.br, com utilização facultada aos advogados previamente cadastrados e sujeita às regras e condições do serviço constantes do manual do usuário, também disponível nesse sítio.

§ 1º O interessado deverá cadastrar-se no e-STF e, em seguida, registrar sua senha de segurança, que deverá ser pessoal e sigilosa, assegurando a remessa identificada das petições e dos documentos.

§ 2º As petições eletrônicas enviadas deverão, obrigatoriamente e sob pena de não-recebimento, ser gravadas em um dos seguintes formatos: doc (Microsoft Word), rtf (Rich Text Format), jpg (arquivos de imagens digitalizadas), pdf (portable document format), tiff (tagged image file), gif (graphics interchange file) e htm (hypertext markup language).

Art. 3º As petições e os documentos enviados serão impressos e protocolados de forma digital pela Coordenadoria de Registros e Informações Processuais durante o horário de atendimento ao público, das 11h às 19h, nos dias úteis, sendo que os expedientes encaminhados após as 19h somente serão protocolados no dia útil subsequente.

§ 1º É de inteira responsabilidade do remetente o teor e a integridade dos arquivos enviados, assim como a observância dos prazos.

§ 2º A tempestividade da petição será aferida pela data e hora de recebimento dos dados pelo sistema, observando-se, rigorosamente, o limite de horário para o protocolo de petições estabelecido no caput.

§ 3º Não será considerado, para efeito de tempestividade, o horário da conexão do usuário, o momento do acesso à página do Tribunal na internet ou qualquer outra referência de evento.

§ 4º Os arquivos recebidos em desacordo com os formatos estabelecidos nesta Resolução ou que estejam, no todo ou em parte, incompletos ou danificados, por qualquer eventualidade técnica, não serão protocolados, cabendo ao interessado acompanhar o seu completo recebimento pelo sistema.

§ 5º A simples remessa do arquivo pelo sistema não assegura seu protocolo, cuja efetivação dependerá de cumprimento das formalidades previstas nesta Resolução.

§ 6º O Tribunal exime-se de qualquer falha técnica na comunicação e no acesso ao seu provedor ou à página do STF na internet, cabendo ao interessado a verificação da integridade do recebimento dos dados.

Art. 4º Deverão acompanhar a petição, em arquivos digitais, os documentos que obrigatoriamente a complementam.

Art. 5º A utilização do sistema não desobrigará o usuário de protocolar os originais, devidamente assinados, junto à Seção de Protocolo e

Informações Processuais do STF, no prazo e condições previstos no artigo 2º e parágrafo único da Lei 9.800/99.

§ 1º A Coordenadoria de Registros e Informações Processuais lançará certidão com a data, a hora do recebimento e o protocolo da petição eletrônica na petição original e nos documentos que a acompanham, assim como verificará a perfeita semelhança entre esta e os originais recebidos posteriormente.

§ 2º O não-encaminhamento dos originais implicará o arquivamento da via eletrônica da petição, competindo à Coordenadoria de Registros e Informações Processuais certificar, nos respectivos autos, tal ocorrência.

§ 3º Deverão ser juntadas aos autos apenas as peças originais, acompanhadas das certidões relacionadas ao uso do sistema e-STF, arquivando-se em meio magnético no ambiente informatizado do Supremo Tribunal Federal a petição eletrônica e seus anexos.

Art. 6º Eventuais casos omissos serão decididos pelo órgão julgador competente.

Art. 7º Esta Resolução entra em vigor na data de sua publicação.

Ministro MAURÍCIO CORRÊA

Immerhin gibt es in Deutschland die Möglichkeit / Verpflichtung, seine Steuererklärung mit einem Programm namens Elster abzugeben. Auf die Möglichkeit der Einreichung von Schriftsätzen bei Gericht per E-Mail oder Datenfernübertragung wird man wohl noch einige Zeit warten müssen. Generell werden in Deutschland wie auch in Brasilien elektronische Dokumente als Beweismittel mit großer Skepsis betrachtet und oft gar nicht erst als Beweismittel bewertet. Lediglich im Fall digital signierter elektronischer Dokumente liegen die Dinge etwas anders. Dass Vertragsschlüsse – gegebenenfalls unter Einbeziehung von AGB – mittels elektronischer Medien volle Rechtsgültigkeit haben, steht aktuell außer Zweifel, nur die bange Frage lautet dann, wer in einem etwaigen Prozess was wie beweisen kann, wenn es keine Urkunden oder ähnlich zuverlässige Beweise gibt. Das Interesse konzentriert sich nunmehr auch gerade auf die bereits erwähnten Sicherheitsaspekte sowie eine Reihe ungeklärter Haftungsfragen.

Hierzu gibt es eine ganze Reihe lesenswerter Entscheidungen.

In Deutschland ohne Parallele sind einige Urteile, welche Anbieter von Internetdiensten diverser Couleur aufgrund mangelhafter Sicherheitsvorkehrungen in die Pflicht nahmen.

Folgender Sachverhalt lag einer Entscheidung der 6ª Câmara Cível do Tribunal de Alçada de Minas Gerais zugrunde: Dem Kläger waren im Oktober 2004 durch eine Internet-Transaktion

einige tausend Reais von seinem Konto „abgezogen“ worden. Kurze Zeit später forderte ihn die Bank auf, seinen Saldo auszugleichen und drohte mit der Unterrichtung von Wirtschaftsauskunfts- diensten. Begründet wurde die Ersatzpflicht mit einer verschuldens - unabhängigen Haftung nach dem Código de Defesa do Consumidor – zumal handele es sich beim Homebanking um eine risikoreiches Geschäft, von dessen Anfälligkeit die ersatzpflichtige Bank gewusst habe. Dennoch böte sie den Homebanking-Service an und hafte daher auch für die betrügerischen Machenschaften Dritter (Apelação Cível nº 441.467-9).

In einer anderen vom Superior Tribunal de Justiça im Herbst 2004 entschiedenen Sache wurde die Weitergabe von Adress – und Telefondaten einer Psychologin an eine Vermittlungs-Site mit einer Ersatzpflicht von 200 salários mínimos belegt (nicht gerade viel Geld, aber immerhin). Der in Anspruch genommene Internet-Provider mußte sich eine „fragilidade operacional“ entgegenhalten lassen, welche dazu geführt hatte, dass die besagten Daten der Klägerin in einer Site für Amüsierbedürftige landeten. Rechtsgrundlage ebenfalls der CdDC sowie der CC (Resp 566.468).

Recht brisant auch eine neuere Entscheidung, die sich mit einem Hackerangriff auf eine (kommerzielle) Website befasst. Das Unternehmen Websol hatte bei dem Provider Pro Internet seine Internetpräsenz eingerichtet, und musste dann feststellen, dass die Seiten plötzlich statt der ursprünglich publizierten einige pornografische Bilder enthielten. Es dauerte drei Tage, bis die dann auf Verlangen von Websol gesäuberte Seite wieder mit Pornobildchen bestückt war. Der Haftungsausschluss per AGB wurde vom Gericht verworfen. Auch sei irrelevant, dass es lediglich einen mündlichen Vertragsschluss gegeben habe. Die Hackerangriffe seien vorhersehbar gewesen, man habe es versäumt, die entsprechenden Sicherheitsvorkehrungen zu treffen. Aus dem Urteil:

APELAÇÃO CÍVEL Nº 433.758-0 - BELO HORIZONTE - 02.02.2005

EMENTA: AÇÃO INDENIZAÇÃO POR DANOS MORAIS– PROVEDORA DE INTERNET – HOSPEDAGEM DE SITES – INVASÃO DE HACKERS – FOTOS PORNOGRÁFICAS – ABALO NA IMAGEM DA PESSOA JURÍDICA – RESPONSABILIDADE CONTRATUAL – INDENIZAÇÃO.

Provado o dano ou prejuízo sofrido pela vítima, a culpa do agente e onexo causal, surge a obrigação de indenizar, que só será afastada em hipóteses de caso fortuito ou força maior, ou se a responsabilidade pelo evento danoso for exclusiva da parte lesada.

Se, por um lado, a conduta dos hackers é considerada previsível e evitável, atualmente, dependendo apenas da evolução tecnológica, não havendo como aplicar-se a excludente de força maior, por outro, a apuração da responsabilidade das empresas prestadoras de serviços de acesso à rede mundial depende do caso concreto.

A publicidade amplamente divulgada garantindo segurança aos assinantes da provedora implica responsabilidade da empresa nos exatos termos da oferta apresentada, já que respondem os provedores pelos serviços prestados aos usuários por força de obrigação contratual.

Em questão de responsabilização, há de se ter em conta se a empresa veiculou publicidade quanto à existência de segurança para a hospedagem dos sites, ou se comprovou ter informado a seus clientes, de maneira transparente, sobre as questões relativas às invasões dos hackers. A ausência de qualquer informação nesse sentido pode dar ensejo à responsabilidade da provedora.

3. Gewerblicher Rechtsschutz, Urheberrecht

Der Schutz geistigen / industriellen Eigentums in Brasilien ist wie bekannt von einigen regionalen Besonderheiten geprägt, die im Ergebnis auf eine vergleichsweise niedrige Schutzintensität hinauslaufen. Eher selten sind Fälle, in denen für (auch vorsätzliche) Verletzungen von Urheberrechten und gewerblichen Schutzrechten auch nur halbwegs akzeptable Entschädigungen bezahlt werden mussten. Beklagt wurde und wird auch die fehlende Effizienz des INPI.

Es dauert ca. 5 Jahre bis zu einer Markenregistrierung und bei der Registrierung von Patenten gibt es kaum vertretbare Verzögerungen (zu diesen Fragen etwa Gustavo Leonardos, O Estado de Sao Paulo, 27.8.2005).

Immerhin beginnen sich die brasilianischen Gefängnisse aufgrund des verschärften Vorgehens gegen organisierte Produktpiraterie zu füllen.

Brasilien ist noch heute nach China der Vizeweltmeister der Produkt – und insbesondere Softwarepiraterie, ca. 50 % der in Brasilien genutzten Programme sind Raubkopien. Die weltweit größte Kopiermaschine ist das Internet.

Die Gesetzeslage steht zu diesen Phänomenen – ein nicht so regionaltypischer Faktor – in einem konträren Verhältnis. Computerprogramme werden wie literarische Werke geschützt, mit einigen Einschränkungen hinsichtlich der Urheberpersönlichkeitsrechte (Art. 2 des Gesetzes 9609 / 98). Die Schutzdauer beträgt 50 Jahre gerechnet ab dem 1.1. des auf die Veröffentlichung folgenden Jahres. Eine Registrierung ist nicht erforderlich (Art. 3), wohl aber zu empfehlen.

Der strafrechtliche Schutz fällt etwa im Vergleich zum deutschen Recht eher schwach aus (Art. 12) und reicht bis zu einer Strafdrohung bis max. 2 Jahren Freiheitsstrafe im Falle der illegalen Vervielfältigung in Gewinnerzielungsabsicht, zudem handelt es sich prinzipiell um ein Antragsdelikt.

Höchstrichterlich klargestellt ist nunmehr, dass es sich bei Computersoftware um ein literarisches Werk handelt, das dem Urheberrechtsschutz unterfällt und nicht dem gewerblichen Rechtsschutz (propriedade industrial).

Der Schutz von Datenbanken elektronischer Art ist bisher gesetzlich expressis verbis nicht geregelt. Im UrhG findet sich – der entsprechenden EU-Richtlinie folgend – gleich ein ganzer Abschnitt. Mit etwas gutem Willen kann man allerdings Art. 7 Ziff. XIII des Gesetzes 9610 / 98 in der Weise interpretieren, dass unter „base de dados“ eben auch Datenbanken auf

elektronischen Speichermedien zu verstehen sind. Insbesondere verweist auch Art 29 Ziff. IX auf das ausschließliche Recht des Autors, das Werk in Datenbanken einzuspeisen oder aber auf einem Computer zu speichern. Art. 87 I schließlich konstituiert das exklusive Recht, die Datenbank zu vervielfältigen, und zwar „por qualquer meio ou processo“. Es bedarf keiner weiteren Erläuterung, dass gerade für Betreiber von Websites der Datenbankschutz von elementarer Bedeutung ist. Detailliertere Regelungen gibt es als Gesetzgebungsvorhaben.

Für einen Patentschutz von Softwaresystemen gibt es in Brasilien nach hiesiger Einschätzung aktuell keine Rechtsgrundlage.

Im Zentrum der Diskussion in Brasilien stand / steht weiterhin die Frage, ob das Phänomen der lizenzfreien Software (software livre) ein legales Phänomen darstellt. Ein Ende der Debatte ist nicht abzusehen. Dem einen oder anderen großen Softwarekonzern ist jedenfalls der kleine Pinguin , der gratis über die Bildschirme wackelt, ein Dorn nicht nur im Auge, und die Lobbytätigkeit in den USA zeigt erste juristische Wirkungen in Form interessanter Konstrukte im Sinne der Auftraggeber.

Die brasilianische Regierung wiederum wünscht, auf ihren Systemen möglichst viele kleine schwarzgelbe Pinguine zu sehen und hat sich expressis verbis für die Nutzung von software livre ausgesprochen. Erklärtes Ziel ist nun, jedem Brasilianer einen Computer zu verschaffen.

IV. Weiterführende Links

Für weiterführende Recherchen seien nachstehende Links empfohlen:

ABPI

<http://www.abpi.org.br/>

AdvocatiLocus

<http://www.advogado.com/>

Centro Brasileiro de Estudos Jurídicos da Internet

<http://www.cbeji.com.br/>

Crimes de Informática

Carlos Daniel Vaz de Lima

<http://www.magatur.com.br/mambo>

Dannemann Siemsen

<http://www.dannemann.com.br/>

Instituto Brasileiro de Peritos em Comércio Electronico e Telemática

<http://www.ibpbrasil.com.br/>

InternetLegal
<http://www.internetlegal.com.br/>

República Federativa do Brasil
<http://www.brasil.gov.br/servicos.asp>

Berlin, November 2005