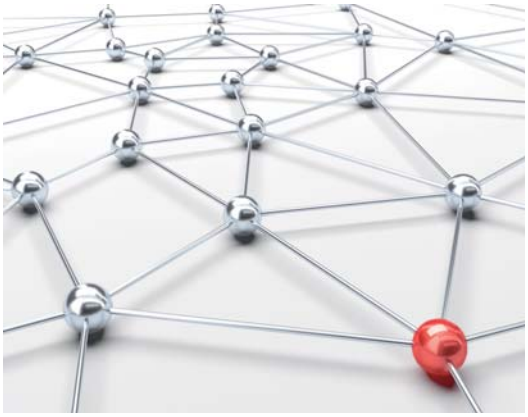
Konrad Adenauer Stiftung

NETZPOLITIK AUS INTERNATIONALER PERSPEKTIVE

Tobias Wangermann | Helmut Reifeld (Hrsg.)



LÄNDERBERICHTE AUS DEN USA, GROSSBRITANNIEN, SPANIEN, POLEN, INDIEN UND KOREA

forum digital

Umschlagfoto: © fotolia | beawolf
Gestaltung: SWITSCH Kommunikationsdesign, Köln.
Printed in Germany.
Gedruckt mit finanzieller Unterstützung der Bundesrepublik Deutschland.

ISBN 978-3-942775-06-9

INHALT

VORWORT

Die Präsenz des Internets in fast allen Arbeits- und Lebenszusammenhängen brachte auch die politischen Rahmenbedingungen für die Nutzung dieses Mediums in die politische Diskussion. Das als Netzpolitik bezeichnete Politikfeld umreißt nicht nur die juristischen Bedingungen für Betrieb und Nutzung dieses Mediums, sondern reflektiert auch die kulturellen und politischen Positionen dazu. Dabei geht es sowohl um Fragen des Urheberrechts, der Datensicherheit, der Persönlichkeitsrechte, der Informationszugänge wie auch der Kriminalitätsbekämpfung oder der Wettbewerbsbedingungen.

Die Einsetzung einer Enquete-Kommission des 17. Deutschen Bundestages „Internet und digitale Gesellschaft", eine lebhafte Debatte in den Medien sowie eine wachsende Zahl an Diskussionsveranstaltungen und Plattformen zeigen, dass es sich nicht mehr um ein Thema weniger Internetexperten handelt, sondern in der Mitte der Gesellschaft angekommen ist. Unter dem Stichwort „digitale Bürgerrechte" wird das Verhältnis von Freiheit und Reglementierung im Internet dabei exemplarisch für das Verhältnis von Staat und Bürger gesetzt.

Die deutsche Debatte um die Netzpolitik wird von verschiedenen Aspekten bestimmt. Die Forderung nach Sicherheit besonders in Hinblick auf die persönlichen Daten, die Gewährung der Freiheit dieses Mediums ohne staatliche Eingriffe, die Diskussion um adäquate Formen des Urheberrechts und seiner Durchsetzung sowie eine Fokussierung auf die Risiken verbunden mit einem latenten Vorwurf eines unbedingten Reglementierungswillens des Staates sind einige Eckpunkte dieser Debatte. In einzelnen Themenfeldern ist die Debatte zurzeit festgefahren. Dazu gehören beispielsweise die Vorratsdatenspeicherung, das Zugangserschwerungsgesetz und das Urheberrecht.

Allein die Tatsache, dass es sich beim Internet um ein global vernetztes Medium handelt, macht es zwingend, nach international gültigen Rahmenbedingungen und Durchsetzungsinstrumenten zu suchen. Es lenkt aber auch den Blick auf einen internationalen Markt der politischen Konzepte und Modelle, welche auf die anstehenden Fragen Antworten geben sollen. Ein Austausch über diese Konzepte kann die Debatte in Deutschland befruchten.

Die Publikation soll mit dem Blick auf die netzpolitischen Entscheidungen und Diskussionen in anderen Ländern einen Referenzrahmen für die deutsche Debatte in der Netzpolitik anbieten. Die Berichte aus sechs demokratischen Staaten von unterschiedlichen Kontinenten geben Auskunft, wie dort die netzpolitischen Kernthemen gehandhabt werden. Die Konrad-Adenauer-Stiftung versteht sich aus ihrem internationalen Engagements heraus als Mittler in diesem Prozess. Mein Dank gilt allen Autoren und Übersetzern für ihre Beiträge.

Berlin, im Januar 2011

Michael Thielen
Generalsekretär der Konrad-Adenauer-Stiftung e.V.

<< zurück zum Inhaltsverzeichnis

EINLEITUNG

Tobias Wangermann

Durch die rasante technologische Entwicklung wie auch die explosionsartige Verbreitung haben digitale Medien wie Internet und Mobilfunk Einzug in alle beruflichen, öffentlichen und privaten Bereiche des Lebens genommen. Ihre globale Vernetzung in Echtzeit, die geringen Zugangsbarrieren und die interaktiven Optionen gestatten sowohl qualitativ wie auch quantitativ eine andere Kommunikation als bisher.

So ist es nicht verwunderlich, dass die Rahmenbedingungen für diese digitalen Medien neben den traditionell gesetzten Themen der Politik in der politischen wie gesellschaftlichen Diskussion aktuell so präsent sind. Ob es der Schutz der Persönlichkeitsrechte ist, wie es die Debatten um Google-Streetview, Facebook oder die Vorratsdatenspeicherung zeigen; ob es die Auseinandersetzung über adäquate Formen des Urheberrechtsschutzes im Internet ist, die Bedrohung der Netzneutralität oder die Optionen für einen Kinder- und Jugendschutz – die Fragen der Netzpolitik beschäftigen das Feuilleton ebenso wie den Bundestag und betreffen uns selbst in den alltäglichsten Dingen beim Nutzen dieser Medien.

In Deutschland werden diese Themen mit hoher Sensibilität wahrgenommen und die politischen Entscheidungen einer breiten und kritischen Diskussion unterzogen. Von der Politik wird erwartet, eine Netzpolitik zu betreiben, die eine Balance zwischen Offenheit und Regulierung garantiert. Denn um die Möglichkeiten dieser Medien auszuschöpfen, muss sie Sicherheit im Sinne ihrer rechtsstaatlichen Aufgaben durch Regulierung herstellen und zugleich Freiheit für die kreative Nutzung in Wirtschaft, Wissenschaft, Kultur, Politik und Gesellschaft ermöglichen. Die Ansprüche der Nutzer an diese Balance sind zudem – je nach Art und Umfang der Mediennutzung – oft auch unterschiedlich, ja schwankend.

Dabei steckt die Politik in einem Dilemma. Mit den ihr zur Verfügung stehenden Instrumenten einer nationalstaatlichen Gesetzgebung ist ein global vernetztes Medium, welches eine territoriale Beschränkung bzw. einen Geltungsbereich des Rechts überspringt, schwerlich zu fassen. Auch wenn im Moment der Nutzung der jeweilige Standort und der juristische Geltungsbereich in einen direkten Zusammenhang gebracht werden können und damit ein Rechtszugriff möglich ist, bleibt das Problem und verweist auf einen internationalen Verständigungsrahmen. Denn Anbieter und Nutzer unterliegen all zu oft unterschiedlichen Bedingungen.

Gleichwohl ist die Politik aufgerufen die Rahmenbedingungen zu definieren – national wie auch international. Und sie tut es in vielen Handlungsfeldern auch.

Der Blick zu unseren Nachbarn wie auf die Bühne der Europapolitik zeigt, dass es dabei zu ganz unterschiedlichen Lösungen kommen kann und die Debatte auch dort oft kontrovers geführt wird. Das einem „3-strikes-out"-Modell entsprechende sogenannte Loi Hadopi (*Haute Autorité pour la Diffusion des Oeuvres et la Protection des Droits sur Internet*) in Frankreich oder die mit dem Begriff „Censilia" karikierten Regulierungsbemühungen der EU-Kommissarin Cecilia Malmström verdeutlichten, wie konfliktreich sich solche wie auch andere Eingriffe auf benachbarte Rechtsfelder wie das der Informationsfreiheit, des Datenschutzes, des Eigentums- oder der Persönlichkeitsrechte auswirken können.

Schaut man sich die einzelnen Konfliktfelder an, ist zu erkennen, dass sich die Gegenstände, die ursprünglich von der entsprechenden Gesetzgebung erfasst wurden, in ihrer digitalen Existenz oft grundlegend andere Eigenschaft aufweisen oder sich in einem anderen Umfeld bewegen. Die

räumlich wie zeitlich quasi unbegrenzte Beweglichkeit, Veränder- und Verknüpfbarkeit von Daten im Internet und das hohe Innovationstempo ihrer Verarbeitungsmöglichkeiten verleihen ihnen eine Dynamik, die von den gesellschaftlichen Institutionen nur schwer zu fassen ist.

Ob Urheberrecht, Datenschutz und Datensicherheit, Netzneutralität Persönlichkeitsrechte, Netzabdeckung oder Informationszugang – sie setzen Rechtsrahmen und Rechtsdurchsetzung im engeren sowie Nutzer- bzw. Bürgerinteressen gegenüber staatliche Verantwortung im weiteren Sinne im digitalen Kontext neu ins Verhältnis. Freiheit, Demokratie und Rechtsstaatlichkeit müssen sich auch in diesem Zusammenhang als lebendige Grundwerte unserer Verfasstheit beweisen.

Es ist offensichtlich, dass bei einer global vernetzten Infrastruktur wie es das Internet ist, diese Zusammenhänge so oder ähnlich in anderen Ländern als Anforderungen an Politik und Gesellschaft vorliegen. Die Frage ist also naheliegend, wie diese Themen dort gehandhabt werden. Sowohl was die rechtlichen Regelungen, die Institutionen und Strukturen betrifft wie auch die politische Diskussion über die Themen der Netzpolitik in der Öffentlichkeit.

Die hier zusammen gestellten Länderberichte geben einen Einblick in die Situation in den USA, Großbritannien, Spanien, Polen, Indien, und Korea. Für die Auswahl steht nicht nur das Netzwerk der Auslandsbüros der Konrad-Adenauer-Stiftung, sondern waren auch Überlegungen zur Eingrenzung und Streuung der Quellen leitend. Daher sind es Länder mit weitgehend vergleichbaren freiheitlichen, demokratischen und rechtsstaatlichen Strukturen und deshalb finden sowohl unsere europäischen Nachbarn Beachtung als auch Länder auf anderen Kontinenten.

Um eine Vergleichbarkeit der Angaben und Aussagen in den einzelnen Länderberichten zu unterstützen, wurde den Autorinnen und Autoren für die Erstellung Ihrer Berichte folgender Fragenkatalog zu Orientierung angeboten:

- Welchen Platz nimmt die Diskussion um netzpolitische Fragen in der politischen Debatte ein?
- Wird eine Vorratsdatenspeicherung (z.B. wegen Kriminalitätsbekämpfung) vorgenommen und wie wird sie politisch begründet bzw. diskutiert?

- Wie wird Datenschutz und Datensicherheit gehandhabt und welche Institutionen existieren zu ihrer Gewährleistung?
- Welche Regelungen existieren über den freien Zugang zu öffentlichen Daten (z.B. Verwaltungsdaten, sogenanntes open data) und welche Modelle gibt es für Ihre Nutzung?
- Gibt es die Praxis der Netzzugangssperren, wie ist sie geregelt und wie wird sie gehandhabt?
- Welche Konflikte mit den bisherigen Urheberrecht existieren und wie werden diese Konflikte gelöst, bzw. diskutiert?
- Existieren politische Programme zu Sicherstellung einer flächendeckenden Breitbandversorgung?
- Sind Interessenverbände der Zivilgesellschaft an der Debatte beteiligt?

Im Fokus stand nicht, eine vergleichbare Auflistung von Daten zu erheben, sondern einen Einblick in die politische Umsetzung und Diskussion netzpolitischer Themen in anderen Ländern zu ermöglichen. So zeigen die Beiträgen welche Institutionen, Programme und Strukturen zur Umsetzung netzpolitischer Ziele eingesetzt und welche Instrumente zur Regulierung rechtlicher Konflikte Verwendung finden. An Beispielen wird die politische Diskussion nachgezeichnet und Akteure der Netzpolitik vorgestellt.

Deutlich ist zu erkennen, dass der Ausbau eines Breitbandnetzes fast durchgängig von hoher politischer besonders aber wirtschaftlicher Priorität gesehen wird. Welche Anstrengungen beispielsweise in Indien für einen flächendeckenden Anschluss notwendig sind und wie stark das Gefälle zwischen Großstadt und ländlichem Raum dort bestehen, wird ebenso deutlich. Durchaus unterschiedlich ist die Institutionalisierung in Form von Behörden oder Kommissionen zur Durchsetzung von netzpolitischen Programmen oder zur Regulierung und Kontrolle: etwa wie in Korea durch eine direkte Anbindung an den Ministerpräsidenten oder durch Datenregister der Branchen wie in Polen. Wie eng dabei technische Innovationen und gesellschaftliche Veränderungen ineinander greifen können, zeigt beispielhaft der Erfolg einer Online-Verkaufsplattform für Eisenbahnfahrkarten in Indien, welche die Kunden von den bestehenden Netzwerken korrupter Zwischenhändler unabhängig macht.

Dass die Perspektive einer sogenannten digitalen Gesellschaft und die damit verbundene Dynamik an den Optionen einer Wissensgesellschaft zu partizipieren von vielen wirtschaftlichen wie auch politischen Rahmenbedingungen abhängt, bekräftigt die Schlüsselfunktion einer aktiven Netzpolitik. Grundlegende Voraussetzung dafür ist ein Anschluss an eine Breitbandverbindung. Von gleicher Bedeutung ist eine gestärkte Medienkompetenz. Denn die Vermittlung von Strategien zum Erlangen und Bewerten von Informationen, zum Meinungsaustausch, zu den rechtlichen wie auch ethischen Spielregeln im Netz und zu den kreativen Optionen, die dieses Medium bietet, ist eine Voraussetzung für eine aktive und (mit)gestaltende Nutzung.

Denn der Zugang zum Netz und die Kompetenz im Umgang mit den digitalen Angeboten des Internets sind entscheidende Kategorien für die Zukunftsfähigkeit eines Landes. Dabei handelt es sich sowohl um eine wirtschaftliche Dimension wie auch um eine kulturelle und politische, ja um eine gesellschaftliche. Denn die Potentiale, die das Internet für die Wirtschaft, die Wissenschaft, die Kultur wie für die Politik bietet, sind für unsere Gesellschaft nur gewinnbringend zu nutzen, wenn möglichst viele in diese Wertschöpfung eingebunden sind. Hier stehen Deutschland und Europa mit anderen Ländern im politischen Wettbewerb der Ideen und Konzepte.

<< zurück zum Inhaltsverzeichnis

LÄNDERBERICHTE

<< zurück zum Inhaltsverzeichnis

USA

Roman Sehling

ZUR NETZPOLITIK IN DEN USA

Nach der Wahl Barack Obamas hegten viele Firmen im Silicon Valley die Hoffnung, dass der *Internet-Präsident* sich, wie im Wahlkampf versprochen, für die Netzneutralität stark machen würde. Anfänglich schien dies auch der Fall zu sein: Eine Reihe von Obamas Spitzenberatern kam direkt von Google oder Facebook, die Position des Aufsichtsratsvorsitzenden des wichtigen *Federal Communications Committee* (FCC) wurde mit Netzneutralität-Verteidiger Julius Genachowski besetzt und das im Vorjahr verabschiedete Konjunkturpaket beinhaltete auch 7,2 Milliarden Dollar für die Ausweitung der Breitband-Internet-Versorgung im ganzen Land. Damit sollte nicht nur die Netzneutralität, sondern insbesondere der Wettbewerb unter den verschiedenen Internetanbietern, die Innovationsfähigkeit und damit die amerikanische Wirtschaft insgesamt langfristig gestärkt werden.

Es ist jedoch anders gekommen als geplant. Die Telefon- und Kabelnetzanbieter sind weiterhin gegen die strikte Anwendung der Netzneutralität und plädieren für das Recht, Datenpakete unterschiedlich zu behandeln, da sonst ihre Gewinnaussichten beträchtlich vermindert und dadurch wichtige Investitionen in den Ausbau und die technologische

Erneuerung der Netze verhindert würden. Damit würde dann das genaue Gegenteil von dem erreicht, was sich Präsident Obama zum Ziel gesetzt hatte. Bestärkt wurden die Internetanbieter dabei von einem in diesem Jahr ergangenen Urteil eines Berufungsgerichts, welches der FCC die Vollmacht aberkannte, das Prinzip der Netzneutralität anzuwenden.

Mittlerweile ist Google in dieser Frage offenbar zu einem Übereinkommen mit der Telekommunikationsfirma Verizon gekommen, das beispielgebend für den Rest des Sektors sein könnte. Man einigte sich darauf, Netzneutralität für die Datenübermittlung per Festnetz zu akzeptieren, jedoch diese Regelung nicht auf Funknetze anzuwenden. Sollten andere Firmen diesem Arrangement folgen, könnten weitere zeitraubende Gerichtsverfahren unnötig werden. Der amerikanische Kongress scheint diese Art von Kompromisslösung ebenfalls zu bevorzugen – schließlich sorgen sich insbesondere Republikanische Abgeordnete um eine zu große staatliche Beteiligung in der Wirtschaft. Angesichts der zunehmenden Verschmelzung ehemals getrennter Ton-, Video- und Datenübertragung sowie dem Trend vom Festnetz zum Mobilfunknetz, scheint es ratsam, dass der *Telecommunications Act of 1996* den Neuerungen grundlegend angepasst wird, um die weitere Entwicklung des Internets nicht zu gefährden.

Andere Themen wie Urheberschutz, Vorratsdatenspeicherung und Schutz der Privatsphäre werden ebenfalls diskutiert, aber generell von der Diskussion um die Netzneutralität in den Schatten gestellt, da diese die größten Firmeninteressen gegeneinander aufstellt. Stattdessen nimmt das Interesse an internationalen Aspekten der Netzpolitik zu: die Bedeutung des Internets bzw. neuer Technologien im Freiheitskampf unterdrückter Völker und die damit verbundene Zusammenarbeit amerikanischer Technologiefirmen bei der politischen Zensur in repressiven Regimestaaten. Neben diesen innenpolitischen Entscheidungen anderer Länder hat die Gefahr des Cyberterrorismus bzw. der -kriegsführung zunehmend an Gewicht gewonnen, nachdem sie bereits in Estland und Georgien in den letzten Jahren „erfolgreich" demonstriert wurde.

NETZDURCHDRINGUNG

Angesichts der Vielzahl ernstzunehmender innen- und außenpolitischer Probleme der USA, wird die Netzpolitik in der amerikanischen öffentlichen Debatte eher als ein Randthema wahrgenommen. Unabhängig davon schafften es gut vernetzte Blogger und Konsumentenorganisationen im

Jahr 2008, eine Frage zur Position der Demokratischen Präsidentschaftskandidaten zur Netzneutralität während der MTV/MySpace-Debatte als die am meisten gewünschte Zuschauerfrage zu wählen.[1]

Auch wenn das Thema in der amerikanischen Öffentlichkeit nur bedingt diskutiert wird, so sind sich die Politiker der Bedeutung von *Internet Governance* natürlich mehr als bewusst. Es existieren über 700 Millionen Computer in den USA und 65 Prozent der Haushalte des Landes verfügen über Broadband-Internetzugänge – ihre Zahl hat sich innerhalb der letzten vier Jahre verdoppelt.[2] Von Dezember 1999 bis Dezember 2007 wuchs die Zahl der Anschlüsse mit einer Übertragungsgeschwindigkeit von mindestens 200 kbps von 2,8 Millionen auf 121,2 Millionen.[3] Laut der Information, Technology & Innovation Foundation ist die amerikanische Wirtschaft innerhalb der letzten zehn Jahre aufgrund des Internets um zwei Billionen Dollar gewachsen, wobei ein jährliches Wachstum um 300 Milliarden Dollar bei einer kompletten Internetabdeckung des Landes möglich wäre, so die Beratungsfirma TechNet.[4]

Trotz dieser ermutigenden Zahlen sehen sich die USA vor der Realität eines wachsenden Rückstandes gegenüber zahlreichen europäischen und asiatischen Ländern: u.a. liegt man bei den Datenübertragungsraten zurück, gewisse Bevölkerungsschichten und ländliche Regionen bleiben weiterhin nicht oder nur schwach vernetzt. Der FCC zufolge haben zwischen 92 und 95 Prozent der Haushalte Zugriff auf einen Netzbetreiber, 78 Prozent haben die Wahl zwischen zwei Anbietern, jedoch können sich lediglich vier Prozent zwischen drei oder mehr Zugangsanbietern entscheiden. Die FCC betrachtet diesen Zustand für die Förderung eines gesunden Wettbewerbs als unzureichend.[5]

Mit der stetig wachsenden Bedeutung des Internets für die wirtschaftliche Entwicklung der amerikanischen Informationsgesellschaft in den letzten zehn Jahren, in der zunehmend alle Bereiche des Lebens vom Internet beeinflusst werden, beschäftigt man sich daher mit der Frage, wie man zukünftiges Wachstum und Innovation fördern könnte – wie man ein neues Google ermöglichen könnte, so Präsident Obama. Aus diesem Grund hatte er sich bereits als Präsidentschaftskandidat im Wahlkampf für Netzneutralität stark gemacht und versprochen, mehr staatliche Mittel für den Ausbau des Breitbandnetzes zur Verfügung zu stellen.

INFORMATIONS- ODER KOMMUNIKATIONSDIENSTE?

In den vergangenen Jahren gab es im Kongress eine Reihe von Gesetzesinitiativen zur Netzneutralität des Internets, die es allerdings nicht geschafft haben, von beiden Häusern verabschiedet zu werden.[6] Deswegen basieren die Richtlinien der Federal Communications Commission immer noch weitestgehend auf dem mittlerweile antiquierten *Telecommunications Act* von 1996, welcher seinerseits nur eine, wenn auch in Anbetracht des zeitlichen Abstands natürlich wesentliche, Erneuerung des ersten *Communications Act* aus dem Jahr 1934 darstellt. Das Gesetz von 1996 kreierte die FCC und gab ihr die Aufgabe und Vollmacht sicherzustellen, dass Dienstleistungsunternehmen wie Festnetz- und Funknetztelefonanbieter, Radiosender, sowie Kabel- und Satellitenfernsehanbieter als *common carriers,* also öffentliche Versorgungsunternehmen, handelten. Diese sollten allen Nutzern ihre Dienstleistungen gleichwertig anbieten und durften diesbezüglich keine Unterschiede zwischen einzelnen machen.

Damals ging es in dem Gesetz aber mehr um die Sicherstellung des Wettbewerbes unter den sieben regionalen Festnetztelefonanbietern. Deren Märkte waren zuvor noch geographisch begrenzt gewesen, was 1996 aufgehoben wurde. Damit konnten die sieben Firmen gegenseitig ihre Netze nutzen, wobei die Nutzungsgebühr staatlich reguliert wurde. Gleichzeitig wurde neuen Wettbewerbern der Zugang zu den Netzen dieser Telefonanbieter erleichtert, wodurch die ersten Internetdienste angeboten werden konnten. Verständlicherweise tauchte der Begriff *Broadband* 1996 nur einmal im Gesetzestext auf, der Begriff *Internet* immerhin elfmal.[7]

Allerdings differenzierten die Abgeordneten 1996 bei der Vergabe des *common carrier* Mandats noch zwischen Telekommunikations- und Informationsdienstleistern. Diese Unterscheidung hatte jedoch innerhalb weniger Jahre zu Problemen geführt, da Netzanbieter, die ihr Telefonnetz nutzten, um Internetzugänge anzubieten (z.B. DSL), strenger kontrolliert wurden und mehr an den Staat abführen mussten, als Netzbetreiber, die den gleichen Service über ihr Kabelfernsehnetzwerk anboten: erstere waren nach dem 1996er Gesetz Telekommunikationsdienstleister, letztere Informationsdienstleister.

Diese Regeln wurden daraufhin 2005 gelockert und DSL-Internetanbieter auch als Informationsdienstleister deklariert. Parallel dazu gab es in diesen Jahren auch erste juristische Herausforderungen. Eine Reihe von Netzbetreibern (z.B. Cox Communications und AT&T) hatten begonnen, ihren Kunden Nutzungseinschränkungen vorzuschreiben sowie anderen Dienstleistungsanbietern Nutzungsrechte an ihren Netzen zu verweigern (VoIP).[8]

Daraufhin wurden 2005 vier Prinzipien mit einem *Internet Policy Statement* eingeführt, welche die „common carrier" Regeln ersetzen sollten. Jedoch stellten sie keine juristisch verbindlichen Regeln dar und waren insoweit nicht einklagbar.[9]

Internetnutzer sollten demnach:

1. Zugang zu allen gewünschten legalen Daten erhalten,
2. jegliche Anwendungen ausführen können,
3. jegliche Geräte anschließen dürfen, die das Netzwerk des Anbieters nicht schädigen, sowie
4. zwischen verschiedenen Netzbetreibern aussuchen können.

Kritiker empfanden diese vier Punkte als zu vage, um als Richtlinien zu gelten, trotzdem wurden diese im Kongress nicht weiter mit einer entsprechenden Gesetzgebung spezifiziert.[10]

NETZNEUTRALITÄT UNTER OBAMA

Angesichts der Langwierigkeit einer Reform des *Communications Act of 1996* versucht die Regierung Präsident Obamas einen anderen Weg zu gehen und das Ziel der Netzneutralität über die FCC zu erreichen. Die *Federal Communications Commission* wurde mit dem *Communications Act* im Jahre 1934 eingeführt, um die verschiedenen Kommunikationswege (Radio-, Fernseh-, Kabel-, Satelliten- und Leitungsübertragung) zu regulieren und damit sicher zu stellen, dass alle Bürger einen preiswerten und gleichwertigen Zugang zu Kommunikationsdienstleistungen haben. Die Kommission besteht aus fünf Mitgliedern, die vom Präsidenten für fünf Jahre ernannt und vom Senat bestätigt werden. Zu keiner Zeit dürfen mehr als drei Mitglieder einer Partei Teil der Kommission sein.[11]

Der neue Aufsichtsratsvorsitzende der Kommission, Julius Genachowski, begann nun zu versuchen, die oben genannten Prinzipien zumindest in bundesweite Vorschriften zu verwandeln und dabei zwei weitere Regeln hinzuzufügen: Netzanbieter sollten einerseits Datenpakete, Anwendungen und Dienstleistungen neutral behandeln sowie andererseits Informationen darüber freigeben, wie sie die übertragenen Datenmengen auf ihren Netzwerken verwalten.[12]

DER NATIONALE BREITBANDPLAN

Nachdem sich Präsident Obama bereits als Kandidat im Wahlkampf für Netzneutralität stark gemacht und versprochen hatte, mehr staatliche Mittel für den Ausbau des Breitbandnetzes zur Verfügung zu stellen, erfüllte er dieses Versprechen bereits zum Teil. Das Konjunkturpaket vom letzten Jahr enthielt 7,2 Milliarden Dollar für Studien und Darlehen, um die flächendeckende Breitbandversorgung zu fördern.[13] Gleichzeitig forderte der Kongress die dafür zuständige *Federal Communications Commission (FCC)* dazu auf, einen National Broadband Plan zu entwerfen. Im Sinne des „open governments" ging die FCC unter ihrem neuen Vorsitzenden Julius Genachowski mit gutem Beispiel voran, öffnete sich vor einem Jahr für Vorschläge von Bürgern, Konsumentenorganisationen und Netzbetreibern und veröffentlichte nach 45 öffentlichen Veranstaltungen und 74.000 Seiten mit Kommentaren ihren Plan.

Dieser Plan besteht aus vier Programmpunkten:

1. Einerseits soll die Breitbandnetzinfrastruktur erweitert werden, wobei insbesondere die Abdeckung in ländlichen Regionen in zehn Jahren für alle erschwinglich sein soll.
2. Diesbezüglich sollen zudem mindestens 15,5 Milliarden Dollar aus den Mitteln des Universal Service Fund, der momentan die Festnetztelefonabdeckung fördert, für Breitbandabdeckung aufgewendet werden.
3. Gleichzeitig soll der Wettbewerb unter Netzanbietern stimuliert und damit der Nutzen für die Verbraucher gefördert werden.
4. Des Weiteren soll Maßnahmen bzgl. Cybersecurity gefördert werden – sowohl was die Verhinderung des Missbrauchs von Daten angeht als auch was Wirtschaftsspionage aus dem Aus- und Inland betrifft.

Bei diesen Punkten soll die Netzneutralität dabei aber nur indirekt gefördert werden: Netzanbieter die Mittel in Anspruch nehmen wollen, müssten sich auch dazu verpflichten, Netzneutralität auf ihren Netzen gelten zu lassen.[14]

Vor kurzem hat jedoch ein U.S. Appeals Court beschlossen, dass die FCC nicht die Vollmacht hat, den Breitbandanbietern Netzneutralität aufzuzwingen.[15] Dabei befasste sich das Berufungsgericht mit einer Klage des Netzanbieters Comcast, der 2007 die Peer-to-Peer Firma BitTorrent auf seinem Netz beschränkt hatte. Comcast verteidigte sein Handeln damals und argumentierte, dass dies nötig geworden sei, um allen Nutzern weiterhin den ungehinderten Zugang zu ermöglichen – die exzessive Nutzung von Peer-to-Peer Verbindungen hätte das Netz zu sehr belastet. Laut BitTorrent hat Comcast damit aber gegen das I*nternet Policy Statement* der FCC verstoßen. Die FCC stimmte der Beschwerde von BitTorrent später zu und rief Comcast dazu auf, in Zukunft spezifische Dienstleister nicht zu diskriminieren.[16]

Comcast ging daraufhin in Berufung, so dass die FCC sich gezwungen sah, ihre Befugnis zu verteidigen: In dem Gerichtsfall berief sich die FCC auf ihre *ancillary authority* (sekundäre Vollmacht), da Netzanbieter nicht mehr als *common carrier*-Telekommunikationsdienstleister klassifiziert würden, und verwies auf die soeben verabschiedeten Vorschriften, welche die weitere Entwicklung des Internets sichern und landesweit effiziente Kommunikationsdienstleistungen ermöglichen sollten. Aus Sicht des Gerichts waren diese Vorschriften jedoch nur „policy statements" und als solche keine wirklichen Gesetze. Insofern hat die FCC offenbar vorerst keine Befugnis, bei den verschiedenen Breitbandanbietern die Netzneutralität zu erzwingen.[17]

Die Auseinandersetzung um dieses Problem ist damit natürlich noch lange nicht zu Ende. Es bestünde nun die Möglichkeit für Genachowski, sämtliche Breitbandanbieter wieder als Telekommunikationsdienstleister zu klassifizieren und sie damit wieder wie *common carrier,* also öffentliche Versorgungsunternehmen, zu regulieren. Diese Position wäre legal vielleicht inzwischen vertretbar: Im Jahr 2002 favorisierten drei der neun Obersten Richter (u.a. der konservative Richter Antonin Scalia) diese Klassifizierung im Fall *NCTA v. Brand X*.[18] Allerdings wäre auch in diesem Fall nicht ganz klar, ob die FCC die Befugnis dafür hat und deshalb würde sich wohl eine Flut von Klagen anschließen.

Stattdessen sucht Genachowski einen Kompromiss – Netzanbieter sollen wieder als öffentlichen Versorgungsunternehmen deklariert werden, allerdings unter Befreiung von der Mehrheit der damit verbundenen strikten Auflagen. Sie müssten sich jedoch neu verpflichten, keine Diskriminierung beim Dienstleistungsangebot und bei der Gebührenberechnung zu praktizieren, was der Netzneutralitätsdefinition sehr nahe kommen würde.

Die Umsetzung dieses Plans hätte wahrscheinlich den Rest des Jahres in Anspruch genommen, worauf es jahrelange gerichtliche Auseinandersetzungen gegeben hätte, bis schließlich der Kongress eingeschritten wäre – der letzte Reformprozess dauerte auf diese Weise nahezu zwanzig Jahre und wurde erst vor vierzehn Jahren abgeschlossen. Insoweit überrascht es nicht, dass es eine Reihe von Politikern im Kongress bevorzugt, sich weitestgehend aus diesem Prozess herauszuhalten. Der Demokratische Abgeordnete und Vorsitzende des zuständigen *House Energy and Commerce*-Ausschusses, Henry Waxmann, sowie sein Kollege im Senat und Vorsitzende des *Committee on Commerce, Science, and Transportation*, Jay Rockefeller, wollen z.B., dass die FCC ihre Strategie gemeinsam mit den Netzanbietern entwickelt und möchten sich nur auf lange Sicht direkt engagieren. Eine ähnliche Ansicht vertritt auch der *Information Technology Industry Council*, der vor zu strenger Regulierung warnt, da diese die wirtschaftliche Entwicklung stören könnte. Die Republikanischen Kollegen im Abgeordnetenhaus und Senat dürften jedoch hinsichtlich der Aktivitäten der FCC eine ganz andere Sichtweise vertreten – sie sprechen ihr generell das politische Mandat ab: Gesetze würden immer noch im Kongress geschrieben, so die Senatorin Kay Bailey Hutchison.[19]

CLASH OF THE TITANS?

Die Mehrheit der Netzanbieter hatte währenddessen angedeutet, dass sie die Netzneutralität weiterhin einhalten würde – ohne explizit dazu gezwungen zu werden. Jedoch würden sie sich das Recht vorbehalten, in Zukunft höhere Raten für gewisse Datenpakete bzw. Webseiten zu berechnen oder den Zugang zu ihnen einzuschränken, weil sie zu viel Kapazität in Anspruch nehmen würden. Die Argumentation war hier vergleichbar mit der in anderen Ländern. Ohne die Aussicht auf hohe Profitmargen würden Internetanbieter wie Verizon, AT&T und Comcast keine Mittel auf der Wall Street einholen können, um ihre Netze auszubauen und neue Innovationsvorhaben zu realisieren. Ihre Netze wären

bereits jetzt zum Teil überladen von dem Datenflusszuwachs, der gesteuert werden müsse. Gemeinsam mit ihren Lobbyfirmen und Interessenverbänden wie der CTIA Wireless Association kämpfen sie schlichtweg um die Entscheidungshoheit über ihre Netze.[20]

Walter McCormick, der CEO der *U.S. Telecom Association,* meint, dass die Regierung sehr wohl das Problem des privaten Investment versteht und daher die Gesetzgeber (bisher) Netzneutralität nicht genauer bzw. strenger definierten, als wie es die Netzanbieter momentan praktizieren würden.[21] Die Netzanbieter würden neue Technologien entwickeln, die ihre Dienstleistungen verbessern würden und diese müssten finanziert aber auch unterstützt werden. So führte er die Maßnahmen zum Schutz gegen Cyberattacken an und verwies auf die normale Priorität von wichtigeren Kunden – sollte die Übermittlung von medizinischen Daten wie Röntgenbildern genauso behandelt werden wie ein Hamstervideo auf YouTube?

Auch argumentiert AT&T, dass Google seinen Suchmaschinenservice ebenfalls zur Netzneutralität verpflichten sollten, sonst könnte die Firma die Webseiten ihrer Partner favorisieren. Davon abgesehen sorgen sich die Netzanbieter jedoch vor allem darum, dass ihnen *net neutrality* Gesetzgebung nicht erlauben würde, dem Geschäftsmodell der Unterhaltungsindustrie zu folgen und ihre Netze mit exklusiven Angeboten ihrer Partner unter den Filmstudios, Spieleentwicklern, Handyherstellern und Fernsehkanälen zu kombinieren.[22] Die Breitbandausweitung wäre für sie schlichtweg wichtiger als die Netzneutralität.

Damit könnte es allerdings langfristig zu immer weniger Firmen kommen, die zudem vertikal integriert wären und nicht unbedingt ein Interesse an technologischer Neuerungen hätten – eine Entwicklung, die erklären würde, warum die USA bereits in den letzten Jahren bei der qualitativen Netzabdeckung im Vergleich zu anderen OECD Staaten zurückgefallen sind, meinen Kritiker. Zu ihnen gehören vor allem Google, Amazon, Ebay und Facebook, die von zahlreichen Konsumentenorganisationen wie Public Knowledge und Free Press sowie Think Tanks wie der Sunlight Foundation, dem Center for Democracy and Technology als auch der Electronic Frontier Foundation tatkräftig unterstützt werden. Gemeinsam mit den zahlreichen Lobbyisten dieser Internetfirmen bilden diese Gruppen jedoch nur eine schnell wechselnde Allianz die sich von Thema zu Thema ändert. Sie wollen jedoch alle u.a. sicher stellen, dass kleine bzw.

neue Unternehmen ihre Dienstleistungen gleichberechtigt anbieten könnten, damit ein nächstes Google nicht verhindert, damit freie Meinungsentfaltung nicht behindert und damit Innovationen ohne spezielle Erlaubnis von den Netzanbietern getätigt werden können, so David Sohn von Center for Democracy and Technology.

IST DIE SCHLACHT ABGEWENDET?

Mit jährlichen Ausgaben in Millionenhöhe für ihre Lobbyisten schienen sich die beiden Lager um Google und Verizon nun nicht nur juristisch zu belangen, sondern begannen auch sich aktiver in der politischen Debatte zu bekriegen. Anfang August überraschten die beiden Firmen jedoch mit einem Kompromissvorschlag, der von Netzneutralitätsbefürwortern mit einem Dolchstoß für Genachowskis Kompromissvorschlag gleichgesetzt wurde.

Man einigte sich darauf, Netzneutralität für die Datenübermittlung per Festnetz weitestgehend zu akzeptieren, jedoch diese Regelung nicht auf Funknetze anzuwenden. So würde Verizon für bestimmte Dienstleistungen wie der qualitativ hochwertigen Übermittlung von medizinischen Daten und besonderen Unterhaltungsprogrammen zusätzliche finanzielle Mittel erhalten. Diese Entscheidung wurde kurz nach dem Ende der Verhandlungen zwischen der FCC und den Internetanbietern bekanntgegeben.[23] Sollten andere Firmen diesem Arrangement folgen, könnten weitere zeitraubende Gerichtsverfahren unnötig werden und der Rest des Sektors und die FCC sich dieser Lösung eventuell anschließen. Der amerikanische Kongress scheint diese Art von Kompromisslösung ebenfalls zu bevorzugen – schließlich sorgen sich insbesondere Republikanische Abgeordnete, um eine zu große staatliche Beteiligung in der Wirtschaft.

1| Glaser, Mark, „TechPresident, 10 Questions Put Spotlight on ‚Voter-Generated Content‘," PBS, 28. November 2007, http://www.pbs.org/mediashift/2007/11/techpresident-10questions-put-spotlight-on-voter-generated-content332.html.
2| Hatch, David, „The FCC Keeps It Broad," National Journal, 20.03.2010.
3| Figliola, Patricia Moloney und Gilroy, Angele A., und Kruger, Lennard G., The Evolving Broadband Infrastructure: Expansion, Applications, and Regulation (Washington, DC: Congressional Research Service, 2009)
4| Wasserman, Elizabeth, „Charging Up for the Next New Things", CQ Weekly, 09.07.2007, S. 2017-2022.

5| Perine, Keith, „The Medium, Or the Message?" CQ Weekly, 10.05.2010, S. 1140-1144.
6| Tessler, Joelle, „House Vote 239: Telecommunications Overhaul." CQ Weekly, 01.01.2007, S. 62-62, und Tessler, Joelle, „2006 Legislative Summary: Telecommunications Overhaul." CQ Weekly, 18.12.2006, S. 3370-3370, und Wasserman, Elizabeth, „Charging Up for the Next New Things," CQ Weekly, 09.07.2007, S. 2017-2022.
7| Wasserman, Elizabeth, „The New Telecom Wars: Looking to Update A Landmark Law," CQ Weekly, 14.11.2005, S. 3049-3056.
8| „Controlling the Internet," CQ Researcher, 12.05.2006.
9| Kroepsch, Adrianne, „Obama Win Yields Shift in High-Tech Priorities," CQ Weekly, 01.12.2008, S. 3187-3189.
10| Ruane, Kathleen Ann, The FCC's Authority to Regulate Net Neutrality after Comcast v. FCC (Washington, DC: Congressional Research Service, 2010)
11| Figliola, Patricia Moloney, The Federal Communications Commission: Current Structure and Its Role in the Changing Telecommunications Landscape (Washington, DC: Congressional Research Service, 2010).
12| Anderson, Nate, „FCC Chairman wants network neutrality, wired and wireless," ars technica Webseite, 21. September 2009, http://arstechnica.com/tech-policy/news/2009/09/fcc-chairman-wants-network-neutrality-wired-and-wireless.ars.
13| Kruger, Lennard G., Broadband Infrastructure Programs in the American Recovery and Reinvestment Act (Washington, DC: Congressional Research Service, 2010)
14| Munro, Neil, „Obama's Tech Plans Put Telecoms On The Defensive," National Journal, 14.03.2009, und Muno, Neil, „Tech Giants Anything But Neutral In Access Fight," National Journal, 20.03.2010.
15| Pike, George, „What the Future Holds for Net Neutrality," Information Today, Juni 2010, Jahrgang 27, Nr. 6, S. 1,45.
16| Perine, Keith, „The Medium, Or the Message?" CQ Weekly, 10.05.2010, S. 1140-1144.
17| Brauer-Rieke, Aaron K., „The FCC Tackles Net Neutrality: Agency Jurisdiction and the Comcast Order," Berkeley Technology Law Journal, Jahrgang 24, S. 593-615, und Perine, Keith, „The Medium, Or the Message?" CQ Weekly, 10.05.2010, S. 1140-1144 und Ruane, Kathleen Ann, The FCC's Authority to Regulate Net Neutrality after Comcast v. FCC (Washington, DC: Congressional Research Service, 2010)
18| Ruane, Kathleen Ann, The FCC's Authority to Regulate Net Neutrality after Comcast v. FCC (Washington, DC: Congressional Research Service, 2010).
19| Perine, Keith, „The Medium, Or the Message?" CQ Weekly, 10.05.2010, S. 1140-1144.
20| Wasserman, Elizabeth, „Charging Up for the Next New Things," CQ Weekly, 09.07.2007, S. 2017-2022.
21| Munro, Neil, „Obama's Tech Plans Put Telecoms On The Defensive," National Journal, 14. März 2009.
22| Munro, Neil, „Obama's Tech Plans Put Telecoms On The Defensive," National Journal, 14.03.2009, und Muno, Neil, „Tech Giants Anything But Neutral In Access Fight," National Journal, 20.03.2010.
23| Shilds, Todd und Stone, Brad, „The FCC's Crusade to Keep the Internet Free," Bloomberg Bussinesweek, 11.08.2010.

<< zurück zum Inhaltsverzeichnis

GROSSBRITANNIEN

Laura Johnson

1. NETZPOLITISCHE FRAGEN IN DER POLITISCHEN DEBATTE

Die Bedeutung netzpolitischer Fragen in der politischen Debatte Großbritanniens hat in den letzten Jahren spürbar nachgelassen. Das ist einerseits auf die thematische Dominanz der Finanzkrise zurückzuführen und liegt andererseits daran, dass der rechtliche Rahmen zu einem gewissen Grad ausgereift ist. Ausgewählte Themen haben jedoch die Aufmerksamkeit einer Reihe von Parlamentsmitgliedern und der Mainstreampresse erlangt. Dazu gehören die Pläne für eine großangelegte Speicherung persönlicher Daten wie durch das *Interception Modernisation Programme* (IMP, Abhör-Modernisierungsprogramm) zur Speicherung von Daten des Kommunikationsverkehrs sowie einer geplanten umfangreichen Datenbank von Patientendaten des *National Health Service* (Staatlicher Gesundheitsdienst).[1] Vorschläge der Regierung, gegen illegalen Datentausch hart durchzugreifen, lösten ebenso erhebliche politische Diskussionen aus[2] wie auch – durch einen aktuellen Telefonabhörskandal sowie enorme Datenverluste der Regierung im Jahre 2007 – Fragen der Datensicherheit und des Datenschutzes. Obwohl diese Themen nicht mit dem Internet zu tun haben, sondern mit Papier- und Datenträgerverlusten bzw. mit dem Abhören von Telefonen verbunden sind, zeigen sie, dass ein ähnlicher Vorfall bezüglich der Sicherheit elektronischer Daten umfangreiche Medienberichterstattung erlangen und eine öffentliche Debatte zum Thema provozieren könnte. Derzeit ist die Debatte über die meisten internetbezogenen Themen aber auf die spezialisierten Technologieseiten der Presse sowie auf die Computerpresse beschränkt.

2. DIE DISKUSSION UM EINE VORRATSDATENSPEICHERUNG

Die erste Aufforderung des britischen Innenministeriums an Telekommunikationsdienstleister, Daten zu speichern, geschah unter einem *Voluntary Code of Practice on Data Retention* (Freiwilligen Verhaltenskodex zur Vorratsdatenspeicherung) auf der Grundlage des Zweiten Teils des *Anti-Terrorism, Crime and Security Act* (Anti-Terror-, Verbrechens- und Sicherheitsgesetz) von 2001. Der Verhaltenskodex forderte die Speicherung von Kundenstammdaten und Telefoniedaten für einen Zeitraum von zwölf Monaten; SMS-, E-Mail und Internetdienstanbieterdaten für einen Zeitraum von sechs Monaten; und Internet-Aktivitätsprotokollen (einschließlich besuchter URLs) für einen Zeitraum von vier Tagen. Zu den Daten gehörten Nutzerdaten und Verkehrsdaten. Die Speicherung von Inhalten, beispielsweise was in einem Telefonanruf oder einer E-Mail tatsächlich gesagt wurde, war nicht gefordert und nicht erlaubt. Die spezifischen Daten bezüglich E-Mail-Verkehr waren: Benutzername, Datum und Uhrzeit des Ein- und Ausloggens, IP-Adresse, von der aus eingeloggt wurde, sowie der Benutzername, die E-Mail-Adressen in den Feldern „Von", „An" und „CC", „Datum" und „Uhrzeit" gesendeter und empfangener E-Mails.[3]

Der Verhaltenskodex erlaubte also die Vorratsdatenspeicherung durch Telekommunikationsanbieter für geschäftliche Zwecke, etwa Kundenabrechnung, über den dafür erforderlichen Zeitraum hinaus, bis zu den oben genannten Zeiträumen. Allerdings, wenn die von einem Unternehmen gespeicherten Daten den Zeitraum für geschäftliche Zwecke überschritten, mussten sie als solche gekennzeichnet werden, und das Unternehmen durfte nicht für eigene Zwecke darauf zugreifen. Die Vorratsdatenspeicherung unter diesen Richtlinien kam dem *Data Protection Act* (Datenschutzgesetz) von 1998 nach, da es unter Absatz 5 von Anhang 2 des Gesetzes fiel, „dass es notwendig ist, dass der Telekommunikationsanbieter Daten speichert, um dem Innenminister zu ermöglichen, seinem Auftrag zum Schutz der nationalen Sicherheit nachzukommen". Sicher-

heits-, Nachrichtendienst- und Vollstreckungsbehörden konnten Zugang zu Kommunikationsdaten, die unter dem freiwilligen Verhaltenskodex gespeichert wurden, erhalten, und zwar gemäß dem bestehenden *Regulation of Investigatory Powers Act* (RIPA, Gesetz über die Regulierung von Untersuchungsbefugnissen) von 2000, das vom *Information Commissioner* (Datenschutzbeauftragter) überwacht wird[4] (siehe Abschnitt 3).

Im März 2009 hat das Vereinigte Königreich in Übereinstimmung mit der Politik der EU den abschließenden Teil der EU-Richtlinie über die Vorratsdatenspeicherung 2006/24/EC bezüglich des Zugangs zu Internet, E-Mail und Internettelefonie verabschiedet. Die Richtlinie verlangte, dass Internetdienstanbieter in den Mitgliedstaaten für einen Zeitraum zwischen sechs Monaten und zwei Jahren Kommunikationsdaten speichern – Daten darüber, wer mit wem kommuniziert hat, und wann. Mit der Entscheidung für einen Zeitraum von zwölf Monaten hat das Vereinigte Königreich faktisch den bestehenden Verhaltenskodex in eine verbindliche Rechtsvorschrift umgewandelt. Bevor die EU-Rechtsvorschriften angenommen wurden, wurden mehrere Themen bezüglich der Machbarkeit angesprochen. Es ging dabei darum, ob kleine Internetdienstanbieter über die Finanzkraft und die Technologie verfügten, um die neuen Vorschriften zur Speicherung und zur Abfrage von Daten einzuhalten.[5] Dies war besonders deswegen für die Regierung von Belang, da sie Internetdienstanbietern für die zusätzlichen Kosten, die durch die Einhaltung der neuen Rechtslage entstehen würden, kompensieren sollte, so wie sie es bereits unter dem freiwilligen Kodex für mehrere der großen Internetdienstanbieter praktiziert.[6] Die Regierung berücksichtigte dies, indem sie bestimmte, dass die größeren Kommunikationsdienstleister, beispielsweise BT, die bereits in großem Umfang Daten speichern, auch für die Sammlung des Datenverkehrs kleinerer Nutzer verantwortlich seien. Deswegen würde die Regierung nur diese größeren Anbieter für die Abfrage von Daten kompensieren müssen und nicht für deren Speicherung. Daher würden nur diejenigen Kommunikationsdienstleister, die vom Minister einen formalen Bescheid erhalten, verpflichtet sein, Kommunikationsdaten zur Einhaltung von EU-Vorschriften zu speichern. Der Minister muss einen solchen Bescheid ausstellen, es sei denn, ein anderer Dienstleister speichert bereits die in Rede stehenden Daten.[7] Wie beim freiwilligen Kodex unterliegt der Zugang zu den gespeicherten Informationen über Internet- und E-Mail-Nutzung dem RIPA.

Um die EU-Frist einzuhalten, wurde die Richtlinie im März 2009 in britisches Recht als eigenständige Rechtsverordnung umgesetzt. Daher war die Zustimmung von Parlamentsabgeordneten nicht erforderlich. Allerdings war geplant worden, dass die Richtlinie Teil eines breiter angelegten *Communications Data Bill* (Kommunikationsdatengesetzentwurf) sein sollte. Der geplante *Communications Data Bill*, der bis heute nicht ins Parlament eingebracht worden ist, war angelegt, um die EU-Richtlinie in Form des für die spätere Umsetzung des langfristigen *Interception Modernisation Programme* (IMP) notwendigen Gesetzes zu ergänzen.

Das IMP wurde etabliert, um neue Technologien sowie Möglichkeiten zur Implementierung der Sammlung, Speicherung und Abfrage von Daten aus dem Internet zu untersuchen. Es sollte Pläne für die Öffnung von Datenpaketen und den Zugriff und die Aufzeichnung von Daten erarbeiten, beispielsweise darüber, wer über soziale Netzwerke wie Facebook, Webmail, Instant Messenger sowie Online-Spiele wen kontaktiert hat, und wann. Diese Pläne gehen über die von der EU-Richtlinie vorgesehenen Pläne zur Datenspeicherung weit hinaus. Im Januar 2010 wurde die Schaffung einer neuen Abteilung im britischen Innenministerium, das *Communications Capabilities Directorate* (CCD, Abteilung für Kommunikationsressourcen), angekündigt. Das neue CCD besteht aus zwei separaten Teams: Das eine ist für hergebrachtes Abhören, etwa von Telefonen, zuständig, während das zweite am IMP arbeitet.[8]

Ein weiterer Aspekt des IMP, der vor mehreren Jahren zur Diskussion gestellt wurde, hatte die Planung einer zentralisierten Datenbank für Daten des Kommunikationsverkehrs zum Gegenstand. Daten der Nutzer aller Kommunikationsdienstleister sollten in einem einzigen zentralen System gesammelt werden. Solche Pläne wurden angeblich von den Geheimdiensten vorangetrieben, besonders vom *Government Communications Headquarters* (GCHQ, Hauptquartier der Regierung für Kommunikation), das in einem Programm namens *„Mastering the Internet*" („Beherrschung des Internets"), an Technologien und Methoden arbeitet, um Erkenntnisse aus großen Mengen von Überwachungsdaten zu extrahieren. Diese Pläne für eine enorme zentralisierte Datenbank wurden vor einigen Jahren derart heftig kritisiert, dass man davon ausgehen muss, dass sie aufgegeben wurden. Die Kritik machte sich hauptsächlich daran fast, dass eine solche Datenbank die Behörden in die Lage versetzen würde, die Beantragung einzelner Daten gemäß RIPA zu vermeiden, und dass daher der Zugang zu Daten ohne bedeutende Kosten (die gegen-

wärtig durch die Bearbeitung einzelner Anfragen entstehen) oder Kontrolle durch den *Interception of Communications Commissioner* (Beauftragter für das Abhören von Kommunikation) möglich würde. Überdies behaupteten Technologieexperten, dass die Datenbank noch nicht einmal im Kampf gegen den Terrorismus, dem ausdrücklich genannten Hauptgrund für ihre Einrichtung, Erfolg haben würde. Ängste bezüglich falscher Ergebnisse und der Beschuldigung unschuldiger Kommunikationsnutzer waren weitere herausragende Kritikpunkte.[9]

Die Zukunft aller Pläne für die Speicherung elektronischer Daten ist seit Amtsantritt der neuen Koalitionsregierung starken Zweifeln ausgesetzt. Die Arbeit am *Interception Modernisation Programme* (IMP) wird gegenwärtig fortgesetzt. Allerdings verspricht die Koalitionsvereinbarung, die die Konservativen und die Liberalen bei ihrem Amtsantritt unterzeichnet haben, das „Ende der Speicherung von Internet- und E-Mail-Daten ohne guten Grund", und es ist bislang unklar, was dies genau nach sich ziehen wird. Großbritannien hat bereits die EU-Richtlinie über die Vorratsdatenspeicherung in nationales Recht umgesetzt, und es ist unwahrscheinlich, dass diese Entscheidung revidiert werden wird, da das Land einer der Hauptbefürworter dieses Programms in Europa ist. Wahrscheinlich wird es einen immensen Druck der Sicherheitsbehörden geben, um im Rahmen des IMP die Pläne zu *Deep Packet Inspection* und sogar einer großen zentralisierten Datenbank, in die bereits erhebliche Gelder investiert worden sind, fortzusetzen.[10]

3. DATENSCHUTZ UND DATENSICHERHEIT IN GROSSBRITANNIEN

Die drei Hauptgesetze, die Datenschutz und Datensicherheit im Vereinigten Königreich regeln, sind das *Computer Misuse Act* (Computermissbrauchsgesetz, 1990), das *Data Protection Act* (1998) und das *Regulation of Investigatory Powers Act* (2000).

Das *Computer Misuse Act* definierte, was bezüglich des Zugangs zu Rechnern als strafbar zu bezeichnen war und was nicht, und spezifizierte drei Typen von Straftaten. Der erste Typ ist der wissentliche Versuch, sich ohne Befugnis Zugang zu einem Programm oder zu Daten auf einem Rechner zu verschaffen. Gemäß dem zweiten Typ ist es eine Straftat, sich unautorisierten Zugang zu einem Rechner zu verschaffen, in der Absicht, weitere Straftaten zu begehen oder zu fördern, beispielsweise

die Beschaffung von Finanz- oder Verwaltungsdaten. Der dritte Typ umfasst unautorisierte Handlungen mit der Absicht, den Betrieb eines Rechners, eines Computerprogramms oder von auf einem Rechner gespeicherten Daten zu beeinträchtigen, oder Zugang zu auf einem Rechner gespeicherten Programmen oder Daten zu ver- oder behindern. Das Gesetz legt die Strafen für solche Taten dar, und zwar eine Gefängnisstrafe von nicht mehr als zwölf Monaten in England und Wales oder sechs Monaten in Schottland, oder eine Geldstrafe, die über das gesetzliche Höchstmaß nicht hinausgeht.[11]

Das *Data Protection Act*, das eine EU-Richtlinie in britisches Recht umsetzte, etablierte die Prinzipien und Anforderungen für die Speicherung persönlicher Daten. Das Gesetz verpflichtet Organisationen, die persönliche Daten verarbeiten, sich an mehrere Prinzipien zu halten: Dass die Daten fair und rechtmäßig verarbeitet werden; dass sie für begrenzte Zwecke verarbeitet werden; dass die Verarbeitung angemessen, relevant und nicht unverhältnismäßig ist; dass sie richtig und auf dem neuesten Stand ist; dass die Daten nicht länger als notwendig gespeichert werden; dass die Verarbeitung mit individuellen Rechten konform ist; dass sie sicher ist und dass Daten nicht in andere Länder übermittelt werden, die keinen angemessenen Schutz vorsehen. Das Gesetz stattet Einzelpersonen mit dem Recht aus, zu erfahren, welche Informationen über sie gespeichert werden, sowie unrichtige Informationen zu korrigieren.[12] Das *Information Commissioner's Office* (Büro des Informationsbeauftragten), eine unabhängige britische Stelle, ist u.a. dafür zuständig, die Prinzipien des *Data Protection Act* durchzusetzen. Sie berät Organisationen über die Einhaltung des Gesetzes und Bürger über ihre Rechte gemäß dem Gesetz und betreibt eine Beschwerdestelle für Bürger, die der Ansicht sind, dass eine Organisation die Bedingungen des *Data Protection Act* verletzt. Das *Commissioner's Office* zahlt nicht selbst Kompensation an Einzelpersonen, aber es kann bei der Durchsetzung des Gesetzes Organisationen zwingen, ihre Verfahrensweisen zu ändern, um das Gesetz einzuhalten.[13]

Im Jahr 2000 hat das *Regulation of Investigatory Powers Act* zum ersten Mal Vorschriften dargelegt, die die Befugnisse der öffentlichen Behörden, Überwachungen durchzuführen und Kommunikationen abzuhören, regelten. Das Gesetz umfasst sowohl wer einen Antrag auf Zugang zu gespeicherten Kommunikationsdaten, etwa gesendeten E-Mails, stellen kann, wie oben dargestellt, als auch wer Kommunikationen abhören kann, um

beispielsweise den Inhalt einer E-Mail zu lesen. Ermächtigungen zum Abhören müssen vom Minister autorisiert werden, aber autorisierte Stellen können direkt von den Kommunikationsdienstleistern Zugang zu gespeicherten Informationen verlangen. Zu den Stellen, die gemäß RIPA mittlerweile autorisiert sind, Zugang zu Informationen zu erlangen, gehören die Polizei, die Geheimdienste, der *National Criminal Intelligence Service* (Nationales Kriminalamt) und die *Serious Organised Crime Agency* (Stelle für ernsthafte organisierte Kriminalität), *HM Revenue and Customs* (das britische Finanzamt), NHS (der staatliche Gesundheitsdienst) und – möglicherweise am kontroversesten – Gemeinderäte. Einige wenige Vorfälle des Abhörens durch Gemeinderäte in Bagatellen haben erhebliche Aufmerksamkeit in der Presse erlangt.[14]

Solche Stellen erhalten nur dann Zugang zu gespeicherten Daten, wenn dies im Interesse

- der nationalen Sicherheit,
- der Verhütung oder Aufdeckung von Verbrechen oder Störungen,
- des wirtschaftlichen Wohlergehens des Vereinigten Königreichs,
- der öffentlichen Sicherheit,
- des Schutzes der öffentlichen Gesundheit,
- der Festsetzung oder Einziehung jeglicher Steuern, Zölle oder Umlagen, die an eine öffentliche Stelle zu zahlen sind,
- der Verhinderung von Tod oder Verletzung sowie
- der Verhinderung oder Minderung der Verletzung oder Schädigung der physischen oder psychischen Gesundheit eines Menschen ist.[15]

Der *Interception of Communications Code of Practice* (Verhaltenskodex zum Abhören von Kommunikationen) ergänzt RIPA, indem er Schutzmaßnahmen bezüglich des Zugangs zu Daten vorschreibt. Das *Investigatory Powers Tribunal* (IPT, Tribunal zu Überwachungsbefugnissen), eine unabhängige und unparteiische Stelle, existiert ebenfalls, um das Gesetz zu überwachen. Jeder, der der Ansicht ist, dass die Behörden die in RIPA niedergelegten Vorschriften bezüglich ihrer Person missachtet haben, kann an das IPT eine Beschwerde oder eine Rüge gemäß dem *Human Rights Act* (Gesetz über die Menschenrechte) einreichen, und das IPT wird die Angelegenheit untersuchen.[16]

Das Vereinigte Königreich versorgt außerdem öffentliche Stellen und kritische Bereiche der nationalen Infrastruktur mit technischer Unterstützung zum Schutz ihrer Systeme und ihrer Daten. Das *Centre for the Protection of National Infrastructure* (CPNI, Zentrum für den Schutz der nationalen Infrastruktur) bietet integrierte Sicherheitsberatung für die Organisationen und Unternehmen an, die die nationale Infrastruktur bilden, um ihre Verwundbarkeit zu reduzieren. Die von CPNI angebotene Sicherheitsberatung umfasst physische, personelle und informationstechnische Sicherheit. Regierungsstellen haben dabei zu gewährleisten, dass Schritte innerhalb ihres Arbeitsbereichs unternommen werden, um die Sicherheit zu verbessern und schützenswerte Infrastruktur zu identifizieren. Zu diesen Arbeitsbereichen gehören Kommunikation, Notdienste, Energie, Finanzen, Nahrungsmittel, Regierung, Gesundheit, Verkehr und Wasser. Zu den Beratungsleistungen für Organisationen und Unternehmen mit einer Infrastruktur von nationaler Bedeutung gehören Training und persönliche Beratung durch Teams aus auf den Arbeitsbereich spezialisierten Beratern und Experten, sowie Onlineberatung und Beratungsmaterialien. Das CPNI kann auch Wissen über Bedrohungen und Verwundbarkeiten mit Schlüsselstellen der nationalen Infrastruktur austauschen und Möglichkeiten vorschlagen, solche Bedrohungen abzuwenden. Außerdem existiert eine starke Partnerschaft zwischen dem CPNI, dem *National Counter Terrorism Security Office* (Nationales Antiterrorsicherheitsbüro) der Polizei und einem landesweiten Netzwerk spezialisierter *Counter Terrorism Security Advisers* (Antiterror-Sicherheitsberater) der Polizei, die das CPNI unterstützen, indem sie kritische Organisationen beraten. Eine Abteilung innerhalb des GCHQ, die *National Technical Authority for Information Assurance* (CESG, Nationale technische Behörde für Informationssicherung) unterstützt ebenfalls CPNI. Die CESG ist beim GCHQ für Informationssicherung (*information assurance*, IA) zuständig und erfüllt diese Aufgabe durch Beratung und Unterstützung zur Gewährleistung der Sicherheit von Kommunikations- und elektronischen Daten. Die CESG bietet ein Spektrum an technischer Beratung an, darunter Beratung zu spezifischen IA-Themen und Unterweisungen zum Einsatz kryptographischer und anderer zertifizierter IA-Produkte. Außerdem produziert die CESG Dokumentationen zur Systemsicherheit und berät bezüglich technischer Dokumentation. Die CESG unterstützt Regierungsstellen und -behörden, die Streitkräfte und die verschiedenen Organisationen und Unternehmen, die eine Infrastruktur von nationaler Bedeutung kontrollieren.[17]

Um Unternehmen und Organisationen, die nicht zur nationalen Schlüsselinfrastruktur gehören, zu helfen, wurden Industrienormen entwickelt, die Richtlinien für Unternehmen bezüglich der von ihnen umzusetzenden Datenschutzstrategien vorgeben. Eine private Initiative, *Stay Safe Online* (Bleib online sicher), unterstützt ebenfalls einzelne Bürger, Bildungsinstitutionen und kleine Unternehmen durch die Beratung über Datenschutz online.[18]

4. OPEN DATA – ÜBER DEN FREIEN ZUGANG ZU ÖFFENTLICHEN DATEN

Das *Freedom of Information Act* (Gesetz zur Wahrung des Rechts auf Auskunft) macht die inneren Abläufe des Regierungs- und Verwaltungshandeln gegenüber der Öffentlichkeit auskunftspflichtig. Das Gesetz ist auf fast alle öffentliche Behörden anzuwenden und auch auf Unternehmen, die im vollständigen Besitz der öffentlichen Behörden sind. Dies bedeutet, dass Anfragen nach Informationen gemäß dem Gesetz stattgegeben werden muss, es sei denn, die Information fällt unter eine der 23 aufgelisteten Ausnahmen.[19] Das Gesetz verlangt auch, dass öffentliche Behörden einen genehmigten Plan haben müssen, wie sie der Öffentlichkeit Informationen aktiv zugänglich machen. Das *Information Commissioner's Office*, das das *Freedom of Information Act* sowie die RIPA-Gesetzgebung überwacht, hat ein Modell für einen genehmigungsfähigen Publikationsplan entwickelt, den alle öffentlichen Behörden annehmen müssen. Dazu gehört die Art der Information, die zur Verfügung gestellt werden soll, einschließlich separater Richtlinien für bestimmte Typen von öffentlichen Stellen, wie etwa Schulen und Gemeinderäte. Außerdem wird gefordert, dass eine Anleitung zu den Typen von zur Verfügung stehenden Dokumenten von jeder Stelle geführt und veröffentlicht werden muss. Organisationen, die imstande sind, einen Internetauftritt zu verwalten, müssen gemäß dem Kodex Informationen online zur Verfügung stellen und sollen auch die entsprechende Anleitung auf ihrer Webseite an einem leicht auffindbaren Ort veröffentlichen.[20] Darüber hinaus ist es die Sache der einzelnen Stellen und Regierungsbehörden zu bestimmen, wieviele ihrer Informationen sie online zur Verfügung stellen. Die *Bank of England* und das *Office for National Statistics* (Büro für nationale Statistiken) verwalten öffentliche Zeitreihen ökonomischer Daten, und das *Land Registry* (Grundbuchamt) verkauft sogar Zugang zu den tatsächlich erzielten Immobilienpreisen online.[21]

5. DIE PRAXIS DER NETZZUGANGSSPERREN

Die *Internet Watch Foundation* (IWF, Stiftung zur Überwachung des Internets), eine 1996 geschaffene, selbstregulierte Stelle, unterhält eine Online-Hotline, an die Internetnutzer Internetseiten melden können, die potenziell illegale „Inhalte von sexuellem Missbrauch von Kindern, kriminellen Öbszonitäten mit Erwachsenen und Anstachelung zum Rassenhass" zeigen.[22] Für Internetseiten auf Servern im Vereinigten Königreich betreibt die Stiftung einen Dienst zur „Benachrichtigung und Entfernung", der Internetdienstleister und Hosting-Unternehmen über illegale Seiten benachrichtigt, sodass sie diese von ihren Netzwerken entfernen können. Für Seiten, die Bilder des Missbrauchs von Kindern zeigen und die auf Servern im Ausland liegen, moderiert IWF eine von der Branche angeführte Initiative, Zugang zu den jeweiligen Seiten zu sperren, indem sie Internetdienstleistern, Mobilfunkbetreibern, Suchmaschinen und Inhaltsanbietern eine Liste mit den URLs von Seiten, die sexuellen Missbrauch von Kindern zeigen, zur Verfügung stellt.[23] Diese Seiten werden gemäß britischem Recht bewertet, und jedes Bild wird entsprechend der Kriterien des britischen *Sentencing Guidelines Council* (Rat für Richtlinien zur Strafbemessung) kategorisiert. Die Liste enthält 500 bis 800 Webseiten und wird zweimal am Tag aktualisiert. Die Systeme und Prozesse von IWF werden von unabhängigen Experten periodisch untersucht und auditiert, und jedermann kann gegen die Beurteilung einer URL durch die IWF Rechtsmittel einlegen, wenn er glaubt, dass sie ihm den Zugang zu legalen Inhalten verwehren.[24]

In Zeitungen veröffentlichte Zahlen legen nahe, dass 98,5 Prozent der Internetdienstanbieter jetzt IWF benutzen, um illegale Seiten zu entfernen oder zu blockieren, aber die Regierung beginnt, in dieser Angelegenheit eine aktivere Rolle einzunehmen.[25] Im März dieses Jahres wurde öffentlichen Stellen verboten, Internetdienstanbieter zu nutzen, die solche vom IWF als Anbieter von Bildern des sexuellen Missbrauchs an Kindern eingestufte Webseiten nicht aktiv blockieren. Die Anweisung an alle Regierungsabteilungen, Behörden und *Quangos* (Quasi-Nichtregierungsorganisationen) besagte, dass diese neue Politik auf Internetunternehmen, Mobilfunkanbieter, Suchmaschinen und Filterunternehmen anzuwenden ist.[26]

Gemäß Absatz 3 des *Terrorism Act* (Terrorismusgesetz) von 2006 hat die Regierung das Recht, Internethostinganbieter im Vereinigten Königreich zu zwingen, extremistisches Material zu entfernen. Allerdings hat der ehemalige Sicherheitsminister Lord West zugegeben, dass die Vorschrift sich bislang als unnötig erwiesen hatte, da die Polizei die Hostingunternehmen im Vereinigten Königreich davon überzeugt hatte, solches Material freiwillig zu entfernen. Die Regierung hat gegenwärtig nicht die rechtliche Befugnis, solche Internetseiten zu blockieren, wenn sie im Ausland gehostet werden. Allerdings kann sie empfehlen, dass Filterunternehmen in ihren Jugendschutzeinstellungen solche Seiten aufnehmen, was bedeutet, dass sie für gewisse Nutzer, etwa in Schul- oder Collegenetzwerken, gesperrt wären.[27]

Was individuelle Nutzer betrifft, erlaubt der *Digital Economy Act* (Internetwirtschaftsgesetz), der am Ende der letzten Legislaturperiode verabschiedet wurde, dem Minister, Internetdienstanbieter anzuweisen, Nutzerkonten temporär zu sperren, wenn beurteilt wird, dass sie regelmäßig Copyrightregelungen verletzt haben.[28] Ein in letzter Minute eingebrachter Zusatz zu Klausel 8 des Gesetzentwurfs erlaubt dem Wirtschaftsminister auch, Internetdienstanbieter anzuweisen, „einen Ort im Internet [zu sperren], von dem das Gericht sich überzeugt hat, dass er für bzw. im Zusammenhang mit einer Aktivität, die das Urheberrecht verletzt, genutzt wurde, genutzt wird oder wahrscheinlich genutzt werden wird".[29]

6. KONFLIKTFELD URHEBERRECHT

Im Zusammenhang mit der Stärkung der Rechte von Urheberrechtsinhabern bei der Bekämpfung von Filesharing erwuchs jüngst ein Konflikt mit der Gesetzgebung. Das *Digital Economy Act* (Internetwirtschaftsgesetz), im April 2010 verabschiedet, hat eine Verfahrensweise für den Umgang mit Verletzungen des Online-Urheberrechts geschaffen, das Bücher, Filme und Musik umfasst. Gemäß dem Gesetz können Urheberrechtsinhaber, die der Ansicht sind, ihr Urheberrecht sei verletzt worden, einen Bericht über die Verletzung an den jeweiligen Internetdienstanbieter einreichen, in dessen Verantwortung es liegt, ein Verzeichnis von solchen Verletzungen durch Nutzer zu führen. Wenn Kunden eine vorgegebene Anzahl von Verletzungen erreichen, werden ihre IP-Adressen auf einer anonymen *Copyright Infringement List* (Urheberrechtsverletzungsliste) geführt. Urheberrechtsinhaber können mithilfe einer gerichtlichen Anordnung Zugang zur Liste bekommen und können dann gegen die die Verstöße

begehenden Kunden Verfahren eröffnen. Das Gesetz erhöht die Höchststrafe für Online-Urheberrechtsverletzungen. Kontrovers ist die auf dem Gesetz fußende Macht des Ministers, Internetdienstanbieter anzuweisen, technische Maßnahmen gegen Nutzer zu verhängen, die eine gewisse Anzahl von Verstößen erreichen. Dazu gehören Kappung der Bandbreite oder temporäre Sperrung eines Kontos.[30] Ein früherer Plan, dauerhaft den Internetzugang zu sperren, wurde im Juni 2009 ausgeschlossen.[31] Es liegt in der Verantwortung von *Ofcom*, der die Kommunikationsbranche regulierenden Behörde, die operationellen Details des Gesetzes auszuarbeiten. *Ofcom* ist die unabhängige Behörde zur Regulierung der Kommunikationsbranche, insbesondere bezüglich des Wettbewerbs. Sie ist für Fernsehen, Radio, Festnetz- und Mobiltelekommunikation sowie die Funkwellen drahtloser Geräte zuständig. Gemäß dem *Communications Act* (Kommunikationsgesetz) von 2003 ist es die rechtliche Pflicht der Behörde, die Interessen von Bürgern und Konsumenten zu fördern, indem sie eine breitgefächerte qualitativ hochwertige Programmgestaltung sicherstellt, Konsumenten vor anstößigen Inhalten schützt, und, ganz entscheidend, eine große Auswahl an elektronischen Kommunikationsdienstleistungen, darunter Breitband, gewährleistet.[32]

Die Vorschriften des *Digital Economy Act* von 2010 selbst, und dazu *Ofcoms* Entwurf für einen Kodex für dessen Umsetzung, haben unter den verschiedenen betroffenen Parteien erhebliche Kontroversen ausgelöst. Bedenken sind bezüglich der zum Nachweis von Verstößen heranzuziehenden Standards aufgekommen, denn die Pläne von *Ofcom* legen weder die Mittel zur Beschaffung von Beweismitteln noch das erforderliche Beweismaß fest.[33] Es wird befürchtet, dass alle Nutzer einer IP-Adresse für die Handlungen einer einzigen Person bestraft werden, zum Beispiel, dass Eltern für illegales Herunterladen durch ihre Kinder verantwortlich gemacht werden. Pläne, den Internetzugang zu sperren, werden außerdem durchweg als Angriff auf die Bürgerrechte verurteilt.[34] Weitere Kontroversen sind in jüngster Zeit bezüglich der finanziellen Arrangements für die neue Politik aufgekommen. Die Finanzlast für die Verfolgung von Personen, die illegal Daten herunterladen, soll entsprechend dem Gesetz gemeinsam von Urheberrechtsinhabern und Kommunikationsdienstleistern im Verhältnis 75:25 getragen werden. Auf der einen Seite haben Urheberrechtsinhaber gegen die Tatsache protestiert, dass sie gezwungen werden, für den größeren Teil der finanziellen Belastung aufzukommen. Die Regierung hat den Gesetzesentwurf mit der Begründung gerechtfertigt, die Maßnahmen würden die Kreativwirtschaft um

etwa 200 Milliarden GBP pro Jahr begünstigen, und dass es deswegen angemessen sei, dass Urheberrechtsinhaber den Großteil der Kosten zu tragen hätten. Auf der anderen Seite der Debatte, so argumentiert eine Verbraucherschutzgruppe, bestehe die Gefahr, dass die Internetdienstleister die zusätzlichen Kosten als Preiserhöhungen an die Verbraucher weitergeben. Im Ergebnis könnten sich Tausende Konsumenten „keinen Breitbandzugang mehr leisten".[35] Dies, so wird behauptet, widerspricht direkt der Politik der Regierung, Breitbandzugänge ausweiten zu wollen.[36]

7. PROGRAMME ZUR FLÄCHENDECKENDEN BREITBAND-VERSORGUNG

Ende Januar 2009 hat der Kommunikationsminister der Labour Party eine „universelle Bereitstellungsverpflichtung" bekanntgegeben, nach der bis zum Jahre 2012 jeder Haushalt in Großbritannien die Möglichkeit eines Breitbandzugangs mit einer Geschwindigkeit von mindestens 2Mbps haben soll. Dieses Versprechen war eines von mehreren, die im Bericht „*Digital Britain*" (Digitales Großbritannien) vom selben Monat enthalten sind.[37] Der Plan sah vor, dass die Regierung und private Netzwerkdienstleister zusammenarbeiten sollten, um die Netzabdeckung auszuweiten. Die Regierung beabsichtigte, eine Steuer in Höhe von 0,50 GBP auf alle Festnetztelefonanschlüsse einzuführen, um die Umsetzung dieser Verpflichtung zu finanzieren.[38] Allerdings wurde die Steuer vor den Wahlen im Mai aufgegeben und im neuen Budgetentwurf des Finanzministers vom Juni vollständig abgeschafft.[39] Da es weder rechtlichen Rückhalt gab, um die Verpflichtung seitens der Internetdienstanbieter durchzusetzen, noch Subventionen, um die Ausweitung des Angebots zu fördern, wurden Bedenken laut, ob das von der Regierung formulierte Ziel überhaupt zu erreichen sei. Eine Schätzung aus der jüngsten Zeit legt nahe, dass 160.000 Haushalte immer noch überhaupt keinen Breitbandzugang bekommen können, und etwa zwei Millionen Haushalte lediglich über Verbindungen unter 2 Mbps verfügen.[40]

Am 15. Juli hat der neue Kulturminister Jeremy Hunt das Datum für das Erreichen der vollständigen Netzabdeckung auf 2015 verschoben. BT hat sich bereits verpflichtet, 2,5 Milliarden GBP aufzuwenden, um sein Glasfaserbreitbandnetz auszubauen, warnte jedoch, dass es ohne Unterstützung durch die Regierung nicht darüber hinaus gehen könne.[41] Die Regierung plant, Gelder bereitzustellen, um die Ausweitung der Netzabdeckung zu unterstützen, indem sie budgetierte, aber nicht ausgegebene Gelder eines Plans zum Umschalten auf Digitalfernsehen verwendet.[42] Eine Stelle namens *Broadband Delivery UK* (BDUK, Sicherstellung des Breitbandzugangs im Vereinigten Königreich), die innerhalb des *Department for Business Innovation and Skills* (BIS, Abteilung für Unternehmensinnovation und -fähigkeiten) eingerichtet wurde, ist für die Entwicklung von Plänen zur Umsetzung des neuen Versprechens der Regierung und die effektive Investition öffentlicher Gelder zuständig. Der erste Schritt dieser Stelle wird es sein, drei Marktversuche in ländlichen Gebieten durchzuführen. Dabei soll untersucht werden, wie staatliche Mittel in Gegenden, in denen die Einrichtung von Hochgeschwindigkeitsinternetzugängen am wenigsten ökonomisch interessant ist, am besten eingesetzt werden können.[43]

8. ZIVILGESELLSCHAFT UND NETZPOLITIK

Mehrere verschiedene Interessenverbände nehmen an der Debatte über Internetfragen teil. Sie reicht von formalen Konsultationen der Regierung mit großen Industrieverbänden, etwa der Bankengruppe APACS, bis hin zum informellen Druck, der von bestimmten Teilen der Wählerschaft auf Parlamentsmitglieder ausgeübt wird, um beispielsweise besseren Breitbandzugang in ländlichen Wahlkreisen zu erreichen. Einige Verbände wurden speziell zum Zweck der Interaktion mit der Regierung über diese Themen etabliert. Der *Information Assurance Advisory Council* (IAAC, Beirat für Informationssicherung) beispielsweise, dessen Ziel es ist, „für die Schaffung einer sicheren Informationsgesellschaft zu arbeiten", bringt Entscheidungsträger aus Wirtschaft, Politik, Strafverfolgungsbehörden sowie der Forschung zusammen, um Ideen auszuarbeiten. Die Mitglieder seines *Government Liaison Panel* (Verbindungsgremium zur Regierung) kommen aus einem breiten Spektrum an Regierungs- und Sicherheitsstellen, darunter dem *UK Office of Cyber Security* (Büro für Cybersicherheit des Vereinigten Königreichs), dem *Centre for the Protection of National Infrastructure*, dem Verteidigungsministerium und der *Serious Organised Crime Agency*.[44]

Viele andere Gruppen verschiedenster Couleur existieren, um auf die Regierung Druck auszuüben, etwa *Privacy International* (Datenschutz International) und die *Open Rights Group* (Gruppe offene Rechte).[45] Die Regierung kann mit solchen Gruppen mittels Konsultationen über Gesetzesentwürfe, formale Eingaben und Teilnahme an parlamentarischen Anhörungen interagieren. Sie kann aber auch weniger formale

Kanäle wie etwa Veranstaltungen von *Chatham House*, *The Royal Institute of International Affairs* dafür nutzen.

Übersetzung ins Deutsche: Sandra H. Lustig

1| *David Leppard, „There's no hiding place as spy HQ plans to see all", The Sunday Times, 05.10.2008. http://www.timesonline.co.uk/tol/news/uk/article4882622.ece (Letzter Zugriff 22.9.2010); James Sturke und Denis Campbell, „NHS database raises privacy fears, says doctors", guardian.co.uk, 07.03.2010, 18.40 GMT. http://www.guardian.co.uk/society/2010/mar/07/nhs-database-doctors-warning (Letzter Zugriff 25.09.2010).*

2| *Kevin Anderson, „Government details proposed filesharing crackdown", guardian.co.uk, 25. August 2009 12.16 GMT. http://www.guardian.co.uk/media/2009/aug/25/internet-file-sharing-digitalbritain (Letzter Zugriff 14.09.2010).*

3| *Home Office Retention of Communications Data under Part II: Anti-Terrorism, Crime & Security Act 2001: Voluntary Code of Practice, Appendix A. http://www.opsi.gov.uk/si/si2003/draft/5b.pdf (Letzter Zugriff 13.09.2010).*

4| *Home Office Retention of Communications Data under Part II: Anti-Terrorism, Crime & Security Act 2001: Voluntary Code of Practice http://www.opsi.gov.uk/si/si2003/draft/5b.pdf (Letzter Zugriff 13.09.2010).*

5| *Chris Williams, „Home Office preps fudgetastic ISP data rules: Cash-strapped Whitehall gives small ISPs free pass", The Register, 13. Oktober 2008 14:10 GMT. http://www.theregister.co.uk/2008/10/13/home_office_eudrd/ (Letzter Zugriff 14.09.2010).*

6| *Ebd.*

7| *Chris Williams, „UK.gov to tap BT as data harvester", The Register, 16.02.2009, 09:52 GMT. http://www.theregister.co.uk/2009/02/16/eu_data_retention_transposition/ (Letzter Zugriff 15.09.2010).*

8| *„Entanet raises concern over government's communications interception plans", infosecurity.com, 16. Februar 2010 http://www.infosecurity-magazine.com/view/7341/entanet-raises-concern-over-governments-communications-interception-plans/ (Letzter Zugriff 15.09.2010).*

9| *Chris Williams, „UK.gov £12bn comms überdatabase ‚wouldn't spot terrorists'" The Register, 08.10.2008 12:19 GMT. http://www.theregister.co.uk/2008/10/08/us_gov_data_mining_report/ (Letzter Zugriff 15.09.2010); Chris Williams, „Confusion reigns ahead of comms überdatabase debate", The Register, 09.01.2010, 13:57 GMT. http://www.theregister.co.uk/2009/01/09/imp_eudrd/ (Letzter Zugriff 14.09.2010).*

10| *Chris Williams, „ConLibs leave open question over net surveillance", The Register, 14.05.2010 10.02 GMT, http://www.theregister.co.uk/2010/05/14/conlib_imp/ (Letzter Zugriff 13.09.2010).*

11| *Government Legislation Website: Computer Misuse Act 1990 http://www.legislation.gov.uk/ukpga/1990/18/contents (Letzter Zugriff 21.09.2010).*

12| *Government Legislation Website: Data Protection Act 1998 http://www.legislation.gov.uk/ukpga/1998/29/schedule/1 (Letzter Zugriff 21.09.2010); Information Commissioner's Office Website: Data Protection Act http://www.ico.gov.uk/for_the_public/the_acts.aspx (Letzter Zugriff 22.09.2010).*

13| *Information Commissioner's Office http://www.ico.gov.uk/complaints/data_protection.aspx (Letzter Zugriff 22.09.2010).*

14| *„Spy law 'used in dog fouling war'", BBC News, 27.04.2008 11.35 GMT. http://news.bbc.co.uk/1/hi/uk/7369543.stm (Letzter Zugriff 26.09.2010).*

15| *Government Legislation Website: Regulation of Investigatory Powers Act 2000 http://www.legislation.gov.uk/ukpga/2000/23/contents (Letzter Zugriff 21.09.2010).*

16| *Ebd.; Der Richter in einem Verfahren vor dem Europäischen Gerichtshof für Menschenrechte hat kürzlich ein Urteil gegen einen Bürger des Vereinigten Königreichs gefällt. Dieser hatte dargelegt, dass sein Menschenrecht auf „Achtung [seines] Privat- und Familienlebens, [seiner] Wohnung und [seiner] Korrespondenz" (Artikel 8 der Konvention zum Schutze der Menschenrechte und Grundfreiheiten) durch angebliches auf der Grundlage von RIPA autorisiertes Abhören verletzt worden sei. Der Richter lobte die Vorschriften des RIPA und die diesbezügliche Rechtsprechung des IPT. („UK's secret surveillance regime ‚does not breach human rights'„, The Register, 20.05.2010, 08:02 GMT. http://www.theregister.co.uk/2010/05/20/surveillance_human_rights_ruling/ (Letzter Zugriff 17.09.2010).*

17| *The National Technical Authority for Information Assurance website http://www.cesg.gov.uk/ (Letzter Zugriff 26.09.2010).*

18| *Stay Safe Online Website http://www.staysafeonline.org/ (Letzter Zugriff 26.09.2010).*

19| *Government Legislation Website: Freedom of Information Act 2000 (http://www.legislation.gov.uk/ukpga/2000/36/schedule/1?view=plain); Bezüglich Leitlinien über Ausnahmen siehe The Information Commissioner's Office website http://www.ico.gov.uk/for_organisations/freedom_of_information/information_request/reasons_to_refuse.aspx (Letzter Zugriff 27.09.2010).*

20| *The ICO Model Publication Scheme http://www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/generic_scheme_v1.0.pdf (Letzter Zugriff 27.09.2010).*

21| *Bank of England website http://www.bankofengland.co.uk/statistics/gdpdatabase/ (Letzter Zugriff 26.09.2010); Office for National Statistics website http://www.statistics.gov.uk/cci/nugget.asp?id=192 (Letzter Zugriff 26.09.2010); The Land Registry Website http://www.landsearch.net/landregistry/?gclid=CIf6stWrraQCFYGX2AodRmCQcg (Letzter Zugriff 26.09.2010).*

22| *Internet Watch Foundation Website http://www.iwf.org.uk/ (Letzter Zugriff 26.09.2010).*

23| *Ebd. http://www.iwf.org.uk/public/page.103.htm (Letzter Zugriff 26.09.2010).*

24| *Ebd. http://www.iwf.org.uk/public/page.148.htm (Letzter Zugriff 26.09.2010).*

25| *Jane Merrick, „Internet providers face child porn crackdown", The Independent, 0609.2009. http://www.independent.co.uk/news/uk/crime/internet-providers-face-child-porn-crackdown-1782530.html (Letzter Zugriff 18.09.2010).*

26| *Sean O'Neill, „Government ban on internet firms that do not block child sex sites", The Times, 10.03.2010. http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article7055882.ece (Letzter Zugriff 18.09.2010).*

27| *Chris Williams, „UK Gov moves to block Hamas kids site", The Register, 14.01.2010. http://www.theregister.co.uk/2010/01/14/ellman_hamas/ (Letzter Zugriff 18.09.2010).*

28| *Richard Taylor, „The Digital Economy Act 2010 and online copyright infringement", The Law Gazette, 9. September 2010. http://www.lawgazette.co.uk/in-practice/the-digital-economy-act-2010-and-online-copyright-infringement (Letzter Zugriff 17.09.2010).*

29| *Charles Arthur, „Digital economy bill rushed through wash-up in late night session", guardian.co.uk, 8. April 00.05 BST. http://www.guardian.co.uk/technology/2010/apr/08/digital-economy-bill-passes-third-reading (Letzter Zugriff 17.09.2010).*

30| *Richard Taylor, „The Digital Economy Act 2010 and online copyright infringement", The Law Gazette, 9. September 2010. http://www.lawgazette.co.uk/in-practice/the-digital-economy-act-2010-and-online-copyright-infringement (Letzter Zugriff 24.09.2010).*

31| *Kevin Anderson, „Government details proposed filesharing crackdown", guardian.co.uk, 25. August 2009 12:16 BST. http://www.guardian.co.uk/media/2009/aug/25/internet-file-sharing-digitalbritain (Letzter Zugriff 23.09.2010).*

32| *Ofcom website. http://www.ofcom.org.uk/about/what-is-ofcom/ (Letzter Zugriff 07.10.2010).*

33| *„Draft filesharing code flawed, says Open Rights Group", Charles Arthur, guardian.co.uk, 22. Juli 2010 15.40 BST. http://www.guardian.co.uk/technology/2010/jul/22/filesharing-ofcom-open-rights-group (Letzter Zugriff 23.09.2010).*

34| *Kevin Anderson, „Government details proposed filesharing crackdown", guardian.co.uk, 25. August 2009 12:16 BST. http://www.guardian.co.uk/media/2009/aug/25/internet-file-sharing-digitalbritain (Letzter Zugriff 23.09.2010).*

35| *Mark Sweney, „Illegal downloads: music industry to carry cost of catching pirates", guardian.co.uk, 14.09.2010, 15:37 BST. http://www.guardian.co.uk/technology/2010/sep/14/illegal-downloads-music-industry (Letzter Zugriff 24.09.2010).*

36| *Kevin Anderson, „Government details proposed filesharing crackdown", guardian.co.uk, 25. August 2009 12:16 BST. http://www.guardian.co.uk/media/2009/aug/25/internet-file-sharing-digitalbritain (Letzter Zugriff 23.09.2010).*

37| *Digital Britain: The Final Report http://interactive.bis.gov.uk/digitalbritain/report/executive-summary/universal-service-committment/ (Letzter Zugriff 17.09.2010).*

38| *Jane Wakefield, „Broadband tax ‚to be made law'", BBC News, 23.09.2009, 12:56 GMT http://news.bbc.co.uk/1/hi/8270772.stm (Letzter Zugriff 15.09.2010).*

39| *Chris Williams, „Broadband tax scrapped in ‚wash-up'", The Register, 07.04.2010, 12:14 GMT. http://www.theregister.co.uk/2010/04/07/broadband_cider/ (Letzter Zugriff 15.09.2010).*

40| *Graeme Wearden, „Broadband target put back to 2015", guardian.co.uk, 15.07.2010, 17:54 BST. http://www.guardian.co.uk/technology/2010/jul/15/fast-broadband-target-put-back (Letzter Zugriff 15.09.2010).*

41| *Ebd.*

42| *Department for Business Innovation & Skills website: Broadband Delivery UK, http://www.bis.gov.uk/BDUK (Letzter Zugriff 15.09.2010).*

43| *Ebd.*

44| *The Information Assurance Advisory Council website http://www.iaac.org.uk/ (Letzter Zugriff 24.09.2010).*

45| *Privacy International website http://www.privacyinternational.org/ (Letzter Zugriff 27.09.2010); Open Rights Group website http://www.openrightsgroup.org/ (Letzter Zugriff 27.09.2010).*

<< zurück zum Inhaltsverzeichnis

SPANIEN

SPANISCHE PERSPEKTIVEN ZU KONTROLLE UND MEINUNGSFREIHEIT IM INTERNET

Hans Günter Kellner

Rund die Hälfte der spanischen Haushalte hat Zugang zum Internet, fast alle davon verfügen über einen Breitbandanschluss, sei es per ADSL oder Kabel. Einer Studie der „Fundación Orange" des französischen Telekommunikationskonzerns France Telekom zufolge (eEspaña 2010[1]) sind die Breitbandanschlüsse vor allem in den Metropolenregionen Madrid und Katalonien besonders weit verbreitet, was die Autoren nicht nur der Beliebtheit dieser Anschlüsse zuschreiben, sondern auch ihrer Verfügbarkeit. In Flächenregionen wie Kastilien-La Mancha, Kastilien-León oder der Extremadura wird vielerorts aufgrund der hohen Kosten für die notwendigen Investitionen kein DSL oder Kabelanschluss angeboten. Einen Rechtsanspruch auf Internet gibt es nicht.

Am meisten nutzen die Spanier das Internet, um ihre E-Mails zu lesen. Im europäischen Vergleich ragt in Spanien vor allem der Konsum der Informationsmedien im Internet heraus. 64 Prozent der Spanier mit Netzanschluss lesen Zeitungen im Internet (EU: 43 Prozent), 42 Prozent hören Radio oder sehen dort fern (EU: 37 Prozent). 32 Prozent der Spanier besuchen auch soziale Netzwerke wie Facebook und Tuenti, eine Art spanische Version des deutschen StudiVZ. Die Beschwerden über die schlechten Datenschutzstandards bei US-amerikanischen „Social Networks" teilt auch die spanische Datenschutzbehörde. Die Zusammenarbeit mit dem spanischen Netz „Tuenti" lobt die Behörde hingegen. Tuenti fordert seine Nutzer notfalls auch auf, eine Kopie des Personalausweises einzusenden, um die Altersangaben zu überprüfen. Bei unter 14-Jährigen ist das elterliche Einverständnis Voraussetzung für die Teilnahme an einem virtuellen sozialen Netzwerk.

Unterdurchschnittlich bleibt hingegen das Einkaufen und Internetbanking: Weniger als 40 Prozent der spanischen Internetnutzer tätigen Überweisungen im Internet, in der EU sind es schon die Hälfte. Der Gebrauch von P2P-Netzwerken zum Austausch urheberrechtlich geschützter Werke ist in Spanien der Musikindustrie zufolge weit verbreitet, der Nachweis mit verlässlichen Zahlen fehlt hier jedoch. Der Studie eEspaña 2010 zufolge tauschten 2009 rund elf Prozent der spanischen Internetnutzer Filme aus, rund 7,5 Prozent Musik. Diese Zahlen sind im Vergleich zum Vorjahr rückläufig.

RECHTLICHER RAHMEN

Die spanische Internetgesetzgebung ist relativ neu. Erst am 1. Juli 2002 verabschiedete das Parlament das „Gesetz über die Dienstleistungen der Informationsgesellschaft und den elektronischen Handel", abgekürzt LSSI. Dem Gesetzgeber ging es dabei vor allem um die Rechtssicherheit für den Handel im Internet. Das Gesetz bedeutete die Umsetzung der zwei Jahre zuvor vom EU-Parlament und dem EU-Rat beschlossenen Richtlinie 2000/31/EU und zudem bereits älterer Verbraucherschutzbestimmungen der Union.

Darüber hinaus behandelt der Text aber auch Fragen der Freiheiten von Anbietern von Inhalten und der Rechte der Nutzen. Vor allem war es damals auch der erste rechtliche Rahmen für die Kontrolle der Beteiligten im Netz. Noch während der parlamentarischen Beratungen wurden auch EU-Bestimmungen zum Datenschutz und zur Speicherung von Verbindungsdaten, besuchter Internetseiten und elektronischer Kommunikationen umgesetzt. Das Gesetz ist beispielhaft für die Probleme, nationale Gesetze im globalen Netz umzusetzen. So ist in Spanien offiziell unerwünschte Werbung – „spam" – verboten, was die Spanier in der Praxis jedoch auch nicht effektiver vor Angeboten aller Art, Gewinnspielen oder Bauerntricks schützt.

Während der größte Teil des Gesetzes zur Zeit der parlamentarischen Beratungen in der Öffentlichkeit kaum Beachtung fand, wurden gerade die Fragen der Kontrolle und sogar die Möglichkeiten der Schließung von Internetauftritten heftig debattiert. Von einem „Gesetz Orwell" wurde gesprochen, von der Wiedereinführung einer Zensurbehörde. In den folgenden Jahren wurde das Gesetz aktualisiert, aber die Zensur-Befürchtungen haben sich nicht bestätigt.

BEKÄMPFUNG STRAFRECHTLICH RELEVANTER INHALTE

Spaniens erst 1978 installierte parlamentarische Demokratie hat sich traditionell schwer getan mit der Kontrolle von Inhalten, nicht nur im Internet, sondern in allen Formen von Veröffentlichungen. Als Beispiel dafür darf der Umgang mit rechtsradikalen und verfassungsfeindlichen Schriften gelten, die in Spanien bis in die 1990er Jahre gedruckt, gehandelt und somit leicht zu kaufen waren. Dadurch wurde das Land zu einem der wichtigsten Umschlagsplätze solcher Literatur. Dahinter verbarg sich nicht etwa ein tatsächlicher gesellschaftliche Einfluss solcher Gruppierungen, sondern der Gedanke, dass eine demokratische Gesellschaft auch undemokratische Tendenzen nicht unterdrücken darf, sondern im offenen Diskurs mit ihnen stehen muss, und sich gerade so als besonders stark und wehrhaft erweist.

Erst mit der Ausweitung der Bekämpfung des Terrorismus der ETA auch auf die Schriften von Organisationen, die für die Justiz unter der Kontrolle des Terrornetzwerks stehen, setzte sich die Meinung durch, dass auch die Meinungsfreiheit in einer Demokratie Grenzen haben muss. Mit einem völlig überarbeiteten Strafrecht wurden 1995 schließlich Schriften, „die den Völkermord negieren oder rechtfertigen oder die zum Ziel haben, Regime zu installieren, die den Völkermord beabsichtigen" auf die gleiche Stufe mit Schriften gestellt, die den Terrorismus verherrlichen. Ganz offensichtliche Straftaten, wie etwa Kinderpornografie, waren schon damals auch als Veröffentlichungen verboten.[2]

DER FALL BATASUNA

2002 wurden auf der Grundlage eines neuen Parteiengesetzes die Partei Batasuna, der politische Arm der ETA, sowie einige weitere Nachfolgeorganisationen verboten. Der Europäische Gerichtshof bestätigte das Verbot. In der Folge sollten auch die Aktivitäten der Partei im Internet eingestellt werden. Dieser Fall ist exemplarisch für die Funktionsweise des Gesetzes und auch für die Probleme seiner Anwendung.

Auch in Spanien hat die Justiz einen schnellen Zugang zu Servern im Inland. Service-Provider haben zwar nicht die Pflicht, die Inhalte auf ihren Servern zu überwachen, müssen sie aber vom Netz nehmen, sobald die Untersuchungsgerichte sie dazu auffordern. Mit dem Gesetz von 2002 wurde auch möglich, den Zugang zu Seiten im Netz zu beschränken, also nicht nur die Kontrolle des Angebots, sondern auch der Nachfrage, wenn ein Richter dies anordnet.

Der bekannte Untersuchungsrichter Baltasar Garzón gab damals die Anweisung, mehrere Webseiten Batasunas von Spanien aus unzugänglich zu machen. Diese Sperrung des Zugangs zu bestimmten Seiten ermöglichte das damals neue Internetgesetz LSSI. Das Prinzip ist einleuchtend: Wenn die Justiz keinen Zugang zu den Servern im Ausland hat, wo diese Auftritte gespeichert sind, soll zumindest der Zugang von dem Territorium aus nicht möglich sein, für das sie bestimmt sind. Es soll folglich nicht die Straftat an sich verhindert werden, da sich dies als unmöglich herausstellt, sondern ihre Folgen im Inland.

Im Fall batasuna.org und mehreren ähnlichen Seiten hatte das Untersuchungsgericht die internationale Registrierungsorganisation ICANN (*Internet Corporation for Assigned Names and Numbers*) aufgefordert, diese URLs zu löschen, und auch keine Registrierungen von neuen Seiten mit den Namen Batasuna, Euskal Herritarrok oder Herri Batasuna zu ermöglichen. Zudem wurden mehrer Server in Australien und den USA aufgefordert, die Domain batasuna.org und ähnliche weitere zu löschen. Doch keiner dieser Adressaten wollte die Zuständigkeit der spanischen Justiz anerkennen, zumal die Seiten teilweise noch von Frankreich aus registriert worden waren. Andere Domains wurden unter der Angabe falscher Identitäten registriert. So soll auch der ehemalige sozialistische Politiker Ernest Lluch eine Seite für den politischen Arm der ETA registriert haben, was nicht eines besonderen Zynismus entbehrt: Lluch war zuvor von der ETA ermordet worden. Als Adresse des angeblichen Domain-Besitzers wurde das Haus angegeben, in dem die Terroristen Lluch erschossen hatten. Erst Jahre nachdem der Zugang von Spanien aus unterbunden wurde, verschwanden die Seiten aus dem Netz.

Der Fall Batasuna zeigt folglich die Schwierigkeiten der Arbeit der Strafverfolgungsbehörden im Internet, die sich durchaus auf andere Straftaten übertragen ließen, wie etwa die in Deutschland intensiv diskutierte Frage zum Umgang mit Kinderpornografie im Internet.

DATENSPEICHERUNG

Während die Möglichkeiten zur Sperrung von Seiten heftige Proteste auslösten, wurden in Spanien nur wenige Vorbehalte gegen die Auflagen zur Speicherung der Verbindungsdaten durch die Serviceprovider artikuliert. Sie müssen ein Jahr lang die IP-Nummern zur Identifizierung der Nutzer speichern und darüber hinaus jede damit verknüpfte Netzaktivität. So kann die Polizei auf richterliche Anordnung bis zu einem Jahr nachverfolgen, wer welche Seiten besucht, und insbesondere welche Inhalte auf Servern im Netz gespeichert hat. Gegen eine ähnliche Bestimmung zur Positionsbestimmung im Mobilfunknetz hatten Verbraucherschützer hingegen lauter protestiert. Sie ermöglichen der Polizei den Ort eines aktiven Mobiltelefons zu ermitteln – und dies mit einer Frist von einem Jahr auch rückwirkend. Die Inhalte von E-Mails müssen die Serviceprovider hingegen nicht speichern.

URHEBERRECHT: ALLES ERLAUBT?

Die spanische Musikindustrie schlägt Alarm. In fünf Jahren werde es keine spanische Musikproduktion mehr geben, wenn die Regierung den Schutz der Autorenrechte verbessere, klagt der Liedermacher Luis Eduardo Aute, andere etablierte Musikgruppen wie Ketama haben sich getrennt, weil ihre Platten zwar als illegale Kopien reißenden Absatz fanden, aber nicht in den CD-Läden. Die Zahlen sprechen eine deutliche Sprache: Für 2009 gab der Branchenverband der Musikindustrie einen Umsatzrückgang von 126,5 Millionen Euro auf 77 Millionen bekannt. Ähnlich argumentiert die Filmindustrie: Filmax, eine der bekanntesten Produktionsgesellschaften, hat Konkurs angemeldet. Die großen Musik- und Filmverlage haben demzufolge in nur sechs Jahren 90 Prozent ihrer Beschäftigten entlassen. [c]

Schuld habe daran der mangelnde Respekt vor dem Urheberrecht, behauptet die Kulturindustrie, und selbst die US-amerikanische Regierung, die Spanien in ihren Jahresberichten über Urheberrechtsverletzungen aufgenommen hat.[4] Spanischen Zeitungen zufolge soll sogar US-Präsident Obama bei Spaniens Regierungschef Zapatero angerufen haben, um ihn zu einer Gesetzesreform zu drängen.[5]

Kritik findet bei der US-Regierung insbesondere eine Anweisung der spanischen Generalstaatsanwaltschaft an die Staatsanwaltschaften in den Provinzen, Urheberrechtsverletzungen nicht als Straftaten zu werten, wenn dabei kein Gewinnstreben nachweisbar ist. Allerdings folgt die Staatsanwaltschaft damit nur der geltenden Rechtsprechung.

So sorgte ein Freispruch gegen den Betreiber einer Internetseite wegen mutmaßlicher Urheberrechtsverletzungen im Mai 2010 für große Aufmerksamkeit bei der Musikindustrie wie in der Internetszene.[6] Auf der Seite werden bis heute Filmtitel angegeben, man kann sie sich als „stream" live im Netz ansehen, oder herunterladen. Es gibt ein Ranking der am meisten gesehenen Titel. Zum Freispruch führte jedoch der Umstand, dass der Download nicht direkt von der betreffenden Seite geschah, sondern ein Klick auf den Filmtitel zu Links auf Servern wie „megaupload" führte, auf denen diese Filme heruntergeladen werden konnten.

Obwohl dem Betreiber der immer noch zugänglichen Seite das Gewinnstreben durch die massive Werbung darauf ohne Probleme nachgewiesen werden konnte, wurde er freigesprochen. Denn dem Strafrecht zufolge muss zudem das durch das Urheberrecht geschützte Werk auch durch den Beschuldigten angeboten werden. Eine reine „Verlinkung" reicht also nicht aus.

In Spanien wurde der Freispruch so interpretiert, als habe das Urheberrecht praktisch keine Gültigkeit im Internet. Auch mit solchen Fällen beschäftigte Rechtsanwälte erwecken bei ihren zahlreichen Konferenzen diesen Anschein. Allerdings hatte die Musikindustrie, die hier die Klage führte, einen entscheidenden Fehler gemacht, sagt Paloma Llaneza González, eine der bekanntesten Expertinnen zum Internet-Recht in Spanien. Die Musikindustrie habe unbedingt einen aufsehenerregenden Strafrechtsprozess gewinnen wollen, mit einer Gefängnisstrafe für den Betreiber der Seite. Hätte sie auf eine Entschädigung geklagt, wären die Erfolgsaussichten weitaus besser gewesen, und die Seite vermutlich eingestellt worden, meint die Rechtsanwältin. Doch so finden sich auf der Seite des geschäftstüchtigen Angeklagten bis heute die Downloadlinks für die gesamte internationale Filmproduktion – und in Spanien

verbreitet sich der falsche Gedanke, Urheberrechtsverletzungen seien völlig legal.

DAS „GESETZ SINDE"

Das spanische Kulturministerium versucht derzeit, mit einer Gesetzesnovelle die Urheberrechtsverletzungen im Internet einzuschränken. Auch die soeben beschriebenen Linksammlungen sollen bestraft werden können. Allerdings ist hier nicht das Strafrecht der Ansatz: Eine zu diesem Zweck zu bildende und dem Kulturministerium unterstehende Kommission zum Urheberrechtsschutz sollen auf Antrag von Rechteinhabern (Autoren, Verlage, Musikindustrie etc.) die Löschung von Internetauftritten anordnen dürfen, wenn sie dort eine Verletzung dieser Rechte erkennen. Zuvor sollen die Betreiber der Seiten angehört werden. Sie können gegen die Entscheidung zur Löschung auch Beschwerde vor dem Nationalen Gerichtshof einlegen dürfen. Der Gerichtshof muss innerhalb von vier Tagen darüber entscheiden.

Der Nationale Gerichtshof soll jedoch gar nicht darüber verhandeln, ob tatsächlich eine Urheberrechtsverletzung vorliegt, sondern nur, ob die Schließung der Seite ein Grundrecht wie das Recht auf freie Meinungsäußerung einschränkt. Gegen die eigentliche Schließung der Seite kann der Betreiber der schließlich vor den örtlichen Gerichten klagen.

Zufrieden ist mit dieser noch im Parlament zu verhandelnden Regelung nur die Kulturministerin González-Sinde, nach der die Presse das Gesetz benennt. Damit würde verfolgt, wer „sich auf illegale Weise an der Arbeit anderer bereichert", also wer das Urheberrecht verletzt, aber nicht die im Grunde unzulässigen Downloads, wie etwa in Frankreich, betont die Ministerin, nach der die Presse das Reformvorhaben benannt hat.

Die Verbände von Internetnutzern meinen hingegen, mit dem Gesetz müsse die Regierung sogar die Seiten von Suchdiensten wie Google schließen, schließlich fänden sich dort zahlreiche Links zu Seiten, auf denen Urheberrechtsverletzungen begangen würden.[7] [8] Verfassungsrechtler halten ein wichtiges Prinzip für gebrochen. Ein Streit um eine Urheberrechtverletzung führten stets zwei Parteien, ein Rechtinhaber, der einen Zweiten beschuldigt, diese Rechte zu verletzen. Mit dem Gesetzesentwurf würde eine Regierungsbehörde dabei selbst zur Partei, meint Paloma Llaneza.

Warum die Regierung nicht einfach einen Entwurf für eine Strafrechtsreform vorlegt, mit der auch die Verlinkung von Seiten, auf denen urheberrechtlich geschützte Werke zum Download angeboten werden, zur Straftat würden, versteht in Spanien kaum jemand. Vermutlich befürchte die Regierung Zapatero, die vielen Prozesse wegen mutmaßlicher illegaler Urheberrechtsverletzungen würden in der völlig überlasteten spanischen Justiz schlicht viel zu lange dauern und somit kaum abschreckend wirken.

Verfassungsrechtler Lucrecio Rebollo von der UNED-Universität beklagt sich, es entstehe der Eindruck, Themen wie das Urheberrecht seien der Regierung einfach unangenehm und sollten schlicht vom Tisch. Das Urheberrecht, Verbände von Rechteinhabern und Maßnahmen zur Sicherung ihrer Interessen wie eine Abgabe auf Datenträger oder Gebühren für die Reproduktion im öffentlichen Raum sind in Spanien extrem unpopulär, die Verbände von Internetnutzern schalten sich immer wieder in die Debatte zum Urheberrecht im Netz ein.

Der Gesetzesentwurf soll noch in diesem Jahr vom spanischen Parlament verhandelt werden. Aufgrund der unklaren Mehrheitsverhältnisse in beiden Kammern ist jedoch nicht absehbar, welche Gestalt das Gesetz schließlich haben wird. Die konservative Volkspartei will es zur völligen Neubearbeitung an die Regierung zurückschicken.

1| http://www.informeeespana.es/docs/eE2010.pdf
2| Weiterführende Literatur zur Internetgesetzgebung in Spanien: „Aplicación Práctica de La LSSI-CE", Paloma Llaneza González, Barcelona 2003
3| http://www.elpais.com/articulo/opinion/Descargas/ilegales/gratuitas/elpepuopi/20100804elpepiopi_9/Tes
4| http://www.elpais.com/articulo/cultura/EE/UU/abronca/Espana/pirata/elpepicul/20090506elpepicul_1/Tes
5| http://www.elpais.com/articulo/tecnologia/Estados/Unidos/coloca/Espana/paises/pirateria/elpeputec/20100520elpeputec_1/Tes
6| http://www.filmica.com/david_bravo/
7| http://www.noalcierredewebs.com/
8| http://www.internautas.org/html/3588.html

<< zurück zum Inhaltsverzeichnis

POLEN

DER EINFLUSS DER DISKUSSIONEN UM DIE NETZPOLITISCHEN FRAGEN AUF DIE POLITISCHE DEBATTE

Aneta Zwolińska | Bohdan Wyżnikiewicz

Das Internet ist in Polen ein Medium, welches von Anfang an eine starke und seitdem stetig zunehmende Rolle im öffentlichen Leben spielte.

Die Umfragen des Hauptstatistikamtes (GUS) zeigten, dass 95 Prozent der Unternehmen im Jahre 2008 Computer nutzten und beinahe 59 Prozent der Haushalte über mindestens einen Computer verfügten, verglichen mit dem Durchschnitt von 68 Prozent in der Europäischen Union. Laut Eurostat hatten 51 Prozent der Haushalte in Polen im Jahre 2009 eine Breitbandverbindung (2008 waren es 38 Prozent). Der EU-Durchschnitt betrug 56 Prozent im Jahr 2009 und 49 Prozent 2008. Diese Zahlen weisen auf einen starken Nachholbedarf in der Internetentwicklung Polens im Vergleich mit anderen EU-Mitgliedsstaaten hin.

Die Entwicklung des Internets und seine steigende Bedeutung erfolgt, wie in anderen demokratischen Gesellschaften, auf spontane Art. Staatliche Maßnahmen werden am häufigsten als Reaktion auf vollendete Tatsachen durchgeführt, und wenn rechtliche Regelungen überhaupt eingeführt werden, dann geschieht das gewöhnlich erst in Nachhinein. Als Beispiel kann hier die Besteuerung der durch das Internet erfolgenden Finanztransaktionen (Transfer) genannt werden, oder aber das Interesse der Steuerbehörden an den Umsätzen der online getätigten Transaktionen, wie z.B. Onlineshopping. Ein anderes Beispiel wäre die Einführung von Vorschriften, welche die Verführung von Minderjährigen im Internet als kriminell einstufen.

Mit der Entwicklung des Internets entstehen Debatten, die sich aus den neuen Phänomenen im Netz ergeben. Die rechtlichen Regulierungen, die sich auf das Internet und seinen Einfluss auf das Recht beziehen, werden von den schnellen Veränderungen im Netz überholt. Der Staat nimmt langsam die Tatsache zur Kenntnis, dass sich manche netzrelevanten Fragen rechtlich nicht regulieren lassen und dass man sich damit abfinden muss.

Die Politiker bewahren ebenfalls eine gewisse Distanz in Bezug auf das Internet, obwohl zwei grundsätzliche Arten sichtbar werden, wie Politiker mit der Gesellschaft mittels dieses Mediums kommunizieren. Die erste bezieht sich auf die Debatten der führenden Politiker in Internetchats, was insbesondere während der Wahlkampagnen verbreitet ist. Als zweites sind die Blogs der Politiker zu nennen, welche normalerweise Einträge mit kontroversen Thesen und Kommentaren beinhalten, die wiederum sofort von anderen Medien aufgegriffen und veröffentlicht werden.

An die breite Öffentlichkeit gelangen aber häufiger die Botschaften der Oppositionspolitiker als von der regierenden Partei. Die regelmäßige Teilnahme an den von Sejm-Abgeordneten geführten Blogs ist durchaus populär geworden. Außerdem dient es in den Augen von vielen Beobachtern zur Gewinnung politischer Anhänger. Der mit Abstand größten Beliebtheit erfreut sich der Blog von einem extrem radikalen (ultraliberalen) Politiker, der seit langer Zeit außerhalb des Parlaments fungiert.

Die Fragen um das Internet selbst stoßen immer dann Diskussionen an, wenn die vorgeschlagenen Veränderungen oder rechtliche Lösungen auf irgendeine Art die breit verstandenen Interessen der Internetnutzer gefährden könnten.

Im Dezember 2008 erklärte die Regierung die „Strategie der Entwicklung zur Informationsgesellschaft in Polen bis 2013", die unter dem Begriff „Informatisierungsstrategie" des Landes bekannt ist. Die Strategie soll dazu dienen, „der Gesellschaft eine allgemeine und effektive Nutzung

des Wissens und der Informationen für eine harmonische Entwicklung in gesellschaftlicher, wirtschaftlicher und persönlicher Dimension zu ermöglichen." Laut dieser Strategie sind Maßnahmen geplant, welche auf die Menschen (Entwicklung des intellektuellen und gesellschaftlichen Kapitals), auf Unternehmen (Steigerung der Effektivität, Innovation und Wettbewerbsfähigkeit) und auf die öffentliche Verwaltung (Steigerung der Effektivität und des Zugangs zu Dienstleistungen der öffentlichen Verwaltung) gerichtet sind.

Der Formulierung dieser Strategie gingen breite Konsultationen in gesellschaftlichen Kreisen, in öffentlichen und privaten Institutionen, in akademischen und wissenschaftlichen Forschungseinrichtungen sowie in Nichtregierungsorganisationen voraus. Ebenso soll sie die Prioritäten der europäischen Politik erfüllen, welche in der Kommuniqué der Europäischen Kommission „i2010: Eine europäische Informationsgesellschaft für Wachstum und Beschäftigung" genannt werden.

DATENSPEICHERUNG (DATA STORAGE)

Die Datenspeicherung (*data storage*) stellte bislang keinen Gegenstand der öffentlichen Debatten in Polen dar. Die Fragen, die mit der Datenspeicherung zusammenhängen, gehören zum Rechtsgebiet Schutz der personenbezogenen Daten. Die Öffentlichkeit zeigt kein breites Interesse an dieser Frage. Nur ab und zu wird im Parlament diskutiert, wie lange die Justiz und die Geheimdienste sensible personenbezogene Daten aufbewahren und wie umfangreich diese Informationen sein dürfen. Die häufigste Lösung ist eine fünfjährige Frist zur Datenspeicherung.

DATENSCHUTZ, DATENSICHERHEIT UND DIE DAFÜR ZUSTÄNDIGEN INSTITUTIONEN

Die Fortschritte in der Wirtschaft sowie die Entwicklung von neuen Technologien – insbesondere im IT-Bereich – stellen eine zunehmende Gefährdung für die menschliche Privatsphäre, im Sinne von personenbezogenen Daten, dar. Die Erweiterung des Umfangs der von verschiedenen öffentlichen und privaten Institutionen gesammelten Daten führte dazu, dass eine Kontrollausübung durch eine Person über den Umlauf und Inhalt der Informationen, die den Einzelnen betreffen, praktisch unmöglich wurde. Man sah die Notwendigkeit, diesen Teil der Privatsphäre staatlich zu schützen.

Mit der Verfassung der Republik Polen aus dem Jahr 1997 wurde in das polnische Recht das Prinzip des Schutzes von personenbezogenen Daten eingeführt. Im Art. 51 der Verfassung heißt es: „Eine Verpflichtung, Informationen über die eigene Person zu offenbaren, besteht nur auf Grundlage eines Gesetzes. Jedermann hat das Recht auf Zugang zu den ihn betreffenden amtlichen Dokumenten und Datensammlungen. Eine Einschränkung dieses Rechtes darf nur vom Gesetz bestimmt werden". Darüber hinaus: „Jedermann hat einen Anspruch auf Berichtigung oder Löschung falscher, unvollständiger oder in widerrechtlicher Weise beschaffter Informationen."

Ebenfalls im Jahr 1997 wurde das Gesetz zum Schutz personenbezogener Daten verabschiedet. Das Gesetz präzisierte das in der Verfassung jedem Bürger garantierte Recht, zu entscheiden, wem, in welchem Umfang und zu welchem Zweck seine personenbezogenen Daten weitergegeben werden. Außerdem regelt das Gesetz die Datenverarbeitung sowie Rechte, die sich ausschließlich auf natürliche Personen beziehen. Die Vorschriften des Gesetzes werden aber nicht bei der Verarbeitung von Informationen durch andere Träger angewandt, wie etwa juristische Personen, Organisationen ohne juristischen Charakter und natürliche Personen, die ein wirtschaftliches Gewerbe auf der Basis von Vorschriften des Gesetzes von 2004 über die Freiheit der wirtschaftlichen Tätigkeit führen.

Kraft des Datenschutzgesetzes wurde der Generalinspekteur zum Schutz der personenbezogenen Daten (*polnische Abkürzung*: GIODO) einberufen. Dieser hat darüber Aufsicht, dass das Recht der Bürger auf den Schutz ihrer personenbezogenen Daten eingehalten wird. Der Generalinspekteur führt ein landesweites, offenes Register der Sammlungen von personenbezogenen Daten. Die personenbezogenen Daten können in unterschiedlicher Form aufbewahrt werden, entweder als sogenannte Datensammlungen oder in Form von Einzeldaten, wenn sie in IT-Systemen gespeichert werden (z.B. ein Computernetz im Büro). Die Sammlung der personenbezogenen Daten meint jede strukturierte Zusammenstellung von Daten mit persönlichem Charakter, die nach bestimmten Kriterien zugänglich ist. Ein Beispiel einer solchen Datensammlung ist die Zusammenstellung von Personaldaten der Arbeitnehmer, das Register der Patienten einer Arztpraxis oder das Register der Steuerzahler.

Die Datensammlung sollte vom Datenverwalter vor Beginn ihrer Verarbeitung beim Datensammlungsregister angemeldet werden, ein Register das vom Generalinspekteur zum Schutz der personenbezogenen Daten geführt wird.

Die Pflicht zum Eintrag in die Sammlung der personenbezogenen Daten gilt nicht in den folgenden Fällen:

- bei Datenverwaltern, die aufgrund verschiedener Vorschriften vom Staatsgeheimnis abgedeckt sind,
- im Fall von Daten, die infolge von operativen Ermittlungstätigkeiten von Vertretern der dazu berechtigen Organe gesammelt wurden,
- Daten, die für Gerichtsverfahren verarbeitet werden,
- Daten von Menschen, die medizinische Dienstleistungen und Dienstleistungen von Notaren und Rechtsanwälten nutzen,
- Daten, die zur Durchführung von Wahlen sowie lokalen und allgemeinen Volksabstimmungen erstellt werden.

Die Einsicht in das Verzeichnis der Informationskategorien, welche im Register aufgeführt sind, wird durch das System e-giodo im Internet ermöglicht. Dieses System gestattet die Suche von Datensammlungen anhand zahlreicher Kriterien wie z.B. des Namens der Datensammlung, des Namens des Datenverwalters oder aber seines Sitzes. Das Register beinhaltet Informationen, die von Datenverwaltern während der Dateneintragung angemeldet werden. Informationen über konkrete Personen sind nicht zu finden.

Aus dem GIODO-Bericht von 2009 geht hervor, dass noch mehr Menschen die ICT-Systeme in Anspruch nehmen würden, wenn sie keine Angst vor Cyberkriminalität hätten. Diese Befürchtungen sind auch vollkommen berechtigt. Der Fall von 2004, als ein 23-jähriger Informatiker die personenbezogenen Daten von einer Million Polen aus der Firma seines Arbeitgebers stahl und versuchte, diese für eine halbe Million Euro an Werbeagenturen zu verkaufen, ist nur eins von vielen Beispiele.

Aus Daten der Firma Symantec über Straftaten wie etwa das *phishing* oder *pharming* geht hervor, dass der Online-Zugriff auf Bankkonten oder Internetdienstleistungen in der letzten Zeit in Polen zugenommen hat. Die schlimmste dieser Bedrohungen sind Hackerangriffe.

In Polen gibt es kommerzielle Organisationen, die sich mit den Verstößen gegen die Netzsicherheit beschäftigen. Die wichtigste von ihnen ist CERT Polska (*Computer Emergency Response Team*). Sie ist in den Strukturen des führenden polnischen Netzbetreibers tätig und wird von ihm finanziert. CERT Polska ist seit 1996 aktiv und seit 1997 ist sie Mitglied des FIRST (*Forum of Incidents Response and Security Teams*). Im Rahmen dieser Organisation arbeitet sie mit ähnlichen Teams weltweit. Zu den Aufgaben von CERT gehört unter anderem:

- die Registrierung und Bearbeitung von Fällen, welche die Netzsicherheit beeinträchtigen,
- Internetnutzer über das Auftreten von unmittelbaren Bedrohungen zu alarmieren,
- Durchführung von Maßnahmen, die zur Steigerung des öffentlichen Bewusstseins über die ICT-Sicherheit führen,
- Durchführung von Untersuchungen und Vorbereitung von Berichten über die Sicherheit der polnischen Internetressourcen,
- Unabhängiges Testen von Produkten und Lösungen aus dem Bereich der ICT-Sicherheit.

Die Tätigkeit von CERT Polska ist ein Beispiel davon, wie sich ein auf dem Internetmarkt präsenter kommerzieller Träger für Maßnahmen einsetzt, die sowohl für ihn als auch für die Gesellschaft nützlich sind.

ZUGANG ZU ÖFFENTLICHEN INFORMATIONEN

Als öffentliche Informationen gelten jene, die von einer öffentlichen Verwaltung erstellt bzw. die auf sie oder andere öffentliche Träger bezogen wird, sofern diese öffentliche Funktionen erfüllen und das kommunale bzw. staatliche Eigentum bedienen.

Das Recht auf Informationen über die Maßnahmen der öffentlichen Organe wird durch Art. 61 der polnischen Verfassung gewährleistet. Der Zugang zu diesen Informationen wurde wiederum hauptsächlich im Gesetz über den Zugang zu öffentlichen Informationen aus dem Jahr 2001 bestimmt.

Laut diesem Gesetz umfasst das Recht auf öffentliche Information:

- das Erlangen einer öffentlichen Information, darunter einer Information, welche in einem Umfang verarbeitet wurde, welcher für das öffentliche Interesse besonders wichtig ist,
- die Einsicht in amtliche Dokumente,
- den Zugang zu Sitzungen der kollegialen Organe der öffentlichen, in allgemeinen Wahlen gewählten Verwaltung.

Die obige Vorschrift beschränkt die Art der Umsetzung des Rechts auf Information wesentlich, denn in Artikel 61 der polnischen Versfassung ist vom Zugang zu Dokumenten die Rede. Das Recht auf Zugang zu einem Dokument berechtigt zum Erhalten einer Kopie dieses Dokuments. Eine Kopie zu besitzen bedeutet ständigen Zugang zum Dokument zu haben, sowie die Möglichkeit, die dort enthaltenen Informationen zu verarbeiten und zu veröffentlichen (Art. 54 der Verfassung). Dagegen haben die Bürger laut Gesetz über den Zugang zur öffentlichen Information keinen Zugang zu den Informationsquellen.

Jeder polnische Bürger hat das Recht auf einen Zugang zu öffentlichen Information, ein durch die Verfassung gewährleistetes Recht. Auch Ausländer haben dieses Privileg, garantiert durch das Gesetz über den Zugang zur öffentlichen Information. Die Schaffung des Zugangs zu öffentlichen Informationen erfolgt durch die Bekanntmachung dieser Informationen, z.B. in amtlichen Dokumenten, in der Bulletin der Öffentlichen Information (*polnische Abkürzung*: BIP). BIP ist ein einheitliches System von Internetseiten, welches geschaffen wurde, um öffentliche Informationen allgemein und kostenlos zur Verfügung zu stellen. Für die BIP-Seiten wurden die Organe der öffentlichen Verwaltung, territorialen Selbstverwaltung und wirtschaftlichen Selbstverwaltung, sowie Gewerkschaften, politische Parteien und andere staatliche Institutionen und Träger, welche öffentliche Aufgaben erfüllen, verpflichtet.

Zugang zu öffentlichen Informationen beinhaltet auch das Recht auf Zutritt zu Sitzungen der öffentlichen Verwaltung und den Zugang zu Materialien (darunter auch audiovisuelle und ICT-Materialien), welche diese Sitzungen dokumentieren. Allerdings bedeutet ein Zutritt zu Sitzungen der öffentlichen Organe kein Recht auf die Beteiligung an diesen. Zwar dürfen die Bürger den Ablauf der Sitzungen und ihre Teilnehmer beobachten, sie haben aber kein Mitspracherecht, usw.

Im Allgemeinen ist der Zugang zu öffentlichen Informationen kostenlos und ein an den Informationen interessierter Bürger muss kein rechtliches Interesse nachweisen können.

Eine öffentliche Information, die im Bulletin der Öffentlichen Information nicht veröffentlicht wurde, kann auf Antrag eines Interessenten zur Verfügung gestellt werden. Die Mitarbeiter der Behörden, die öffentliche Informationen verpflichtend zur Verfügung stellen, können bei Verweigerung dieser Tätigkeit mit einer finanziellen Strafe, Freiheitsbeschränkung oder Freiheitsentzug bis zu einem Jahr bestraft werden.

NETZZUGANGSSPERREN

In der aktuellen Rechtsprechung gibt es keine Vorschriften, welche die Sperrung von ausgewählten Internetseiten zulassen. Im November 2009 verkündete das Finanzministerium den Vorschlag, ein „Register von unzulässigen Webseiten und Dienstleistungen" zu erstellen. Die Grundlage dafür hätte ein zum Gesetz über das Telekom-Recht hinzugefügter Artikel sein sollen, dessen Ziel die Zugangserschwerung mittels des Internets zu folgenden Webseiten gewesen wäre:

- Webseiten mit Inhalten, welche die faschistische oder eine andere totalitäre Ideologie bzw. das faschistische oder ein anderes totalitäres Staatssystem verbreiten,
- Webseiten mit pornografischen Darstellungen von Minderjährigen unter dem 15. Lebensjahr, Pornografie mit Gewaltakten oder Präsenz von Tieren, Pornografie mit erstellten bzw. verarbeiteten Bildern von Minderjährigen,
- Inhalte, deren Darstellung heimtückische Irreführung und letztlich Vermögensvorteile ermöglichen, wie z.B. durch erzwungene Informationen, die zur Durchführung von finanziellen Operationen ohne Zustimmung der Finanzmittelinhaber dienen können,
- Inhalte, die verbotene Werbung darstellen sowie Werbung bzw. unberechtigtes Informieren über das Sponsoring, im Sinne des Gesetzes, von Glücksspielen oder Dienstleistungen zur Durchführung verbotener Glücksspiele.

Laut Projektinhalt sollte das Register der unzulässigen Webseiten und Dienstleistungen im IT-System offen sein und vom Vorsitzenden des Amtes für Elektronische Kommunikation geführt werden, einem regulie-

renden Organ im Bereich der Post-, Telekom- und Frequenzwirtschaft. Im Januar 2010 ist eine weitere Fassung des Projekts entstanden, die auf der Homepage des Finanzministers veröffentlicht wurde. Laut der neuen Version wird das Bezirksgericht in Warschau in Form eines Beschlusses, der auf Antrag der Polizei, der Agentur für Innere Sicherheit, der Steuerkontrollbehörde bzw. der Zollbehörden gefasst wurde, über die Eintragung in das Register entscheiden. Den Antrag kann man dann stellen, wenn sich andere Mittel als unzureichend erwiesen haben oder wenn es „hochwahrscheinlich ist, dass sie ineffizient bzw. unnützlich sein werden." Von einer Sperre von Internetseiten, welche faschistische oder totalitäre Staatssysteme gut heißen, ist im Projekt nicht mehr die Rede. Des Weiteren wurden auch Vorschriften ausgeschlossen, die sich auf die Sperre von Inhalten beziehen, „dessen Präsentation eine heimtückische Irreführung zwecks Erlangung materieller Gewinne zulässt". Die Sperrung unerlaubter Webseiten aufgrund einer Gerichtsentscheidung ist zweifellos weniger kontrovers als ohne gerichtliche Entscheidung.

Darüber hinaus sieht das Projekt vor, dass die Betreiber eine Nachricht über die Internetsperre an die Internetnutzer senden. Darin werden die Rechtsgrundlage und das entsprechende Organ, welches das Register der unzulässigen Webseiten und Dienstleistungen führt, genannt. Das ändert jedoch nichts an der Tatsache, dass die Einrichtung vieler Internetsperren auf der Ebene der Telekom-Betreiber kontrovers gesehen wird, da es auch mit hohen Kosten verbunden ist.

Das oben genannte Projekt führte zu einer Kontroversen und heftigen Debatten. Vertreter verschiedener Kreise, u.a. der Internetportale, Politiker, Journalisten, Unternehmer und Dozenten brachten ernsthafte Vorbehalte zu dem hier dargestellten Projekt vor. Insbesondere wurde das Argument der Verfassungswidrigkeit erhoben, denn die Verfassung garantiert die Meinungsfreiheit und die Freiheit zum Erhalt und zur Verbreitung von Informationen. Außerdem hält Artikel 54 der Verfassung deutlich fest, dass die Präventivzensur von Massenmedien und das Konzessionieren der Presse verboten sind. Die Autoren betonten, dass das jetzige Rechtssystem die Möglichkeit vorsieht, nach Autoren von Webseiten mit Kinderpornographie, Nazi-Propaganda oder auch Rassen- bzw. Religionshass usw. zu fahnden. Die Erstellung eines neuen Registers sei daher nicht nötig.

Die Schaffung des Registers soll über eine Million Euro kosten. Seine Effizienz wird jedoch bezweifelt. Das Protestschreiben gegen das Register haben über 80.000 Menschen unterschrieben – sie sind der Meinung, dass solche Vorschriften die Meinungsfreiheit im Netz einschränken könnten. Der Druck der Internetnutzer führte bisher zu einem Treffen mit Premierminister Donald Tusk. Die Debatte fand gleichzeitig unter Teilnahme von Internetnutzern und Vertretern von Nichtregierungsorganisationen in der Kanzlei des Premierministers sowie in einigen allgemein zugänglichen Online-Netzwerken statt. Nach einem über dreistündigen Treffen zog die Regierung die Vorschriften über die Internetzensur aus dem Gesetzentwurf zurück. Allerdings ist diese Idee nicht verschwunden und könnte in der kommenden Zeit auch wieder aufgegriffen werden.

Auch die kommerziellen Provider sperren manchmal die Seiten ihrer Kunden, wenn Seiten mit schädlichen Inhalten festgestellt werden oder aber eine wesentliche Bedrohung besteht. Solche Maßnahmen haben aus Sicht der Provider präventiven Charakter, um ihren guten Ruf zu sichern. Es ist allerdings vorgekommen, dass die von polnischen Providern gesperrten Seiten auf Server ausländischer Betreiber verlegt wurden. Das führte sowohl zur Zusammenarbeit der polnischen Polizei mit der Polizei des jeweiligen Staates als auch zur Fahndung auf dem Gebiet Polens nach Personen, die rechtswidrig gehandelt haben.

SCHUTZ DES RECHTES DES GEISTIGEN EIGENTUMS

Das in Polen geltende Recht garantiert den Schutz des geistigen Eigentums auf zwei wesentlichen Gebieten. Zum einen ist es das Urheberrecht, das vom Urheberrechtgesetz und anderen relevanten Rechten aus dem Jahr 1994 geregelt wird. Zum anderen sind Patentrechte und die damit zusammenhängenden Rechte, wie etwa Warenzeichen, geographische Bezeichnungen und Industriemuster geschützt.

Um den Rechtsschutz für Produkte aus dem Bereich des Industrieeigentums zu gewährleisten, wurde bereits 1918 das Patentamt der Republik Polen mit Sitz in Warschau geschaffen. Das dort eingetragene Patent wird zwanzig Jahre, vom Jahr der Erfindungsanmeldung an gezählt, geschützt. Das Schutzrecht für Gebrauchsmuster gilt zehn Jahre und für Industriemuster haben wir es mit einer Laufzeit von 25 Jahren zu tun. Die perio-

dischen Gebühren für den Schutz von Erfindungen und Gebrauchsmuster sind obligatorisch. Eine Grundgebühr für die Anmeldung einer Erfindung oder eines Gebrauchsmusters beträgt derzeit ca. 120 Euro.
Der Schutz von Urheberrechten entsteht automatisch bei der Erstellung des Werks und es bedarf keiner Eintragung bzw. Zertifizierung. Dies bezieht sich sowohl auf die materiellen als auch die immateriellen Urheberrechte. Die materiellen Urheberrechte können durch Vererbung oder durch den Abschluss eines entsprechenden Vertrages (z.B. über die Übertragung der materiellen Urheberrechte) an andere Personen übertragen werden.

Am häufigsten werden die Urheberrechte durch folgende Fälle verletzt:

a) die Eintragung (auf der eigenen Website) eines fremden Textes, der mit dem eigenen Namen und Nachnamen unterzeichnet wird,
b) Kopieren und Nutzung von Werken in wirtschaftlichem Gewerbe,
c) Anschaffung von Urheberrechten oder einer Lizenz von jemandem, der kein Recht auf den Verkauf oder auf die Erteilung der Lizenz hatte,
d) Aneignung von fremden Skripten oder Applets.

Die rechtliche Konsequenz von Verstößen gegen die Urheberrechte und deren Nutzung ohne die Zustimmung des Autoren ist eine Haftstrafe und die strafrechtliche Haftung desjenigen, der gegen das Urheberrecht verstoßen hat.

Der Autor, dessen Rechte beeinträchtigt wurden, darf vor dem Zivilgericht unter anderem folgendes fordern: Schadenersatz, Unterlassung der Aktivitäten, die sich gegen seine Interessen richten und die Veröffentlichung einer entsprechenden Pressemeldung bzw. öffentliche Bekanntmachung der Gerichtsentscheidung in Teilen oder in voller Länge.

Zum anderen handelt es sich um die strafrechtliche Haftung; hier wird von einer kriminellen Straftat ausgegangen. Diese Art der Haftung ist bei widerrechtlicher Nutzung fremder Materialien vorgesehen. Jemand, der die Urheberrechte beeinträchtigt hat, kann mit einer finanziellen Strafe bzw. mit Freiheitsentzug bis zu fünf Jahren bestraft werden.

Allmählich werden in Polen die Rechte zum Schutz des geistigen Eigentums auch praktisch durchgesetzt. Einige Strafprozesse gegen Personen oder Institutionen, die gegen dieses Recht verstoßen haben, hatten auch einen durchaus starken Bildungseffekt.

Darüber hinaus kann man bei Warenzeichen den Schutz in Form von gemeinschaftlichen Warenzeichen in Anspruch nehmen (die Eintragung erfolgt im Harmonisierungsamt für den Binnenmarkt in Alicante, Spanien) oder das Warenzeichen international schützen lassen (die Eintragung erfolgt im Büro der Weltorganisation für geistiges Eigentum WIPO in Genf).

PROGRAMME ZUR SICHERSTELLUNG EINER FLÄCHENDECKENDEN BREITBANDVERSORGUNG

Die polnische Regierung plant die Sicherstellung einer flächendeckenden Breitbandversorgung in Polen bereits für 2015. In Anbetracht der Fortschritte in den letzten zwei bis drei Jahren ist dieses Vorhaben realistisch. Allerdings muss man mit der Tatsache rechnen, dass der Erfolgsindex ein wenig unter 100 Prozent liegen könnte.

Bis 2012 soll das Regierungsprogramm „Digital-Polen" die Verbreitung des Breitbandinternetzugangs hauptsächlich in drei Richtungen fördern: Zum einen geht es um die Ausarbeitung von Mechanismen zur Investitionsanregung in der Telekom-Infrastruktur. Als zweites ist die Abschaffung von rechtlichen, administrativen und technischen Hürden geplant. Die dritte Maßnahme wäre die Schaffung von möglichst günstigen Bedingungen zur Nutzung von zu diesem Zweck bestimmten EU-Mitteln.

Als Folge der seit einigen Jahren laufenden Aktivitäten des Amtes für Elektronische Kommunikation verringerten sich die Preise für Internet- und Telekom-Dienstleistungen. Außerdem entwickelten sich gesunde Wettbewerbsmechanismen. Beides beseitigte in den letzten Jahren spürbar die finanziellen Barrieren, die auch die Entwicklung des Internets in Polen erschwerten.

Ein wesentlicher Schritt zur Umsetzung des Regierungsprogramms war der Beschluss des sogenannten Megagesetzes zur Förderung der Entwicklung von Telekom-Dienstleistungen im Mai 2010. Dieses Gesetz stieß auf positive Resonanz bei Experten und Netzbetreibern. Einer der wesentlichen Vorteile dieses Gesetzes ist die Schaffung institutioneller und rechtlicher Bedingungen für Investitionen in Internetverbindungen für die kommunale Selbstverwaltung und öffentliche Daseinsvorsorge. Weitere wesentliche Regelungen beziehen sich auf den Zugang zur Telekom-Infrastruktur, die aus öffentlicher Hand finanziert wird. Der

geschaffene Rechtszustand ermöglicht den Ausbau einer Breitbandverbindung im Wesentlichen durch EU-Finanzmittel.

Die Umsetzung des Regierungsprogramms wird im Rahmen einer informellen Gruppe – dem sogenannten Landesbreitbandforum – koordiniert. Es ist eine Plattform der Zusammenarbeit aller, die sich für den Aufbau der Breitbandinfrastruktur der Telekom in Polen einsetzen. Darin beteiligt sind die Regierung, die Organe der kommunalen Selbstverwaltung, Telekom-Betreiber, Finanzinstitutionen, Nichtregierungsorganisationen und die Marktregulationsbehörden. Das Forum wird durch ein Internetportal unterstützt, welches der Kommunikation, Wissenssammlung und zum Erfahrungsaustausch unter den Teilnehmern dieser Initiative dient.

Das Regierungsprogramm berücksichtigt aber auch den globalen technologischen Wettlauf, der zu einer Anhebung der technischen Parameter für das Breitband führt und ständige Investitionen in die Telekom-Infrastruktur zur Folge hat.

BETEILIGUNG AN DER DEBATTE VON INTERESSENVERBÄNDEN AUS DER ZIVILGESELLSCHAFT

Die Effizienz der administrativen Maßnahmen zum Aufbau der Informationsgesellschaft wird nicht als hoch bewertet und stößt häufig auf Kritik in den Medien und der Öffentlichkeit. Die Gemeinschaft der Internetnutzer ist dabei sehr aktiv, weist einen hohen Grad an Selbstorganisation auf und nutzt effizient populäre Online-Netzwerke. Es gibt zahlreiche Organisationen wie etwa *Internet Society Poland* oder *Fundacja Rozwoju Społeczeństwa Informacyjnego* (Stiftung für die Entwicklung der Informationsgesellschaft). Das Ziel dieser Organisationen ist die Förderung der Internetentwicklung und die Vorbereitung der Menschen auf das Leben in einer globalen Informationsgesellschaft. Derartige Organisationen arbeiten auf breiter Ebene mit ihren internationalen Pendants zusammen.

Erwähnenswert sind hier einige solcher von Internetnutzern durchgeführten Aktionen, welche die Präsenz des Internets im gesellschaftlichen und wirtschaftlichen Leben erhöhen sollten. Diese Aktionen betrafen folgende Aktivitäten:

- Die Möglichkeit zur Einreichung der Steuererklärung online – mit Erfolg,
- Anerkennung durch Steuerbehörden der Rechnungen, die mittels Internet und nicht nur per Post geschickt werden – mit Erfolg,
- Durchführung von allgemeinen Wahlen online – ohne Erfolg.

Die Erweiterung der Internetnutzung im gesellschaftlichen und wirtschaftlichen Leben erfolgt mehr durch den Druck der Internetnutzer als durch Maßnahmen der öffentlichen Behörden. Besonders wichtig ist dabei die Effizienz von Aktivitäten zivilgesellschaftlicher Akteure bei der Mobilisierung der Verwaltung zur Durchsetzung gesellschaftlich nützlicher Maßnahmen.

Während einer Konferenz „Städte im Internet" im Juni 2010, die ein Bündnis aus der Organisation der territorialen Selbstverwaltung gemeinsam mit zwölf Nichtregierungsorganisationen im Bereich Internet veranstaltete, wurde eine „Erklärung über die notwendigen Änderungen im Entwicklungsmanagement von Informationsgesellschaft in Polen" verkündet. Darin wurde unter anderem das Problem der sogenannten „digitale Analphabeten" (ca. 13 Millionen erwachsene Polen) thematisiert. Die Autoren der Erklärung rufen die Behörden zu dynamischeren Maßnahmen auf, um den digitalen Analphabetismus einzuschränken. Eine weitere in diesem Text thematisierte Frage bezog sich auf die Kluft zwischen den digitalen Kompetenzen der meisten Grund- und Mittelschulschüler und dem traditionellen, in Schulen umgesetzten Bildungsprogramm. Diese Kluft müsste mehr beachtet werden.

Übersetzung ins Deutsche: Iwona Łatwińska

<< zurück zum Inhaltsverzeichnis

INDIEN

INTERNET IN INDIEN – EINE FALLSTUDIE

Rajat Kathuria | *Mahesh Uppal*

I. EINLEITUNG

Die Fähigkeit des Internets zum Erkenntnisgewinn, zur Integration verschiedener Märkte und zur Befähigung von Bürgern, sich in ihrer Gemeinschaft und der Gesellschaft stärker zu engagieren, findet breite Anerkennung. Es ist eine Tatsache, dass die Nutzung des Internets von dessen Verfügbarkeit abhängig ist. Ersteres wird ohne letzteres nicht möglich sein. Allerdings ist die Nutzung jeglicher Technologie abhängig vom gesamten Ökosystem, einschließlich des rechtlichen Rahmens, der sich im lokalen Kontext um eine Technologie herausbildet. Beispielsweise wurde die Nachfrage in der Republik Korea anfangs durch die Einführung von Breitband für den Online-Aktienhandel, Bildungsdienstleistungen und Spiele gefördert.

Später verlagerte sich der Schwerpunkt hin zu interaktiven Dienstleistungen, etwa Einkaufen, sowie E-Mail und Teilnahme an Cyber-Communities, und heute liegt der Fokus auf Spielen und dem Herunterladen von Musik. E-Government (E-Regierung), E-Commerce (Internethandel) und computergestütztes Lernen sind in Korea ebenfalls wichtige Faktoren bei der Einführung von Breitband in großem Maßstab. In den USA wird das Internet wie Wasser und Strom als ein Teil der grundlegenden öffentlichen Daseinsvorsorge betrachtet, der die Gesamtgesellschaft betrifft. Angesichts des Potenzials von Breitband, die Erholung des Vereinigten Königreichs von einem schweren ökonomischen Abschwung zu unterstützen, lancierte die dortige Regierung im Jahre 2009 das *Digital Britain*-Programm (Digitales Großbritannien). Während manche Forschungsarbeiten über das Internet und seine Potenziale für die Demokratisierung den homogenisierenden Einfluss betonen, haben andere gezeigt, dass es auch auf den lokalen Kontext ankommt.

Dieses Papier untersucht die Evolution des Internet-Ökosystems Indiens gerade im lokalen Kontext. Das Internet ist hier viel weniger erfolgreich als die mobile Sprachtelefonie, bei der schwindelerregende Nutzerzahlen ständig zur bereits hohen Zahl der Teilnehmer hinzukommen. Im Gegensatz dazu ist die Verbreitung des Internets weiterhin extrem niedrig, und Indien wird in länderübergreifenden Forschungsarbeiten über das Internet fast gar nicht erwähnt.[1] Von den 1,4 Milliarden Internetnutzern weltweit Ende 2008 lebte die größte Anzahl in China (298 Millionen), gefolgt von den USA (191 Millionen) und Japan (88 Millionen). Andererseits hat der Erfolg Indiens bei der mobilen Sprachtelefonie breite Beachtung erlangt.[2]

Allerdings deutet genug darauf hin, dass eine Veränderung möglicherweise bevorsteht. Die Internetnutzung ist in den letzten Jahren gestiegen, und die erfolgreiche Versteigerung von 3G und kabellosen Breitbanddiensten in Indien im April 2010 verheißen Gutes für Verfügbarkeit und Nutzung. Angesichts des geringen Ausbaus der Festnetzinfrastruktur wird der drahtlose Zugang zum Internet in absehbarer Zeit dominieren. Überdies hat sich die *Telecom Regulatory Authority of India* (TRAI, Telekommunikationsregulierungsbehörde Indiens) zur Aufgabe gestellt, die die Ausbreitung des Internets besonders durch Breitbandverbindungen in Indien zu beschleunigen.[3] Denn ein Breitbandinternetzugang bietet die Möglichkeit, Dinge anders zu tun, bessere Ergebnisse zu erzielen und soziale und ökonomische Entwicklung zu gewährleisten. Zusätzlich gibt es einige staatliche Initiativen, beispielsweise die geplante *Public Information Infrastructure* (PII, Öffentliche Informationsinfrastruktur) sowie mehrere Initiativen im Rahmen des *National E-Governance Plan* (NeGP, Nationaler E-Governance-Plan), Internetkioske auf lokaler oder Distriktebene einzurichten, sowie eine bessere und zukunftsweisende Gesetzgebung mit dem Ziel, die Internetlandschaft dauerhaft zu verändern.

Als das Internet Mitte der 1990er Jahre boomte, wurde häufig behauptet, dass es die Transparenz von Preisen verbessern, Mittelsmänner überflüssig und Märkte effizienter machen würde. Für diese These gibt es in Indien reichlich anekdotische und zunehmend auch wissenschaftliche Evidenz. Im Gegenzug gibt es wenig Forschungsarbeiten in den Bereichen Sicherheit, Privatsphäre und Schutz im Internet. Dieses Papier kann die Lücke nicht füllen, aber es versucht doch, ein erstes Verständnis des Internet-Ökosystems in Indien zu liefern. Dieses Papier ist wie folgt gegliedert. Der folgende Abschnitt fasst den institutionellen Rahmen für das Internet und das Wachstum von Internetdienstleistungen seit der Liberalisierung in den späten 1990er Jahren kurz zusammen. In Abschnitt III wird die Bedeutung internetbezogener Themen in der politischen Debatte bewertet, während in Abschnitt IV die Art und die Auswirkungen der Vorratsdatenspeicherung in Indien untersucht werden, einschließlich der vorgesehenen *Unique Identity* (UID, eindeutige Identifikationsnummer) für alle Bürger. In Abschnitt V werden Fragen des Datenschutzes und der Datensicherheit diskutiert, inklusive dem öffentlichen Zugang zu bestimmten Arten von Daten. Die Sperrung gewisser Internetseiten wird auch thematisiert. In Abschnitt VI wird das gegenwärtige System der geistigen Eigentumsrechte untersucht, und in Abschnitt VII werden das Vorhaben, die Breitbandversorgung in Indien zu verbessern, sowie die Rolle der Zivilgesellschaft in dieser Hinsicht analysiert. In Abschnitt VIII werden Schlussfolgerungen präsentiert.

II. DER INSTITUTIONELLE RAHMEN FÜR DAS INTERNET UND DAS WACHSTUM VON INTERNETDIENSTLEISTUNGEN

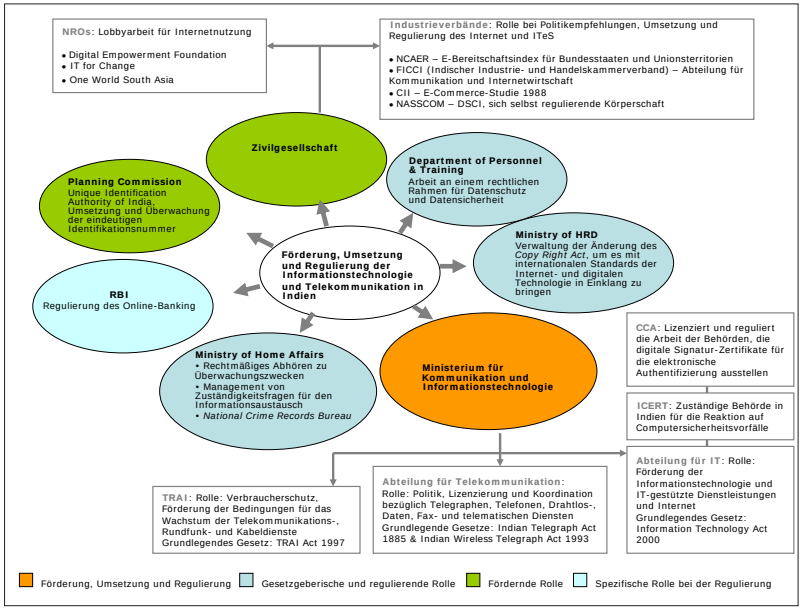
Die Behörden, die den Kern des institutionellen Rahmens für Telekommunikationsdienstleistungen bilden, sind die *Department of Telecommunications* (DoT, Abteilung für Telekommunikation) und die *Telecom Regulatory Authority of India* (TRAI, kurz: „*the Authority*"). Das zuständige Ministerium ist das *Ministry of Communications and Information* (MoC&IT, Ministerium für Kommunikation und Information). DoT und TRAI sind für Politik bzw. Regulierung bezüglich der Internetdienstanbieter verantwortlich. Die *Department of Information Technology* (DIT, Abteilung für Informationstechnologie) desselben Ministeriums hat das *Information Technology Act* (IT Act, Informationstechnologiegesetz) geschrieben, des grundlegenden Gesetzes zur Computersicherheit in Indien. Das *Ministry of Human Resources Development* (MHRD, Ministerium für die Entwicklung von Humanressourcen) überwacht den Zusatz zum *Copy Right Act* (Urheberrechtsgesetz), um es angesichts der Entwicklungen in der Internet- und Digitaltechnik mit internationalen Standards in Einklang zu bringen. Die *Department of Personnel & Training* (DoPT, Abteilung für Personal & Training) schafft zum ersten Mal in Indien einen rechtlichen Rahmen für Datenschutz und -sicherheit. Die *Planning Commission of India* (Planungskommission Indiens) ist für die Umsetzung des UID-Projekts für indische Bürger zuständig, und das *Ministry of Home Affairs* (MHA, Innenministerium) verwaltet die *National Crime Records* (nationale Unterlagen über Verbrechen). Außerdem reguliert die *Reserve Bank of India* (RBI, indische Zentralbank) Online-Banktransaktionen.

Überdies gibt es eine Reihe zivilgesellschaftlicher Organisationen, die an bestimmten Aspekten der Internetlandschaft beteiligt sind. Beispielsweise hat der *National Association of Software and Service Companies* (NASSCOM, Nationale Verband von Software- und Dienstleistungsunternehmen) eine unabhängige Datenschutzorganisation etabliert, den *Data Security Council of India* (DSCI, Datensicherheitsrat Indiens), um die Datenschutzpraktiken der indischen IT-Branche zu überwachen. Nicht. regierungsorganisationen (NRO), etwa *IT for Change* und die *Digital Empowerment Foundation* (DEF) betreiben Lobbyarbeit. In Abbildung 1 (Seite 70 oben) ist der institutionelle und Governance-Rahmen schematisch dargestellt.

Die große Zahl öffentlicher Behörden, die am Governance des Internets beteiligt sind, spiegelt die multidimensionale Natur der Aufgabe wider. Datensicherheit, geistige Eigentumsrechte und digitale Signaturen sind relativ neue und komplexe Themen, und verschiedene öffentliche Stellen sind damit betraut. Daher sind einige Elemente des rechtlichen Rahmens relativ neu und noch in der Entwicklung begriffen. Diese Aspekte werden in den jeweiligen Abschnitten dieser Studie behandelt.

Was die Verfügbarkeit und Nutzung des Internets betrifft, ist die Leistung Indiens aufgrund einer Vielzahl an Faktoren recht begrenzt. In Indien gab es im März 2010 etwa 16 Millionen Internetnutzer, eine Zahl, die von den 584,3 Millionen Mobiltelefonanschlüssen zum selben Zeitpunkt deutlich in den Schatten gestellt wird. Deswegen könnte das Internet als Opfer des Erfolgs der Mobiltelefonie betrachtet werden, da die Dienstanbieter sich auf das lukrative Geschäft mit Sprachtelefonie konzentrierten. Es gibt in Indien 104 Internetdienstanbieter, jedoch wird ein überwältigender Anteil des Markts von fünf Anbietern beherrscht, die übrigens auch Mobiltelefo-

Abbildung 1: Schematische Darstellung des institutionellen und Governance-Rahmens für das Internet in Indien



Quelle: Verfasser

niedienstleister sind.[4] Da der Markt für Mobiltelefonie Zeichen der Sättigung aufweist, insbesondere in städtischen Gebieten, wird es zunehmend wahrscheinlicher, dass die Dienstanbieter ihre Bemühungen, Datendienste anzubieten, verstärken werden.[5]

Tabelle 1: Internetnutzung und Bevölkerungszahlen

Jahr	Nutzer	Bevölkerung	Verbreitung in %
1998	1.400.000	1.094.870.677	0,1
1999	2.800.000	1.094.870.677	0,3
2000	5.500.000	1.094.870.677	0,5
2001	7.000.000	1.094.870.677	0,7
2002	16.500.000	1.094.870.677	1,6
2003	22.500.000	1.094.870.677	2,1
2004	39.200.000	1.094.870.677	3,6
2005	50.600.000	1.112.225.812	4,5
2006	40.000.000	1.112.225.812	3,6
2007	42.000.000	1.129.667.528	3,7
2009	81.000.000	1.156.897.766	7,0

Quelle: Internet World Stats

Gegenwärtig nutzen etwa sieben Prozent der Bevölkerung Indiens das Internet, was 81 Millionen Nutzern entspricht. Allerdings werden die Nutzerzahlen typischerweise als ein Vielfaches der Anschlüsse betrachtet[6]; die tatsächlichen Anschlüsse sind in Tabelle 2 angegeben. Außerdem ist die Verbreitung des Internets auf die Städte konzentriert. Sogar diejenigen Menschen, die häufig das Internet nutzen, verwenden einen langsamen und unzuverlässigen Zugang. PCs und Laptops sind selten vorhanden, und die Zahl mobiler Internetzugänge beginnt erst jetzt zu steigen. Es gibt knapp neun Millionen Zugänge mit Geschwindigkeiten von mindestens 256 kbps, dem Orientierungswert für Breitbandanschlüsse.[7] Für ihren Zugang zum Internet sind viele Nutzer auf gemeinsam genutzte Rechner in Internetcafés oder am Arbeitsplatz angewiesen. Diese Tatsache reduziert die Flexibilität, dämpft die Nachfrage und schränkt die Nutzung auf Funktionen und Dienste, die von unmittelbarem Interesse sind, ein. Sie verhindert auch, dass Menschen die vielen anderen Möglichkeiten des Internets, ihr Leben zu verändern, erkunden. Da mehr Frauen als Männer ans Haus gebunden sind, und da der Internetzugang in städtischen Gebieten einfacher ist, ist die Internetnutzung in der Bevölkerung ungleich verteilt, und zwar zugunsten in der Stadt lebender Männer. Da die Regierung und die öffentlichen Behörden, etwa die Versorgungsunternehmen, bislang kaum über eine bemerkenswerte Onlinepräsenz verfügten, hatten die Bürger außerdem bis vor kurzem keinen Anreiz, in einen relativ teuren PC oder einen Zugang zum Internet zu investieren.

Tabelle 2: Internet- und Breitbandanschlüsse

Jahr	Breitbandanschlüsse (in Millionen)	Internetanschlüsse gesamt (in Millionen)
März 2010	8,75	16,18
März 2009	6,22	13,54
März 2008	3,87	11,09
März 2007	2,34	9,27
März 2006	1,35	6,94
März 2005	0,18	5,55
März 2004	0,02	4,55
März 2003	0,01	3,6

Quelle: TRAI

Allerdings gibt es Anzeichen dafür, dass diese Situation sich ändert. Tabelle 2 zeigt, dass die Anzahl der Anschlüsse in den letzten Jahren schneller gewachsen ist als in der Zeit davor. Entsprechend hat sich die Nutzung ausgeweitet. Beispielsweise nutzen heute mehr Inder das Internet, um Bahnfahrkarten online zu kaufen. Die *Indian Railway Catering and Tourism Corporation Limited* (IRCTC, Indische Bahncatering- und -tourismusgesellschaft mbH), ein öffentliches Unternehmen, hat das Potenzial des Internets genutzt, um die Verkaufszahlen zu erhöhen und die Transparenz zu verbessern. Der Onlinefahrkartenverkauf ist exponentiell gewachsen, von etwa 3.300 Fahrkarten im Monat August 2002 auf über 2,4 Millionen im März 2008.[8] Ein weiterer enormer Vorteil ist die Reduzierung von Mittelsmännern bei solchen Transaktionen. Der Erfolg des IRCTC-Portals hat in großem Umfang ermöglicht, mehr über die Bekämpfung der Korruption in öffentlichen Behörden zu lernen. Das Portal, eines der erfolgreichsten E-Commerce-Portale in Indien, hat Millionen von Zugreisenden in die Lage versetzt, der Korruption, die vor seiner Einführung beim Fahrkartenverkauf in Indien vorherrschte, zu entgehen. Da die indische Eisenbahn die größte in Asien ist und täglich etwa 20 Millionen Fahrgäste transportiert, hat der Onlinefahrkartenverkauf transformierende Wirkungen gehabt.

Außerdem greifen die Menschen immer häufiger auf das Internet für Social Networking sowie für die Arbeits- und Partnersuche zu.[9] Mit fast 600 Millionen Mobiltelefonanschlüssen und erschwinglichen Preisen ab einen Cent pro Minute sind drahtlose Technologien die Hauptmöglichkeit, um Zugang zu vielen Internetdiensten zu bekommen, besonders zu solchen, bei denen der kleine Bildschirm sich als weniger hinderlich erweist, etwa Informationsaustausch und Musik. Obwohl es Hinweise darauf gibt, dass die Internetnutzung in kleineren Ortschaften und ländlichen Gegenden zunimmt, steckt das Ökosystem rund um das Internet in ländlichen Gebieten noch in den Kinderschuhen. Neben Versorgungslücken erweist sich das Fehlen von lokalen Inhalten ebenfalls als Hürde.

In Indien gibt es 22 von der Verfassung anerkannte Sprachen und mehr als 1.600 regionale Dialekte. Von der gesamten lese- und schreibkundigen Bevölkerung sind 37 Prozent in städtischen Gebieten des Englischen mächtig und 17 Prozent in ländlichen Gegenden. Die übrige Bevölkerung (d.h. 63 Prozent in städtischen und 83 Prozent in ländlichen Gegenden) können kein Englisch. Hindi nimmt den dritten und Bengali den achten Platz unter den zehn weltweit am weitesten verbreiteten Sprachen ein,

aber unter den zehn häufigsten Sprachen im Internet ist keine indische Sprache zu finden. Nutzer in kleineren Städten wendet begeistert Applikationen und Dienste in der lokalen Sprache an, obwohl es in Indien nur 1.249 Internetseiten in lokalen Sprachen gibt.[10] Im Gegensatz dazu sind Apps und Inhalte in Ländern wie China, Japan und Korea zu einem sehr großen Teil lokalisiert, und die Entwicklung in diesen Ländern geht hin zu anspruchsvolleren Technologien. Daher ist die Entwicklung von lokalen Inhalten zwingend, wenn die Internetnutzung in den unterversorgten Gebieten zunehmen soll.

III. DIE BEDEUTUNG INTERNETBEZOGENER THEMEN IN DER POLITISCHEN DEBATTE

Breit angelegte Beteiligung verschiedener Teile der Bevölkerung ist für eine demokratische Gesellschaft unentbehrlich. Studien in Industrieländern zeigen, dass das Internet eine vermehrte Beteiligung der Bürger unterstützt, indem es den Zugang zu Nachrichten und Informationen vereinfacht und kollektives Handeln erleichtert. Außerdem berichten einige politisch passive Bürger, zusätzlich zu den politisch Aktiven, dass Blogs den Online-Austausch mit anderen Bürgern fördern, indem sie sich ad hoc über politische Themen unterhalten und Informationen austauschen können.[11] In Indien rückte die Macht des Internets in der Politik und der Lobbyarbeit in den Vordergrund, als der Sozialaktivist Arvind Kejriwal eine Unterschriftenkampagne gegen die vorgeschlagenen Änderungen des RTI-Gesetz (siehe unten) startete.[12] Gegenwärtig werden Internetseiten lediglich als Ergänzungen zu traditionellen Informationsquellen in Papierform genutzt, und die Nutzung des Internets in der Politik steckt in Indien noch in den Kinderschuhen.[13] Alle großen politischen Parteien und die wichtigsten politischen Führungspersönlichkeiten haben einen eigenen Internetauftritt, auch wenn manche nicht besonders interaktiv sind. Zu den politischen Parteien mit eigenem Internetauftritt gehören die *Bharatiya Janata Party (BJP),* der *Indian National Congress (INC),* die *Communist Party of India (Marxist) (CPI(M)),* die *Samajwadi Party,* die *All India Anna Dravida Munnetra Kazhagam (AIADMK),* die *Shivsena,* die *Bahujan Samaj Party (BSP),* die *Rashtriya Janata Dal (RJD)* und die *Humanist Party.* Die drei führenden Parteien Indiens, der INC – die BJP und die CPI (M) – nutzen ihre Webseiten, um das Bewusstsein der Bevölkerung zu bilden und sie über ihre Agenda, ihren historischen Hintergrund und ihre Vision für die Zukunft zu informieren. Sie stellen eine Bandbreite an Informationen zur Verfügung, u.a. historischer Hinter-

grund, öffentliche Reden der Parteiführer, Parteiprogramme und andere Veröffentlichungen. Der INC, als eine der großen Parteien der Regierungskoalition, nutzt seine Webseite auch, um Informationen über Regierungsinitiativen bereitzustellen, etwa RTI, NREGA, Empowerment ethnischer Minderheiten und das Programm zum Verzicht auf die Rückzahlung landwirtschaftlicher Darlehen. Eine Studie aus der jüngsten Zeit, die die Webportale der großen politischen Parteien in den letzten Jahren untersuchte, kam zum Schluss, dass das Internet ein Instrument für effektive Kommunikation werden kann, aber dass sein Einsatz heute recht begrenzt ist.[14]

Die Bedeutung des Internets ist dem politischen Establishment natürlich bewusst. In ihrer Ansprache an das Parlament zum Amtsantritt stellte die amtierende Präsidentin Pratibha Patil u.a. fest, dass die Regierung zum Ziel hat, die Breitbandversorgung derart auszuweiten, dass jeder Panchayat[15] innerhalb von drei Jahren an ein Breitbandnetzwerk angeschlossen wird.[16] Um dieses Ziel zu erreichen, hat die Regierung die Initiative *Public Information Infrastructure* (PII) konzipiert, die den Internetzugang mit Apps verbinden soll, die öffentliche Dienstleistungen bereitstellen – und zwar in einem Maßstab, den kein Land der Welt bislang umgesetzt oder sich auch nur vorgestellt hat. Obwohl dieser Plan ambitioniert ist, hat er – richtige Umsetzung vorausgesetzt – das Potenzial, die Informations- und Governanceinfrastrukturen in Indien dauerhaft zu revolutionieren.[17] Die Hauptkomponenten von PII sind die Einrichtung von vier nationalen Datenzentren und schrittweise Hochgeschwindigkeitsdatenverbindungen für die 265.000 Panchayats und städtischen Gebietskörperschaften, die das Rückgrat der lokalen Governance bilden. Dies wird weitreichende Auswirkungen nicht nur auf Governance und die Systeme zur Bereitstellung öffentlicher Dienstleistungen haben, sondern auch auf die Wettbewerbsfähigkeit. Laut Auskunft von Sam Pitroda, der die PII-Initiative anführt,[18] ist ihr Kern die Ermöglichung des besseren Zugangs zu Informationen. Genauso wie der Zugang zu Telekommunikation ein wichtiger Katalysator für die Verwirklichung von Verbesserungen der Produktivität und der Effizienz geworden ist, hat der Zugang zu Information das Potenzial, die Art und Weise der Erbringung öffentlicher Dienstleistungen zu ändern, was unter Umständen die Möglichkeit eröffnet, die Vorteile des Wirtschaftswachstums breiter zu verteilen.[19]

Der Zugang zu Information hat weiterhin das Potenzial, das Leben der Menschen und die Politik zu verändern und Indiens Demokratie zu stärken. Indiens *Right to Information Act* (RTI, Gesetz über das Recht auf Informationen) wurde vom Parlament im Jahre 2005 in seiner heutigen Form verabschiedet und ermöglicht Indern den Zugang zu öffentlichen Akten. Das Gesetz erlaubt es jedem Bürger Indiens, von Behörden der Zentralregierung, der Regierungen der Bundesstaaten oder von öffentlichen Unternehmen oder Banken Informationen zu fast jeder Frage im Zusammenhang mit der Arbeit der Behörde oder des Unternehmens zu verlangen, und zwar in einem vernünftigen Zeitraum und zu einem äußerst niedrigen Preis. Obwohl das Gesetz nicht vorschreibt, dass gewisse Sorten von Informationen, z.B. bezüglich Sicherheit, offengelegt werden müssen, ist sein Geltungsbereich breit angelegt und wenig reguliert. Versuche seitens der Regierung, das RTI derart zu ändern, dass es nicht mehr als effektives Instrument für Rechenschaftspflichtigkeit gewirkt hätte, riefen Proteste von Sozialaktivisten auf den Plan. Im August 2006 zog die Regierung die vorgeschlagenen Änderungen des *Right to Information Act* zurück und versprach, bei jeglicher künftigen Aktion zu diesem Thema den demokratischen Prozess einzuhalten.

Das RTI hat viele öffentliche Diskussionen und Debatten ausgelöst, und zwar in einem unter gewöhnlichen Bürgern untypischen Ausmaß. Das Internet hat wesentlich dazu beigetragen. Obwohl das RTI-Gesetz weithin als Instrument zur Eindämmung der Korruption im öffentlichen Leben begrüßt wird, ist es auch deswegen bedeutend, weil es die staatliche Rechenschaftspflichtigkeit verbessern könnte. Demokratische Governance erfordert eine informierte Bürgerschaft, und ein Mangel an Transparenz staatlichen Handelns hat den Effekt, das Wirken von Partikularinteressen gegen das öffentliche Interesse zu verbergen.[20] Indem es die öffentliche Beteiligung am Regierungsgeschehen erleichtert, könnte das RTI potenziell den Weg für eine tatsächlich partizipatorische Demokratie bereiten. Die Bedeutung von Internet- und Informationstechnologie wird dementsprechend in politischen Diskussionen immer stärker aufgeworfen. Die BJP hat zum ersten Mal ein IT-Manifest für die Parlamentswahlen 2009 erstellt. Die Regierungskoalition hat die Rolle des Internets in ihrem *National Common Minimum Programme* (etwa: Koalitionsvereinbarung) aufgenommen. Es ist zu erwarten, dass der oben beschriebene, ambitionierte E-Governance-Plan der Regierung, öffentliche Dienstleistungen online bereitzustellen, das Leben der Menschen sowie die Politik grundlegend verändern wird.

IV. DIE ART UND DIE AUSWIRKUNG DER IN INDIEN DURCHGEFÜHRTEN DATENSPEICHERUNG, EINSCHLIESSLICH DER EINDEUTIGEN IDENTIFIKATIONSNUMMER (UID)

Das *Ministry of Home Affairs* hat ein *National Crime Record Bureau* (NCRB, Nationales Büro für Kriminalakten) eingerichtet, um „eine Datenbank auf nationaler Ebene über Verbrechen, Verbrecher und Eigentum im Zusammenhang mit Verbrechen zu führen".[21] Ähnliches wird auf der Ebene der Bundesstaaten durchgeführt. Eine der explizit genannten Ziele des NCRB ist es, „die Sammlung, Speicherung, Abfrage, Analyse, den Transfer von Daten und Informationen sowie den Datenverbund unter Polizeistationen, Distrikten, Leitstellen auf Bundesstaatenebene und anderen Organisationen/Behörden, auch auf der nationalen Ebene, zu erleichtern". Die gespeicherten Daten umfassen u.a. Fingerabdrücke sowie persönliche und kulturelle Informationen und Fotografien von Individuen. Detaillierte Unterlagen über Eigentum an Automobilen und Immobilien etc. gehören ebenfalls dazu. Allerdings gibt es wenig öffentliche Diskussion über den NCRB, seine Arbeitsweise oder seine Effektivität.

Im Gegensatz dazu hat das UID-Projekt immenses Interesse geweckt. Im Januar 2009 hat die Regierung Indiens die *Unique Identification Authority of India* (UIDAI, Indische Behörde für eindeutige Identifikation) als ein der *Planning Commission* zugeordnetes Büro eingerichtet. Der Auftrag der UIDAI ist die Schaffung „einer eindeutigen Identifikationsnummer (UID), die online und kosteneffizient verifiziert und authentifiziert werden kann, und die ausreichend robust ist, um doppelte und falsche Identitäten zu eliminieren"[22]. Die UID soll eine einzigartige Zahl sein, die sowohl grundlegende Informationen zu Demografie und Identität einer Einzelperson als auch biometrische Informationen (zehn Fingerabdrücke, Iris-Scan und Fotografie) speichern wird. Die UID wird als kritisch für den Aufbau einer *National Citizens Database* (Nationalen Bürgerdatenbank) betrachtet, einem wichtigen *Mission Mode Project* (etwa: prioritäres Projekt) des *National E-Governance Plan* (NeGP).

Bei der Etablierung des NCRB und der UIDAI handelt es sich um administrative Entscheidungen der zuständigen öffentlichen Stellen. Es gibt keine gesetzliche Grundlage für die beiden Behörden. Allerdings ist der Entwurf zum UIDAI-Gesetzentwurf im Umlauf; er ist dem Parlament noch nicht vorgelegt worden. Außerdem fallen beide Behörden in den Geltungsbereich des *Right to Information Act* (2005).

Während es bislang wenig Stellungnahmen der Öffentlichkeit zum NCRB gegeben hat, hat die UIDAI viel mehr Aufmerksamkeit erregt. Die Medien und andere Analysten unterstützen großenteils den Schritt zu einer eindeutigen Identität für jeden Bürger. Die Befürworter argumentieren, dass eine UID Millionen von Menschen helfen wird, besonders den Armen, die heute nicht in der Lage sind, ihren Anspruch auf Leistungen geltend zu machen, da sie sich nicht ausweisen können. Arme Menschen werden jetzt Zugang zu vielen Leistungen erhalten, beispielsweise staatlich subventionierte Lebensmittel, Beihilfen für Behinderte, Zuschüsse für verschiedene wirtschaftliche Aktivitäten, Nothilfe und viele andere mehr, die die Folgen von ungezügelter Armut, Naturkatastrophen, weitverbreiteten Behinderungen, Todesfällen und Vernichtung von Existenzgrundlagen abmildern können.

Allerdings gibt es auch deutliche Unruhe in mehreren Teilen der Zivilgesellschaft. Am 3. September 2010 haben Jean Dreze und Aruna Roy, zur Ikone gewordene Mitglieder des *National Advisory Council* (NAC, Nationaler Beirat) ernsthafte Bedenken bezüglich des UID-Projekts geäußert. Ihnen geht es um das Vorhaben, Arbeitslosenunterstützung im Rahmen des renommierten *Mahatma Gandhi National Rural Employment Guarantee Scheme* (MGNREGS, Nationales Programm zur Beschäftigungsgarantie im ländlichen Raum „Mahatma Gandhi") mit dem UID zu verbinden. Da Unsicherheiten bezüglich des gesetzlichen Rahmens des UID-Projekts bestehen, sind sie der Ansicht, dass es besonders gefährlich und unangemessen wäre, gegenwärtig Schritte zu einer solchen Verknüpfung zu unternehmen.

Viele zivilgesellschaftliche Organisationen betrachten die UID als Sicherheitsprojekt.[23] Sie befürchten, dass der Missbrauch der UID eine ernsthafte Bedrohung der Privatsphäre und der bürgerlichen Freiheiten darstellt. Sie argumentieren dahingehend, dass die Sicherheitsbehörden die UID missbrauchen werden, um Einzelpersonen ins Visier zu nehmen, mit dem Ziel, legitime Protest- und Demokratiebewegungen zu unterdrücken. Es bestehen Befürchtungen, dass UID-Daten in das vom *Ministry of Home Affairs* vorgeschlagene *National Intelligence Grid* (Natgrid, Nationales Geheimdienstraster), das Bedrohungen durch Terroristen und andere Extremisten verfolgen soll, eingespeist werden. Jedoch gibt

es nur wenige Informationen von offizieller Seite über Schaffung, Funktionsweise und Befugnisse des *National Intelligence Grid* sowie die dazugehörige Rechenschaftspflichtigkeit. Es gibt dahingehend Vorbehalte, dass die UID den Herrschaftsbereich des Staates im Leben des Bürgers ausweiten und die Beobachtung und Überwachung durch Sicherheitsbehörden, die eine durchwachsene Bilanz bezüglich rechtmäßigen Verhaltens aufweisen, erleichtern wird.[24] Es ist behauptet worden, dass weniger der normale Bürger und eher Nutzer aus dem privaten Sektor von der UID profitieren werden.

Die UIDAI argumentiert jedoch, dass der Erwerb einer UID freiwillig sein wird, und dass nur ein Personalausweis ausgestellt werden wird. Nutzer des Dienstes, beispielsweise Banken, Fluggesellschaften und öffentliche Behörden werden auf ihre Anfragen an die Datenbank zur Authentifizierung der Identität einer Person lediglich ja oder nein als Antwort erhalten. Die Verwendung der UID wird das Versickern öffentlicher Gelder aufhalten und helfen, öffentliche Dienstleistungen effektiver einzusetzen. Das UID-Programm ist das größte Beispiel für Bemühungen, den Großteil der Bevölkerung Indiens in den formellen Sektor zu bringen, aber es wird ein paar Jahre dauern, bis seine Auswirkungen sichtbar sein werden. Die erste zwölfstellige, auf biometrischen Daten basierende Identifikationsnummer wurde im Bundesstaat Maharashtra am 29. September 2010 ausgestellt, und die Regierung plant, bis zum Jahre 2014 für 600 Millionen Menschen UID-Nummern auszustellen.

Die möglicherweise größte Auswirkung des Programms wird bei einer anderen Initiative der Regierung zu spüren sein. Sie zielt darauf ab, die finanzielle Eingliederung zu fördern. Denn arme Menschen sowohl in ländlichen als auch in städtischen Räumen in Indien können häufig kein Bankkonto eröffnen, da sie keinen Personalausweis vorlegen können. Dadurch sind sie von den Vorteilen von Finanzdienstleistungen, beispielsweise Mikrofinanz, ausgeschlossen. Obwohl die UID notwendig ist, mag sie nicht ausreichend sein. Sie muss dadurch Unterstützung erfahren, dass Banken für Personen mit UIDs Bankkonten eröffnen. Außerdem muss es eine große Anzahl Bankfilialen geben, die Transaktionen ermöglichen. Obwohl die UID ein leistungsstarkes Instrument sein kann, um armen Menschen bei der Feststellung ihrer Identität zu helfen, damit sie die *know your customer*-Normen (KYC, kenne deinen Kunden) der Banken erfüllen können, werden indische Banken etwa 500 Millionen Bankkonten eröffnen müssen, eine Erhöhung um den Faktor fünf gegenüber der heutigen Zahl, wenn eine positive Wirkung erzielt werden soll.[25]

V. FRAGEN DES DATENSCHUTZES UND DER DATENSICHERHEIT, EINSCHLIESSLICH DES ÖFFENTLICHEN ZUGANGS ZU BESTIMMTEN ARTEN VON DATEN

Die Kultur von Gesellschaft und Arbeit in Indien scheint bezüglich Datenschutz und -sicherheit unbesorgt zu sein. Solche Themen haben offenbar in Europa und Nordamerika viel mehr Aufmerksamkeit erlangt als in Indien. Eine Undercover-Reportage für den Fernsehsender *Channel 4* in Großbritannien hatte im Jahre 2006 behauptet, dass Finanzunterlagen von Hunderttausenden von Briten zum Verkauf zur Verfügung stünden. Über diesen Vorfall wurde ausführlich in den Medien berichtet, und es wurde über die Art der Bedrohung spekuliert, die er für Indiens erfolgreiche Business Process Outsourcing-Branche im besonderen und IT-Dienstleistungen im allgemeinen darstellen könnte.[26] Indiens *Information Technology Act* enthält einige Vorschriften, die mehr oder weniger auf das Übereinkommen des Europarats über Computerkriminalität abgestimmt sind, obwohl Indien diesem internationalen Übereinkommen nicht beigetreten ist. Das *Information Technology Act*, 2000 (IT Act) ist das wichtigste Gesetz bezüglich Computersicherheit in Indien. Im Dezember 2008 hat das indische Parlament in Form des *Information Technology (Amendment) Act*, 2008 (*IT Amendment Act*, IT-Änderungsgesetz) weitreichende Änderungen des *IT Act* beschlossen. Während einige der Reformen des *IT Amendment Act* Gegenstand mehrjähriger Konsultationen mit Stakeholdern waren, wurden andere (darunter auch einige der neuen Antiterrormaßnahmen) als Folge der Anschläge in Mumbai im November 2008 eingeführt.

Das *IT (Amendment) Act*, 2008, schreibt vor: „Im Falle, dass eine juristische Person, die jegliche sensiblen persönlichen Daten oder Informationen, die sie besitzt oder bearbeitet, in einer Computerressource, die er besitzt, kontrolliert oder betreibt, bei der Implementierung und dem Erhalt von „*reasonable security practices and procedures*" („gebotene Sicherheitspraktiken und -verfahren) fahrlässig ist, und dadurch irgendeiner Person ungerechtfertigte Verluste oder ungerechtfertigte Gewinne herbeiführt, ist eine solche juristische Person haftpflichtig, der in dieser Weise betroffenen Person Schadenersatz zu leisten in Form von Kompensation." Das Gesetz stellt klar, dass „*reasonable security practices and*

procedures" so viel bedeutet wie Sicherheitspraktiken und -verfahren, die dazu angelegt sind, solche Informationen vor unautorisiertem Zugang, Schädigung, Verwendung, Modifizierung, Offenlegung oder Beeinträchtigung zu schützen. Sie können wie in einer Vereinbarung zwischen den Parteien spezifiziert sein, oder wie in irgendeinem Gesetz, das bis auf weiteres Gültigkeit hat, und in Ermangelung einer solchen Vereinbarung oder eines solchen Gesetzes, solche gebotenen Sicherheitspraktiken und -verfahren wie von der Zentralregierung nach Konsultation mit den Berufsverbänden und -vereinigungen, die sie für angemessen erachtet, vorgeschrieben werden.

Das *IT Amendment Act* kriminalisiert jetzt viele der Aktivitäten, die die Kerndelikte des Übereinkommens des Europarats über Computerkriminalität ausmachen. Dies wird durch den neuen Paragraphen 66 erreicht, der u.a. folgendes vorschreibt:

- Unautorisierter Zugang zu einem Computer, einem Computersystem oder -netzwerk (Paragraph 70 des IT Act kriminalisiert auch den unautorisierten Zugang zu Computersystemen, die von Regierungen als zu schützen bezeichnet werden);
- Unautorisierte Einführung von Computerviren in einen Computer, ein Computersystem oder -netzwerk;
- Unautorisierter Schaden an einem Computer, Computersystem oder -netzwerk, sowie an Daten oder Software;
- Unautorisierte Störung eines Computers, eines Computersystems oder -netzwerks;
- Unautorisierte Zugangsverweigerung zu einem Computer, einem Computersystem oder -netzwerk; sowie
- Unautorisierte Zerstörung oder Modifizierung von Daten in einem Computernetzwerk.

Diese neuen Delikte können mit bis zu drei Jahren Gefängnis und/oder Strafe von INR 500.000 (etwa USD 11.000) bestraft werden, aber nur, wenn „Betrug" oder „Unehrlichkeit" für solche Delikte nachgewiesen werden kann. Dies wird damit begründet, dass neue Nutzer in einem Land, in dem die Internetnutzung überhaupt neu ist, diese Taten unwissend begehen könnten und für ihre Neugier nicht hart bestraft werden dürfen. Die *Department of Information Technology* (DIT) der indischen Regierung hat das *Indian Computer Emergency Response Team* (CERT-in, Indisches Computernotfallteam) ins Leben gerufen, um auf Computersicherheitsvorfälle reagieren zu können, sofern und sobald sie geschehen. CERT-in leistet auch bei der Implementierung proaktiver Maßnahmen zur Reduzierung der Risiken von Computersicherheitsvorfällen Unterstützung. CERT-in agiert als zentrale Stelle, an die Vorfälle gemeldet werden, und unterhält eine Datenbank von Vorfällen. Die Stelle analysiert außerdem Trends und Muster der Aktivitäten von Eindringlingen.

Das *Indian Telegraph Act*, 1885 (Indisches Telegrafengesetz von 1885) reguliert die Überwachung von Kommunikation in Indien und deckt dabei die Telefonüberwachung und das Abfangen persönlicher Post ab. Paragraph 5 erlaubt es der Regierung, jegliche Verbindungen in jeglichem Telekommunikationsnetzwerk abzufangen. Allerdings hat das Oberste Gericht Indiens *(Supreme Court of India*) in einer Grundsatzentscheidung 1997 festgestellt, dass Artikel 21 der indischen Verfassung, der dem Individuum das Recht auf Leben und Freiheit gibt, implizit ein Recht auf Privatsphäre garantiert. Daher haben staatliche Behörden kein Recht, ohne ausreichenden Grund oder Befugnis Nachrichten abzufangen. Das Oberste Gericht hat restriktive Leitlinien darüber erlassen, wann und wie die Regierung abhören darf: Nur der *Union Home Secretary* (Innenminister) und sein bzw. ihr Amtskollege auf Bundesstaatenebene kann eine Anordnung zum Abhören verfügen, und dabei muss dargelegt werden, dass die begehrte Information auf keine andere Weise erlangt werden kann. Obwohl abgehörte Telefongespräche vor indischen Gerichten nicht als Beweismittel erster Ordnung gelten, ist die Praxis der Telefonüberwachung nicht ungewöhnlich, und Privacy International hat festgestellt, dass es weiterhin eine Lücke zwischen der durch das *Telegraph Act* etablierten Ordnung und ihrer Durchsetzung gibt.

Gleichzeitig kriminalisiert das *Telegraph Act 1885* illegales Abfangen von Daten über Computernetzwerke. Paragraph 26 kriminalisiert das Abhören von Botschaften durch Mitarbeiter der Telefongesellschaft und gewisse andere Beamte, und laut Paragraph 25 ist es eine strafbare Handlung, wenn ein Person in der Absicht, den Inhalt einer Nachricht abzuhören, eine Telegrafenleitung „oder jeglichen anderen Gegenstand überhaupt, der Teil eines Telegrafen oder in einem Telegrafen oder in der Nähe eines Telegrafen ist oder zu dessen Funktionieren benutzt wird" „beschädigt, entfernt, manipuliert oder berührt".

Die Gesellschaftshaftung gemäß dem *IT Act* ist für Geschäftsführer besonders schwerwiegend – die Haftpflicht für Übertretungen des Gesetzes durch Firmen wird denjenigen Personen, die für das Unternehmen verantwortlich sind, auferlegt, es sei denn, dass diese Personen nachweisen können, dass die Übertretung ohne ihr Wissen stattgefunden hat (und dass sie nicht fahrlässig gehandelt haben) oder dass sie die gebührende Sorgfalt haben walten lassen, um die in Rede stehende Zuwiderhandlung zu verhindern (und dass sie ihr nicht stillschweigend zugestimmt haben). Die praktischen Implikationen dieses Paragraphen sorgten im Dezember 2004 für internationale Aufregung, als der damalige Geschäftsführer von eBay Indien (damals unter dem Namen Baazee bekannt) verhaftet und für vier Tage ins Gefängnis gesperrt wurde, als ein zu beanstandender Videoclip auf der Baazee-Webseite zu finden war.

Es ist wenig überraschend festzustellen, dass Datenschutz und der offene Zugang zu Informationen häufig miteinander im Widerspruch stehen. Mit dem Anstieg der Nutzung des Internets ist auch das Bewusstsein für seine Macht, Arbeits-, persönliche, soziale und politische Räume zu stören, gewachsen. Es gibt jetzt zunehmende Sorge über Datenschutz, Datensicherheit und Onlinesicherheit (besonders von Kindern). Gleichermaßen bestehen Bedenken, dass Extremisten möglicherweise sichere Netzwerke missbrauchen, um gesetzeswidrige Handlungen durchzuführen, einschließlich der Planung und Ausführung terroristischer Angriffe. Wie oben festgestellt wurde Indiens *Information Technology Act 2000* im Jahre 2008 ergänzt, um die Vorschriften bezüglich vieler aktueller Bedenken zu stärken. Der neugefasste Paragraph 69 erlaubt den Zentral- und bundesstaatlichen Regierungen und ihren autorisierten Beamten, jede öffentliche Behörde anzuweisen, jegliche Information, die in jeglichem Computer generiert, übertragen, empfangen oder gespeichert werden, abzuhören, zu überwachen oder zu dechiffrieren (oder zu veranlassen, sie abzuhören, zu überwachen oder zu dechiffrieren). Behörden können Vermittler, Nutzer oder Personen, die für Computerressourcen verantwortlich sind, dazu heranziehen, bei diesen Aufgaben zu helfen. Die erbetene Unterstützung nicht zu leisten, wird mit sieben Jahren Gefängnis und einer Geldstrafe in unbestimmter Höhe bestraft.

Das ergänzte Gesetz enthält auch höhere Strafen für Dienste, die den Datenschutz verletzen. Paragraph 43 (2) behandelt den Umgang mit sensiblen persönlichen Daten. Paragraph 67 (2) behandelt Kinderpornografie und schreibt höhere Strafen dafür vor. In jüngster Zeit sind Fragen

bezüglich des Online-Zugangs zu Informationen über das Vermögen und die Einkommensquellen von Staatsdienern aufgekommen. Kandidaten in Parlamentswahlen auf nationaler und bundesstaatlicher Ebene sind gesetzlich verpflichtet, ihr Vermögen offenzulegen. Die Behauptung, dass das Gesetz nicht auf Richter anzuwenden sei, da sie nicht als „Staatsdiener" zu betrachten seien, löste erhebliche Kontroversen aus. Wahrscheinlich aufgrund des immensen öffentlichen Drucks haben Richter, darunter der Oberste Richter, allerdings zugesagt, ihr Vermögen und ihr Einkommen offenzulegen.

Nachdem Medienberichte behaupteten, dass von Indiens IT-Unternehmen verarbeitete persönliche Daten von manchen Mitarbeitern illegal weitergeleitet wurden, hat die profilierte und erfolgreiche IT-Branche Indiens neben der Gesetzgebung und ihrer Durchsetzung bezüglich der Datensicherheit ein selbstregulierendes System etabliert, um die Sicherheit und das Image der Branche zu verbessern. Im Jahre 2007 hat NASSCOM eine unabhängige Datenschutzorganisation eingerichtet, den Datensicherheitsrat Indiens (DSCI, *Data Security Council of India*), mit dem Auftrag, Mitglieder bei der Einhaltung von Datensicherheitsnormen in den vielen Ländern, in denen sie tätig sind, zu unterstützen. Er ist Mitgliedern bei Auditierung, Kapazitätsaufbau und Benchmarking behilflich. Allerdings ist er noch keine Körperschaft des öffentlichen Rechts.[27]

Ein Gerangel zwischen Indiens *Department of Telecommunications* und dem Hersteller des BlackBerry Smartphone, dem kanadischen Unternehmen Research in Motion (RIM), bezüglich des Zugangs zu unverschlüsselten Versionen von Nachrichten erlangte viel Aufmerksamkeit und fasst den Konflikt zwischen Datenschutz und nationaler Sicherheit eloquent zusammen. In Zeiten der tatsächlichen Bedrohung der nationalen Sicherheit ist Indien nicht das einzige Land, das sich mit solchen Themen auseinandersetzt. Die indische Regierung forderte RIM auf, Zugang zu seinen verschlüsselten E-Mail und Messenger-Diensten zu Zwecken der nationalen Sicherheit zuzulassen, sie drohte andernfalls mit einem Verbot der Dienste in Indien. Die Sorge seitens der geschäftlichen wie auch der allgemeinen BlackBerry-Nutzer ist, dass der Staat durch diese Maßnahme über die größte Sammlung an Informationen verfügen würde, ohne dass die Nutzer irgendeine Vorstellung davon hätten, wie er diese Informationen in der Zukunft nutzen könnte. Zudem wird von einigen behauptet, dass eine moderne, im Netzwerk eingebettete Technologie häufig Verschlüsselungssysteme verwendet, die für jede Nachricht einen neuen

Code-Schlüssel erzeugt, weswegen es fast unmöglich wäre, alles so zu entschlüsseln, dass der Staat es lesen könnte. Das DoT hat alle Netzwerkbetreiber aufgefordert, ihre Netzwerke aufzurüsten, sodass es Informationen, die über die Messenger-Dienste von RIMs BlackBerrys gesendet und empfangen werden, abhören kann, und hat dem Unternehmen eine Frist im Oktober 2010 gesetzt, um eine Lösung anzubieten. Andernfalls werde die Regierung ein Verbot aussprechen. Außerdem hat Indien Google, Skype und RIM aufgefordert, lokale Server in Indien aufzubauen und den Sicherheitsbehörden zu erlauben, den Datenverkehr zu überwachen.

Wie oben festgestellt werden die Betreiber von Telekommunikationsdienstleistungen, etwa Festnetz- oder Mobiltelefonie oder Internetdienstanbieter gemäß dem *Indian Telegraph Act 1885* reguliert, der eine Lizenzierung vorschreibt. Paragraph 5 dieses Gesetzes gibt dem Staat die übergeordnete Macht, jegliche Kommunikationen abzuhören. Paragraph 69 des *Information Technology (amendment) Act* von 2008 verstärkt dies weiter und verpflichtet alle Netzwerkbetreiber, solches Abhören zu erleichtern, wenngleich die entsprechende autorisierte Person zunächst das vorgeschriebene Verfahren für solche Aktionen beachten muss. Der Staat hat in einigen Fällen diese Macht benutzt, um den Zugang zu bestimmten Webseiten zu sperren. Die Sperrung von Webseiten fing 1996 an, als Internettelefonie-Webseiten von der damaligen Monopolgesellschaft für internationale Fernsprechverbindungen in Indien, VSNL, blockiert wurden. Im Jahre 2003 hat CERT-in unter Aufsicht des DIT Richtlinien für die Sperrung von Webseiten entwickelt, indem sie eine Liste von Behörden mit dem Recht zu sperren erstellt hat und den Prozess des Sperrens und die zulässigen Gründe dafür definierte. In den meisten Fällen, die das Sperren bestimmter Seiten betreffen, schreibt eine Stelle des *Ministry of Communication and Information Technology* (Ministerium für Kommunikations- und Informationstechnologie) einen kurzen, vertraulichen Vermerk an die Internetdienstanbieter, in dem sie angewiesen werden, den Zugang zu den genannten Seiten zu sperren. Die Internetdienstanbieter müssen den Empfang solcher Vermerke sowie ihre Einhaltung bestätigen.[28]

Zur Veranschaulichung: Der indische Staat hat im Jahre 2006 die Internetdienstanbieter aufgefordert, den Zugang zu den folgenden Webseiten zu sperren.

Tabelle 3: Liste verbotener Webseiten in Indien 2006

www.soniamaino.com	www.hinduunity.org
mypetjawa.mu.nu	pajamaeditors.blogspot.com
exposingtheleft.blogspot.com	thepiratescove.us
commonfolkcommonsense.blogspot.com	bamapachyderm.com
princesskimberley.blogspot.com	merrimusings.typepad.com
mackers-world.com	www.dalitstan.org
hinduhumanrights.org/hindufocus.html	nndh.com
bloodroyaltriped.com	imagessearchyahoo.com
imamali8.com	rahulyadav.com

Quelle: http://censorship.wikia.com/wiki/List_of_Sites_Banned_in_India

In jüngster Zeit hat sich die Praxis dahin entwickelt, den Zugang zu spezifischen IP-Adressen (z.B. 173.194.36.104) statt zum Hostnamen (z.B. www.google.com) zu sperren. Über die Gründe, den Zugang zu bestimmten Webseiten zu sperren, wird viel spekuliert. In den meisten Fällen ist man der Ansicht, dass die Webseiten antiindisches, extremistisches oder anderes volksverhetzendes Material veröffentlichen. In einigen Fällen meint man, dass die Webseiten indische Gefühle bei der Darstellung von Sexualität verletzen. Allerdings scheinen die Listen zu kurz zu sein, um alle oder auch nur die meisten Seiten aufzuführen, die wahrscheinlich ähnliches Material darstellen. Häufig wird behauptet, dass Willkür im Spiel ist.

Unter den vielen Gesetzen, die in den letzten Jahren zu den Themen Daten und Informationen erlassen wurden, wird Indiens *Right to Information Act*, 2005, als Meilenstein betrachtet. Sein Ziel ist, für Bürger den „Zugang zu Informationen, die von den öffentlichen Behörden kontrolliert werden, [zu gewährleisten,] um Transparenz und Rechenschaftspflichtigkeit beim Funktionieren jeder öffentlichen Behörde" zu fördern. Der Begriff „Information" im Gesetz bezieht sich auf jegliches Material in jeglicher Form, einschließlich Akten, Dokumente, Vermerke, E-Mails, Meinungsäußerungen, Empfehlungen, Presseerklärungen, Rundschreiben, Anordnungen, Logbücher, Verträge, Berichte, Papiere, Warenmuster, Modelle und Datenmaterial, das in jeglicher elektronischer Form vorliegt sowie Informationen bezüglich jeglicher privaten Körperschaft, zu denen eine öffentliche Behörde unter jeglichem anderen geltenden Gesetz Zugang hat.

Das Recht auf Information beinhaltet das Recht,

- Arbeit, Dokumente und Akten zu prüfen;
- aus Dokumenten oder Akten Notizen oder Extrakte oder beglaubigte Kopien anzufertigen;
- beglaubigte Materialproben zu nehmen; und
- Informationen in Form von Disketten, Bändern, Videokassetten oder in jeglichem anderen elektronischen Modus oder durch Ausdrucke zu erlangen, wenn solche Informationen auf einem Rechner oder in jeglichem anderen Gerät gespeichert ist.

Das Gesetz erfüllt ein seit langem bestehendes Bedürfnis, Bürger in die Lage zu versetzen, ohne großen Aufwand Informationen von „öffentlichen Behörden" zu erlangen. Das Gesetz betrifft solche Behörden, die direkt oder indirekt im Besitz der Regierung sind oder von ihr kontrolliert oder finanziert werden. Die Geheimdienste und Sicherheitsbehörden fallen im Allgemeinen nicht unter das RTI, obwohl auch dort Korruption nicht außerhalb des Geltungsbereichs dieses Gesetzes ist. Das RTI-Gesetz schreibt vor, dass alle öffentlichen Behörden ihre Akten angemessen katalogisiert und in einer Art und Weise erschlossen führen müssen, die das Recht auf Information gemäß dem Gesetz erleichtert. Um den Zugang zu solchen Unterlagen zu erleichtern, sollen alle angemessenen Unterlagen computerbasiert erfasst und alle Behörden landesweit durch ein Netzwerk verbunden werden. Wer gemäß diesem Gesetz Informationen erlangen möchte, muss schriftlich oder elektronisch einen entsprechenden Antrag einreichen und die vorgeschriebene Gebühr entrichten. Antragsteller brauchen keinen Grund für ihren Antrag auf Auskunft anzugeben.

Vom RTI wird beträchtlich Gebrauch gemacht. Die folgende Tabelle weist die zehn öffentlichen Behörden mit den meisten RTI-Anfragen und deren Status aus.

Tabelle 4: Nutzungsstatistiken der zehn öffentlichen Behörden mit den meisten Anfragen im Zeitraum 1. Januar 2008 bis 12. September 2010

Rang	Öffentliche Behörde	Anfragen gesamt	In Bearbeitung	Erledigt (%)
1	Department of Personnel & Training (Abteilung für Personal & Training)	5.581	2.074	3507 (62,84 %)
2	Bharat Petroleum Corporation Limited (BPCL)	4.264	237	4027 (94,44 %)
3	Ministry of Environment & Forests (Ministerium für Umwelt und Forsten)	3.356	1.352	2004 (59,71 %)
4	Central Vigilance Commission (Antikorruptionskommission)	1.991	907	1084 (54,45 %)
5	Steel Authority of India Ltd. (SAIL)	1.375	966	409 (29,75 %)
6	CSIR Hqrs., New Delhi	1.156	82	1074 (92,91 %)
7	Ministry of Mines (Bergbauministerium)	921	104	817 (88,71 %)
8	NHPC Ltd.	866	26	840 (97,00 %)
9	Delhi Polizei	833	518	315 (37,82 %)
10	Ministry of Civil Aviation (Ministerium für zivile Luftfahrt)	691	11	680 (98,41 %)

Quelle: http://164.100.42.72/rtistatus/RTIMISStatus.aspx

Tabelle 4 zeigt, dass die beantragten Informationen häufig Versorgungsbetriebe, Arbeitsplätze und Lebensgrundlagen, staatliche Leistungen, Infrastruktur, illegale Bauten, andere umweltrelevante Themen sowie polizeiliche Ermittlungen betreffen. Personen, die mittels RTI Informationen beantragt haben, haben mehrere hundert Erfolgsfälle sehr detailliert dokumentiert.[29]

Es hat aber auch Rückschläge gegeben. Ein RTI-Aktivist, der Umweltschützer Amit Jethwa, wurde am 20. Juli 2010 getötet, vermutlich weil er unliebsame Fragen über den Bergbau im Bundesstaat Gujarat gestellt hat. Im Januar wurde Satish Shetty, der angeblich viele Grundstücksbetrügereien in Maharashtra enthüllt hatte, ebenfalls ermordet. Während solche extremen Vergeltungsmaßnahmen ungewöhnlich sind, scheint es doch, dass der Erfolg von RTI-Fällen manchmal von der wahrgenommenen Auswirkung auf Kapitalinteressen abhängt, deren Interesse es ist,

dass gewisse Informationen vertraulich bleiben.[30] Einerseits soll das RTI Governance stärken, andererseits funktioniert es aber ebenfalls im Rahmen der gegenwärtigen, verzerrten Governance. Mehr Erfolgsfälle werden hoffentlich dazu dienen – schrittweise, wenn nicht auf einmal – den politischen Willen zu stärken, das RTI-Gesetz robuster durchzusetzen, indem diejenigen, die aufgrund ihrer Nutzung des Gesetzes geschädigt werden könnten, geschützt werden.

VI. DAS GEGENWÄRTIGE SYSTEM DER GEISTIGEN EIGENTUMSRECHTE IN INDIEN

Indien hat bereits früh den Schutz geistiger Eigentumsrechte als sehr wichtig eingeschätzt. Indien war ein früher Unterzeichnerstaat sowohl der Berner Konvention als auch des TRIPS-Übereinkommens.[31] Indien ist allerdings kein Unterzeichnerstaat von WCT[32] und WPPT.[33] Das *Indian Copyright Act*, 1957 (ICA, indisches Urheberrechtsgesetz)[34] und die dazugehörigen *Copyright Rules* (Urheberrechtsregeln)[35] sollen Fragen im Zusammenhang mit den Rechten der Urheber geistigen Eigentums behandeln. Das Gesetz ist mehrmals geändert worden (1983, 1984 und 1994), um es mit internationalen Praktiken in Einklang zu bringen. Der *Copyright (Amendment) Bill*, 2010 (Gesetzentwurf zur Ergänzung des Urheberrechtsgesetzes, 2010) im Aufgabenbereich des MHRD wird derzeit von einem parlamentarischen Ausschuss überprüft.[36] Im Allgemeinen ist das Ziel des ICA, die legitimen Interessen der Urheberrechtsinhaber gegen die Interessen der Bürger an einem fairen und erschwinglichen Zugang zu urheberrechtlich geschütztem Material abzuwägen. Das Gesetz legt die Strafen für Urheberrechtsverletzungen fest. Es schreibt auch in bestimmten Fällen die Lizenzierung geistigen Eigentums zwingend vor.

Die meisten Länder folgen dem Modell des *Digital Millennium Copyright Act* (DMCA) der USA, um die Herausforderung bezüglich des Urheberrechtsschutzes angesichts der steigenden Digitalisierung zu meistern. Das Internet wird zunehmend eine Quelle für Datendiebstahl, wie an den Auswirkungen auf die Musik- und Verlagsbranchen offenkundig zu sehen ist. Die Filmbranche Indiens besitzt und produziert eine beträchtliche Menge geistigen Eigentums in Form von Filmen, Musik etc. In den letzten Jahren haben die Biotechnologie- und Informationstechnologiebranchen ebenfalls bedeutendes geistiges Eigentum geschaffen. Daher sind sie wichtige Stakeholder in einem Regelwerk geistiger Eigentumsrechte, das ausreichend auf die Belange der Urheber geistigen Eigentums eingeht.

Allerdings gibt es in Indien einen immensen Markt für Raubkopien von Musik und Filmen. Die *Special 301 Reports*,[37] die jährlich vom Büro des *United States Trade Representative* (USTR, Repräsentant für Handelsfragen der USA) veröffentlicht werden, führen Indien unter denjenigen Ländern auf, die seinen Bürgern und Unternehmen ausreichenden und effektiven Schutz der geistigen Eigentumsrechte verweigern. Es wird angenommen, dass die USA häufig Lobbyarbeit betreiben, um das System geistiger Eigentumsrechte Indiens strenger zu machen. Die Filmbranche Indiens im Besonderen hat die Unterstützung der Regierung erbeten, um ihr geistiges Eigentum, das sich in Dutzenden von Ländern großer Beliebtheit erfreut, zu schützen. Die Branche behauptet, dass ihr geistiges Eigentum in großem Maßstab illegal veröffentlicht oder heruntergeladen wird, was zu einem beträchtlichen Einkommensverlust ihrer Mitglieder führt. Die indische Filmbranche, allgemein als *Bollywood* bekannt, produziert mehr Filme als Hollywood. Dennoch liegen ihre Erträge bei nur zwei Prozent dessen, was in Hollywood verdient wird. Ein Bericht von Price Waterhouse Coopers im März 2010 behauptete, dass die indische Filmbranche im Jahre 2008 USD 959 Millionen und etwa 571.000 Arbeitsplätze aufgrund von Datendiebstahl verlor.[38]

Indiens Regelwerk zum geistigen Eigentum darf als schwach bezeichnet werden. Man geht davon aus, dass Urheberrechtsverletzungen so häufig vorkommen, dass man sie nicht verfolgen kann. Daher werden sie meist übersehen oder toleriert. Es wird argumentiert, dass Akteure in der Wertschöpfungskette, beispielsweise Internetdienstanbieter, wenige Anreize haben, in die Technologie und die Zeit zu investieren, die ein Sperren von Urheberrechtsverletzungen erfordern würde. Allerdings sind mehrere wichtige Initiativen in den letzten Jahren eingeleitet worden. Im Jahre 2006 haben Business Software Alliance und NASSCOM zusammengearbeitet, um die Verfolgung des Softwareunternehmens Netflix zu veranlassen. Der erzielte Vergleich schließt u.a. eine Schadenersatzzahlung in Höhe von USD 30.000, das Entfernen aller unlizenzierten Software (bzw. Raubkopien) und die Zulassung eines Audits der Computersysteme ein.

Im Kontext des sich entwickelnden Rechtssystems hält man digitales Rechtemanagement für dasjenige Instrument, das den Schutz des Urheberrechts leistet. Es beinhaltet die Anwendung einer Reihe von technischen und rechtlichen Mechanismen, die es Urheberrechtsinhabern ermöglichen, den Zugang zu ihren Werken zu kontrollieren sowie die

Arten zulässiger Nutzungen und den letztendlichen Vertrieb ihrer Werke in der digitalen Welt zu bestimmen. Im Einzelnen integriert es die Identifikation und den Schutz geistigen Eigentums in digitaler Form durch *Technology Protection Measures* (TPM, technologische Schutzmaßnahmen) und *Rights Management Information Systems* (RMI, Informationssysteme zur Rechtewahrnehmung). TPM sind Systeme und Technologien, die es Urheberrechtsinhabern ermöglichen, den Zugang zu ihren Werken zu kontrollieren, die Arten und Konditionen zulässiger Nutzungen sowie den letztendlichen Vertrieb ihrer Werke in der digitalen Welt zu bestimmen. RMI sind Mechanismen, die digitale Werke identifizieren, und die eingesetzt werden, um die Bereitstellung von Material an Kunden zu verwalten. Die vorgeschlagenen Ergänzungen des ICA beinhalten die Einführung des Paragraphen 2(xa), der RMI definiert, und Paragraph 65B, der den Schutz von RMI vorsieht. Der vorgeschlagene Paragraph 65A führt den Schutz technologischer Maßnahmen ein. Außerdem sorgt das *IT Act* 2000 für die durch das Wachstum von E-Commerce und E-Governance notwendige Befugnis des *Controller of Certifying Authorities* (CCA, Überwachungsbehörde für die Stellen, die elektronische Signaturen ausstellen), digitale Signaturen zu überwachen.

Allerdings sind die Schätzungen des Ausmaßes von Datendiebstahl und der diesbezüglichen Schäden umstritten. Es wird auch argumentiert, dass diese Zahlen eine Unkenntnis der sozioökonomischen Realitäten in Indien erkennen lassen, da die vielen Menschen, die geistiges Eigentum illegal herunterladen, sich die hohen Preise nicht leisten können. Die durch sie entstehenden Verluste sind symbolisch.[39] Tatsächlich besteht das Argument, insbesondere von den Befürwortern von Open Source Software, dass geistige Eigentumsrechte nicht nur nicht durchsetzbar sind, sondern auch unnötig, und dass sie sogar diejenigen Menschen, die sich die exorbitanten Preise legaler Filme, Videos oder Software nicht leisten können, ausbeuten. Behörden der indischen Regierung, z.B. die *National Knowledge Commission* (Wissenskommission), haben häufig ihre Unterstützung von Open Source Software geäußert.

VII. VORSCHLÄGE ZUR VERBESSERUNG DER BREITBAND-VERSORGUNG

Die sehr dürftige Breitbandversorgung in Indien bereitet vielen Stakeholdern, darunter Nutzer, Akteure der Industrie, die Regulierungsbehörde und die Regierung, Sorge. Mit knapp neun Millionen Verbindungen, was

weniger als eine für mehr als hundert Nutzer bedeutet, liegt Indien weit hinter seinen eigenen bescheidenen Zielen. Dies hat offensichtliche Implikationen für die große Mehrheit der Bevölkerung, besonders für diejenigen Menschen, die auf den *India National E-Governance Plan* angewiesen sind.

Glücklicherweise gibt es umfangreiche Bemühungen im Rahmen des *E-governance Plan*, die Konnektivität auszuweiten. Der Plan sieht die Schaffung von Breitbandverbindungen in allen Panchayats Indiens mittels öffentlich-privater Partnerschaften vor. Die *Common Service Centres* (CSC, Gemeinsame Dienstleistungszentren) unter dem NeGP verfügen über Breitbandverbindungen und werden dabei helfen, viele Dienstleistungen der Regierung online bereitzustellen. Der Staat setzt eine umfangreiche Infrastruktur ein, um die Dienstleistungen in den CSCs zu unterstützen und verfolgt das Ziel, die Effizienz von Projekten des privaten Sektors zu erreichen.

Die Telekommunikationsregulierungsbehörde TRAI hat ebenfalls die Notwendigkeit erkannt, die Breitbandversorgung auszuweiten und schließt derzeit ihren konsultativen Prozess ab, um Inputs bezüglich der Methoden zur Steigerung des Breitbandwachstums einzuholen.[40] Auf Grundlage der Themen, die im Konsultationspapier behandelt werden, werden die Empfehlungen wahrscheinlich fast alle relevante Aspekte abdecken, einschließlich Ausbau des Netzwerks, Mix aus Drahtlos- und Glasfasernetzwerken, die Vorzüge der verschiedenen Breitbandtechnologien, Endgeräte, Applikationen und andere Maßnahmen, die die Breitbandtechnologie betriebswirtschaftlich umsetzbar machen.

Der *Universal Service Obligation Fund* (USOF, Fonds für universelle Dienste) wurde 2002 eingerichtet, um die Telekommunikationsinfrastruktur im ländlichen Raum zu finanzieren. Seine Finanzierung kommt von einer fünfprozentigen Abgabe auf die Einkünfte aller Anbieter von Orts- und -ferngesprächen. Der USOF hat seit seiner Gründung vor acht Jahren etwas USD 5,5 Milliarden eingenommen und weniger als die Hälfte davon ausgegeben. Er ist dabei, Pläne für die Ausweitung des Breitbandzugangs auszuarbeiten. Diese umfassen die Unterstützung der glasfasergestützten Verbindungen für den Backhaul-Datenverkehr, der aufgrund des phänomenalen Wachstums der Mobiltelefondienstleistungen in Indien rapide ansteigt. Die Regierung hat kürzlich die Auktion von Radiofrequenzen für 3G- und kabellose Breitbanddienste (BWA) abge-

schlossen. Die Sieger der Auktionen, ein Mix aus bestehenden und neuen Akteuren auf dem Markt für drahtlose Dienste, haben bereits den Betrag ihrer Gebote in voller Höhe bezahlt. Die Regierung hat im Gegenzug ihr Versprechen eingehalten, den Siegern das vereinbarte Spektrum zuzuordnen. Dies ist eine erfreuliche Wendung. Man geht davon aus, dass kabellose Breitbanddienste, 3G und BWA (Broadband Wireless Access – drahtloser Breitbandanschluss) Ende 2010 oder Anfang 2011 zur Verfügung stehen werden und dass dies ein enormer Anstoß für Wachstum und Nutzung von Breitband in Indien sein wird. Es wird erwartet, dass die Anbieter der mobilen und internetbasierten Dienste, Indiens schnell wachsender Markt für mobile Mehrwertdienste, die Chance wahrnehmen werden, die die neue Breitbandkapazität im großenteils ungesättigten Markt für Dienste in Indien bietet.

VIII. SCHLUSSFOLGERUNGEN

Die deutliche Auslandspräsenz von Indiens erfolgreicher IT-Branche hat sie einer genaueren Prüfung durch Geschäftspartner bezüglich Datensicherheit, Datenschutz und geistige Eigentumsrechte ausgesetzt. Dieser Umstand war Anlass für Ergänzungen der existierenden Gesetzgebung, obwohl einige Elemente des gesetzlichen Rahmens sich noch immer entwickeln. Terroranschläge wie der in Mumbai haben die Regierung auch gezwungen, Gesetzgebungsverfahren einzuleiten, um Telekommunikationsverkehr und Computernetzwerke zu überwachen. Die niedrige Verbreitung des Internets und der Breitbandversorgung, besonders in ländlichen Regionen, hat den Staat gezwungen, sich auf Möglichkeiten zur Ausweitung der Versorgung in diesen Bereichen zu konzentrieren. Daher hat die Regierung einen Plan entwickelt, 265.000 Panchayats mit Breitbandinfrastruktur zu verknüpfen. Ziel ist es, viele öffentliche Dienstleistungen mittels des Internets zu erbringen und zu helfen, mehr Menschen in der Mitte der Gesellschaft zu integrieren. Gleichzeitig denkt die Telekommunikationsregulierungsbehörde über Möglichkeiten nach, USOF-Gelder für eine schnellere Einführung der Infrastruktur in unterversorgten Gebieten zu verwenden. All dies hat im Laufe der vergangenen zehn Jahre zu einer größeren Mitwirkung vieler öffentlicher Behörden und Verbände des privaten Sektors in internetbezogene Themen geführt. Entsprechend hat sich der Governance-Rahmen bis zur Unkenntlichkeit gewandelt.

Anstelle der Vernachlässigung dieses Themenbereichs sind intensive Konsultationen und Debatten getreten, zu denen nicht zuletzt das Internet selbst beigetragen hat. Ein markantes Merkmal dieser Debatte ist die Beteiligung zivilgesellschaftlicher Organisationen. In Indien gibt es eine lebendige Kultur von zivilgesellschaftlichen Organisationen und Aktivitäten. Die Zivilgesellschaft hat eine Schlüsselrolle bei der Bestimmung und der Beeinflussung einiger, doch gewiss nicht aller, großen Entscheidungen bezüglich des Internets gespielt. Eine frühe Entscheidung, Internetdienstanbieter von der Zahlung von Gebühren für ihre Lizenzen zu befreien, ist ein typisches Beispiel. Ähnlich folgte das *Right to Information Act* 2005 – eine Version aus dem Jahr 2002 wurde zurückgezogen, da man ihren Geltungsbereich für zu begrenzt hielt – Jahren der Lobbyarbeit durch zivilgesellschaftliche Akteure, etwa *Mazdoor Kisan Shakti Sangathan* (MKSS) unter der Leitung von Aruna Roy, heute Mitglied des einflussreichen *National Advisory Council* der Regierung. Anna Hazare, eine berühmte Aktivistin aus Maharashtra, hat sich bereits früh für Transparenz staatlichen Handelns eingesetzt. Mehrere Aktivisten, darunter die *National Campaign for People's Right to Information* (Nationale Kampagne für das Recht der Menschen auf Information), halfen bei der Entwicklung des später verabschiedeten Gesetzesentwurfs.

Die Macht des Internets in der Politik und der Lobbyarbeit kam während der Kampagne gegen die vorgeschlagenen Ergänzungen des RTI-Gesetzes zum Vorschein. Versuche seitens der Regierung, das RTI sogar nach seiner Verabschiedung derart zu ändern, dass es nicht mehr als effektives Instrument für Rechenschaftspflichtigkeit gewirkt hätte, riefen Proteste von Sozialaktivisten auf den Plan. Im August 2006 zog die Regierung die vorgeschlagenen Änderungen des *Right to Information Act* zurück und versprach, bei jeglicher künftigen Aktion zu diesem Thema den demokratischen Prozess einzuhalten.

Arvind Kejriwal, ein prominenter Aktivist für Transparenz staatlichen Handelns, kündigte einen sicheren Arbeitsplatz im öffentlichen Dienst, um die NRO *Parivartan* (Wandel) zu gründen, die Bürgern hilft, die volle Potenz des RTI-Gesetzes auszunutzen. *Parivartan* arbeitet mit mehreren Stakeholdern zusammen, z.B. mit Mietervereinen in ganz Indien, um ihnen zu helfen, mit dem Instrumentarium des RTI-Gesetzes Dienstleistungen wie Gesundheitsfürsorge und Versorgungseinrichtungen für Wasser, Strom, Bauarbeiten usw. zu verbessern.[41] *Parivartan* hat auch umfangreiche Kampagnen zur Bewusstseinsbildung durchgeführt, um Aufmerksamkeit

auf das Potenzial des RTI zu lenken. Die Webseite von *Parivartan* bietet eine Reihe hochwertiger Tools und Informationen an, um Bürger zu unterstützen. Die Organisation hat auch Auszeichnungen eingeführt, um besonders effektive mit TRI befasste Regierungsbeamte zu ehren.

Obwohl noch viel mehr zu tun ist, entwickelt sich das System in die richtige Richtung. Größere Verfügbarkeit und deswegen größere Nutzung des Internets wird zu mehr Transparenz, erhöhter Rechenschaftspflichtigkeit und natürlich zu einem besseren Zugang zu Informationen führen. Genauso wie der Zugang zur Telekommunikation ein wichtiger Katalysator zur Verwirklichung von Verbesserungen der Produktivität und Effizienz wurde, hat der Zugang zum Internet und zu Informationen das Potenzial, die Art und Weise, in der Bürger und Staat miteinander interagieren, zu verändern.

Übersetzung ins Deutsche: Sandra H. Lustig

BIBLIOGRAPHISCHE ANGABEN

- *Bhartiya Janata Party, führende Oppositionspartei Indien: http://www.bjp.org/*
- *Confederation of Indian Industry (October 2010): http://www.cii.in/*
- *Controller of Certifying Authorities (CCA): http://cca.gov.in/rw/pages/guidelinesissuedbycca.en.do*
- *Department of Technology (DOT), (Stand: 1. Oktober 2010): http://www.dot.gov.in/*
- *Federation of Indian Chambers of Commerce & Industry (Stand: Oktober 2010): http://www.ficci.com/events.asp*
- *Indian Computer Emergency Response Team (CERT-In), (Stand: 30. September 2010): http://www.cert-in.org.in/*
- *Indian National Congress, führende politische Partei Indiens: http://www.congress.org.in/new/*
- *International Telecommunication Union (ITU), The ICT Development Index, 2009.*
- *International Telecommunication Union (ITU), United Nations agency for information and communication technology issues, (Stand: 3. Oktober 2010): http://www.itu.int/net/about/index.aspx*
- *Ministry of Information Technology (MIT), (Stand: 29. September 2010): http://www.mit.gov.in/*
- *NASSCOM (Oktober 2010): http://www.nasscom.in/*
- *National Sample Survey of India (NSSO), Census: Literacy and Levels of Education in India, 2001: http://www.mospi.gov.in/mospi_nsso_rept_pubn.htm*
- *RTI Gateway: http://www.rtigateway.org.in/index.jsp*
- *Telecom Regulatory Authority of India (TRAI), National BroadBand Plan, Diskussionspapier, 31. Juli 2010, (Stand: 27. September 2010): http://www.trai.gov.in/ConsultationPapers_content.asp*
- *Telecom Regulatory Authority of India (TRAI), (Stand: 27. September 2010): http://www.trai.gov.in/Default.asp*
- *Telecommunication Regulatory Authority (TRAI), Performance Indicators Report: The Indian Telecom Services Performance Indicators January-March 2010, (Stand: 27. September 2010): http://www.trai.gov.in/WriteReadData/trai/upload/Reports/51/finalperformanceindicatorReport9agust.pdf*
- *World Bank, Building Broadband: Strategies and Policies for the developing World, Januar 2010: http://siteresources.worldbank.org/INFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/BuildingBroadband_cover.pdf*

1| *UNCTAD Information economy 2009: Die Zahl der Internetnutzer in Entwicklungsländern stieg Ende 2008 fünfmal so schnell wie in Industrieländern. Allerdings gehört Indien nicht zu den bezüglich Internetwachstum dynamischen Entwicklungsländern der Welt oder Südostasiens.*

2| *ICT Development Index report 2009 von ITU: Indien hat seinen Platz in der Rangfolge gehalten und stand 2007 auf dem 118. Platz, im Vergleich mit dem 117. Platz 2002. Während das Land sich beim Teilindex zu Zugang etwas verbessert hat (beispielsweise hat sich die Verbreitung von Mobiltelefonen stark ausgeweitet), weist es noch immer begrenzte Bandbreite pro Internetnutzer sowie niedrige Verbreitungsraten für Heimcomputer und Internet auf. Außerdem ist Indien auf Platz fünf der zehn Volkswirtschaften mit dem kostengünstigsten Mobiltelefon-Sub-Korb, hinter Dänemark, Hong Kong, Bangladesch und Macau.*

3| *Die TRAI hat im Juni 2010 ein Diskussionspapier in Umlauf gebracht, um einen National Broadband Plan (Nationalen Breitbandplan) zu entwickeln, der verschiedene Aspekte, die Herausforderungen für das Wachstum von Breitband in Indien sind, behandeln sollte: von der Definition von Breitband über die Ausweitung der Infrastruktur bis hin zu mehreren ordnungspolitischen Themen.*

4| *National Broadband Plan 2010: Die zehn größten Breitbanddienstanbieter besetzen 95 Prozent des Marktes, von denen 70 Prozent von den staatlichen BSNL und MTNL bedient werden. Mehr als 89 Prozent des Marktes gehören klar nur fünf Dienstanbietern, die über ein eigenes landesweites Netzwerk verfügen.*

5| *3G- und BWA-Frequenzen sind bereits zugeordnet, und dies wird zu erhöhter Nutzung für die Datenübertragung führen. Außerdem werden die in diesem Papier beschriebenen Initiativen der Regierung ebenfalls die Ausweitung von Datendiensten zur Folge haben.*

6| *Da eine Verbindung von vielen Nutzern genutzt wird, könnte der Faktor in manchen Jahren sogar neun betragen. Durchschnittlich wird der Faktor sechs in Indien angenommen.*

7| *TRAI, Definition des Begriffs Breitband: Eine „stets eingeschaltete" Datenverbindung, die interaktive Dienste, einschließlich Internetzugang, unterstützen kann und die eine Downloadgeschwindigkeit von mindestens 256 Kilobit pro Sekunde (kbps) vom Einwahlknoten (POP) des Breitbanddienste anbietenden Dienstanbieters zum einzelnen Anschluss aufweist, wo viele solcher einzelnen Breitbandverbindungen aggregiert sind und der Nutzer Zugang zu diesen interaktiven Diensten, einschließlich des Internets, durch diesen Einwahlknoten erlangen kann.*

8| *http://www.egovonline.net/articles-list/48-case-study/7262-helping-e-government-step-into-web-20.html*

9| *Verweis auf naukri.co, monster jobs, babajobs.com, bharat matrimony, shaadi.com usw.*

10| *Forschung von IAMAI und IMRB http://www.iamai.in/PRelease_Detail.aspx?nid=1744&NMonth=12&NYear=2008*

11| *Net gains in political participation: Secondary effects of Internet on community, Andrea Kavanaugh; B. Joon Kim; Manuel A. Perez-Qui Jones, Joseph Schmitz, Philip Isenhour in: Information, Communication and Society, Band 11, Nr. 7, Oktober 2008, Routledge*

12| *http://en.wikipedia.org/wiki/Arvind_Kejriwal#cite_note-8*

13| *Link analysis of Indian political parties web sites: a temporal comparison. Bhaskar Mukherjee. Assistant Professor, Department of Library & Information Science, Annals of library and Information studies Sept. 2009*

14| *a.a.O.*

15| *Gram Panchayats sind Kommunalverwaltungen auf der Dorf- oder Kleinstadtebene. Mit Stand 2002 gab es etwa 265.000 Gram Panchayats in Indien. Der Gram Panchayat bildet die Grundlage des Panchayat-Systems. Ein Gram Panchayat kann in Dörfern mit mindestens 300 Einwohnern etabliert werden. Manchmal werden zwei oder mehr Dörfer zusammengefasst, um ein Group-Gram Panchayat zu bilden, wenn die Bevölkerung der einzelnen Dörfer weniger als 300 beträgt.*

16| *Ansprache des ehrenwerten Präsidenten Indiens, Shrimati Pratibha Devisingh Patil, an das Parlament, New Delhi, 4. Juni 2009*

17| *Herr Sam Pitroda ist für dieses Projekt verantwortlich. Er ist Berater des Premierministers bezüglich öffentliche Information, Infrastruktur und Innovation. Er hat dem Premierminister bereits den Entwurf vorgelegt.*

18| *http://www.iii.gov.in/index.php*

19| *Auf einer einzigen Plattform werden öffentliche Daten zu Gesundheit, Arbeit, Ernährung, Preise, Bevölkerung, Verkehr, Geburten, Todesfälle, Erdbeben und Eheschließungen bereitgestellt. Nutzer können mit einem Mausklick auf Informationen über Städte und Dörfer sowie über Schlüsselinfrastrukturen, etwa Stromnetze, Bergwerke, Dämme, Flüsse und Nationalparke zugreifen. In ähnlicher Weise kann man nach Daten zu Pensionen, Kindergeldprogrammen, E-Justiz, öffentlichen Verteilungssystemen, Gefängnissen und Polizei, Grundbüchern und Wohlfahrtsprojekte suchen. Landkarten, Daten und Analysen werden über ein gemeinsames Portal zugänglich sein.*

20| *http://rti.aidindia.org/content/view/136/107/*

21| *http://ncrb.nic.in/index.htm*

22| *http://www.uidai.gov.in/*

23| *Siehe z.B. die Webseite http://cis-india.org/events/unique-identity-project*

24| *Usha Ramanathan, Economic & Political Weekly, 24.07.2010*

25| *http://www.livemint.com/2010/09/30214432/UID-programme-will-take-a-few.html?atype=tp*

26| *Siehe z.B. http://ibnlive.in.com/news/thursday-could-spell-doom-for-call-centres-in-india/23165-7.html (letzter Zugriff: 06.09.2010)*

27| *DSCI ist eine gemeinnützige Einrichtung mit einem unabhängigen Aufsichtsgremium. Die erklärten Ziele der Organisation sind:*

- *indische IT-/ITeS-Organisationen in die Lage zu versetzen, einen hohen Sicherheitsstandard und Datenschutz einzuhalten, indem sie „best practices" anwenden [ITeS: information technology enabled services, informationstechnologiegestützte Dienstleistungen];*
- *einen angemessenen Sicherheits- und Datenschutzstandard für die indische IT/ITeS-Branche zu entwickeln, zu überwachen und durchzusetzen, der adäquat, kosteneffektiv, anpassbar und mit den globalen Standards vergleichbar ist;*
- *Kapazitäten aufzubauen, um eine Sicherheitszertifizierung für Organisationen durchführen zu können;*
- *eine gemeinsame Plattform zu schaffen, um den Wissensaustausch über Informationssicherheit zu fördern und eine Gemeinschaft der Fachkräfte und Unternehmen im Sicherheitsbereich auszubauen;*
- *unter Fachkräften der Branche und anderen Stakeholdern ein Bewusstsein für Sicherheits- und Datenschutzthemen zu wecken.*

28| *Die Sperrung der Webseite der Separatistengruppe Kynhun wurde international diskutiert. Es hat mehrere weitere kontroverse Ereignisse in der Geschichte des Content-Management und der Sperrung von URLs/Webseiten gegeben.*

29| *http://www.rtiindia.org/forum/59746-success-stories.html*

30| *http://www.thehindu.com/opinion/Readers-Editor/article698823.ece*

31| *Trade-Related aspects of Intellectual Property Rights, handelsbezogene Aspekte der Rechte des geistigen Eigentums*
32| *WIPO-Urheberrechtsvertrag von 1996*
33| *WIPO-Vertrag über Darbietungen und Tonträger von 1996*
34| *http://www.copyright.gov.in/CprAct.pdf*
35| *http://www.copyright.gov.in/CopyrightRules1958.pdf*
36| *copyright.gov.in/Documents/CopyrightAmendmentBill2010.pdf*
37| *Siehe z.B.: http://www.ustr.gov/sites/default/files/Full%20Version%20of%20the%202009%20SPECIAL%20301%20REPORT.pdf*
38| *http://timesofindia.indiatimes.com/india/Piracy-cost-Bollywood-959m-Report/articleshow/5703165.cms#ixzz0zBmdOmw8*
39| *Siehe z.B.: http://www.cis-india.org/advocacy/ipr/blog/consumers-international-ip-watch-list-2009/?searchterm=None*
40| *Diskussionspapier über den National Broadband Plan, 10. Juni 2010, Zugriff über www.trai.gov.in/WriteReadData/trai/upload/ConsultationPapers/202/consultationon10june10.pdf*
41| *http://www.parivartan.com/home.asp*

<< zurück zum Inhaltsverzeichnis

KOREA

DER GEGENWÄRTIGE STAND DER IT-POLITIK UND IHRE AUSSICHTEN

Seong-Woo Ji

I. EINE EINFÜHRUNG: DIE INFORMATIONSGESELLSCHAFT KOREAS SIEHT DAS LAND ALS FÜHRENDE NATION. DER GRUNDGEDANKE DER IT-POLITIK

Dank seiner anhaltenden Bemühungen, seine in den vergangenen zehn Jahren erworbene Führungsrolle im elektronischen Bereich auszubauen, hält Korea gegenwärtig Platz 1 des *UN-Entwicklungsindex für Elektronische Verwaltung* (*UN Development Index of Electronic Government*) für Januar 2010. Die von der Regierung verordneten hierarchisch ausgerichteten Methoden zur Förderung der Informationsgesellschaft sind nicht nur bei der Planung der Infrastruktur auf Anerkennung gestoßen, sondern auch beim Ausbau des Dienstleistungsbereichs.

Jedoch wird das Land sich einem wachsenden Bedarf gegenüber sehen, der einen völlig neuen Weg erfordert, um für das bevorstehende Jahrzehnt eine nicht durch die Regierung gelenkte Informationsgesellschaft aufzubauen. Die neuen IT-Trends wie das Zusammenwachsen von Medien und Kommunikationsbereich, eine gesteigerte Mobilität, eine softwarebasierte Entwicklung und Personalisierung beschleunigen zudem diese Tendenz. Das Jahr 2010 stellt einen

bedeutenden Wendepunkt im Sinne einer Weiterentwicklung der „Informationsgesellschaft 1.0" hin zur „Informationsgesellschaft 2.0" dar und verankert neue Systeme einer informationsorientierten Strategie.

Die koreanische IT-Industrie ist trotz der Einflüsse des weltweiten wirtschaftlichen Abwärtstrends in den letzten Jahren erfreulicherweise gewachsen. Ende 2008 sah sich die Industrie des Landes im Zuge der Weltwirtschaftskrise in einer Talsohle, doch dank der 2009 von der Regierung gesetzten wirtschaftlichen Impulse vermochte sie sich zu erholen und hält sich derzeit im Aufwärtstrend. Die Leistungen der IT-Industrie können im positiven Sinne als Antriebskraft für eine Wiederbelebung des Wirtschaftslebens betrachtet werden.

Seit 2010 beginnt die IKT-Industrie sich auch dank der zahlreichen Investitionspakete der führenden Industrieländer zu erholen. Laut Angaben des Bundes der Koreanischen Industrie wird sich die Anziehungskraft der landeseigenen Industriemarken – bei anhaltender Erholung im Jahre 2010 – in beachtlicher Weise steigern.

Auch die koreanische IDC sah voraus, dass der IT-Markt des Landes um 3,9 Prozent wachsen und sich einem Volumen von 15 Milliarden Dollar annähern wird. Das Jahr 2010 muss daher zum Ausgangsjahr für eine neue Blüte der koreanischen IT-Industrie werden. Es ist also unbedingt nötig, den Blick eher auf die Maßnahmen der IT-Politik zu lenken als auf die IT als solche, um die wirtschaftlichen, sozialen und gesellschaftlichen Folgen einschließlich der negativen Nebeneffekte in den Griff zu bekommen.

Für die Administration des amtierenden Präsidenten Lee ist die Erreichung greifbarer Ergebnisse auf dem Feld der Informationsgesellschaft ein Muss. Um die Ziele Lees wie *Green IT*, *Cloud Computing* usw. zu erreichen, ist eine Zusammenfügung der Vorschläge und Pläne zur Förderung des Wirtschaftslebens unabdingbar. Die 2009 angekündigten Pläne müssen auf jedem Gebiet umgesetzt und ihre Ergebnisse regelmäßig überprüft werden. Insbesondere sind die Koreaner aufgerufen, unter dem kürzlich ins Leben gerufenen Präsidialrat für die Informationsgesellschaft (*Presidential Council on Information Society*) die Kraft eben dieser Informationsgesellschaft zu aktivieren und einen neuen landesweiten zweiten *To-Be*-Plan zu entwerfen.

Außerdem ist eine aktive Strategie als Reaktion auf den schnell wachsenden drahtlosen Internet-Markt notwendig. Die Verkaufszahlen beim drahtlosen Internet werden erwartungsgemäß diejenigen beim drahtgestützen Netz angesichts der schlagartig wachsenden Verbreitung des Smart Phones im Jahre 2010 übersteigen. Wichtig ist, eine solide und offensive Politik zu verfolgen, um die eingetretene Verzögerung auf dem Gebiet des drahtlosen Internets zu überwinden. Erforderlich ist ein Entwurf von Politiken aus verschiedenen Perspektiven heraus – wie etwa aus den Bereichen offener Zugang, Ausweitung der Smart Phone-Positionierung, einfache und kostengünstige Mobilfunk-Datenbanken, Sicherstellung von Hochqualitätsinhalten sowie Anhebung der Netz-Investitionen für den Offload-Mobildatenaustausch.

Schließlich wird die Sicherheitsfrage zukünftig prioritär zu behandeln sein. Die Industrie ist sich, zumal nach der DDoS-Attacke (*Distributed Denial of Service-Attacke*) des Jahres 2009, des Stellenwerts der Sicherheit durchaus bewusst. Denn die IT-Ökosysteme der Unternehmen und deren geschäftliche Integrität sind insgesamt bedroht. Sehr wichtig ist insbesondere eine zeitige Reaktion auf die Sicherheitsfrage in den neuen aufstrebenden Segmenten – etwa den Bereichen Virtuelle Realität, ARS (*Augmented Reality Systems*), Cloud-Systeme und dem Mobilbereich. Großer Bedarf besteht ferner beim Aufbau kooperativer Systeme durch die öffentlich-private Zusammenarbeit zur Bekämpfung von Cyber-Gewalt und Rechtsbrüchen. Darüber hinaus wäre auch das individuelle Sicherheitsbewusstsein kontinuierlich zu stärken.

II. DIE INFORMATIONSGESELLSCHAFT KOREAS UND DER DERZEITGE STATUS DER IT

II.1 Der Koeffizient von Internet-Nutzung und Nutzerzahl

Die Internet-Nutzung in Korea wächst beständig, und laut Stand vom Jahr 2009 nutzen annähernd 37 Millionen Menschen, d.h. 77,2 Prozent der Bevölkerung im Alter von über drei Jahren, das Internet. Wenn die als Muster zugrunde gelegte Bevölkerung das Alter von sechs Jahren überschritten hat, nutzen 77,6 Prozent das Netz, was ungefähr 35,7 Millionen Nutzern entspricht.

II.2 Nutzerverhalten bei der Internet-Nutzung

Die durchschnittliche Internet-Nutzung beträgt 13,9 Stunden pro Woche, wobei 48,3 Prozent der User das Web mehr als 14 Stunden pro Woche nutzen. 80 Prozent der Internet-Nutzer bedienen sich des Webs zur Einholung von Informationen und Rechercheergebnissen (89,4 Prozent), von Musik, Spielen und Unterhaltung (88,4 Prozent) sowie zwecks Austauschs von E-Mails, Nutzung der Messenger-Funktion und für andere Kommunikationsformen (87,0 Prozent).

II.3 Internet und Kommunikation

85,2 Prozent der Internet-Nutzer (angestiegen um 1,0 Prozent p.a.) erweisen sich als E-Mail-Nutzer, die die E-Mail-Funktion mindestens einmal in den letzten zwölf Monaten genutzt haben. Von diesen wiederum nutzten 68,3 Prozent die genannte Funktion im vergangenen Monat. Und wiederum 51,0 Prozent der Internet-Nutzer (angestiegen um 1,1 Prozent p.a.) haben Instant Messenger zuletzt in den vergangenen zwölf Monaten genutzt, und von diesen erneut 38,8 Prozent in der vergangenen Woche.

59,7 Prozent der Internet-Nutzer (angestiegen um 1,6 Prozent p.a.) sind Blog-User, die den Blog anderer Teilnehmer im vergangenen Jahr besucht haben. Von diesen sind 44,6 Prozent (angestiegen um 1,5 Prozent p.a.) Blog-Manager, die ihren eigenen Blog im Verlauf des vergangenen Jahres besucht und unterhalten haben.

II.4 Internet und wirtschaftliche Aktivitäten

Forschungsergebnissen zufolge sind 62,3 Prozent der Internet-Nutzer (angestiegen um 1,7 Prozent im Vergleich zum Vorjahr) „Internet-Nutzer mit Einkaufsabsicht", die zumindest einmal im Verlauf der letzten zwölf Monate Dienstleistungsprodukte (einschließlich Reservierung und Vorverkauf) erworben haben. 23,4 Prozent von ihnen haben in den letzten Monaten von dieser Funktion Gebrauch gemacht.

41,2 Prozent der Internetnutzer (angestiegen um 1,2 Prozent im Vergleich zum Vorjahr) haben im Verlauf der letzten zwölf Monate Internet-Banking getätigt. 31,6 Prozent von ihnen haben diesen Service in den letzten Monaten genutzt.

Zwischenzeitlich sind 9,0 Prozent der über 18-jährigen Internetnutzer (angestiegen um 1,8 Prozent im Vergleich zum Vorjahr) Nutzer des Wertpapierhandels im Internet geworden; sie haben diesen Web-Service im Verlauf des letzten Jahres genutzt.

II.5 Das Internet-Umfeld

Mit Stand des Jahres 2009 verfügen 81,2 Prozent (angestiegen um 0,6 Prozent im Vergleich zum Vorjahr) der Haushalte über einen Internetanschluss. Dies bedeutet einen Anstieg um 9,0 Prozent seit 2004 (72,2 Prozent). Die möglichen Wege der Internetverbindung daheim sind der xDSL-Service mit dem höchsten Prozentsatz von 75,6 Prozent, gefolgt von Fiber-optic LAN (einschließlich des Internet-Zugangs durch Hausgemeinschaften, FTTH) mit 27,0 Prozent, Kabel-Modem mit 25,0 Prozent und Wireless LAN mit 8,3 Prozent.

III. DIE INFORMATIONSGESELLSCHAFT, DER DERZEITIGE STAND DER IT SOWIE DIE DAMIT VERBUNDENEN FRAGESTELLUNGEN

III.1 Das Feld der Informationsgesellschaft: Cloud Computing und Green IT als die dynamischsten Faktoren zur Förderung des Green Growth

Sowohl in Korea als auch auf dem Weltmarkt hat *Cloud Computing* dank seiner Fähigkeit der Ausgabendrosselung durch die Übernahme neuer Systeme und schneller Dienstleistungsformen als IT-Faktor große Beachtung erlangt.

Die koreanische Industrie unternimmt Anstrengungen, um durch eine frühe Anwendung von *Cloud Computing* in der öffentlichen Nutzung die Marktführung zu übernehmen. Durch eine ganze Reihe von Projekten – etwa des Ministeriums für Öffentliche Verwaltung und Sicherheit („Einführung und Verbreitung von *Cloud Computing* für die öffentliche Nutzung"), durch das Ministerium für Wissensökonomie („Strategie zum Einsatz von *Cloud Computing* im Geschäftsleben") oder des Koreanischen Kommunikationsausschusses („Vorschlag zur Förderung eines K-Cloud-Service") – wurden verschiedene Strategien angeschoben. Im Dezember 2009 unterbreiteten zudem die drei beteiligten Institutionen den sogenannten „Generalvorschlag zur Verankerung von *Cloud Computing*".

Inzwischen hat auch die *Green IT*-Agenda der Regierung zur Unterstützung von *Green Growth* Anerkennung gefunden. So fasste das Präsidialkomitee für *Green Growth* (*Presidential Committee for Green Growth*) die politischen Maßnahmen verschiedener Abteilungen, die zum Thema Green Technology tätig sind, im Sinne der Nationalen Strategie zusammen. Entsprechend dem Generalvorschlag plant die Regierung bis zum Jahr 2013 die Investition von annähernd zwei Milliarden Dollar, um zehn verschiedene Maßnahmenkataloge auf drei verschiedenen Feldern umzusetzen. Im Zuge der Umsetzung ist zu erwarten, dass sich für die Produktion ein Anschubeffekt von fünf Milliarden Dollar, die Schaffung von 52.549 Arbeitsplätzen sowie eine Kohlenstoffverringerung von 18,4 Millionen Tonnen bis zum Jahr 2010 einstellen.

III.2 Das Internet: *Micro Blogging* und *Smart Search* im Rampenlicht

Dank der raschen Verbreitung des Smart Phone brachte das vergangene Jahr einen rapiden Anstieg von mobilen *social network service* (SNS). Die Zahl der SNS-Nutzer erreichte weltweit ganze 200 Millionen, wobei ein Anwachsen der Zahl auf acht Millionen bis zum Jahresende 2010 (eMarketer, 2009) erwartet wird. *Micro Blogging*-Dienste wie etwa Twitter erweisen sich als besonders gefragt.

Mit der Einführung des iPhone im November 2009 stieg auch in Korea die Zahl der Smart Phone-Nutzer deutlich an. Dem von der Nationalen Internet-Entwicklungs-Agentur (*National Internet Development Agency*) Koreas im Juni 2009 vorgestellten und veröffentlichten Bericht zufolge liegt die Nutzung des koreanischen mobilen SNS lediglich bei 5,4 Prozent. Allerdings gaben 47,8 Prozent der Nutzer an, künftig diese Dienstleistung nutzen zu wollen.

III.3 Kommunikation: Die durch das iPhone zu Jahresbeginn hervorgerufene zunehmende Beliebtheit des Smart Phone

Das Jahr 2010, so wird erwartet, ist wohl das „Jahr Nr. 1" einer wachsenden Beliebtheit des Smart Phone. Die Einführung des iPhone zum Ende November 2009 war der Startschuss für einen veritablen Smart Phone-Markt in Korea. Dem Samsung Wirtschaftsforschungsinstitut *(Samsung Economic Research Institute*) zufolge belegte das Smart Phone 2009 den fünften Platz unter den zehn führenden Bestsellern im Land.

Zusätzlich ist auch der Anstieg der App Stores – Märkte für offene Anwendungen im Mobilbereich – durchaus bemerkenswert. Apple lancierte den App Store 2008 und erzielte hierdurch mehr Profite als durch den Verkauf von iPhones, wobei koreanische Unternehmen wie Samsung, LG und SK als Wettbewerber in den App Store-Markt einstiegen. Auch Web-Unternehmen wie Daum und Naver stellen eigenen Plattformen für verschiedene Mobilanwendungen und auch mobile Web-Anwendungen bereit.

III.4 Die Medien: Der Beginn eines Zeitalters von Millionen IPTV-Nutzern und eines Mischmedien (*Cross Media*)-Fiebers

Offene Rechtsfragen haben zu einer mehrjährigen Verzögerung des IPTV-Dienstes geführt. Nachdem die diesbezügliche Gesetzgebung neugefasst wurde und die Regierung das Projekt nachhaltig unterstützte, etablierten sich diese Dienste auch in Korea. Die Zahl der Nutzer des Dienstes liegt nach nur neun Monate bei über einer Million (10/2009). Darüber hinaus lässt sich auch eine Änderung der Vermarktungsdynamik beobachten. Eine aggressive Marketing-Kampagne des IPTV-Geschäftsbereichs führte dazu, dass eine wachsende Zahl von Haushalten ihre Analog-Dienste gekündigt hat.

Das vielfach spekulierte Bündeln bzw. Zusammenführen von drahtgestützten und drahtlosen Diensten ist nun mit einer Reihe von Unternehmensfusionen aus den beiden Bereichen Wirklichkeit geworden. Im Juni 2009 fusionierten KT and KTF, und im Januar 2010 entstand aus den drei Kommunikationsunternehmen LG Telecom, G Dacom und G Powercom die „vereinigte" LG Telecom. Die Kommunikationsfirmen sind nun in der Lage, ihre Dienstleistungen effizienter anzubieten, indem sie das Hochgeschwindigkeitsnetz mit IPTV, Internet-Telefoniediensten und Mobiltelefonie-Diensten verknüpfen.

Als neuester Trend in der koreanischen Unternehmenslandschaft zeichnen sich Geschäftsmodelle ab, die auf Mischmedien (*Cross Media*) basieren. *Chosun Daily* beispielsweise präsentierte einen neuen Weg der Nachrichtenberichterstattung, indem Materialien sowohl über die traditionellen (Zeitungen/terrestrischer Rundfunk) als auch über die neuen Medien (Kabel, Satellit, Digital Multimedia Broadcasting und Internet) verbreitet wurden.

III.5 Sicherheit und Negativfunktion: Die wachsende Vorsicht vor Cyber-Terror nach dem DDoS-Angriff vom 7. Juli

Der DDos-Angriff (*Distributed Denial of Service-attack*) vom 7. Juli 2009, der führenden Unternehmen, Portalen und Finanzorganisationen im In- und Ausland Schaden zugefügt hat, war eine Warnung, den Blick verstärkt auf die Bedeutung der Internet-Sicherheit zu lenken.

Der Vorfall machte ganz offenbar eine Reihe von Problemen deutlich, wie etwa das Fehlen eines zentralen Kontrollsystems, die mangelhafte Funktionsweise der internationalen Kooperationssysteme, bestehende Defizite bei Experten und Ausstattung sowie eine unzureichende PC-Wartung durch die Internet-Nutzer selbst.

Mit dem unvermindert aggressiven Internet- und Messenger *Phishing*, das sich von Tag zu Tag raffinierter zeigt – ganz zu schweigen von bösartigen Virencodes und *Hacking* –, ist das Krisenbewusstsein im Bereich der persönlichen Information gewachsen. *Voice Phishing*, das typischerweise eine Zielperson anspricht und eine drahtgestützte Verbindung bzw. eine spezifische persönliche Information erfordert, ist im Messenger *Phishing* aufgegangen und zeigt sich nun schädlicher als je zuvor. Es handelt sich um einen Betrugsvorgang, der darauf basiert, dass aus dem Bekanntenkreis eine Identifikationsnummer gestohlen und Geld abgehoben wird. Messenger *Phishing* ist tückischer und organisierter geworden, der gestohlene Geldbetrag höher. Die Zahl der registrierten Betrugsfälle ist seit Januar 2009 von 109 auf 810 im August 2009 angestiegen.

IV. EINE STRATEGIE FÜR KOREA, ZU EINER FORTSCHRITTLICHEN WISSENSGESTÜTZTEN INFORMATIONSGESELLSCHAFT ZU WERDEN

IV.1 Ein Fördersystem für die Informationsgesellschaft

Der Präsidialrat für die Informationsgesellschaft (*Presidential Council on Information Society*) wurde offiziell im November 2009 mit dem Ziel gegründet, neue Perspektiven für den Aufbau einer landesweiten Informationsgesellschaft anzuregen und sich der Verbreitung dieser Idee sowie der Vorbereitung der Bürger zu widmen.

Der Rat selbst, der dem Büro des Präsidenten angegliedert und der öffentlich-privaten Zusammenarbeit an die Seite gestellt ist, ging als aufgestockte und umgestaltete Organisation aus dem früheren dem Büro des Premierministers unterstellten Komitee zur Informationsgesellschaft (*Committee on Information Society*) hervor. Seine Aufgabe ist es, als höchste Vermittlungseinrichtung Überlegungen zu Projektvorschlägen als auch Maßnahmen, zur Vernetzung von entsprechenden Politiken, zur Förderung der Informationskultur und zur Überwindung der digitalen Kluft anzustellen. Darüber hinaus ist es die Aufgabe des Rats, als Kontrollinstanz, indem er eine zukunftsorientierte Politikagenda für eine Informationsgesellschaft entwirft und vorantreibt.

Insgesamt besteht der Rat aus 31 Komiteemitgliedern einschließlich des Premierministers und eines zivilen Experten (Kak-Beom Lee, Professor an der KAIST) als Co-Vorsitzende. Die übrigen Mitglieder sind 15 Regierungsbeamte sowie 14 weitere zivile Experten.

Hauptfunktion des Rates ist die Umsetzung seiner Rolle als Kontrollinstanz, die die politischen Maßnahmen insgesamt verwaltet und miteinander harmonisiert. Ferner hat er die politischen Schlüsselmaßnahmen des Staates wie *Green Growth* auf taktischem Wege sowie die Aktivierung der Wirtschaft zu unterstützen, um so durch den Entwurf einer zukunftsorientierten Agenda zu einer fortgeschrittenen wissensgestützten Informationsgesellschaft zu gelangen.

IV.2 Konkrete Pläne für die Informationsgesellschaft

IV.2.1 Erstellung der Grundlagen zur Konversion ins IPv6

Der Koreanische Kommunikationsausschuss (*Korea Communications Commission*) und die Nationale Internet-Entwicklungsagentur haben ein Jahresziel sowie ein Konversionsprojekt angeschoben, um IPv6 (*Internet Protocol Version 6*) zu verankern. IPv6 wurde für den nationalen ISP mit dem Ziel konzipiert, es bis 2009 für das allgemein genutzte Netz anzuwenden. Dafür wurden Anstrengungen sowohl im Bereich Fortbildung als auch im Bereich Personaltraining unternommen.

Insgesamt flossen 1,8 Millionen Dollar in ein Modellprojekt, das zunächst eine Überprüfung der Technologie vornahm, um anschließend IPv6 auf das allgemeine und von der heimischen ISP betriebene Netz anzuwen-

den. Getragen wurde das Projekt von einem Konsortium aus elf Organisationen, die IPv6 erfolgreich übernehmen hatten.

Die Zahl der landeseigenen Organisationen, die dadurch IPv6 angenommen haben, liegt derzeit bei 43. Dies bedeutet einen Anstieg von sieben Prozent im Vergleich zum Vorjahr.

IV.2.2 Eine nächste Netzwerk-Generation für die Zukunft

IV.2.2.1 Das Giga-Internet

Durch die Regierung wurde im April 2009 ein „Vorschlag zum Einstieg in das Giga-Internet" unterbreitet, um den Einstieg in das allgemein genutzte Giga-Netz nach 2012 vorzubereiten. Der modellhafte Geschäftsbereich wurde durch die Nationale Agentur für die Informationsgesellschaft gefördert. Der Vorschlag umfasst den Aufbau eines Modellnetzwerks im Zeitraum 2009 bis 2012, Modelldienstleistungen, die Entwicklung der Technologie und die Schaffung eines geeigneten Umfelds. Auf diese Weise soll erreicht werden, dass die Leistungen des Giganetzes, das die zehnfache Geschwindigkeit des Breitbandkonvergenznetzes (BcN) aufweist, einer möglichst großen Zahl allgemeiner Haushalte zur Verfügung gestellt werden können. Gleichzeitig soll die Entwicklung künftiger Netzwerktechnologien ebenso wie die Erstellung einer Bedarfsperspektive im Dienstleistungsbereich in den Blick genommen werden.

IV.2.2.2 Das Breitbandkonvergenznetz
(Broadband Convergence Network, BcN)

Die Regierung hat den Aufbau des Breitbandkonvergenznetzes (BcN) unterstützt, eines kombinierten Netzwerks der kommenden Generation, das die problemlose, jederzeit sichere und ortsunabhängige Nutzung von Breitband-Multimediadienstleistungen der kombinierten Bereiche Kommunikation, Übertragung und Internet ermöglicht.

Ziel war der Aufbau eines Weltklasse-BcN als Nutzernetzwerk, das die Verfügbarkeit von Breitband-Multimedia-Leistungen mittels eines BcN-Roll-Out-Programms vorsieht. Als Ergebnis des BcN-Aufbauprogramms kann nun auch ein umfassender Hochqualitäts-Breitbanddienst für insgesamt ca. 37 Millionen Abonnenten (12 Millionen Haushalte verdrahtet, 25 Millionen Abonnenten drahtlos, laut Stand vom Dezember 2009) mittels eines intensivierten BcN-Abonnenten-Netzwerks angeboten werden.

Gefördert wird der BcN-Aufbau, um ein Informations- und Kommunikationsumfeld für jederman zu schaffen, das die Nutzung von QPS (*Quadruple Play Service* – gebündeltes, vierfaches Angebot von Internet, IP-Telefonie, Fernsehen, *video-on-demand* und Mobilfunk) praktisch zu jeder Zeit und an jedem Ort ermöglicht und zudem den Ausbau des 2010 bereits 40 Millionen Nutzer umfassenden drahtgestützten und drahtlosen Netzwerks vorantreibt.

IV.2.2.3 Die Implementierung von IP-USN

IP-USN (*IP-Ubiquitous Sensor Network* – IP basiertes universelles Sensor Netzwerk) ist eine Technologie, die auf praktische und sichere Weise objektive Informationen empfangen und übertragen kann. Sie ist kostengünstig und mit Blick auf Ausdehnung und Transfer von großer Reichweite innerhalb der Verbindung zu einer Internet-Infrastruktur wie etwa BcN und IPv6, die vor allem die Nutzer selbst, aber auch die Nutzung von 2G/3G sowie die WiBro-Technologie im Blick hat. Sie könnte als Schlüssel-Infrastruktur zum Einsatz kommen, die bei der Entwicklung von Green Growth benötigt würde – im Bereich der Verringerung der Kohlenstoffproduktion, der Energiedrosselung und der Schaffung einer umweltschonenden Umgebung. Hierzu sollten jene Sensor-Netzwerke zusammengefügt werden, die bislang sporadisch bei der Katastrophenprävention und bei der Wetterbeobachtung, aber auch in der Meeresmeteorologie, bei der Grundeigentumsverwaltung und in anderen Bereichen zum Einsatz gelangt sind.

IV.2.3 Die Belebung des IT-Geschäfts

Die IT-Exporte, die sich auf einen Wert von 120,9 Milliarden Dollar beliefen, sind aufgrund der Weltwirtschaftskrise und des von großer Zurückhaltung geprägten Konsumentenbewusstseins in den führenden IT-Nationen wie China und den USA im Vergleich zum Vorjahr um 7,8 Prozent zurückgegangen. Der allgemeine Industrieexport ist im Vergleich zum Vorjahr um 13,9 Prozent gesunken, was einem Abstieg um das 1,8-Fache im Vergleich zur IT-Branche entspricht. Der Umfang der von der IT-Industrie generierten Exporte beträgt 33,3 Prozent, dies bedeutet einen Anstieg von 2,2 Prozent im Vergleich zum Jahre 2008.

Die Regierung hat eine „IT Zukunftsstrategie Korea" (*IT KOREA Future Strategy*) angekündigt, als Maßnahme zur Umsetzung einer umfassenden Zukunftsvision der Regierung von Präsident Myung-Bak Lees. Ihr Ziel ist der Aufbau einer IT-Industrie, die zur Hauptantriebskraft der im Wachsen begriffenen Nation werden soll. Die Strategie umfasst fünf Schlüsselmaßnahmen: die Unterstützung der Vereinigung von zehn für den IT-Sektor strategisch wesentlichen Industrieunternehmen (1), die Forcierung des SW-Business als Quelle der Wettbewerbskraft im Industriesektor (2), den Aufbau einer weltweiten Lieferbasis für die führende ITZ-Ausrüstung (3), den Aufbau einer zweckmäßigen und fortschrittlichen Übertragungs- und Kommunikationsdienstleistung (4) sowie ein schnelleres und sichereres Internet (5).

IV.2.4 Der Informationsschutz

Die Zahl der Berichte über Viren in Form von Würmern, die durch die Nationale Internet-Entwicklungsagentur im Jahre 2009 in Korea registriert wurden, lag bei 10.395 (d.h. durchschnittlich 866 Fälle pro Monat). Dies entspricht einem Zuwachs von 22,7 Prozent im Vergleich zum Jahr 2008 (mit durchschnittlich 706 Fällen pro Monat). Die Zahl der berichteten Fälle von *Hacking*-Attacken betrug 2009 insgesamt 21.230, was einen Anstieg von 33,2 Prozent gegenüber 2008 mit damals 15.940 Fällen bedeutet. Aufgeteilt nach Art der Angriffe entfallen auf die Bereiche Spam Relay 56,4 Prozent, *Hacking* 4,2 Prozent und Manipulation von Webseiten 96 Prozent pro Jahr. Die verzeichneten Fälle von zwischengeschalteten Seiten zwecks Phishing Scam und einfache Angriffe sind um 15 Prozent zurückgegangen bzw. um 13,6 Prozent im Vergleich zum Vorjahr.

Bösartige Codes wie derjenige, der für den DDoS-Angriff vom 7. Juli 2009 zum Einsatz kam, werden zunehmend komplizierter und getarnter, so dass ihre Aufdeckung selbst Probleme mit sich bringen könnte, sie zu einem bestimmten Zeitpunkt aktiv werden oder eine komplexe Technik zur Ausführung nutzen. Zusätzlich hierzu verbreiten sich die jüngsten Angriffcodes nicht nur automatisch schlichtweg über verwundbare Punkte, so wie es für frühere Internet-Würmer typisch war, sondern breiten sich auch über das System der sozialen Netzwerke aus, wobei sie verschiedene Medien wie das Internet, E-Mails, IM und SMS nutzen, entsprechend dem jeweils unterschiedlichen Kommunikationsverhalten der Internet-Nutzer.

Unter dem Eindruck des genannten DDoS-Angriffs ist der Informationsschutz R&D laut Stand von 2010 aktiv dabei, Technologien zu entwickeln, die gewaltsame Internet-bezogene Eingriffe verhindern sollen. Insbesondere vier Projekte befinden sich in Entwicklung, deren Ziel es ist, einen neuerlichen Angriff in der Art der DDoS-Attacke vom 7. Juli 2009 unmöglich zu machen: eine neue Art der Aufdeckung und der technologischen Reaktion, um die Angriffsquelle im Vorfeld zu eliminieren; die automatische Analyse eines intelligenten bösartigen Codes sowie die Entwicklung einer Technologie zur Aufdeckung von temporären und zirkulierenden Seiten; die Entwicklung einer Technologie, um im Falle eines erfolgten DDos-Angriffs mittels einer schnellen Reaktion durch ein Tool zur Verweigerung der Verbreitung des angreifenden Codes den Schaden zu minimieren; sowie ein kombiniertes Sicherheitskontrollsystem, das eine effiziente Weiterleitung von Informationen über gewaltsame Eingriffe betreibt und das sich in Entwicklung befindet, um bereits im Vorhinein eine weitere Attacke in der Art des DDos-Angriffs zu verhindern.

Darüber hinaus intensiviert die KISA (*Korea Information Security Agency*) ihre Anstrengungen im Sinne einer Verbesserung der Sicherheit von verwundbaren Webseiten, um so bestehende Probleme auf dem Gebiet der Homepage-Sicherheit – etwa mit Blick auf Regierungsorganisationen – zu lösen. Zudem entwickelt sie Tools zur *Hacking*-Erkennung und stellt diese den genannten Organisationen kostenlos zur Verfügung.

Zum gegenwärtigen Zeitpunkt sind drei Arten von Programmen verfügbar, um Angriffe auf Webseiten zu verhindern bzw. diesen zu begegnen: eine Technologie zur Verhinderung von Angriffen auf Homepages (*castle*), eine Technologie zur Aufdeckung von Hackerstrategien gegenüber Homepages (*whistle*) sowie eine offene Web-Firewall (ModSecurity, WebKnight).

Übersetzung ins Deutsche: Dr. Benedikt M. Helfer

HERAUSGEBER UND AUTOREN

Professor Dr. Seong-Woo Ji
ist Professor an der rechtswissenschaftlichen Fakultät der Dankook-Universität, Jukjeon Campus, Korea.

Laura Johnson
studierte Geschichte an der Universität Leeds und forscht gegenwärtig am Department of War Studies des King's College London zur BBC.

Professor Dr. Rajat Kathuria
ist Professor für General Management, Economics and Strategy am International Management Institute in Neu Delhi, Indien.

Hans Günter Kellner
ist freier Journalist für Print und Funk, u.a. für den „Evangelischen Pressedienst" (epd) und Deutschlandfunk. Er lebt und arbeitet in Madrid.

Dr. Helmut Reifeld
ist Leiter der Stabstelle Grundsatzfragen in der Hauptabteilung Europäische und Internationale Zusammenarbeit der Konrad-Adenauer-Stiftung in Berlin.

Roman Sehling
ist Senior Program Officer bei der Konrad-Adenauer-Stiftung in Washington, wo er die Themengebiete der Außen- und Entwicklungspolitik betreut. Unter anderem ist er verantwortlich für den Blog „uspolitik.info". Er studierte Internationale Beziehungen an der School of Foreign Service der Georgetown University, dem Moscow State Institute of International Relations und Wirtschaftswissenschaften an der Denison University.

Dr. Mahesh Uppal
ist Berater und Telekommunikations-Analyst sowie Direktor von Com First (India) Ltd. in Neu Delhi, Indien. Nach der Erlangung des Ph.D. am India Institut of Technology in Kanpur erhielt er den MA in Communications Policy an der City University in London.

Michael Thielen
ist seit 2008 Generalsekretär der Konrad-Adenauer-Stiftung. Er studierte Politische Wissenschaften, Neuere Geschichte und Philosophie und war von 2006 bis 2008 Staatssekretär im Bundesministerium für Bildung und Forschung.

Tobias Wangermann
ist Koordinator Beratungsmanagement in der Hauptabteilung Politik und Beratung und leitet zur Zeit die Projektgruppe Digitale Kultur der Konrad-Adenauer-Stiftung in Berlin.

Dr. Bohdan Wyżnikiewicz
ist stellvertretender Vorsitzender des Danziger Instituts für Marktwirtschaftsforschung, von 1991 bis 1992 war er Vorsitzender des Hauptstatistikamtes (GUS). Er ist Autor von zahlreichen Berichten und wissenschaftlichen Aufsätzen, Publizist und Gastdozent an polnischen Hochschulen, unter anderem an der Universität Warschau und an der Universität Danzig. Experte in mehreren polnischen und ausländischen Think Tanks.

Aneta Zwolińska
ist Juristin, Doktorandin an der Fakultät für Recht und Verwaltung der Universität Warschau. Absolventin des Aufbaustudiengangs Internetrecht an der Fakultät für Management und Soziale Kommunikation im Institut des Rechts für Geistiges Eigentum an der Jagiellonen-Universität. Dozentin an der Fakultät für Gesundheitswesen der Medizinischen Universität in Łódź. Autorin von Texten aus dem Bereich Internetrecht.

ANSPRECHPARTNER IN DER KONRAD-ADENAUER-STIFTUNG

Tobias Wangermann
Koordinator Beratungsmanagement
Hauptabteilung Politik und Beratung
10907 Berlin
Telefon: +49(0)-30-2 69 96 33 80
E-Mail: tobias.wangermann@kas.de

Barthel Schölgens
Leiter Stabsstelle Medienpolitik
Rathausallee 12
53757 Sankt Augustin
Telefon: +49(0)-22 41-2 46 25 25
E-Mail: barthel.schoelgens@kas.de