

Kontroll- und Verwertungsinteressen vs. Gleichheit und Freiheit im Netz*

Warum die Digitalisierung die Eigentumsfrage stellt und diese die Freiheit von Kommunikation nicht außen vorlässt

Das Internet, 1969 entstanden aus der Vernetzung von zunächst vier Rechnern in US-Forschungseinrichtungen, hat in der kurzen Geschichte seines Bestands bereits mehrere Wandlungen durchlaufen: vom militärisch finanzierten nationalen Forschungsnetz in den USA der 1970er Jahre über das internationale Wissenschafts- und Grassroots-Netzwerk der 1980er Jahre zum globalen Ökonomie- und Gesellschaftsnetz der 1990er Jahre (Rilling 2004, 1449) – bis hin, sofern Anschluss besteht, zum weltweiten Leitmedium seit der Jahrtausendwende. Über die Jahre gleichgeblieben allerdings sind wesentliche seiner Grundvoraussetzungen. Sie bestehen in einer verteilten, zentrumslosen Struktur und einer paketvermittelten, nicht diskriminierenden Steuerung. Anders ausgedrückt: Das Netz besitzt weder einen einheitlich lokalisierbaren Eigentümer noch eine zentrale Leitung. Das sind in Verbund mit einer grundlegend offenen Systemarchitektur und der aktiven Partizipation der Nutzerinnen und Nutzer die Garanten seines fortbestehenden Erfolges und seiner ungebremsten Dynamik (Abbate 2000, 208, 217). Das sind zugleich die Grundlagen eines Systems der offenen Informationsbereitstellung, das in zunehmendem Maße auf den Widerstand von Kontroll- und Geschäftsinteressen stößt und weitreichenden Einschränkungen unterworfen werden soll.

Als ein probates Mittel dazu erweist sich die mediale Skandalisierung. Mit dieser wird das Abbild vom Netz als das eines Tummelplatzes der Unmoral, eines Horts der Perversion, des beständigen Tabubruchs, eines Abgrunds an Terrorismus und Verbrechen gezeichnet (Fischbach 2009b, 38). Forderungen nach Eindämmung von Sex, Kindesmissbrauch, Extremismus und Gewalt im Netz gehen einher mit solchen nach schärferen Sanktionen gegen *Diebstahl geistigen Eigentums*, Unterbindung der Teilnahme an staatlich nicht kanalisiertem Glücksspiel, Schließung des Zugangs zu digital gehandelten Produktplagiaten, patentgeschützten Medikamenten und vielem mehr. Die Agenda der aus politischen und ökonomischen Partialinteressen mittels Access-Blocking zu begegnenden Inhalte ist lang (exempl. BDWi 2010). Nicht fehlen darf im Kampf gegen die *digitale Unterwelt* auch der Hinweis auf den vermeintlich ubiquitär erforderlichen Ausbau staatlicher Sicherheits- und Kontrollbefugnisse, inklusive des Mantras nach anlassloser Vorratsspeicherung von Verbindungsdaten als Allzweckwaffe gegen jedwede Formen des tatsächlichen, aber auch des imaginierten Cybercrime. Die Beschwörung der *dunklen Seite* des Netzes dient in diesem Monolog der Ängste und Phobien als Instrument zur Durchsetzung von technischen wie juristischen Kontroll- und Eigentumstiteln.

Ausgiebig beschrieben, zumeist ohne empirisch verifizierte Grundlage, werden die aus vermeintlichen Freiheiten herrührenden Herausforderungen des Netzes, um sie für die Einhegung des Netzes nach je eige-

* Der Text steht unter der Creative Commons-Lizenz CC BY-SA 3.0.

nen Kontroll- und Verwertungsinteressen zu instrumentalisieren. Als maßgebende Akteure in einem sich „herausbildenden Internet-Kontrollregime“ (Fischbach 2009b, 39) erweisen sich die Vertreter der klassischen Medien- und Unterhaltungsindustrie (Musik, Print, Film und TV). In ihrer transnationalen, US-dominanten Form fordern sie, das Internet „von einem Basar der Diebe in einen sicheren, lichtdurchfluteten Marktplatz“ (AFTRA et al. 2010, 9) zu verwandeln. Das Netz soll als Medium zum Kaufen, Sehen und Hören – kurz: zum passiven Konsum von Information und Unterhaltung – ausgestaltet werden, nicht aber zur aktiven Teilhabe, zum Reden, Gehörtwerden und Teilen (Rilling 2004, 1448). Den Vorgaben der Unterhaltungs- und Medienindustrie folgend sollen die Internet-Zugangsanbieter gezwungen werden, die von ihnen übertragenen Inhalte in Echtzeit zu überwachen und nach mutmaßlich illegalen Nutzungsaktivitäten zu durchleuchten. Im Repressionskatalog enthalten sind Internetsperren gegen missliebige Angebote und Inhalte, nach Kommunikationsausschluss von Nutzerinnen und Nutzern im Falle wiederholter Rechtsverletzungen sowie nach Beseitigung verdächtiger Hinweise aus den Indizes von Suchmaschinen.

Delikt Kopie

Das von der Rechteindustrie zur Verhandlung gebrachte Delikt *Kopie* erweist sich bis in die Begrifflichkeiten und die Bewertung des Schadensausmaßes hinein als vermint. Verbreitete Terminologien wie Internetpiraterie und Raubkopie sind als „irreführend“ (Brodowski/Freiling 2011, 109) einzustufen, schließlich bezeichnet Raub die Wegnahme einer Sache unter Gewalt oder unter Bedrohung für Leib und Leben (§ 249 StGB), zählt entsprechend zu mittelschwerer und schwerster Kriminalität, ebenso wie Piraterie juristisch besehen für schwerste Gewaltkriminalität auf Hoher See steht. An einer Dekomposition solcher in den allgemeinen Sprachgebrauch eingegangenen Begriffssemantiken muss sich gleichwohl nicht versucht werden, zumal urheberrechtskritische Ökonomen umgekehrt dazu übergegangen sind, das Verhalten der Unterhaltungsindustrie als Raubrittertum zu brandmarken. Wie ehemals die „Raubritter“ (Grossmann/Kirsch 2012, 17) gegenüber Bauern und Städtern im Spätmittelalter erziele die Content-Industrie heute ein leistungsloses Einkommen in Form einer von Urhebern und Nutzern abgepressten Rente. Insbesondere die Künstler und Autoren, gleichsam von ihren industriellen Verwertern als „menschliche Schutzschilde“ (ebd.) eingesetzt, seien die Verlierer in einer Machtdisposition, die im vordigitalen Zeitalter erworben wurde und unter gänzlich anderen Produktionsbedingungen fortgeschrieben werden sollte. Tatsächlich, darin ist dem Befund generell zu folgen, haben die Kreativen im Regelfall ihre Urheberrechte an die Industrie abgetreten und erhalten – von wenigen Stars und Starlets abgesehen – im Gegenzug wenig bis nichts.

Ähnliches gilt für das Ausmaß der von der Content-Industrie reklamierten Schäden. Verlässliche oder gar statistisch robuste Zahlen über die Auswirkungen von Piraterie auf das wirtschaftliche Wachstum liegen nicht vor, lautet das Diktum des Berichts einer unabhängigen Kommission zum Zustand des Urheberrechts in Großbritannien (Hargreaves 2011a, 73). Der von der britischen Regierung unter David Cameron in Auftrag gegebene Prüfreport kommt unter Auswertung zahlreicher, auch internationaler Untersuchungen zum Ausmaß von Urheberrechtsverletzungen im Netz zu dem Ergebnis, diesen keine validen Angaben zur

Größenordnung und zu den Folgewirkungen illegaler Nutzungshandlungen entnehmen zu können – weder im Vereinigten Königreich noch weltweit. Ohne die Evidenz von illegalem Filesharing selbst zu negieren, verweist der Bericht auf erhebliche methodologische Mängel in nahezu all diesen Studien. Exemplarisch und in besonderem Maße gilt das für die sogenannte TERA-Studie, die am 17. März 2010 in Brüssel der Presse präsentiert und anschließend Mitgliedern des Europäischen Parlaments und der Europäischen Kommission vorgestellt wurde. Erstellt von einer Unternehmensberatung im Auftrag der von der Internationalen Handelskammer (ICC) betriebenen Anti-Piraterie-Lobbyinitiative Business Action to Stop Counterfeiting and Piracy (BASCAP), erschien sie zeitgleich in fünf Sprachen – Englisch, Französisch, Italienisch, Spanisch, Deutsch. Für die 27 Mitgliedstaaten der Europäischen Union (EU) wird darin für die Branchen Film, TV, Musik und Software ein auf Piraterie zurückzuführender Umsatzverlust von 10 Mrd. Euro sowie ein Beschäftigungsabbau von mehr als 185.000 Arbeitsplätzen in 2008 behauptet. Gleichzeitig werden bis 2015 kumulierte Umsatz- und Jobverluste in Höhe von 240 Mrd. Euro bzw. 1,2 Mio. Arbeitsplätzen vorhergesagt (TERA Consultants 2010, 6). Die adaptierte Untersuchungsmethode – zuvor bereits in mehreren ähnlichen Studien im Auftrag der US-amerikanischen Musik-, Film- und Software-Industrie zur Anwendung gelangt – berechnet Umsatzverluste, indem die Anzahl von Urheberrechtsverletzungen zum Ausgangsjahr auf Basis einer angenommenen Substitutionsrate entgangener Käufe zunächst in Volumenverluste, sodann durch Multiplikation zu Ladenstückpreisen in entgangene Umsätze und schließlich mit einem linearen Piraterieanstieg nach Maßgabe eines prognostizierten Wachstums des globalen Internet-Traffic zeitlich bis zum Prognosejahr 2015 fortgeschrieben wird. Beschäftigungsverluste ergeben sich, indem die entgangenen Umsätze durch die durchschnittlichen Umsatzerlöse pro Beschäftigten dividiert und sodann unter Berücksichtigung der Zulieferindustrie mit dem hypothetischen Faktor zwei multipliziert werden (ebd., 27–30, 59/60).

Ogleich die TERA-Studie medial breit rezipiert und insbesondere von den Unternehmens- und Arbeitgeberverbänden der europäischen Kreativwirtschaft nahezu einhellig als Negativausweis für Ausmaß und Folgewirkungen von Piraterie propagiert wurde, halten die dort präsentierten Zahlen nüchterner wissenschaftlicher Prüfung nicht stand. Die erwähnte Hargreaves-Kommission fällt geradeheraus ein vernichtendes Urteil (Hargreaves 2011b, 6–11). Sie sprach von „*sehr frustrierenden*“ Einlassungen, die politischen Entscheidungsträgern zur Bewertung des tatsächlichen Piraterieausmaßes vorgelegt werden. Weder seien die Anzahl der zugrundegelegten Urheberrechtsverstöße, die gewählten Substitutionsraten und weitere zahlenmäßige Angaben explizit verifizierbar, noch stimmten in mehreren Fällen die Berechnungen aufgrund der eigenen Zahlenangaben selbst. Allein für das Vereinigte Königreich ergäben sich auf Basis selbstgesetzter Zahlen weniger als die Hälfte der errechneten Verluste, auch könnten die kumulierten Hochrechnungen auf die Gesamtheit der EU-27 nicht nachvollzogen werden. Schon aus diesen Gründen disqualifiziert sich die TERA-Studie als eine Untersuchung zur interessengeleiteten Lenkung von Politik. Sie ist Ausfluss einer Lobby der transnationalen Unterhaltungsindustrie, deren Projekt in der Dienstbarmachung von Nationalstaaten zur Verankerung eines global sanktionierten Urheberrechtsregimes im Netz besteht.

Verankerung informationeller Eigentumsrechte

Das internationale Handelsabkommen Anti-Counterfeiting Trade Agreement (ACTA), über das Australien, Japan, Kanada, die Republik Korea, Mexiko, Marokko, Neuseeland, Singapur, die Schweiz, die USA sowie die EU und ihre 27 Mitgliedstaaten von Juni 2008 bis November 2010 unter striktem Ausschluss der Öffentlichkeit verhandelten, sollte dazu die Blaupause liefern. Ziel des Übereinkommens ist es, globale Standards für die Durchsetzung der Rechte am *geistigen Eigentum* und die effektive Bekämpfung des Handels mit gefälschten Waren und Raubkopien zu schaffen. Es war eine zunehmend postnational organisierte kritische Öffentlichkeit im Netz, die die Geheimverhandlungen durch das *Leaken* von zugespielten Verhandlungsdokumenten durchbrach und das ursprüngliche Vorhaben einer „Koalition multinationaler Unternehmen aus der Unterhaltungsindustrie, der Pharmaziebranche und der Luxusgüterindustrie“ (Mann 2010) vereitelte, Internet-Providern und Suchmaschinenbetreibern Kontroll- und Haftungsregeln für Verletzungen des *geistigen Eigentums* aufzuerlegen sowie eine Three-Strikes-Regelung gegen Urheberrechtsverletzer im Netz einzuführen. Mussten konkretisierende Handlungsanweisungen dazu im Verlauf der Verhandlungen aus dem Abkommen herausgenommen werden, so blieb doch die elementare Vorgabe mit Artikel 27 bestehen (ACTA 2010, 15–17), „wirksame“ Maßnahmen zur zivil- und strafrechtlichen Rechtsdurchsetzung vorzusehen und die Provider letztlich in die Rolle von Hilfssheriffs zur Ahndung von Urheberrechtsverletzungen zu drängen. Faktisch rückte mit einem Inkrafttreten von ACTA die Notwendigkeit zu einer grundlegenden Reform des Urheberrechts „in weite Ferne“ (Grossmann/Kirsch 2012, 17). Mit dem Übereinkommen würden die Bedingungen eines im Digitalzeitalter aus den Fugen geratenen Urheberrechts zementiert. Das war der Grund, weshalb im Januar und Februar 2012 europaweit Proteste gegen das umstrittene Abkommen aufflammten. In zahlreichen Demonstrationen und Kundgebungen artikulierte sich eine netzbasierte Öffentlichkeit, die den globalen Urheberrechtsvorgaben dieser Form des Konzernkapitalismus im digitalen Umfeld entgegentrat. Sie bewogen schließlich die EU-Kommission dazu, die Ratifizierung von ACTA bis auf weiteres auszusetzen und den Vertragstext dem Europäischen Gerichtshof zur Prüfung auf Vereinbarkeit mit den Europäischen Verträgen vorzulegen.

Informationelle Eigentumsrechte abzusichern gelang der Medien- und Unterhaltungsindustrie hingegen zuvor in Frankreich und Großbritannien. Dort kam es zur rechtlichen Verankerung von Systemen der *abgestuften Erwidern* (Graduated response). Nutzerinnen und Nutzer, die urheberrechtlich geschützte Inhalte über Peer-to-Peer-Netze, tendenziell auch über Sharehoster oder andere Online-Quellen herunterladen, erhalten demnach zunächst eine Verwarnung, die bei wiederholtem Zuwiderhandeln in eine strafrechtliche Verfolgung bis hin zur Sperrung des Internetanschlusses überführt werden kann. So trat in Frankreich zum 1. Januar 2010 das „Gesetz zur Verbreitung und zum Schutz kreativer Inhalte im Internet“ in Kraft, das nach der neugeschaffenen Aufsichtsbehörde Haute Autorité pour la diffusion des oeuvres et la protection des droits sur l'Internet (Hadopi) auch als Loi Hadopi bezeichnet wird. Ergänzt um ein weiteres Gesetz in 2010 (Hadopi II) und präzisiert durch zehn Dekrete (Schwartzmann 2012, 88), sieht ein Bündel von Maßnahmen die Ahndung von – realen, in der Praxis auch vermeintlichen – Urheberrechtsverletzungen in Form eines sogenannten Three-Strikes-

Verfahren vor. Das der generellen US-amerikanischen Justizpraxis zur instrumentellen Handhabung wiederholter Gesetzesverstöße entnommene Prinzip lautet: *Drei Urheberrechtsverstöße, und du bist raus*. Urheberrechtsverletzer werden den Bestimmungen zufolge zunächst zweimal verwahrt – zuerst per E-Mail, im Wiederholungsfall per Einschreiben – und sodann in einem vereinfachten Gerichtsverfahren zu Geldstrafen verurteilt oder mit einer bis zu einjährigen Sperrung des Internetzugangs belegt (Haber 2011, 306; Schwartmann 2012, 97–103).

In Großbritannien sieht der im April 2010 erlassene Digital Economy Act (DEA) ebenfalls ein System der *abgestuften Erwidern* vor. Bei entsprechenden Urheberrechtsverletzungen verschicken die Provider auf Basis von Benachrichtigungen durch die Rechteinhaber zunächst Warnhinweise. Zugleich überwacht die Medienaufsichtsbehörde Office of Communications (OFCOM) die Effektivität dieser Maßnahme. Sollte das Ausmaß an Internetpiraterie nicht abnehmen, kann sie technische Verpflichtungen anordnen, die von einer Drosselung der Zugangsgeschwindigkeit bis hin zu einer Sperrung des Netzzugangs reichen (DEA 2010, 13). Federführend beteiligt an den Gesetzesverschärfungen waren in beiden Ländern formelle und informelle Bündnisse aus Unterhaltungsindustrie und Kreativen. In Frankreich wurde die Einführung eines Systems der *abgestuften Erwidern* von der Unterhaltungsindustrie seit langem gefordert und durch eine Petition von 10.000 – in größerer Anzahl auch fiktiven – Kulturschaffenden unterstützt (Haber 2011, 305). In Großbritannien bildete sich eine Creative Coalition Campaign. Sie setzte sich aus verschiedenen Gewerkschafts- und Unternehmensverbänden der insbesondere unter der Blair-Administration maßgeblich geförderten britischen Creative Industries zusammen und wurde im August 2009 der Regierung als *Pressure Group* zur Bekämpfung von Copyright-Verletzungen im Netz zur Seite gestellt.

In den USA blieben Initiativen zur gesetzlichen Verankerung eines verschärften Urheberrechtsregimes im Netz bislang ohne Erfolg. Nachdem Ende 2010 der Combating Online Infringement and Counterfeits Act (COICA) im Senat scheiterte, liegen gegenwärtig mit der Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 (PROTECT IP) und der Stop Online Piracy Act (SOPA) zwei erneute Anläufe vor, Behörden und Rechteinhaber mit umfangreichen Mitteln im Kampf gegen Urheberrechtsverletzungen auszustatten. Passierten PROTECT IP oder SOPA beide Häuser des Kongresses und erlangten Gesetzeskraft, wären Netzsperrungen gegenüber den US-Behörden entzogenen Inhalten und Diensten auf Ebene des Domain Name System (DNS) sowie die Zensur von Suchmaschinenergebnissen die unmittelbare Folge (PROTECT IP 2011, 9, 11; SOPA 2011, 13–15). Im Falle von SOPA drohte zusätzlich die Kodifizierung einer *universellen* Zuständigkeit US-amerikanischer Gerichte zur Urheberrechtsdurchsetzung im Internet. Der im Text des Gesetzentwurfs enthaltene Begriff der *personal jurisdiction* (Bettinger 1998, 660; SOPA 2011, 8) erlaubte der US-Gerichtsbarkeit, eine personenbezogene Zuständigkeit zur Ingressnahme ausländischer Anbieter zu begründen, deren Webseiten von den USA aus abrufbar sind.

Angesichts der globalen Konnektivität des Netzes war mit diesen Bestrebungen unverhohlen ein staatlich induzierter Kontroll- und Zensurzugriff ausgesprochen. Entsprechend entfaltete sich gegen PROTECT

IP und SOPA im Januar 2012 eine beispiellose Protestwelle, die im Netz rasch weltweite Ausmaße annahm und in den USA selbst Befürworter der Gesetzesentwürfe vor ihren Ansinnen zurückschrecken ließ. Unabhängig davon allerdings wurde bereits im Juli 2011 hinter den Kulissen und von einer breiteren Öffentlichkeit unbemerkt ein privatwirtschaftliches Übereinkommen zwischen den einflußreichen Verbänden der Unterhaltungsindustrie Motion Picture Association of America (MPAA), Recording Industry Association of America (RIAA), Independent Film and Television Alliance (IFTA), American Association of Independent Music (A2IM) sowie namhaften Netzbetreibern, darunter AT&T, Verizon, Comcast, Cablevision sowie Time Warner Cable, getroffen. Dieses sieht ein System der *abgestuften Erwidern* in insgesamt sechs Schritten vor (CCI 2011, 7–14). Bei Abruf von inkriminierten Inhalten werden Nutzerinnen und Nutzer zunächst über Sicherheitsmaßnahmen ihres Netzanschlusses und legale Alternativen aufgeklärt. Im Wiederholungsfall ist ein Warnhinweis mit ausdrücklich zu bestätigender Einwilligung in den Abruf solcher Inhalte verbunden. Beide Schritte können von den Providern wiederholt werden. In einem letzten Schritt schließlich erfolgen die Drosselung der Verbindungsgeschwindigkeit auf Seiten des Anschlussinhabers oder die Sperrung von abgerufenen Internetdiensten.

Die Tendenz, die Zugangsanbieter zu einer zivilrechtlichen Regelung zu drängen, zeichnet sich auch in Deutschland ab. Hier fordern die Rechteinhaber – bestehend aus einer Phalanx von Allianz Deutscher Produzenten, Börsenverein des Deutschen Buchhandels, Bundesverband Musikindustrie, Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte (GEMA), Gesellschaft zur Verfolgung von Urheberrechtsverletzungen (GVU), Markenverband, Spitzenorganisation der Filmwirtschaft (SPIO), Verband Privater Rundfunk und Telemedien (VPRT), Verband der unabhängigen Musikunternehmen (VUT) in Einklang mit den deutschen Repräsentanten der transnationalen Medienindustrie Motion Picture Association (MPA), NBC Universal, Sky Deutschland (i.e. News Corporation) und Universal Music Entertainment – ein „sanktioniertes Aufklärungs- und Warnhinweismodell“ (Schwartzmann 2012, 25). Nach diesem sollen die Provider auf Grundlage von zuvor durch die Rechteinhaber ermittelten Internet-Protokoll-Adressen Warnhinweise verschicken. Nutzerinnen und Nutzer illegaler Downloads droht im Wiederholungsfall eine „ernstzunehmende Sanktion“ – auch technischer Art. Die geforderte *Inpflichtnahme* der Zugangsanbieter wird sich, und das scheint durchaus Kalkül hinter der Forderung, schon bald als nur ein erster Schritt in einem zu eröffnenden Reigen weiterer Maßnahmen zur Rechtsdurchsetzung erweisen. Schließlich könnten die Rechteinhaber, so sie denn wollten, schon heute Warnhinweise selbstständig verschicken, anstatt die von ihnen durch beauftragte Dritte ermittelten IP-Adressen für kostenpflichtige Abmahnschreiben nutzen zu lassen. Auch ist das Modell ausschließlich auf die Bekämpfung von Peer-to-Peer-Filesharing beschränkt. Dessen Anteil an der Gesamtheit aller Rechtsverletzungen liegt in Deutschland nach Berechnungen auf Basis von Zahlen der Rechteinhaber bei etwa 20 % (ebd. 198/199, 317). Nahe liegend aus Sicht und Interessenkonstellation der Rechteinhaber wäre es daher, eine umfassendere Lösung anzustreben und nachfolgend die Ausweitung in der Bekämpfung von Rechtsverletzungen im Internet auf die übrigen 80 % – beispielsweise die Nutzung der Angebote von Sharehostern oder Streaming-Diensten – einzufordern.

Das *sanktionierte Aufklärungs- und Warnhinweismodell* ist dem Umstand geschuldet, dass nach dem Scheitern des Zugangerschwerungsgesetzes (ZugErschwG) Internetsperren hierzulande gegenwärtig nicht durchsetzbar sind. Das Gesetz sah vor, den Zugriff auf kinderpornographischen Seiten im Internet mittels einer vom Bundeskriminalamt (BKA) zu führenden Sperrliste zu unterbinden. Es stieß in der politischen Öffentlichkeit des Netzes auf massiven Widerspruch. Letzterer fand Ausdruck in einer von 135.000 Menschen unterzeichneten Onlinepetition des Bundestags und begründete sich maßgeblich darin, dass Kinderpornographie durch Internetsperren nicht bekämpft, gleichsam aber eine Infrastruktur zur generellen Zensur im Internet errichtet würde (Meister 2011, 53). Tatsächlich sollte sich beides in einem gewissen Grade bestätigen: Technologisch wurde im Verlauf der Debatte einer breiteren Öffentlichkeit deutlich, dass jegliche Arten von Netzsperrern mit erheblichen, meist unvorhersehbaren Nebenwirkungen verbunden sind – insbesondere in Form des sogenannten *Overblocking*, der Beeinträchtigung von nicht von der primären Sperrmaßnahme intendierten Inhalten und Diensten (Pfitzmann/Köpsell/Kriegelstein 2008, 6, 73; Meister 2011, 18/19). In der kriminalpolizeilichen Zusammenarbeit schließlich erwies sich die vom Bundesinnenministerium in einer zur Nichtanwendung des Gesetzes erlassenen Anweisung an das BKA, die inkriminierten Inhalte zu löschen, anstatt zu sperren, als erfolgreich. Eine Evaluation der BKA-Zahlen für Januar 2011 ergab, dass in 97 von 143 Fällen (68 %) die kinderpornografischen Inhalte innerhalb einer Woche gelöscht waren. Nach zwei Wochen lag die Quote bereits bei 93 % und stieg nach drei Wochen auf 98 % sowie nach vier Wochen auf 99 %. Die Zahlen ließen erkennen, dass das Löschen von illegalen Inhalten, wie von den Kritikern des Gesetzes gefordert, auch international möglich ist (Ihlenfeld 2011).

Strategische Kontrollzugriffe

Grundlegender Ansatzpunkt aller Strategien zur Kontrolle des Internet bildet der Zugriff auf die physische Transportinfrastruktur (Goldsmith/Wu 2008, 73). Provider und Netzbetreiber sind als Gatekeeper und Intermediäre von Kommunikation vorrangiges Ziel staatlicher wie privater Bestrebungen zur Rechtsdurchsetzung. Zunehmend im Besitz der entsprechenden Steuerungstechnologien verfügen sie über ein Werkzeug, das es erlaubt, Datenpakete potentiell nach Inhalt, Quelle oder Ziel zu differenzieren, und eben auch, missliebige Datenverkehre zu unterbinden. Maßgebende Akteure der Medien- und Unterhaltungsindustrie suchen daher seit geraumer Zeit, das eigene Agenda-Setting in die Debatte um Netzneutralität hineinzutragen und in die Prozesse administrativer Entscheidungsfindung zu inkludieren. Bereits im März des Jahres 2010 hatte sich in den USA ein Bündnis aus Medienindustrie und neokorporatistisch agierenden Gewerkschaften mit einem weitreichenden Forderungskatalog an die US-Regierung gewandt. Darin enthalten war die Aufforderung, die Intermediäre im Kampf gegen Urheberrechtsverletzungen einzubinden und die Thematik in die von der Federal Communications Commission (FCC) geleiteten Verhandlungen zur Netzneutralität aufzunehmen (AFTRA et al. 2010, 9).

Das strategische Ziel der Unterhaltungsindustrie, über die Provider Rechtszugriff auf die Infrastruktur zu erlangen, wird ebenso in einer Verlautbarung des Verbands der US-Regisseure Directors Guild of America

(DGA), zugleich Mitglied dieses Bündnisses, benannt. Die Debatte um Netzneutralität, so heißt es dort in realistischer wie einliniger Einschätzung der Situation, werde letztendlich darüber geführt, „*wer das wertvollste und leistungsfähigste Transportsystem des 21. Jahrhunderts kontrolliert*“ (Keen 2009/2010, 26 [24]). Zur Überwachung des Netzes empfohlen wird der Einsatz der Technik der tiefen Paketinspektion (Keen 2010, 30 [20]). Auch UNI Europa, die europäische Sektion des internationalen Dachverbands der Gewerkschaften des Medien- und Unterhaltungssektors UNI-MEI, deren deutsches Mitglied die Dienstleistungsgewerkschaft ver.di ist, hat sich gegenüber der Europäischen Kommission für die Durchleuchtung jeglichen Netzverkehrs ausgesprochen. Laut gewerkschaftlicher Stellungnahme zum offenen Internet und zur Netzneutralität sollen zur Bekämpfung von Urheberrechtsverletzungen nicht nur die Technologien des Netzwerkmanagements zum Einsatz kommen, sondern auf deren Basis auch Nutzerinnen und Nutzer illegaler Angebote im Vorfeld auf die Rechtswidrigkeit des Abrufs hingewiesen werden sowie „*geeignete Schritte*“ für ein Access-Blocking solcher Inhalte ergriffen werden (UNI Europa 2010, 4).

Die Auswirkungen des Einsatzes von Netzwerktechnologien zur Rechtsdurchsetzung auf die Kommunikations- und Meinungsfreiheit allerdings sind bekannt. So ermöglicht es Deep Packet Inspection (DPI), sowohl den Header eines Datenpaketes auszulesen als auch das dazugehörige Datenfeld selbst (Bedner 2009, 6). Letzteres beinhaltet die eigentlichen Nutzinformationen. Verglichen mit der Beförderung eines Postbriefes werden beim Durchlaufen von (digitalen) Inspektionsstellen zusätzlich zu den Absender- und Empfängeradressen auf dem Umschlag (Header) ebenfalls der Inhalt des Briefes (Datenfeld) ausgewertet. Ein entsprechend ausgestatteter Router ermittelte also nicht nur, wohin das Datenpaket unterwegs ist, sondern ebenso, welche Art von Daten transportiert und welche Inhalte befördert werden. Im Falle der klassischen Briefpost käme das dem Öffnen und Sichten eines jeden Briefes gleich. Zwar bekunden Anbieter von DPI-Systemen, dass auf Basis der Technologie nur das gefunden werden könne, was auch gesucht werde, und dass die Kosten für ein tatsächliches Erfassen aller Datenpakete unverhältnismäßig seien, daher nur einige Pakete eines Datenstroms nach bestimmten Markern (Bit-Mustern) gerastert würden (Mochalski/Schulze 2009, 3).

Doch erweisen sich solche Einwände nicht nur vor dem Hintergrund einer beständigen Leistungssteigerung in der digitalen Datenverarbeitung als wenig stichhaltig. Schließlich muss, wie im Falle aller Filtertechnologien eine Indizierungsliste (Blacklist) mit vom Transport auszuschließenden Inhalten – hier in Form von Bit-Mustern – angelegt werden. Da Kontrollen auf Basis von Markern, zu letzteren zählen ebenso versteckt in Dateien eingebettete digitale Wasserzeichen, durch Manipulationen an Bildern und Textdokumenten relativ einfach zu umgehen sind – beispielsweise durch Kompression, Größen- und Farbänderungen von Bildern, der Schreibweise von Wörtern („Sehx‘ anstelle von ‚Sex‘“) oder der Verwendung von *Leetspeak* („|3OM|33‘ für ‚BOMBE‘“) in Texten (Pfitzmann/Köpsell/Kriegelstein 2008, 49, 61) –, käme es, neben der Entscheidung darüber, welche Inhalte generell zu indizieren wären, allein aus diesem Grund bereits zu einem raschen, letztlich unkontrollierbarem Anwachsen der Blacklist. Ferner wäre auch verschlüsselte Kommunikation vor DPI-Kontrollen nicht grundsätzlich gefeit (Bedner 2009, 11; Mochalski/Schulze 2009, 5). Statistische und verhaltensbasierte Er-

kennungsverfahren etwa ermöglichen es, die Anwendung und Existenz von Verschlüsselung aufzudecken, um anschließend den Weitertransport solcher Datenpakete zu unterbinden oder diese für Versuche der Entschlüsselung zu spiegeln.

Bereits diese wenigen Beispiele zeigen: Der Einstieg in die Überwachung der Inhalte des Netzverkehrs enthielte bereits die Bedingungen seiner Ausweitung. Bekannte und neu ersonnene Umgehungsformen stießen, sobald in größerem Maße zur Anwendung gebracht, auf stets weitreichendere Überwachungsforderungen. In einer Art Katz-und-Maus-Spiel träte eine technische Aufrüstungsspirale hin zu immer ausgefeilteren Überwachungstechnologien in Gang. Eine Konsequenz übrigens, die nicht technologieimmanent aufzulösen ist. Entgegen weit verbreiteter Meinung laufen Zensurmaßnahmen im Netz nicht aufgrund seines technischen Aufbaus ins Leere. Vielmehr ist es das Ausmaß an Technologie, dass die Effektivität von Zensur bestimmt. Grundlegend gilt: je größer der technische Kontrolleinsatz, desto besser das zu erzielende Überwachungsergebnis. Unabhängig von dem Befund, dass das Durchleuchten der Inhalte mittels DPI-Analyse in Deutschland einen Eingriff in das Fernmeldegeheimnis (Art. 10 GG) und das Recht auf informationelle Selbstbestimmung (Art. 2 GG i.V.m. Art. 1 GG) darstellte (Bedner 2009, 3), implizierte eine solche Überwachung des Datenverkehrs eine Zensur jeglicher Netzaktivitäten. Es entstünde eine Kultur der Kontrolle, des Ausschlusses von missliebiger Kommunikation nach Sicherheits- und Verwertungsinteressen, eine expandierende Auslegung zu schützender Ziele und eine gigantische Indizierungsliste. Eine verhandlungsbasierte oder vertragsrechtliche Ausgestaltung zur Rechtsdurchsetzung bedingte eine fortschreitende „Zensur ohne Zensurbehörde“ (Fischbach 2009a, 110), eine Regelung auf gesetzlicher Grundlage eine fortschreitende Zensur mittels eines vom Staat zu benennenden Zensors. Dass das letztgenannte Szenario den Bedingungen des digitalen Überwachungsstaates im Iran oder in China nahe käme, in denen DPI-Analysen des Netz-Traffics bereits heute erfolgen, bildete keineswegs eine im Kontext differierender gesellschaftlicher Normen und Verfassungen zu vernachlässigende Petitesse. Überwachungsinfrastrukturen folgen als technologische Kontrolleinrichtungen grundlegend eigenen Systemeigenschaften. Ihre Differenz zu den sie einsetzenden Gesellschaften, ob demokratisch oder autoritär, ist nachgelagerter Art.

Geschäftskonstellationen

In dem sich herausbildenden Internet-Kontrollregime stehen die Vertreter der klassischen Medien- und Unterhaltungsindustrie „in der ersten Reihe“ (Schiller 2007, 116). Sie sind nicht die einzigen Akteure. Auf die Konvergenz von informationellen Verwertungsinteressen und dem Drängen nach erweiterten Kontrollrechten durch nationalstaatliche Sicherheitseinrichtungen und Befürworter des digitalen Sicherheitsstaates wurde eingangs verwiesen. Darüber hinaus haben auch Netzbetreiber und Hersteller von Netztechnologien ein ökonomisches Interesse, Kontrollinteressen zu bedienen. Beispielsweise beliefert Router-Weltmarktführer Cisco nicht nur Chinas Zensurinfrastruktur mit seinen Standardprodukten, sondern sucht mit seiner Technik auch an einem verbesserten Renditestrom der Netzbetreiber teilzuhaben (Fischbach 2009a, 129–131). Zwar zeigten die Carrier in den 1990er Jahren – gleichsam in einer ersten Phase nach der Privatisierung der Telefon-

dienste in den meisten OECD-Staaten – „inhaltliche Zurückhaltung“ (Coy 1998, 141) und wahrten Neutralität gegenüber den transportierten Inhalten. Eine Disposition, die bei vielen den Blick darauf verstellte, dass die Telcos als Marktunternehmen gezwungen sind, Revenuen zu erzielen, und Investitionsentscheidungen keineswegs aus altruistischen Motiven treffen. Doch gehen die Konzerne mit der Marktreife und Marktdurchdringung von jüngeren Technologien des DPI-basierten Netzwerkmanagements nun dazu über, erweiterte Renditequellen zu erschließen. Künftig sollen Datenströme gegen Aufpreis auf der Grundlage einer Klassifizierung nach Herkunft, Anwendung und Inhalt priorisiert behandelt werden. Der diskriminierungsfreie Informationsfluss im Netz wäre aufgehoben. Ein Geflecht aus Vorzugsbehandlung und Bevormundung von Anwendungen, Diensten und Inhalten in Abhängigkeit von Geschäftsinteressen, Finanzkraft und Einkommen träte an seiner Stelle. Zugleich entstünden neue Interessenskonvergenzen: Die durch unterschiedliche Ausgangssituationen geprägten Geschäftskonstellationen von Netzbetreibern und Rechteverwertern näherten sich einander an.

Ähnliche Tendenzen zeichnen sich auf dem Feld des jüngsten Expansionspfads des Netzes ab. Marktführer Apple setzt bei Smartphones, Tablet-Computern und Apps für das mobile Internet auf proprietäre Lösungen – sprich: eigentumsrechtlich abgesicherte Hard- und Softwaretechnologien. Über den Zugang zu den Inhalten wacht der Konzern selbst. Die Regeln, wer welche Programme über den App Store und entsprechende Hardware verbreiten darf, sind strikt und nach den unternehmenseigenen Geschäftsbedingungen grundsätzlich variabel (Kurz/Rieger 2011, 106). Sie folgen in den Augen von Beobachtern wahlweise den rigiden Moralvorgaben des Konzerns oder aber den Verwertungsinteressen aus der engen Geschäftsverbindung von Apples langjährigem Vorstandsvorsitzenden mit Hollywoods Walt Disney Company. Nach dem Motto: *We sell, and you buy*, ist es zunehmend Ein-Weg-Kommunikation, die den Nutzerinnen und Nutzern hier begegnet. Digital eingezäunt darf vom Produkt nur kosten, wer Einlass erhält in die kapitalistisch eingehetzten Architekturen. Der Geschäftsstrategie eines *Walled Garden* folgt ebenso der Social Network-Riese Facebook. Information und Kommunikation werden in dessen „Universum“ innerhalb eines weitgehend geschlossenen Systems abgewickelt – mit dem kommoden Nebeneffekt, das „Online-Dasein“ außerhalb desselben tendenziell überflüssig zu machen (ebd., 94). Im Gegensatz dazu setzt Google demonstrativ auf die Offenheit des Netzes und auf offene Systemplattformen.

Das Geschäftsmodell des vielkritisierten, nach Markenwert – mittlerweile abgelöst durch Apple – einst mächtigsten Konzerns der Welt, der wie kein anderer die Idee des Netzes zu verkörpern scheint, kann im Kern als in Äquidistanz zu den Polen von Content und Transport stehend analysiert werden (Wu 2010, 283/284). Sein Erfolg basiert darauf, das Chaos im World Wide Web zu organisieren und für den Einzelnen nutzbar zu machen. Doch was sich lange als Vorteil bewährte, wird zunehmend zu Googles wunden Punkt. Der Verzicht auf den Betrieb von Transportinfrastruktur und die Produktion von Content macht den Konzern unter den Bedingungen eines verschärften Wettbewerbs mit kaum weniger mächtigen Akteuren angreifbar. Infrastruktur-, Urheberrechts- und Geräteindustrie bilden in einer fortgeschrittenen Informationsökonomie mit Monopolisierungstendenzen „*natürliche Verbündete*“ (ebd., 290). Ein

vertikales Konglomerat aus Hollywoods Inhalten, AT&Ts Netzen und Apples Maschinen setzte verlockende Aussichten auf erweiterte Revenuen frei und vollzöge im 21. Jahrhundert lediglich jene Prozesse von Konzentration und Zentralisation nach, die Film-, Radio- und Telefonindustrie jeweils für sich im Rahmen des ökonomischen Zyklus bereits im 20. Jahrhundert durchliefen (ebd., 296/297). Inwieweit Googles Einstieg in den Aufbau eines eigenen Glasfasernetzes, das Abkommen mit dem Netzbetreiber Verizon (beide 2010), die angekündigte Übernahme von Motorola Mobility sowie die Einführung des Facebook-Doubles Google+ (beide 2011) im Rahmen einer konkurrenzgetriebenen Entwicklung bereits das stillschweigende Eingeständnis beinhalten, die Offenheit des Netzes nicht auf Dauer behaupten zu können, verbleibt bis auf weiteres in der strategischen Verantwortung des Konzerns und zugleich nicht umstandslos abzuwarten.

Auch andernorts wird konzediert, dass sich der maßgebende Entwicklungspfad des Netzes im Rahmen des regulären ökonomischen Verwertungszyklus von einer freien, prinzipiell offenen Plattform hin zu einem geschlossenen, proprietären Medium vollzieht und mit ihm die „*Medienmogule alten Stils*“ (Anderson/Wolff 2010) in neuem Gewand zurückkehrten. Die fortschreitende Kommerzialisierung von digitaler Information und Kommunikation läßt die Trennung vormals gesonderter Mediengattungen und Branchen erodieren. In einem Prozeß sich herausbildender Konglomerate einer digitalen Kulturindustrie aus Content-Verwertern, Netzbetreibern, Technologie- und Diensteanbietern steht das Netz „*an der Schwelle zu einer weiteren institutionellen Metamorphose*“ (Schiller 2007, 144), seiner Entwicklung hin zu einem allgegenwärtigen Verkaufs- und Kontrollraum. Evident ist, dass die Kämpfe über Vorherrschaft und Kontrolle im Internet in einer Intensität zugenommen haben, die über das bislang Bekannte weit hinausreichen.

Die zunehmende Kolonisierung des Netzes durch Staat und Wirtschaft folgt den Grundsätzen technologiegetriebener Überwachungslogiken. Kommunikation und Information als ein Geschäft entwickeln sich zusammen mit ubiquitären staatlichen Sicherheitsinteressen zur „Bedrohung von Gleichheit und Freiheit im Netz“ (Fischbach 2009a, 131). Vor diesem Hintergrund bilden Eingriffe in die technologische Basis des Internet zugleich Eingriffe in die Grundlagen des Systems der offenen Informationsbereitstellung, somit in seine mediale wie globale Struktur. Eine technische Filterung der Inhalte nach je differierenden gesellschaftlichen oder nationalstaatlichen Normen und Gesetzen beschränkte den Zugriff des Netzes auf voneinander abgegrenzte Regionen. Die Folge wäre eine Reterritorialisierung des Internet als vormals globaler öffentlicher Raum. Schon wird vorhergesagt, es zerfiele entlang der Triade Nordamerika, Europa und China in drei separate geographische Kontrollregionen – inklusive solcher Staaten und Regionen, die sich einem dieser lediglich im Ausmaß ihrer Überwachungsintensität differierenden Modelle anschließen (Goldsmith/Wu 2008, 184).

Offenheit als Kontingenz

Tatsächlich muss die praktizierte und noch bestehende Offenheit des Netzes als „*kontingent*“ (ebd., 184) angesehen werden. Umgekehrt allerdings gilt das ebenso für seinen prognostizierten Zerfall in Territorien. Beide Szenarien verweisen in ihren grundlegenden Implikationen zurück auf zu führende politische Auseinandersetzungen. Denn folgendes ist zu

proklamieren: Obgleich die Offenheit des Netzes nicht als Wesensnotwendigkeit zu begründen ist, so bleibt sie doch politisch möglich. Darauf reflektiert in besonderer Dringlichkeit ebenfalls ein jüngerer Mahnruf von Tim Berners-Lee. Die konkreten Bedrohungen auflistend – Einzäunung und Abschottung von Informationen in Sozialen Netzwerken, Smartphones und Pads; Drosselung und Unterbindung des Zugangs zu rivalisierenden Diensten im mobilen Internet; fortschreitende Überwachungszugriffe auf die Informationsinfrastruktur durch autoritäre ebenso wie durch demokratische Regierungen –, konstatiert er: *„Sollten wir, die Nutzer des Netzes [im Orig.: Web], diese und andere Tendenzen weiterhin ungehindert an uns vorbeiziehen lassen, zerbricht das Netz in fragmentierte Inseln. Wir verlieren die Freiheit zur Vernetzung mit den Webseiten unserer Wahl.“* (Berners-Lee 2010) Auf die Frage, warum das die Nutzerinnen und Nutzer tangieren sollte, antwortet der Begründer des World Wide Web: *„Weil das Netz euch gehört. Es ist eine öffentliche Ressource, auf die ihr, eure Wirtschaft, euer Gemeinwesen und eure Regierung angewiesen seid. Das Netz ist ebenso unverzichtbar für die Demokratie – ein Kommunikationskanal, der ein kontinuierliches weltweites Gespräch ermöglicht.“* (ebd.) Bereinigt vom emphatischen Überhang und idealistischen Impetus verbleibt in Berners-Lees Aussagen der Hinweis auf das Netz als öffentliche Ressource, die implizite Aufforderung zur Revitalisierung und Zurückgewinnung des öffentlichen Raums Internet.

Nicht grundlos scheint an dieser Stelle die Eigentumsfrage auf. Netzförmige Infrastrukturen und immaterielle Informationen gelten der neoklassischen ökonomischen Theorie als öffentliche Güter (Kollektivgüter). Im Unterschied zu privaten Gütern, die als uneingeschränkt marktfähig bewertet werden, wird die Inanspruchnahme von Kollektivgütern nicht durch einen Knappheitspreis gesteuert. Mit Hilfe der Klassifikationskriterien Ausschließbarkeit vom Konsum und Rivalität im Konsum ist es in Fortschreibung dieses Ansatzes möglich, unterschiedliche Arten von Kollektivgütern zu unterscheiden und gegenüber privaten Gütern abzugrenzen (Hess/Ostrom 2007, 8/9). Während die Netzinfrastruktur ein *unreines* öffentliches Gut darstellt – sprich: das Ausschließen eines Nutzers vom Konsum ist nicht oder nur schwer möglich, gleichwohl wird der Nutzen des Gutes (zumindest ab einer kritischen Größe) durch weitere Nutzer eingeschränkt –, handelt es sich im Falle von digitalen Informationen um *reine* öffentliche Güter. Sie besitzen im Konsum die Prinzipien Nicht-Ausschließbarkeit und Nicht-Rivalität. In Differenz zum Konsum eines privaten Gutes, für das der Merksatz gilt: *Ein Apfel kann nur einmal gegessen werden*, werden zusätzliche Nutzer weder ausgeschlossen, noch wird der Konsum eines solchen Gutes durch weitere Konsumenten desselben Gutes beschränkt. Aus diesen Gründen betragen die Grenzkosten des Konsums reiner öffentlicher Güter ebenso wie deren Marktpreis Null (Boyle 2003, 42; Benkler 2006, 36). Kosten fallen lediglich für das Erstellen der ersten Kopie (First Copy) an. Im Falle unreiner öffentlicher Güter ist es ähnlich, hier sind die Grenzkosten niedrig, die Fixkosten zur Erstellung der Infrastruktur enorm. Markt- oder Wettbewerbsversagen ergibt sich zudem aus den Eigenschaften eines natürlichen Monopols. Das Verlegen paralleler Netze führte in der Regel dazu, dass die relevante Nachfragemenge zu volkswirtschaftlich höheren Kosten produziert würde.

Folglich können Märkte öffentliche Güter nicht effizient bereitstellen. Es bedarf daher einerseits einer Fülle von Regulierungsmaßnahmen, um für den privaten Betrieb von Netzinfrastrukturen wettbewerbliche Marktbedingungen zu schaffen (Fischbach 2009a, 126), andererseits Strategien des Ausschlusses vom Konsum (Kopplung an stoffliche Träger, Verschlüsselung) in Verbund mit der Errichtung ausschließlicher Nutzungsmöglichkeiten durch geistige Eigentumsrechte oder der Finanzierung auf Umwegen (Datenhandel, Werbung), um Informationsgüter marktfähig zu machen (Goldhammer 2006, 87, 102). In der Vergangenheit waren solche informationellen Verwertungsstrategien durchaus erfolgreich. In Form von – um nur einige zu nennen – Print-Medien, CDs, DVDs (Kopplung an stoffliche Träger), Pay-TV (Verschlüsselung) sowie Privat-TV (Werbung) gelang es der Medien- und Unterhaltungsindustrie, für sie praktikable Geschäftsmodelle zu etablieren. Unter den Bedingungen einer netzwerkbasieren Informationsökonomie allerdings stellt sich die Frage nach Geschäftsmodellen neu: Einerseits bestehen Verschlüsselung, Datenhandel und Werbung als Strategien zur Kommodifizierung reiner öffentlicher Güter fort, andererseits bereitet die Bindung von Informationen an das materielle Trägermedium fortgesetzte Schwierigkeiten. Proprietäre Hard- und Software, Clouds und andere *Walled Garden*-Geschäftsmodelle bilden hier den Pol zur Inwertsetzung auf der einen, der Zugriff bis hinein in die Kommunikationsprotokolle und die Ebene des Datentransports jenen auf der anderen.

Wissen–Information–Daten

Wie tiefgreifend der Kontrollzugriff aus der Perspektive gesellschaftlicher Organisation und Teilhabe tatsächlich ist, wird deutlich unter Betrachtung des zugrundeliegenden Systems in dem Verhältnis von Wissen, Information und Daten. In ihm bezeichnen Daten kodierte Informationen in Form roher Bits (Einsen und Nullen), Informationen die strukturierte Anordnung von Daten in einem Kontext sowie Wissen – verstanden als Ensemble aller intelligiblen Aktivitäten – die Aufnahme und das Verstehen von Informationen (Hess/Ostrom 2007, 8). Entsprechend gilt die Korrelation: „*Wissen entstammt Information, ebenso wie Information Daten entstammt.*“ (Davenport/Prusak 1998, 6) Aus der wechselseitigen Beziehung Wissen–Information–Daten resultiert im digitalen Umfeld unmittelbar zweierlei: Erstens erfolgt der Kontrollzugriff nicht allein zur Unterbindung der Zirkulation des noch letzten *freigesetzten* Werkes, sondern auch im Wettbewerb und Konkurrenzkampf um erweiterte Akkumulationsressourcen. Zu benennen sind Bestrebungen zur Patentierung von Datenanordnungen etwa im Falle von Gensequenzen oder des Schutzes in der Zusammenstellung von ausgestalteten Bit-Folgen zur Kontrolle noch kleinster, verwertbarer Informationseinheiten (Boyle 2003, 39). Zweitens ist der Kontrollzugriff auf der Ebene der Datenübertragung unabdingbar verbunden mit einem Eingriff in die Freiheit von Kommunikation selbst. Denn: „*Kommunikation ist der Austausch von Bedeutungsgehalten durch den Austausch von Informationen.*“ (Castells 2009, 54) Die Prozesse der Kommunikation werden entsprechend durch die Technologie der Kommunikation und ihrer Einbettung in den Kontext der sozialen Beziehungen definiert. Aus diesen Gründen können im digitalen Zeitalter die Protokolle der Kommunikation nicht länger zu den Prozessen kommunikativen Handelns ausgelagert begriffen werden (ebd., 126).

Die ausgreifende Landnahme auf dem Gebiet der Kommunikations- und künftigen Akkumulationsressource Wissen–Information–Daten wird von den Vertretern des aus dem kritischen Teil eines grundlegend offeneren US-Wissenschaftsmilieus entstammenden, in Europa weitgehend noch randständigen Diskurses über *Digital Commons* (Digitale Gemeingüter) als „zweite Einhegungsbewegung“ (Boyle 2003, 37) benannt. Nach der Einhegung und gewaltsamen Umwandlung von Gemeindeland in Privateigentum zu Beginn der industriellen Revolution erfolgt diesem Befund zufolge heute die „Einhegung der immateriellen Gemeingüter des Geistes“ (ebd.). Die Gemeingüter der Kommunikationsrevolution des Netzes werden zur erweiterten Profitgenerierung und zur Verwandlung persönlicher Freiheiten in Waren durch die Unterhaltungsindustrie angeeignet, die sozialen Subjekte gleichsam „expropriert“ (Castells 2009, 414), heißt es an anderer Stelle. Auch wird aus dieser Denkrichtung darauf verwiesen, dass es aus wohlfahrtsökonomischer Sicht effizienter wäre, digitale Informationen allen potenziellen Nutzerinnen und Nutzern unentgeltlich – oder allenfalls zu Kosten, die ihre Erstellung verursachen – zur Verfügung zu stellen (Benkler 2006, 37). Im Fokus des Commons-Diskurses stehen neue institutionelle Formen nicht-marktvermittelter Produktion und Distribution im digitalen Umfeld. Konträr zum Prozess der Privatisierung und Inwertsetzung von Gemeingütern werden das Recht auf Zugang, Nutzen und Teilen, die Bewahrung des Gemeinguts Wissen und der Erhalt des Gemeinguts Kommunikation proklamiert (Benkler 2006, 60; Hess/Ostrom 2007, 8; Castells 2009, 431).

Das Netz im Sinne einer *Public Domain* (Öffentliche Domäne) oder einer *Common-Pool Resource* (Gemeinressource) als handlungs- und nutzungsoffenen Raum zu gestalten, bedarf neuer institutioneller Formen gesellschaftlicher Teilhabe. Forschungsarbeiten zu Regulationsmodellen von Gemeinressourcen jenseits von Markt und Staat liegen vor, konkretisierende Überlegungen zur institutionellen Gestaltung des komplexen Systems Internet allerdings befinden sich noch in den Anfängen. Andere Gestaltungsoptionen jenseits von Überwachung und Inwertsetzung bestehen nicht. Eine Revitalisierung und Zurückgewinnung des Netzes als öffentlicher Raum kann angesichts eines globalen Informationsraums nicht über eine Wiederherstellung überlieferter Formen von Staatseigentum bewerkstelligt werden. Neue institutionelle Formen von nicht-marktvermittelter Produktion und Distribution bedürfen ferner neuer Vergütungsmodelle für Wissens-, Kultur- und Informationsproduzenten. Mit Konzepten wie der *Content-Flatrate* (Grassmuck 2008), auch unter den Bezeichnungen *Kulturflatrate* und *Tauschlizenz* bekannt, oder der *Kulturwertmark* (CCC 2011) liegen erste Vorschläge zu einer pauschalen Vergütung von Urheberinnen und Urhebern digitaler Werke vor. Trotz Unterschiede in Philosophie und Details: Gemeinsam ist ihnen, dass sie eine bessere Entlohnung von Kreativen sicherstellen und den Krieg gegen das Kopieren und das nicht-kommerzielle Filesharing beenden wollen. Es sind erste Hervorbringungen zur Ausgestaltung von sozialen Ökonomien im Digitalzeitalter, für dessen Gesellschaften gilt, dass die „Protokolle der Kommunikation nicht auf dem Teilen von Kultur, sondern auf der Kultur des Teilens“ beruhen (Castells 2009, 126).

Es sind zugleich Gestaltungsentwürfe in Form einer alternativen Eigentumspolitik. Diese steht konträr zu einem sich herausbildenden informationellen Akkumulationsregime des „digitalen Kapitalismus“ (Schiller 2007, 144), dessen Voraussetzungen auf der proprietären und verknäp-

penden Aneignung von Gemeingütern sowie deren Verrechtlichung durch die Schaffung informationeller Eigentumsrechte beruhen. Die Auseinandersetzungen um digitale Commons und die Kämpfe gegen die Überwachung des Netzes sind, ob bewusst oder nicht, folglich zugleich globale Gegenbewegungen zu einer Politik der Privatisierung im Rahmen des sogenannten *Washington Consensus* (Boyle 2003, 51; Castells 2009, 339). Mit ihm wird seit den 1990er Jahren die neoliberale Globalisierung des Konzernkapitalismus betrieben und mit ihm werden die kulturellen und informationellen Ressourcen im Prozess fortschreitender Digitalisierung zu gewichtigen Sektoren der Kapitalakkumulation. Daher stellt sich die Frage: Kann dieser Kampf um eine digitale Allmende gewonnen werden? Unsere Antwort lautet: Wir wissen es nicht! Gewiss scheint lediglich: „*Es ist die Aufgabe der Generation von heute, die Pfade der Erkenntnis offen zu halten.*“ (Hess/Ostrom 2007, 8) Und: Es wird keine leichte Aufgabe sein, den „*Machthabern der Netzwerkgesellschaft*“ aus Konzernkapitalismus und Staat in dem Bestreben „*zur Einhegung freier Kommunikation in kommerzialisierten und überwachten Netzwerken*“ (Castells 2009, 431/432) entgegenzutreten.

Literatur

Zitationen aus dem Englischen wurden im Text stillschweigend übersetzt und durch Kursivsetzung in Anführungszeichen kenntlich gemacht. Auf den technischen Unterschied zwischen Internet und World Wide Web wurde nicht näher Bezug genommen. Der synonym gebrauchte Begriff „Netz“ bezieht sich in Zweifelsfällen immer auf ersteres. Letztes Abrufdatum für Online-Dokumente in der nachfolgend benannten herangezogenen Literatur war 1. März 2012.

Abbate, Janet 2000: *Inventing the Internet*, Cambridge/Mass., London.

ACTA 2010: Anti-Counterfeiting Trade Agreement. Final ACTA text, December 3. URL: <http://trade.ec.europa.eu/doclib/html/147937.htm>.

AFTRA et al. 2010: Comments of Creative Community Organizations. American Federation of Television and Radio Artists (AFTRA), Directors Guild of America (DGA), International Alliance of Theatrical Stage Employees (IATSE), Motion Picture Association of America (MPAA), National Music Publishers' Association (NMPA), Recording Industry Association of America (RIAA), Screen Actors Guild (SAG) to the United States Intellectual Property Enforcement Coordinator (IPEC). In the Matter of Request for Submissions Regarding Development of a Federal Effort Against Intellectual Property Infringement, March 24. URL: <http://www.mpaa.org/Resources/0c72c549-89ce-4815-9a71-de13b8e0a26f.PDF>.

Anderson, Chris/Wolff, Michael 2010: *The Web Is Dead. Long Live the Internet*. Wired, August 17. URL: http://www.wired.com/magazine/2010/08/ff_webrip/all/1.

BDWi 2010: *Rechtsverstöße im Internet. Bedrohung für Kultur, Wirtschaft und Gesellschaft*. Bundesverband der Dienstleistungswirtschaft e. V. (BDWi), Berlin. URL: http://www.bundesverband-dienstleistungswirtschaft.de/fileadmin/user_upload/bdwi-internet-rechtsverstoesse.pdf.

Bedner, Mark 2009: *Rechtmäßigkeit der „Deep Packet Inspection“*. Projektgruppe verfassungsverträgliche Technikgestaltung (provet), Universität Kassel. URL: <http://kobra.bibliothek.uni-kassel.de/bitstream/urn:nbn:de:hebis:34-2009113031192/5/BednerDeepPacketInspection.pdf>.

- Benkler, Yochai 2006: The Wealth of Networks. How social production transforms markets and freedom, New Haven, London. URL: http://www.benkler.org/Benkler_Wealth_Of_Networks.pdf.
- Berners-Lee, Tim 2010: Long Live the Web: A Call for Continued Open Standards and Neutrality. Scientific American, November 22. URL: <http://www.scientificamerican.com/article.cfm?id=long-live-the-web>.
- Bettinger, Torsten 1998: Der lange Arm amerikanischer Gerichte: Personal Jurisdiction im Cyberspace. GRUR Int., Zeitschrift der Deutschen Vereinigung für Gewerblichen Rechtsschutz und Urheberrecht, S. 660–666. URL: http://www.bettinger.de/fileadmin/mediapool/downloads/Der_Lange_Arm.pdf.
- Boyle, James 2003: The Second Enclosure Movement and the Construction of the Public Domain. In: Law and Contemporary Problems, Vol. 66, Winter/Spring, S. 33–74. URL: <http://www.law.duke.edu/pd/papers/boyle.pdf>.
- Brodowski, Dominik/Freiling, Felix C. 2011: Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft. Forschungsforum Öffentliche Sicherheit, Schriftenreihe Sicherheit Nr. 4, Freie Universität Berlin, März. URL: http://www.sicherheit-forschung.de/schriftenreihe/sr_v_v/sr_4.pdf.
- Castells, Manuel 2009: Communication Power, New York. URL: <http://www.ufabcdigital.blog.br/wp-content/uploads/2012/02/Castells-Manuel-Communication-Power-2009.pdf>.
- CCC 2011: Kulturwertmark. Chaos Computer Club (CCC) schlägt neues Vergütungsmodell für Kreative vor, 26. April. URL: <http://ccc.de/system/uploads/65/original/kulturwertmark-neu.pdf>.
- CCI 2011: Memorandum of Understanding – Center for Copyright Information (CCI). Final, July 6. URL: http://www.copyrightinformation.org/sites/default/files/Momorandum_of_Understanding.pdf.
- Coy, Wolfgang 1998: Media Control – Wer kontrolliert das Internet? Vortrag an der Freien Universität Berlin im Rahmen der Ringvorlesung „Medien–Computer–Realität“ am 12.12.1996. In: Sybille Krämer (Hrsg.): Medien, Computer, Realität. Wirklichkeitsvorstellungen und Neue Medien, Frankfurt a. M., S. 133–151. URL: http://waste.informatik.hu-berlin.de/coy/Media_Control_4_97.html.
- Davenport, Thomas H./Prusak, Laurence 1998: Working Knowledge: How Organizations manage what they Know, Boston/Mass.
- DEA 2010: Digital Economy Act 2010. c. 24, April 8. URL: http://www.legislation.gov.uk/ukpga/2010/24/pdfs/ukpga_20100024_en.pdf.
- Fischbach, Rainer 2009a: Zensur, technische Kontrolle und Verwertungsinteressen. In: Lothar Bisky, Konstanze Kriese, Jürgen Scheele (Hrsg.): Medien – Macht – Demokratie. Neue Perspektiven, Berlin, S. 109–133. URL: http://www.rosaluxemburgstiftung.de/fileadmin/rls_uploads/pdfs/Texte-54.pdf.
- Fischbach, Rainer 2009b: Das Internet als Nischenmedium und Kontrollraum – Versteck der Perversion, Bühne der Provokation oder Benthamsches Panoptikum? In: Klaus-Dieter Felsmann (Hrsg.): Mediale Tabubrüche vs. political correctness. Erweiterte Dokumentation zu den 12. Buckower Mediengesprächen 2008, München, S. 35–41.
- Goldhammer, Klaus 2006: Wissensgesellschaft und Informationsgüter aus ökonomischer Sicht. In: Jeanette Hofmann (Hrsg.): Wissen und Eigentum. Geschichte, Recht und Ökonomie stoffloser Güter, Bonn, S. 81–106. URL: <http://www.bpb.de/files/MJPQ2J.pdf>.
- Goldsmith, Jack/Wu, Tim 2008: Who Controls the Internet? Illusions of a Borderless World. With a new Preface, New York, Oxford.
- Grassmuck, Volker 2008: Nutzungsfreiheit, Datenschutz und Urhebervergütung: die Content-Flatrate. eco Kongress, 11. September. URL: http://waste.informatik.hu-berlin.de/grassmuck/Texts/08-09-11_ECO_Filtering.pdf.
- Grossmann, Volker/Kirsch, Guy 2012: Acta oder der Schutz der Raubritter. Frankfurter Allgemeine Zeitung für Deutschland, 23. Februar, S. 17. URL: <http://www.faz.net/aktuell/wirtschaft/urheberrechte-im-internet-acta-oder-der-schutz-der-raubritter-11658717.html>.

- Haber, Eldar 2011: The French Revolution 2.0: Copyright and the Three Strikes Policy. In: Journal of Sports & Entertainment Law, Vol. 2, No. 2, Spring, Harvard Law School, S. 297–339. URL: <http://harvardjsel.com/wp-content/uploads/2011/06/Haber.pdf>.
- Hargreaves, Ian 2011a: Digital Opportunity. A Review of Intellectual Property and Growth, May. URL: <http://www.ipo.gov.uk/ipreview-finalreport.pdf>.
- Hargreaves, Ian 2011b: Digital Opportunity. A Review of Intellectual Property and Growth. Supporting Document CC. Data on the Prevalence and Impact of Piracy and Counterfeiting. URL: <http://www.ipo.gov.uk/ipreview-doc-cc.pdf>.
- Hess, Charlotte/Ostrom, Elinor 2007: Introduction: An Overview of the Knowledge Commons. In: Charlotte Hess, Elinor Ostrom (eds.): Understanding Knowledge as a Commons: From Theory to Practice, London, S. 3–26. URL: <http://mitpress.mit.edu/books/chapters/0262083574intro1.pdf>.
- Ihlenfeld, Jens 2011: Kinderpornografie: Löschen statt Sperren funktioniert laut BKA-Zahlen. Golem.de, 18. März. URL: <http://www.golem.de/1103/82182.html>.
- Keen, Andrew 2009/2010: What Price Internet? DGA Quarterly, Winter, S. 24–27, 76–77. In: Internet Theft. A Collection of Nine Articles from the DGA Quarterly on Issues of Digital Piracy, [S. 22–27]. URL: <http://www.directorsguild.org/internet-theft/DGA-Piracy-Articles.pdf>.
- Keen, Andrew 2010: Keeping the Internet Safe. DGA Quarterly, Spring, S. 28–30. In: Internet Theft. A Collection of Nine Articles from the DGA Quarterly on Issues of Digital Piracy, [S. 18–20]. URL: <http://www.directorsguild.org/internet-theft/DGA-Piracy-Articles.pdf>.
- Kurz, Constanze/Rieger, Frank 2011: Die Datenfresser. Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen, Frankfurt a. M.
- Mann, Erika 2010: Ein Trauerspiel namens ACTA. Die Zeit, 31. März. URL: <http://www.zeit.de/digital/internet/2010-03/acta-europa-fail/komplettansicht>.
- Meister, Andre 2011: Zugangerschwerungsgesetz. Eine Policy-Analyse zum Access-Blocking in Deutschland. Arbeit zur Erlangung des Akademischen Grades Master of Arts, Humboldt-Universität Berlin, 20. April. URL: <http://netzpolitik.org/wp-upload/Master-Meister-Zugangerschwerungsgesetz.pdf>.
- Mochalski, Klaus/Schulze, Hendrik 2009: Deep Packet Inspection. Technology, Applications & Net Neutrality. Ipoque White Paper. URL: <http://www.ipoque.com/sites/default/files/mediafiles/documents/white-paper-deep-packet-inspection.pdf>.
- Pfitzmann, Andreas/Köpsell, Stefan/Kriegelstein, Thomas 2008: Sperrverfügungen gegen Access-Provider – Technisches Gutachten, Technische Universität Dresden. URL: http://www.kjm-online.de/files/pdf1/Gutachten_Sperrverfuegung_Technik_2008.pdf.
- PROTECT IP 2011: Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011. S. 968. 112th Congress, 1st Session, May 26. URL: <http://www.gpo.gov/fdsys/pkg/BILLS-112s968is/pdf/BILLS-112s968is.pdf>.
- Rilling, Rainer 2004: Internet. In: Wolfgang Fritz Haug (Hrsg.): Historisch-kritisches Wörterbuch des Marxismus. Band 6/II: Imperium bis Justiz, Hamburg 2004, S. 1445–1459. URL: <http://www.rainer-rilling.de/texte/inkrit-internet.html>.
- Schiller, Dan 2007: How to Think about Information, Urbana, Chicago.
- Schiller, Dan 2009: Der Informationskrieg. In: Lothar Bisky, Konstanze Kriese, Jürgen Scheele (Hrsg.): Medien – Macht – Demokratie. Neue Perspektiven, Berlin, S. 228–241. URL: http://www.rosaluxemburgstiftung.de/fileadmin/rls_uploads/pdfs/Texte-54.pdf.
- Schwartzmann, Rolf 2012: Vergleichende Studie über Modelle zur Versendung von Warnhinweisen durch Internet-Zugangsanbieter an Nutzer bei Urheberrechtsverletzungen. Im Auftrag des Bundesministeriums für Wirtschaft und Technologie. Unter Mitwirkung von Caspar Bunke, Marie-Anne Buron, Izabela Dumistracel, Klaus Gennen, Laureline Kergueris, Nicola Lamprecht-Weißborn, Gila Polzin, Petra Silberkuhl, Januar. URL:

<http://bmwi.de/BMWi/Redaktion/PDF/Publikationen/Technologie-und-Innovation/warnhinweise-lang,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf>.

SOPA 2011: Stop Online Piracy Act. H. R. 3261. 112th Congress, 1st Session, October 26. URL: <http://www.gpo.gov/fdsys/pkg/BILLS-112hr3261ih/pdf/BILLS-112hr3261ih.pdf>.

TERA Consultants 2010: Aufbau einer digitalen Wirtschaft: Die Bedeutung der Sicherung von Arbeitsplätzen in der Kreativwirtschaft der Europäischen Union, 3. März. URL: <http://www.iccwbo.org/uploadedFiles/BASCAP/Pages/Aufbau%20einer%20digitalen%20Wirtschaft.pdf>.

UNI Europa 2010: Response to the Public Consultation on the Open Internet and Net Neutrality in Europe, Brussels, September 29. URL: http://ec.europa.eu/information_society/policy/ecom/doc/library/public_consult/net_neutrality/comments/08industry_social_consumer_orgs_etc/uni.pdf.

Wu, Tim 2010: The Master Switch. The Rise and Fall of Information Empires, New York.