# 4. Überwachung und Kontrolle

Im Folgenden möchte ich darstellen, wie Überwachung prinzipiell gesellschaftlich wirksam werden kann und wie sie funktioniert. Dabei beziehe ich mich vor allem auf Foucaults Adaption des Benthamschen Panoptismus. Zentrale These dabei ist, dass eine lückenlose Überwachung nicht notwendig ist, um den gewünschten Kontroll- und Disziplinierungseffekt zu erzielen.

In Bezug auf das Internet soll dann dargestellt werden, welche Mittel der Überwachung und Kontrolle existieren, aus welchen Motiven sie eingesetzt werden und welche Effekte einerseits und Gegenbewegungen andererseits sie zeitigen. In diesem Rahmen werde ich auch wieder verstärkt auf technische Hintergründe eingehen, da sich in dem Gegensatz von Öffentlichkeit und Privatheit, von Überwachung und ihrer Vereitelung technische Lösungen und gesellschaftliche Effekte ständig überschneiden und wechselseitig bedingen: die sozialen Tatbestände der Privatheit oder Öffentlichkeit und ihre Herstellung bzw. ihre Einschränkung werden direkt durch technische Mittel bestimmt.

Sowohl Foucault als auch Bentham gingen von der materiellen Welt aus, in der das panoptische Prinzip wirksam würde. Hier soll trotz der allgegenwärtigen Ausweitung panoptischer Mechanismen auch in der materiellen Welt (Videoüberwachung, Biometrie, Personenerkennungssysteme anhand von Gesichtsaufnahmen, Stimme, Gehweise etc.) ausschließlich auf den Panoptismus im Internet eingegangen werden. Jenes wird in diesem Zusammenhang als Sozialraum betrachtet, dessen Nutzung selbstverständlich bis notwendig ist oder werden wird.

## 4.1. Das Panopticon

Ein zentrales Element der Foucaultschen Analyse von Macht und Kontrolle ist das Panopticon. 1791 von Bentham vorgestellt, ist es die architektonische Umsetzung der vollständigen Überwachung bei gleichzeitigem Unwissen der Überwachten darum, ob sie augenblicklich überwacht werden einerseits und der Gewissheit, dass eine solche Überwachung im Augenblick stattfinden könnte andererseits. Benthams ursprünglicher Entwurf sah eine ringförmige Gebäudeanlage mit nebeneinander angeordneten Zellen vor, die vom Ringzentrum aus einsehbar waren. In Zentrum des Rings wiederum befand sich ein zentraler Turm, in welchem sich der oder die Aufseher befanden. Mittels eines Systems von geschickt positionierten Lichtquellen, Spiegeln und Jalousien konnte erreicht werden, dass einerseits die Person im Zentralturm jede Zelle vollständig einsehen und überwachen konn-

te, es dem Häftling jedoch nicht möglich war zu erkennen, ob er gerade beobachtet wird oder ob überhaupt im Moment ein Aufseher anwesend ist.

> „Das Panopticon ist eine Maschine zur Scheidung des Paares Sehen/Gesehenwerden: im Außenring wird man vollständig gesehen, ohne jemals zu sehen, im Zentralturm sieht man alles, ohne je gesehen zu werden.“[223]

Es werden gleichermaßen Strukturen von Macht und Kontrolle entpersonalisiert, sie sind in der Art des Gebäudes mitangelegt und finden bereits ohne direkte menschliche Tätigkeit statt - ein Aufseher muss nicht einmal anwesend sein, damit das Prinzip funktioniert.

### 4.1.1. Das Panopticon bei Foucault

Das Panopticon ist somit ein Idealtypus der von Foucault postulierten ‚Disziplinargesellschaft’, die in der Neuzeit immer subtiler, aber auch immer allumfassender und totaler wirkt. Dementsprechend sieht er das Panopticon als Methode nicht nur für die Gefängnisse, die Fabriken oder die Klöster voraus, sondern postuliert eine Adaption des panoptischen Prinzips auf sämtliche Gesellschaftsbereiche:

> „Das Panopticon liefert die Formel für diese Verallgemeinerung. Es programmiert auf der Ebene eines einfachen und leicht zu übertragenden Mechanismus das elementare Funktionieren einer von Disziplinarmaßnahmen völlig durchsetzten Gesellschaft.“[224]

Selbst das Opfer des Panoptismus wird zum Akteur in dieser Machtstruktur, die er mitträgt und durch die er seine Unterwerfung und Disziplinierung internalisiert:

> „Derjenige, welcher der Sichtbarkeit unterworfen ist und dies weiß, übernimmt die Zwangsmittel der Macht und spielt sie gegen sich selber aus; er internalisiert das Machtverhältnis in welchem er gleichzeitig beide Rollen spielt, er wird zum Prinzip seiner eigenen Unterwerfung.“[225]

Nun wurde Foucault der Vorwurf gemacht, nicht nur zu ignorieren, dass niemals tatsächlich ein Panopticon gebaut wurde, sondern diese nichtexistente Reinform ohne weitere Bedenken auf die gesamte Gesellschaft zu übertragen.

> „Von der Peripherie, wo alle ‘totalen Institutionen’ entstehen, rückt der ‘Panoptismus’, verallgemeinert und verwissenschaftlicht, in das Zentrum der Gesellschaft vor. Foucaults Fazit: Die Gefängnistore könnten eigentlich geöffnet werden, weil die ‘Dis-

[223] Foucault, 1995, S. 259
[224] ebd. S. 268
[225] ebd. S. 260

> ziplinargesellschaft' selber zum allumfassenden Gefängnis geworden ist. Wann und wie sich die Disziplinierungsmächte des Gefängnisses, der Klinik, des Militärs, der Fabrik zur Eroberung der Gesellschaft vereinigen können, bleibt historisch ebenso ungeklärt wie der Übergang der Ausnahmedisziplin in ‚totalen Institutionen' zur Veralltäglichung und Verbetrieblichung der generalisierten Disziplin."[226]

Nun geht Foucault nicht von einer an Weber orientierten Begrifflichkeit von Macht als Verhältnis zwischen einem machtausübenden Subjekt und dem Objekt der Machtausübung aus, welches gegebenenfalls auch gegen seinen Willen und seine Interessen durch das machtausübende Subjekt zu Handlungen gezwungen wird. Ebenso wenig wird ihre Reduktion auf ‚Unterdrückung' ihrem Wesen gerecht. Vielmehr ist Macht immer ein Kräfteverhältnis, in Abgrenzung zu der ‚greifbaren', Subjekten eindeutig zuordenbaren Macht Webers, die in dieser reinen Form laut Foucault nicht existiere, da sie „nicht gegeben wird, [...] weder getauscht noch zurückgenommen wird, sondern [...] ausgeübt wird und nur in actu existiert."[227] Macht mündet in ein Kräfteverhältnis ein, welches ständig ‚ausgetragen' wird und sich im Handeln in der Gesellschaft permanent reproduziert. Wehler fasst dies zusammen, indem er von Gesellschaft als „einem 'Geflecht aus Machtbeziehungen'" spricht: „Es gibt kein dominantes politisches, ökonomisches, ideologisches Zentrum mehr. Macht strahlt polyzentrisch von vielfältigen Konstellationen und Beziehungen aus."[228]

Dem panoptischen Prinzip folgend, ist die Gesellschaft somit durchdrungen von vielfältigen Strukturen der Machtausübung, in denen der Einzelne von verschiedensten Machtstrukturen in seinem Verhalten kontrolliert und diszipliniert wird, ohne jedoch konkrete Akteure seiner Disziplinierung ausmachen zu können. So ist das Panopticon der Idealtypus, die Reinform einer entpersonalisierten Macht, die in der Gesellschaft, in den Beziehungen ihrer Akteure untereinander, wirksam ist und deren konkrete Gestalter aus der Sichtbarkeit verschwinden. Wie in der architektonischen Lösung Benthams macht es in der gesellschaftlichen Umsetzung des Prinzips der Disziplinargesellschaft keinen Unterschied mehr, ob der - reale oder imaginierte – Kontrolleur noch anwesend ist, denn seine Machtausübung und seine gesamtgesellschaftliche Kontrollfunktion ist in den Strukturen der Gesellschaft und den prinzipiell denkbaren ‚Sichtbarkeiten' mit angelegt.

[226] Wehler, 1998, S. 53
[227] Foucault, 1978, S. 70
[228] Wehler, a.a.O., S. 65

### 4.1.2. Panoptismus in der Gesellschaft

Gesellschaftlich wirksam werden panoptische Strukturen auf zweierlei Weise. Einmal dadurch, dass im Alltagsleben die Überwachung jedes einzelnen ständig als möglich und potentiell sanktionierbar erscheint. Dieses Prinzip ist in jeder Gesellschaft dadurch schon gegeben, dass sich alle ihre Angehörigen Regeln und Normen unterwerfen, Einigkeit über gesellschaftlich akzeptierte Verhaltensweisen besteht etc. Die reine Anwesenheit anderer Personen führt direkt dazu, dass das individuelle Verhalten der Beobachtbarkeit und der damit impliziten Kritisier- und Sanktionierbarkeit angepasst wird.

Die Ausweitung dieses Prinzips, durch Videoüberwachung, Biometrie, der Kontrolle des Aufenthaltsorts am Arbeitsplatz, die mögliche Peilung über GMS - Handys etc. sind nicht Thema dieser Arbeit, es soll nur darauf hingewiesen werden, dass parallel zu den beschriebenen Möglichkeiten im virtuellen Raum auch eine Ausweitung panoptischer Strukturen in nichtvirtuellen Umgebungen stattfindet, die erste und elementarere Möglichkeit panoptischer Strukturen ebenfalls erweitert wird und es augenblicklich kein Gegengewicht zu den entsprechenden Trends in der Virtualität gibt, das den Privatheitsverlust in der virtuellen Welt möglicherweise ausgleichen oder relativieren könnte.

Die zweite Möglichkeit der Ausweitung panoptischer Strukturen ist die Etablierung neuer Kommunikationsstrukturen, welche einfacher als die bestehenden Sozialräume einer Überwachung unterworfen werden können. Eine Kontrolle des physischen Sozialraums stößt auf bestimmte Grenzen, wenngleich sie auch unbestreitbar stattfindet und ausgeweitet wird. In virtuellen Sozialräumen fällt diese physikalisch-materiell bedingte Schwelle weg, prinzipiell ist technisch das komplette Überwachen von virtuellen Sozialräumen möglich (und findet üblicherweise statt, nur werden die entstehenden Daten gewöhnlich kurz- bis mittelfristig gelöscht, werden nicht, nur auf Antrag[229] oder nur stichprobenartig ausgewertet und nicht mit anderen Datenquellen verknüpft). Weiterhin gibt es mit der Auskunftspflicht der Provider einerseits und der Möglichkeit der Verknüpfung von Surfprofilen mit Kundendaten beispielsweise bei Online - Shops andererseits neu entstehende Strukturen, die Kommunikationen aus der Anonymität herausheben. Während weiterhin das Verwenden biometrischer Systeme in der Öffentlichkeit gewöhnlich demokratisch legitimierten Institutionen vorbehalten bleibt, fallen Beschränkungen dieser Art im Netz weitgehend weg.

Die Durchsetzung des Panopticon als gesellschaftsstrukturierendes Prinzip scheiterte bisher an seiner Totalität, die seinen flächendeckenden Einsatz unmöglich machten. Das

[229] Ich erhielt bei einer Selbstmordankündigung auf einer von mir betreute Internetpräsenz binnen weniger Stunden Rückmeldung des betreffenden Zugangsproviders, den ich aus den Logdateien rekonstruiert hatte, die entsprechende Person sei inzwischen bekannt und wohlauf.

Panopticon funktioniert nur dann als Mittel zur Disziplinierung einer gesamten Gesellschaft, wenn sich der größte Teil - und nicht, wie bei Foucault meist angenommen, die devianten peripheren Gruppen - der Kontrolle durch panoptische Strukturen nicht entziehen kann. Niemand darf die Einbahnstraße durchbrechen. Aber es ist physikalisch nicht möglich, eine derart totale architektonische Struktur der Kontrolle zu einer Matrix zu machen, in der das physische Leben des größten Teils der Bevölkerung stattfindet, auch wenn die Möglichkeiten ständig anwachsen. Die Totalität wird nicht erreicht, der Aufwand einer kompletten Überwachung bleibt zu hoch. So ist es bisher schlicht unpraktikabel (und auch nicht unbedingt sinnvoll), ständig beispielsweise die Position eines Handys zu erfassen und zu protokollieren, vor allem, wenn man bedenkt, dass dieses ausgeschaltet werden kann etc.

Dies wird mit den Überwachungsformen, die das Netz bietet, anders. Im Panopticon der Benthamschen Vorstellung konnte aus der physisch - räumlichen Lage des Individuums die Möglichkeit der Überwachung direkt abgeleitet werden: es lokalisiert sich in einer dafür prädestinierten architektonischen Umgebung. Im Internet wird die Annahme einer solchen, Überwachung ermöglichenden Struktur in der Kommunikation mittels digitaler Medien weitaus abstrahierter und versteckter umgesetzt, und wirkt damit auch durchaus begünstigend auf das Entstehen einer paranoide Grundhaltung ein, die das Prinzip des Panoptismus primär erst wirksam werden lassen - man weiß nicht sicher, ob eine Überwachung stattfindet, oder möglich ist, (oder zwar möglich sei, jedoch aktuell nicht durchgeführt wird) und neigt dazu, vorsichtshalber vom Schlimmsten auszugehen. Diese Unsicherheit über Ausmaße und Möglichkeiten macht Bedenken dieser Form für nicht ausgewiesene Experten weiterhin schwerer thematisierbar. Indem Überwachungsprozesse in ihrer Potentialität für den einzelnen nicht mehr in der Wahrscheinlichkeit einschätzbar sind, setzt sich genau das Prinzip durch, das Foucault als maßgeblich für die Disziplinierung betrachtet: das Wissen über eine mögliche Kontrolle und das Unwissen über das tatsächlich stattfindende Ausmaß.

Mehr noch als bei Benthams panoptischen Strukturen, in denen ein Aufseher einige hundert Häftlinge, Arbeiter etc. beobachtete und einen dementsprechend kurzen Anteil an Aufmerksamkeit für den einzelnen aufbringen konnte, wird in der potentiellen Überwachbarkeit und Protokollierbarkeit des Netzes diese zu einer irreal erscheinenden Konstruktion, die aber öffentlich nie vollkommen belegbar oder widerlegbar werden kann. Die historische Wurzel des Panoptismus, der immer auf zumindest potentiell totalitären Institutionen beruhte, wird mit dem Internet zum ersten Mal auf ein Medium oder eine gesellschaftliche Kommunikationssphäre abgebildet, dass die Kategorie der Devianz der überwachten Individuen transzendiert; die prinzipiell jeden mit einschließt, der willens ist, das neue (und notwendige) Medium zu nutzen. So spricht Foucault vom

> „...Übergang vom Modell der Ausnahmedisziplin zu dem der verallgemeinerten Überwachung ... der fortschreitenden Ausweitung der Disziplinarsysteme... ihre Vervielfältigung durch den gesamten Gesellschaftskörper hindurch, die Formierung einer Disziplinargesellschaft.“[230]

Der Panoptismus durchdringt von den Peripherien aus die Gesellschaft, indem er ein Mittel zur Disziplinierung von Devianz zu sein scheint. Er bleibt in den Zentren der Gesellschaft weitgehend unbemerkt, aber dies vor allem daher, weil seine Ausübung, sein Sichtbarwerden nur in Ausnahmefällen notwendig ist. Seine Präsenz wird aber nicht bestritten. In Bezug auf das Internet wird momentan die prinzipielle Sanktionierbarkeit jeglicher Kommunikation als gesellschaftliche Realität dargestellt. Das Umgehen dieser Möglichkeiten ist alles andere als trivial, hier sei nur darauf hingewiesen, dass die Möglichkeit der unzensierten Äußerung einerseits an technischer Kompetenz festgemacht und die Wahrnehmung dieser Inhalte angesichts der Dominanz kommerzieller Inhalte im Netz eher unwahrscheinlich ist.

### 4.1.3. Panoptismus im Netz: Überwachung

Mit der Überwachungsdebatte im Zusammenhang mit Telekommunikationsdiensten im Allgemeinen und internetgestützten Diensten im Besonderen stehen zwei Institutionen im Zentrum vieler Diskurse im und über das Netz: Europol/Enfopol und Echelon. Speziell für Deutschland relevant sind die Abhörbefugnisse, die die neue Telekommunikations-Überwachungsverordnung (TKÜV*) mit sich bringt.

Europol ist momentan Vorreiter einer international sich abstimmenden und Daten austauschenden Überwachungspraxis seitens europäischer Polizeibehörden. Enfopol, die ‚Enforcement Police’ ist der Entwurf einer Institution auf europäischer Ebene, die für die Einrichtung von Abhörschnittstellen im elektronischen Datenverkehr kombiniert mit einem grenzüberschreitenden Austausch von Abhördaten im Rahmen von Strafverfolgung und Prävention zuständig ist.

Echelon ist ein Abhörprogramm der NSA*, eines US - amerikanischen Geheimdienstes, welches in Kooperation mit Großbritannien und Neuseeland betrieben wird. Es dient der Überwachung des Datenverkehrs auch und gerade von Privatpersonen und Wirtschaftsunternehmen. Es gibt Anhaltspunkte für ähnliche Systeme unter französischer Ägide.

Die TKÜV ist momentan noch nicht verabschiedet. Ziel ist die nationale Umsetzung europäischer Abhörstandards und die Schaffung von umfassenden Möglichkeiten zur

[230] Foucault, 1995, S. 269

zeitnahen Überwachung möglichst jeglicher elektronisch übertragener Kommunikation in Deutschland.

#### *4.1.3.1. Europol/Enfopol*

Enfopol ist die ‚Arbeitsgruppe für polizeiliche Zusammenarbeit', die auf der Ebene des Europäischen Rats angesiedelt ist. Aktuell tritt sie mit Forderungen nach umfassenden Abhör - und Archivierforderungen von elektronischer Kommunikation, ihren Inhalten und der jeweiligen Verbindungsdaten in Erscheinung. Ziel ist die Effizienzsteigerung bei Abhörmaßnahmen generell, weiterhin die Substitution der durch Verschlüsselung verlorengehenden Informationsmöglichkeiten durch die Möglichkeit, mittels der Kontaktdaten Kommunikationsnetzwerke und -strukturen zu erkennen.

Das Problem der Datenbanken von Europol und den Abhörbefugnissen und Auswertungsbefugnissen, die die Forderungen von Enfopol ermöglichen sollen, ist nicht nurin den faktisch zu erwartenden Abhörmaßnahmen zu sehen, sondern eben in der disziplinierenden Wirkung auf potentiell Betroffene. Die Digitalisierung der belauschten Daten vereinfachten eine massenhafte und größtenteils computerisierte Auswertung, anders als bei analoge Medien, die gewöhnlich aufwendigere und personalintensivere Analysemethoden verlangen. Durch die Aufwandssenkung werden Abhör- und Überwachungsmaßnahmen praktikabler und wird die Knappheit der Ressourcen, die bislang eine natürliche Untergrenze der Wichtigkeit von Abhörgründen geschaffen hat, weitgehend beendet.

Bei Europol ist ein weiteres Problem, dass es sich um eine Institution mit nur rudimentären Rechtfertigungspflichten handelt. Über die üblichen Arbeitsfelder Menschen- und Drogenhandel, organisierte Kriminalität, Geldwäsche und Handel mit radioaktivem Material ist die Ausweitung auf beispielsweise Computerdelikte, Betrug, Organhandel und Produktpiraterie geplant. Interessanterweise wurde Kinderpornografie der Kategorie Menschenhandel zugerechnet und damit eine Zuständigkeit geschaffen. Problematisch ist dabei, dass Europol im Prinzip keinem Parlament eines europäischen Staates rechenschaftspflichtig ist und die Beamten diplomatische Immunität genießen. Dabei entsteht momentan eine umfassende Datenbank, die aus den verschiedenen Datenbanken der europäischen Strafverfolger zusammengetragen wird. Richterliche Beschränkungen, welche Daten erhoben und gesammelt werden dürfen, gibt es bislang nicht. Die Erhebung und Sammlung der Daten von allenfalls verdächtigen Personen zusammen mit der Option der Zusammenarbeit mit Interpol und der implizierten Weitergabe von Daten an Interpol schafft rechtliche Grauzo-

nen, in denen das deutsche Recht auf informationelle Selbstbestimmung abgeschafft wird.[231]

Üblicherweise werden als die zu bekämpfenden Feinde im Internet die Anbieter von Kinderpornografie und Anbieter verbotener rechtsextremer Inhalte genannt, ebenso das organisierte Verbrechen, aber auch die Koordination der Aktionen und Anschläge extremistischer Gruppen.

Ein positiver Effekt ist fraglich, so wird das vielzitierte organisierte Verbrechen gewöhnlich sichere oder nur unter hohem Aufwand knackbare kryptografische oder steganografische Verfahren verwenden (siehe Punkt 4.4.5. unten). Auf der anderen Seite stehen leicht kriminalisierbare Gruppen wie Bürgerrechtsbewegungen, Atom-AktivistInnen etc. vor dem Problem, ihre elektronische Koordination und Aktivität plötzlich als Sicherheitsrisiko betrachten zu müssen. Eine abschreckende Wirkung auf potentielle Aktivisten angesichts einfacherer Auf-Verdacht-Überwachung diesbezüglich auffallender Personen ist die eine Folge, das Verknüpfen von vergleichsweise risikoärmeren Protestformen an notwendige informationstechnische Kompetenz ist eine andere.

Im europäischen Parlament sind inzwischen Planungen im Gang, die europäischen Provider dazu zu verpflichten, den Datenverkehr über ihre Einwahlpunkte (je nach Vorschlag) zwischen 90 Tagen und sieben Jahren zu speichern.[232]

#### *4.1.3.2. Echelon*

Echelon dagegen ist von der US-amerikanischen NSA betriebenes Abhörsystem, welches vor allem satellitengestützte Kommunikation großflächig abhört und Teil des gegenseitigen Bespitzelns der Industriestaaten ist. Über das tatsächliche Ausmaß der Überwachung sind dementsprechend wenig sichere Informationen bekannt, sondern die Annahmen stützen sich auf die Analyse des technisch Möglichen einerseits und der Auswertung der aus den beobachtbaren Ressourcen gewinnbaren Informationen andererseits (so beispielsweise die Standorte undeklarierter Antennenstationen und die Abstrahlwinkel von Telekommunikationssatelliten etc.) Kabelkommunikation kann abgehört werden, wenn die Leitungen an den Teilnehmerstaaten Großbritannien, Australien und Neuseeland oder den USA anlanden. Kupferkabel können induktiv abgehört werden, Glasfaserkabel sind technisch schwieriger zu belauschen, da sie zur Entnahme durchtrennt, die Signale verstärkt und dann gesplittet werden müssten, um danach wieder weitergeschickt zu werden. Eine solche Unterbrechung müsste von den inzwischen zumeist privaten Kabelbetreibern be-

[231] Krempl in Schulzki-Hadoutti, 2000, S. 25f.
[232] Rötzer 2001

merkt werden. Eine Überwachung der Handykommunikation oder von Richtfunkstrecken sei dagegen sehr schwierig vorstellbar und ihr Einsatz daher nicht anzunehmen.

Eins der Hauptmotive dürfte Industriespionage sein, wenngleich auch regelmäßig beteuert wird, die Daten würden nur geheimdienstintern verwendet oder man würde ausschließlich Verdachtsfälle von Bestechung und Korruption verfolgen wollen.[233] Seitens des ehemaligen CIA - Direktors Woolsey wurde auf die „europäische Tradition der Bestechung“ hingewiesen, die solche Maßnahmen notwendig machen würden. Weiterhin solle das Einhalten beispielsweise von Handelsbeschränkungen oder Boykottmaßnahmen kontrolliert werden.

Echelon verdeutlicht mehrere Sachverhalte: zum einen die Machbarkeit des Handlings sehr großer Datenmengen und ihrer nutzenbringenden Auswertung, zum anderen die eklatante Skrupellosigkeit, mit der mittels der Durchführung und Duldung von Überwachung Bürgerrechte missachtet werden. Der Leiter des Echelon - Untersuchungsausschusses Schmid betont im Interview, der Umfang der Abhörmaßnahmen sei nach Bekanntwerden der Echelonstrukturen lange Zeit überschätzt worden,[234] weiterhin äußert er sich nur sehr vorsichtig über die Möglichkeit der Wirtschaftsspionage. Anders kommt jedoch der Abschlussbericht des Echelon - Untersuchungsausschusses in Brüssel zu den Ergebnissen, die volkswirtschaftlichen Schäden könnten in Größenordnungen von zwei- bis dreistelligen Milliardenbeträgen[235] reichen und weiterhin hätten bewusste Verstöße gegen die Menschenrechte bezüglich des Verletzens der Privatsphäre der BürgerInnen stattgefunden.[236]

Die Abhörstation im bayrischen Bad Aibling wird nach Angaben der CIA in absehbarer Zeit geschlossen. Es ist anzunehmen, dass dies nicht einer neuen Haltung bezüglich des Datenschutzes und der Industriespionage seitens der NSA geschuldet ist, sondern dem Ausbau von Stationen in Großbritannien und dem auch von Schmid attestierten Bedeutungsverlust der Satellitenkommunikation zugunsten der Seekabel. Problematisch ist weiterhin, dass Echelon nicht das einzige System dieser Art sein dürfte, Schmid sagt in Bezug auf französische Aktivitäten:

> „Mit einem Kontrollausschuss für Geheimdienste konnten wir nicht reden, weil es in Frankreich nämlich kein parlamentarisches Kontrollgremium für die Geheimdienste gibt, was Herr Paecht in seinem Bericht auch beklagt. Das Interessante beim Gespräch mit Herrn Malet war, dass er sich gar nicht so darüber beschwert hat, was die Amerikaner machen.[...] Es gibt Gerüchte, dass die Amerikaner den Franzosen beim Aufbau des eigenen Abhörsystems technisch geholfen haben. Es ist trotz des politischen The-

[233] vgl. Rötzer 2000c, Campbell 2000b
[234] Schulzki-Hadoutti, 2001a
[235] Campbell, 2001b
[236] Campbell, 2001c. Vorsichtiger kann man von einer Grauzone redden, da die diesbezügliche Menschenrechtskonvention zum Schutz des wirtschaftlichen Wohlergehens eines Staates ausgesetzt werden kann, es jedoch fraglich ist, ob eine Abhörmaßnahme generell einem Staat und nicht vielmehr einem Unternehmen zugute kommt.

aterdonners nicht so, dass auf der Ebene der Nachrichtendienste nicht etwas entspannter zusammen gearbeitet werden würde."[237]

Letztendlich kann anhand des Beispiels Echelon davon ausgegangen werden, dass sich Abhörmaßnahmen nicht nur auf polizeiliche Maßnahmen beschränken, die einer Kontrolle durch die Exekutive als auch einer rechtlichen Deckung unterstehen müssen, sondern auch und in großem Stil von Institutionen durchgeführt werden, welche diesen Beschränkungen nicht unterworfen sind. Dem Wohl der jeweils begünstigten Konzerne wird das Recht auf Privatsphäre der Abgehörten untergeordnet, eine demokratische Hinterfragung oder gar Kontrolle ist nicht möglich. Die Gefahr, die ein System wie Echelon darstellt, unterscheidet sich dahingehend von anderen Abhörmaßnahmen, dass sie der demokratischen Kontrolle nicht mehr unterworfen sind und Symptome einer Überidentifikation der Nationalstaaten mit ihren Konzernen darstellen, die staatliche Institutionen für ihre Zwecke instrumentalisieren können. Staatliche Interessen werden mit Konzerninteressen gleichgesetzt, letztere werden ungeachtet der Störungen des diplomatischen Verhältnisses zu den observierten Staaten oder der Bürgerrechte mit staatlichen Mitteln verfolgt.

#### *4.1.3.3. Das neue TKÜV*

Die Telekommunikationsüberwachungsverordnung, kurz TKÜV, ist in Bezug auf die Bedeutung des Internets nicht auf dem Stand der aktuellen Technik und wird momentan den Möglichkeiten der neuen Kommunikationsmedien angepasst. Die überarbeitete Fassung sieht die Einrichtung von standardisierten Abhörschnittstellen bei Internetprovidern ein, die die Analyse und das Protokollieren des Traffics nach Benutzerkennungen, d.h. der Einwahlnummer, der Mailadresse oder der Kreditkartennummer erlaubt.

Ausnahmen sind Kleinprovider und Internetdienstanbieter mit weniger als 2000 Endnutzern oder Anbieter von ohnehin öffentlich einsehbaren Internetdiensten wie Chaträumen und Webseiten.[238] Auch wenn entwarnt wird, eine komplette Trafficanalyse nach dem Vorbild von Carnivore (siehe unten) sei mit dem neuen Entwurf rechtlich nicht gedeckt (es darf zwar der komplette Traffic durch den Provider gescannt werden, er ist jedoch nur zur Herausgabe der Verbindungsdaten mit der angefragten Kennung verpflichtet), stellt sich die Frage, weshalb bei der in Deutschland ohnehin im EU - Schnitt höchsten Abhörquote von Telefongesprächen ohne eine daraus resultierende höhere Aufklärungsrate bei Straftaten die Abhörkapazitäten und -befugnisse weiterhin ausgeweitet werden.

[237] Schulzki-Hadoutti, 2001a
[238] Entwurf für das TKÜV, Stand 2/2001

Da die Provider die Kosten für die Einrichtung der Überwachungsschnittstellen selber tragen müssen, existiert nicht nur seitens der Datenschützer eine Gegenfront zu den TKÜV - Plänen, in der Realität jedoch ist die reibungslose Zusammenarbeit der Provider mit der Staatsanwaltschaft offenbar entgegen der Lobbyaktivitäten gegen die Regelung bereits an der Tagesordnung.[239] Seitens der Datenschützer wird die Regelung vereinzelt sogar begrüßt, da bisher angesichts des vollständigen Fehlens direkter Regelungen Provider dazu neigen, Verbindungsdaten auf Anfrage der Ermittlungsbehörden herauszugeben, ohne überhaupt auf eine richterliche Anordnung zu bestehen.

Bei anderen Institutionen angesiedelt, aber auf dieselbe Zielgruppe gerichtet ist die bereits verabschiedete Änderung der Befugnisse des BND. Dieser ist seit 1999 dazu berechtigt, abgehörte Daten an die Polizei weiterzuleiten, wenn sie bestimmte Straftaten zum Thema haben, darunter aber nicht nur für die innere Sicherheit relevanten Tatbestände, sondern ebenso auch beispielsweise Verstöße gegen das Betäubungsmittelgesetz. Letztendlich werden so weitere Kapazitäten auch für die Überwachung des nationalen Datenverkehrs etabliert. Dementsprechend wird die Trennung zwischen Polizei und Geheimdiensten im Rahmen von Abhörmaßnahmen zunehmend aufgeweicht.[240]

#### *4.1.3.4. Techniken der Trafficanalyse*

Carnivore, Perkeo und INTERMiT sind drei verschiedene Varianten eines Verfahrens, automatisiert Netztraffic auf bestimmte Inhalte zu scannen. Allen gemein ist, dass sie in der Lage sind, große, fließende Datenmengen auf spezielle Inhalte zu überprüfen und bei positiven Resultaten automatisiert bestimmte Reaktionen ausführen zu können.

Die Software Perkeo wird providerseitig eingesetzt. Sie scannt automatisiert nach kinder- und tierpornografischen Abbildungen vordringlich in Newsgroups, kann aber auch zur Filterung des Traffics von Email - Anbietern, Webseiten und verschiedenen Servern (ftp etc.) eingesetzt werden. Mit aktuell über 100MB/s Suchkapazität eignet sich die Software auch für größere Netzwerkbetreiber und Provider. Eine automatische Benachrichtigung der Strafverfolgungsbehörde ist möglich, ebenso ein automatisierter Update der Suchdatenbank (Perkeo scannt nach typischen Datenstrukturen bereits bekannter kinder- oder tierpornografischer Bilder). Die Anbieter brüsten sich nicht nur mit der ‚reinen' Leistungsfähigkeit ihrer Software, sondern auch mit dem bereits angeführten Einschüchterungseffekt, der durch die Bekanntgabe der stattfindenden Überwachung entsteht und die

[239] Schulzki-Hadoutti, 2001b
[240] Gesetz zur Neuregelung von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses, weiter auch Schulzki - Hadoutti, 2001c

Foucault als einen Aspekt der Disziplinargesellschaft betrachten würde: auf einer nicht näher bezeichneten hessischen FH sollen nach dem Bekanntwerden des Suchlaufs von Perkeo 80% aller Daten auf studentischen Homepages seitens ihrer Eigentümer vorsorglich gelöscht worden sein.[241] Mit diesen Begründungen wird von den Entwicklern der Software ein Beenden der Verantwortungslosigkeit und ein „flächendeckender Einsatz bei allen Providern“ gefordert.

INTERMiT ist eine Metasuchmaschine, die anders als Perkeo nicht auf Bilder, sondern auf Begriffe abzielt, Überwachungsziel sind nicht Emails oder Chaträume, sondern nur das WWW*.

Hier ist zu beachten, dass es durchaus bereits Metasuchmaschinen gibt, mittels derer riesige Bereiche des Webs indexiert erschlossen werden können. Krempl bringt die neue Suchmaschine folgerichtig auch nicht vordringlich mit dem Web selber in Verbindung, sondern mit den Plänen der Enfopol, Verbindungs- und Trafficdaten im Netz über Jahre hinweg zu speichern. Zur Sichtung der anfallenden immensen Datenmengen bietet sich die Entwicklung von auf die konkreten Ziele der Strafverfolger zugeschnittene Suchinstrumenten an.[242] Auch hier werden Vorwürfe laut, dass die genannten Probleme Kinderpornografie und Rassismus nicht selbst bekämpft werden, sondern zur Legitimierung von Überwachung und der Kontrolle der Netzkommunikation missbraucht werden.

Carnivore ist ein noch länger bekanntes Trafficanalysesystem auf Hardwarebasis, das vom FBI entwickelt wurde. Es wird beim Provider einer verdächtigen Person eingesetzt, scannt den kompletten Emailtraffic, der über den Provider läuft und filtert die Emails der zu überwachenden Person heraus. Problematisch ist dabei, dass der komplette Emailverkehr dabei auf Schlüsselwörter gescannt wird, d.h. nicht nur die Mails der verdächtigen Person, sondern alle über den angeschlossenen Rechner laufenden Mails werden prinzipiell durch die Software gesichtet. Da die Hardware nicht vom Provider, sondern als Black Box vom FBI gestellt wird, existiert auch keine Kontrolle darüber, was tatsächlich alles letztendlich mitgeschnitten wird.[243] Interne FBI - Tests sollen ergeben haben, dass mittels Carnivore der komplette Email- und Chat - Traffic des belauschten Providers mitgeschnitten werden kann, nicht etwa nur die Mails angegebener Verdächtiger.[244]

Es liegt in der Natur der Sache, dass nicht bekannt ist, nach welchen Kriterien Traffic abgehört wird. Ebenso ist zur Zeit schwer vorstellbar, dass in größerem Stil verschlüsselte Kommunikation abgehört werden kann. Rein spekulativ möchte ich eine entsprechende Debatte kurz umreißen, die nach dem Bekanntwerden der Echelon - Problematik über die Diskussionsmailingliste des CCC ging. Nach anfänglichen Überlegungen über (ohnehin schon bekannte und praktizierte) Scanwortlisten, um die Zahl der herausgefilterten Mails

[241] AUTEM GmbH, 2000
[242] Krempl, 2001a, 2001b
[243] Rötzer, 2000b

zu maximieren und die Arbeit der Überwacher zu erschweren, wurde recht schnell festgestellt, dass es genügend Ausschlusskriterien gibt, mittels derer die Effizienz weiter gesteigert werden kann, ob dies nun die Begriffshäufung bei einfachen Listen, die Unverfänglichkeit der Absender, Vielsprachigkeit, grammatischer Sinn, thematisches Passen der Begriffe zueinander etc. - mit dem Ergebnis, dass es recht schwierig würde, überzeugend firmeninterne Emailkommunikation mit Patentinformationen, Geschäftsangeboten etc. zu simulieren. Doch selbst, wenn das erreicht werden solle, hätte man damit weniger der Freiheit der Information und dem gleichberechtigten Zugang aller zum Netz einen Dienst erwiesen, sondern nur eine Aktion zugunsten der Interessen der europäischen Konzerne durchgeführt.

Letztendlich ist ein Aushebeln der Trafficanalyse effektiv nur mit starker Kryptografie möglich, Gesetzesentwürfe, welche die Herausgabe der Schlüssel erzwingen können, sind in Großbritannien jedoch bereits verabschiedet.[245]

### 4.1.4. Panoptismus im Netz: dezentrale Datensammlung

Über Umwege ist die Gewinnung von weitreichenden Informationen auch durch private Akteure bereits gängige Praxis. Der Privacy-Aktivist Richard Smith beschreibt die gängigen Taktiken anhand der Methoden der Werbefirma DoubleClick, die umfassend mit manchen Suchmaschinen zusammenarbeitet: anhand der eingegebenen Suchbegriffe werden Nutzer profiliert und ihre Interessensgebiete ausgewertet. Mittels Cookies - kleinen Textdateien, die auf der heimischen Festplatte angelegt werden - werden die User identifiziert. Diese Bündelung von Wissen über den Nutzer kann nun genutzt werden, um zielgruppenorientiert Werbung einzublenden. Der Benutzer ist dabei noch anonym, d.h. es ist für einen unbekannten Menschen bekannt, was er für Interessen besitzt und es besteht die Möglichkeit, diesen wieder zu identifizieren, wenn er wieder online ist. Über Verlosungen, Wettbewerbe oder Online-Einkauf auf Partnerseiten werden jedoch die persönlichen Angaben gesammelt, die dann von DoubleClick mit den Daten aus der Profilerstellung zusammengeführt wurden.[246] Prinzipiell ist somit über das Netz im Vergleich zu beispielsweise dem Fernsehen eine weitaus direktere Observierung der NutzerInnen möglich. Diese Bidirektionalität liegt natürlich in der Struktur des Internet selbst begründet, dass sie letztend-

[244] Corinth, 2000
[245] Vgl. Medosch, 2000. Der Gesetzestext ist einsehbar unter [http://www.hmso.gov.uk/acts/acts2000/00023--e.htm] Die Herausgabekriterien sind sehr weit gefasst, angeführt wird die Angemessenheit der Schlüsselherausgabe „(a) in the interests of national security; (b) for the purpose of preventing or detecting crime; or (c) in the interests of the economic well-being of the United Kingdom.“. (ebd.)
[246] vgl. Smith, 2000

lich vorherrschend in eine Richtung eingesetzt wird, schafft die neue Unterscheidung zwischen Beobachtern und Beobachteten. Typisch für die Einseitigkeit ist, dass der User gewöhnlich mit dem Angeben personenbezogener Daten - beispielsweise dem Abonnieren eines Email-Newsletters oder dem Online-Einkauf - keine Kontrolle mehr über das weitere Schicksal der Daten behält. Ebenso wird das Vermeiden der Angabe persönlicher Daten immer schwieriger - so ist es für den ‚Normalnutzer' nicht mehr nachvollziehbar, wo er eventuell durch das reine Email-Lesen über eingebaute unsichtbare Grafiken in Werbeemails Aufschluss über sein Werbeleseverhalten vermittelt, oder ob eine Webseite übermittelte persönliche Daten automatisch weitergibt. Inwieweit Kundendatenbanken von Pleitefirmen zur Konkursmasse gehören und verkauft werden dürfen, ist ebenfalls rechtlich nicht überall gesichert: schon allein die unterschiedlichen nationalen Gesetzgebungen vereiteln hier die Versuche der Herstellung genereller Sicherheiten.[247]

## 4.2. Manipulation und Filterung der Netzinhalte

Netzinhalte können auf verschiedene Art und Weise manipuliert werden. Zu Beginn soll exemplarisch ein Experiment vorgestellt werden, das in kleinem Rahmen die Manipulationsmöglichkeiten vorstellt, welche mittels einer zentralisierten Kontrolle über die Zugänge einer Gruppe von Netznutzern bestehen.

In den folgenden Unterpunkten sollen ebenfalls anhand von Beispielen Möglichkeiten beschrieben werden, die Manipulationen am sichtbaren Gesamtangebot des Internet ermöglichen. Grob kann man zwischen dem Verhindern oder der Entfernung der Publikation unterscheiden (Löschung von Inhalten, Mailaccounts, Adressen; d.h. dem Einschränken dessen, was im Netz veröffentlicht werden darf) und dem Verstecken der prinzipiell weiterhin vorhandenen Daten vor bestimmten Netznutzern (Filterung durch Provider für die Kunden, durch sämtliche Provider eines Landes oder direkt an den Backbones, die ein Land ans Netz anbinden, Filterung schließlich auf einem bestimmten Rechner, der manche Informationen schlicht nicht anzeigt; d.h. der Einschränkung der Sichtbarkeit mancher Inhalte).

[247] vgl. Zarzer, 2000

### 4.2.1. Ein Experiment zu Machtstrukturen und Zensur im Internet

Zwischen dem 27. November und dem 4. Dezember führten Dragan Espenschied und Alvar Freude ein Experiment an der Merz-Akademie in Stuttgart durch. Im Lauf des Experiments wurde der gesamte Webtraffic der Studierenden an der Merz-Akademie über einen Proxyserver* geführt, der in mehrfacher Beziehung manipulierend auf die Inhalte einwirkte.[248] Ihre Zielsetzung beschreiben sie folgendermaßen:

> „Um zu beweisen, dass das Internet nicht ‚von Natur aus' ein freies Medium ist, sondern eines, in dem Hierarchien und Machtstrukturen abgebildet und erschaffen werden können, manipulierten wir unbemerkt das Hausnetzwerk an unserer Hochschule, der Merz Akademie. Wir wollten gleichzeitig überprüfen, ob die Furcht vor Filter-Systemen tatsächlich gerechtfertig ist, wie schnell die Manipulation auffliegt und mit wie viel Aufwand das Filtern zu realisieren ist."[249]

Nach einer mehrwöchentlichen Analyse des von den Studierenden verursachten Traffics waren die beliebtesten Seiten der Studierenden bekannt und auf dem Proxyserver wurden dementsprechend Filter und Manipulationsinstrumente eingerichtet. So wurden einzelne Worte und Begriffe, die auf den häufig besuchten Seiten vorkamen, durch die Filtersoftware ausgetauscht, Kohl wurde zu Schröder und umgekehrt, die Worte ‚Aber', ‚Und' und ‚Auch' wurden gegeneinander mit bestimmter Wahrscheinlichkeit ausgewechselt, um Sinnzusammenhänge zu verdrehen. Später wurden offensichtlichere Fakes eingebaut, so wurde ‚olitik' zu ‚ropaganda', Deutschland zu ‚Das Reich' und der Minister zum Gauleiter etc.[250]

Weiterhin wurde mit einer bestimmten Wahrscheinlichkeit beim Aufrufen einer neuen Seite ein Werbeblock von für das Internet bedeutsamen Institutionen wie InterNIC, Corenic, ICANN*, Network Solutions und dem amerikanischen Wirtschaftsministerium eingeblendet, bei dem die Surfer beispielsweise auf Anzeigen der NRA[251] klicken konnten, um den kostenlosen Weiterbestand des Internet zu sichern. Über Frames wurde auf jeder Seite, die über Google, Yahoo, Lycos oder Web.de (die augenblicklich populärsten Suchmaschinen und Webkataloge) gefunden wurde, ein Formular eingeblendet, mittels dem man die gefundene Seite nach Kategorien wie ‚anstößig', ‚pornografisch', ‚extremistisch' oder ‚Gotteslästerung' usw. bewerten konnte, um das Netz von „unerwünschten Inhalten zu

[248] Sehr viele Internetprovider sehen die Benutzung eines Proxyservers* (ugs. Proxy), einem Rechner, der zwischen den User und das Internet geschaltet ist, zwingend voraus, allen voran AOL*. Insofern ist die dargestellte Methode durchaus auch auf größere Strukturen übertragbar.
[249] Espenschied; Freude, 2001
[250] Eine komplette Ersetzungsliste ist unter http://online-demonstration.org/static/insert_coin/wordlist.txt einsehbar.
[251] Die National Rifle Association, eine erzkonservative Lobbyvereinigung zum Schutz und der Förderung des Schusswaffenbesitzes in den USA.

befreien“.[252] Die populäre Musiktauschbörse Napster wurde mit einer gewissen Wahrscheinlichkeit mit einer Umfrage versehen, die sehr detailliert personenbezogene Daten abfragte.

Der Versuch lief eine Woche, dann musste er aufgrund eines ausgefallenen Speicherchips in dem manipulierten Server abgebrochen werden: bis der Server wieder aufgesetzt war, fanden die Netztechniker die Manipulation heraus, wenngleich das Experiment bedingt immer noch weiterläuft:

> „Da das allgemeine Interesse an technischen Dingen unter den Studenten jedoch nicht sonderlich ausgeprägt zu sein scheint, wurde der Filter nur sporadisch deaktiviert und läuft auf vielen Maschinen bis heute munter weiter. – Obwohl wir eine Deaktivierungs-Anleitung veröffentlichten.“[253]

Resultierend aus der Vorstellung des Experiments und seines Ergebnisses ergab sich eine heftige Diskussion auf der fitug – Mailingliste[254] darüber, wie weit eine solche Manipulation der Surfer zulässig sei und weiterhin, welches Ausmaß an technischer Kompetenz einem Normalsurfer zugemutet werden darf, dem angesichts des üblichen Werbebombardements und der Unzuverlässigkeit der Technik nicht zum Vorwurf gemacht werden könne, dass er nicht in der Lage wäre, selbständig einen Proxyserver* aus der Browserkonfiguration auszutragen oder fingierte Werbeanzeigen einer fiktiven ‚InterAd.gov’ - Agentur angesichts ihrer Unverschämtheit von ‚normaler’ Werbung zu unterscheiden.

Dem gegenüber wäre zu sagen, dass das Experiment an einer Design – Hochschule stattfand, in der eine diesbezügliche Medienkompetenz eher zu erwarten gewesen wäre als beispielsweise bei den AOL* – NutzerInnen des Einwahlpunktes Heilbronn. Die Sensibilisierung für eine mögliche Manipulation der sichtbaren Netzinhalte scheint extrem niedrig zu sein, da die Reaktionen auch nach einer aufklärenden Rundmail weitgehend ausblieben und noch Monate später der manipulierende Proxyserver von einigen Rechnern der Akademie genutzt wird.

Es wäre falsch, angesichts dieses Ergebnisses einfach auf den Charakter des Internet als unzuverlässiges Medium zu verweisen, welches an Seriösität und Verlässlichkeit seiner Inhalte eben noch hinter Fernsehen und manchen Printmedien anzusiedeln sei. Es zeigt vielmehr, dass im Netz Manipulationen einfacher zu machen sind, Überwachung und Kontrolle dessen, was die UserInnen zu sehen bekommen, durchaus großflächig durch- und umsetzbar ist und die Sensibilisierung der UserInnen für diese Möglichkeit als zu niedrig

[252] Die Nähe zur CDU - Formulierung auf www.netzgegengewalt.de, „Wenn Ihnen Adressen extremistischer oder gewaltverherrlichender Seiten bekannt sind, so können Sie diese in der Eingabemaske unten melden.“, dürfte beabsichtigt sein.
[253] Espenschied; Freude, a.a.O.
[254] Erstes Posting der Diskussion von Espenschied; Freude: [http://www.fitug.de/debate/0012/msg00249.html] Fitug ist der Förderverein Informationstechnik und Gesellschaft.

angesehen werden kann. Die beiden Autoren beziehen sich ebenfalls explizit auf die ‚Code is Law' - These Lessigs, wenn sie betonen, dass es kein ‚Wesen des Netzes' gäbe, welches solche Manipulationen unmöglich macht. Das Bonmot, das Netz interpretiere Filter und Sperren als Störung und route den Datenverkehr einfach um diese herum, kann nicht aufrecht erhalten werden.

Der Vorwurf, das Experiment lasse weniger Aussagen über die Struktur des Internets zu als vielmehr über die Dummheit seiner Anwender, kann zwar erhoben werden, letztendlich werden die Kommunikationsstrukturen aber von den Usern geprägt. Ein Netz, dessen Nutzer die Filtermacht abgeben, wird wohl gefiltert werden, Freiheit der Kommunikation und weitgehende Freiheit von hierarchischen Strukturen sind nicht genuines Wesen des Netzes, sondern müssen erkämpft und ihr Vorhandensein ständig überprüft werden. Ein Netz, dessen User nicht in der Lage sind, dies zu gewährleisten, wird dementsprechend kontrolliert werden.

Es ist unmöglich für einen Normalanwender, diese Kontrolle durchzuführen. Die zugrundeliegende Technik ist inzwischen bei weitem zu komplex. Dieses Ergebnis kristallisierte sich offenbar selbst auch an einer Kunsthochschule heraus, deren Angehörigen qua Alter, Bildung und der intensiven Beschäftigung mit Medien eigentlich potentiell überdurchschnittlich kompetent sein müssten. Diese Kontrolle muss somit offenbar durch eigens qualifizierte Experten geleistet werden. In diesem Kontext ist die Demontierung der Begrifflichkeit des ‚Hackers' in den Medien durchaus bedenklich. Eine ‚Expertisierung' der User wird weder gewünscht, noch wäre sie im notwendigen Umfang überhaupt machbar. Espenschied folgert in der fitug - Debatte: „Das Netz soll konsumiert werden, nicht gestaltet oder genutzt. Die Oberflächen aller Programme sind darauf ausgelegt, möglichst viel von den technischen Abläufen zu verbergen."[255] Dennoch wird das Prinzip von ‚Security through Obscurity' gerade im Bereich des Internet häufig angewandt und werden Experten, die eine Kontrolle der tatsächlichen Sicherheitslücken und Schnittstellen für Manipulation und Überwachung leisten könnten, immer weiter in rechtliche Grauzonen gedrängt.

Analog dazu wird weniger die Kompetenz der User gefördert, selbst wenn es um vergleichbar einfache Sicherheitsmassnahmen geht (es sei an den Melissavirus erinnert, dessen Verbreitung davon abhing, dass der User ein Attachment einer automatisch generierten Mail startete, und den Bill Gates nicht ganz zu Unrecht als ‚Intelligenztest für den User' bezeichnete), sondern es werden eher die Personen, die den unreflektierten Gebrauch der meisten User ausnutzen, kriminalisiert.

[255] vgl. [http://www.fitug.de/debate/0012/msg00262.html]

### 4.2.2. Die digitale Schere 1: Filterung seitens der Provider

Prinzipiell kann man auf der Providerseite von zwei Möglichkeiten der Filterung respektive der Kontrolle über die Netzinhalte sprechen, die anhand der ‚Erfolge' zweier linker Aktionsgruppen[256] exemplarisch vorgestellt werden sollen.

#### *4.2.2.1. Kontrolle des Webspace*

Jeder Webinhalt liegt bei einem Webspaceprovider, jedes Emailaccount ist auf einem bestimmten Mailserver eingerichtet, Betreiber von Newsgroupservern haben die Möglichkeit, konkrete Newsgroups anzubieten oder dies bleiben zu lassen (so wurde die bereits vorgestellte alt. - Hierarchie von vielen universitären Newsservern nicht angeboten, andere liessen nur selektiv Gruppen mit hohem Datenaufkommen - alt.erotica.binaries.pictures beispielsweise - weg).

Im Zuge des aktuellen Staatsantifaschismus ist es relativ einfach geworden, deutsche Provider davon zu überzeugen, dass es ihrem Ansehen (und verbunden damit ihren Umsätzen) nicht gut tut, wenn sie rechtsextremistische Webseiten hosten. Nach der peinlichen Panne beim Provider Strato, welcher unbesehen die Domain www.heil-hitler.de eingerichtet hatte und dafür massiv kritisiert wurde, wurden Adressen mit strafrechtlich relevanten Namen schnell gesperrt.

Inhalte von rechten Netzseiten wurden beispielsweise von der Netz-Antifa regelmäßig observiert und strafrechtlich bedenkliche Inhalte den Providern gemeldet, welche dann meist die Präsenz löschten. Im Endeffekt wird damit bewirkt, dass rechtsextreme Seiten zunehmend bei US - amerikanischen Providern gehosted werden, bei denen das Recht auf freie Meinungsäußerung auch Inhalte dieser Art schützt, beliebt sind beispielsweise yoderanium.com und front14.org. Ähnlich läuft die aktuelle Aktion zum Boykott des Emailproviders gmx, welcher entgegen seiner Allgemeinen Geschäftsbedingungen rechtsextreme Mailadressen nur in den seltensten Fällen löschte.[257]

Man hat es hier mit einer nahezu deckungsgleichen Adaption der Konflikte zwischen rechter und linker Szene im ‚Real Life' zu tun, es wird versucht, gegnerische Kom-

[256] namentlich der Netz-Antifa (www.netz-antifa.com) und der Aktion Kinder des Holocaust (www.akdh.ch). ‚Erfolge', weil die Wertung als ‚Erfolg' sehr streitbar ist. Die Netz - Antifa hat sich mittlerweile aufgelöst. (interessanterweise begründete der Verantwortliche für das Hosting der Internetpräsenz sein gesunkenes Interesse ausdrücklich mit der Problematik der von der Netz-Antifa implizit geforderten Zensur. Ein anderer Hoster für die Präsenz fand sich nicht, da persönliche Risiken seit dem Auftauchen der netz-antifa im Verfassungsschutzbericht nicht mehr ausgeschlossen werden konnten.)

[257] vgl. die Seite der Netz-Antifa selbst und den Bericht von Klarmann in der TP mit den treffenden Titel „Virtuelles Steinewerfen?" Klarmann 2001

munikation zu stören und den ‚öffentlichen Raum' zu beherrschen. An Ansichten und letztendlich auch den Kommunikationsinfrastrukturen ändert sich nichts, Öffentlichkeit und Vernetzung bleiben erhalten, man macht sich zwar das Leben schwer, wo möglich, aber mehr als der symbolische Akt, den .de, .ch und .at - Namensraum von militant faschistischen Inhalten freizuhalten, kann auf diese Art nicht erreicht werden. Demonstriert wird immerhin die Unerwünschtheit der jeweiligen Ansichten im jeweiligen Land, verallgemeinert könnte man sagen, dass Ansichten, die aktuell unpopulär sind, eben der Landesgrenzen verwiesen werden und ihre Vertreter den vermehrten Aufwand haben, sich um ausländische Hoster zu kümmern.

#### *4.2.2.2. Kontrolle sämtlicher nationaler Provider*

Auf Betreiben der Schweizer Organisation von Überlebenden des Holocaust und deren Nachkommen ‚Aktion Kinder des Holocaust' sperrten die Schweizer Provider Swisscom und Sunrise/Diax „754 rechtsextreme Internetsites" (dpa). Genauer betrachtet wurde nur der besagte Server www.front14.org gesperrt, d.h., alle rechtsextremen Seiten, die von diesem Webspaceprovider gehosted waren, sind von den KundInnen der besagten Schweizer Provider nur erschwert abrufbar. Hier wurde definitiv das Recht auf die informelle Selbstbestimmung der Netznutzer ausgehebelt und eine Bevormundung seitens der Provider eingeführt.[258]

In Anbetracht dessen, dass eine solche Zensurmaßnahme aktuell noch alles andere als wirkungsvoll ist, sollte der konkreten Aktion wenig Gewicht beigemessen werden. Bereits die Sperrung des niederländischen Providers xs4all.nl durch Compuserve, um eine Verbreitung der linksextremen Netzzeitschrift „radikal" zu verhindern, blieb durch das schnelle Erstellen von gespiegelten Seiten auf anderen Servern wirkungslos bis kontraproduktiv. Zumeist haben solche Sperrungen aktuell eher die Wirkung einer Werbeaktion für die betroffenen Seiten. Umgangen werden können die Sperren durch die bereits erwähnten Spiegelungen auf anderen Servern, durch das Verlagern der Distribution der Inhalte auf Mailinglisten, durch das Zwischenschalten von freien Proxyservern, welche nicht von der Sperre betroffen sind usw. Letztendlich wird so der Zugang zu den zensierten Inhalten üblicherweise erschwert und verstärkt an Netzkompetenz und Technikverständnis gebunden, aber keinesfalls verhindert. Hier wie im später angeführten Punkt der Zensur des öffentlich zugänglichen Angebots ist zu attestieren, dass höchstens das Bild, welches sich dem weniger interessierten Menschen bietet, ändert, die ‚Netzrealität' ist für diejenigen, die nicht

[258] vgl. den Pressespiegel von AKdH.

gewillt sind, allerlei technische Tricks anzuwenden, in eine bestimmte Richtung verschoben und geschönt.

Es ist bei einer solchen Praxis somit zu befürchten, dass einerseits die öffentliche Wahrnehmung extremistischer Inhalte manipuliert werden kann. Je nach Sperrpraxis können Bedrohungsgefühle so erzeugt oder gedämpft werden.

Weiterhin weist nichts darauf hin, dass es bei diesen Kriterien zur Kontrolle der sichtbaren Inhalte durch die Provider bleiben muss. Mit der Bereitschaft, auf entsprechende Weisungen mit Sperrungen zu reagieren, wird ebenso die Bereitschaft signalisiert, beliebige andere, unbequeme oder im jeweiligen Rechtsverständnis illegale Inhalte auf Antrag zu sperren. In dieselbe Richtung zielen momentan die Vorstöße der verschiedenen Phonogesellschaften wie der RIAA* und in Deutschland dem Landesverband der IPFI*, welche eine restriktivere Kontrolle der Distributionskanäle digitalisierter Musik fordern. So ist der Versuch der IFPI, mittels eines digitalen Codes, welcher in unhörbarer Form in der digitalen Aufnahme eines Musikstücks codiert ist, nur dann von einer gewissen Logik, wenn gleichzeitig der digitale Austausch eben dieser Daten auf irgendeine Art und Weise weitgehend flächendeckend kontrolliert werden kann.[259] Hier gilt, wie überall anders auch, dass ‚ein bisschen Zensur' schlicht nicht möglich ist. Die Kriterien, was momentan politisch korrekt ist, mögen sich ändern, die Bestrebungen, vor allem den Transport digitalisierter, copyrightgeschützter Daten zu kontrollieren und zu beschränken, werden von für ihre Ausdauer und ihren Einflussreichtum bekannten Institutionen getragen.

### 4.2.3. Die digitale Schere 2: Filterung des öffentlichen Angebots

Eine andere Taktik besteht im Installieren einer Filtersoftware auf bestimmten Rechnern. Auch hier ist eine gewisse Zentralisierung vonnöten, da nicht jeder einzelne Nutzer eine eigene Liste erlaubter und/oder verbotener Inhalte erstellen kann. Dementsprechend arbeiten Filter mit den Daten einer Selbstklassifizierung der Inhaltsanbieter oder den

[259] vgl. IFPI*, 1997. Zusammengenommen mit einer Software wie das bereits vorgestellte Perkeo kann so die Kontrolle über Datentransfers auf Audiodaten ausgedehnt werden. Generell sind die Phonoindustrien Vorreiter bei der Forderung nach einer lückenlosen Kontrolle des Internet-Traffics. Mittels dem RPS (Rights Protection System) können gemäß der IFPI tatsächlich gezielt großflächig Seiten gesperrt werden. So verlautet auch hierzu der Antrag der IFPI: „Konsequenterweise setzt das RPS bei genau den ISPs* (Internet Service Provider = Diensteanbieter) mit einer Auslandsverbindung an. Dies sind in Deutschland nicht mehr als 50-70 Stellen. Die vorgeschlagene Lösung des RPS ist für den ISP sowohl technisch möglich und als auch wirtschaftlich zumutbar. Kleineren ISPs entsteht kein Nachteil, da diese in der Regel ihre Auslandsverbindungen über große Anbieter anmieten. Sie müssen die RPS-Technologie also nicht selbst bei sich einführen. Das RPS bietet die Möglichkeit, gezielt den Zugriff auf einzelne URLs für den Internetnutzer zu unterbinden." IFPI, 2001

Blacklists privater Unternehmen, welche mehr oder weniger beliebige Bewertungskriterien anlegen.

Das Beispiel der USA zeigt, wie eine Filterung nur der öffentlich zugänglichen Netzinhalte aussehen kann. Es bildet sich gewissermaßen ein Zweiklassensystem weniger der Information als der Weltbeschreibung, welches die Nutzer eines privaten Netzzugangs von den zur Nutzung öffentlicher Angebote gezwungener Personen trennt.

Mit dem Terminus der ‚Weltbeschreibung' möchte ich den Kern der Argumentation dahingehend verschieben, dass es nicht darum geht, dass alle möglichst die selbe Menge an ‚Informationen' bekommen und das reine Fehlen einer beliebigen Sexseite eine ‚Informationsungerechtigkeit' bedeutet, wie es in Diskussionen zum Thema oft dargestellt wird. Das Problem besteht in der hochselektiven Arbeit der Filter und im Befördern einer Verschiebung der Sicht auf die Wirklichkeit, die in gezielter Art manipuliert wird. Nicht das Fehlen einer speziellen Seite von und für Schwule verändert die Situation der Nutzer, sondern das Erzeugen einer medienvermittelten Realität, in der sexuelle Minderheiten nicht normal sind.

Was den USA die sexuellen Minderheiten, das ist in Deutschland der Rechtsextremismus: hier wie dort wird versucht, eine Zensur einzuführen, mittels der ein gefiltertes Bild der Realität vermittelt werden soll. Dieses ist nach den ästhetischen und politischen Kriterien einer Elite geschönt, die definiert, welche Inhalte der Normalbevölkerung ‚zumutbar' und generell moralisch vertretbar sind.

Ergebnis ist, unabhängig von den Anlässen, ein Filtersystem, welches Privatnutzern die Option lässt, ob es genutzt wird oder nicht, und welches Menschen, die auf den öffentlichen Zugang angewiesen sind, zwangsweise ein selektives Bild der Wirklichkeit verschaffen.

Das erfolgversprechendste Modell scheint aktuell jenes der ICRA* zu sein, der Internet Content Rating Association.[260] Nach dem Vorbild der amerikanischen RSCA* (Recreational Software Advisory Council) sollen einige Schlüsselkriterien für internationale Netzinhalte erstellt werden, nach denen sich die Betreiber dann selbst klassifizieren sollen. Es ist dabei nicht die Frage, ob diese Lösung kommt, sondern in welcher Form. So zitiert Monika Ermert den Vorsitzenden des EU - Gremiums zur Einführung der ICRA*, Jens Waltermann,

[260] vgl. ICRA, 2001. ICRA basiert auf PICS*, der Platform for Internet Content Selection, einem Klassifizierungssystem von Webseiten. Dieses war die Grundlage von RSAC, einer Ratingmethode, die vom W3C* entwickelt wurde. Die ICRA erweitert und internationalisiert diese frühen Klassifizierungsmethoden. Typisch für die Funktionsweise solcher ‚freiwilligen' Ratingsysteme ist die Sperrung nichtbewerteter Seiten, da sonst die Filterung keinen Sinn machen würde. So gibt auch die ICRA zu, dass unbewertete Seiten voreinstellungsmäßig gesperrt werden: „Als Anbieter einer kommerziellen oder irgend einer anderen Site, die nur einen geringen oder gar keinen Anteil an anstößigem Material enthält, wird Ihnen sicher daran liegen, dass Ihre Site nicht ‚automatisch' blockiert wird." ICRA, ebd.

> „'...Zweitens wollten wir auch unterschiedliche Standpunkte, gerade auch Vertreter der Free-Speech-Bewegung, in diesem Gremium haben. Allerdings haben wir weder Hardliner von der einen noch Hardliner von der anderen Seite.'[...] 'Das Ergebnis der Beratungen wird nicht sein, dass es keinen Filter geben wird', stellt Waltermann klar."[261]

Die Ziele dabei sind reichlich ambitioniert, so wird nicht nur der europäische Surfer zum Ziel der Filterungen gemacht, sondern die Kriterien sollen global anwendbar sein. Kulturelle Unterschiede werden kleingeredet, die europäischen Kriterien beanspruchen weltweite Gültigkeit:

> „'Die Unterschiede zwischen den Kulturen sind gar nicht so groß, manchmal sogar kleiner als innerhalb unserer pluralistischen Gesellschaften', sagt aber Nigel Williams, Direktor der britischen Organisation Child International und von ICRA mit dem Vorsitz des so genannten 'Weltfilterrates' betraut",

zitiert Ermert[262].

Es ist die Frage, wie weit es eine Rolle spielt, wenn Filter bei Bedarf abgeschaltet werden können. Ungeachtet der Tatsache, dass diejenigen, die auf öffentlichen Zugang angewiesen sind, nur die besagte verschobene Realität angeboten bekommen, wird jedoch auch die unzensierte Informationsbeschaffung sichtlich erschwert. So schreibt Alexander Gruhler:

> „Heute kann der Internetsurfer noch selbst bestimmen, ob er ein Rating-System in Anspruch nehmen möchte oder nicht. Populäre Suchmaschinen wie Lycos oder Yahoo kündigten aber an, bald nur noch PICS-registrierte Angebote zu verzeichnen. Damit wären Webmaster, die ihre Seiten einer möglichst großen Zahl von Surfern zugänglich machen wollen, gezwungen, die Inhalte schon aus reinem Selbsterhaltungstrieb PICS-kompatibel und möglichst jugendfrei zu gestalten."[263]

Während seitens des W3C* und der Verantwortlichen der ICRA* noch damit geworben wird, Regierungen durch die Selbstverwaltung von zuständigen, supranationalen Internetgremien aus dem Regelungsvorgang herauszuhalten, ist vollkommen klar, dass Verstöße gegen die Selbstklassifizierungen höchstens von den nationalen Staatsanwaltschaften verfolgt und geahndet werden können und sollen. Schwerer als diese Widersprüchlichkeiten sind aber die Auswirkungen auf das Medium. Sind die statischen, unidirektionalen Angebote der Medienkonzerne relativ bequem zu klassifizieren, ist diese für Privatanbieter häufig zu aufwendig und bei den verbreiteten kosten- und werbefreien Projekten vieler Idealisten im Netz schlicht nicht mehr machbar. Völlig unmöglich wird die Bewertung von Kommunikationskanälen im Netz wie den Diskussionsforen oder Cha-

[261] Ermert, 2000, S. 37
[262] ebd.
[263] Gruhler, 1998

Chaträumen, die in Echtzeit laufen, da im Voraus nichts über die von den verschiedenen Usern kommenden Inhalte bekannt ist und eine Echtzeitkontrolle nicht möglich ist. Der Charakter des Internet als Kommunikationsmedium wird so vollkommen zerstört, wie Espenschied und Freude auch treffend diagnostizieren:

> „Bei einer Filter-Default-Einstellung wäre damit das Netz ein klinisch sauberer Distributions-Kanal für Firmen, die sich das korrekte Auszeichnen ihrer Inhalte leisten können. Schon durch die Idee, ein den Broadcast-Medien entnommenes Konzept der inhaltlichen Selbstkontrolle zu verwenden, zeigt, dass das Netz hier nicht als Kommunikations- sondern als Broadcast-Medium verstanden wird.“[264]

Folgern kann man daraus, dass eine Filterung von Netzinhalten generell abzulehnen ist. Es ist illusorisch anzunehmen, dass zwar eine akzeptierte Form von Inhaltsfiltern auf dem Markt wäre, diese jedoch nicht auf öffentlich zugänglichen Rechnern installiert werden würde. Wenn eine Verfolgung von Falschauszeichnungen gewährleistet sein soll, müssen nationale Kontrollgremien geschaffen werden, welche Seiten und ihre Auszeichnung beurteilen. Damit würde über die Hintertür eine staatliche Zensurbehörde geschaffen. Die ICRA* setzte sich natürlich zum Ziel, eben diese „eiserne Strenge der staatlichen Gesetzgebung“[265] überflüssig zu machen, jedoch kann sie natürlich nur dann funktionieren, wenn eben diese Strenge geboten ist, falls jemand das System mit Falschklassifikationen überlisten will. Genauer, es werden nicht mehr nur im jeweiligen Land illegale Netzinhalte verfolgt, sondern zusätzlich noch werden Personen, die falsche Inhaltsangaben zu ansonsten legalen Angeboten machen, kriminalisiert.

Angesichts der faktischen Unumsetzbarkeit entsprechender Gerichtsbeschlüsse stellt sich die Frage, wie die Umsetzung der Bekämpfung illegaler Inhalte vonstatten gehen soll und was ihre logische Konsequenz wäre. Letztendlich läuft es auf eine repressive Politik gegenüber Staaten heraus, die westliche Wertvorstellungen nicht teilen.

So begründete der BGH das Urteil gegenüber Frederic Törben, einem australischen Holocaustleugner mit den Worten:

> „Es ist offenkundig, daß jedem Internet-Nutzer in Deutschland die Publikationen des Angeklagten ohne weiteres zugänglich waren. Die Publikationen konnten zudem von deutschen Nutzern im Inland weiter verbreitet werden. Dass gerade deutsche Internet-Nutzer - unbeschadet der Abfassung in englischer Sprache - zum Adressatenkreis der Publikationen gehörten und gehören sollten, ergibt sich insbesondere auch aus ihrem Inhalt, der einen nahezu ausschließlichen Bezug zu Deutschland hat [...]Das deutsche Strafrecht gilt für das abstrakt-konkrete Gefährdungsdelikt der Volksverhetzung nach § 130 Abs. 1 und Abs. 3 StGB auch in den Internet-Fällen. Seine Anwendbarkeit ergibt sich aus § 3 StGB in Verbindung mit § 9 StGB. Denn hier liegt eine Inlandstat (§

[264] Espenschied; Freude, a.a.O.
[265] ICRA, a.a.O.

> 3 StGB) vor, weil der zum Tatbestand gehörende Erfolg in der Bundesrepublik eingetreten ist (§ 9 Abs. 1 3. Alt. StGB).“[266]

Es bleibt zu fragen, wie es umsetzbar sein soll, jegliches Landesrecht auf das gesamte Netz anzuwenden. Espenschied und Freude führen dies mit einem treffenden Beispiel ad absurdum:

> „Der BGH spricht von Äußerungen, die den Frieden im Inland stören würden. Solche Argumente ist man ansonsten nur von autoritären Regimes gewöhnt, und welche Folgen dies haben kann, lässt sich einfach ausmalen: In Ländern wie dem Iran wird ‚der innere Frieden' massiv gestört, wenn Frauen unverhüllt abgebildet werden. Wie groß wäre der Aufstand, wenn ein deutscher Werber im Iran zum Tode verurteilt werden würde, weil er die auch im Iran abrufbare Internetseite eines Dessous-Herstellers gestaltete? Es wirft sich unweigerlich die Frage auf: Kann es sich ein Staat wirklich erlauben, seine Gesetzgebung auf ein globales Medium auszudehnen?“[267]

Dem gegenüber wäre einzuwenden, dass eben die Filterung der Inhalte solche Dilemmas vermeiden helfen soll: können die Inhalte nicht im Ursprungsland bekämpft werden, wird wenigstens die einheimische Bevölkerung vor den bedenklichen Inhalten geschützt. Diese Vorgehensweise ist im Rahmen der reinen Kontrolle öffentlich zugänglicher Rechner jedoch eine Farce und führt ihre eigene Berechtigung ad absurdum: entweder hat man es mit ‚schädlichen' Inhalten zu tun, ergo müssen diese konsequenterweise gesperrt werden, oder es muss davon ausgegangen werden, dass die Bevölkerung mit den Inhalten umzugehen versteht, dann ist die Diskriminierung der Gruppe der NutzerInnen ohne privaten Zugang nicht hinnehmbar. Es bleibt der fade Beigeschmack, die Filterbefürworter legen mehr Wert auf eine desinformierte Gesellschaft, die vor unbequemen Begründungen bestmöglich geschützt wird, als auf eine aufgeklärte Bevölkerung, wo Wahrheit und nicht soziale Erwünschtheit einer Debatte den öffentlichen Diskurs oder das überhaupt Öffentliche prägt.[268]

---

[266] Urteilsbegründung des BGH, 12. 12. 2000

[267] Espenschied; Freude, a.a.O.

[268] Es gibt sehr viele Seiten, die sich mit der Widerlegung der Auschwitzlüge beschäftigen, welche teilweise hervorragend recherchiert wurden. Interessanterweise wird beispielsweise die Seite Burkhard Schröders (www.burks.de), der auch die umfangreiche Widerlegung des Leuchter-Reports auf seiner Seite anbietet, regelmäßig von der Staatsanwaltschaft beanstandet, weil er Links auf neonazistische Seiten legt. Seine eigene antifaschistische Einstellung ist auf der Seite klar zu erkennen, er befürwortet ausdrücklich das Wissen um die Strukturen, die man bekämpft. Durch die Debatte über die Verbreitung der Auschwitzlüge per Internet wurde auch ein Diskurs weiter belebt, der nach dem Willen vieler besser in der Versenkung verschwunden wäre, durch ihn wurden gerade die Seiten der Revisionistengegner interessant und zum Gegen-stand öffentlicher Aufmerksamkeit.
Ein anderes Beispiel ist das beispielhafte Engagement einiger Fach- und Allgemeinärzte, die nach dem Auftauchen einiger Diskussionsforen zur ‚Neuen Medizin' beim Forenhoster Parsimony aufklärend aktiv wurden.(die Neue Medizin lehnt unter anderem Impfungen als Instrument einer pharmazeutischen Verschwörung komplett ab, betrachtet Aids und Krebs als praktisch nichtexistente Erfindungen der Medizin respektive der Pharmaindustrie etc. Dem Begründer Hamer wurde die Approbation entzogen, nachdem er zusammen mit den Eltern ein krebskrankes Kind entführte, welches nur knapp mit einer Notoperation nach der Wiederauf-

Ungeachtet der Einwände gegen Filterung allgemein, sei auch auf die zentrale Bedeutung der Wertvorstellungen der agierenden westlichen Welt hingewiesen, die ausdrücklich ‚ihre' und nur ihre Filterkriterien durchgesetzt wissen mag. So zitiert Ermert den Filter-Erfinder Balkin:

> „'Sicherlich werden Filter- und Ratingsysteme für andere Zwecke genutzt werden als für den Schutz von Kindern.' Politische Kategorisierungen sind aber im Grundwortschatz nicht vorgesehen. Trickreicher erscheint die Absicherung des Grundwortschatzes durch Verschlüsselung. 'Die Verschlüsselung der Selbstbewertungen lässt keiner Regierung Zeit zur Dechiffrierung aller durchgeleiteten Daten, ohne das System zu beeinträchtigen.'"[269]

Mögen angesichts der Komplettüberwachung des Netzverkehrs in totalitären Staaten derartige Überlegungen überflüssig wirken, verdeutlichen sie dennoch den Alleinvertretungsanspruch der Akteure bezüglich der Wahrheit darüber, was den Netznutzerinnen zumutbar sein kann und soll.

### 4.3. Die Disziplinargesellschaft und ihre Kontrollfunktion

Überwachung geschieht nicht nur im Kontext der Überwachung durch die Bedrohung von außen, dem eigentlichen, verfassungsgemäßen Auftrag von Geheimdiensten, sondern ist immer auch gegen etwaige GegnerInnen, Unruhestifter und Unzufriedenen im Innern des Staates gerichtet. Die Überwachung des Privat - und Alltagslebens stößt in der stofflichen Welt jedoch an natürliche Grenzen: das System, in dem alle nur damit beschäftigt sind, die anderen zu überwachen, ist das Phantasieprodukt eines Paranoikers. Die Realität scheitert früher, so war eine Spitzenleistung das Verhältnis in der DDR, welches mit der Quote eines Stasiagenten auf 200 Einwohner die Gestapo mit 1 zu 10 000 deutlich schlug.[270] In diesem Kontext sind Prozesse, die den Schlüssel von Überwachern zu Überwachten senken können, ohne die Effizienz mitzusenken, von hoher Bedeutung. Es ist potentiell möglich, auch ohne eine entsprechend hohe Durchdringung der Bevölkerung mit ÜberwacherInnen, an totalitäre Strukturen angelehnte Sieb - und Filtermechanismen in der Gesellschaft zu etablieren. Für die letztendliche Umsetzung ist weniger relevant, was aktu-

findung gerettet werden konnte.) Auch hier hat man es mit Verstößen gegen die ärztliche Sorgfalt zu tun, die jedoch konsequent mit engagierter Gegenaufklärung bekämpft wird, einer fruchtbareren Methode als die zwangsläufige Unmündigkeit der Betroffenen, wäre die Diskussion grundsätzlich gesperrt. Im negativen Sinn seien hier als Beispiele die Foren 60117, 51884 und 55247 genannt (‚Neue Medizin', AIDS und Impfkritik), im positiven Sinn 49144 (kritische Betrachtung der ‚neuen Medizin') und 58088 (Kinder und Kinderkrankheiten, Impfungen).

[269] Ermert, a.a.O.

[270] Whitaker, 1999, S. 34

ell gängige Praxis ist, sondern auch hier gilt das panoptische Prinzip der bloßen Möglichkeit: handlungsrelevant für den einzelnen ist, was er befürchten oder erwarten kann, und erwartbar ist einerseits alles, was technisch realisierbar ist oder in der Zeit, in der Daten archiviert bleiben, technisch erwartbar sein könnte. Wie in der Folge sanktioniert werden kann, zeigen in einem vergleichsweise milderen Kontext die Beispiele der Berufsverbote in der BRD der 60er, die Ära des McCarthyismus in den USA, die Relevanz der parteilichen Opportunität in der DDR deutlich auf, was machbar ist, als ein extremes Beispiel dagegen sei die aus den unterschiedlichen Datensammlungspraxen resultierende unterschiedliche Effizienz der Judenvernichtung im Dänemark und Norwegen des Dritten Reiches angeführt. Immer größere Bereiche unseres Lebens, unseres Handelns, unserer Kommunikation werden digitalisiert, in der Folge archivierbar, in actu oder noch Jahre später recherchierbar, elektronisch durchsuchbar und beliebig komplexen Algorithmen der Komprimierung und Verknüpfung unterwerfbar. Es soll an dieser Stelle nochmals betont werden, dass es eben nicht um augenblicklich realisierbare Praxen geht, sondern um diese, denen die heute angelegten Logfiles der Provider und der Netzadministratoren theoretisch irgendwann in der näheren Zukunft unterworfen werden können. Bei einer angenommenen Fortsetzung des Mooreschen Gesetzes,[271] welches die Verdoppelung der Rechenleistung bei gleichzeitiger Halbierung der Halbleiterstrukturen im achtzehn - Monate - Rhythmus seit den siebziger Jahren zutreffend voraussagt und einem ähnlich steilen Anstieg der Kapazitäten von Speichermedien, kann man davon ausgehen, dass eine mehr oder minder zentrale Auswertung der anfallenden Datenströme und -archive kein Problem der technischen Realisierbarkeit, sondern eine solche des politischen Willens sein wird.

Während die Datensammler die gewonnenen Vorteile direkt verwerten können, ist ein solcher Vorteil beim Einsatz von Filterprogrammen nicht in dieser Form sichtbar. Bisher bestehende Filter- und Zensurmaßnahmen können momentan noch unterlaufen werden, eine praktikable Möglichkeit der technische Umsetzung einer tatsächlich wirksamen, umfassenden Netzzensur lässt noch auf sich warten. Wenn man bedenkt, dass keine der Filterlösungen das leistet, was sie eigentlich erreichen soll, nimmt es Wunder, dass dennoch derart vehement auf den Einsatz einer nachweislich augenblicklich noch weitgehend wirkungslosen Technik gepocht wird. Martin Rost stellte in der Debate - Mailingliste der fitug die These auf, dass nicht die Wirksamkeit der Filter, sondern die Möglichkeit, ihren Einsatz trotz fehlender technischer Funktionalität durchzusetzen, die eigentlich angestrebte Machtdemonstration ist. Es geht weniger darum, tatsächlich Inhalte zu kontrollieren, sondern darum, sich einen Anschein von Macht zu erhalten, der sich gegen die anarchische Struktur des Internet durchsetzen kann; weiterhin auf der Faktenebene den Anspruch zu wahren, das Internet juristisch kontrollieren zu können. Die oft beschworene Formel ‚was

[271] benannt nach der Prognose eines der Gründer der Prozessorschmiede Intel

offline Unrecht ist, muss auch online Unrecht sein‘ demonstriert so neben dem Fehlen technischen Verständnisses auch das Nichteingestehen der Existenz von Räumen im Internet, die legitimerweise nicht der jeweiligen Jurisdiktion unterworfen werden können.

## 4.4. Gegenbewegungen und ihre Auswirkungen

### 4.4.1. Alternative Netzwerke[272]

Seit versucht wird, Netzinhalte zu kontrollieren und gegebenenfalls zu unterdrücken, gibt es Gegenbewegungen, die diese Kontrolle unterlaufen oder technisch von vorneherein ausschließen wollen. Je nach Gesetzesauslegung sind sie mit einer massiven Rechtsunsicherheit für die Betreiber und/oder NutzerInnen verbunden, was nicht unbedingt von vorneherein eine Kriminalisierung bedeutet, jedoch allein die Möglichkeit, eventuell gegen meist finanzkräftige Gegner oder die Staatsanwaltschaft Prozesse führen zu müssen, wirkt hier kontrollierend.

Auch dieser Form der Unsicherheit wird in vielen Ansätzen begegnet, beispielsweise über Strukturen, mittels der eine Zensur oder Löschung nicht mehr möglich ist, bzw. der physikalische Ort von Daten unbekannt bleibt bzw. ständig wechselt.

Weitere grundsätzliche Schwierigkeiten bei der Etablierung alternativer Netzwerke sind Skalierbarkeit, Schwierigkeit der technischen Umsetzung bei fehlenden Standards, die ‚kritische Masse‘ an Nutzern, Bandbreite und Plattenplatz, die ein alternatives Netz überhaupt erst attraktiv machen, und nicht zuletzt die aus der Entwicklung neuer Netzwerke resultierenden Provozierung von immer umfassenderer Gegenmaßnahmen, die geeignet sind, die Privatsphäre der ‚Normalnutzer‘ wenigstens an kontrollierbareren Punkten immer weiter einzuschränken.

In Kürze sollen hier die drei Hauptströmungen vorgestellt werden, in welche die verschiedenen Ansätze alternativer Netzwerke eingeordnet werden können und die für ‚normale‘ Nutzer auch zugänglich sind.[273]

[272] Möller 2000a-d

[273] so sind gerade beim Tausch copyrightgeschützter Musik auch Firmennetzwerke, Wohnheime und LAN - Partys effektive Umschlagspunkte, stehen aber nicht jedem Nutzer offen. Deshalb sollen sie hier nicht weiter berücksichtigt werden.

### 4.4.2. Zentralisierte Peer - to Peer - Netzwerke

Peer - to - Peer - Netzen ist gemein, dass sie die Hierarchien zwischen Anbietern und Nutzern weiter abflachen. Bei den meisten Netzdiensten kann zwischen Clients und Servern unterschieden werden, also Rechnern, die bevorzugt Anfragen entgegennehmen, und Rechnern, die diese bevorzugt anbieten. So ist ein Browser ein Programm, welches als Client gegenüber Webservern fungiert, d.h. Anfragen an Webserver stellen kann. Diese können im Idealfall die Anfrage beantworten, der Client gibt diese Antwort dann aus.

Im Falle eines Peer - to - Peer - Netzwerks agiert jeder Teilnehmer sowohl als Client als auch als Server. Es gibt keine Masse an Informationssuchenden, welche informationsanbietende Server frequentieren, sondern die Masse der Nutzer stellt gleichzeitig die Ressource dar, aus der die Daten abgeschöpft werden können. Mittels dieses dezentralen Datenaufbewahrungsprinzips wird es erschwert, einzelne Inhaltsanbieter für ihr Angebot zur Verantwortung zu ziehen oder den Zugang zu verhindern.

Problematisch ist jedoch das Auffinden von Daten. Während es im Netz gewöhnlich auf eine relativ einfache Weise unklar ist, wo sich eine bestimmte Datei befindet, stellt sich bei den Peer - to - Peer - Netzen die zusätzliche Frage, wo man überhaupt nach dem Ort einer bestimmten Datei nachzufragen beginnen kann, ganz zu schweigen von der Frage, wie die gesuchte Datei überhaupt heißt.

Eine Lösung dieses Problems besteht in der Wiedereinführung zentraler Instanzen, an die sich jeder Teilnehmer anmeldet. So funktionieren die Musiktauschbörsen Napster und seine Klone nach dem Prinzip einer zentralen Datenbank, an die sich die Nutzer jedes Mal anmelden, wenn sie das Programm starten. Von dort aus wird ihr eigenes Angebot indexiert und anderen NutzerInnen zusammen mit den Angeboten aller eingeloggten Usern dargestellt. Eine Anfrage nach einer bestimmten Datei wird vom Server mit der Liste der Anbieter beantwortet, der eigentliche Datentransfer funktioniert nach diesem Vermittlungsdienst völlig unabhängig von der zentralen Datenbank. Napster beschränkte sich auf Audiodateien im mp3 - Format, mit verschiedenen Tools war diese Beschränkung jedoch auch bei Napster selber zu umgehen. Modifizierte Versionen des Programms erlauben den Tausch beliebiger Dateitypen.

Rechtlich unklar ist, wer sich im Fall des Verbreitens copyrightgeschützten oder illegalem Material strafbar macht. Die letzten Gerichtsurteile stellten den Datenbankbetreiber klar als Verursacher der illegalen Aktivitäten dar und forderten effektive Maßnahmen, um von der Betreiberseite aus die Vermittlung des Transfers von geschütztem Material unmöglich zu machen. Mit den zentralen Datenbanken bleibt ein ‚Single Point of Failure', dessen Betrieb gesperrt oder erschwert werden kann oder auf den der Zugriff providerseitig unterbunden wird. Im Fall von Napster wurde mittels eines Gerichtsbeschlusses erzwungen, dass bestimmte Musiktitel nicht vermittelt werden dürfen. Wie weit mit diesen Filter-

mechanismen das Auffinden und Tauschen der Dateien unmöglich wird, wird sich in den kommenden Wochen und Monaten zeigen. Der von Napster hauptsächlich betroffenen Musikindustrie dürfte Genüge getan sein, wenn der Aufwand, an die letztendlich immer verfügbaren Daten zu kommen, derart ansteigt, dass es sich zumindest für die kaufkräftige Klientel eher lohnt, den Titel zu kaufen anstatt mit hohem Zeitaufwand zu versuchen, ihn kostenlos aus dem Netz zu bekommen.

Ableger desselben Prinzips stehen grundsätzlich vor dem Problem, entweder klein, damit wegen mangelndem Angebot auch unattraktiv zu bleiben, oder groß zu werden und damit automatisch in die Schusslinie der einschlägigen Organisationen wie RIAA*, WIPO*, VG Wort, IFPI* usw. zu gelangen. Private Anbieter solcher Dienste stellen das Angebot aus Angst vor Prozesskosten gewöhnlich auf Aufforderung ein.

### 4.4.3. Dezentrale Peer - to - Peer - Netzwerke

Alternativ dazu wurden in letzter Zeit dezentrale Netzwerke entworfen, in denen die zentrale ‚Meldestelle' wegfällt. Mit Gnutella existiert bereits ein anwendungsreifes System. Beliebige Dateitypen sind tauschbar, ein zentraler Vermittlungspunkt ist nicht mehr notwendig.

Beim Start des Programms auf dem lokalen Rechner schickt Gnutella ein Broadcast - Signal an eine Reihe von IP - Adressen, bis es einen Rechner trifft, welcher auf dem Port Gnutellas antwortet. Die jenem Rechner bekannten Kontaktadressen werden an den anfragenden Rechner übermittelt, mit welchen dann wiederum direkt Kontakt aufgenommen wird. So baut sich ein Netz auf, in dem jeder Rechner die IP-Adressen einer Handvoll anderer Rechner besitzt. Neben der IP werden noch einige Basisdaten übertragen, so Menge und Größe der zur Verfügung gestellten Dateien etc.

Damit mit dem reinen Netzaufbau und - Betrieb nicht die komplette Bandbreite aufgezehrt wird, arbeiten fast alle Anfragen und Dienste mit einem TTL - Code (‚Time To Live'). Eine Suchanfrage nach einem Dateiname wird so beispielsweise mit einer TTL von 7 an alle benachbarten Rechner geschickt. Diese merken sich die Herkunftsadresse, prüfen den eigenen Dateibestand, ob die Datei vorhanden ist und schicken die Anfrage mit einer um 1 verminderten TTL weiter. So wächst die Zahl der angefragten Rechner exponentiell, bis die TTL auf Null abgesunken ist, dann endet sie und alle Rechner, die die Datei besitzen, teilen dies dem anfragenden Rechner unter Angabe ihrer IP mit - man könnte den Anfragemechanismus ein ‚selbstterminierendes Schneeballsystem' nennen.

Die positiven Bescheide nehmen denselben Weg zurück wie die Anfrage und werden beim anfragenden Rechner aufgelistet. Ein Rechner aus der Übermittlungskette vermag

nicht zu erkennen, wer genau die Anfrage gestellt hat, weil jeder Rechner nur seine direkt benachbarten Rechner ‚kennt'. Wenn der anfragende Rechner die gesuchten IP's übermittelt bekommen hat, kontaktiert er diese direkt und ohne den Umweg über die bei der Anfrage zwischengeschalteten Rechner.

Hier wie auch bei Napster ist Anonymität nicht benutzerseitig erzwingbar. Es fehlt zwar eine zentrale Stelle, wo Logs über Downloads geführt werden können, aber für die Anbieterseite ist die IP-Adresse des anfragenden Rechners sichtbar. Ein Auslegen illegaler Köder mit dem Rückverfolgen der Downloader ist somit ohne weiteres möglich.

Systeme wie Freenet oder Publius fügen der Dezentralität noch Anonymität und faktische Unzensierbarkeit hinzu. Freenet gibt nicht gewisse Dateien auf der Festplatte des Nutzers frei, sondern speist sie in einen verteilten Datenpool ein, der auf den Rechnern der Nutzer angelegt wird. Die Inhalte werden zum einen gesplittet, zum andern verschlüsselt und redundant gespeichert.

In einem sehr komplexen Verfahren werden Pfadangaben, mittels derer bestimmte Dateien angefordert werden können, in Prüfsummen umgewandelt, die keinen Aufschluss mehr über die Art der Daten gibt, die angefordert werden. Ebenfalls mit einem TTL - Verfahren wird der die zur Prüfsumme gehörende Datei dann gesucht. Anders als bei Gnutella werden die gefundenen Daten beim Rücktransport auf jedem passierten Rechner wieder gespeichert, so dass häufig angeforderte Daten auch häufiger und somit im Schnitt schneller erreichbar gespeichert werden, andererseits, damit die Daten auch nach und nach eher in den Regionen des Netzes abgelegt werden, wo sie auch häufig abgerufen werden. Für die neu in einen routenden Rechner gespeicherten Daten werden beim Überschreiten der maximalen Kapazität die am längsten unangeforderten Daten gelöscht, so dass Daten nicht dort Platz verschwenden, wo sie nie gesucht werden. So optimiert sich das System topologisch selbst.

Ein Rückverfolgen der Daten zum ‚Einspeiser' ist nicht mehr möglich. Die Verschlüsselung der Daten vor der Einspeisung macht es für die Nutzer unmöglich, herauszufinden, was genau auf ihrer eigenen Festplatte gespeichert ist. Namenskollisionen beim Einspeisen bereits vorhandener Dateien werden beim Upload verhindert, so ist ein Überschreiben einmal eingespeister Daten unmöglich. Die einzige Art, auf die Material verloren gehen kann, ist sein langer Nichtabruf, woraufhin es nach und nach aus den einzelnen Speicherorten herausfällt. Das gezielte Suchen nach ‚umstrittenen' Inhalten fördert dagegen nur ihre weitere Verbreitung.

### 4.4.4. Alternative Namensräume

Es gibt mehrere kommerzielle Versuche, den Internetnamensraum zu erweitern oder alternative Bereiche zu schaffen. Seitens des CCC* erfolgte Ende 2000 die Ankündigung, zumindest ein für den internen Gebrauch funktionsfähiges alternatives Netz aufzubauen, welches eigene Nameserver betreiben würde, die von der Politik ICANNs* unabhängig wären, vor allem in Bezug auf die Gültigkeit amerikanischer Rechtsprechung und dem Markenrecht. Mit Sicherheit wäre ein besserer Schutz vor Entscheidungen gegeben, die einseitig US - amerikanischen Rechtsauffassungen Rechnung tragen; ob es möglich ist, einerseits einen öffentlichen Raum herzustellen, darin öffentlich geltendes Recht aber nicht anzuerkennen, ist jedoch fraglich. Bei dem Projekt des CCC* scheint die Bildung eines internen Netzes wahrscheinlich, eine Öffnung für alle stellt sowohl Betreiber als auch den Staat jedoch vor die Probleme, inwieweit es möglich ist, im Rahmen eines öffentlichen Informationsmediums geltendes Recht für dort nicht anwendbar zu erklären.

Von den kommerziellen Versuchen, Gegen - ICANNs aufzustellen und alternative Namespaces zu errichten, ist diesbezüglich keine Veränderung des legalen Status von Netzinhalten zu erwarten. So versucht ImageOnlineDesign die .web - Domäne in Eigenregie zu vertreiben und existiert ein Konsortium, die mit dem BeatNIC eine alternative Registrierungsinstanz für weitere alternative TLDs* gegen ICANN etablieren will. Während die vom CCC vertretenen Ziele ausdrücklich die einer Abkoppelung von den an Vermarktungsrechten orientierten Kontrollinstanzen des bisherigen Netzes ist, sind die anderen Gegenentwürfe ihrerseits allenfalls als Kapitalisierungsversuche noch ‚unbebauter' Namensraumbereiche zu werten. Eine neue Qualität von Nutzung ist nicht erkennbar.

### 4.4.5. Kryptographie / Steganographie

Kryptografie ist das Mittel der Wahl, wenn verhindert werden soll, dass unbefugterweise Daten von Dritten eingesehen werden können. Populär ist hier vor allem die Verschlüsselungssoftware PGP (Pretty Good Privacy), in der ein Public - Key - Verfahren[274] mit bislang mathematisch nicht brechbarer Verschlüsselung Anwendung findet. Mittels PGP können auch ganze Festplatten verschlüsselt werden.

Aufgrund der Wichtigkeit starker Kryptografie auch und gerade für Regierung und Wirtschaft wird an ihrer weiteren Verbreitung nichts mehr zu ändern sein. Entwürfe exis-

[274] d.h. es existieren zwei Schlüssel, ein öffentlicher und ein geheimer. Der öffentliche Schlüssel ist ein ‚Einwegschlüssel', er eignet sich nur zum Chiffrieren der Nachricht, nicht zur Rückentschlüsselung. Diese ist nur mit dem zweiten Schlüssel möglich.

tieren, nach denen die Offenlegung der Schlüssel durch die Staatsanwaltschaft angeordnet werden kann. Wie bereits erwähnt,[275] nimmt Großbritannien mit der Regelung, die Herausgabe von Schlüsseln gerichtlich anordnen zu lassen, einen sehr weitreichenden Eingriff in die Rechtsprinzipien vor, um Kryptografie kontrollierbar zu halten.

Eine Lösung ist das Verstecken von Daten in unauffälligen anderen Daten, die Steganographie. Hier existieren mittlerweile einige Tools, mit welchen ein Auffinden einer Botschaft im Trägermaterial (einer Bild - oder Tondatei, beispielsweise) unmöglich wird.[276] In der Anwendung ist Steganographie bislang wenig verbreitet, jedoch wird sie juristisch interessante Konsequenzen haben, da der Beweis der reinen Existenz einer Botschaft bereits problematisch wird.

Die grundsätzlichen Probleme dieser Verschlüsselungsmethoden bestehen einerseits darin, dass Privatsphäre keine Grundvoraussetzung ist, sondern ein Zustand, der mit einigem Aufwand hergestellt werden muss und diese Wiederherstellung an das Vorhandensein technischer Kompetenz einerseits und dem Verfügen über entsprechende materiellen Ressourcen andererseits gebunden ist, der Einsatz auf öffentlich zugänglichen Surfterminals scheint absurd. Weiterhin stellt auch Kryptografie keinen vollkommen sicheren Schutz dar, der Angriffspunkt verlagert sich nur vom Brechen der Verschlüsselung auf das Ausspähen der Passworteingabe.

### 4.4.6. Ziele und Motive

Es stellt sich die Frage, ob die Argumentation der ‚freien Rede' angesichts der größtenteils nur zum Tausch copyrightgeschützter Software (incl. Audio- und Videodateien) verwendeten Programme eine reine Alibifunktion besitzt. Die augenblickliche Situation ist die, dass rechtlich umstrittene bis illegale Inhalte auch im ‚gewöhnlichen' Netz zu finden sind und gerade die symbolträchtigsten Dateien im ‚alten' Internet augenscheinlich dem Freenet - Prinzip des ‚je mehr verfolgt wird, desto mehr Angebote werden gemacht' gehorcht - nur nicht automatisiert, sondern durch aktives Handeln der UserInnen selbst.[277]

[275] vgl Medosch, 2000 und oben Kapitel 4.2.3.4.
[276] vgl. Westfeld, 2001
[277] der erste Präzedenzfall war die bereits erwähnte umstrittene Sperrung der linksradikalen Zeitschrift „radikal" durch Compuserve, nachdem die Staatsanwaltschaft mit dieser Anordnung auf die dort veröffentlichten Anleitungen zur Bahnsabotage anlässlich der Castortransporte reagiert hat. „Mein Kampf" kann aktuell nur mit einigen Tricks von deutschen Providern aus bei ebay oder Yahoo ersteigert werden, die elektronische Fassung ist jedoch weit verbreitet und problemlos beispielsweise bei der NSDAP/AO abrufbar. [http://www.cs.cmu.edu/~dst/DeCSS/Gallery/] ist die Heimat der DeCSS -Gallery. DeCSS ist ein Verschlüsselungssystem für DVDs, welches kurz nach dem Erscheinen am Markt geknackt wurde. Der Programmcode wird unter anderem als T-Shirtaufdruck, in Gedichtform oder als Musikstück angeboten, um auf die fließende Grenze zwischen dem Beschreiben eines Algorithmus und der Freiheit der Rede hinzuweisen.

Die vom reinen Datenaufkommen her maßgebliche Nutzung der neuen Tauschmöglichkeiten besteht tatsächlich auch nicht im Propagieren ansonsten zensierter Inhalte, sondern im Aushebeln von Copyrightbestimmungen und der Rechte an geistigem Eigentum. Dieser Prozess ist Teil des bereits dargestellten übergeordneten Konflikts zwischen Gruppen, die Eigentumsfähigkeiten immer weiter ausdehnen wollen, und anderen, die sie zurückdrängen: einerseits durch die Schaffung allgemein kostenfrei und von der direkten Vermarktung ausgeschlossenen Software, andererseits durch die faktische Realisierung einer Kultur des Überflusses, in welcher Software schlicht verfügbar ist, ungeachtet der eigentlich benannten Preise.

Andererseits ist die umgekehrte Schlussfolgerung ebenso zulässig. Während softwareseitig Raubkopieren ein Indiz dafür ist, dass eine Software den Markt dominiert und dementsprechend hohe Absatzzahlen zu erwarten sind, sind auch im Musikbereich die Umsätze mit legal gehandelter Musik und die online getauschten Titel weitgehend im Gleichschritt gestiegen. Ob ein sechzehnjähriger AutoCad - Raubkopierer ein Verlust in fünfstelliger Höhe ist oder ein bereits gewonnener späterer Kunde, ist reine Auslegungssache. Die Folgerung, Raubkopien schmälerten Unternehmensgewinne, ist in dieser Eindeutigkeit auf keinen Fall haltbar.

Diese Betrachtungsweise beschränkt sich auf die Frage, ob eine an sich kriminalisierte Handlung letztendlich für die Betroffenen Nutzen oder Schaden darstellt. Weitet man den Blick auf die gesellschaftliche Dimension dieser neuen Distributionswege, zeigt sich, dass die kriminalisierte Raubkopierszene die eine Hälfte eines Prozesses ist, in dem einerseits versucht wird, mit freier Software und freien Informationen soviel öffentliches Eigentum wie möglich neu zu schaffen; andererseits versucht wird, soviel privates Eigentum in digitaler Form wieder zu kollektivem Eigentum zu machen oder zumindest die faktische Verfügbarkeit herzustellen. So schreibt Möller:

> „Eines sollte deutlich geworden sein: Die einzige Hemmschwelle für das Kopieren des nächsten Mediums nach Text, Bildern und Musik ist die Bandbreite. Wie dann die Dateien letztlich getauscht werden, ist prinzipiell irrelevant."

Mit der Verfügung wird jedoch kein legaler Status hergestellt, was er problematisch findet, da kollektives Wissen zu einer von einzelnen ausbeutbaren Ressource gemacht wird. Das freie Kopieren von Daten dient dem Schutz der Gesellschaft davor, von an sich nicht ‚eigentumsfähigen' Algorithmen zwangsenteignet zu werden.

> „Durch Zensur ist die digitale Evolution nicht aufzuhalten, es sei denn, man zerstört dabei die Technologie. Das wird die Industrieverbände und zelotische Einzelpersonen nicht davon abhalten, Jagd auf Urheberrechtsverletzer zu machen - solange, bis das Gesetz es unmöglich macht. Urheberrechtsgesetze, die nichtkommerzielles Kopieren verbieten, sind in der Internet-Ära gefährlich, so gefährlich wie obsolete Patent- und

> Markenschutzgesetze, die von findigen und skrupellosen Anwälten zur Geldmacherei ausgenutzt werden können.“[278]

Alternative Netzwerke wiederum, die nicht mittels Löschungen und Sperrungen zu kontrollieren sind, stellen eine faktische Versicherung gegen die komplette Zensur von Information dar. Sie sind eine Rückversicherung dafür, dass es bei hinreichendem öffentlichen Interesse an einem Thema unmöglich wird, Informationen total zu kontrollieren.

Dennoch kommt ihnen aktuell ein eher symbolischer Wert zu. Informationen sind auf Multiplikatoren angewiesen, die Kontrolle umfasst gewöhnlich die ‚üblichen’ Kanäle, die von der Masse der Personen verwendet werden.

[278] Möller, 2000d