Alvar C.H. Freude

Ludwig–Blum–Straße 37
70327 Stuttgart

alvar@a–blast.org
http://odem.org/

(01 79) 13 46 47 1

Alvar C.H. Freude | Ludwig-Blum-Straße 37 | 70327 Stuttgart

An die Staatsanwaltschaften
Düsseldorf, Dortmund, Münster, Siegen,
Köln, Bonn, Bochum, Paderborn

Stuttgart, den 21. Januar 2002

Strafanzeige gegen zu ermittelnde Mitarbeiter von Internet–Providern und der Bezirksregierung Düsseldorf

Sehr geehrte Damen und Herren,

hiermit erstatte ich Strafanzeige und stelle – soweit dies nicht von Amts wegen erfolgt – Strafantrag gegen die im folgenden benannten Tatverdächtigen wegen aller in Frage kommenden Delikte aus den auf den folgenden Seiten beschriebenen Sachverhalten.

Ich möchte Sie bitten, die Angelegenheit sorgfältig zu untersuchen und ein Ermitt–lungsverfahren einzuleiten.

Weiterhin bitte ich um Eingangsbestätigung mit Angabe des Aktenzeichens und Mitteilung des Ermittlungsergebnisses nach Verfahrensabschluß.

Sollten Sie technische, inhaltliche oder sonstige Fragen haben, können Sie sich selbstver–ständlich an mich wenden:

E–Mail: alvar@a–blast.org
Telefon: (01 79) 13 46 47 1

Dieses Dokument ist auch im Internet unter der folgenden URL in einer Hypertext–Version abrufbar, um Tipparbeit bei Links zu sparen:

http://www.odem.org/zensur/anzeige/anzeige.html

Mit freundlichen Grüßen

Alvar Freude

Inhaltsverzeichnis

1 Einführung

Einige Internet−Provider, Hochschulen und Forschungseinrichtungen in Nordrhein−Westfalen sperren ausgewählte Internet−Inhalte bzw. leiten Anfragen dieser Seiten auf eigene Inhalte um; weiterhin werden E−Mails, die an bestimmte Empfänger gerichtet sind, auf eigene Server dieser Provider umgeleitet.

Ich habe daher den Verdacht, dass die betreffenden Provider sich der Datenveränderung bzw. Datenunterdrückung nach § 303a StGB und/oder Computersabotage nach § 303b StGB sowie der Verletzung des Fernmeldegeheimnisses nach § 85 TKG und § 206 StGB strafbar machen.

Die Sperrungen von Daten, Veränderungen und Umleitungen gehen auf Initiative von Mitgliedern der Bezirksregierung Düsseldorf zurück.

Daher habe ich den Verdacht, dass sich die unten genannten und evtl. weitere zu ermittelnde Personen sich u.a. der Anstiftung (§ 26 StGB) und Nötigung in einem besonders schweren Fall (§ 240 Absatz 4, Missbrauch der Befugnisse als Amtsträger) schuldig machen.

2 Verdächtigte

Die Strafanzeige richtet sich gegen verantwortliche Mitarbeiter bei den im folgenden genannten Firmen und Institutionen

2.1 Verdacht auf Anstiftung und/oder Nötigung

Mitglieder der Bezirksregierung Düsseldorf mit Amtssitz
Cecilienallee 2
40474 Düsseldorf

Namentlich im Zusammenhang bekannt:

Jürgen Büssow, Regierungspräsident
Jürgen Schütte
Markus Leroch

2.2 Verdacht auf Datenveränderung, Datenunterdrückung, Computersabotage sowie Verletzung des Fernmeldegeheimnisses

Der Verdacht betrifft u.a. zu ermittelnde Mitarbeiter der folgenden und evtl. weiterer ebenfalls zu ermittelnder Internet−Provider, Behörden und Hochschulen

ISIS Multimedia Net GmbH & Co KG
Kaistraße 6
40221 Düsseldorf

Ahrens Online GmbH
Markt 4
59348 Lüdinghausen

Versatel Deutschland GmbH & Co. KG
Unterste−Wilms−Straße 29
44143 Dortmund

Vision Consulting Deutschland oHG
Osterather Str. 7
50739 Köln

RWTH Aachen
Templergraben 55
52056 Aachen

Universität Siegen, HRZ
Hölderlinstr. 3
57068 Siegen

Ruhruniversität Bochum
Universitätsstrasse 150
44801 Bochum

2.3 Versuch bzw. Planung von Datenmanipulation

Die folgenden Unternehmen und Institutionen planen Systeme zur Datenmanipulation und Datenunterdrückung. Sie sollen zum großflächigen Einsatz kommen und die bisherigen Methoden ablösen

webwasher.com AG
Vattmannstraße 3
D−33100 Paderborn

BOCATEL GmbH & Co.
Bonner Centrum für angewandte Telekommunikation KG
Kronprinzenstraße 46
D−53173 Bonn

Universität Dortmund
44221 Dortmund

IntraNet GmbH
Kronprinzenstrasse 46
53173 Bonn

2.4 Angeschriebene Staatsanwaltschaften

Die angeschriebenen Staatsanwaltschaften ergeben sich aus den Anschriften der Verdächtigten:

Generalstaatsanwaltschaft Düsseldorf
Sternwartstraße 31
Postfach 19 01 52
40111 Düsseldorf
Telefax (02 11) 90 16−200

Staatsanwaltschaft Düsseldorf
Postfach 10 11 22
40002 Düsseldorf
Telefax (02 11) 77 07−476

Staatsanwaltschaft Dortmund
Postfach 10 29 42
44029 Dortmund
Telefax (02 31) 926−25090

Staatsanwaltschaft Münster
Postfach 5921
48135 Münster
Telefax (02 51) 494−555

Staatsanwaltschaft Siegen
Postfach 10 12 61
57012 Siegen
Telefax (02 71) 33 73−437

Staatsanwaltschaft Köln
Am Justizzentrum 13
50939 Köln
Telefax (02 21) 477−40 50

Staatsanwaltschaft Bonn
Herbert−Rabius−Straße 3
53225 Bonn
Telefax (02 28) 97 52−600

Staatsanwaltschaft Paderborn
Postfach 25 20
33055 Paderborn
Telefax (0 52 51) 126−555

Staatsanwaltschaft Bochum
Postfach 10 24 49
44724 Bochum
Telefax (02 34) 967−25 87

3 Beschreibung

3.1 Datenunterdrückung durch Provider

Die oben aufgeführten Internet−Service−Provider (ISP) sperren für ihre Kunden entweder den Zugriff auf alle Computer, die den folgenden Domains angehören oder auf einzelne Computer aus den folgenden im Ausland gehosteten Domains:

- rotten.com
- stormfront.org
- front14.org
- nazi−lauck−nsdapao.com

Sowie möglicherweise weitere zu ermittelnde Domains.

Die Sperrungen schließen, zumindest in den mir bekannten Fällen, alle Internet−Protokolle ein. Es wird also der Datenaustausch über das World Wide Web (WWW) mittels des Hypertext Transfer Protocols (HTTP) mit einem Computer innerhalb der betroffenen Domains verhindert oder auf andere Systeme umgeleitet, E−Mails werden blockiert oder zu anderen Systemen und damit anderen Empfängern umgeleitet, eine Kommunikation mittels IRC, ICQ oder anderen Diensten wird pauschal unterdrückt.

Damit wird nicht nur die Informationsfreiheit (§ 5 GG) von Kunden der ISPs drastisch eingeschränkt, sondern jegliche Kommunikation mit den betroffenen Computersystemen unterbunden.

Eine weitere Methode zur Sperrung ist, im Router oder im Firewall die IP−Adressen der zu sperrenden Computersysteme entweder komplett zu sperren, eine Datenverbindung zu dem vom Kunden ausgewählten Zielrechner also auch bei direktem Zugriff unter Umgehung des DNS zu unterbinden, oder einen Zugriff auf solche IP−Adressen durch manipulierte Routing−Tabellen wiederum zu eigenen Servern umzuleiten.

Technisch wird die Sperrung oder Umleitung zumeist mittels gefälschter Einträge im Domain Name System (DNS) bei den Providern erreicht. Details zu den Hintergründen mitsamt Angabe von Quellen der technischen Spezifikationen können Sie Anhang A.1 entnehmen.

Für den Autor dieser Strafanzeige besteht der naheliegende Verdacht, dass sich die betreffenden Internet−Provider aufgrund der Sperrungen bzw. Umleitungen strafbar machen:

- Durch die Sperrung bzw. Manipulation fremder Daten (Umleitung auf andere Inhalte) der Datenveränderung bzw. Datenunterdrückung nach § 303a StGB. Möglicherweise bzw. in speziellen Fällen (siehe unten) auch nach § 303b StGB der Computersabotage.

- Durch die Umleitung und/oder Unterdrückung von E−Mails und anderer persönlicher Kommunikation der Verletzung des Fernmeldegeheimnisses nach § 85 TKG sowie § 206 StGB, insbesondere Absatz 1 und Absatz 2, Nr. 2 (Unterdrückung der Sendung)

Die ISPs sind als Netzwerkbetreiber und bloßer Transporteur der Daten weder Anbieter der betreffenden Daten oder Homepages noch stellen sie diese bereit. Sie sind nach dem Tele−dienstegesetz (TDG) nicht für durchgeleitete Informationen verantwortlich, was in der ak−tuellen Fassung des Gesetzes in § 9 nochmals konkretisiert wurde.

Internet Service Provider, die einen Netzzugang anbieten, fungieren ähnlich wie die Be−treiber der Telefonleitungen oder wie die Post: sie übermitteln Daten und Informationen. Anders als gelegentlich von Laien behauptet ist das Internet in keinster Weise mit dem Rundfunk vergleichbar.

Siehe auch Anlage A.4

Der Verdacht gründet sich unter anderem auf online verfügbare Quellen wie:
http://www.ccc.de/censorship/

Weitere Quellenangaben sind in Anhang A.3 nachzulesen.

3.1.1 Verdacht gegen die ISIS Multimedia GmbH

Die ISIS Multimedia GmbH manipuliert wie oben beschrieben DNS−Einträge der betref−fenden Domains, um einen Datenaustausch mit dem vom Kunden gewählten Server zu verhindern. Eine Auflistung und die Details zu den manipulierten DNS−Einträgen sind in Anlage B.1 nachzulesen.

Anfangs wurden die DNS−Einträge für ISIS−Kunden so manipuliert, dass ein Zugriff auf eine der oben genannten Domains auf die Rechner der Bezirksregierung Düsseldorf umge−leitet wurde. Beispielsweise hatte ein Zugriff auf die Website von Rotten.com (***http://www.rotten.com/***) zur Folge, dass stattdessen auf die Website der Bezirksregierung Düsseldorf zugegriffen wurde. Die Bezirksregierung Düsseldorf wurde so in die Lage ver−setzt, unrechtmäßig Daten über über Benutzer aufzuzeichnen, die diese Website abrufen wollten.

Ebenso wurde die E−Mail−Kommunikation umgeleitet. Auf den Servern der Bezirksregie−rung Düsseldorf sind also E−Mails angekommen, die für andere Empfänger gedacht waren.

In der Zwischenzeit wurden nach Protesten die DNS−Einträge für alle betreffenden Do−mains auf 127.0.0.1 (localhost) gesetzt, Kontaktversuche werden also auf den Computer des Kontaktierenden geleitet.

Quellen:

- Pressemitteilung ISIS:
  http://www.isis.de/presse/textarchiv2001/m011122.htm
- Verschiedene Beiträge im Forum der Bezirksregierung Düsseldorf:
  http://www.brd.nrw.de/cgi–bin/ubb/forumdisplay.cgi?action=topics&number=9
- Anlage B.1
- Angaben zu den DNS–Manipulationen von ISIS:
  http://www.kleinbus.org/news/20011122.html

ISIS ist anscheinend Provider für den Landtag in Nordrhein–Westfalen:
http://www.cisco.com/warp/public/3/de/3–produkte/isp/114–isis.html

Damit trifft die Datenmanipulation bzw. Datenunterdrückung auch die Landtags–abgeordneten und ihre Mitarbeiter.

Aufgrund der aufgeführten Tatsachen ergibt sich der Verdacht, dass die ISIS Multimedia GmbH bzw. deren verantwortliche Mitarbeiter gegen die folgenden Gesetze verstoßen:

1) **§ 303a StGB Datenveränderung und Datenunterdrückung**
   Der Zugriff auf Daten der genannten Computer wurde umgeleitet bzw. ganz unterdrückt
2) **§ 303b StGB Computersabotage**
   Den ISIS–Kunden (u.a. Landtag in NRW) ist der Zugriff auf die beanstandeten Websites sowie auf weitere auf den gesperrten Computersystemen liegende Daten verwehrt
3) **§ 206 StGB Verletzung des Post– oder Fernmeldegeheimnisses**
   Vom Kunden versendete E–Mails werden nicht zugestellt sondern geblockt (Verstoß gegen § 206 StGB Absatz 2, Nummer 2 und Nummer 3) bzw. wurden zur Bezirksregie–rung Düsseldorf umgeleitet (Verstoß gegen § 206 StGB Absatz 1 und Absatz 5)
4) **§ 85 TKG Fernmeldegeheimnis**
   Aufgrund der Umleitung von E–Mails und anderer Kommunikation via Internet an die Bezirksregierung Düsseldorf

3.1.2 Verdacht gegen Ahrens Online GmbH

Ähnlich manipuliert die Ahrens Online GmbH die DNS–Server, um eine Sperrung des Zugriffs auf die betreffenden Computersysteme zu erreichen. Alle Zugriffe werden auf ei–nen Rechner mit der IP–Adresse 193.97.199.5 und dem Namen www10.ahrens.de, der zum Ahrens–Netzwerk gehört, umgeleitet (siehe Anlage B.2 für Details zur DNS–Manipulation).

Ein HTTP–Zugriff auf den Rechner ergibt bei Angabe eines gesperrten Hosts eine lapidare Meldung von Ahrens (siehe auch Anlage C.1):

„Auf Veranlassung der Bezirksregierung Düsseldorf, die der Ahrens Online GmbH am 6. Oktober 2001 zugestellt wurde, haben wir die nebenstehenden Internetpräsenzen dauerhaft gesperrt."

Im HTTP−Header ist ersichtlich, dass diese Datei zum letzten mal am Vormittag des 6. Oktobers 2001 geändert wurde. Details und HTML−Quelltext siehe Anlage C.1.

Gleichzeitig wurde, wie aus Anlage B.2 auf Seite 28 ersichtlich, der sog. MX−Eintrag, der den zuständigen Server für den Empfang von E−Mails bezeichnet, auf mail.ahrens.de gesetzt.

Es wird durch das explizite Setzen des MX−Eintrags bewusst und absichtlich jeglicher E−Mail−Verkehr mit Empfängern der oben genannten Domains auf einen Ahrens−Mailserver umgeleitet. Ahrens macht sich damit bewusst zum Empfänger aller E−Mails, die an eine der oben genannten Domains gerichtet sind.

Aufgrund der aufgeführten Tatsachen ist der Verdacht naheliegend, dass die Ahrens Online GmbH gegen die folgenden Gesetze verstößt:

1) **§ 303a StGB Datenveränderung und Datenunterdrückung**
   Der Zugriff auf Daten der genannten Computer wird umgeleitet, die Informationsfreiheit der Kunden eingeschränkt
2) **§ 303b StGB Computersabotage**
   Je nach Kunden der Ahrens Online GmbH könnte auch der Straftatbestand der Computersabotage erfüllt sein
3) **§ 206 StGB Verletzung des Post− oder Fernmeldegeheimnisses**
   Vom Kunden versendete E−Mails werden anscheinend nicht dem eigentlichen Empfänger zugestellt sondern auf einen Server von Ahrens umgeleitet. Damit dürfte ein Verstoß gegen § 206 StGB Absatz 2, Nummer 1 bis 3 vorliegen. Weiterhin erlangen Mitarbeiter der Ahrens Online GmbH durch die Umleitung unbefugt Zugang zu Informationen über die näheren Umstände von versendeten E−Mails und verstoßen damit gegen § 206 StGB Absatz 5.
4) **§ 85 TKG Fernmeldegeheimnis**
   Aufgrund der Umleitung von E−Mails und anderer Kommunikation

3.1.3 Verdacht gegen die Versatel Deutschland GmbH & Co. KG

Es ist zu lesen, dass auch die Versatel Deutschland GmbH & Co. KG die betreffenden Domains sperrt.

Siehe u.a.:
http://www.ccc.de/censorship/

Eine Anfrage beim Nameserver von Versatel ergab die korrekten IP−Adressen; eine Über−prüfung, ob die entsprechenden IP−Adressen mittels Firewall−Regeln gesperrt oder via Routing−Tabellen umgeleitet werden, ist dem Autor dieser Strafanzeige nicht möglich; dies ist nur innerhalb des Netzwerks der Versatel möglich.

Es wäre mit geeigneten Methoden zu ermitteln, ob dies zutrifft.

Sollte dies der Fall sein, dürften sich auch die verantwortlichen Mitarbeiter der Versatel Deutschland GmbH & Co. KG möglicherweise den bereits genannten Straftatbeständen schuldig machen, da bei einer IP−Sperrung jegliche Kommunikation mit dem betreffenden Server unterbunden wird.

3.1.4 Verdacht gegen die Vision Consulting Deutschland oHG

Die Vision Consulting Deutschland oHG verhindert mittels der oben genannten DNS−Manipulation den Datenaustausch mit Computern in den genannten Domains. Ähnlich wie bei der Ahrens Online GmbH wird mittels gefälschter Einträge im DNS der Kunde beim Aufruf eines Computers der betreffenden Domains auf einen Provider−eigenen Server mit der IP−Adresse 212.102.232.10 und dem Namen www3.vision−net.de umgeleitet; Details zu den Nameserver−Einträgen Finden Sie in Anlage B.3. Der HTTP−Zugriff ergibt die in An−lage C.2 wiedergegebene Antwort.

Da in diesem Fall keine explizite Angabe eines eigenen Mailservers (MX) für die Domains angegeben ist, wird der normale A−Record, also die normale IP−Adresse, herangezogen. Damit werden auch hier wieder E−Mails zu einem falschen Empfänger umgeleitet.

Aufgrund der aufgeführten Tatsachen habe ich den Verdacht, dass die Vision Consulting oHG gegen die folgenden Gesetze verstößt:

1. **§ 303a StGB Datenveränderung und Datenunterdrückung**
   Der Zugriff auf Daten der genannten Computer wird umgeleitet, die Informationsfreiheit der Kunden eingeschränkt
2. **§ 303b StGB Computersabotage**
   Je nach Kunde der Vision Consulting Deutschland oHG könnte auch der Straftatbestand der Computersabotage erfüllt sein
3. **§ 206 StGB Verletzung des Post− oder Fernmeldegeheimnisses**
   Vom Kunden versendete E−Mails werden nicht dem eigentlichen Empfänger zugestellt sondern auf einen Server von Vision umgeleitet. Auch wenn dies hier nicht wie im Fall von Ahrens über spezielle MX−Einträge geregelt ist, wird im Prinzip der gleiche Effekt erzielt. Damit dürfte ein Verstoß gegen § 206 StGB Absatz 2, Nummer 1 bis 3 vorliegen. Weiterhin erlangen Mitarbeiter der Ahrens Online GmbH durch die Umleitung unbefugt Zugang zu Informationen über die näheren Umstände von versendeten E−Mails und verstoßen damit gegen § 206 StGB Absatz 5.
4. **§ 85 TKG Fernmeldegeheimnis**
   Aufgrund der Umleitung von E−Mails und anderer Kommunikation

3.1.5 Verdacht gegen die RWTH Aachen und die Universität Siegen

Laut Berichten u.a. in der Newsgroup de.org.ccc sperren die Universität Aachen und die Universität Siegen Verbindungs−Anfragen zu den oben genannten Domains bzw. den da−zugehörigen IP−Adressen. Der gesamte Thread zu dem Thema ist im Usenet ab Msg−ID 3c14d09b@si−nic.hrz.uni−siegen.de nachzulesen.

Sollten Sie über keinen Zugang zum Usenet oder keinen Newsreader verfügen, ist die Nachricht sowie der gesamte Diskussionsverlauf (Thread) auch im WWW über Google Groups erreichbar:

http://groups.google.com/groups?as_umsgid=3c14d09b%40si−nic.hrz.uni−siegen.de

Auch im Heise−Newsticker wird über die IP−Blockade an der RWTH Aachen berichtet:

http://www.heise.de/newsticker/data/cgl−11.12.01−002/

Sollten sich diese Berichte bestätigen, würde das bedeuten, dass die Hochschulen die ge−samte Kommunikation mit den betroffenen Servern, einschließlich E−Mails, verhindern.

Aufgrund der genannten Berichte ist zu vermuten, dass sich die verantwortlichen Mitar−beiter der beiden genannten Hochschulen der folgenden Delikte schuldig machen:

1. **§ 303a StGB Datenunterdrückung**
   Der Zugriff auf Daten der genannten Computer wird unterdrückt, die Informationsfrei−heit sowie Freiheit von Forschung und Lehre der Mitarbeiter und Studierenden der Hochschulen eingeschränkt
2. **§ 303b StGB Computersabotage**
   Möglicherweise ist auch der Straftatbestand der Computersabotage erfüllt; es wäre zu klären, ob die Computersysteme der gesperrten IP−Adressen von wesentlicher Bedeu−tung für bestimmte Bereiche von Forschung und Lehre sind, beispielsweise für den Fachbereich 3 *Medienwissenschaften* der Universität Siegen.
3. **§ 206 StGB Verletzung des Post− oder Fernmeldegeheimnisses**
   Von Studierenden oder Mitarbeitern der Hochschulen versendete E−Mails werden nicht dem eigentlichen Empfänger zugestellt sondern blockiert; dabei dürfte es sich um einen Verstoß gegen StGB § 206, Absatz 2 Nummer 2 handeln.
4. **§ 85 TKG Fernmeldegeheimnis**
   Firewall−Regeln sind in der Regel so aufgebaut, dass gesperrte Verbindungsanfragen in Protokolldateien (Logfiles) protokolliert werden. Dies wäre mit geeigneten Mitteln zu überprüfen. Sollte dies der Fall sein, liegt nach Ansicht des Autors ein Verstoß gegen TKG § 85 Fernmeldegeheimnis vor. Absatz 1 besagt ausdrücklich, dass sich das Fern−meldegeheimnis auch auf die näheren Umstände erfolgloser Verbindungsversuche er−streckt.

Abgesehen von den rechtlichen Belangen ist äußerst erschreckend, wenn selbst an Hochschulen und wissenschaftlichen Einrichtungen keine Informationsfreiheit gewährt und die wissenschaftliche Arbeit eingeschränkt wird.

Den Verantwortlichen der Universität Aachen ist durchaus bewusst, dass sie gegen die im Grundgesetz garantierte Informationsfreiheit verstoßen und dass die Anordnung der Bezirksregierung Düsseldorf durchaus nicht rechtlich abgesichert ist. Dies geht aus dem Protokoll der Senatssitzung vom 13.12. 2001 hervor, das auszugsweise in Anhang D.1 wiedergeben ist.

3.1.6 Verdacht gegen die Ruhruniversität Bochum

An der Ruhruniversität Bochum sind die Nameserver−Einträge wieder entsprechend geändert: sie zeigen auf 134.147.64.11. Verbindungsversuche via HTTP werden auf die folgende URL umgeleitet:

http://www.ruhr−uni−bochum.de/www−rz/zollehcc/_rz/unzulaessig.htm

Siehe auch:
http://www.bo−alternativ.de/zensur.htm

Auf dieser Seite steht in großer rosa Schrift ausschließlich der folgende Satz:

> *„Der Inhalt der aufgerufenen Webseite ist nach deutschem Recht unzulässig."*

Im normalerweise nicht sichtbaren HTML−Quelltext der Seite steht ein Kommentar, in dem der tatsächliche Grund deutlicher wird:

> *„Auf Anweisung des Regierungspraesidenten wurde der Zugriff gesperrt.*
>
> *Ruhr−Universitaet Bochum*
> *Rechenzentrum*
> *Der Technische Direktor"*

In Anlage C.3 befindet sich der komplette Quelltext der Seite.

Aufgrund der angegebenen Tatsachen vermute ich, dass sich die verantwortlichen Mitarbeiter der Ruhruniversität Bochum der folgenden Delikte schuldig machen:

1. **§ 303a StGB Datenveränderung und Datenunterdrückung**
   Der Zugriff auf Daten der genannten Computer wird umgeleitet, die Informationsfreiheit der Studierenden und der Mitarbeiter eingeschränkt
2. **§ 303b StGB Computersabotage**
   Möglicherweise ist auch der Straftatbestand der Computersabotage erfüllt; es wäre zu klären, ob die Computersysteme der gesperrten IP−Adressen von wesentlicher Bedeutung für bestimmte Bereiche von Forschung und Lehre sind.
3. **§ 206 StGB Verletzung des Post− oder Fernmeldegeheimnisses**
   Vom Kunden versendete E−Mails werden nicht dem eigentlichen Empfänger zugestellt sondern auf einen Server der Ruhruniversität Bochum umgeleitet. Damit dürfte ein Verstoß gegen § 206 StGB Absatz 2, Nummer 1 bis 3 vorliegen. Weiterhin erlangen Mitarbeiter der Ruhruniversität Bochum durch die Umleitung unbefugt Zugang zu Informationen über die näheren Umstände von versendeten E−Mails und verstoßen damit gegen § 206 StGB Absatz 5.
4. **§ 85 TKG Fernmeldegeheimnis**
   Aufgrund der Umleitung von E−Mails und anderer Kommunikation

3.2 Verdacht gegenüber Mitgliedern der Bezirksregierung Düsseldorf

Die Bezirksregierung Düsseldorf ist als letztendliche Urheberin der Sperrungen bekannt. Die Sperrungen wurden aufgrund von Anweisungen und/oder Drohungen durchgeführt.

Herr Jürgen Büssow und andere Mitglieder der Bezirksregierung Düsseldorf möchten bestimmte Internet–Inhalte für Deutschland ausblenden. Sie sind nicht nur der Ansicht, dass es illegal wäre diese von Deutschland aus zu verbreiten, sondern sie möchten auch die Informationsfreiheit der Bürger einschränken und den Zugriff auf bestimmte Inhalte aus dem Ausland mit technischen Mitteln verhindern und fordern Service–Provider auf, diese Inhalte rechtswidrig zu sperren.

Die Informationsfreiheit wird hier insofern eingeschränkt, als die Einfuhr von in Deutschland möglicherweise unzulässigen Inhalten unterbunden wird, nicht aber die Publikation solcher Inhalte. Es handelt sich also nicht um eine Einschränkung der Meinungsfreiheit, sondern um die Verhinderung, sich über Vorgänge im Ausland zu informieren. Durch die technische Sperrung haben Bürger keine Möglichkeit mehr, sich über die Rechtfertigung dieser Sperre eine eigene Meinung zu bilden, wenn sie flächendeckend eingesetzt wird.

3.2.0.1 Aufruf zur Sperrung

Aus dem Heise–Newsticker vom 26. 8. 2000:
http://www.heise.de/newsticker/data/jk–26.08.00–005/default.shtml

> *„Büssow droht mit Strafen bis 500.000 DM; für inhalte ausländischer Provider seien die Leitungsanbieter in Deutschland haftbar.“*

Heise Online, 28. 5. 2001:
http://www.heise.de/newsticker/data/em–28.05.01–000/default.shtml

> *„Büssow droht mit Strafen bis zu 1.000.000 DM: 'Online–Anbietern, die eine Sperrung verweigern, drohten Zwangsgelder bis zu einer Million Mark.'“*

Brief der Bezirksregierung Düsseldorf an die Provider:
http://www.ccc.de/CRD/CRD20011004–NRWLAD.html

Ob auch weitere Sperrungen als die in 3.1 aufgeführen auf Anforderungen der Bezirksregierung hervorgehen wäre zu ermitteln, siehe beispielsweise:

http://www.dailysoft.com/berlinwall/eb.htm

3.2.0.2 Berufung auf den Mediendienstestaatsvertrag

Bei den Sperr−Anordnungen beruft sich die Bezirksregierung auf den Mediendienste−staatsvertrag, der aber nach Ansicht von Experten nicht für Internet Service Providern gilt, die ihren Kunden einen Netzzugang zur Verfügung stellen.

Eine Aufarbeitung des Themas findet sich beispielsweise in dem Telepolis−Artikel „Scharfe Kritik an den rheinischen Sittenwächtern“:

http://www.heise.de/tp/deutsch/inhalt/te/11225/1.html

> *„Der Düsseldorfer Regierungspräsident Jürgen Büssow, der zugleich für die Me−dienaufsicht in Nordrhein−Westfalens zuständig ist und auf die Provider des Landes seit Monaten Druck ausübt, hält seine Aktion allerdings für erfolgreich.*
>
> *[...]*
>
> *Um seine Forderung zu unterstreichen, zunächst vier auf seine Schwarze Liste gesetzte Adressen zu sperren, hat der Regierungspräsident Bußgelder 'bis zu 1 Million Mark' ins Spiel gebracht.*
>
> *[...]*
>
> *Doch unter Rechtsexperten erfreut sich just die entgegen gesetzte Ansicht 'immer stärkerer Beliebtheit', wie Sascha Loetz , wissenschaftlicher Mitarbeiter am Zen−trum für Europäische Integrationsforschung an der Universität Bonn (ZEI) ge−genüber Telepolis erläuterte. Seiner Meinung nach unterliegen Access−Provider dem weniger restriktiven Telekommunikationsgesetz (TKG) – und nicht etwa dem Teledienstegesetz auf Bundes− oder dem MDSV auf Länderebene.*

Es bleiben nach § 2 Absatz 1 MdStV die Regelungen des Telekommunikationsgesetzes (TKG) unberührt, weiterhin gilt der MdStV nach Absatz 2 nur für Verteildienste, nicht aber für Abrufdienste, bei denen der „individuelle Leistungsaustausch oder die reine Übermitt−lung von Daten im Vordergrund steht.

Im Internet steht bei Verwendung des Hypertext Transfer Protokolls (HTTP) eindeutig

a) der individuelle Leistungsaustausch
b) die reine Übermittlung von Daten

im Vordergrund. Punkt b) gilt insbesondere für Service−Provider.

In den genannten Fällen stellen die betreffenden Provider die Daten nicht bereit, sie sorgen nur für einen reibungslosen Datenaustausch. Ihre Aufgabe ist also vergleichbar mit der Post oder einem Telefon−Dienste−Anbieter: Die Post kann ebenso wenig haftbar gemacht wer−den für den Inhalt von Postsendungen die sie transportiert wie die Telekom für den Inhalt von Telefongesprächen.

Quellenangaben zur technischen Spezifikation der Internet−Protokolle wie dem für Web−seiten genutzten HTTP sind in Anhang A.2 zu finden.

Weiterhin ist in § 5 MdStV klar die Verantwortlichkeit benannt: Absatz 3 besagt, dass An−bieter *„für fremde Inhalte, zu denen sie lediglich den Zugang zur Nutzung vermitteln, nicht ver−antwortlich“* sind. Wenn man also annimmt, dass das Internet unter den MdStV fallen würde oder es in Zukunft bestimmte Anwendungen gibt, die einen Mediendienst über das

Internet anbieten, so sind Access–Provider trotzdem nicht für die übermittelten Inhalte verantwortlich, die deren Kunden von fremden Servern abrufen.

Auch nach dem TKG hat die Bezirksregierung Düsseldorf keine Befugnisse, Internet–Provider zu einer Sperrung von unerwünschten Inhalten zu zwingen, wenn diese die Inhalte nicht selbst bereitstellen.

3.2.0.3 Höhe des angedrohten Bußgeldes

Die Bezirksregierung Düsseldorf droht unter Berufung auf den Mediendienstestaatsvertrag mit Strafen bis zu einer Million DM, obwohl dieser in § 20 Absatz 2 ausdrücklich nur Strafen *„bis zu fünfhunderttausend Deutsche Mark“* vorsieht.

Der Betrag von einer Million DM wird u.a. in Pressemitteilungen der Bezirksregierung genannt:

http://www.brd.nrw.de/cat/SilverStream/Pages/presseframe?BeitragsID=6408

3.2.0.4 Nötigung

Ebenso wird aus Pressemitteilungen der Bezirksregierung und der Firma ISIS deutlich, dass die Bezirksregierung ISIS und andere Provider massiv dazu genötigt hat, die gewünschten Sperrungen durchzuführen:

Aus der Pressemitteilung der Bezirksregierung:

> *„Versuch von "ISIS" leider abgebrochen, 12 Provider bleiben bei Sperrung“*
> *[...]*
>
> *„Es ist bedauerlich, dass auf Druck offenbar ganz gezielter Nutzer rechtsradikaler Angebote im Internet die Firma "ISIS" in Düsseldorf auf Selbstregulationsmaßnahmen verzichtet.“*

Quelle:
http://www.brd.nrw.de/cat/SilverStream/Pages/presseframe?BeitragsID=6408

Aus der Pressemitteilung von ISIS:

> *„Doch dies* [temporäre Aufhebung der Sperrung, Anm. des Verfassers] *habe zur Folge gehabt, dass ISIS in der öffentlichen Wahrnehmung plötzlich als Förderer rechten Gedankenguts da stehe, so Schäfers weiter, obwohl lediglich der ursprüngliche Zustand wieder hergestellt worden sei. 'Wir Telekommunikationsunternehmen können in so einer Situation machen was wir wollen, wir sind immer die Dummen. Sperren wir, wird Zensur beklagt. Tun wir nichts, fördern wir angeblich den Rechtsradikalismus', beklagt Schäfers. In dieser Zwickmühle habe er sich dafür entschieden, bis auf Weiteres die fragwürdigen Angebotsseiten zu sperren, auch obwohl bekannt sei, dass mit einfachen Veränderungen der Interneteinstellungen durch den Nutzer diese Hürde überwunden werden könne.“*

Quelle:
http://www.isis.de/presse/textarchiv2001/m011122.htm

Aufgrund dieser beiden Pressemitteilungen dürfte klar sein, dass sich ISIS von der Bezirksregierung zu der Sperre genötigt fühlt.

3.2.0.5 Umgeleitete E-Mails?

In der erwähnten Pressemitteilung der Bezirksregierung steht weiterhin:

> *„'ISIS' hatte negative Reaktionen per E−Mail auf die Sperrung mit einem Link auf die Bezirksregierung Düsseldorf umgeleitet. Die Bezirksregierung geht davon aus, dass es sich nach den Inhalten zahlreicher E−Mails , die sie heute erhalten hat, um die Nutzer rechtsextremistischer Angebote im Internet handelt."*

Aufgrund dieser Sätze und der unter 3.1.1 beschriebenen Umleitungs−Methode kann vermutet werden, dass Mitglieder der Bezirksregierung rechtswidrig E−Mails gelesen haben, die nicht für sie sondern für die gesperrten Empfänger bestimmt waren.

3.2.0.6 Wissen über Nebenwirkungen der Sperr-Methoden

Die von den Providern durchgeführten Sperr−Methoden wurden von der Bezirksregierung empfohlen, wie Teilnehmer der Anhörung in der FITUG−Mailingliste berichteten. Der Bezirksregierung sollten daher auch die Auswirkungen der jeweiligen Sperr−Methoden auf Kommunikations−Dienste sowie unbedenkliche Inhalte bekannt sein; spätestens auf der Anhörung wurden diese unerwünschten Nebenwirkungen erörtert.

Die Mails der FITUG−Mailingliste können im Web−Archiv nachgelesen werden:

http://www.fitug.de/debate/0111/threads.html (Archiv November 2001)
http://www.fitug.de/debate/0111/msg00130.html (Auflistung von Filtermöglichkeiten)

Es wird durch diese Sperrungen als Nebenwirkung aber nicht nur der E−Mail−Verkehr und andere Kommunikations−Protokolle unterbunden, sondern auch grundsätzlich der Zugriff auf alle Webseiten der entsprechenden Domains oder IP−Adressen – auf denen durchaus mehrere vollkommen unterschiedliche Domains gehostet sein können – unterbunden, ohne eine jeweilige Einzelfalluntersuchung durchzuführen.

Insbesondere bei Rotten.com ist dies äußerst problematisch, da dort durchaus viele Webseiten ohne zu beanstandende Inhalte sind. Zu Details siehe Anhang A.5.

3.2.0.7 Verstoß gegen Artikel 5 GG

Die Bezirksregierung gibt an, z.B. im Forum auf ihrer Website, dass durch ihre Maßnahmen die Meinungsfreiheit von Rechtsextremisten und Verbreitern geschmackloser Bilder im Rahmen der durch das Grundgesetz gedeckten Möglichkeiten beschnitten wird. Dies wäre möglicherweise korrekt, wenn sich die Maßnahmen gegen die Urheber richten würden.

Hier wird aber nicht die Meinungsfreiheit des Anbieters, sondern das Recht des sich−informieren−dürfens des Konsumenten beschränkt, also die Informationsfreiheit oder Rezipientenfreiheit der Bürger ebenso wie die Arbeit von Forschung und Lehre.

So umfasst das Recht sich zu unterrichten sowohl die schlichte Informationsaufnahme als auch die aktive Informationsbeschaffung. Ungehindert bedeutet frei von rechtlich angeordneter oder faktisch verhängter staatlicher Abschneidung, Behinderung, Lenkung, Registrierung und sogar *„frei von unzumutbarer Verzögerung“*, wie das Bundesverfassungsgericht in seiner Entscheidung im Fall „Einfuhrverbot / Leipziger Volkszeitung“ entschieden hat (BVerfGE 27, 71). Eine Sperrung von bestimmten Inhalten ist somit nicht verfassungskonform sondern verstößt gegen Artikel 5 GG.

Vergleiche auch:
http://www.jura.uni-duesseldorf.de/dozenten/sachs/sachs/SoSe01/b5.asp

Ähnlich entschied das Bundesverfassungsgericht auch im „Parabolantennen-Urteil“(BVerfG E 90, 27), siehe:
http://www.uni-wuerzburg.de/dfr/bv090027.html

3.2.0.8 Inhaltsfilter allgemein

Weitere Informationen zu Internet-Inhaltsfiltern sind u.a. hier nachzulesen:

http://www.odem.org/insert_coin/kontrolle/fazit.html
http://www.koehntopp.de/kris/artikel/blocking/index.html

3.2.1 Zusammenfassung des Verdachts gegen Mitglieder der Bezirksregierung

- Provider wurden mit Hinweis auf Bußgelder bis zu einer Million DM dazu genötigt, von der Bezirksregierung unerwünschte Inhalte aus dem ausländischen Internet vor Zugriffen aus Deutschland zu sperren.
- Nach MdStV sind aber nur Bußgelder bis zu einer Höhe von 500 000 DM vorgesehen
- Als Begründung für die angedrohte Sperr-Anweisung wird der Mediendienste-staatsvertrag herangezogen, dieser gilt aber nach Expertenansicht nicht für das Internet
- Provider, die keine Sperrung vornehmen, werden der Förderung des Rechtsextremismus bezichtigt
- Es ist klar, dass nicht nur beanstandete Inhalte sondern jegliche Kommunikation mit den betroffenen Servern bzw. Domains unterbunden wird
- E-Mails und andere private Kommunikation wird bzw. wurde zur Bezirksregierung bzw. zu anderen falschen Empfängern geleitet
- Kritiker wurden von der Bezirksregierung pauschal des Rechtsextremismus bezichtigt, was aber offensichtlich (wenn überhaupt) nur in sehr wenigen Fällen der Fall sein dürfte
- Die Einschränkung der Informationsfreiheit der Bürger ist nicht mit dem Grundgesetz vereinbar

Nach Ansicht des Autors missbraucht Herr Büssow die Autorität seines Amtes, um sich politisch als „Kämpfer gegen rechtsradikale Ideologie“ zu profilieren. Tatsächlich wird durch die unrechtmäßigen Sperrungen keine Publikation von rechtsextremen Texten unterbunden, sondern nur der Eindruck erzeugt, dass das was nicht gesehen wird auch nicht existiere. Zudem wurde die Rechtmäßigkeit oder Unrechtmäßigkeit der gesperrten Inhalte nicht gerichtlich geprüft; insbesondere bei Rotten.com ist es sehr zweifelhaft, ob die dort publizierten Inhalte überhaupt rechtlich zu beanstanden sind. Siehe auch die genauere Betrachtung von Rotten.com in Anhang A.5.

3.2.2 Mögliche Straftatbestände

Aufgrund der beschriebenen Tatsachen ist zu untersuchen, ob und inwieweit die eingangs genannten sowie eventuell weitere zu ermittelnde Mitglieder der Bezirksregierung sich möglicherweise folgender und weiterer Straftatbestände schuldig machen:

1. **Anstiftung** (§ 26 StGB) zur Datenunterdrückung, Datenveränderung, Computersabotage, Verletzung des Fernmeldegeheimnisses und anderer Straftaten
2. **Nötigung** (§ 240 StGB) bzw. Nötigung in einem besonders schweren Fall nach § 240 StGB Absatz 4 Nummer 3 (Missbrauch der Stellung als Amtsträger) zur Datenunterdrückung, Datenveränderung, Computersabotage, Verletzung des Fernmeldegeheimnisses und anderer Straftaten
3. Verstoß gegen das das **Fernmeldegeheimnis** nach § 85 TKG
4. **Verletzung des Post– oder Fernmeldegeheimnisses** nach § 206 StGB Absatz 1 Nummer 3 sowie Absatz 5.
5. **Verstoß gegen Artikel 5 Grundgesetz:** Meinungsfreiheit, Zensurverbot; Freiheit von Wissenschaft, Forschung und Lehre: Verstoß gegen GG Artikel 5, Absätze 1 und 3

3.3 Versuch bzw. Planung von Datenmanipulation

Die in 2.3 genannten Unternehmen und Institutionen planen Systeme zur perfektionierten Datenunterdrückung bzw. Datenmanipulation.

Im entsprechenden Strategiepapier zur Inhaltsfilterung und Inhaltsmanipulation wird in Punkt 3.3.2 deutlich die Zielsetzung beschrieben: Blockierung von Daten (Datenunterdrückung) und Manipulation von Daten (Datenveränderung).

Siehe:
http://www.bocatel.de/Docs/2001-1219-Strategiepapier_Filtering1.pdf

Sollte ein solches System etabliert und zur Pflicht für jeden Provider werden, würde dies einen drastischen Eingriff in die Informationsfreiheit bedeuten. Es ist davon auszugehen, dass bei Installation eines solchen Manipulationssystems die Anzahl der zu manipulierenden Sites drastisch ansteigen wird.

Es würde nicht nur die Informationsfreiheit der Bürger, sondern auch die Freiheit von von Presse, Wissenschaft und Forschung eingeschränkt werden. Eine unabhängige Prüfung der gesperrten oder manipulierten Inhalte wäre nicht möglich.

Vor dem Hintergrund von Markenrecht und Urheberschutz ließen sich viele haarsträubende Sperrungen veranlassen.

Als Beispiel sei hier die Telekom genannt, die Anspruch auf alleinige Nutzung des Buchstabens T sowie der Farbe Magenta erhob:

http://www.heise.de/newsticker/data/axv-02.08.01-005/
http://www.heise.de/newsticker/data/axv-26.07.01-001/

Zu weiteren möglichen Folgen siehe beispielsweise auch:
http://www.odem.org/insert_coin/kontrolle/

Aus rechtlicher Sicht ist zu prüfen, ob Planung und Feldversuch bzw. Beauftragung eines solchen Manipulationssystems den Straftatbestand der versuchten Datenveränderung nach StGB § 303a Absatz 1 und 2 sowie der versuchten Computersabotage nach StGB § 303b Absatz 1 und 2 erfüllen.

4 Anhang

Anhang A: Verschiedene Hintergrundinformationen

In diesem Angang sind verschiedene, knappe Hintergrundinformationen zu finden. Sie ersetzen natürlich nicht eine tiefer gehende Recherche sondern können nur einen Anhalts- bzw. Startpunkt für eine solche geben.

Anhang A.1: Domain Name System (DNS)

Computer können im Internet nur mittels ihrer IP-Adresse, einer durch Punkte getrennten Ziffernfolge von vier mal 0-255 (also z.B. 195.143.204.190) angesprochen werden. Dies ist natürlich relativ schwer zu merken, daher wurde mit dem Domain Name System (DNS) eine Methode eingeführt, jedem Computer einen oder mehrere Namen zu geben. In obigem Beispiel könnte so anstatt der IP-Adresse auch der Name gnarzelwicht.delirium-arts.de verwendet werden.

Eine einfache Erklärung zum DNS finden Sie u.a. unter

http://www.netplanet.org/adressierung/dns.html

Bei den eingesetzten DNS-Manipulationen erheben die entsprechenden Provider anstatt der normalerweise zuständigen Name-Server eigene Server zur Autorität über die entsprechende Domain und diese geben auf Anfrage falsche IP-Adressen zurück. Durch diese Verletzung von Internet-Standards wird der Zugriff auf die Original-Computer unterdrückt und stattdessen die Verbindungen mit anderen, meist dem Provider gehörenden, Rechnern aufgebaut.

Details zum DNS finden Sie in den DNS-spezifischen RFCs:

http://www.crynwr.com/crynwr/rfc1035/rfc1035.html
http://www.dns.net/dnsrd/rfc/
http://www.ietf.org/rfc/rfc1034.txt

RFCs sind die technischen Spezifikationen des Internets und können u.a. auf der Website der Internet Engineering Task Force (IETF), der Organisation die die Internet-Standards verabschiedet, nachgeschlagen werden:

http://www.ietf.org/

Anhang A.2: HTTP

Die genaue Definition von HTTP finden Sie in RFC2068

http://www.ietf.org/rfc/rfc2068.txt

Grob gesagt funktioniert es so:
Ein Client (z.B. der Webbrowser eines Internet−Nutzers) fragt beim Server (z.B. www.rot−ten.com) nach einem vom Anwender gewünschten Dokument. Sowohl die Anfrage als auch die Antwort −die vom Server für jeden Abruf individuell zusammengestellt wird (auch wenn dies teilweise aus Anwendersicht nicht so aussieht) − passieren dabei Knotenpunkte, die Anfrage und Antwort weiterleiten, ähnlich wie die Vermittlungsstellen der Telekom Telefongespräche schalten. Dies ist die einzige Stelle, an der die Provider mit den entspre−chenden Daten in Verbindung treten.

Anhang A.3: Weitere Quellen und URLs

In der Regel können ausgehend von den im folgenden genannten Quellen weitere über Links erreicht werden; teilweise sind auch den Leser−Kommentaren weitere Informationen zu entnehmen.

Diplomarbeit des Autors dieser Strafanzeige über Filter, Zensur und Kontrolle im Internet, darin insbesondere die Kapitel über Kontrolle und Zensur:

http://www.odem.org/insert_coin/
http://www.odem.org/insert_coin/kontrolle/

Diverse Artikel bei Heise−Online zum Thema Internet−Sperre in NRW:

http://www.heise.de/newsticker/data/hod−21.11.01−000/
http://www.heise.de/newsticker/data/jk−22.11.01−001/
http://www.heise.de/newsticker/data/anw−22.11.01−003/
http://www.heise.de/newsticker/data/anw−22.11.01−008/
http://www.heise.de/newsticker/data/fr−22.11.01−001/
http://www.heise.de/newsticker/data/anw−05.12.01−001/
http://www.heise.de/newsticker/data/wst−08.12.01−001/
http://www.heise.de/newsticker/data/cgl−11.12.01−002/
http://www.heise.de/newsticker/data/cgl−17.12.01−000/
http://www.heise.de/newsticker/data/mur−20.12.01−001/

Artikel im Online−Magazin Telepolis zur Internet−Sperre in NRW:

http://www.heise.de/tp/deutsch/inhalt/te/11175/1.html
http://www.heise.de/tp/deutsch/inhalt/te/11177/1.html
http://www.heise.de/tp/deutsch/inhalt/te/11188/1.html
http://www.heise.de/tp/deutsch/inhalt/te/11306/1.html
http://www.heise.de/tp/deutsch/inhalt/glosse/11423/1.html

Offenes Forum der Bezirksregierung Düsseldorf (Übersichtsseite):
http://www.brd.nrw.de/cgi−bin/ubb/forumdisplay.cgi?action=topics&number=9

Offener Brief von Dr. Michael Boettcher:
http://www.bezreg−duesseldorf.nrw.de/ubb/Forum9/HTML/000045.html

Bericht im Handelsblatt:
http://www.handelsblatt.com/hbiwwwangebot/fn/relhbi/sfn/buildhbnw/bmc/cn_hnavi_nw/bmname/0/bmc/cn_artcomm_nw/bmc/cn_comm_titel_nw/strucid/PAGE_201525/pageid/PAGE_201527/docid/476066/SH/0/depot/0/cmpl/1/

Bericht bei WDR−Online:
http://online.wdr.de/online/computer/internet/webzensur.phtml

Bericht bei SPIEGEL−Online:
http://www.spiegel.de/netzwelt/politik/0,1518,170019,00.html

Weitere URLs werden in der Online−Version dieser Anzeige bei Bedarf ergänzt.

Anhang A.4: Internet ist nicht Rundfunk

Inhalte aus dem Internet werden zwar zumeist auf Datensichtgeräten dargestellt, die einem Fernseher ähneln: auf Monitoren. Dies sind aber auch schon alle wesentlichen Gemeinsamkeiten zwischen Rundfunk und Internet.

Im Gegensatz z.B. zum Rundfunk und analog zu Telefongesprächen wird jeder Zugriff auf Webseiten einzeln durchgeführt. Während beim Rundfunk ein Sender sendet und beliebig viele Empfänger empfangen können, ist im WWW jeweils eine direkte Kommunikation zwischen Server und Client nötig: Jeder Client fragt beim Server an und erhält eine eigene individuelle Antwort.

Siehe auch Giesbert Damaschke in Internet Professionell:
http://www.damaschke.de/marginal/1997/ip0997.htm

Im Unterschied zum Fernsehen oder Radio ist der Internet−Nutzer aktiv: Er wählt jede Seite und jedes Dokument das er anschauen möchte selbst aus. Im Fernsehen könnte es theoretisch passieren, dass der Zuschauer vom Sender ungewollt mit Nazi−Propaganda berieselt wird − im Internet entscheidet der Nutzer selbst, wann und warum er sich eine Nazi−Site anschauen möchte. Und es ist wohl kaum anzunehmen, dass jemand durch Betrachtung z.B. von ***http://www.nazi−lauck−nsdapao.com/*** zum Nazi wird, das Gegenteil dürfte eher der Fall sein.

Anhang A.5: Gesonderte Betrachtung von rotten.com

Die Domain Rotten.com ist eine der Domains, die von der Bezirksregierung als zu sperrend angegeben wurden. Anders als die übrigen drei Domains sind auf den Rechnern von Rotten.com keine rechtsextremen Inhalte erreichbar.

Es ist eine Site mit mehr oder minder geschmacklosen Bildern von Unfällen bis zu Schieße–reien und peinlichen Fotos von mehr oder minder berühmten Persönlichkeiten.

Eine zufällige Auswahl einiger Beispiele:

http://vatican.rotten.com/easter/
http://coke.rotten.com/french–algeria/
http://vatican.rotten.com/sexcat/
http://coke.rotten.com/dog–knowledge/
http://coke.rotten.com/mother–of–all–sandcastles/
http://coke.rotten.com/john–fu/
http://coke.rotten.com/kashmir/
http://coke.rotten.com/babyseal/
http://vagina.rotten.com/fecaljapan/
http://vagina.rotten.com/childhood/
http://vagina.rotten.com/fish/
http://coke.rotten.com/jesus–with–boy/

Einige dieser Beispiele sind zwar anstößig und möglicherweise „Jugendgefährdend“, dies trifft aber auf keinen Fall auf alle Bilder zu. Trotzdem soll bzw. wird von den genannten Providern der Zugriff auf alle Unterseiten gesperrt (werden).

Zur Domain Rotten.com gehören mindestens die folgenden Computersysteme; bei der eingesetzten DNS–Manipulation wird der Zugriff auf alle Rechner ungeachtet der im ein–zelnen erhältlichen Inhalte gesperrt:

www.rotten.com, coke.rotten.com, vagina.rotten.com, fotm.rotten.com, omerta.rotten.com, vatican.rotten.com, more.rotten.com.

Bei IP–Blockaden wird i.d.R. Nur www.rotten.com gesperrt; nur da drauf liegen keine der zu beanstandenden Bilder. Es wird also der Zugriff auf harmloses Material unterbunden, aber auf die geschmacklosen Bilder, denen die Sperre gelten soll, nicht.

Anhang B: Manipulierte Nameserver-Einträge

Im folgenden sind die manipulierten Nameserver−Einträge aufgeführt, wie sie sich für die Kunden der betreffenden Unternehmen darstellen.

Die Abfragen werden mit dem `nslookup`−Kommando getätigt: Abfrage nach einem Fully Qualifyed Domain Name (FQDN), also z.B. nach computername.beispieldomain.com in der Shell (Windows: Eingabeaufforderung); die Abfragen nach den Zonen−Einträgen innerhalb des `nslookup`−Kommandos nach Start ohne Parameter und Setzen des entsprechenden Servers.

Sie können die Angaben selbst verifizieren: Das `nslookup`−Kommando ist unter Unix−Betriebssystemen (Linux, BSD, ...) sowie unter Windows NT und Windows 2000 verfügbar.

Anhang B.1: ISIS Multimedia GmbH

Abfrage nach www.rotten.com beim ISIS-Nameserver

```
> nslookup www.rotten.com ns.isis.de
Server:  issv0099.isis.de
Address:  195.158.131.2

Name:    www.rotten.com
Address:  127.0.0.1
```

Abfrage des Zonen-Eintrags für rotten.com beim ISIS-Nameserver

Abfrage innerhalb des nslookup−Kommandos:

```
> ls -d rotten.com
[issv0099.isis.de]
$ORIGIN rotten.com.
@                       1D IN SOA       issv0099.isis.de. webmaster.isis.de. (
                                        2001072601      ; serial
                                        13h23m20s       ; refresh
                                        2H              ; retry
                                        1W              ; expiry
                                        1D )            ; minimum

                        1D IN NS        issv0099.isis.de.
                        1D IN A         127.0.0.1
*                       1D IN CNAME     www
www                     1D IN A         127.0.0.1
@                       1D IN SOA       issv0099.isis.de. webmaster.isis.de. (
                                        2001072601      ; serial
                                        13h23m20s       ; refresh
                                        2H              ; retry
                                        1W              ; expiry
                                        1D )            ; minimum
```

Abfrage nach www.stormfront.org beim ISIS-Nameserver

```
> nslookup www.stormfront.org ns.isis.de
Server:  issv0099.isis.de
```

```
Address:  195.158.131.2

Name:    www.stormfront.org
Address:  127.0.0.1
```

Abfrage des Zonen-Eintrags für stormfront.org beim ISIS-Nameserver

Abfrage innerhalb des nslookup–Kommandos:

```
> ls -d stormfront.org
[issv0099.isis.de]
$ORIGIN stormfront.org.
@                       1D IN SOA       issv0099.isis.de. webmaster.isis.de. (
                                        2001072601      ; serial
                                        13h23m20s       ; refresh
                                        2H              ; retry
                                        1W              ; expiry
                                        1D )            ; minimum

                        1D IN NS        issv0099.isis.de.
                        1D IN A         127.0.0.1
*                       1D IN CNAME     www
www                     1D IN A         127.0.0.1
@                       1D IN SOA       issv0099.isis.de. webmaster.isis.de. (
                                        2001072601      ; serial
                                        13h23m20s       ; refresh
                                        2H              ; retry
                                        1W              ; expiry
                                        1D )            ; minimum
```

Abfrage nach www.front14.org beim ISIS-Nameserver

```
> nslookup www.front14.org ns.isis.de
Server:  issv0099.isis.de
Address:  195.158.131.2

Name:    www.front14.org
Address:  127.0.0.1
```

Abfrage des Zonen-Eintrags für front14.org beim ISIS-Nameserver

Abfrage innerhalb des nslookup–Kommandos:

```
> ls -d front14.org
[issv0099.isis.de]
$ORIGIN front14.org.
@                       1D IN SOA       issv0099.isis.de. webmaster.isis.de. (
                                        2001072601      ; serial
                                        13h23m20s       ; refresh
                                        2H              ; retry
                                        1W              ; expiry
                                        1D )            ; minimum

                        1D IN NS        issv0099.isis.de.
                        1D IN A         127.0.0.1
*                       1D IN CNAME     www
www                     1D IN A         127.0.0.1
```

```
@                       1D IN SOA       issv0099.isis.de. webmaster.isis.de. (
                                        2001072601      ; serial
                                        13h23m20s       ; refresh
                                        2H              ; retry
                                        1W              ; expiry
                                        1D )            ; minimum
```

Abfrage nach www.nazi-lauck-nsdapao.com beim ISIS-Nameserver

```
> nslookup www.nazi-lauck-nsdapao.com ns.isis.de
Server:  issv0099.isis.de
Address:  195.158.131.2

Name:    www.nazi-lauck-nsdapao.com
Address:  127.0.0.1
```

Abfrage des Zonen-Eintrags für nazi-lauck-nsdapao.com beim ISIS-Nameserver

Abfrage innerhalb des nslookup–Kommandos:

```
> ls -d nazi-lauck-nsdapao.com
[issv0099.isis.de]
$ORIGIN nazi-lauck-nsdapao.com.
@                       1D IN SOA       issv0099.isis.de. webmaster.isis.de. (
                                        2001072601      ; serial
                                        13h23m20s       ; refresh
                                        2H              ; retry
                                        1W              ; expiry
                                        1D )            ; minimum

                        1D IN NS        issv0099.isis.de.
                        1D IN A         127.0.0.1
*                       1D IN CNAME     www
www                     1D IN A         127.0.0.1
@                       1D IN SOA       issv0099.isis.de. webmaster.isis.de. (
                                        2001072601      ; serial
                                        13h23m20s       ; refresh
                                        2H              ; retry
                                        1W              ; expiry
                                        1D )            ; minimum
```

Anhang B.2: Ahrens Online GmbH

Abfrage nach www.rotten.com beim Ahrens-Nameserver

```
>nslookup www.rotten.com ns.ahrens.de
Server:  ns.ahrens.de
Address:  193.97.199.2

Name:    www.rotten.com
Address:  193.97.199.5
```

Reverse-Lookup 193.97.199.5

```
>nslookup 193.97.199.5
Server:  localhost.delirium-arts.de
Address:  127.0.0.1
```

```
Name:    www10.ahrens.de
Address:  193.97.199.5
Aliases:  5.199.97.193.in-addr.arpa
```

Abfrage des Zonen-Eintrags für rotten.com bei Ahrens

```
> ls -d rotten.com
[ns.ahrens.de]
$ORIGIN rotten.com.
@                       1D IN SOA       ns.ahrens.de. hostmaster.ahrens.de. (
                                        2001100600      ; serial
                                        8H              ; refresh
                                        2H              ; retry
                                        1W              ; expiry
                                        1D )            ; minimum

                        1D IN NS        ns.ahrens.de.
                        1D IN NS        ns2.ahrens.de.
                        1D IN MX        100 mail.ahrens.de.
                        1D IN MX        200 mail.de.uu.net.
                        1D IN A         193.97.199.5
www                     1D IN A         193.97.199.5
@                       1D IN SOA       ns.ahrens.de. hostmaster.ahrens.de. (
                                        2001100600      ; serial
                                        8H              ; refresh
                                        2H              ; retry
                                        1W              ; expiry
                                        1D )            ; minimum
```

Eindeutig ist hier zu Sehen: E–Mails werden an mail.ahrens.de geleitet, wenn dieser Server ausfällt an mail.de.uu.net.

Abfrage von www.stormfront.org bei Ahrens

```
>nslookup www.stormfront.org ns.ahrens.de
Server:  ns.ahrens.de
Address:  193.97.199.2

Name:    www.stormfront.org
Address:  193.97.199.5
```

Abfrage des Zonen-Eintrags für stormfront.org bei Ahrens

```
> ls -d stormfront.org
[ns.ahrens.de]
$ORIGIN stormfront.org.
@                       1D IN SOA       ns.ahrens.de. hostmaster.ahrens.de. (
                                        2001100600      ; serial
                                        8H              ; refresh
                                        2H              ; retry
                                        1W              ; expiry
                                        1D )            ; minimum

                        1D IN NS        ns.ahrens.de.
                        1D IN NS        ns2.ahrens.de.
                        1D IN MX        100 mail.ahrens.de.
```

```
                        1D IN MX        200 mail.de.uu.net.
                        1D IN A         193.97.199.5
www                     1D IN A         193.97.199.5
@                       1D IN SOA       ns.ahrens.de. hostmaster.ahrens.de. (
                                        2001100600      ; serial
                                        8H              ; refresh
                                        2H              ; retry
                                        1W              ; expiry
                                        1D )            ; minimum
```

Abfrage von www.front14.org bei Ahrens

```
>nslookup www.front14.org ns.ahrens.de
Server:  ns.ahrens.de
Address:  193.97.199.2

Name:    www.front14.org
Address:  193.97.199.5
```

Abfrage des Zonen-Eintrags für front14.org bei Ahrens

```
> ls -d front14.org
[ns.ahrens.de]
$ORIGIN front14.org.
@                       1D IN SOA       ns.ahrens.de. hostmaster.ahrens.de. (
                                        2001100600      ; serial
                                        8H              ; refresh
                                        2H              ; retry
                                        1W              ; expiry
                                        1D )            ; minimum

                        1D IN NS        ns.ahrens.de.
                        1D IN NS        ns2.ahrens.de.
                        1D IN MX        100 mail.ahrens.de.
                        1D IN MX        200 mail.de.uu.net.
                        1D IN A         193.97.199.5
www                     1D IN A         193.97.199.5
@                       1D IN SOA       ns.ahrens.de. hostmaster.ahrens.de. (
                                        2001100600      ; serial
                                        8H              ; refresh
                                        2H              ; retry
                                        1W              ; expiry
                                        1D )            ; minimum
```

Abfrage von www.nazi-lauck-nsdapao.com bei Ahrens

```
>nslookup www.nazi-lauck-nsdapao.com ns.ahrens.de
Server:  ns.ahrens.de
Address:  193.97.199.2

Name:    www.nazi-lauck-nsdapao.com
Address:  193.97.199.5
```

Abfrage des Zonen-Eintrags für nazi-lauck-nsdapao.com bei Ahrens

```
> ls -d nazi-lauck-nsdapao.com
[ns.ahrens.de]
$ORIGIN nazi-lauck-nsdapao.com.
```

```
@                       1D IN SOA       ns.ahrens.de. hostmaster.ahrens.de. (
                                        2001100600      ; serial
                                        8H              ; refresh
                                        2H              ; retry
                                        1W              ; expiry
                                        1D )            ; minimum

                        1D IN NS        ns.ahrens.de.
                        1D IN NS        ns2.ahrens.de.
                        1D IN MX        100 mail.ahrens.de.
                        1D IN MX        200 mail.de.uu.net.
                        1D IN A         193.97.199.5
www                     1D IN A         193.97.199.5
@                       1D IN SOA       ns.ahrens.de. hostmaster.ahrens.de. (
                                        2001100600      ; serial
                                        8H              ; refresh
                                        2H              ; retry
                                        1W              ; expiry
                                        1D )            ; minimum
```

Anhang B.3: Vision Consulting Deutschland oHG

Abfrage nach www.rotten.com beim Vision-Nameserver

```
> nslookup www.rotten.com ns.vision-net.de
Server:  ns.vision-net.de
Address:  212.102.232.2

Name:    www.rotten.com
Address:  212.102.232.10
```

Abfrage des Zonen-Eintrags für rotten.com beim Vision-Nameserver

Abfrage innerhalb des nslookup–Kommandos:

```
 ls -d rotten.com
[ns.vision-net.de]
$ORIGIN rotten.com.
@                       1D IN SOA       www blacklist.vision-net.de. (
                                        2001100802      ; serial
                                        1D              ; refresh
                                        2H              ; retry
                                        1W              ; expiry
                                        1D )            ; minimum

                        1D IN NS        ns.vision-net.de.
                        1D IN NS        ns.oberberg-online.de.
                        1D IN A         212.102.232.10
www                     1D IN A         212.102.232.10
@                       1D IN SOA       www blacklist.vision-net.de. (
                                        2001100802      ; serial
                                        1D              ; refresh
                                        2H              ; retry
                                        1W              ; expiry
                                        1D )            ; minimum
```

Abfrage nach www.stormfront.org beim Vision-Nameserver

```
> nslookup www.stormfront.org ns.vision-net.de
Server:  ns.vision-net.de
Address:  212.102.232.2

Name:    www.stormfront.org
Address:  212.102.232.10
```

Abfrage des Zonen-Eintrags für stormfront.org beim VisionNameserver

Abfrage innerhalb des nslookup–Kommandos:

```
> ls -d stormfront.org
[ns.vision-net.de]
$ORIGIN stormfront.org.
@                       1D IN SOA       www blacklist.vision-net.de. (
                                        2001100802      ; serial
                                        1D              ; refresh
                                        2H              ; retry
                                        1W              ; expiry
                                        1D )            ; minimum

                        1D IN NS        ns.vision-net.de.
                        1D IN NS        ns.oberberg-online.de.
                        1D IN A         212.102.232.10
www                     1D IN A         212.102.232.10
@                       1D IN SOA       www blacklist.vision-net.de. (
                                        2001100802      ; serial
                                        1D              ; refresh
                                        2H              ; retry
                                        1W              ; expiry
                                        1D )            ; minimum
```

Abfrage nach www.front14.org beim Vision-Nameserver

```
> nslookup www.front14.org ns.vision-net.de
Server:  ns.vision-net.de
Address:  212.102.232.2

Name:    www.front14.org
Address:  212.102.232.10
```

Abfrage des Zonen-Eintrags für front14.org beim Vision-Nameserver

Abfrage innerhalb des nslookup–Kommandos:

```
> ls -d front14.org
[ns.vision-net.de]
$ORIGIN front14.org.
@                       1D IN SOA       www blacklist.vision-net.de. (
                                        2831138838      ; serial
```

```
                                1D              ; refresh
                                2H              ; retry
                                1W              ; expiry
                                1D )            ; minimum

                        1D IN NS        ns.vision-net.de.
                        1D IN NS        ns.oberberg-online.de.
                        1D IN A         212.102.232.10
www                     1D IN A         212.102.232.10
@                       1D IN SOA       www blacklist.vision-net.de. (
                                2831138838      ; serial
                                1D              ; refresh
                                2H              ; retry
                                1W              ; expiry
                                1D )            ; minimum
```

Abfrage nach www.nazi-lauck-nsdapao.com beim Vision-Nameserver

```
> nslookup www.nazi-lauck-nsdapao.com  ns.vision-net.de
Server:  ns.vision-net.de
Address:  212.102.232.2

Name:    www.nazi-lauck-nsdapao.com
Address:  212.102.232.10
```

Abfrage des Zonen-Eintrags für nazi-lauck-nsdapao.com beim ISIS-Nameserver

Abfrage innerhalb des nslookup–Kommandos:

```
> ls -d nazi-lauck-nsdapao.com
[ns.vision-net.de]
$ORIGIN nazi-lauck-nsdapao.com.
@                       1D IN SOA       www blacklist.vision-net.de. (
                                2001100802      ; serial
                                1D              ; refresh
                                2H              ; retry
                                1W              ; expiry
                                1D )            ; minimum

                        1D IN NS        ns.vision-net.de.
                        1D IN NS        ns.oberberg-online.de.
                        1D IN A         212.102.232.10
www                     1D IN A         212.102.232.10
@                       1D IN SOA       www blacklist.vision-net.de. (
                                2001100802      ; serial
                                1D              ; refresh
                                2H              ; retry
                                1W              ; expiry
                                1D )            ; minimum
```

Anhang C: Seiten mit Sperr-Hinweisen

Provider, die Zugriffe auf Seiten mit einer Sperr–Meldung umleiten, nehmen in diesen Sperr–Seiten i.d.R. Bezug auf die Bezirksregierung Düsseldorf. Daraus ist ersichtlich, dass es eine Sperr–Anordnung der Bezirksregierung gab.

Anhang C.1: Sperr-Seite der Ahrens Online GmbH

HTML–Quelltext der Sperr–Seite inklusive Kommandos zum Abruf eben dieser Seite und HTTP–Header der Antwort:

```
>telnet 193.97.199.5 80
Trying 193.97.199.5...
Connected to www10.ahrens.de.
Escape character is '^]'.
GET / HTTP/1.1
Host: www.rotten.com

HTTP/1.1 200 OK
Server: Microsoft-IIS/4.0
Content-Location: http://www.rotten.com/index.htm
Date: Mon, 14 Jan 2002 18:28:12 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Sat, 06 Oct 2001 10:37:01 GMT
ETag: "303c4fd5524ec11:4460"
Content-Length: 2430

<html>

<head>
<meta http-equiv="Content-Language" content="de">
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<meta name="GENERATOR" content="Microsoft FrontPage 4.0">
<meta name="ProgId" content="FrontPage.Editor.Document">
<title>Gesperrt durch die Bezirksregierung Düsseldorf.</title>
</head>

<body bgcolor="#FFFF00">

<p align="center"><b><font face="Arial" size="5">Sie haben eine gesperrte Seite
aufgerufen!</font></b></p>
<table border="1" width="100%" cellspacing="18" cellpadding="6">
  <tr>
    <td width="50%" valign="top" bgcolor="#FFFFFF"><font face="Arial" size="3">Auf
      Veranlassung der Bezirksregierung Düsseldorf, die der Ahrens Online GmbH
      am 6. Oktober 2001 zugestellt wurde, haben wir die nebenstehenden
      Internetpräsenzen dauerhaft gesperrt.</font>
      <p><font face="Arial" size="3">Diese Angebote sind unzulässig, weil
sie</font></p>
      <ul type="square">
        <li><font face="Arial" size="2">gegen Bestimmungen des Strafgesetzbuches
          verstoßen</font></li>
        <li><font face="Arial" size="2">den Krieg verherrlichen</font></li>
```

```
        <li><font face="Arial" size="2">geeignet sind, Kinder und Jugendliche
          sittlich schwer zu</font></li>
        <li><font face="Arial" size="2">gefährden</font></li>
        <li><font face="Arial" size="2">die Menschenwürde verletzen</font></li>
        <li><font face="Arial" size="2">gegen die verfassungsmäßige Ordnung,
          allgemeine Gesetze und</font> <font face="Arial" size="2">Bestimmungen
          zum Schutz der persönlichen Ehre verstoßen.</font></li>
      </ul>
      <p><font face="Arial" size="3">Wir bitten um Ihr Verständnis!</font></p>
      <p><b><font face="Arial" size="3">Ahrens Online GmbH<br>
      </font><font face="Arial" size="1">Ihr Internetprovider im Münsterland<br>
      <br>
      </font></b><font face="Arial" size="3">Markt 4, <br>
      59348 Lüdinghausen<br>
      Telefon 02591-5008 mo-fr 9-14 Uhr</font></p>
      <p><font face="Arial" size="3">Email an <a
href="mailto:online@ahrens.de">online@ahrens.de</a>
      </font></td>
    <td width="50%" valign="top" bgcolor="#FFFFFF"><b><font color="#FF0000"
face="Arial" size="4">www.front14.org<br>
      www.stormfront.org<br>
      www.nazi-lauck-nsdapao.com<br>
      www.rotten.com<br>
      </font></b></td>
  </tr>
</table>

</body>

</html>
```

Anhang C.2: Sperr-Seite der Vision Consulting Deutschland oHG

HTML–Quelltext der Sperr–Seite inklusive Kommandos zum Abruf eben dieser Seite und HTTP–Header der Antwort:

```
>telnet 212.102.232.10 80
Trying 212.102.232.10...
Connected to www3.vision-net.de.
Escape character is '^]'.
GET / HTTP/1.1
Host: www.rotten.com

HTTP/1.1 200 OK
Date: Mon, 14 Jan 2002 19:44:51 GMT
Server: Apache/1.3.19 (Unix) PHP/4.0.4pl1
X-Powered-By: PHP/4.0.4pl1
Transfer-Encoding: chunked
Content-Type: text/html

822
<html>
<head>
<title>Routing Denied</title>
```

```
</head>

<body text="#000000" bgcolor="#FFFFFF">
<table width=80% height=80% align=center><tr><td>
<font face="Arial,Verdana" size="6">Die von Ihnen gew&uuml;nschte Seite wird nicht
angezeigt.</font>

<br><br>
<font face="Arial,Verdana" size="3">Sinngem&auml;&szlig;er Auszug aus dem Medien-
dienstestaatsvertrag (MdStV) vom 17.Sept. 1997 (GVBB1. 1997)
<br><br>
Angebote im Internet sind unzul&auml;ssig, wenn sie
<ol type="1">
<li><font size="3" face="Arial,Verdana">gegen Bestimmungen des Strafgesetzbuches
versto&szlig;en (§ 8 Abs. 1 Nr. 1 MdStV),</font></li>
<li><font size="3" face="Arial,Verdana">den Krieg verherrlichen (§ 8 Abs. 1 Nr. 2
MdStV),</font></li>
<li><font size="3" face="Arial,Verdana">offensichtlich geeignet sind, Kinder oder
Jugendliche sittlich schwer zu gef&auml;hrden (§ 8 Abs. 1 Nr. 3
MdStV),</font></li>
<li><font size="3" face="Arial,Verdana">Menschen, die sterben oder schweren
k&ouml;rperlichen oder seelischen Leiden ausgesetzt sind oder waren, in einer die
Menschenw&uuml;rde verletzende Weise darstellen und ein tats&auml;chliches Ge-
schehen wiedergeben, ohne dass ein &uuml;berwiegendes berechtigtes Interesse ge-
rade an dieser Form der Berichterstattung vorliegt; eine Einwilligung ist unbe-
achtlich (§ 8 Abs. 1 Nr. 4 MdStV),</font></li>
<li><font size="3" face="Arial,Verdana">in sonstiger Weise die Menschenw&uuml;rde
verletzen (§ 8 Abs. 1 Nr. 5 MdStV),</font></li>
<li><font size="3" face="Arial,Verdana">gegen die verfassungsm&auml;&szlig;ige
Ordnung, gegen die allgemeinen Gesetze und gegen die gesetzlichen Bestimmungen zum
Schutz der pers&ouml;nlichen Ehre versto&szlig;en (§ 7 Abs. 1 MdStV).</font></li>
</ol></font>
<br><br>

<table border=0 width=100% cellspacing=10><tr>
 <td><a href="http://www.vision-net.de"><img src="visionlogo.gif" border="0"
alt="Vision Consulting Deutschland OHG"></a></td> <td align=right><a
href="http://www.oberberg.net"><img src="oois-logo.jpg" border="0" alt="Oberberg-
Online Informations Systeme GmbH"></a>
</td>
</tr></table>

</td></tr></table>
</body>
</html>
```

Anhang C.3: Sperr-Seite der Ruhruniversität Bochum

HTML–Quelltext der Sperr–Seite der Ruhr–Uni Bochum:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
    "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
  <meta http-equiv="Content-Type" content="text/html">
```

```
  <title>Webseite mit rechtlich unzulässigem Inhalt</title>
  <!--
  Der Inhalt der aufgerufenen Webseite ist nach deutschem Recht unzulaessig.
  Auf Anweisung des Regierungspraesidenten wurde der Zugriff gesperrt.

  Ruhr-Universitaet Bochum
  Rechenzentrum
  Der Technische Direktor
  -->
</head>

<body lang="DE" bgcolor="aqua">

<div>

<table border="0" cellspacing="0" cellpadding="0">
  <tbody>
    <tr>
      <td width="757" valign="top"><strong><span
        style="font-style: normal; color: #FF00FF; font-size: 60pt; font-family:
courier">
        Der Inhalt der aufgerufenen Webseite ist nach deutschem Recht
        unzulässig.</span></strong></td>
    </tr>
  </tbody>
</table>
</div>
</body>
</html>
```

Anhang D: Sonstige Quellen

Anhang D.1: Auszug aus dem Protokoll der Senatssitzung vom 13.12. 2001 der RWTH Aachen

Quelle:

Msg−ID 3C4AB461.7080700@gmx.de im Usenet (Newsgroup rwth.general)

Im WWW z.B. via Google−Groups nachlesbar:

http://groups.google.com/groups?as_umsgid=3C4AB461.7080700%40gmx.de

„Top 9 Bericht des Rektors“

[..]

> „Außerdem wird aus der Gruppe der Studierenden bezüglich der Sperrung von vier Webadressen nachgefragt, insbesondere, aus welchem Grund die Bezirksregierung Düsseldort zuständig sei. Der Kanzler führt aus, vor ca. vier Wochen sei ihm von der Bezirksregierung Düsseldorf, die nach dem Medienstaatsvertrag zwischen den deutschen Bundesländern zuständig sei,

eine Ordnungsverfügung angekündigt worden, mit der der Hochschule aufgegeben werde, den Zugang zu vier Seiten im Internet zu sperren, da diese rechtsradikalen und damit strafbaren Inhalt verbreiten würden. Bei einer Anhörung seien überwiegend technische Fragen erörtert worden. Die Bezirksregierung hab eine Arbeitsgruppe eingesetzt, um die technischen Möglichkeiten einer Sperrung dieser Seiten zu klären. Wegen des Inhalts der Seiten habe er Professor Bischof vom Rechen− und Kommunikations−zentrum gebeten, den Zugang zu diesen Seiten über den Hochschul−Server zu sperren. Es sei allerdings denkbar, dass diese Sperrung gegen das Grundrecht auf Informationsfreiheit (Art. 5 des Grundgesetzes) verstoße. Allerdings finde dieses Grundrecht seine natürlichen Schranken unter an−derem in der Strafgesetzgebung, aber auch in einer Konkretisierung der Netzordnung der Hochschule, die eine Nutzung der Seiten nicht erlaube. Aus diesem Grunde sei bisher davon abgesehen worden, diese Seiten wie−der zu öffnen.

Aus der Gruppe der Studierenden wird angemerkt, dass an der RWTH eventuell auch zum Thema "Rechtsradikalismus im Internet" geforscht werde. Der Kanzler antwortet, für spezielle Forschungszwecke könne über geeignete Mittel der Zugang gegebenenfalls wieder geöffnet werden.

Die Studierenden biten, künftig über die Sperrung von Internet−Seiten besser und ausführlicher informiert zu werden.“