

## **Fighting illegal internet content – May access providers be required to ban foreign websites? A recent German approach.**

*by Pascal H. Schumacher<sup>1</sup>*

### **1 Introduction**

The internet provides a free flow of all kinds of information and remarkable means of communication. At the same time, these opportunities have significant drawbacks as well. In particular there is the possibility that the power of the internet will be abused by the imparting of undesirable content. The internet is being (ab)used as a platform for anti-constitutional content and morally harmful information for adolescents. The widespread impact of such information may even exceed that of the conventional media.

In reaction to this, the federal government and states have introduced the “States Treaty covering Media Services” and the “Act on the Utilization of Tele Services” (briefly “Tele Services Act”) in 1997. These laws provide comprehensive instruments for the public supervision of media- and tele services. But so far, the district governments – being responsible for internet regulation – have declined to exercise their sovereign control. Especially their power to prohibit or ban illegal content has not been exercised. Now, it seems as though a turning point in this matter has been reached. On October 18<sup>th</sup> 2001, the Düsseldorf district government, being responsible for the federal state of North Rhine-Westphalia, asked the local access providers to block the access to four websites, hosted in the USA, because they contained material that was “harmful for adolescents”<sup>2</sup>. After hearing the 80 concerned access providers, the district government finally decreed the blocking of only two American websites with racist and anti-Semitic content<sup>3</sup> on February 6<sup>th</sup> 2002<sup>4</sup>. About

---

<sup>1</sup> Author works for the Institute for Information-, Telecommunications- and Media Law (ITM) in Münster (Germany).

<sup>2</sup> <http://www.front14.org> , <http://www.stormfront.org> , <http://www.nazi-lauck-nsdapao.com> and <http://www.rotten.com> .

<sup>3</sup> <http://www.stormfront.org> and <http://www.nazi-lauck-nsdapao.com> .

<sup>4</sup> The blocking order is available on [http://www.nps-brd.nrw.de/BezRegDdorf/autorenbereich/Dezernat\\_21/PDF/39sperrverf\\_022002.pdf](http://www.nps-brd.nrw.de/BezRegDdorf/autorenbereich/Dezernat_21/PDF/39sperrverf_022002.pdf) .

half of the providers followed the decree. The other half filed an objection. The district government however dismissed the objection on July 22<sup>nd</sup> 2002.

These blocking decrees have triggered off a controversy about the providers' legal responsibility in general and especially the access providers' responsibility for web content. Lobbyist groups, such as the German Chapter of the Internet Society (ISOC.DE) and the Association of the German Internet Economy (eco-forum e.V.), have articulated indignation towards the district government's measures<sup>5</sup>. The decrees have been labeled as public censorship and calls for protection of freedom of expression have risen<sup>6</sup>.

Instead of blocking decrees, critics claim to rely upon the providers' voluntary self-regulation and an improvement of the users' media-competence. On the other hand, the German protestant church explicitly supported the decision, because "finally somebody dares to involve the internet in the public debate on media-ethical and media-political responsibilities"<sup>7</sup>. Some authors have even described the decrees as "reasonable measures of regulation in a stable democracy and healthy community"<sup>8</sup>.

It might be the political explosiveness of the topic that has recently set off a great number of comments and statements. In the following report, the various aspects of this controversial argument will be portrayed, discussed and evaluated along with the current problems.

## **2 Legal Basis**

The district authority supports its procedure on the legal basis of § 22 (2) of the States Treaty on Media Services. § 22 authorizes it to act when the treaty is being violated. The authority may especially prohibit internet services and order their blocking. In the literature, the recourse to § 22 of the treaty as legal basis has had to bear strident criticism.

For instance, many authors maintain that access providers do not supply media services in the sense of the states treaty at all. One can find a range of qualifications of their activity: They have been classified as tele-, media- and even as telecommunication-service providers.

---

<sup>5</sup> <http://www.isoc.de/presse/index.htm> .

<sup>6</sup> Compare among others *Krempel*, in: Telepolis, available on: <http://www.heise.de/tp/deutsch/inhalt/buch/13265/1.html> .

<sup>7</sup> *Schütte*, in: NJW 23/2002 Editorial.

<sup>8</sup> *Mankowski*, Die Düsseldorfer Sperrverfügung – Alles andere als rheinischer Karneval, in: MMR 2002, p. 277.

Depending on their classification, they respectively fall under either to the States Treaty on Media Services, to the Tele-Services Act or the Telecommunications Act.

## **2.1 Access providers as telecommunication service providers**

First, there is a strict distinction between telecommunication services on the one hand and tele- and media services on the other. This separation is due to the fact that the technical procedures of telecommunication are set down in the Telecommunications Act, whereas the States Treaty on Media Services and the Tele Services Act contain rules for the general content of Information- and Communication-Services (IaC-Services) and their application<sup>9</sup>.

§ 3 No. 18 of the Telecommunications Act defines telecommunication services as “the commercial offer of telecommunication including the offer of transmission paths”. Telecommunication is hence the “technical procedure of transmitting, forwarding and receiving messages of any kind in form of signs, language, pictures or sounds” (§ 3 No. 16 Telecommunications Act).

In order to categorize access providers, the content of their service has to be specified first. The access provider offers a distinct form of data-transmission that allows the user to access a computer network. Besides this dial-up via the public telephone network, the access provider makes the log-functions available, which is indispensable for using the network. This includes especially the IP-address, the name service and the so-called routing<sup>10</sup>. Hereby, the access provider’s service exceeds the so-called network provider. The latter only provides transmission paths and –capacities, whereas the access provider makes the user’s computer become part of the communication network<sup>11</sup>. Nonetheless, the access provider does not supply IaC-Services in the sense of the States Treaty on Media Services or the Tele Services Act per se; only it’s facilities enable the user to finally receive such services. It provides part of the “technical telecommunication basis”<sup>12</sup> that precedes the use and application of Information- and Communication-Services. Therefore, access providing fits the definition of telecommunication according to § 3 No. 16 Telecommunications Act. As far as this service is offered commercially, the access provider supplies a telecommunication service that is subordinated to the Telecommunications Act.

---

<sup>9</sup> *Roßnagel*, Neues Recht für Multimediadienste, in: NVwZ 1998, p. 2 (3).

<sup>10</sup> *Koenig/Loetz*, Sperrungsanordnungen gegenüber Network- und Access-Providern, in: CR 1999, p. 438 (439).

<sup>11</sup> [http://www.nps-brd.nrw.de/BezRegDdorf/autorenbereich/Dezernat\\_21/PDF/39sperrverf\\_022002.pdf](http://www.nps-brd.nrw.de/BezRegDdorf/autorenbereich/Dezernat_21/PDF/39sperrverf_022002.pdf) , p. 2.

<sup>12</sup> *Koenig/Loetz* (footnote 10), p. 439.

## 2.2 Is the States Treaty applicable to access providers?

The strict separation of telecommunication services on the one hand and media- and tele services on the other, is likely to lead to the conclusion that neither the States Treaty on Media Services, nor the Tele Services Act are applicable to access providers. Assuming this, the district government basing its decree upon § 22 of the States Treaty would have acted incorrectly. Yet, § 3 No. 1 of the States Treaty on Media Services, legally defining the term “services supplier” of IaC-Services, could impede this assumption. In this context it is crucial to know, whether the notion of “service suppliers” as it is defined in § 3 No. 1 also includes access providers. And if so, how does this affect the principle of strict separation between Telecommunication- and IaC-Services?

“Service supplier” in the sense of § 3 No. 1 of the States Treaty on Media Services is every natural or juridical person, either holding her own or someone else’s media services ready for use or simply supplying access for the utilization of media services to the user<sup>13</sup>. An access provider might fit the last alternative of supplying access to media services. The Düsseldorf district government interprets the definition of “service supplier” this way<sup>14</sup>. *Spindler, Volkmann* and *Meier* share this view<sup>15</sup>: They principally understand the notion of “supplying access” in the sense of § 3 No. 1 as technical realization of entering the internet for example via telephone lines. This service being characteristic for access providers, they therefore subsume them under this definition.

On the other hand *Germann* and *Greiner* contradict this interpretation<sup>16</sup>, explicitly referring to the strict separation between Telecommunication- and IaC-Services: The merely technical procedure of providing access simply lacks any component with regards to the content of information, which is just typical for IaC-services. Therefore, neither the States Treaty on Media Services, nor the Tele Services Act could apply to access providers. In *Greiner’s* view, the notion of “supplying access” only includes services that have a specific relation to the content of information such as navigation support. This would especially be search engines and thematically arranged hyperlink lists<sup>17</sup>. However, the obviously biggest weakness of this view is the wording of § 3 No. 1 of the States Treaty on Media Services.

<sup>13</sup> *Meier*, in: Roßnagel, Recht der Multimedia-Dienste, 4<sup>th</sup> part § 3 no. 6.

<sup>14</sup> [http://www.nps-brd.nrw.de/BezRegDdorf/autorenbereich/Dezernat\\_21/PDF/39sperrverf\\_022002.pdf](http://www.nps-brd.nrw.de/BezRegDdorf/autorenbereich/Dezernat_21/PDF/39sperrverf_022002.pdf), p. 6.

<sup>15</sup> *Spindler/Volkmann*, Die öffentlich-rechtliche Störerhaftung der Access-Provider, in: K&R 2002 p. 398 (399); *Meier*, in: Roßnagel, Recht der Multimedia-Dienste, 4<sup>th</sup> part § 3 Rn. 18.

<sup>16</sup> *Greiner*, Sperrungsverfügungen als Mittel der Gefahrenabwehr im Internet, in: CR 2002 p. 620 (621);

*Germann*, Gefahrenabwehr und Strafverfolgung im Internet, Berlin 2000, p. 446.

<sup>17</sup> *Greiner*, Die Verhinderung verbotener Internetinhalte im Wege polizeilicher Gefahrenabwehr, Hamburg 2001, p. 75.

According to it, everybody who “supplies access for the use” of even somebody else’s media services is covered by the law. Singularly taking into consideration this wording, the access provider fits the definition clearly. On the other hand it remains debatable, whether the latter arguments suggest and justify a restrictive interpretation of the law in a way that excludes access providers from the definition. At first sight, the strict principle of separation between Telecommunication- and IaC-Services seems to favour this approach. Yet, one must also take into account the legal intention of § 3 No. 1 which does not claim to define access providing as a tele- or media service at all. It refers rather to (juridical) persons who supply access to *someone else’s* IaC-Service. For this reason, there is no fundamental contradiction with the principle of separation. Furthermore a systematic analysis of the States Treaty on Media Services reveals that access providers are covered very well: The §§ 7 ff. of the treaty exempt providers from any liability for “unfamiliar information that they transmit in a communication network or supply access to”, as long as they do not “arrange the transmission, choose the addressee and select or modify the transmitted information”. These restrictions of liability definitely refer to access providers, especially since neither content- nor service providers can be meant: Content providers publish their own content and therefore *select the transmitted information* of course. Service providers hold someone else’s information ready for use and thus *select* the transmitted information as well. The restrictions to liability can therefore neither refer to content- nor service providers. Only the access provider supplies access to information without arranging the transmission or choosing the addressee or content. It’s service consists of providing the technical access to the internet, not filtering or arranging information in any way. This confirms that the States Treaty on Media Services does in fact extend to access providers. The principle of separation between Telecommunication- and IaC-Services does not obstruct the applicability of § 22 of the states treaty as legal basis for the blocking decrees.

### 2.3 The blocked websites as media services

However, *Hoeren*<sup>18</sup> does not qualify the blocked sites as media, but as tele services and therefore concludes that § 22 is not applicable as a legal basis.

---

<sup>18</sup> *Hoeren*, Stellungnahme zur geplanten Sperrungsverfügung der Bezirksregierung Düsseldorf, p. 2, available on <http://www.odem.org/zensur/stellungnahme-prof-hoeren.pdf>.

The conceptual demarcation between tele- and media services is very complex<sup>19</sup>. The main difference being that tele services are meant to cover *individual* use. On the other hand media services are characterized by an editorial design intending to address *public use*.

The blocked sites are similarly created. The design is similar to that of a newspaper and the content is subdivided into topics and shaped in a journalistically editorial way [compare attachment 1 and 2]. The articles, statements, symbols and pictures are intended to present racist ideas to the users and thus influence their opinion. The editorial layout is addressed to the entirety of all internet users, the websites are freely available and therefore directed towards mass and not individual communication. Insofar, the blocked sites are evidently media services; the classification as tele services is not convincing. Therefore § 22 of the States Treaty on Media Services is the correct legal basis for the blocking decree towards access providers.

### **3 Requirements of the States Treaty on Media Services**

§ 22 requires an offence against the states treaty. In the present case the blocked websites might violate § 12 (1). According to § 12 (1) web content is illicit, if it offends criminal laws, glorifies war or if it “obviously represents a serious moral menace to children and adolescents”. With no doubt the content of the blocked sites violates criminal laws. On the one hand, it is sedition<sup>20</sup>, because content that incites hatred for parts of the population or certain ethnic minorities fulfils the requirements of criminal sedition. The blocked websites explicitly promote hatred for Jews and foreigners. These minorities are being insulted, disdained and defamed [compare attachment 3]. Furthermore, the site <http://www.stormfront.org> fulfils § 86 (1) No 4 StGB: It contains propaganda for the NSDAP (Hitler’s party) and aims at continuing its political goals *contra constitutionem* [compare attachment 4]. Finally, all of the websites glorify war and are therefore representing a serious moral menace to children and adolescents. At first sight one might object this point, saying that one does not surf and get to these sites by coincidence. Only those who look for this content will get it and therefore the sites do not really represent a menace. A closer look however reveals that the mere existence of these websites already represents a menace. As

---

<sup>19</sup> *Holznapel/Kussel*, Möglichkeiten und Risiken bei der Bekämpfung rechtsradikaler Inhalte im Internet, in: MMR 2001, p. 347 (348).

<sup>20</sup> In German Criminal law: § 130 (1), (2) StGB

shown above, the websites violate various criminal laws. Hence they disturb public order. And, speaking in legal terms, such a disturbance is nothing but the realization of a previous menace. Furthermore one has to consider the state's public duty of protecting minors. For example, § 6 No. 1 of the "Law on Dissemination of Scripts and Media Content Representing a Danger for Adolescents"<sup>21</sup>, qualifies hate speech on websites as an extreme harm for adolescents. Therefore the law prohibits to publish such content via IaC-Services under the threat of 1 year prison sentence (§ 21 of the law). This law reveals that the protection of minors in the context of internet and other media is based upon the idea that children do not possess full moral strength, yet. Therefore, any confrontation with these websites and their harmful content, no matter if unintentional or even intentional, is a serious threat for a child and its moral concept. All in all, the websites violate § 12 of the states treaty and are therefore unlawful.

Yet, according to § 22 (3) decrees are only lawful as long as they request something technically feasible. Thus, the blocking of the websites has to be technically possible for the access providers. There are many ways of blocking websites<sup>22</sup>. Blocking procedures may either step in at the beginning of the communication-line (content provider) or at the end (user). But the present decree pertaining to access providers is not compatible with either of these options. Access providers have neither influence on the transmitted content, nor on the users' behavior. Thus, only devices that interfere in the communication between the content provider and user are suitable. In its decree, the district government proposed three different methods to the access providers. First it suggested the exclusion of domains in the DNS server, secondly the utilization of a proxy server. And last, it proposed the exclusion of IP-addresses by a manipulation of the router. The question is, whether these proposals are in fact technically feasible:

The internet varies fundamentally from classical communication networks such as telephone, radio and television<sup>23</sup>. In contrast to these, the internet – as a "network of networks"<sup>24</sup> – is not subdivided into a hierarchy. Technically, it only links standardized data protocols (so called IP-packages). These are not devoted to a certain network, but simply connect all online-

---

<sup>21</sup> Gesetz über die Verbreitung jugendgefährdender Schriften und Medieninhalte (GjSM).

<sup>22</sup> Köhntropp/Köhntropp/Seeger, Sperrungen im Internet – Eine systematische Aufarbeitung der „Zensur-diskussion“, in: DuD 1997, p. 626 (628).

<sup>23</sup> Hornig, Möglichkeit des Ordnungsrechts bei der Bekämpfung rechtsextremistische Inhalte im Internet, in: ZUM 2001, p. 846 (847).

<sup>24</sup> Hartmann, Medienphilosophie, Vienna 2000, p. 309.

computers to an “a-centric”<sup>25</sup> network. At junctions between the various networks, there is a router passing on the IP-packages from one into the other. This is a crucial point for the blocking of IP-addresses: On the one hand, there are possibilities of making the router reject all inquiries to a certain address. Yet, this method would turn down all of the communication with the server, including e-mail and other forms of individual communication<sup>26</sup>. A more selective router-based blocking may be achieved with the TCP-port number. Choosing a service in the TCP/IP-protocol usually happens through this port number. Some routers are capable of blocking mass communication to an address while allowing the individual communication to pass through.

At the level of application-protocols, employing a proxy server allows an exact blocking of certain sites and services. The URL (*Uniform Resource Locator*) as coordinator for an individual website on its respective server may be blocked with a proxy server. This permits the filtering of single web elements and messages. However, the preconfigured filters are up to now only reacting to components of names and addresses<sup>27</sup>. Thus, there is a great chance of filtering socially permissible information at the same time. For instance internet users have had difficulty finding the “Babcock International Group PLC” in a web based search engine, because the part “cock” in Babcock, employed in a sexual context, is a swearword in English. Finally, the manipulation of the DNS server is another way of denying access to a website. The DNS may be configured so that requests in form of URLs concerning the illicit websites are diverted to a different site. Nonetheless, the questionable websites can then still be reached by entering the IP-address into the browser.

As shown, none of these technical possibilities provide absolute protection, as there still are certain ways of circumventing the blocking system used. However, this is a question of their effectiveness which is treated below. At this point it is sufficient to record, that there are technologies allowing access providers to block certain websites. Thus, the district government does not impose an impossible task to the access providers. This also reflects in the idea, that the district government contents itself with one of these technical devices enumerated in the decree.

---

<sup>25</sup> Hornig (footnote 23), p. 847.

<sup>26</sup> Federrath, Zur Kontrollierbarkeit des Internet, in: ZUM 1999, p. 177 (180).

<sup>27</sup> Spindler/Volkmann (footnote 15), p. 406.



#### 4 Categorizing the access-provider's legal responsibility

Under general German police law, the authorities can only task somebody under certain circumstances taking into account his legal responsibility<sup>28</sup>. In those categories the access provider has to be categorized as a non-disturber: Neither does it cause the danger by its behaviour, nor can it be attributed to a source that it is responsible of. Although he does objectively transmit the illegal content, the access provider does not have any influence on the transmitted information. The brink of illegality is already trespassed by the content providers<sup>29</sup>. They, and not the access provider, are immediately legally culpable. Moreover, he can neither be reproached a subjective motivation to impart the illegal information, nor can this be construed from an objective context<sup>30</sup>. The access provider only wants to provide paths of communication. This is socially appropriate behaviour. He is therefore not even indirectly responsible for the illegal content.

In the field of the States Treaty covering Media Services, however, these general requirements are substituted by special requests in § 22 (3) of the treaty. According to this, measures towards access and service providers are subsidiary to those towards the content provider. Only if, for legal reasons or matters of fact, he cannot be held responsible, the district government may address the access provider. Presently both, the content- and service providers act from within the USA. On August 9<sup>th</sup> 2000, the Düsseldorf district government addressed the responsible American service providers and asked them to block the websites. The request was not successful<sup>31</sup>. Also initiatives to identify the content providers have failed. They act anonymously and “obviously use code-names and trick-addresses”<sup>32</sup>. Furthermore legal measures, e.g. the judicial prosecution in the USA, are not promising either, as a precedent case demonstrates: In May 2000, two French Non-Governmental Organisations (NGOs), the French Union of Jewish Students and the League Against Racism and anti-Semitism sued *Yahoo! Inc.* at a French Court of emergency proceedings, called the “*Tribunal de Grande Instance de Paris*”. The NGOs complained that *Yahoo! Inc.* was allowing the sale of thousands of pieces of Nazi memorabilia through its online auction service, whereas in France the sale of Nazi-related items is regarded as a criminal offence. The auction site was hosted in the US but could of course be accessed from France. Under

<sup>28</sup> In North Rhine-Westphalia for instance §§ 17-19 OBG NW.

<sup>29</sup> *Zimmermann*, Polizeiliche Gefahrenabwehr und das Internet, in: NJW 1999, p. 3145 (3149).

<sup>30</sup> *Spindler/Volkmann* (footnote 15), p. 403.

<sup>31</sup> [http://www.nps-brd.nrw.de/BezRegDdorf/autorenbereich/Dezernat\\_21/PDF/39sperrverf\\_022002.pdf](http://www.nps-brd.nrw.de/BezRegDdorf/autorenbereich/Dezernat_21/PDF/39sperrverf_022002.pdf) , p. 3.

<sup>32</sup> [http://www.nps-brd.nrw.de/BezRegDdorf/autorenbereich/Dezernat\\_21/PDF/39sperrverf\\_022002.pdf](http://www.nps-brd.nrw.de/BezRegDdorf/autorenbereich/Dezernat_21/PDF/39sperrverf_022002.pdf) , p. 3.

the threat of a 16.000 € daily penalty, the Court ordered *Yahoo! Inc.* to take all appropriate measures in order to deny internet users the access to auction sales of Nazi items from French territory, and more broadly from accessing any other site or service that promotes Nazism or denies Nazi crimes<sup>33</sup>. Concurrently, *Yahoo! Inc.* filed a counter-suit in a federal district court, San José, California, requesting that the French decisions be declared void under the First Amendment of the US Constitution. The company also contested the French rulings on the ground, that the French court had overstepped its jurisdiction, in other words that it should not be able to impose its national laws on a US company. In its verdict on November 7<sup>th</sup> 2001, the US District Court in fact issued the declaration that the First Amendment of the Constitution that embodies the right to free expression precludes enforcement within the US of the French ruling<sup>34</sup>. The two French NGOs that launched the proceedings in France have appealed this decision and contended that *Yahoo! Inc.* should not be shielded from French law by the First Amendment. But they are unlikely to succeed because of the legal principles that prohibit the enforcement of foreign judgements when the latter are contrary to the public policy of the forum<sup>35</sup>. This precedent shows that even legal measures against the American content providers is unpromising. Consequently, content providers cannot be addressed with orders for both, legal reasons and matters of fact. Hence, the access providers may in fact be addressed in accordance with § 22 (3) of the States Treaty covering Media Services.

Yet, § 22 (3) can only be applied, if the access provider's responsibility is not a priori excluded. Thus, *Waldenberger*<sup>36</sup> maintains that § 7 (1) of the treaty, stipulating limits to the access provider's civil liability, forbids the authority to address it with a blocking decree. But this idea is not convincing. § 6 (2) 2 clarifies that the duty of blocking certain information is independent of the legal responsibility of the addressed. The provider has a public duty of stopping and blocking the incriminated content regardless of limits to its civil liability.

---

<sup>33</sup> Verdict available on <http://www.juriscom.net/txt/jurisfr/cti/tgiparis20000522.htm>.

<sup>34</sup> YAHOO vs. LICRA, 28 USC §2201 available on <http://www.juriscom.net/en/txt/jurisus/ic/dccalifornia20011107.htm>.

<sup>35</sup> *Frydman/Rorive*, Regulating Internet Content through Intermediaries in Europe and the USA, in: Zeitschrift für Rechtssoziologie, Stuttgart, Lucius, 2002, vol. 23 (1), p. 41 (44), available on [http://www.droit-technologie.org/2\\_1.asp?dossier\\_id=99](http://www.droit-technologie.org/2_1.asp?dossier_id=99).

<sup>36</sup> *Waldenberger*, Der juristische Dauerbrenner: Haftung für Hyperlinks im Internet, in: AfP 1998, p. 373.

## 5 Legal Consequences

Thus, the blocking decrees meet the requirements of § 22 (2) of the treaty. As legal consequence the law enables the authority to take the “appropriate measures towards the provider in order to remove the infraction”. According to § 22 (2) of the treaty, it may primarily “prohibit content and order their blocking”. Insofar, the law concedes a sphere of discretion to the authority. On the one hand it can choose from various kinds of measures and on the other, it can address its decrees to different providers. The question is, whether it translated this sphere of discretion into action faultlessly or not.

As far as the choice of the addressed providers, the district government has met the right decision. As described above, measures towards any other responsible party (e.g. content providers) were fruitless for legal reasons or matters of fact. Furthermore, the district government chose the right measure by decreeing a blocking order, because access providers are technically not able to impose restrictions in regard to the content of the websites. They only provide technical access to them, without being able to influence the content themselves. However, the Düsseldorf district government would still have exceeded its authority, if the legal consequences were disproportionate for the access providers. This general idea of German and European law is also specified in § 22 (2), (3) of the states treaty<sup>37</sup>: The decree has to be suitable to reach its objective and it has to be the relatively mildest intrusion for the access provider. Finally, the public interests in blocking the content must outweigh the provider’s privacy.

Many authors have criticized the blocking decrees as being unsuitable to reach their objective, saying they commit the access providers to an impossible task. *Sieber*<sup>38</sup> and *Schneider*<sup>39</sup> for instance point out, that the blockings can be bypassed in various ways. The illegal content could either be “mirrored” to other servers, or still be viewed if one were constantly switching IP-addresses and ports. Other ways of getting around the blockings are web-based translation services or simply connecting to the internet via another non-blocking provider. From these findings they draw the conclusion that blocking is inefficient and therefore unsuitable for reaching the goal of banning that content from the internet<sup>40</sup>. One has to admit, that regardless of the chosen measure, it will by no means be possible to totally eliminate the

---

<sup>37</sup> *Kuch*, Der Staatsvertrag über Mediendienste, in: ZUM 1997.

<sup>38</sup> *Sieber*, Verantwortlichkeit im Internet: technische Kontrollmöglichkeiten und multimedienrechtliche Regelungen, Munich 1999, p. 204.

<sup>39</sup> *Schneider*, Die Wirksamkeit der Sperrung von Internet-Zugriffen, in: MMR 1999, p. 571 (572).

<sup>40</sup> *Hoeren* (footnote 18), p. 3.

possibility of viewing the sites, which is due to the diverse ways of circumvention. Nevertheless, the general duty of public policy is to provide an efficient protection against dangers<sup>41</sup>. In a case, where the complete removal of the menace is impossible, the authority must be enabled to take measures that allow it to approach its objective<sup>42</sup>. In Germany there are nowadays almost 25 million internet users<sup>43</sup>. The vast majority of them are technically not very well versed. Since the leading browsers are easy to handle, minimal practical knowledge is sufficient to use the internet. Thus, for the average internet user even simply obstructing the URL, the easiest blocking to get around, would cause considerable difficulty in order to view a particular site<sup>44</sup>. The manipulation of the DNS server has similar consequences. The need to type in a long number instead of being able to use the easily memorable URL-Names impinges on the simplicity of calling up the websites. The critics however point out, that the DNS-blocking could be avoided even without special knowledge<sup>45</sup>. They point towards a manual provided by the Chaos Computer Club (CCC)<sup>46</sup> that explains how to circumvent the blocking<sup>47</sup>. Yet, this manual demonstrates the exact opposite: It is composed of 12 different steps and requires a supplementary 9-digit IP-Address from another non-blocking server [compare attachment 5]. This proves that one needs additional knowledge of details that the average internet user does not possess. Therefore the DNS-blocking is suitable to restrain the menace arising from the blocked websites.

Nevertheless, the multiple ways of circumventing the blocking represent a problem that cannot simply be disregarded. Especially the alternative of dialling up via a non-blocking provider is an easy way of getting around the blocking. The Düsseldorf district government's power is geographically limited to the boundaries of North Rhine-Westphalia. Providers that are situated in another country or even federal German state are hence not subordinated to the blocking order. Switching to a non-blocking provider will therefore oftentimes not even encumber the user with higher phone-charges. For this reason the state would be well served by keeping up a close and permanent dialogue with the internet economy and foremost the content-, service- and access providers. Only a joint procedure will be able to ensure an effective banning of hate speech and racist content from the web. For instance, co-regulatory models will allow a more diverse approach combining content rating, filtering and blocking,

---

<sup>41</sup> *Spindler/Volkmann* (footnote 15), p. 406.

<sup>42</sup> BVerfGE 33, p. 171 (187); 63, p. 88 (115).

<sup>43</sup> <http://focup.msn.de/D/DD/DD36/DD36A/dd36a.htm> .

<sup>44</sup> *Spindler/Volkmann* (footnote 15), p. 406.

<sup>45</sup> *Stadler*, Sperrungsverfügung gegen Access Provider, in: MMR 2002, p. 343 (345).

<sup>46</sup> <http://www.ccc.de/censorship/dns-howto/> .

<sup>47</sup> *Stadler* (footnote 45), p. 345.

notice-and-take-down procedures, as well as public awareness. Examples of early co-regulatory efforts in Japan indicate in practice that codes of conduct can help the industry move to protect customers and reduce the threat of government regulation<sup>48</sup>.

Technically speaking, isolated public law enforcement has only a few alternatives to the order of blocking of websites. As shown above, it is not possible to task those, who are responsible for the content, because they are located abroad. Also regulating content with pre-configured filters at the proxy-server is inappropriate. This alternative has been discussed for content- and service providers<sup>49</sup>, but it is not practical for access providers. The filter-technique is based upon the recognition of certain name- or address fragments. If this technique were employed on the DNS server, there would be a great chance that legal content is filtered as well (compare example “Babcock” above on p. 8). Thus affecting the rights of unconcerned third parties, the filter technique is not as mild as the blocking of certain websites.

Critics have furthermore suggested that internet users should self-protect themselves from illegal content<sup>50</sup>. Considered by itself, this is not an appropriate alternative: The blocking shall not only protect upright users, but also and especially make the connection more difficult for those who purposely aim at viewing this illegal content. Offering the voluntary self-protection to those people is obviously inapt and therefore inefficient. On the other hand side, self-protection may increase the effectiveness of a combined co-regulatory model. All self-regulatory approaches rely on the user being informed enough to take advantage of them. In this context, the protection of minors needs to be turned to with special concentration. Parents need to know what the meaning and relevance of different age categories in content rating is and be able to make a decision on whether the content is really appropriate for their child. Cultural and other differences among families make empowering of parents necessary for content rating to be successful. With filter software and notice-and-take-down, media literacy may play a decisive role in whether such co-regulative strategies will successfully be implemented en masse. Filtering software carries with it not only the requirement of awareness but also technical knowledge of first being able to install such software and then being able to prevent one’s children from circumventing the filter. Notice-and-take-down requires consumers to be able to know whom to contact, in what situations, and to know what to expect once they make a complaint. In this respect, self-protection and public awareness certainly are crucial elements for a successful (co-)regulation of internet content.

---

<sup>48</sup> *Frydman/Rorive*, (footnote 35), p. 44.

<sup>49</sup> *Holznapel/Kussel* (footnote 19), p. 349.

<sup>50</sup> <http://www.tauss.de/service/presse/stellungnahmesperrungsverfuegung/> .

Lastly it needs to be examined, whether the need for an official intervention into private rights predominates the access providers' interest in warding off the decree. In this context, two different aspects have to be considered. On the one hand side, the blocking must not overtax the access providers' economic independence and on the other, the impact on their Constitutional Rights must be weighed against the menace to public welfare.

### **5.1 Impact on economic capacities**

Many opponents reproach the district government for overtaxing the providers capacities<sup>51</sup>. They say the blocking requires an immense technical, economic and personnel expenditure<sup>52</sup>. In fact, this is true for methods such as the blocking of IP-addresses and above all the inset of proxy-servers. In contrast, the favored manipulation of the domain-name-service (DNS) server is possible without any expense worth mentioning. It is activated by a simple and singular configuration of the DNS-server. In its reasons for the blocking decree, the authority explicitly favors this DNS-manipulation by saying that "regarding the present state of technology, an exclusion of the domains in the domain-name-server is sufficient"<sup>53</sup>. Consequently, it consciously chose a technique that does not overtask the access providers.

### **5.2 Impact on Constitutional Rights**

In its reasons for the blocking decree, the district government hardly mentions and justifies impacts on constitutional rights. Yet, the requirement touches the access providers' freedom of profession, their right of free ownership and also the freedom of the press and the freedom of expression in general.

First of all the district government should have discussed, whether the Right of free ownership<sup>54</sup> is offended. This Constitutional Right protects private possession from public intervention and expropriation. In fact, this also counts for the access providers' right to use their own DNS servers without restraint. However, the Right of free ownership is limited to a suitable utilization within the bounds of legality<sup>55</sup>. The access providers cannot claim the

---

<sup>51</sup> *Stadler* (footnote 45), p. 345.

<sup>52</sup> *Hoeren*, (footnote 18), p. 3.

<sup>53</sup> [http://www.nps-brd.nrw.de/BezRegDdorf/autorenbereich/Dezernat\\_21/PDF/39sperrverf\\_022002.pdf](http://www.nps-brd.nrw.de/BezRegDdorf/autorenbereich/Dezernat_21/PDF/39sperrverf_022002.pdf) , p. 8.

<sup>54</sup> Art. 14 of the German Constitution.

<sup>55</sup> BGHZ 45, p. 150 (155).

right of free ownership for a transmission of illegal content such as racist and xenophobic websites<sup>56</sup>. This idea can be transferred to the freedom of profession, too. The mere practice of one's profession is limited to the bounds of general laws such as § 130 and § 86 (1) N<sup>o</sup> 4 StGB.

The case is more difficult for the freedom of expression<sup>57</sup>. *Spindler* claims that access providers cannot invoke the free expression and free press protections themselves<sup>58</sup>. Singularly providing the technical access to the content, they were neither part of the press, nor would they utter their opinion at all. This assumption may be true. Nevertheless, both freedoms of expression and press have to be considered for two reasons. On the one hand, German authorities have to consider certain constitutional rights towards foreigners as well<sup>59</sup>. This concerns the American content providers' freedoms of expression. On the other hand, the free expression and press clauses also protect the ability of disseminating information via any medium. In the current issue, the freedom of expression therefore comprehends the ability of communicating information via internet. Therefore, the technical procedure of connecting to the internet does at last protect the access providers' service very well. However, the free expression protections to the medium of communication are limited to information that is protected by the free expression clause itself. Only if the moot content is covered by the freedom of expression, its imparting via the medium of communication will be protected at all. The freedom of expression guarantees the right to express and impart one's opinion. Opinions are characterized by a subjective link between the orator and his content<sup>60</sup>. Therefore they cannot be identified as right or wrong. This understanding of opinion has to be distinguished from the promotion of obviously wrong facts, which is not safeguarded by the German understanding of freedom of expression. Such an obviously wrong fact being, for instance, denying the persecution of Jews during World War II (so called Auschwitz-Lie). The blocked websites contain the Auschwitz-Lie in various spots [compare attachment 6]. On the other hand, one could argue that the state should not write history and decide which facts really occurred, are obviously right and which ones not. If the state determined which opinion is worth being protected and which ones not, it would contradict fundamental constitutional principles itself. In this understanding of constitutional freedoms and especially the freedom

---

<sup>56</sup> *Greiner*, Die Verhinderung verbotener Internetinhalte im Wege polizeilicher Gefahrenabwehr, Hamburg 2001, p. 156.

<sup>57</sup> Art. 5 (1) of the German Constitution.

<sup>58</sup> *Spindler/Volkman* (footnote 15), p. 407.

<sup>59</sup> Compare Art. 1 (3) of the German Constitution; BVerfGE 6, p. 290 (295); BVerfGE 57, p. 9 (23).

<sup>60</sup> BVerfGE 33, p. 1 (14)

of expression, the state rather plays the role of a referee. *Owen Fiss* for example claims that in some cases, the state “may have to allocate public resources - hand out megaphones - to those whose voices would not otherwise be heard in the public square. It may even have to silence the voices of some in order to hear the voices of the others.”<sup>61</sup> The Constitution implements a certain duty of the state to facilitate a possibly broad exertion of everybody’s constitutional freedom rights. If a certain group is overly disadvantaged the state has the public duty of counteracting the preponderant forces. The content on the blocked websites may be summed up as pure libel of Jews and other minorities; it is beyond polemic criticism and only aims at depreciating those persons. This completely one-sided, aggressive and despising hate speech has a “silencing effect”<sup>62</sup> on the disadvantaged. At this point, the state has to interfere in order grant an equal exercising of constitutional freedoms. In other terms, defamation of this kind has to step back behind the personal rights of the dispraised. Hence, the free speech clause does not protect the communicated content. In consequence, the freedom of expression does not grant the submission of such incriminated content via the medium of communication either.

The blocking decrees have furthermore been criticized as censorship and thus unconstitutional<sup>63</sup>. Yet, the prohibition of public censorship only covers preventive measures that interfere before the publication. The blocking decrees however can logically only step in after the publication in the internet, because the authorities cannot notice the incriminated content before any other user does. Later repressive measures are not universally forbidden but restricted to infractions of general laws<sup>64</sup>. As shown above, the content under discussion infringes upon such general laws.

But the decrees hurt the users’ Constitutional Right of unrestrained information that includes the ability to acquire information from sources in foreign countries<sup>65</sup>. On the other hand side, the illegal content violates different laws and other peoples’ Constitutional Rights as shown above. Thus, there is a need to balance the protected rights and the intensity of their infractions one against the other. On the one hand, the constitutional right of unrestrained information is an important prerequisite for a free and well informed democratic public. Insofar, one has to consider that the intellectual, controversial and emancipated public dialogue on National Socialism and far-right attitudes needs information on their arguments

---

<sup>61</sup> *Owen Fiss*, *The Irony of Free speech*, Harvard University Press, 1998, chapter 1, p. 2.

<sup>62</sup> *Owen Fiss*, (footnote 61), chapter 1.

<sup>63</sup> <http://www.tauss.de/service/presse/stellungnahmesperrungsverfuegung> .

<sup>64</sup> *Spindler/Volkmann* (footnote 15), p. 407.

<sup>65</sup> BVerfG NJW 1970, p. 235 (237).



and (even if wrong) facts. Some authors maintain that the moot websites did not contain any information worth being read<sup>66</sup>. They argue, the far-rights themselves would oftentimes not seek the intellectual-political discussion as the incriminated content revealed<sup>67</sup>. Irrespective of this judgement, the proportionality of the order cannot depend on a qualification of content by the state. If the state was to determine what content is worth being protected and which information does not need to be taken note of, it would contradict fundamental constitutional principles itself. The decisive aspect is thus not the intellectual value of information, but much rather the threats for the public emanating from the content. The concerned content infringes upon human dignity, attacks the German Constitution and disturbs public peace. It furthermore fulfils several criminal laws, glorifies hate and violence. Calling up the websites therefore poses a moral threat especially to adolescents<sup>68</sup>. The state has a public duty of protecting its citizens from any danger. Protection of minors has an outstanding importance. The websites, supporting the reestablishment of the NSDAP, also aim at attacking the German Constitution. It's public duties oblige the state to take all measures appropriate to safeguard the Constitution. Therefore, restrictions in respect of the information do not necessarily endanger the democratic system. In contrast, the internet allows the authors to reach a broad public. This means a wide dissemination of illegal content and harm to democratic principles at the same time. All things considered, the public interest in fighting racist and xenophobic internet content prevails over the damage to the affected Constitutional Rights. The menace especially to moral integrity of the youths is very significant, whilst the intensity of the intervention is rather modest for the access providers.

## **6 The access providers' right to compensation**

As described above, access providers correspond to non-disturbers in legal terms. In general German police law, non-disturbers who are being required to remove a threat have a right to compensation for their expense and other loss arising from the removal<sup>69</sup>. However, the special rules of the States Treaty on Media Services do not provide such a claim for the access provider who was engaged without having caused the disturbance at all. *Jürgen Büssow*, head

---

<sup>66</sup> *Spindler/Volkmann* (footnote 15), p. 401.

<sup>67</sup> *Sieber*, *Internationales Strafrecht im Internet*, in: NJW 1999, p. 2065 (2067).

<sup>68</sup> *Holznagel/Kussel* (footnote 19), p. 349.

<sup>69</sup> For North Rhine Westphalia for example § 39 (1) a OBG NW.

of the Düsseldorf district government, hence concludes that there is no need to compensate the access providers for their efforts. According to *Büssow*, the states treaty holds ultimate regulations simply not providing compensation for access providers who were disturbers “sui generis”. This view is not convincing. A comparative analysis will reveal that access providers do need to be compensated for their efforts in the end.

For lack of a special legal basis, official decrees such as blocking orders concerning tele services have to be based on general German police laws<sup>70</sup>. This recourse to the general rules also makes it possible for the addressees to claim compensation of their effort. Knowing that many services on the internet are designed for individual use and therefore tele services, access providers hence transmit both tele- and media services. So far as the district government had decided to order the blocking of tele services, access providers would have had the chance of claiming compensation. But this result is unsatisfactory. Access providers cannot technically differentiate between the transmission of one or the other service<sup>71</sup>. As shown above, they do not have any influence on the transmitted information. The access provider’s service only consists in transmitting bits and bytes in a merely technical process. From his point of view the chance to obtain compensation would thus depend on the coincidence that the district government chooses to block a tele- instead of a media service. But this oddity cannot free the state from the general obligation to compensate someone who has only been tasked because of his special skills<sup>72</sup>. In the present matter, the state could otherwise be seduced to restraint it’s blocking orders to media services for the only reason of getting around the duty of compensation. This inference reveals the inconsistency of *Büssow*’s assumption. The discrepancy must be resolved. A feasible way is the analogue application of general police law to the field of the States Treaty on Media Services.

Besides access providers, there are also content- and service providers involved in the broadcasting of media services. In contrast to access providers, however, content- and service providers will not be compensated for their efforts. Content providers present their own content in the internet, creating and maintaining the websites themselves. They bear the full legal responsibility for their provided content. This includes information that the content provider does not create himself but adopts from other websites. Evidentially, content providers are the immediate origin of the infraction and thus legal disturbers who cannot claim compensation. The service provider makes somebody else’s content available (e.g.

---

<sup>70</sup> *Spindler/Volkman* (footnote 15), p. 400.

<sup>71</sup> *Stadler* (footnote 45), p. 347.

<sup>72</sup> BGHZ 117, p. 307 f.

internet search engines). He is only responsible for inappropriate content to some extent. On the one hand his liability is limited to content that he is aware of and on the other he may only be tasked to block them if it is technically possible and reasonable. Presuming their consciousness of the illegal content and the technical possibility of acting, service providers also have to be regarded as legally liable<sup>73</sup> and are hence not entitled to compensation either.

## **7 Conclusion**

All in all, the blocking decrees are lawful. Yet, in parts the criticism to them is intelligible, in particular the argument for the various possibilities of circumventing the blockings, as well as the question for the access providers legal responsibility. At least they must be compensated for their efforts. Nevertheless, in the end it is an unconvincing conclusion to contest the legitimacy of the decrees. Such a surrender to the complexity of the problem and the ubiquity of the internet as a source of information cannot seriously be considered from the point of view of a constitutional state. The public interest in suppressing racist and xenophobic internet content prevails.

As concluded above, the many ways of getting around the imposed blockings still suggest a combination of governmental regulation and private self-regulation. For instance, providers could agree to a code of conduct engaging them to suppress illegal internet content. In a counter-move, the state should restrain its official interventions to cases where the voluntary self-regulation fails. In addition, both government and internet economy share a vital interest in building consumer confidence by removing concerns and ensuring protection of their rights. Public awareness campaigns will help improving the users' media competence and self-protective knowledge. Such co-operation in form of co-regulation would combine the existing technical and legal possibilities for maximum success.

---

<sup>73</sup> Zimmermann (footnote 29), p. 3148; Hornig (footnote 23), p. 856; Stadler (footnote 45), p. 344; Spindler/Volkman (footnote 15), p. 403.

## Attachment 1

Stormfront White Pride World Wide - Microsoft Internet Explorer


Adresse: <http://www.stormfront.org>

## Stormfront.org

### The measure of greatness

NATIONAL VANGUARD Editorial from 1989

April 20 of this year is the 100th anniversary of the birth of the greatest man of our era -- a man who dared more and achieved more, who set his aim higher and climbed higher, who felt more deeply and stirred the souls of those around him more mightily, who was more closely attuned to the Life Force which permeates our cosmos and gives it meaning and purpose, and did more to serve that Life Force, than any other man of our times.



And yet he is the most reviled and hated man of our times. Only a few tens of thousands of men and women, in scattered groups around the world, will celebrate his birthday with love and reverence on April 20, while all of the scribblers and commentators of the controlled news media, the controlled politicians, and the controlled churchmen will pour out their hatred and venom and lies against him, and those lies will be believed by hundreds of millions.

**What is the measure of greatness in a man?**

Only the most vulgar and doctrinaire democrat would seriously equate greatness with popularity -- although in any polling of average citizens on their choice for the greatest man of the century there are certain to be substantial numbers of votes for Elvis Presley, John Kennedy, Billy Graham, Michael Jackson, and various other high-visibility lightweights: charismatic entertainers on the stage of politics, rock concerts, spectator sports, or what have you.

More serious citizens would pass by the lightweights and choose men who have changed the world in some way. We would hear choices like Franklin Roosevelt ("he saved the world from fascism"), Albert Einstein ("he taught us about the nature of our universe"), and Martin Luther King ("he helped us achieve racial justice"), depending upon whether one's personal inclinations lay more in the direction of politics, science, or racial self-abasement, respectively.

Graphical design of <http://www.stormfront.org>

## Attachment 2

Nazi Lauck NSDAP/AO Letzte Meldungen - Microsoft Internet Explorer

Adresse: <http://www.nazi-lauck-nsdapao.com/>

## Nazi Lauck NSDAP/AO

# Letzte Meldungen

Aktualisiert am 4. November 2003 (114)

**FRONTBERICHT VOM 9.10.2003/114 AUS DER TSCHECHEI: "Czech TV1" hat am 7.10. den mehrminütigen Bericht "Udalosti" ("Geschehen") gesendet. Etwa 3,6 Millionen Zuschauer haben ihn gesehen. Die Netzseiten der NSEC and der NSDAP/AO mit dem ganzen Warenangebot sind gross und ganz deutlich gezeigt worden!" - In Oktober hat die NSDAP/AO-Netzseite mehr tschechische Besucher als amerikanische gehabt! Nur in Deutschland und in Ungarn sind es mehr gewesen.**

**LENI RIEFENSTAHL** ist am 8. September 2003 (114) im Alter von 101 Jahren gestorben. Die Systempresse hat sie auch im Tode verleumdet, anständige Menschen sie jedoch geehrt.

**DAS NEUE BUCH "Der Rechtsextremismus und der Radikalismus in der Tschechischen Republik"** berichtet über die Rolle der NSDAP/AO und ihre Schwesterorganisation NSEC in jenem Lande.

**NACHKRIEGSREKORD:** Die Zahl antijüdischer Übergriffe in Europa habe den höchsten Stand seit 1945 erreicht, berichtet – laut die deutsche Presse - das Simon-Wiesenthal-Zentrum.

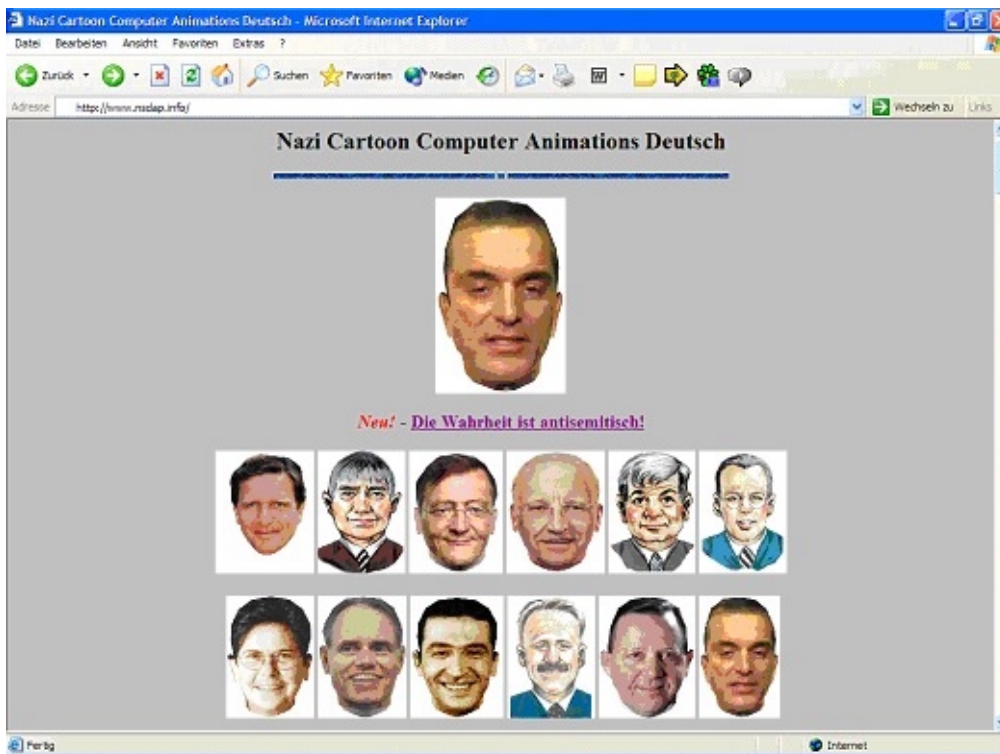
**SCHWARZE LISTE IN DER SCHWEIZ:** Ungarische Kameraden berichten, sie hätten ein Einreiseverbot für die Schweiz, und zwar ausschließlich wegen ihrer politischen Gesinnung, die die Behörden für eine Gefahr für die Gesellschaft halten. Dabei sei auch die NSDAP/AO erwähnt worden.

**"STAATLICHE ANERKENNUNG":** Der tschechische Verfassungsschutzbericht für das Jahr 2002 bestätigt die NSDAP/AO und ihre Schwesterorganisation NSEC als wichtige Quelle von NS-Propaganda. Darüberhinaus sei bedauerenswert, daß die NSEC-Netzseite in den USA (vom Kameraden Lauck) gehostet und damit unangreifbar ist. (Siehe [www.nsec-88.org](http://www.nsec-88.org) )

**RAZZIA:** Eine bewaffnete Elitetruppe (die "antiterroristische" OS13) vom englischen Scotland Yard hat am 4. Juli eine Razzia gegen acht Häuser von maßgeblichen RVF ("Revolutionary Volunteer Force") Mitgliedern durchgeführt, die keinen Widerstand leistenden Kameraden mit vorgehaltener Schußwaffe festgenommen, die Wohnungen durchsucht und die Computers und die Mobiltelefone beschlagnahmt. Der MIS-

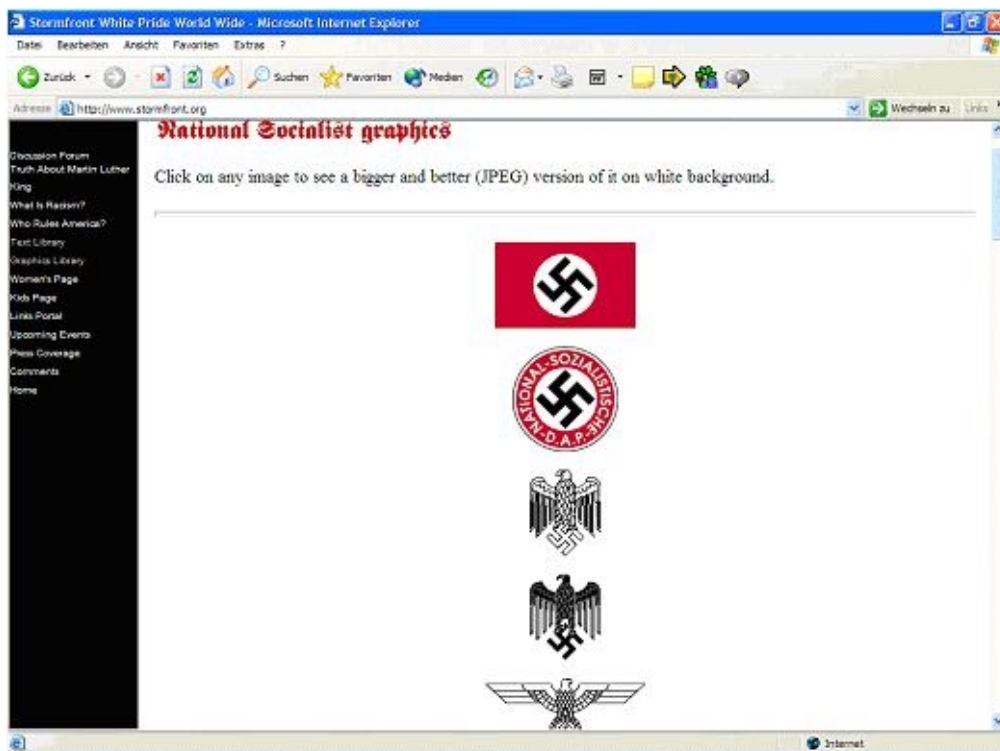
Graphical design of <http://www.nazi-lauck-nsdapao.com>

Attachment 3



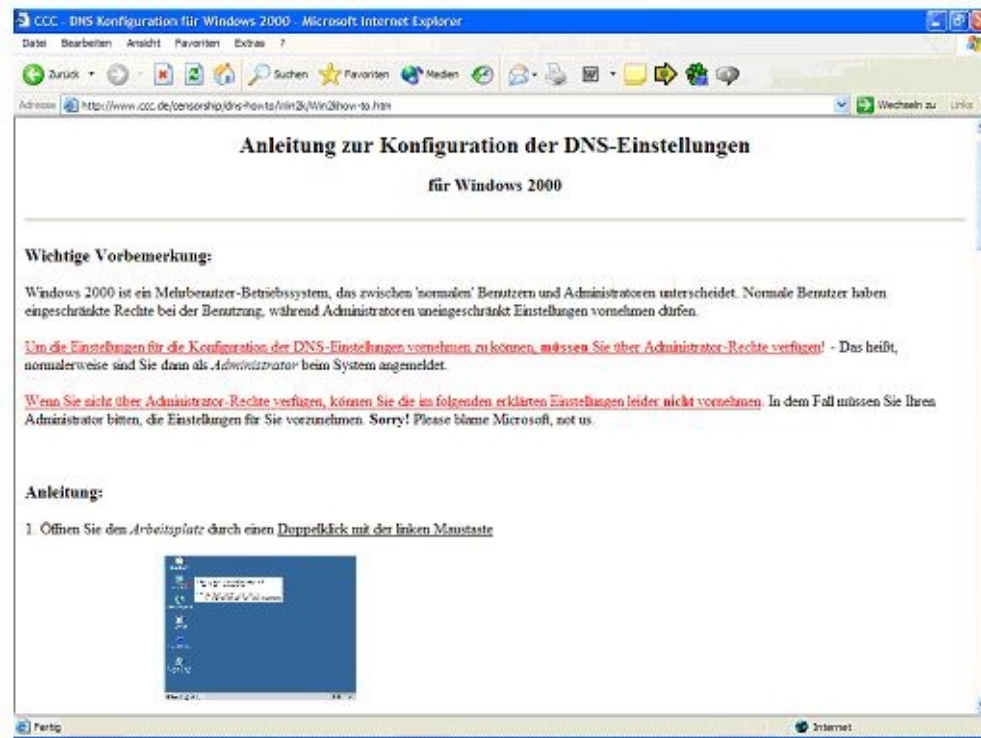
Anti-Semitism on <http://www.nsdap.info>

Attachment 4



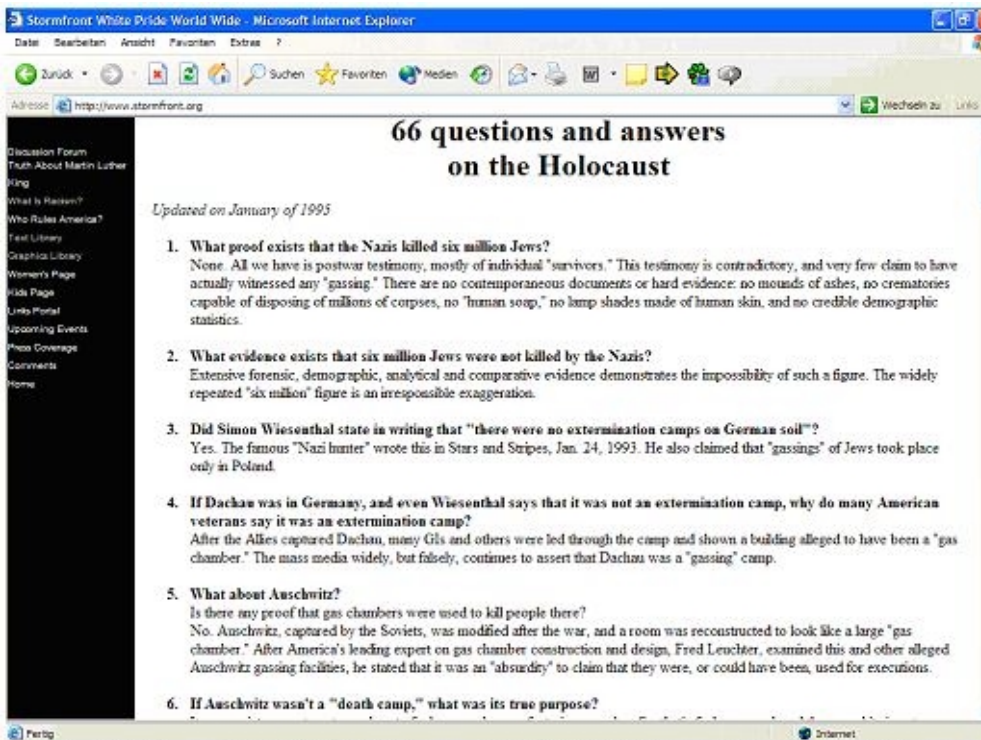
Nazi-Symbols on <http://ww.stormfront.org>

## Attachment 5



Manual for the configuration of the DNS provided by the Chaos Computer Club on <http://www.ccc.de/censorship/dns-howto/Win2k/Win2khow-to.htm>

## Attachment 6



Auschwitz-lie on <http://www.stormfront.org>