Criminal liability of Internet providers in Germany and other jurisdictions

Antje Elisabeth Margarete Funk

Thesis submitted in partial fulfilment of the requirements of the degree of Master of Laws in the Faculty of Law, University of Stellenbosch

Supervisor: Mr Gerhard Kemp

December 2004

Declaration

I, the undersigned, hereby declare that the work contained in this thesis is my own original work and that I have not previously in its entirety or in part submitted it at any university for a degree.

Antje Funk

December 2004

Abstract

This thesis deals with the criminal liability of Internet providers. The focus is on *Germany*, but the analysis is put in a wider, *comparative context*. This is done with reference to South Africa, as well as Europe and the American system. This thesis demonstrates and discusses the existing legal norms to regulate Internet provider liability for illegal content on the Internet and the *international* efforts to deal with this issue. In the introduction it is shown how the Internet has given rise to a new form of global communication and the accompanying legal problems. This is followed by an examination of the different functions Internet providers have.

A survey of some of the important crimes affecting the Internet and also some Internet-specific offences put the more general issue of liability in a more specific context. Traditional and new forms of crimes are discussed. This section is followed by an analysis of Internet provider liability under German criminal law and Germany's Teleservices Act. From an international criminal law perspective some international instruments, like the Cybercrime Convention of the Council of Europe, is discussed. National legislation, especially in the context of the European Union, must always be put in the proper regional and international context.

The thesis concludes with some thoughts on alternative, or perhaps complementary, methods to fight illegal and criminal conduct on the Internet. This is done not as a critique of the responses to Internet crime, but rather to strengthen the many hands trying to reduce Internet crime.

Opsomming

Hierdie tesis handel oor die strafregtelike aanspreekliheid van Internet diensverskaffers. Die fokus val op Duitsland, maar die analise word ook geplaas in 'n wyer, vergelykende konteks. Dit word gedoen met verwysing na Suid-Afrika, sowel as Europa en die VSA. Die tesis demonstreer en bespreek die bestaande regsnorme wat Internet diensverskaffers reguleer met spesifieke verwysing na aanspreeklikheid vir onwettige inhoud op die Internet en internasionale pogings om hierdie probleem aan te spreek. Ter inleiding word daar aangetoon hoe die Internet aanleiding gee tot nuwe vorme van globale kommunikasie en die regsprobleme wat dit tot gevolg het. Dit word gevolg deur 'n ondersoek na die verskillende funksies van Internet verskaffers.

'n Ontleding en bespreking van Internet-spesifieke misdrywe plaas die meer algemene vraagstuk in 'n meer gefokusde konteks. Tradisionele en nuwe vorme van misdaad word bespreek. Hierdie afdeling word gevolg deur 'n ontleding van Internet diensverskaffer aanspreeklikheid ingevolge Duitse reg en die Duitse wetgewing op die terrein van telediens. Uit 'n internasionale strafreg oogpunt word sekere internasionale instrumente, soos die *Cybercrime Convention* van die Raad van Europa, bespreek. Nasionale wetgewing, veral in die konteks van die Europese Unie, word ook in die relevante regionale en internasionale konteks geplaas.

Die tesis word afgesluit met sekere gedagtes oor alternatiewe, of moontlik komplimentêre, metodes in die stryd teen Internet-kriminaliteit. Dit moet nie gesien word as kritiek op die huidige stand van sake nie, maar eerder as 'n poging om die talle rolspelers in die stryd teen Internet misdaad se hande te sterk.

Table of Contents

Abbreviations

AfP	Archiv für Presserecht
AG	Amtsgericht
Arpanet	Advanced Research Project Agency Net
BayObLG	Bayrisches Oberlandesgericht
BGH	Bundesgerichtshof
BGHSt	Bundesgerichtshofentscheidungen im Strafrecht
BKA	Bundeskriminalamt
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BVerGE	Entscheidungen des Bundesverfassungsgerichts
CR	Zeitschrift Computerrecht
dpa	Deutsche Presse Agentur
GG	Grundgesetz
GjS	Gesetz über die Verbreitung jugendgefährdender Schriften und Medieninhalte
GRUR	Zeitschrift für Gewerblichen Rechtsschutz und Urheberrecht
IP	Internet Protocol
IRC	Internet Relay Chat
IuKDG	Informations- und Kommunikationsdienstegesetz
JuS	Juristische Schulung
JZ	Juristenzeitung

LG	Landgericht
MMR	Zeitschrift Multimedia und Recht
NJW	Neue Juristische Wochenschrift
NStZ	Neue Zeitschrift für Strafrecht
OLG	Oberlandesgericht
PPP	Point to Point Protocol
SLIP	Serial Line Internet Protocol
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TDG	Teledienstegesetz
UrhG	Urhebergesetz
WWW	World Wide Web
ZUM	Zeitschrift für Urheber und Medienrecht

1 Introduction

The revolution in information technologies has changed society fundamentally and will probably continue to do so in the future. The World Wide Web[1] (WWW) has become one of the main sources of information and provides a forum for the worldwide distribution of information. Where originally only some specific parts of society had rationalised their working procedures with the help of information technology, now hardly any sector of society has remained unaffected.

Furthermore, the Internet has to a certain extent replaced the traditional means of communication. Classical telephone calls have been overtaken by the exchange of vast amounts of data, comprising voice, text, music and pictures. It is no longer relevant whether a direct connection can be established. Nowadays it suffices that data is entered into a network with a destination address or made available for anyone who wants to access it. The Internet has created a new form of universal communication.[2] The ease of accessibility and searchability of information contained on the Internet combined with the practically unlimited possibilities for its exchange and dissemination, regardless of geographical borders, has lead to an explosive growth in the amount of information available.

These developments have given rise to an unprecedented economic and social change, but they also emerge new types of crime as well as the commission of traditional crimes by means of new technologies.

Manifold cases show that the Internet can be misused for criminal

---

[1] World Wide Web (WWW) is an Internet service for the dissemination of text- and multimedia contents.

[2] Bleisteiner 1999 *Rechtliche Verantwortung im Internet* 2.

activities, including crimes relating to copyright infringements, libel and hate speech, the transmission of child pornography, agitation against minorities or the disparagement of victims of the National Socialist crimes.[3] Nowadays, all of the above forms of content relating to crimes are accessible from every computer anywhere in the world. Moreover, the consequences of criminal behaviour can be more far-reaching than before the invention of the Internet, because they are not restricted by national boundaries or geographical limitations. The recent spread of computer viruses all over the world has provided proof of this reality.

A society's values find expression in its legal system. The law protects values that are regarded as very important, often by criminal law. This is also the case regarding communication. Since the Internet makes world-wide distribution and reception of information much easier than by traditional means of communication, countries encounter new, hitherto unknown problems of how to defend themselves against forbidden communication content and how to hold the persons who create and distribute such content liable for their actions. The Internet challenges existing legal concepts. Information and communications flow more easily around the world. Increasingly, criminals are located not in the places where their acts have effect, but rather in locations outside of the jurisdiction in which the victims are located.

Moreover, in democratic societies any attempt regulating communication has to be balanced against the important constitutional rights of freedom of expression and freedom of speech.

---

[3] Section 130 (agitation of the people) of the German Criminal Code (Strafgesetzbuch (StGB)) and section 220 (a) (genocide) of the StGB.

Therefore, the purpose of this thesis is to give an insight into the legal difficulties every country faces vis-à-vis this new form of criminal offences. Activities that have been classified as being criminal are, of course, still criminal when committed via the Internet. Therefore, this thesis will not focus on the liability of the authors and the purchasers but will raise the question whether the Internet providers should be held liable for illegal contents on the Internet.

To make the problem concrete, consider an example drawn from the Bavarian prosecution authorities' 1995 threat to prosecute the German subsidiary company of CompuServe America Inc., the CompuServe GmbH[4], for carrying on-line discussions involving persons from around the globe that violated German anti-pornography laws. CompuServe initially blocked access to these discussion groups in Germany. Because CompuServe could not control the geographical transmission of the contents of the discussion- or so-called newsgroups, its response to the prosecutor's regulation had the effect of blocking access to these discussion groups for all CompuServe users worldwide.

The huge significance of the Internet raises the questions: should the Internet providers be held liable for illegal contents on the Internet? Are the existing legal norms sufficient to regulate the actual and the expected conflicts of different interests?

A quotation by American Paul C. Paules about the German multimedia act has been widely circulated on the Internet: "The Americans invented the

[4] (German) private limited company.

Internet, the Germans regulate it. Each does what he can do best".[5]

In two cases, Germany was the first country to create computer-specific laws: the Hesse Data Protection Act of 1970 (*Hessisches Datenschutzgesetz*) and the Information and Communication Services Act of 1997 (*Informations- und Kommunikationsdienstegesetz*). With the so called "multi media act" *Informations- und Kommunikationsdienstegesetz* (IuKD) Germany created the first Internet law in the world. On the basis of this Act, the "Internet provider liability law", the Teleservices Act (*Teledienstegesetz*) was created.[6] Since Germany has taken a leading role in adapting its legal system to the phenomenon of Internet crimes, the thesis will mainly examine the German approach, which may be used as a model for other countries. This paper focuses on liability of Internet providers. The legal problems of modern data transfer have increasingly become a topic of debate in the German legal literature.[7]

Because of the melting of national and international computer networks resulting in the global Internet, a criminal act committed in a single country can affect the worldwide information transfer, raising the question of where the crime occurred. Basically, one faces not only the problem of whether the conventional substantial law is applicable and sufficient but also whether the national law itself is applicable. In other words, one has to examine the international scope of application of the national criminal law and its procedural enforcement.[8] Accordingly, this thesis analyses the applicability of

---

[5] www.unmoralische.de/zitate/zitate9.htm.
[6] See the grounds for the IuKDG-draft BR-Drucks. 966/96, 18, 28.
[7] For example: Spindler *Vertragsrecht der Internetprovider* (1999); Lohse *Verantwortlichkeit im Internet* (2000).
[8] Breuer "Anwendbarkeit des deutschen Strafrechts auf extraterritoriale Internet-Benutzer" 1998 *MMR* 141.

the German criminal law[9] in the light of the global cyberspace and examines the liability of Internet providers. Like the World Wide Web, this discussion is not therefore limited to Germany but concerns all democratic countries. It is an international issue.

In chapter 2 the technical and historical aspects of the Internet are discussed and its target groups determined. Knowledge of the technical background is necessary for any analysis of Internet-related law. The role of Internet providers and their potential liability according to their function will be illustrated by the presentation of cases. In the case of the traditional media like print, television and radio, functions and liabilities are clearly definable. At the beginning of the information-chain is the one who spreads his own contents via the medium, like the journalist or publisher or the editor. At the end of the information-chain we find the reader, TV viewer or auditor. But the boundaries of functions and liabilities have become fluid in the case of the Internet. On the Internet, we find – among others – the so-called content providers who supply their own contents. The access provider offers user's access to the Internet. In so-called newsgroups, it is possible both to contribute one's own information and to use other people's contents. This functional overlapping makes the legal understanding of facts relatively difficult. For that reason the technical functioning of the Internet has to be understood in order to assess provider liability. The presentation of some famous Internet cases will be used to illustrate that legal norms have to be analysed in light of the technical aspects, because the different functions are subject to different legal norms and can accordingly result in different legal

[9] Knauer, ibid.

consequences.

Chapter 3 deals with the problem of whether the Internet is a medium without borders and/or if there is a point of reference for the application of German criminal law. Since legal theory differs from country to country and law is enormously influenced by historical, moral and cultural backgrounds, in some countries a certain activity might not be classified as criminal whereas in other countries the same activity will clearly be considered a criminal offence under the respective legal system. For instance, in some countries freedom of expression has a higher value than the protection of other rights, which demonstrates how differently an activity can be understood in different, nationally moulded legal opinions, thereby leading to conflicting rulings. The protection of minorities and human rights is characteristic for democratic countries. Germany with its history of National Socialism takes firm legal action against crimes like defamation and human rights infringements. South Africa with its history of Apartheid has similar concerns. It is obvious that this attempt at balancing rights can lead to different outcomes in different countries due to differing local values.

Chapter 4 presents several crimes that can be committed via the Internet (such as infringements of personality rights, pornography, etc). They can be divided into so-called computer crimes and post-computer crimes. With regard to these numerous offences, providers feel insecure as to when and to what extent they can be held liable. The crucial question is whether such offences also incriminate the provider who simply offers access to the illegal information of a third party. Germany is one of the first countries to have enacted a law dealing with this question. This "Internet law" also raises new

and complicated legal problems in view of provider liability.

In chapter 5 of the thesis, the criminal liability of Internet providers with regard to the general criminal doctrine in Germany, on the one hand, and on the grounds of the new German Internet law, on the other, is presented. After outlining the German approach, this thesis analyses the Internet law and its regulations in other parts of the world.

In 2002 the European Union passed a new law (E-TDG) that will be presented in the following chapter. Furthermore, I will illustrate how countries like the USA and South Africa are dealing with cyber-crime and the liability of Internet providers. Since nations differ in their regulatory commitments, many Internet transactions will be subject to inconsistent regulations. Unilateral national regulation of the Internet can affect the regulatory efforts of other nations and the Internet activities of parties in other jurisdictions - as the CompuServe case shows. Harmonisation strategies are an important response to the jurisdictional difficulties of Internet regulations. What such harmonisation strategies might look like will be illustrated by the example of the Cybercrime Convention of the Council of Europe.

Finally, this thesis deals with the possibilities of preventing and combating cyber-crime through several measures like filter-software, self-censorship or "codes of conduct".

2 The Internet - participants and technical background

In the following chapter, the various problems caused by the Internet and

its online services will be discussed. In order to illustrate why such problems occur and how they can be solved, a few technical concepts and definitions relating to the Internet must be clarified first.

2 1 Participants involved on the Internet

The participants on the Internet are described using various terms, some of which may have more than one meaning.[10] Usually, the participants are defined in terms of the function that they fulfil on the Internet.

2 1 1 User

A "user" is someone who utilizes a service on the Internet. Such service could be the downloading of data from a website or the copying of a program from the Internet. A user may also be a person who orders something on the Internet or enters into a contract over the Internet. In most circumstances, a user gains access to the Internet via an access provider.

2 1 2 Access provider

The term "access provider" describes an organisation or a company, which offers user's access to the Internet. For this purpose, the user establishes a telephone, cable, or wireless connection with the network of the access provider, which in turn, has a permanent connection to the Internet,

[10] Pichler "Haftung des Host Providers für Persönlichkeitsrechtsverletzungen vor und nach dem Teledienstegesetz" 1998 *MMR* 79-80.

and therefore, to other computers and servers worldwide. An access provider is in other words, the party who owns a computer system, or network, which is permanently connected to the Internet and who sells this access to other users. Thus, a link to an access provider can be considered to be a necessary condition for any use of the Internet.[11]

2 1 3 Network provider

The infrastructure of the Internet consists largely of switches and routers[12], hosts[13] and WAN links[14]. Various government and private organisations whose computers are connected to the Internet, own these switches, hosts and routers. Telecommunications companies, who typically either provide Internet-compliant switching facilities and routing themselves, or lease their capacity to network providers who combine those facilities to create positions on the Internet, own many of the pipes. Telecommunication businesses are intimately involved in the Internet business. Many telecommunications companies have expanded into network and Internet service provision.

Network providers have contractual relations with other networks and their providers, as well as physical links to them. The physical connection enables traffic to directly flow from one network to the next. The contractual relations govern the exchange of information and flow of traffic between the networks.

---

[11] Koenig 1998 *MMR* 6.
[12] Computers designed to receive and forward packets of data.
[13] Hosts store programs and data.
[14] Wide area network telecommunication connections that link the hosts and routers together.

2 1 4 Content provider

On every computer, which is linked to the Internet, services and content can be offered. A content provider is a party that supplies content on its own or another computer. Accordingly, every user can be a content provider, if he provides content.

Content providers are among the most important parties on the Internet. They range from individuals to multinational companies. Content comes in many forms. It can roughly be categorised as real-time content and downloadable content.

2 1 5 (Host) Service provider

The service provider (or host provider) enables a third party to make content available on the hosting server. With this, the service provider performs the combined function of the access provider and the content provider. This is the case when the service provider simultaneously offers access to the Internet and hosts his own content on the network. Examples of service providers are CompuServe, AOL and Microsoft Net. These service providers are also access providers and content providers. Online service providers are service providers that offer access and content, mostly for members or subscribers.[15]

A host is a digital storage facility, accessible via the Internet. The type of

[15] Sieber "Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen" 1997 *CR* 581 (598).

data stored on the host can vary from text documents to graphics, to computer programs or any other kind of data. The way in which the files are stored can vary. A host may also act as a storage facility for Usenet newsgroups or e-mail held in subscribers' mailboxes, or can act as a mail or news server.

The owner of a host can have various connections to the data stored on the host. A company that self-hosts a resource owns and actively controls all of the data. On the other hand, the host owner may have only the most tenuous connection with the stored content. An example of this is the Usenet news server. Usenet is a system of thousands of discussion groups on a huge variety of topics, to which anyone can post public messages. The Usenet host has in practice only two main potential means of control. He can select the newsgroups on his server. The other main control mechanism involves "scrolling off" postings after a few days.

2 2 History and structure of the Internet

The Internet is often described as a network of networks.[16] A lot of terms, which are mostly synonyms, are used to describe the phenomenon of computer networks. These include "cyberspace", "virtual world", and “the net “or” information superhighway"[17] In 2003, the Internet community was celebrating the 20th birthday of the Internet, which was created on January 1, 1983.[18]

---

[16] Hoofacker *Online und Telekommunikation von A-Z* (1995) 98.
[17] Mayer „Recht und Cyberspace“ 1996 *NJW* 1792; Ladeur „Regulierung des Information Superhighway“ 1996 *CR* 614.
[18] www.heise.de/tp/english/inhalte/te/14017/1.html.

The Internet is physically a collection of packet-switched computer networks tied together by a set communication protocol called TCP/IP (Transmission Control Protocol/Internet Protocol). This protocol enables the networks and the computers attached to them to communicate and find other computers attached to the Internet.

Many authors have tried to find a definition for the term Internet. For legal purposes, on October 24,1995 the Federal Network Council (FNC) established, in a resolution, the following definition of the term Internet:

Internet refers to the global system that –

(i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons;

(ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and

(iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein.[19]

The general structure of the Internet is decentralised, as there is no central computer. Instead, the Internet consists of a multitude of connected computers and networks worldwide. This allows for rapid worldwide growth of the Internet through the connection of new computers.[20] Among the most important components of the Internet are the so-called "backbones", the primary high-speed communication links between major data centres to which

[19] Koch *Internetrecht* (1998) 4.
[20] Bleisteiner *Rechtliche Verantwortlichkeit im Internet* (1999) 1.

other networks are connected.[21]

Private Internets, the so-called intranets, are also part of the Internet. Intranets employ the same Internet technology, but are hosted by private servers, which are not accessible to the public via the Internet. Many companies make use of Intranets to facilitate their internal information management, communication and collaboration on projects.[22]

In addition to Intranets, one comes across the term "extranet". This term describes a closed network of user groups of two or more companies. Extranets often result from an extension of a company's intranet.[23]

The special structure of the Internet makes it almost impossible to determine its actual extent. In August 1981, only 213 host-computers existed.[24] Ten years later, more than 1 million computers had been connected to the Internet. By the year 2000 an estimated 330 million people had access to the Internet.[25] The University of Dortmund had the first Internet-access in Germany.[26] The connected computers and networks belong to governments, companies, charitable organisations or private persons. Together they make up a huge, decentralised, global communication medium, called "cyberspace". This system enables people around the world to exchange information almost instantly. Any communication can be directed to a certain person, a group or the whole online-world.

The Internet originated in the United States of America during the time of

---

[21] Börner *Der Internet Rechtsberater* (1999) 18.
[22] Ibid.
[23] Rockey *The e-Commerce Handbook 2000* (2000) 255.
[24] Koch *Internetrecht* (1998) 249.
[25] www.netcraft.com/market, Erster Periodischer Sicherheitsbericht, Bundesministerien des Inneren und der Justiz 2002, 202.
[26] Schwarz *Merkmale, Entwicklungstendenzen und Problemstellungen des Internet* in Prinz & Butz (ed) *Medienrecht im Wandel* (1996) 3.

the Cold War. In those days, the U.S. military feared an atomic strike by the Soviet Union. At first, the Internet was a military network, developed to connect the American department of defence, the Pentagon, with military bases throughout the world. In 1969, the American defence department installed a network called Arpanet (Advanced Research Project Agency Net).[27] The logic of this was to create a network of computers, which would not be dependent on one central computer. The danger of having a centralised computer was that, in the event of a strike, the loss of the main computer would result in the loss of the entire defence system. The goal was to develop a countrywide computer network, which would not fail, even during military attacks. The basis of the communication is the Internet Protocol (IP)[28], a digital standard for moving data around the network. The IP is independent of the computer platform.[29]

Arpanet was so attractive that it was quickly and immensely expanded. By the early 1980s, the Internet had been separated from Arpanet. The host computers on the Arpanet were required to complete their transition from the protocol NCP to the TCP/IP protocol by January 1, 1983. Ten months later, the Arpanet would split into two different networks, the Arpanet and the Milnet. These developments marked the change from the Arpanet as a single network, connecting different computers into the Internet. As the military use and its influence on the Internet decreased, a greater expansion of the Internet became possible. The result was that more and more academic

---

[27] www.vtw.org/speech/decision.
[28] Sieber „Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen" 1997 *CR* 593.
[29] Finke *Die strafrechtliche Verantwortung von Internet-Providern* (1998) 3.

institutions used the Internet system.[30]

In 1986, the National Science Foundation Network (NSFNET) was established, which made transfer of data easier and quicker. From this point onwards, the Internet grew rapidly.[31] With the transfer to private ownership in 1995, the commercial use of the Internet gained huge acceptance worldwide.

2 3 Function of the Internet

From a technical point of view, the Internet merges a huge number of computers, spread out all over the world. These computers are interconnected by a vast number of communication highways; they "speak" the same language or "protocol". The protocol is implemented by specialised software that allows communications between most of these computers. The Arpanet from 1969 also functioned with the help of specialised software, the Network Control Protocol (NCP), which made the decentralised use of the network possible. In the 1980s, the NCP was replaced by a new protocol, the Transmission Control Protocol/Internet Protocol (TCP/IP) that became the standard for moving packets of data around the Internet. The TCP/IP is faster and more efficient than the NCP and is still used today.

In principle, the Internet is the connection of a huge number of networks, which are independent from each other. It basically is a network of nets[32] allowing data to be transported to its destination via vast detours. Data paths of thousands of kilometres are common, even though the computers, amongst

---

[30] www.heise.de/tp/english/inhalte/te/14017/1.html.
[31] Bleisteiner *Rechtliche Verantwortlichkeit im Internet* (1999) 15.
[32] Hoeren „Das Internet für Juristen – eine Einführung" 1995 NJW 3295.

which the data is to be exchanged, may be situated only a few kilometres away from each other. A protocol is a formal set of rules for specifying the format and relationships when exchanging information.[33] It is similar to a language.

The Internet has hierarchic structures. The "backbone" is the primary high-speed communications link between major data centres to which other networks are connected.[34] The job of the backbones is to ensure quicker communication among the individual computers, which in turn allows for faster exchange of data among Internet users.

Difficulties arise in controlling the contents of the Internet, as it is transmitted over winding data highways and is often coded. It is however possible to trace the path that data have travelled in an attempt to identify the author of particular content.

In the traditional media such as press, television and radio, the supplier and the author of information can be easily identified and can therefore be called to account, governmental identification and control of an author publishing on the internet is limited because of the complicated and complex structure of networks. Messages on the Internet can be dismantled into the smallest units.[35] Each of these information units finds its own way through the labyrinth of the Internet.

Different types of information on the Internet have differing life spans. Contents on the servers of content providers are at least temporarily stored.

---

[33] Rockey *The e-Commerce Handbook 2000* (2000) 268.
[34] www.law.vill.edu/vcilp/technotes/whatis5.htm.
[35] Barton *Multimedia-Strafrecht* (1999) 3.

The length of the storage period for www-sites[36] on a www-server for example is not limited. On a news server[37] messages are automatically erased after a specified period of time. Such "long-term storage" of contents does not exist in the case of "real-time services". This communication takes place through a simultaneous and reciprocal sending and receiving of data.[38] The main forum for the spreading of illegal contents in real-time is Internet Relay Chat (IRC)[39], which is often used by paedophile Internet users to make contacts and exchange photo data files.[40]

Because of these possibilities, even an "Internet layman" can use the Internet for illegal activities. To avoid detection and identification, those who do not wish to be caught in their activities use a cyber cafe or Internet-shop, where anyone can chat[41] and "surf"[42] anonymously.

2 4 Misuse of Internet providers

The above technical explanations of the Internet show that different parties are involved in the process of distributing information via the Internet. The different functions, which include the receiving and sending of messages, networking, accessing or providing service, linking and newsgroup moderation, can be illustrated through a study of cases decided all around the world. The criminal liability of Internet providers often depends on their

---

[36] World Wide Web (WWW) is an Internet service for the dissemination of text- and multimedia contents.
[37] Special computer systems which transmit contents.
[38] Sieber *Verantwortlichkeit im Internet* (1999), 38.
[39] Via this Internet service participants can directly enter into contact with each other without time delay.
[40] Sieber *Verantwortlichkeit* 39.
[41] Chatting is the exchanging of text messages in real time.
[42] Surfing is the act of meandering around the Internet from one Web page to another by clicking on hyperlinks.

technical functions. Case law can aid in understanding why criminal liability depends on the technical capability of a provider. Case law further illustrates that it is not easy to distinguish between the different providers, such as the access, service and content providers. Since the Internet is international and crosses borders, foreign case law will be analysed as well.

A famous case, which emphasises the issue of access and network providing, is the *CompuServe* case[43]. In 1995, the public prosecutor of the city of Munich, Germany, put the manager of the German branch of CompuServe under preliminary investigation, as he was suspected of spreading pornographic material over the Internet. German police had served CompuServe with a list of 282 Usenet newsgroups, which, in their view, contained images of violence, child pornography and bestiality. The incriminating content had been stored on CompuServe-USA's newsgroup servers. In response, CompuServe-USA blocked access to the vast majority of the newsgroups by all of its worldwide subscribers, unblocking the newsgroups only after it provided parental control software to its subscribers. Citing section 184[44] (3) of the German Criminal Code, German authorities charged CompuServe-Germany's manager with providing access to illegal content. CompuServe attempted to defend itself under a liability exemption for online service providers in section 5 of Germany's Teleservices Act[45] TDG.[46] However, the court rejected this argument when made on behalf of CompuServe-Germany holding that the subsidiary was not an online service provider by virtue of its simple hard-line connection to CompuServe-USA. On

---

[43] Amtsgericht München 8340 Ds 465 Js 173158/95; *MMR* 1998, 429, 430; www.somm-case.de.
[44] Dissemination of pornographic writings.
[45] Teledienstegesetz TDG.
[46] Wo 5 TDG!!!!

June 3, 1998, the District Court of Munich handed down a two-year suspended sentence and fined the manager US $ 56,200. On November 17, 1999, Chief Judge Lazslo Ember announced the German state court's reversal of the decision. Judge Ember agreed that the technical ability to effectively block content simply did not exist at that time, adding that more could not have been asked of Felix Somm, manager of CompuServe-Germany. This case illustrates clearly that the simple offering of access to the Internet can lead to legal consequences for a provider.

In July 1996, the public prosecution office of Hamburg began investigations into the Internet provider AOL because it was suspected of participating in the spreading of paedophilic pictures. Users had however exchanged such pictures using e-mail. The investigations were therefore dismissed, since the privacy surrounding telecommunications restrains service providers from monitoring the individual e-mail communications.[47]

State prosecutors in Mannheim/Germany were putting pressure on the commercial online service provider T-Online to block access to Internet material the government considered illegal under German law. The German-Canadian neo-Nazi Ernst Zündel[48] had placed Holocaust denying data on his web site in Canada. The prosecutors warned the company of investigations concerning the question whether it was helping to incite racial hatred. Denying the holocaust is a crime in Germany. This was specifically confirmed by the investigation against the service provider giving access to Zündel material. T-Online could be "assisting in inciting racial hatred.[49] T-Online blocked access

---

[47] *Der Spiegel* September 23, 1996, 124.
[48] Zündel is internationally known as a neo-Nazi who seeks to rewrite the history of World War II, saying the Holocaust did not take place.
[49] *New York Times* January 29, 1996 "Germany moves again to censor Internet content".

to the website of the Toronto-based neo-Nazi Ernst Zündel to avoid legal steps against T-Online.

The difficulty in distinguishing pure hosting from possible "colouring" can be demonstrated with the help of two classic American cases referring to the responsibility of online-services for preventing the publication of insulting contents.[50] In 1991 the Federal District Court of New York/USA in *Cubby v. CompuServe*[51] absolved the online-services from responsibility for insults written by third parties.[52] CompuServe had appointed an independent firm to provide and present an internal Journalism Forum. The firm received a letter from a third party, insulting the plaintiff. The author posted this article directly. The court based its decision on CompuServe's lack of knowledge and inability to control the content, since "an online service would only be an electronic (...) library".[53]

In contrast, in *Stratton Oakmont, Inc et al. v. Prodigy Service Co, et al*[54] the court affirmed the responsibility of the online-service, as insulting news was published in its Money Talk forum. The decision was based on the fact that the online-service had marketed the forum's content as being well supervised by filter-software and controlled by external moderators. Because of this distinction the judgment differed from that in the case of *Cubby v. CompuServe*.

Defamatory remarks were the basis of the complaint in the case of *Zeran*

---

[50] www.zeus.bna.com/e-law/docs/tribod.html.
[51] Cubby, Inc., et al. v. Compuserve, Inc., et al., 776 F.Supp. 135 (S.D.N.Y. 1991).
[52] Flechsig „Haftung von Online-Dienstanbietern im Internet" 1996 *AfP* 333-334.
[53] Cubby, Inc., et al. v. Compuserve, Inc., et al., 776 F.Supp. 135, 140 (S.D.N.Y. 1991).
[54] Stratton Oakmont, Inc., et al. v. Prodigy Services Co, et al., 1995 WL 323710 (Trial/IASs pt. 34 Nassau County, N.Y. Sup. Ct. May 24, 1995) (No. 31063/94).

v. AOL.[55] The provider AOL was not held to be liable for the actions of its users anonymously published information stating that the plaintiff had published an advertisement for a T-shirt bearing tasteless references to the Oklahoma City bombing.[56] It was a bad joke. The plaintiff's full name and address were provided in the AOL publication, which led to his being insulted and threatened by angry citizens. The plaintiff demanded that AOL erase the "souvenir advertisement" from the AOL-server. AOL subsequently erased this advertisement without informing the users of AOL that this had been just a bad joke. But soon similar shirts with similar advertisements appeared on the AOL homepage. The plaintiff applied for an injunction and abatement of the information. He reproached AOL for not having reacted appropriately or quickly enough. The case was dismissed under the new Communications Decency Act[57] (U.S.C.).[58] The court referred to 47 U.S.C. § 230 (c) (1),[59] ruling that AOL as the publisher of the insulting statement cannot be held responsible because this would be against the clear wording of the Act and therefore against the intention of the legislature to privilege Internet providers.[60] The court came to the conclusion that the classification of a provider as publisher (*Stratton-Oakment v. Prodigy*) or as a simple operator (*Cubby v. CompuServe*) would stop the provider from voluntarily controlling

---

[55] Kenneth M. Zeran v. American Online, Inc., 958 F.Supp. 1124 (E.D. Va. 1997) aff'd. U.S. Ct. of Appeals 4th Circuit, No. 97-1523 of November 12, 1997 (www.usacaselaw.com/4th/971523P.html).

[56] The „naughty Oklahoma T-shirts" supposedly carried sayings such as „Visit Oklahoma...It's a BLAST!" or „Finally a day care center that keeps the kids quite – Oklahoma 1995".

[57] Titel V of the Telecommunications Act of 1996, Pub.L.No. 104, § § 502, 110 Stat. 56; 133-35.

[58] Wöbke „Meinungsfreiheit im Internet" 1997 *CR* 313-315.

[59] § 230 (c) (1) U.S.C.: Treatment of publisher or speaker – No provider or user of an interactive computer system shall be treated as the publisher or speaker of any information provided by another information content provider.

[60] The intention of that section of the U.S.C. is not to create governmental obligation but to encourage the providers to monitor independently illegal contents on their servers; Gewessler „Das neue US-Telekommunikationsgesetz" 1996 *CR* 626-632.

the contents on his server and blocking them if necessary.[61]

The liability of service providers was also discussed in the case of *Religious Technology Centre v. Netcom*[62]. The plaintiff in this matter applied for a temporary restraining order against the service provider Netcom, as it had allowed third parties access to the Internet, and moreover had enabled them to allegedly save copyright-protected material of the Church of Scientology in a newsgroup on its newsgroup server. Netcom argued that its knowledge after receiving notice of alleged infringement was too equivocal, given the difficulty in assessing whether registrations are valid and in making fair use analyses. Although it refused to hold that liability must be unequivocal, the court did agree that a mere unsupported allegation of infringement does not automatically put a defendant on notice and that if a defendant is unable to reasonably verify a claim of infringement, the defendant's lack of knowledge may be found reasonable, resulting in no liability.

2 5 Summary

The technical explanations of the Internet described in 2 1 above show that various parties are involved in disseminating information via the Internet. The different functions, which include the receiving and sending of messages, networking, accessing or providing service, linking and newsgroup moderation, can be illustrated through case law.

---

[61] U.S. Court of Appeals 1135 FN 23, decision under www.findlaw.com.
[62] Religious Technology Center, et al. v. Netcom On-Line Communications services, Inc., et al., 907 F.Supp. 1361 (N.D.Cal. 1995),

The type of liability and its boundaries for the dissemination of illegal contents must be defined. The cases illustrate that the application of legal norms has to be analysed in light of the technical capabilities and given facts of the new medium, the Internet. It is important to analyse the law with reference to the technical functions of the Internet because on the Internet the same person can fulfil different functions, which are subject to different legal norms and can accordingly result in different legal consequences.

3 General field of application of Internet law

It has never been easier than it is today to contact people from all over the world via email, chat rooms or newsgroups. With no doubt physical borders are losing their significance. Every Internet user can place data on the World Wide Web that can be downloaded simultaneously in more than 150 countries.[63] This opens new dimensions for offenders operating internationally, especially in the area of the dissemination of illegal commentaries and presentations. The omnipresent legal issue arising from this situation is: when does criminal law of one particular nation apply to an offence "occurring" on the Internet.

The Internet holds data from every place and country in the world. Computer systems may be accessed in one country, data manipulated in another, and the consequences may occur in a third country. Trans-national criminality and the competence for the application of national punitive power are problematic in the case of "Internet crimes". The application of national criminal law will depend on whether the offence was committed within the

[63] Cornils „Der Begehungsort von Äußerungsdelikten im Internet" 1999 *JZ* 395.

territorial sovereignty of a country or in a foreign legal system. When an offender uses the Internet for the commission of a crime, the determination of the place of crime can however cause difficulties.

The right of a nation to impose a penalty actually has to be limited under international law.[64] The problems concerning national jurisdiction when a crime is committed on the Internet arise from the fact that the traditional rules concerning the location of a crime have not yet been adjusted to keep pace with technological developments. The traditional rules are fine when dealing with "traditional crime". But when faced with a case where the crime consists of a "mouse click" which triggers the circulation of information in a technically complicated way and without leaving any possibility for the person who used the mouse to control the process, it is difficult both to determine the act and to point to the effect of a potential infringement. What characterises crimes on the Internet is that they are trans-national. The result is that different sovereignties, laws, jurisdictions and rules come into play.

This issue shall be first looked at from an international law perspective and then with special regard to the German jurisdiction.

3 1 Jurisdiction

The existing international rules of jurisdiction were developed when applicability of law was merely a question of were an act was physically committed or which action were to be deemed as the most significant ones. Those rules therefore deal rather poorly with concurrent and conflicting claims

[64] Schönke & Schröder *Strafgesetzbuch Kommentar* (2001) Sections 3-7, 3.

of jurisdiction,[65] which are often resolved by strict territorial limits of enforcement jurisdiction.[66]

3 1 1 Principles of international law

There are however some possibilities which allow for the prosecution of such punishable actions. Points of reference in this regard include the territoriality principle (*Territorialprinzip* or *Gebietsgrundsatz*), the flag-principle (*Flaggenprinzip*), the universality principle[67] (*Weltrechtsprinzip*) and the representation principle (*stellvertretende Strafrechtspflege*). These principles overlap and complement each other. Even with these principles and statutory definitions in place, the determination of the place of an offence and the application of a particular law can be problematic.

Under traditional English common law criminal jurisdiction was limited to crimes committed within the territory of England.[68] But of course no state nowadays is committed to such a restrictive view on criminal jurisdiction. Most states, including Germany, have in fact extended their legal jurisdiction in criminal law matters by appealing to various principles recognised in public international law.

The traditional presentation of international criminal law in doctrine as well as the structure of criminal code invites us to think territorially.[69]

---

[65] Oxman *Jurisdiction of States* in Bernhard (ed) *Encyclopeadia of Public International law* 1987 Vol 10, 277 (282).
[66] Harris *Cases and Material on International law* (1998) 265.
[67] The universality principle mandated that states can prosecute Internet crimes under their own jurisdiction independently from the law of the scene of the crime.
[68] Hailsham Halsbury's Law of England (1990) para. 624. Thus, until the statutory law intervened, an Englishman who killed a person in France did not commit an English crime.
[69] Wong „Criminal Jurisdiction over Internet Crimes" in Holoch *Recht und Internet* (2001) 100.

3 1 2 Relevant international law cases

There is a series of cases, which illustrate the difficulty of applying existing law to a medium such as the Internet.

For example, some American and Asian courts have held resident online providers liable for contents, which could be downloaded through the services of these providers, even if the contents came from abroad.[70] By contrast, a court in Florida (USA) held that it did not have jurisdiction over an online user from New York.[71] This particular user had used a store, which was situated in Florida. The court decided that it did not have sufficient facts to establish jurisdiction, if the only contact between the user and the state of Florida was the use of this information. The court reasoned that to hold otherwise would establish too broad a jurisdiction for local authorities.

In contrast, a court in Tennessee (USA) found that it did have jurisdiction to pass judgement on a couple from California.[72] This couple had been disseminating pornographic material via the Internet. The couple was sentenced to six years imprisonment. A U.S. Federal Appeals Court confirmed the decision. The appellate court reasoned that the couple had acted with the knowledge that the data could be accessed in Tennessee, since the user had accessed it from there.

The former Attorney General of Minnesota stated that authors of illegal data fed into the computer systems from outside the state of Minnesota could

---

[70] SEC v. Scott A. Frye, 95 Civ. 9205; www.sec.gov/news/frye.html.
[71] Pres-Kap, Inc. v. System One Direct Access, Inc., 636 so.2d 1351 (Fla. App. Ct. 1994); www.jmls.edu/cyber/cases/pres-kap.txt.
[72] United States of America v. Robert Allen Thomas and Carleen Thomas, 74 F.3d 701 (6th Cir. 1996).

be punished in Minnesota, In case they know that their data could be accessed from within Minnesota.

A court in New York granted an injunction barring an Antigua-based online gaming company from doing business with New York residents.[73] The court held that regardless of whether gambling is legal in the company's state of incorporation or operation. The court found that the act of entering the bet and transmitting the information from New York via the Internet is adequate to constituting gambling activity within New York State. The company required users to enter a physical address, and rejected customers whose address was in a state where gambling was illegal. However, to test the company's practice, the New York attorney general used a Nevada address from his residence in New York and was hence able to gain access. The court consequently held that the company's measures to screen users was not sufficient to shield the site from liability.

An example of the application of an unrestricted jurisdiction is the French Yahoo! decision[74] where no attempt was made to justify why the relevant action "belonged" to France any more than to any other country.[75] Although the case was a civil action, the actual illegality consisted of a violation of the French Criminal Code, which makes the distribution of Nazi material illegal.[76]

---

[73] State of New York v. World Interactive Gaming Corp, 1999 N.Y. Misc. LEXIS 425 (N.Y. App. Div. 1999); www.cnn.com/TECH/computing/9907/29/gamblelaw.idg.

[74] LICRA & UEJF v. Yahoo! Inc., Tribunal de Grande Instance Paris; www.juriscom.net/txt/jurisfr/cti/tgiparis2000011200.

[75] The Tribunale de Grande Instance de Paris in LICRA & UEFJ v. Yahoo! Ind. & Yahoo France held that Yahoo! Inc., a company incorporated in California must take all necessary measures to dissuade and render impossible any access from French territory via Yahoo.com to a Nazi artefact auction service or any other service or site consisting Nazi crimes. The Tribunal confirmed its decision about the provider liability of Yahoo! on November 20, 2000.

[76] This created room for arguing that the judgement was in fact a penal judgment and thus should have been informed by jurisdictional limitations under international law. This was, amongst other things, argued by Yahoo! Inc. in ist complaint which it filed on December 21, 2000 in the US District Court, Northern District of California (complaint No. C00-21275, at

The Paris court, while acknowledging that the offence committed by Yahoo! Inc. in France was unintentional, based its assertion of jurisdiction on the fact that by "permitting the visualisation in France of these objects and eventual participation of a surfer established in France in such an exposition/sale, Yahoo! Inc. (....) committed a wrong on the territory of France".[77]

3 1 3 German law

The previous examination of international rules of law and of specific cases of different jurisdictions shall now be contrasted with one particular jurisdiction. It shall be analysed when and under which principles German law applies to offences committed on the Internet. The challenge, nevertheless, is the same as mentioned above: by traditional rules the actions are often not committed on German ground.

"Territorial crimes" means that acts committed within the territory of the adjudicating state are still treated differently from "extraterritorial" crimes. Before the different criminal offences that can be perpetrated on the Internet are discussed in chapter 4 in detail, the question must be posed: Is German criminal law applicable and if so, to what extent? I will discuss below this "primacy of territoriality"[78] and argue that the importance given to this primacy is perhaps misplaced. I will then demonstrate that even if one adhere strictly to the territoriality principle the application of this principle in practice may

---

http://pub.bna.com(eclr/21275.htm) and in which it sought declaratory relief that the French orders were neither recognisable nor enforceable in the United States (see: Yahoo!, Inc. v. La Ligue Contre Le Racisme at L'Antisemitisme, 169 F.Supp. 2d 1181 (ND Cal. 2001)).

[77] See the decision of Judge Gomez on May 20, 2000, unofficial English translation available at www.gyoza.com/lapres/html/yahen.

[78] Wong "Criminal Jurisdiction over Internet Crimes" 94.

encompass such a wide scope that it can no longer properly be called "territorial". Given these conflicting considerations, the following chapter of the thesis will show more of a trend in German jurisprudence and legal literature rather than clearly reformulated rules.

Sections 3 to 9 of the German Criminal Code StGB enfold under which circumstances German law can be applied to offences. Section 3 and the sections thereafter, as well as section 9 of the StGB, relating to international criminal law. These norms lay down the scope of the internal state authority by restricting the application of German criminal law to offences that have a connection to foreign countries.[79] If there is no application for German criminal law as a result of a lack of connection or reference to foreign countries, criminal proceedings will be banned. This leads to a withdrawal of the case.[80]

3 1 3 1 The universality principle under German law

The German legislature acted on the universality principle in Sections 5 and 6 of the German Criminal Code. The universality principle (*Weltrechtsprinzip*) allows for an unlimited exercise of jurisdiction to an offence defined in section 6, no.1-9 of the StGB.[81]This principle refers to the

---

[79] Lackner *Strafgesetzbuch Kommentar* (1999) introductory remark to sections 3-7, 2.
[80] BGH 1985 *NStZ* 361.
[81] Section 6 Acts Abroad Against Internationally Protected Legal Interests. German criminal law shall further apply, regardless of the law of the place of their commission, to the following acts committed abroad:
1. Genocide (Section 220a);
2. Serious criminal offences involving nuclear energy, explosives and radiation in cases under Sections 307 and 308 subsections (1) to (4), Section 309 subsection (2) and Section 310;
3. Assaults against air and sea traffic (Section 316c);
4. Trafficking in human beings (Section 180b) and serious trafficking in human beings (181);
5. Unauthorized distribution of narcotics;
6. Dissemination of pornographic writings in cases under Section 184 subsection (3) and (4);
7. Counterfeiting of money and securities (Sections 146, 151 and 152), payment cards and

nature of the crime, which must be of a very high severity, for example genocide or war crimes. The application of German criminal law to the offences mentioned in section 6 of the StGB is unproblematic, as the application is based on the principle of universality (*Weltrechtsprinzip*). This principle includes an enumerative list of particularly severe offences, which are recognised by all legal systems.[82] This principle provides for an exercise of German jurisdiction for the crimes defined in section 6, no.1-9 of the StGB.

This kind of jurisdiction is considered to be in the interest of mankind as a whole and is only restricted by the rules of international law.[83] The principle is based on the idea that there is an international consensus amongst all civilised nations that certain rights must be protected and that it is in the interest of all nations to ensure their protection.

Under the universality principle provided in section 6 of the StGB, German law will be applicable regardless the place of commission or the nationality of the offender. It is also applicable to the distribution of child pornography via data networks.[84] A precondition for the application of German law is that no statutory international law stands in the way of the application of section 6 StGB.

According to section 5 of the StGB, German criminal law is also applicable to acts committed outside of Germany against certain German citizens under legal protection, regardless of the law of the place of

---

blank Eurochecks (Section 152a subsections (1) to (4), as well as their preparation (Sections 149, 151, 152 and 152a subsection (5);
8. Subsidy fraud (Section 264);
9. Acts which, on the basis of an international agreement binding on the Federal Republic of Germany, shall also be prosecuted if they are committed abroad)

[82] Schönke & Schröder *Strafgesetzbuch Kommentar* (2001) Sections 3-9, 7.

[83] Lackner *Strafgesetzbuch Kommentar* Section 13, 2.

[84] Section 6, no.6 StGB.

commission.

The application of German criminal law to offences committed abroad may also be based on section 7 of the StGB.[85] Section 7 of the StGB is relevant where a crime is committed abroad against a German citizen (for example criminal libel against a German via email in a foreign country). According to the representation principle, the national punitive power intervenes in those places where a foreign jurisdiction, which ordinarily would apply its criminal law, is prevented from imposing sanctions, due to the existence of intergovernmental agreements, for example. This principle is defined in section 7 (2) of the StGB.

3 1 3 2 The territoriality principle

The territoriality principle (*Territorialprinzip*) set out in section 3 of the StGB, states that German criminal law applies to acts committed within Germany. This principle determines that authorities of the Federal Republic of Germany can prosecute all offences committed within Germany. In turn, the flag-principle of section 4 of the StGB extends German criminal law to offences committed on board ships and aeroplanes that sail or fly under the German flag.

---

[85] Section 7 Applicability to Acts Abroad in Other Cases
(1) German criminal law shall apply to acts, which were committed abroad against a German, if either the act is punishable at the place of its commission or if the place of its commission is not subject to any criminal law enforcement.
(2) German criminal law shall apply to other acts, which were committed abroad if the act is punishable at the place of its commission or the place of its commission is not subject to any criminal law enforcement and if the perpetrator:
1. was a German at the time of the act or became one after the act; or
2. was a foreigner at the time of the act, was found to be in Germany and, although the Extradition Act would permit extradition for such an act, is not extradited, because a request for extradition is not made, is rejected, or the extradition is not practicable.

According to section 3 of the StGB, German criminal law is only applicable when the offence was committed in Germany. The section expressly states: "German criminal law applies to acts committed within Germany". "Committed within Germany" corresponds with section 9 of the StGB[86] where the offender or the participant committed the criminal act in Germany. This may be the case where the criminal content was put on the Internet in Germany.

Internet providers who have their headquarters in Germany and who are operating from Germany fall under the German jurisdiction in terms of section 9 (1) var. 3 of the StGB.[87] According to section 9 (1) of the German Criminal Code (StGB), a criminal act is committed at every place the perpetrator acted or, in case of an omission, should have acted, or where the result of the offence occurs or should occur according to the understanding of the perpetrator. If the act and the consequence (the statutorily proscribed harm) do not occur at the same place, different places of crimes can be assumed, possibly in different countries. The place of the act (*Handlungsort*) is the place where the perpetrator carries out an action that satisfies the statutory definition of an offence.[88] The place where the result of an act occurs

---

[86] Section 9 StGB Place of Offence
(1) An offence is committed at every place at which the offender acted or, in the case where the offender refrained from an action to which he was obligated, the place at which he should have acted or the place in which the action showed its effects or should have shown its effects in the offender's intention.
(2) Incitement or accessory ship is committed not only at the place where the act was committed, but also at every place where the inciter or accessory acted or, in case of omission, should have acted or where, according to his understanding, the act should have been committed. If the inciter or accessory in an act abroad acted domestically, then German criminal law shall apply to the incitement or accessory ship, even if the act is not punishable according to the law of the place of its commission.

[87] www.anwaltsforum.de/gebiete/straf/pelz/strafrecht.htm.

[88] Dreher & Tröndle *Strafgesetzbuch und Nebengesetze Kommentar* (1995) Section 9, 2.

(*Erfolgsort*) is the location where the consequence comes about.[89] The applicability of German law only requires one of these places *(Handlungs- or Erfolgsort)* to be located in Germany. A similar rule exists in the criminal codes of various other legal systems[90], including those of Sweden, some U.S. states (for example Georgia[91] and New York[92]) and Singapore.[93]

3 1 3 3 Relevant German law cases

In recent years there have been a few milestones of jurisdiction in this particular field of law. A few of those shall now be discussed to represent the current German position on the issue.

An expansion of the reach of national criminal law can be observed in the decision of the German Federal Court of Justice (*Bundesgerichtshof* - BGH) of December 12, 2000 to find the Australian Holocaust-denier Frederic Töben guilty of sedition, based on information found on his Australian-based website.[94] In his publications he denied the mass murder of Jews committed by Germans during the Second World War. Töben had been sentenced to ten months of imprisonment for distributing revisionist leaflets in Germany. The German Federal Court of Justice decided in December 2000 that foreigners might be prosecuted for their online activities, even if these activities originated abroad. The BGH argued, that given Germany's history, there is objectively a special link between Töben's material and German territory,

---

[89] ibid, 3.
[90] Oehler *Internationales Strafrecht* (1987) 269-290.
[91] Georgia Code § 16-9-93.1.
[92] N.Y. Penal Law § 235.21 (3).
[93] Bremer *Strafbare Internet-Inhalte in internationaler Hinsicht* (2001) 86.
[94] Decision of the Federal Court of Justice (*Bundesgerichtshof* - BGH) of December 12, 2000, Reg. No. 1 StR 184/00, published in: *NJW* 2001, 624-628).

which justifies assertion of jurisdiction. It also reasoned that, given the focus of the site on Germans and German history, particularly German users in particular were among the intended addressees of the site.

This content, the Court found, was capable of disturbing the public peace in Germany. The court held that the publication could be prosecuted under German criminal law because although it was published on a server located in Australia, the action was directed against Germany and addressed to the German public. The most interesting aspect of this case is the array of questions concerning both the law of substance as well as issues of procedure. Special attention was given to the question of how to account for the fact that the incriminated publications were distributed through the Internet. The difficult issue before the Court was how to interpret those sections of the German Criminal Code that deal with the principle of territoriality, i.e. whether the Code is applicable to crimes committed outside the German borders.[95] The Internet raises the question of how to define the place where the crime is committed in accordance to section 9 German Criminal Code when precisely these parameters of place and location appear to be in outright contradiction with the nature of the Internet. The Court, drawing on a considerable amount of scholarship[96], held that there was applicability with respect to the effects of the web-publication in German territory.[97] The Court declares the protected good to be closely tied to

---

[95] Decision of the Federal Court of Justice (*Bundesgerichtshof* - BGH) of December 12, 2000, Reg. No. 1 StR 184/00, published in: *NJW* 2001, 624-628).

[96] See chapter 3 1 4.

[97] The Court underlines that the defendant - by "participating" in an ongoing debate about German history and Nazi-crimes - intently addressed his publication to German readers. The court finds that the defendant created a piece of information that had the quality to endanger the communal life between Jews and other groups in the German people. The Federal Court of Justice puts forward the special connection between the defendant's action and the protected good (German public peace).

Germany, especially with regard to German history. It holds this connection[98] to be a further argument for the applicability of German criminal law to the Internet publication in the light of international public law. This does resonate with different voices in German legal publications but also with the common measure taken by the European Council 1996 with regard to fighting racism and hostility against foreigners.[99]

Another famous case is the *Zündel case*. A German prosecutor investigated the providers CompuServe and T-Online because of illegal data that had originated in Canada.[100] The German-Canadian Neo-Nazi Ernst Zündel had placed it on the Internet in Canada. He denied the Holocaust on his web sites. The contents were protected by the Canadian and American constitutions, which are very liberal about the freedom of expression.[101] In Germany however, Zündel's Nazi contents (the so-called Zündel-sites) fulfilled the requirements of the statutory provision of section 130 (3) of the StGB.[102] Section 130 of the StGB combats right-wing extremism and propaganda hostile to foreigners.[103] The prosecutor found that section 130 StGB also

---

[98] For German criminal law to be applied to cases with links to foreign countries there has to be a point of reference, a so-called connecting factor or specific link (*Anknüpfungspunkt*). This factor is necessary to prevent an arbitrary prosecution of criminal offences. It is necessary that there is a certain connection or link between the facts in Germany and abroad. If there is no connection to Germany, the prosecution violates the so-called principle of non-interference (*Nichteinmischungsprinzip)*, which requires that the sovereignty of foreign states be respected.
It has not yet been determined what prerequisites have to be fulfilled to assume such a connection. The application of this rule of law is therefore almost entirely up to the ruling body's or the judge's discretion.

[99] Published in *Amtsblatt der Europäischen Gemeinschaften* L 185, 5.

[100] www.cnn.com/2000/TECH/computing/08/29/hate.sites.idg.

[101] In the United States, the First Amendment protects hate speech. The German Constitution allows free expression only within limits: racial speech is not tolerated under Article 5 of the German Constitution. In 1994, the Federal Constitutional Court decided that Holocaust denial is not protected speech under Article 5 since it expresses a „claim of fact that has been proven untrue" (see: BVerfG *NJW* 94, 1780).

[102] „Auschwitzlüge" (Holocaust denial).

[103] The provision emerged as a reaction to anti-Semitic and National Socialistic recurrences in Germany after the Second World War. It is therefore punishable to approve, to deny or to play down actions committed under the Nazi rule.

includes web pages and corresponding content, managed by foreign nationals on a foreign server, but accessible in Germany, because the content was capable of disturbing the public peace in Germany according to section 9 of the German Criminal Code (crime's effects in German territory).

3 1 4 Proposed solutions to tackle applicability of German jurisdiction

What are in both decisions conspicuous by their absence are references to the laws of other states and to the potential of conflicting regulation. In Germany, through legal definition, the application of the territoriality principle is extended considerably by deeming an act as territorial, not only when it is performed within the territory of the adjudicating state, but also when the effects of the act occur there. The question really is, whether the locality of a criminal act should be irrelevant for certain offences.

Basically the problem is a consequence of different ideologies and different political opinions. On the one hand, democratic countries like Germany, the United States or South Africa have a liberal perspective, which advocates broad freedom of expression with few limitations in the form of criminal political control. On the other hand, the need to criminalize acts which express opinions of a political, religious or sexual character is endorsed. The extension of this liberal perspective is the opinion that a person always has the right to enjoy all the political and civic rights that he enjoys in his state. The extension of the other point of view is the opinion that every state has the right to protect its citizens and itself against criminal information from abroad,

when this information is contrary to the sense of justice in this state.

The problems concerning the national jurisdiction for crimes consisting of illegal texts, topics and contents on the Internet arise in part because provisions concerning such crimes do not contain a requirement of certain external effect. Under German law they are called *Gefährdungsdelikte.*[104] This means that there is no legally relevant effect to use for localising the crime, i.e. the location where the effect of the criminal behaviour occurred. The possibilities of localising the offence to a certain place or country is limited to the place where the act was perpetrated. Such a crime is accordingly deemed to have been committed where the criminal act was perpetrated or, in case of a crime of omission, where the person is situated when he had the duty to act. An example: an American neo-Nazi disseminates threats or expressions of contempt for an ethnic group by creating a web site on the Internet, using his own computer in California. In this example, the crime is deemed to have been committed in California because that is where the offender committed the criminalized act.

3 1 4 1 The principle of the effects of an action

The flexibility of territoriality is understood differently in Germany. In German legal literature some solutions on how to deal with jurisdiction problems can be found. The place where the effects of an action occur (*Erfolgsort*) is important for the application of German criminal law in terms of the dissemination of illegal contents on the Internet. In the opinion of authors

[104] *Gefährdungsdelikte* are classified in "offences of abstract endangerment" and "offences of concrete endangerment".

of German theory on criminal jurisprudence[105], the place where the result of such criminal acts takes place will always be Germany, because the illegal contents can be downloaded in Germany just like in any other country, including the one where they were created. In their opinion, such crimes should be prosecuted as acts committed in Germany.[106]

According to another author[107], the term *Erfolgsort* should be restricted through a subjective interpretation. German jurisdiction should only be applicable if the perpetrator intends to act in Germany specifically. This approach is called the theory of final interest. The argument is based on the fact that section 9 of the StGB is too broad in the area of global communication. Every user of the data highway would have to obtain global legal advice, which is unreasonable to assume. The result of the restricted interpretation is that a person or party will only be punished under German criminal law if it is specifically interested in acting in Germany.

Another view[108] holds that the place where the effects of an action occur (*Erfolgsort*) should only be regarded as being within Germany if there is a direct connection to Germany, i.e. a territorial specification, found by means of objective criteria. Such territorial specification can be in the form of a website designed in Germany or a site making specific reference to German facts or persons.

The determination of the *Erfolgsort* is not difficult in the case of offences like the tampering with data or destruction thereof. The *Erfolgsort* is where the result occurs, for example where the data is stored. Similarly, the *Erfolgsort* of

---

[105] Kuner "Internationale Zuständigkeitskonflikte im Internet" 1995 *CR* 453-455; Conradi & Schlömer Die "Strafbarkeit der Internetprovider" 1996 *NStZ* 368-370.
[106] ibid.
[107] Collardin "Straftaten im Internet" 1995 *CR* 621.
[108] Hilgendorf "Grundfälle zum Computerstrafrecht" 1997 *NJW* 1876-1879.

an offence of concrete endangerment (*konkrete Gefährdungsdelike*) is easy to locate: the place where the effects of an action occur is where the tangible danger happens.[109] The result is the causation of the danger.[110]

3 1 4 2 Offences of abstract endangerment

Offences of abstract endangerment (*abstrakte Gefährdungsdelikte*), for example incitement to commit genocide or the dissemination of pornography, are problematic. Under German criminal law one must differentiate between infringement offences and liability offences. In the case of infringement offences, the completion of the offence presupposes that someone else's legal interests are infringed, for example in the case of damage to property.

In comparison, the liability offence is already committed with the incidence of the endangering. This means that an offence of abstract endangerment (*abstraktes Gefährdungsdelikt*) can occur without any tangible result. These offences do not need the presence of harm or a concrete danger to an object. The mere act itself is punishable because the act is seen as enough of a danger that an additional result is not required.[111] For example, the publishing of child pornography on the Internet or the distribution of a leaflet with racist remarks is punishable in itself. A result is not required. If there is a result, for example someone kills a Jewish or coloured person because the racist leaflet spurred him on, it is not relevant for the fulfilment of an offence of abstract endangerment.

---

[109] Schönke & Schröder *Strafgesetzbuch Kommentar* (2001) Section 9, 6.
[110] ibid.
[111] Cornils "Der Begehungsort von Äußerungsdelikten im Internet" 1999 *JZ* 395.

The dominant opinion[112] is that there is no application of German criminal law for typical Internet offences, because all dissemination crimes are *abstrakte Gefährdungsdelikte* (offences of abstract endangerment). This opinion is based on the view that *abstrakte Gefährdungsdelikte* do not have an *Erfolgsort* (place where the effects of an action occur) and, in the absence of that, German punitive power in terms of section 9 of the StGB cannot be invoked. One exception does however exist, namely section 6, no. 6 of the StGB allows for punitive power for hardcore pornography according to the universality principle.[113]

According to another opinion in German legal literature[114], it is sufficient for punishment under German law that it be possible to download illegal contents in Germany (even if they fulfil the elements of an offence of an *abstraktem Gefährdungsdelikt*). This view is generally rejected in the legal literature because of the borderless Internet, as all illegal content would then be judged according to German criminal law.[115] A novel view is the extension of the term *Erfolgsort* (section 9 (1) of the StGB) so that categories like *Gefährdungsdelikte* (offences of endangerment) no longer matter.[116]

Some authors[117] refer to a "virtual presence" because of the borderless structure of the Internet: every user of the Internet is virtually present in every country in the world. Accordingly, the crime is committed at the same time in every location in the world because it can be downloaded everywhere. It is not unusual in German criminal law to see an act as a unit in a criminal law

---

[112] Lackner & Kühl *Strafgesetzbuch Kommentar* (1997) introductory remark to Section 13, 32; Ringel "Rechtsextremistische Propagnada aus dem Internet" 1997 *CR* 302-303.
[113] See chapter 3 1 3 1.
[114] Collardin "Straftaten im Internet" 1995 *CR* 618-621.
[115] Cornils "Der Begehungsort von Äußerungsdelikten im Internet" 1999 *JZ* 395.
[116] ibid 405
[117] Kuner "Internationale Zuständigkeitskonflikte im Internet" 1996 *CR* 454.

sense, even if the act was committed in different places.[118]

Another solution would be based on the judgment that an act can be perpetrated at the same time in several locations.[119] If the place of the act (*Handlungsort*) is decisive and there can be different *Handlungsorte*, the same has to apply *mutatis mutandis* for offences committed on the Internet, when a criminal offence is committed on two connected servers at the same time. In terms of this view, the previously mentioned American racist who publishes the illegal contents of his web site on a web server in Germany has to be punished under German law. A restriction would mean a clear restriction of German state authority.

3 1 5 Conclusion

From the above discussion, the following conclusions can be drawn: Illegal Internet publications from Germany are always punishable under German jurisdiction in terms of section 3 of the StGB.

A computer crime is also regarded as having been committed in Germany and falling under German jurisdiction, if it is purposefully placed on a German server (as the *locus delicti* is Germany). If the texts made available satisfy the requirements of German criminal law and are made available knowingly by the service provider also in Germany, then the place in which

---

[118] This is accepted in German criminal law for offences with several acts, like robbery. Robbery includes the act *Gewaltanwendung* (use of violence) and the act *Wegnahme* (actual taking). Only the combination of both parts constitutes the offence "robbery". Both acts can be spatially separated.

[119] Cornils "Der Begehungsort von Äußerungsdelikten im Internet" 1999 *JZ* 396.

the data was entered is unimportant.[120]

Illegal contents stored on foreign servers cannot be punished under German criminal law, as the crime is committed abroad. German criminal law is only applicable under certain circumstances (see section 7 of the StGB), for instance, if the criminal act aims at a German object of legal protection[121] or an international object of legal protection[122].

The proposed solutions for applicability of jurisdiction questions may be criticised. The outrage over the CompuServe case[123] was based upon the argument that Germany indirectly "imposed its moral standards across the globe".[124]

The construction of a "virtual presence" would cause very serious problems concerning legal safeguards for the user of the Internet, who would be forced to take into account the possibility of an accusation of a crime in a foreign country, the legal order of which he is quite unaware of or could reasonably not be aware of. The argument that German jurisdiction is applicable if the perpetrator has the intent to act in Germany (final interest) can be criticised because an individual user of the Internet does not have and – due to the technical complexity of the Internet - cannot always have knowledge of the effects of the Internet.

The decision of the German Federal Court of Justice (BGH) in the *Töben case*[125] may also be criticised. The Court ponders at length upon the question

---

[120] Opinion of the Federal Court of Justice (see: *Töben case* (VERWEIs); BGH - 1 StR 184/00).
[121] Defamation of the State and its symbols, sections 5, no.3 (a), (b), 90 (a) of the StGB
[122] Dissemination of "hardcore" pornography, sections 6, no. 6, 184 III, IV of the StGB).
[123] WOOOO
[124] Kohl "Eggs, Jurisdiction and the Internet" in *International & Comparative Law Quaterly* (2002) 579.
[125] See chapter 3 1 3 3.

whether section 9 of the German Criminal Code (crime's effects in German territory) allows a persecution even when the incriminated content was distributed from a website erected in Australia. At the same time, the Court appears to take the matter of the Holocaust denial itself and its incrimination in the Internet almost for granted. One might still ask whether the allusions made by the Court, for example to border-crossing environmental harm[126], are very persuasive. It certainly is highly questionable to compare the spreading of gases or physical rays through space with the Internet and "cyberspace". As a consequence, the quality of the Internet and the effects this has on free speech is not only ignored by the BGH, but also in fact made a non-issue by placing the decision exclusively within the reference system of German substantive and procedural Criminal law. This German ruling is in marked contrast to the reasoning of the New York court in the case *State of New York v. World Interactive Gaming Corp*[127] that focused on the actual actions of local online customers, which were then imputed to the foreign provider to bring him within territorial boundaries.

As German law professor Eric Hilgendorf noted, the matter may be looked at from another side as well: if we can see German Criminal law as claiming a policeman's role for wrongdoing in the Internet, we need to imagine a foreign country incriminating a German national writing in favour of human rights protection in the Internet. That would be the flip side to the claim made by German authorities to persecute Internet contents, even when launched abroad.

Professor Hilgendorf suggests instead the applicability of German

[126] BGH Reg. No. 1 StR 184/00.
[127] See chapter 3 1 2.

Criminal law only in those cases where a specific connection of the offence to Germany is apparent. This proposal of territorially specified crimes again opens the question of how to define in a satisfactory manner just when this territorial connection is given. By taking refuge in a seemingly simple territorial aspect of the crime, the questions of how to establish this territorial effect in a given case remain unanswered. The territorial argument might prove too weak. Even if the intent of the perpetrator to address Germans is stronger than the simple use of the German language, we cannot deny that it will remain a highly arbitrary procedure by which the territoriality of a crime can be established.

While prosecution under German law is possible under certain circumstances, we should consider whether this broad application of German criminal law contravenes the principles of international law. In the debate on Internet-related crimes, we can observe a recurrence of what happened when satellite transmission of radio and TV-programs began years ago. At that time, it was an international task to formulate international rules on the regulation of the criminal responsibility for offences committed in the transmitted programs. In the Nordic countries there was general agreement that the regulation of the criminal responsibility should be based on the legislation in the country from which the program was transmitted.[128]

The same should apply for Internet crimes. Punishing Internet crime has less to do with fair and just results and more with protecting public interests. Germany with its broad definition of the application of German jurisdiction has to be careful not to disadvantage states with a smaller online presence.

[128] Träskman *Internet and Crime* 119.

Provided that each state only claims jurisdiction over a site as far as it affects the state's territory, conflicting claims cannot arise.[129] Moreover, this would correspond to the general principles of international law and the *Lotus* decision[130] of the Permanent International Court. [131] Under the non-interference principle, a link has to be established if a country wants to prosecute crimes that also have links to foreign states.

4 Crimes in Cyberspace

Generally speaking, crimes in the cyber world can be separated into "computer-related offences" and "ordinary crimes". "Computer-related" in the widest sense means offences such as hacking, which typically take place on a computer system compared to "ordinary" (traditional) offences like fraud.[132] No convincing definition has yet been found for the term "computer crime". Generally, it is defined as illegal behaviour involving the processing or the transmission of data,[133] while others[134] define it more strictly as a crime related to the use of computers. In order to clarify the meaning of the term "computer crime", some of the different crimes on the Internet will be described and discussed.

Most computer offences are found in the German Criminal Code, the *Strafgesetzbuch* (StGB), although there are other statutory regulations dealing

---

[129] The German CompuServe judgement was controversial because it effectively precluded concurrent legislation.
[130] *France v. Turkey*, (1927) PCIJ Reports, Series A, No. 10.
[131] In this decision from September 7, 1927, the Permanent International Court agreed that a state may prosecute a crime outside its territory provided that there exists a special connection to the state.
[132] See: Cullen *Computer Crime* in Edward & Waelde (ed) *Law and the Internet* (1997) 207-209.
[133] Barton *Multimedia-Strafrecht* (2001) 23-24.
[134] Bremer *Strafbare Internet-Inhalte* (2001) 61-62.

with computer crimes, for instance the *Gesetz gegen unlauteren Wettbewerb* (Unfair Competition Act) or the *Urhebergesetz* (Copyright Act).

4 1 Introduction to German criminal law

In order to put our problem in perspective, it is necessary to understand the basics of German criminal law.

Case law is not actually a formal source of law in Germany because the function of the courts is to apply the law rather than to create it. The courts are not bound by the decisions of higher courts under a strict doctrine of precedent. However, case law in the sense of principles developed and concretised in judicial decisions is of significant importance. The practical influence of case law is now even more significant than that of academic opinion.

In Germany, an offence is divided into the elements of a crime (*Tatbestand)*, unlawfulness, in English legal terminology: an *actus reus*[135] (*Rechtswidrigkeit)* and guilt (*Schuld*). If one fails, there is no crime and hence no liability. The *Tatbestand* has to meet the statutorily defined elements of the concrete offence. The offence elements are in turn divided into objective and subjective aspects. The objective aspects are the elements which are factual: what happened, how the act was committed and with what instruments. The subjective *Tatbestand* contains the mental elements, the elements that are associated with the mental reasoning of the offender. The offender has to have intent (*Vorsatz*). He has to want or anticipate the result as it is described

[135] Foster *German legal system & laws* (1996) 138.

in the criminal code.

An act that is performed is defined as human conduct carried out by will (*Handlung*) and must also be unlawful (*rechtswidrig*).[136] It is not unlawful if it can be justified by justifications (*Rechtfertigungsgründen*), for example consent (*Einwilligung*) or self-defence (*Notwehr*). Online acts of communication can also be unlawful (*rechtswidrig*) if they conform to the criminal offence of libel, slander or hate speech, but by the same token these online communication acts can be justified (*gerechtfertigt*) on the basis of section 193 StGB (Protection of justifiable interest) or article 5 of the German Constitution[137] (Freedom of speech and expression).

In the area of pornography, the Federal Constitutional Court (*Bundesverfassungsgericht*) decided that pornography is considered to be a form of art and is therefore justified under Article 5 of the *Grundgesetz* (freedom of speech and expression).

Additionally, an offence is only punishable if it is done with guilt (*Schuld*). A person is considered to be guilty if he can be reproached, i.e. called to account because of his responsibility for a criminal offence. This presupposes criminal capacity (*Schuldfähigkeit*) and no grounds for excluding guilt (*Schuldausschliessungsgrund*).

Section 17 s.1 of the German Criminal Code states that one acts without guilt, if he could not know that he acts illegally (for example, if he comes from a country where such an act is legal or habitually respected). This principle also applies to online communication, for instance, if someone advertises something on the Internet, which is legal in his home country, not knowing

[136] Kaufmann *Creifelds Rechtswörterbuch* (1997) under the term "Handlungsbegriff".
[137] Grundgesetz.

that it is illegal in Germany.

However, an adult who downloads child pornography from the Internet can be punished under section 184 (5) of the German Criminal Code because the *Tatbestand* is satisfied: he downloaded pornography (objective *Tatbestand*) and he acted unlawfully with intent. As mentioned previously,[138] under German law punishment is only possible when the requirements of *Tatbestand*, *Rechtswidrigkeit* and *Schuld* are fulfilled.

4 2 Infringements of personality rights (Injuring a person's reputation)

Slander and insult are widespread offences on the Internet. Therefore, defamation liability was one of the first areas of law to be adjudicated in the field of online services. A person who insults another acts against net-internal behaviour rules, but also commits an offence in terms of section 185 of the German Criminal Code (*Strafgesetzbuch* (StGB)). An insult is an attack on the honour of another person, through the declaration of disrespect, deprecation or disregard thereof. The insults offences are independent from the medium through which they are spread. Therefore, insult (section 185 StGB), malicious gossip (section 186 StGB) and defamation (section 187 StGB) may be committed through email. These offences are a criminal law matter in German law and their rules place severe restrictions on free expression. In the first decision relating to insults on data networks, the Magistrate's Court of the city of Rheinbach concluded that the description "Schlampe" (slut) is

[138] See chapter 4 1.

punishable even when such language is the norm in a chat forum.[139]

In addition, the StGB includes special norms, which protect the President and the Federal Republic of Germany against defamatory statements. Section 90 (b) StGB regulates the disparagement of the German constitutional bodies. The insulting of representatives of foreign countries and the insulting of philosophical and religious groups are also punishable under section 103 StGB, if it disturbs the "public peace" (*öffentlicher Frieden*)[140].

The German Constitution (*Grundgesetz*-GG) guarantees the protection of the expression of opinion. This protection is contained in Art. 5 (1) of the GG and is therefore a basic right under the GG. Art. 5 GG provides that everyone shall have the right to freely express and disseminate his own opinion by speech, writing and pictures.[141] Freedom of the press and freedom of reporting by means of broadcast and film are guaranteed. The law of slander, hate speech, insult and defamation seeks to find a balance between the individuals right to a reputation or good name and another's right to free expression.

The legitimate interest of protection against defamation finds its limits in Art. 5 (1) of the GG, as statements made in chat forums must be seen in the light of the basic constitutional right of freedom of expression and the press. The basic constitutional rights of freedom of expression and the press and the right of each individual not to be insulted must be carefully weighed. Freedom of expression can be limited through law. In particular, provisions to protect

---

[139] AG Rheinsbach 2 DS 397/95.
[140] See chapter 3 1 3 3 (*Töben*-case).
[141] Jarass & Pieroth *Grundgesetz für die Bundesrepublik Deutschland Kommentar* (2000) Art. 5, 25.

young people[142] and personal honour[143] bar defamatory statements.

4 3 Manipulation of data resulting in damage to a computer system

In terms of section 303 (a) StGB, whoever unlawfully erases, suppresses, renders useless or alters data may be punished. Data is defined in section 202 (a) of the StGB as "data stored or transmitted electronically, magnetically or otherwise in a not immediately perceivable manner". Section 303 (a) of the StGB was created because the general offence against property damage only covers the destruction or damaging of material objects. The legal interest protected by this provision is the unimpaired disposability of data by the right holder, i.e. others are excluded from the utilisation of that data without consent of the right holder.

In contrast, section 303 (b) StGB[144] deals with computer sabotage, which is the interference in the processing of data either in such manner as mentioned in section 303 (a) (1) StGB or by destroying, damaging, rendering it useless, or by removing or altering a data processing or storage unit.[145]

Section 303 (b) of the StGB protects the right of private enterprises and public administrations to run their computers without malicious intervention.[146] Computer sabotage is a special case of data alteration and results in a more

---

[142] Gesetz über die Verbreitung jugendgefährdender Schriften und Medieninhalte (GjS).
[143] Insult, malicious gossip, defamation (sections 185, 186, 187 StGB).
[144] 303 (b) Computer sabotage
(1) Anybody who interferes with a data processing activity which is of vital importance to the business or enterprise of another or a public authority by
1. committing an offence under section 303 (a) subsection 1 or
2. destroying, damaging, rendering unusable, removing or altering a data processing system or carrier shall be punished with imprisonment not exceeding five years or a fine.
[145] Dreher & Tröndle *Strafgesetzbuch und Nebengesetze Kommentar* (1995) Section 303 (b), 5.
[146] ibid Section 303 (b), 2.

severe punishment. Only if the data processing function of the computer is of vital importance for a business or enterprise, 303 (b) (1) no. 1 applies instead of 303 (a) StGB. It is disputed whether § 303 (b) (2) no. 2 only applies, if the data processing unit or some data storing device is physically damaged, or whether it applies also to the implantation of a computer virus program. If the virus has direct damaging effects on the computer hardware this can be admitted.[147]

Also data spying, section 202 (a), is an offence under German criminal law.[148] The legal interest protected by this provision is the formal right to disposability, i.e. the right holder has a right to determine whom has access to the information contained in the data. The incriminated act is defined as procuring data for the advantage of oneself or another. This means that the control over the information must shift to the offender, but it need not necessarily lead to a complete loss of control on the side of the right holder.

It must be emphasised that simple hacking is not generally punishable in Germany. Instead, there is a lack of a criminal provision against illegal access to computer systems (hacking). The question whether the illegal access to a computer system without any data alteration or computer sabotage - usually referred to as hacking - is punishable under 202 (a) StGB is hotly disputed in German scholarship. The majority of the literature answers in the negative.[149] This is explained with an explicit statement in the legislative report on the

---

[147] Tröndle & Fischer *Strafgesetzbuch und Nebengesetze Kommentar* (2001) Section 303 (b), 7.

[148] Data spying, § 202 (a)
(1) Anybody who without authorisation procures for himself or another person data, which are not meant for him and which are specially secured against unauthorised access, shall be punished with imprisonment for not more than three years or a fine
(2) Data within the meaning of subsection (1) shall be deemed to be only those which are stored or transmitted electronically, magnetically, or in any other not directly perceptible way.

[149] Lackner & Kühl *Strafgesetzbuch Kommentar* (2001) Section 202 (a), 5; Schönke & Schröder *Strafgesetzbuch Kommentar* (2002) Section 202 (a),10.

revision of the German Criminal Code in 1986, which says that merely intruding into a computer system without authorisation was not punishable.[150] The legislature created the provision as part of its legislative efforts against rising commercial delinquency.[151] However, German legal literature[152] suggests that there is no obvious reason why simple hacking should be played down compared to other computer attacks.[153]

The wording of section 202 (a) of the Criminal Code lends itself also to a different interpretation. Committing information contained in a certain data file to memory implies already a procurement of data. Now, upon successfully overcoming the specific protection of a computer system, the hacker automatically gets to know messages from the computer's operation system. If the perceived data contain information (e.g. a password, a file directory, a list of the stored mails), and the hacker memorises it, the intrusion would include a procurement of data and, thus, fit the definition given. There is, as yet, no case law on this particular topic. If data files are opened (e-mail, data sheet, text) and memorised or copied, section 202 (a) of the German Criminal Code applies in any case.

4 4 Sexually explicit materials and (child) pornography

---

[150] BT-Dr.10/5058, 28.

[151] When the lawmaker proposed the provision in 1986, he expressed the opinion that hacking was only an act preparatory to offences like computer fraud and a field of activity for computer-crazy kids (see: BT-Drs. 10/5058, 28).

[152] Sieber "Computerkriminalität und Informationsstrafrecht" 1995 *CR* 103.

[153] In an issued report to the parliament, the Federal government concluded that there is no immediate need for a revision of the Criminal Code provisions related to computer crimes. It stated that the international developments will be carefully studied; this will eventually lead to amendments to the Criminal Code, especially regarding the illegal access to computer systems (www.bundesregierung.de).

Sex sells, and therefore pornography on the Internet has lately received a tremendous amount of public scrutiny. Pornographic images of all variations are available on the Internet. However, many state and federal criminal statutes prohibit the sale and distribution of obscene material.[154] Websites with "sexual" content are not generally forbidden, except where child pornography or so-called "hardcore" pornography is concerned.

Pornography, and particularly child pornography, is a worldwide problem on the Internet. Almost half of all searches made using Internet search engines are seeking pornographic material.[155] For this reason, the Internet is often termed a "heavily used red light district".[156]

4 4 1 Definition of pornography

The term "pornography" is unfortunately very ambiguous. There is no agreed upon definition for (child) pornography in the multinational environment of the Internet, where cultural, moral, sexual, social and legal variations of the entire world make it difficult to define pornographic content in a manner that is acceptable for all.[157]

In the German legal system, pornographic literature and illustrations are, according to the original explanation of the legislature, pornography when

---

[154] For example in German section 184 StGB; UK Obscene Publications Act 1959; Communication Decency Act USA; Films and Publications Act South Africa.
[155] Lloyd *Information Technology Law* (1997) 219.
[156] For a collection of materials on the topic see www2000.orgsm.vanderbilt.edu/cyberporn.debate.cgi.
[157] "The regulation of pornography and child pornography on the Internet", elj.warwick.ac.uk/jiltx97-1aKDZ/default.

they exclusively or mainly intend to serve as a "sexual stimulus".[158] In addition, the material is pornographic when it clearly oversteps the border of "sexual decency".[159] Jurists have however criticised this definition, as it does not correspond with the present moral standards and values of society and it is not a clear guide.[160]

In Germany, representations (writings, broadcasting etc.) with sexual contents fall under the *nomen collectivum* of pornography.[161] So-called "hardcore" pornography refers to material dealing with acts of violence, the sexual abuse of children or sexual acts with animals.[162] Section 184 (1) StGB aims at the protection of children and young person. After the entry into force of the *Informations- und Kommunikationsdienstegesetz*[163] (IuKD) 1997, section 184 StGB was modified through the IuKD. Under the new regulations photomontages including child pornographic elements are regarded as "hardcore" pornography.

"Simple" pornography is defined as "a raw presentation of sex in a drastic and direct way, which reduces the human being to an object of sexual desire".[164] In Germany the isolated presentation of genitals or the simple representation of sexual intercourse is normally not seen as pornography.

4 4 2 Pornographic writings

---

[158] BT-Drs. VI/1552; Dreher & Tröndle *Strafgesetzbuch und Nebengesetze Kommentar* (1995) Section 184, 6.
[159] ibid.
[160] ibid.
[161] See section 119 (3*) Ordnungswidrigkeitengesetz* (Administrative Offence Act).
[162] Schönke & Schröder *Strafgesetzbuch Kommentar* (2002) Section 184, 4.
[163] Law to Regulate Conditions for Information and Communication Services.
[164] The German legislature decided to restrict the publication of "simple" pornography because of the enormous significance of the Basic Right of Article 5 of the German Constitution (freedom of expression), BT-Drs. VI 1552, 33, VI 3521, 58.

The central term of the pornography offences defined in section 184 StGB is the term "pornographic writing". The term "writing" is defined in section 11 (3) StGB and includes sonic and pictorial recordings as well as illustrations and other representations.[165] The coming into effect of the *Informations- und Kommunikationsdienstegesetz* (Law to Regulate Conditions for Information and Communication Services) in 1997 broadened the definition of the term to include "data storage".[166]

4 4 3 Offering and providing access to pornography

Whoever brings a person under the age of 18 years into contact with pornography can be punished under section 184 (1) no. 1 and no. 2 StGB.[167] German criminal law punishes the advertisement, transfer and the access to pornographic material if the "customer" is younger than 18 years old.

It is not necessary for the young person to actually take notice of the pornographic material. On the Internet, "making the content of a website accessible" occurs when the electronically saved information can be called up

---

[165] Lackner & Kühl *Strafgesetzbuch Kommentar* (1999) Section 11, 3.

[166] In its original meaning, the term "writing" was based on the printed representation thereof and the traditional form of communicationg information. The *Informations- und Kommunikationsdienstegesetz* (Law to Regulate Conditions for Information and Communication Services) closed the loophole in the law and filled the "liability gap". Presently, the term „"writing" includes electronic, electromagnetic, optical, chemical and other forms of data storage (see: BT-Drs. 13/7385, 36. With the *Informations- und Kommunikationsdienstegesetz*, specially geared to the legal problems connected with the Internet and its misuse, regulations about the liability of providers were created for the first time anywhere in the world).

[167] Section 184 Dissemination of Pornographic Writings

(1) Whoever, in relation to pornographic writings (section 11 (3)):

1. offers, gives or makes them accessible to a person under eighteen years of age,

2. displays, posts, presents or otherwise makes them accessible at a place accessible to persons under eighteen years of age (...) shall be punished with imprisonment for not more than one year or a fine.

and can be seen on the screen.[168] This does not include situations where the young person obtains the specifically secured pornographic material through criminal means or illegal access.[169]

4 4 4 Dispatch businesses

Section 184 (1) no. 3 and no. 4 StGB prohibits the advertising or transferring of pornography.[170] The accessibility of pornography is being granted whenever a homepage or a newsgroup offering pornographic material will be set up, enabling the access to the corresponding contents. The reason for the strict approach towards dispatch-businesses is that there is no trustworthy and reliable age-control system. As a result of this, pornographic adverts are not permitted on German servers, regardless how safe the access control of the web server may be.[171]

4 4 5 Public adverts of pornography

It is also forbidden to publicly advertise pornographic writings to persons under the age of 18 years.[172] Under German criminal law, pornographic

---

[168] OLG Stuttgart *NStZ* 1992, 38. BVerwGE 85, 169, 175f..
[169] Punishment is excluded for example when a sealed parcel is opened (see: OLG Karlsruhe *NJW* 1984, 1975-1976).
[170] Section 184
(1) Whoever, in relation to pornographic writings:
1. (...) offers or gives them to another (...) through a mail-order business (...);
2. undertakes to import them by means of a mail-order business (...) shall be punished.
[171] Strömer *Online-Recht* (1997) 93.
[172] Section 184

suppliers are allowed to attract the attention of web users and inform them that they hold in reserve an offer for adults only. It is however not permissible to indicate on the "entry page" that this offer contains pornography.[173] The reason for the statutory prohibition of "porno advertising" on the Internet or elsewhere is to prevent persons under 18 years of age from becoming interested in pornographic materials and to prevent their attention being attracted to the source of supply. [174]

4 4 6 Public cinema performance

Public cinema performance for payment is illegal in Germany when it has a pornographic content and the payment is for the performance itself (Section 184 (1) no.7 StGB). The definition of "film" is not clear in German criminal law. The traditional meaning of the word "film" in German is "a strip made from a material coated with a photosensitive layer" or "a sequence of moving pictures, which are projected on a screen".[175] In the German legal literature[176] "film" is defined as the "transformation of a picture and/or sound – carrier into pictures and sounds".[177] According to the predominant opinion,[178]

---

(1) Whoever, in relation to pornographic writings:
5. publicly offers, announces, or commends them at a place accessible to persons under eighteen years of age or into which they can see, or through dissemination of writings outside a business transaction through normal trade outlets (...) shall be punished.

[173] Schönke & Schröder *Strafgesetzbuch Kommentar* (2002) Section 184, 31.

[174] BGH 34, 98, 219.

[175] Duden *Das große Wörterbuch der deutschen Sprache* (1978) under the term "film".

[176] Legal literature such as legal publications or writings of judges and academics may be important enough to be considered as a quasi source of law, although they are not formally recognised. The historical section emphasised the important role played by the universities in the development of German law and so today German legal literature plays much greater role than in common-law countries (see: Foster *German legal system & laws* (1996) 116).

[177] Dreher & Tröndle *Strafgesetzbuch und Nebengesetze Kommentar* (1995) Section 184, 24.

[178] The work of highly reputable authors can carry considerable persuasive authority. This authority is particularly enhanced when it forms part of the dominant view of a number of texts

the prohibition does not include photos, graphics or pornographic slides.[179] It is a totally different situation, when for example a peep show is shown on the Internet. It is questionable whether this is a "film" and is therefore punishable under section 184 (1) no.7 StGB. There may be doubts since what is actually "broadcasted" on the Internet (for example, the peep show) has never been in contact with celluloid, the typical film-material.[180]

4 4 7 Dissemination and possession of pornography

Whoever disseminates and/or gains possession of "hardcore" pornography may be punished in terms of section 184 (3) no.1[181] and subsection (5) [182] of StGB.

In a case heard before the provincial high court of Bavaria (*Bayrisches Oberlandesgericht* (BayObLG)), a man downloaded child pornography and sent it via email to five other persons.[183] It could not be established whether these five persons actually opened the email and downloaded the

---

or legal writers. This is the so-called *herrschende Meinung* (see: Foster *German legal system & laws* (1996) 121).

[179] Dreher & Tröndle *Strafgesetzbuch und Nebengesetze Kommentar* (1995) Section 184, 24.

[180] In German criminal law the possible literal meaning of the norm marks the extreme limits of possible judicial interpretation. This is based on the principle of prohibition of analogy (*Analogieverbot*). This follows from Art. 103 (3) of the German Constitution (*Grundgesetz*), which requires that a deed can only be punished if the punishment was statutorily determined before the deed was committed. For criminal law this means that the possible literal meaning of the norm marks the extreme limit of permissible judicial interpretation (see: BVerfGE 71, 108, 115).

[181] Section 184
(3) Whoever, in relation to pornographic writing, which have as their object acts of violence, the sexual abuse of children or sexual acts of human beings with animals:
1. disseminates them (...) shall be punished.

[182] Section 184
(5) Whoever undertakes to gain possession of pornographic writings (...) which have as their object the sexual abuse of children, if the writings reproduce an actual or true-to-live event (...) shall be punished (annotation : the criminal intent has to be concerned with the possession, i.e. possession without malice aforethought will be exempt from punishment).

[183] BayObLG, resolution of June 6, 2000, 5 St RR 12/00.

pornographic attachments. The person who obtains possession of pornographic writings (pictures) is subject to punishment even if he never took notice of the pornographic material.[184] Knowledge of pornographic material is not required.

Furthermore, the BayObLG had to decide whether the accused could also be punished under section 184 (3) no.1 StGB for the dissemination (*Verbreiten)* of the pornographic material. Accordingly, the mere dissemination of pornography is considered to be liable to prosecution. Whether or not somebody else will take notice of the pornographic material does not make any difference. "To disseminate" implies something real, something physical. The literal meaning of *Verbreiten* is that the pornographic material is distributed in physical form. For a long time one could be punished for the dissemination of pornographic writings only if the storage medium itself was distributed.[185] An alternative view is that "dissemination" is also the transmission by electronic means, merely by way of downloading.

In 2001, the Federal Court of Justice (*Bundesgerichtshof* (BGH)) ruling brought this uncertainty to an end.[186] Dissemination in the sense of section 184 (3) no. 1 StGB is not only the dissemination of the data storage medium itself but also applies if the data is transmitted via Internet and "arrives" on the computer of the receiver, no matter if this happens through up- or downloading.[187] In both opinions the term "to disseminate" in the sense of section 184 (3) no. 1 presupposes in addition, that the pornographic material reaches a large number of people. In the opinion of the German Federal Court

---

[184] *ComputerrechtIntern* 2000, 173.
[185] For example disc, CD-ROM, DVD (see: Tröndle & Fischer *Strafgesetzbuch Kommentar* (2002) 44).
[186] BGH – 1 StR 66/01; BGHSt 13, 257; BGH *CR* 2002, 45-46.
[187] ibid; Tröndle & Fischer *Strafgesetzbuch Kommentar* (2002) 44.

of Justice section 184 (3) no. 1 StGB is only fulfilled if the transmission is to so many people that the "circle of those who obtain knowledge about the material is not controllable anymore".[188]

The BayObLG found the accused guilty of "possession" of child pornography,[189] not its dissemination, and he received one year and four months of probation. Five persons received the child pornography via Internet. In the opinion of the court, distribution to five persons is not punishable because five persons are a controllable circle of people. In consequence of this and the BGH's judgement, the mere possession of child pornography will be liable to prosecution. So under German law, even a quick look at it on the Internet is punishable, whereas the dissemination of pornography via Internet will not invariably incur a penalty.

4 5 Infringements of copyrights

4 5 1 Criminal aspects of copyright law

In the mailbox and Internet world the unauthorised copying of computer software is common. A copyright is a form of protection provided by German law, as well as in most other legal systems of the world. Copyright law (*Urheberrechtsgesetz* (UrhG)) protects the rights of those who create what the law refers to as "original works of authors".[190] In essence, it is a grant of certain exclusive rights to authors in order to allow them to commercially exploit their work (sections 15ff. UrhG). Protected works include computer

[188] BGH – 1 StR 66/01.
[189] Section 184 (5) StGB (see chapter 4 4 7)).
[190] Definition in section 7 UrhG.

programs (section 2 UrhG). The unlawful exploitation of computer games is covered by section 108 (1) no.7 UrhG.

The German copyright law was amended to deal with computer crimes in 1993 when the Second Act to Change the Copyright Law (*Zweites Gesetz zur Änderung des Urheberrechtsgesetzes*, June 9,1993)[191] was enacted. A new statute came into force in Germany on September 10, 2003 in order to address the effects of digital technologies on copyright and related rights legislation.[192] Apart from bringing German law in line with requirements of the two 1996 WIPO Treaties,[193] the bill was also designed to implement the European Union Copyright Directive[194] of May 22, 2001.

The "Law to regulate copyright in the information society" as it is called makes it illegal to reproduce copy-protected or bootlegged CDs and DVDs. It is seen as an additional tool in the fight against Internet and software piracy and is meant to prevent people from downloading music or films from Internet file-sharing platforms.

Given the massive lobbying by authors' and producers' associations, representatives of consumer interests and other groups, which had already accompanied the legislative efforts on the European scale, an exhaustive reform in due time was almost illusory. The completion of Germany's entry into the information age is therefore left to a so-called "Second Basket" of copyright legislation. Preparations of the envisaged follow-up have already

---

[191] Bundesgesetzblatt (BGBL – Federal Law Gazette), Part 1 910.
[192] German Law on the Regulation of Copyright in the Information Society (*Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft*), Federal Law Gazette Part I, No. 46, September 12, 2003, 1774 – 1788.
[193] WIPO Copyright Treaty, December 20, 1996, 36 I.L.M. 76, WIPO Publ. No. 227 (E).
[194] Directive 2001/29/EC of the European Parliament and of the Council, May 22, 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, O.J.L. 167, 22/06/2001, 10-19.

started and are supposed to be completed by the end of 2004.[195]

4 5 2 MP3 and peer-to-peer

One of the most controversial topics in the area of online law is MP3 music data files.[196] In the early 1990s the Frauenhofer Institut in Germany developed the Format Moving Picture Experts Group I Audio Layer 3, better known as MP3. Experts estimate that 80, 000 musical works are stored without authorisation on approximately 26,000 websites. Around three billion pirate copies of CDs and DVDs are produced in Germany every year.[197]

Pieces of music have always been copied since the invention of the cassette recorder. But this earlier kind of "music piracy" took time and involved a loss in purity of sound. The economic losses were not dramatic. With MP3, music pieces can be copied through downloading in seconds without losing tone quality. Since the development of MP3 the world's biggest record companies have taken legal action against file-sharing services like MP3.com, Napster Inc. and Gnutella because of loss of revenue.[198]

In the first conviction for MP3 piracy a 22-year-old student at the University of Oregon was given a suspended sentence of two years with probation under the U.S. No Electronic Theft Act (NET).[199] The student had transmitted data files worth 70,000 U.S. dollars via the university server. The

---

[195] The German Ministry of Justice's press-release, September 16, 2003 at www.bjm.bund.de /ger/service/pressemitteilungen/10000790.

[196] MP3 is a digital format of encoded audio signals. These signals are digitalised by computer and attain almost CD-quality. The controversy arises from the fact that the downloaded music from the Internet deprives the musicians, composers, and record companies of revenue.

[197] www.dw-world.de/dwelle/cda/detail/dwelle.cda.detail.

[198] www.nytimes.com/library/tech/00/08/biztech/articls/31music.html.

[199] www.zdnet.co.uk/news/1999/46/ns11739.html.

NET had been enacted in December 1997 to prevent copyright infringements on the Internet by instituting criminal penalties.[200]

In Germany the criminal nature of downloading MP3 data files from the Internet was a controversial question as well. There has been a tendency to extend privilege to those persons who download music pieces for private use only in terms of section 53 (1) of the former UrhG. Section 53 (1) UrhG allowed, without any criminal law consequences attached, the copying of data files for private use, i.e. its reproduction inside the domestic area or amongst friends or other persons to whom the person who downloaded the files has a special relationship. Private use does not apply to a disc jockey in carrying out his profession.

Section 53 of the new German Copyright Act now sets the conditions of what is permissible under German copyright law, regarding the reproduction for private and other persons´ uses. Despite considerable pressure by publishers' organisations, the legislature decided to maintain the already-existing provision in section 53 (1) UrhG, which allows private copies to be made by other persons.[201]

Today, online delivery of digital copies is a heavily contested field of use for this provision. Under the amended section 53 (1) such a service

---

[200] Section 2319 in conjunction with section 506 (a) United States Copyright Act (U.S.C.A.) render punishable the illicit and wilful reproduction or distribution of copyrighted works, even if the defendant acts without a commercial purpose or does not expect private financial gain. According to the definition laid down in 17 U.S.C. § 101, the term "financial gain" includes even the expectation of receipt of anything of value including the receipt of other copyrighted works.

[201] Under § 53 of the "new" German Copyright Act, digital private copies for domestic non-commercial use remain permitted.

would be permissible, provided no payment is received.[202] By now, reproductions are prohibited if the source is "obviously unlawful". The clause mainly intended to prevent downloads from the so-called "peer-to-peer"[203] platforms.[204] Yet, some commentators have already highlighted a snag: as the wording draws explicitly on the way the source was *produced,* it could be argued that a legally *produced* copy which is later merely *posted* on an illegal platform, does not match this provision.[205] Sooner or later, the tribunals will have to provide clarification. In any case, the requirement for an "*obviously* unlawful source" somewhat reduces the costumer's risk of unknowingly committing a breach of law. Up to now there have not been taken any proceedings against Internet providers of file trading sites in Germany. As for prosecuting Internet piracy it is only the user who is brought into focus by the German copyright law. For the first time in Germany, and in disregard of the legal uncertainties,[206] a German court imposed a fine of Euro 400 on a user who offered thousands of music titles via Kazaa's file-swapping network. [207]

In the USA, in Australia and the Netherlands, things are different: the entertainment industry applying a great number of lawsuits, tries to take proceedings against file trading sites such as Kazaa und Morpheus.[208]

In June 2004, investigators of the Australian recording industry raided Sydney's offices of Internet file-swapping network Kazaa in search of

---

[202] However, according to a ruling of the German Federal Court of Justice of 1999, any delivery of copies sets off a claim to appropriate remuneration for the author which is to be exercised by a collection society (February 25, 1999, Case no. I ZR118/96).
[203] peer-to-peer is the sharing of computer resources and services by direct exchange between systems.
[204] Demand of the *Bundesrat* (Upper House of German Parliament) that the Mediation Committee be convened, May 3, 2003, Bundestag Printed Paper 15/1066, 2).
[205] Lüft in Wandtke/Bullinger (ed) *Ergänzungsband zum Praxiskommentar Urheberrecht* (2003) § 53, 13.
[206] See page 57.
[207] Amtsgericht Potsdam, AFP, June 8, 2004.
[208] www.washingtonpost.com/ac2/wp-dyn/A12994-2004jan13?language.

evidence to support allegations of copyright infringements. In the Netherlands and the USA, however, proceedings against file trading sites were dismissed. The U.S. District Court in Los Angeles found that the creators of the file-trading network Morpheus, Grokster and StreamCast should not be held liable for copyright infringement in which users of their peer-to-peer software might be engaged. The court decided that the two companies were not able to directly control the files traded on networks using their software, and thus did not substantially contribute to infringement.[209]

In the case of Kazaa v Buma/Stemra, the first European decision to protect a file-swapping website against liability for copyright infringement, the Supreme Court in the Netherlands overturned the District Court's ruling that Kazaa was liable for copyright infringement.[210] According to the Supreme Court Kazaa was not responsible for the illegal actions of its users.[211] This decision, as it is widely believed, does not rule that file sharing is legal. It ruled that Kazaa could not be forced to take measures against illegal use of the software.[212]

The decisions mentioned above will take effects on the entire peer-to-peer industry. Record companies might be more prepared for licensing their titles to file trading sites. So Apple's iTunes Music Store and Sony's Connect try to provide against their smaller turnover rates by offering legal downloads

---

[209] www.usatoday.com/tech/news/techpolicy/2004-02-06-kazaa-raid_x.htm.

[210] Hoge Raad der Nederlanden's-Gravenhage LJN-nummer: AN 7253 Zaakur: C 02/186HR (December 19, 2003); www.rechtspraak.nl/hoge_raad.

[211] The Supreme Court settled the issue in 1984 ruling that Sony's Betamax video cassette recorder had "substantial noninfringing use". As for the Betamax case the judge understood that video cassette recorders had many noninfringing uses, and that Sony was not liable if some of its customers also used them to make copies of copyrighted movies (Sony Corp. of America v. Universal City Studios, Inc.; 464 U.S. 417, 104 S.Ct. 774 C (1984)).

[212] Time will tell whether the American congress may agree to the decision. At present experts are discussing controversially about Kazaa´s facilities of stopping illegal downloads. (www.washingtonpost.com/ac2/wp-dyn/A12994-2004jan13?language).

of music titles.[213] Basically however, the entertainment industry will refocus on copyright legislation and on prosecuting individual file traders.

In principle, the Internet and related developments in technology have altered and will continue to change profoundly the ease with which people may engage in infringing activities. The technological advances will provide prosecutors with novel challenges prosecuting online intellectual property violations.

4 6 Conclusion

The above survey illustrates how activities carried out on the Internet can infringe many different statutory provisions.

We can distinguish two different forms of crime: firstly, a classical computer crime and secondly, a post-computer crime. As a rule, the aim in cases of post-computer crime is no longer the influence of data or data processing, but rather the misuse of information technology via the dissemination of illegal content or the infringement of the rights of a third party to this information. Computer crime arose from the use of computers as simple "working assistants". New forms of computer crimes, the so-called post-computer crimes, developed with the growing global exchange of information via the Internet. Since the beginning of the 1980s, the computer as a working assistant has entered the working world and data protection has become an important issue. Previously unknown forms of criminality like "hacking" or computer espionage have arisen and have been summarised

[213] Deutsche Presse Agentur, June 15, 2004.

under the term computer crimes.[214] In the area of computer crimes, the main focus was on the protection of data, data processing and protection from data misuse of property that is restricted. These areas were recognised as being in need of legal protection during the development of data processing. In the area of multimedia, new forms of crimes are developing, which are no longer comparable with the conventional offences, but exhibit other characteristics. The spreading of information with illegal contents like pornography and the infringement of third parties' rights, for example through software piracy (so-called post-computer crimes)[215] are now arguably bigger threats than the attainment of a financial benefit or the manipulation of data processing.

The above survey illustrates likewise that Internet service provider like Kazaa and Napster are mainly in the firing line for indirect infringements of copyright. In Germany until now it is only the user of file sharing platforms who is brought into focus by the German copyright law.

5 Criminal liability of Internet providers

The traditional thinking has been that the position of an Internet service provider equated with that of the traditional telecommunications carrier, that it was merely a conduit that passively allowed for the transmission of data and was therefore not responsible for the nature or character of the data. The simple logic behind this thought is that it would be unjust, unreasonable and impractical to expect an Internet provider to monitor all of the services that it may give access to, so as to safe guard against illegitimate use and or

[214] Winkelbauer "Computerkriminalität und Strafrecht" 1985 *CR* 40-45.
[215] Barton *Multimedia-Strafrecht* (1999) 23-27.

criminal activity. This is an approach that is based in true practicality. Many Internet providers host numerous web-based services, which themselves allow access to countless websites and services. It has often been contended that placing such a burden on an Internet provider would adversely affect the free flowing nature of the Internet.

A broad discussion about provider liability in terms of the dissemination of punishable information has developed in German law. This complex area of law can be divided into two time periods. Firstly, the period before 1997 when liability of providers was regulated by the principles of traditional criminal law and secondly, the period after 1997, after section 5 of the Teleservices Act (*Teledienstgesetz* (TDG)) was enacted to specifically regulate the liability of Internet providers.

The following chapter will illustrate, how and under what circumstances provider liability can be determined and how the TDG should be interpreted. Among the questions to be addressed: Should the TDG be seen as a type of filter, which operates before ordinary criminal law is applied? Or, has it amended traditional criminal law?

5 1 Traditional criminal liability

The liability of an Internet provider is normally based on traditional legal principles.[216] These principles include the rules about perpetration through action (*Tun*) or omission (*Unterlassen*); guarantor's obligations[217] (section 13

[216] Sieber "Verantwortlichkeit von Internetprovidern im Rechtsvergleich" 1999 *ZUM* 198.
[217] Fisher *German legal system* 137.

(1) StGB, the so-called *Garantenpflicht*)[218]; and the rules of perpetration (*Täterschaft*) and participation (*Teilnahme*). These general and fundamental questions were discussed during the *CompuServe* case[219] in Munich. The principles of the act or conduct and omission were developed by the German judiciary[220] in accordance with the criterion *Schwerpunkt der Vorwerfbarkeit* (basis for liability /main emphasis of guilt)[221] which is still the dominant view in German criminal law.[222]

5 2 The regulation of providers in terms of German criminal law

To evaluate the actions of Internet providers in terms of criminal law, one must first consider the quality of the acts of the alleged offender. Then the extent of his participation in an action that is possibly punishable must be determined.

5 2 1 Definition of conduct (positive act) and omission

All the possible Internet offences are committed through an act or an omission. Omission (or crime through a non-action or non-act) can be separated into genuine and non-genuine omission. A genuine omission is

---

[218] Section 13 StGB Commission by omission:
(1) Whoever fails to avert a result, which is an element of a penal norm, shall only be punishable under this law, if he is legally responsible for the fact that the result does not occur, and if the omission is equivalent to the realisation elements of the crime through action.
[219] AG München 1998 *MMR* 429.
[220] Dreher & Tröndle *Strafgesetzbuch Kommentar* (1995) section 13 StGB.
[221] Schönke & Schröder *Strafgesetzbuch Kommentar* (2002) section 13, 4.
[222] German jurisprudence limits the act of omission on the basis of where the main emphasis of the action lies. Let's take the case of someone who is starving: the main emphasis lies in the omission – that is, in the omission of providing food. Another example: if I take away the lifebelt from someone who is drowning I omit to save him, but the basis of liability lies in the conduct – the taking away of the lifebelt.

defined in German criminal law in section 323 (c) of the StGB.[223] A non-genuine omission is the mirror image of an offence by commission. Almost all norms of the StGB punish illegal actions, but they include, like a mirror image, the omission. For example, there is no difference in German criminal law between the scenarios where a mother poisons her child (active) and letting the child starve or drown in a swimming pool (non-genuine omission). This is not stated as such in German criminal law, but it is considered to be the mirror image of section 211 of the StGB (first-degree murder). An omission corresponds to an action, if the incident would not have occurred had the illegal omission not taken place and this can be said with a probability that borders on certainty.[224]

In order to examine the liability of Internet providers, one first has to determine, whether the activity of the provider is an act or an omission. An act is, for example, the establishment of the Internet communication, while an omission could be the failure to prevent the access to illegal contents on the Internet or the failure to control certain contents. First, the case where the Internet provider acts as a *content provider* and places his own contents on the Internet will be examined. Only in this scenario is an active commission possible.

This situation becomes problematic where the provider acts as a *hosting provider* and permits someone else to store material on his computer, who runs a computer system as an access-provider or makes it possible to establish a connection to such servers which store illegal contents, allowing

[223] Section 323 (c) StGB states that the genuine omission occurs in a situation where there is a specific duty to render assistance to those in need in case of accident, common danger or emergency.
[224] Lackner & Kühl *Strafgesetzbuch Kommentar* section 13, 15.

the user to access such contents. Here, it becomes difficult to ascertain where the criminal liability lies.

The German judiciary prefers the normative theory. This theory states that the distinction between an act and an omission is determined by the *Schwerpunkt der Vorwerfbarkeit* (main emphasis of guilt) of the behaviour.[225] This means, one must focus on the criminally relevant behaviour. For example, on a freezing winter night someone injures a person, who subsequently dies. The focus is on an active doing since the injury caused the death. The focus would have been on an omission if the person had died as a result of the cold weather and not because of the injury. In this case, the person would have died because the offender did not offer help. A classic example for an omission is the medical doctor who turns off a respirator. The basis of liability in terms of normative theory is the future medical benefit, which the patient could have received had the respirator not been turned off, as opposed to the active "switching off" of the machine.

The author Altenhain offers another opinion.[226] In his opinion, normative theory is useless in the area of Internet law. For the application of "normative theory" there has to be a starting point, which points to an act or an omission. Only from such a starting point is it possible to define the quality of an action. No such starting points can be defined regarding the mere action of providing Internet access. He concludes that only a positive act is possible in the access cases.

In summary, it can be concluded that the service provider cannot be held

---

[225] Haft *Strafrecht Allgemeiner Teil* (1984) 173; BGH *NJW* 1953, 1924; Schönke & Schröder *Strafgesetzbuch Kommentar* introductory remark section 13 StGB 158.

[226] Altenhain "Die strafrechtliche Verantwortlichkeit für die Verbreitung mißbilligter Inhalte in Computernetzen" 1997 *CR* 487.

responsible as an active perpetrator, if he only indirectly permits access to illegal contents on the Internet. The German judiciary and the legal doctrine assume that the service provider, who does not manage the Internet service himself, could in principle only be liable for omission because he cannot be blamed for the lawful provision of a communication link or storage capacity. The creation of the opportunity to misuse the Internet cannot result in grounds for active perpetration, as this would open the floodgates of liability for providers. After the establishment of the Internet services, no further legally relevant actions are carried out by the service provider in fully automated computer systems.[227] This must be distinguished from the situation where the service provider wilfully makes such contents available, for example in self-managed news groups. In this case, an active commission can be identified.

Since the service provider can always be at best reproached with omission, this problematic issue - like the question of intent and grounds for justification - is analysed in more detail only in view of the dogmatic of offences by omission.

5 2 2 Perpetration through omission

Internet providers can be criminally liable because of perpetration through omission. However, in order to punish a provider for an omission, the following preconditions[228] have to be present:

Firstly, the omission of a reasonable and possible action must be

---

[227] Sieber "Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen" 1996 *JZ* 499.

[228] Tröndle & Fischer *Strafgesetzbuch Kommentar* (201) introductory remark to section 24 StGB 1 (b).

present, which is equivalent to and therefore, corresponds to an active doing.

Secondly, the effect of the criminal act must have been avoidable, had the provider acted. He has to act only if the action is reasonable and lawful. The dissemination of the illegal content must have been preventable with sufficient certainty through the reasonable action of the provider.

Thirdly, the provider must have a legal duty (*Garantenstellung*) to prevent the dissemination of the illegal material. Since 1969, the legislator has paraphrased this necessary condition for the equal status of commission and omission by saying that the person failing to act "must be held legally responsible for the fact that the success does not occur".

5 2 3 Position of being a guarantor

In order for a provider to be held criminally liable, he must be a so-called "guarantor". Previously, the concept of a guarantor originated from the law of contract, cohabitation or public statutes.[229] In terms of the present doctrine, one must differentiate between the duties to exercise proper care (*Obhutspflichten*) and the duties of supervision (*Überwachungspflichten*).[230] The guarantor's duties are: firstly, the duty to guard certain objects of legal protection and secondly, the duty to bear the responsibility for certain sources of threats.[231]

---

[229] RG 63, 394.
[230] Wessels *Strafrecht Allgemeiner Teil* (2001) 104.
[231] Schönke & Schröder *Strafgesetzbuch Kommentar* section 13, 9.

5 2 3 1 Guarantor's obligation arising from preceding action

The guarantor's obligation arising from preceding action (*Ingerenz*) is based upon the prohibition to injure or damage any other person.[232] The committer, or more appropriately, the non-acting perpetrator, has the responsibility and power over the concrete source, from which the danger emanates. It is difficult to establish a control mechanism on the Internet and it demands considerable effort. The different options, such as filter software, will be discussed later in this thesis.[233]

A real risk for the spreading of illegal contents can arise through the running of computers. The problem is that the running itself is not unlawful in principle, just as it is not illegal to use the Internet. With the establishing of computer networks for the Internet, the service provider does not lay claim to special privileges from which a special liability can arise if he does not prevent the access to illegal contents.[234] A party who "through lawful behaviour causes the danger of a foreign criminal offence and who does not prevent this criminal offence or does not avert the consequences of this offence"[235] is not a guarantor. This is the case if the provider lawfully opens up an Internet-connection.

5 2 3 2 A guarantor's position resulting from general safety obligations

Guarantor's obligations to protect third-party legal interest from any

---

[232] ibid 34.
[233] See chapter 8.
[234] Derksen "Strafrechtliche Verantwortung für die in internationalen Computernetzen verbreiteten Daten mit strafbarem Inhalt" 1997 *NJW* 1883.
[235] OLG Köln *NJW* 1973, 861; BGHSt 3, 203.

danger emanating from one's own sphere of control exist moreover for the supervision of sources of risk the control of which is incumbent on the "non-acting offender". This obligation is independent from certain behaviour, which could cause a threat.[236] The classic example of a guarantor's position[237] emanating from a safety obligation is the operator of a nuclear power station. He carries a safety obligation at all times, because he runs a dangerous business and he has influence on its safety devices. The basis for such safety obligations is the real control of a source of threat and an organisation-authority from which other persons are excluded.[238] Service providers have the exclusive power of disposal over their servers and data networks. But this alone is not sufficient to constitute a guarantor's position. This would otherwise create a limitless liability, because the service providers have, in theory, the possibility to control the contents on their nets. In practice, the operational procedure of the provider would collapse on account of the huge amount of data.

If he knows about illegal contents, then, a guarantor's position resulting from a safety obligation obliges the service provider to prevent illegal contents from becoming accessible, once he has become aware of them.

5 2 3 3 Conclusion

A guarantor's position with regard to preventing the transmission of illegal data is only a consideration if the provider has knowledge of the illegal

---

[236] Dreher & Fischer *Strafgesetzbuch und Nebengesetze Kommentar* Section 13, 12.
[237] Jäger & Collardin "Die Inhalteverantwortlichkeit von Online-Diensten" 1996 *CR 238.*
[238] Wessels *Strafrecht Allgemeiner Teil* 107.

contents. If he has knowledge of them, he is obliged to prevent the transmission thereof. This duty arises from *Ingerenz* from the moment of becoming aware of the data and on account of a safety obligation. For providers, a general position of being a guarantor and a general duty to check the entire Internet content cannot be assumed.

5 2 4 Causation and criminal responsibility

In addition to a guarantor's obligation, the criminal liability for omissions subject to a further prerequisite: the offender must fail to take an action which is possible and reasonable for him and which would almost certainly prevent that the elements constituting a criminal offence are fulfilled. The provider must have the possibility to act. This means that the criminal liability for omission first of all depends on the precondition that the non-acting person is physically and actually in a position to take the expected action. The law cannot mandate impossible actions.

The online provider only causes an offence by omission if he refrains from removing illegal contents (of which he is aware) from his server and refrains from preventing such data in an area under his control. This requires that an effective action would in all probability have prevented the offence. Otherwise, the provider cannot be made liable for his omission.

5 2 5 Criminal intent

For criminal liability to exist on the part of the service provider, he must

act with criminal intent. An exception would be where liability is based on negligence. Criminal intent can be assumed, if the provider takes no action, although he has recognised that he has the capacity to prevent illegal contents of which he is aware on his server.

German criminal law distinguishes between different types of intent.[239] Intent can be constituted by *Absicht*, an intensified form of direct intention, which may be adequately present if there is motivation, whereby the offender desires a specific result (*direkter Vorsatz*), or where the offender knows or expects the result of the action and desires this result. Another form of intent is the *Eventualvorsatz*, where the offender seriously expects the result.[240] Intent is present for an offence by commission, if the service provider himself puts illegal contents on the Internet. Intent is present for an offence by omission, if a provider, once he identifies illegal contents or acquires knowledge of their presence, does not act to block such data and therefore does not prevent access to such data.

5 2 6 Unlawfulness

Where the provider has intentionally committed an offence, it must also be unlawful, in order to be punishable. An act is unlawful if it violates the law and cannot be excused by justifications like self defence (section 32 StGB).[241]

In the area of Internet law, a criminal offence can be justified on the basis of "permitted risk", "social adequacy" or "preservation of legitimate

---

[239] Wessels *Strafrecht Allgemeiner Teil* (2001) 211-213.
[240] Foster *German legal system & laws* (1996) 205.
[241] Tröndle & Fischer *Strafgesetzbuch Kommentar* (2001) introductory remark to section 13, 24.

interests". The preservation of legitimate interests (section 193 StGB) is however only applicable to offences of insult.[242] Apart from that, almost every legally established ground of justification for unlawful conduct is applicable to offences that can be committed on and through the Internet. If one has no justification for his action or his commission by omission and he acts also with culpability[243] he will be held liable. The principle *nulla poena sine lege* applies in the German criminal law system and as such, in the area of provider liability. Guilt, according to Section 46 (1) of the StGB, is the basis for punishment and is determined by the ability of the offender to discern between lawful and unlawful conduct.

5 2 7 Conclusion

Access and service providers can be held liable because of their omission to take preventative measures against illegal contents. The judiciary seems to be of the opinion that the liability is based on the omission, not the active act of "opening of a communication connection" or the arrangement of the account for an Internet user. Except in the case where a server is installed specifically to permit the dissemination of illegal content by third parties, or to host such illegal content, the simple setting up or operation of a server is not in itself punishable, even if the server is used to store or transmit illegal content, without the knowledge of the server's operator. Therefore, the basis for liability lies in the omission of an act, where the provider – subsequent to gaining actual knowledge - fails to take adequate steps to remove the illegal

[242] Kröger & Gimmy *Handbuch zum Internetrecht* (2001) 597.
[243] Section 46 (1) StGB.

content or fails to block access to such content.

A service provider may be liable under German criminal law, if he is the author of illegal content or if he makes it accessible to the public at large. The mere possession of child pornography can lead to liability also.[244]

Criminal liability of a provider as access provider has to be ruled out, even if the technical equipment was misused by the user to spread or to make illegal data accessible. Only if he knowingly transmits and makes such material accessible does criminal liability becomes applicable. The same applies to Usenet-administrators, if they knowingly make illegal contents accessible to their users. They have a duty to erase illegal contents on their servers and a duty to block the access to the newsgroups concerned, if they have knowledge of such content. The criminality derives primarily from the function of the data transmitter.

5 3 Provider liability and their modification through the TDG

One of the most important questions relating to the Internet on a national and international basis is liability. Two typical characteristics of the Internet make it difficult for jurists to deal with the topic of liability: its multi-functionality and its global nature.

The risks of liability for providers have motivated the German legislature to enact legislation to protect the future development of the Internet. As shown above, provider liability can be determined by traditional criminal law. Why then has Germany introduced specific Internet laws? This question will now

[244] See BayObLG, chapter 4 4 7..

be addressed.

The Teleservices Act (*Teledienstegesetz* (TDG)) was the first provider liability law to be enacted anywhere in the world. The Teleservices Act is applicable to the individual interactive user. The *Mediendienstestaatsvertrag* (MDStV) is the liability law for services, which address the public. Both acts regulate the liability of Internet providers. What distinguishes the *Mediendienstesttaatsvertrag* from the *Teledienstegesetz* are the terms "individual communication" and "mass communication". Examples for services, which fall under the law of the MDStV, are video-on-demand and electronic press, where journalistic articles are presented to the public. The *New York Times* or the *Herald Tribune* online for example, would fall under the liability law of the MDStV. An example of the TDG is individual communication such as email, newsgroups and the World Wide Web, but also online banking or online learning. It is difficult to distinguish between the two in particular cases, but to apply the correct law to the correct Internet service is unproblematic in practice, because the statutory provisions are almost identical. For the sake of convenience and because it is more relevant in practice, only the TDG will be discussed. Its basis - like that of the MDStV - was the introduction of the Information and Communication Services Act (*Informations- und Kommunikationsdienstegesetz* (IuKDG)) in 1997.

The *Teledienstgesetz* provides for the first time a framework within which to assess the liability of a provider. The TDG/MDStV regulate the liability of providers for own and foreign contents.[245] From this law specific

[245] Koch "Zivilrechtliche Anbieterhaftung für Inhalte in Kommunikationsnetzen" 1997 *CR 193.*

characteristics have developed.[246] This law does not contradict the discussion of the liability of providers presented elsewhere in the thesis. This "Internet law" generally lays down the rules outlined in the preceding chapter. Special regulations apply independently and in addition to the general liability regulations of the different fields of law. In the area of criminal liability of providers this means, that the TDG modifies the liability that arises from the "traditional" criminal law as stated in the Criminal Code of the StGB. A provider can only be liable if the liability preconditions according to the general rules, as well as the rules of the TDG, have been satisfied.[247] The TDG is not *lex specialis* to the liability rules in German criminal law.[248] Only in certain circumstances does the TDG differ from the liability established in traditional criminal law. This means that the TDG offers certain privileges for providers. In other words, the TDG reduces the liability risks for providers.

In January 2002, only a few years after its enactment, the TDG had to be adjusted to the E-Commerce-directive[249]. All member states of the European Union are expected to incorporate the European directives into their national law. Because of this, the German legislature modified the TDG. It is now known as the E-TDG (European-TDG). Since 17 January 2002, all member states have the same law regarding provider liability, which amends their traditional criminal law. Germany's TDG was similar to the regulations in the European E–Commerce-directive, which meant that few changes had to be made to the TDG.

The following part of the thesis will illustrate how the TDG has modified

---

[246] Bortloff "Die Verantwortlichkeit von Online-Diensten" 1997 *GRUR* 387.
[247] BT-Drs. 13/7B85, April 9, 1997.
[248] Sieber "Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen" 1997 *CR* 583.
[249] www.ispo.cec.be/ecommerce/legal.htm; ABl (gazette) EG 199 no. C 30/4.

the liability of providers and what changes have occurred through the enactment of the new E-TDG, based on the E-Commerce Directive. The "old" TDG, the various subsections of section 5 of which documented the possibilities of creating or avoiding liability, illustrates how the Internet law works.

5 3 1 Section 5 TDG

On 22 November 1995, the Munich public prosecutor authorised police to search the premises of CompuServe Germany. They suspected that child pornography was being disseminated through newsgroups using the Internet provider CompuServe. CompuServe Inc, USA immediately blocked these newsgroups worldwide, since the online service was at risk of incurring potential criminal and civil liability in Germany. In May 1998 the county court of Munich sentenced the former managing director of CompuServe Germany Felix Somm to two years probation and a fine of DM 100,000 for the public distribution of pornographic writings.[250]

The excited headline reactions to the *CompuServe* case ranged from "Germany's Internet Angst"[251] to "Efforts to control the Net abuse liberty"[252]. In 1999, an appeal led to Somm's acquittal. The Landgericht (District Court) Munich, as the appeals court, acquitted Somm on the basis of section 5 (3) TDG (*Teledienstegesetz*).[253] Section 5 (3) of the TDG states that providers who only offer a connection to foreign contents are exempt from possible

[250] See introduction; AG München *MMR* 1998, 429, 438.
[251] www.wired.com/news/news/E-mail/other/politics/story/12884.html.
[252] www.sjmercury.com/columnists/gilmore/docs/dg052998.htm.
[253] LG München 1, 2000 *CR* 117-119.

criminal liability.

The discussion of criminal liability of providers was raised by the preliminary investigations such as the famous *CompuServe* case.[254] The German legislature has since regulated the liability of online services in terms of the IuKDG (*Informations- und Kommunikationsdienstegesetz*). Section 5 TDG takes into account the technical characteristics of the international data networks. The liability privilege should reduce the economic loss and loss of reputation that resulted from the *CompuServe* case and other radical prosecutions.[255]

5 3 1 1 Section 5 (1) TDG

Section 5 (1) of the TDG provides that the content provider is liable for its own contents as with every Internet-participant. He is liable under the general statutes (*allgemeinen Gesetze*), for example sections 185 ff of the StGB.[256] There are no grounds for privileges. Therefore, the producer of an Internet newspaper is as liable as a participant of a chat forum or an owner of a homepage.

---

[254] Derksen "Strafrechtliche Verantwortung für die in internationalen Computernetzen verbreiteten Daten mit strafbarem Inhalt" 1997 *NJW* 1878-1882; Sieber "Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen" 1996 *JZ* 429-430.

[255] Sieber "Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen" 1997 *CR* 581-582.

[256] Härting *Internetrecht* (1999) 168.

5 3 1 2 Section 5 (2) of the TDG: the service provider

Since August 1,1997, the liability of the host (or service) provider was explicitly provided for in Section 5 (2) of the TDG. Examples of service providers can be found in the music business, where the providers offer the music of bands under contract on the Internet.

The service provider offers access to foreign contents. Under section 5 (2) of the TDG, the provider is only liable if he is aware of illegal content and if it is technically possible and acceptable for him to block these contents. It is important to remember that the liability of a service provider depends on actual knowledge of the illegal content; it is not sufficient that the provider should have known about it.[257] Constructive knowledge is not enough to create liability of a service provider. In the opinion of the AG Munich in the *CompuServe* case, it was sufficient that CompuServe knew that child and animal pornography was accessible in some Internet forums, using CompuServe as a service provider.[258] With the acquittal of Felix Somm by the District Court Munich, it has become clear what "knowledge" according to section 5 (2) TDG means: knowledge in the sense of *dolus directus* (*unmittelbarer Vorsatz*). In other words, the provider knows about illegal contents to be on his server and permits their continued presence there. Furthermore, the blocking of the contents has to be technically possible and reasonable. The limitation of the liability through the term "reasonable" is necessary in order to prevent a situation where the provider would be forced

[257] Strömer *Online-Recht* (1997) 73.
[258] AG München 1998 *MMR* 429-433.

to incur an enormous expense to avoid the illegal contents.[259] The provider does not have to block an entire service area or suspend the service in its entirety because of minor illegal content. The provider merely has to block unlawful content as soon as he has positive knowledge of it, for example, because of a complaint from a third party. Apart from this, the German legislature did not dictate self-enforcing control obligations on the service provider. There is no obligation for the service provider to monitor. The provider must take steps if contents on his server clearly and identifiably contravene the prevailing law, for example, if a customer offers child pornography for downloading.[260]

5 3 1 3 Section 5 (3) TDG: the access provider

Providers who only offer a connection to foreign contents are exempt from punishment in terms of section 5 (3) TDG.[261] The reasons behind this provision are the above-mentioned technical facts; that the common access provider generally has no way of controlling the data traffic on its nets.

An automatic and short-term storage of foreign contents by the user (so-called Proxy-Cache-Storage)[262] was also privileged as a result of section 5 (3) s.2 TDG. The access provider is even exempt from punishment if he knows

---

[259] To the motives of section 5 (2) TDG (see: BT-Drs. 13/7385, 20).
[260] Strömer *Online-Recht* (2002) 73.
[261] Section 5 TDG Responsibility
(3) Providers shall not be responsible for any third-party content to which they only provide access. The automatic and temporary storage of third-party content due to user request shall be considered as providing access.
[262] Part of the memory of a computer. Used to store interim or current information for fast retrival (see: Rockey *The e-Commerce Handbook* (2000) 254).

about illegal Internet content to which he provides connection.[263] Of course, he is not allowed to explicitly advertise such illegal content, for example with Link-lists.[264]

5 3 1 4 Section 5 (4) TDG

Section 5 (4) TDG provides that any duties to block the use of illegal content under general laws remain unaffected, insofar as the service provider gains knowledge of such content.

Sections 5 (1) – (3) TDG presupposes *Verschulden* (fault) as a precondition for the liability of a provider. Section 5 (4) of the TDG deals with liability of omission, which is *verschuldensunabhängig* (independent from fault). The provider has to block the illegal site when he becomes aware of it and if the blocking is possible and acceptable. This is an exception, because the access provider is generally not responsible for foreign illegal content. He must thus work actively to eliminate the illegal sites.

5 4 (Hyper) Links

The information on the Internet is chaotic. The easiest way to find a way through the information-jungle is to set up a Hyperlink (shortened form: Link) between related sites.

---

[263] Spindler "Haftungsrechtliche Grundprobleme der neuen Medien" 1997 *NJW* 3193, 3198.
[264] ibid.

5 4 1 What is a (Hyper) Link?

A link is a reference that can be established from one point on a website to any other site on the World Wide Web.[265] Links make it unnecessary for users to use a search engine to find a website as they allow a user to easily proceed from one web page to another on the World Wide Web.[266]

5 4 2 Liability

The liability for hyperlinks has not been conclusively established in German law. The same applies to frames.[267] The German legislature has established a privilege by enacting section 5 of the TDG.[268]

The case of the extreme left-wing magazine *radikal* and Angela Marquardt raised the question of criminal liability for links.[269] Content providers and homepage-creators felt insecure.[270] An initiative on the web called Freedom for Links arose.[271] The case attracted worldwide attention.[272] The grounds for the prosecution of the magazine was the assistance it had provided in distributing instructions on how to commit a crime (section 27, 130 (a) StGB) through the setting up of a link.[273] By setting up a link to *radikal*, Angela Marquardt had committed a criminal offence according to the county

---

[265] Rockey *The e-Commerce Handbook 2000* (2000) 255.
[266] www.mbendi.co.za/werkmns/net_law/guide03.htm.
[267] A way of transmitting information in small data packets. Framing occurs when one displays material from another web site within the frame in one's web page (see: Hofman *Cberlaw* (1999) 92).
[268] Härting *Internetrecht* (1999) 169.
[269] Amtsgericht Tiergarten 260 Ds 857/96; 1998 *MMR* 49-50.
[270] www.jra.uni-sb.de/jurpc/aufsatz/19980046.htm.
[271] www.afs-rechtsanwaelte.de/linkhaftung.htm.
[272] *New York Times* June 6, 1997, page 1 "Germany's effort to police the web upset business".
[273] Amtsgericht Tiergarten 260 Ds 857/96; 1998 *MMR* 49-50.

court of Berlin Tiergarten. The County Court dismissed the case in June 1997, ruling that Ms Marquardt had unknowingly supported terrorism. The court said that she had neither installed the link nor maintained it with the knowledge of its illegal contents. In the opinion of the court, the installation of a link without knowledge about the content of the linked text is not illegal.

It is questionable whether setting up a link falls under section 5 (3) TDG. The consequence would be the exemption from liability. The opinions about liability for links are divided. Besides the *radikal* case, the *Terrorist's Handbook* case of the BayObLG (provincial high court of Bavaria) dealt with the important question of link-liability.[274] The accused had a handbook for the production of Molotov-Cocktails (also called petrol-bombs) in his mailbox. He had found the terrorist handbook on the Internet. Another person wrote it. His mailbox was accessible to 800 members of a computer club. The case was dismissed. The opinion of the court was that the simple dissemination of the text with illegal statements, which was not written by the accused, is not punishable. He did not make use of the contents and he did not instruct himself in the production of petrol-bombs.[275] The precondition for a penalty under the relevant section 53 (1) no. 1 of the *Waffengesetz* (Weapons Act) was not fulfilled in this case because the preconditions are the asking for or instruction in the production of flammable substances.

In 1998, the District Court (*Landgericht)* of Hamburg sentenced a website owner to pay compensation for damages, because he had a link to a foreign web page with insulting contents ("The blockhead of the month").[276] The person pointed out that he was not responsible for the foreign content,

[274] BayObLG – 4 St RR 232/97; Bay ObLG 1998 *CR* 564; 1998 *MMR* 262.
[275] BayObLG – 4 St RR 232/97.
[276] Landgericht Hamburg 1998 *CR 565.*

but this argument did not satisfy the court.[277] By the legal decision, the District Court decided that one might be responsible for the contents of the linked page as a result of the creation or making available of links. According to the District Court this can only be prevented if the authors distance themselves clearly from these contents and declare that they do not have influence on the linked contents. The web site owner who had linked to the foreign web page was sentenced to pay compensation for the damage caused.[278] A comment that not he as the linking person but the author of the text shall be liable does not suffice. One has to distance oneself clearly. But the court did not provide an answer to the question of how exactly one can distance oneself clearly from the content to which one sets up links.

The two cases about links with two entirely different outcomes increased the insecurity of the net-community. In the case of the *Terrorist's Handbook*, the court could not find evidence that the perpetrator intended to provide guidance for the production of Molotov-Cocktails and the simple transmission of a data program is not punishable according to the District Court Hamburg. In the court's judgment the crime of instructional guidance for the production of weapons" is an offence that can only be committed by means of a statement (*Äusserungsdelikt*), not by simple dissemination (*Verbreitungsdelik*t). The action in the case of crimes like criminal instructions for the production of weapons or insult and defamation lies in the criminal remark. On the other hand, the illegality of dissemination crimes lies in making

[277] Landgericht Hamburg 312 O 85/98.
[278] In Germany it is possible to sentence a person to pay compensation for damage, as if for a civil injustice if there is also a relevant connection to criminal law. In this case, the insult (section 186 StGB (malicious gossip)) violated the civil-law-relevant offence of an attack on one's honour as a loss of one's civil rights.

illegal contents accessible.[279]

It is important to determine whether the "link" person himself expresses a disclaimer in setting up a link or approves of the insult on the web page. In the Blockhead of the month case ("D-Depp des Monats"), the court ruled that the website owner had not really disassociated himself from the insulting foreign content.

Dissemination of pornography is a different situation. In this case it is sufficient grounds for prosecution if the dissemination of pornographic writings is supported through a link, independent of the will to disseminate. The criteria for criminal liability are satisfied if the linking person knows about the forbidden content on the Internet, but nevertheless sets up a link to this page.[280] Simply providing access to the Internet and to newsgroup servers with illegal content is not punishable in terms of section 5 (3) TDG. This is why the decision of the County Court Munich of May 28, 1998 against the former manager of CompuServe Germany was considered to be incorrect and why the District Court Munich 1 later acquitted him.[281]

5 5 Conclusion

Section 5 TDG is the prototype Internet law. It regulates the liability of Internet providers. The liability of providers depends on the function of the provider. This law takes into account the role of providers and aims primarily at the author of illegal content.

---

[279] Tröndle & Fischer *Strafgesetzbuch Kommentar* (2001) section 74 (d), 5.
[280] See chapter 5 3.
[281] See chapter 3 1 3 3 (*CompuServe*–case).

6 European initiatives and the E-Commerce Directive

The EU-directive for electronic transactions (E-Commerce Directive) was approved by the European Parliament on 4 May 2000 and came into force on July 17, 2000 with its promulgation in the official gazette.[282]

Articles 12-15 of the directive contain specific regulations for the liability of Internet providers.[283] With the enactment of the directive, the different regulations for the liability of providers in the various European countries were harmonised at a European level.[284] The goal of this directive is to protect the freedom of providing services. The directive is primarily designed to create exemptions from liability. These are valid for the intermediaries on both the criminal and the civil level. It is important to note, that the directive recognises that intermediaries have no positive obligation to seek out and monitor illegal information, while simultaneously acknowledging that service providers have a duty to act under certain circumstances, in order to prevent illegal activity.

6 1 Scope of application

Providers[285] are defined in Article 2 (Providing an information society service)[286].[287] An "established service provider" is defined in Article 2 (c) as "a

---

[282] www.ispo.cec.be/ecommerce/legal.htm.
[283] ABl (gazette) EG 199 nr. C 30/4.
[284] Landfermann "Der Richtlinienvorschlag Elektronischer Geschäftsverkehr – Ziele und Probleme" 1999 *ZUM* 795 (800); Geis "Die Europäische Perspektive der Haftung von Informationsanbietern und Zertifizierungsstellen" 1999 *CR* 772-774.
[285] Article 2 (b) "service provider": a natural or legal person providing an information society.
[286] Article 2 (a)"information society service": services within the meaning of Article 1 (2) of Directive 98/34/EC amended by Directive 98/48/EC, as (1) normally for remuneration, (2) at a distance means that the service is provided without the parties being simultaneously present,

service provider who effectively pursues an economic activity using a fixed establishment for an indefinite period. The presence and use of the technical means and technologies required to provide the service do not, in themselves, constitute an establishment of the provider". Even providers, who offer the service of hosting homepages free of charge to private persons and finance themselves by means of advertising, are service providers as anticipated in the directive. For the member states there is no obligation to extend the liability-privileges for providers of private homepages or universities.

The directive only regulates the liability of service providers with regard to contents of a third party, but not to their own content.

Art. 12-14 of the E-Commerce Directive deals with information, which is published on the Internet by a "recipient of the service" (user).[288] "Recipient of the service" of an information society service is also a person, who uses this service to offer information to others as defined in Art. 2 lit. (d). The directive does not regulate every kind of service presently known, but only the simple transmission (Art. 12), the caching (Art. 13) and the hosting (Art. 14) of data. It omits any protection of furnishing information location tools such as directories and hypertext links, helpful communication tools which make the Internet easier to use and are distinct from the provision of content.[289]

---

(3) by electronic means: (...) the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means, no CD-ROMs, telephone or fax ; and (4) at the individual request of the recipient of the services means that the service is provided through the transmission of data on individual request, not television, radio, teletext.

[287] Directive 98/34/EC of the European Parliament and of the Council laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services.

[288] "Recipient of the service" Article 2 (d): any natural or legal person who, for professional ends or otherwise, uses an information society service, in particular for the purpose of seeking information or making it accessible.

[289] See chapter 6 1 1.

The case of the mere conduit, covering both the transmission and the provision of access, is dealt with in Article 12.[290] It establishes an exemption from liability as regards the provision of information society services, which consists in the transmission of information in communication networks whereby the service provider plays a passive role as a conduit of information for third parties (the recipients of the service). This liability exemption covers cases in which a service provider could be held directly liable for an infringement and cases in which a service provider could be considered secondarily liable for someone else's infringement, for example as an accomplice. As for the types of activities covered by this Article, the provider cannot be subject to prosecution in a criminal case.

When the service provider is transmitting its own information, it can no longer be considered to be performing a mere-conduit activity as an intermediary. The same holds if the provider itself modifies the information during the course of the transmission. An exemption from liability will be granted if and when the intermediary does not play any active role in the transmission of the information, neither with regard to the origin (he must not have made the decision to perform the transmission), nor with regard to the destination (as he does not select those to whom the transmission is addressed), nor with regard to its content (he acts merely as a vehicle, which does not make any selection). Transient and intermediate storage taking

---

[290] Article 12 – Mere conduit :
1) Where an information society service that consists of the transmission in a communication network of information provided by the recipient of the service, or the provision of access to a communication network, Member States shall provide in their legislation that the provider of such a service shall not be liable, otherwise that under a prohibitry injunction, for the information transmitted on condition that the provider
a) does not initiate the transmission,
b) does not select the receiver of the transmission and
c) does not select or modify the information contained in the transmission.

place during the transmission of the information in order to carry it out is covered by the mere-conduit exemption. Only those acts of storage which take place during the course of transmitting the information and do not serve any other purpose than carrying out the communication will benefit from exemption. These acts of storage do not include copies made by the provider for the purpose of making the information available to users. This case is addressed on caching, Article 13. The term "automatic" refers to the fact that the act of storage occurs in the ordinary operation of the technology. The term "intermediate" concerns to the fact that the storage of information is made in the course of the transmission. The term "transient" refers to the fact that the storage is for a limited period of time.

Art. 13 deals with caching activity,[291] which is an indemnity against liability, and is comparable with section 5 (3) s.2 TDG.[292] The community directive identifies some conditions for exemption in the event of automatic, intermediate and temporary storage of information, if this is done for the sole purpose of improving the efficiency of the information's further transmission to other recipients of the service upon their request. The provider is mainly obliged to abstain from such actions in which any obligation is combined with a further obligation to respect the rules and standards relating to access of the

---

[291] Article 13 – Conditions
a) The provider does not modify the information
b) The provider complies with conditions on access to the information
c) The provider complies with rules regarding the updating of the information, specified in a manner consistent with industry standards
d) The provider does not interfere with technology, consistent with industry standards, used to obtain data on the use of the information
e) The provider acts expeditiously to remove or to bar access to the information upon obtaining actual knowledge of one of the following
- the information at the initial source of the transmission has been removed from the network
- access to it has been barred
- a competent authority has ordered such removal or barring.

[292] 5 (3) s. 2 TDG: The automatic and temporary storage of third-party content due to user request shall be considered as providing access.

information and its updating.[293] Liability can normally be avoided by checking up regularly that user's server in order to up-date the information of the service provider 's server. The Internet service provider must remove, therefore, the outdated information as soon as he obtains acknowledge that the information has been removed from website or access has been disabled.

Article 14 holds the most important rule.[294] Art. 14 deals exclusively with the liability relating to information stored on request of the user. This regulation is similar to the section 5 (2) hosting-regulation of the TDG.[295] Comparing the seemingly similar wording "actual knowledge of illegal activity or information" in the directive and "knowledge of such content" in section 5 (2) TDG, the Internet provider is only liable if he has actual knowledge of the illegality. There is no criminal liability if the provider, upon obtaining knowledge of illegal activity, acts expeditiously to remove or disable the access to the information. This principle provides a basis for notice-and-take-down procedures, and parties may identify and follow for notifying the service provider about information, which is the subject of illegal activity in order to obtain its removal or disablement.

The "actual knowledge" standard under Article 14 can be a problematic basis for criminal liability arising from the activities of third party Internet users. For example, a low level employee of a service provider who receives a

---

[293] No influence on the content transmitted and no interference with the technical system.

[294] Article 14 - Hosting
1. An information society service consists of the storage of information provided by a recipient of the service, and the Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:
(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances of which the legal activity or information is apparent; or
(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information. 2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.

[295] See chapter 5 3 1 2.

complaint to superiors could trigger criminal liability for the corporation. In view of the fact that most service providers often receive contents from millions of content providers on their servers and also have large numbers of legally unsophisticated customer service support representatives available at any hour who may receive such complaints, criminal liability under these circumstances is not appropriate in case of absent other evidence of criminal intent.[296]

As the Commission developed substantive criminal standards for computer-related crime, it should have made clear for these offences that an intermediary service provider is not liable for content created or developed by users.

6 1 1 No regulation for the liability of (Hyper) Links in Europe

The liability of providers for links, providers of search engines and indexes was deliberately not regulated in the directive. In terms of Art. 21 (2), this liability is explicitly reserved for a later adjustment of the directive, as no general consensus was reached during the legislative process. Contrary to Section 5 of the TDG[297], which was drafted in comprehensive language, the liability rules in the directive are formulated in a technically specific manner. This makes it impossible to include a link-liability through the extensive interpretation or by drawing an analogy, which German jurists thought possible, although link-liability has not legally been settled as such.[298]

The European member states are consequently free to create their own

[296] Freytag "Providerhaftung im Binnenmarkt" 2000 *CR* 608.
[297] See chapter 5 3.
[298] Härting *Internet-Recht* (1999) 169-170.

liability norms to regulate the liability for hyperlinks and search engines. This may lead to enormous complications in the common market.

6 1 2 Conclusion

The Directive limits the liability of Internet service providers when they act as online intermediaries, by setting forth exceptions fore mere conduit, caching and hosting. The limitations apply to both civil and criminal liability. In order to benefit from one or more of the exceptions, certain conditions must be fulfilled. For example, in order to benefit from the liability exemption for hosting, the service provider must have no actual knowledge of illegal activity or information.[299] When the service provider obtains such knowledge, he must act expeditiously to remove or to disable access to the information in order to avoid liability.

The Directive aims at specific activities or functions rather than particular categories of operators. As a result, Internet service providers that provide a wide variety of service, only some of which fall within the definition provided in Articles 12-14, would still benefit from the Directive's provisions on liability, but only with regard to those services that can be characterized as online intermediary activity. The Directive does not address the liability of providers for hyperlinks or search engines. These activities will still be subject to the diverging regulatory approaches of the Member States.

The terms liable and liability in the directive are, similarly to the German law, to be interpreted in the sense of to be responsible for an infringement of

[299] As regards claims for damages: awareness of facts or circumstances from which the illegal activity or information is apparent, Article 14 (1) (b).

rights. In German law, the regulation of criminal liability has been a main area of focus for the German legislature through the creation of laws to regulate the Internet.

Although criminal law is not within EU-competence, criminal liability falls under the directive. The member states have the freedom to create their own criminal law. Criminal law aspects can however become part of EU laws, without having to challenge the autonomy of the member states in this matter, if their regulations are necessary for the function and realisation of the common market.

The directive is not applicable to providers in non-EU-countries. It was intended to be enacted into the national law of the member nations before 17 January 2002. Where this did not occur, the liability-regulations of the directive became directly applicable as a result of the so-called self-executing-nature of European directives. The directive represents the foundation of a European-wide means of regulating electronic commerce and offers a legal framework for this. Problems with non-EU-countries still exist, although the European unification process and the directive formed a basis for a step-by-step evolution of closer co-operation between the respective national legal systems and hence, pragmatic improvements in the regulation of this liability. This demonstrates that no sovereign country will lose its own legal traditions in the process.

6 2 The E-TDG: the new Internet law

As already mentioned, the European Internet liability directive did not change much in the TDG. The regulations in the "new" Internet law are however more accurately formulated.

6 2 1 Content provider

As in the "old" TDG (section 5 (1) TDG), providers are criminally liable in terms of section 8 E-TDG (section 8 deals with the general principles) for any content that they generate, just like every Internet participant who places illegal contents on the net. Providers have no duty to supervise the data they transmit and store. They also do not have to search for circumstances that point to or indicate an illegal activity. This is one of the most important provisions of the E-Commerce Directive. In other words: the law allows the provider to renounce control. If a provider controls and gains knowledge about illegal content or places illegal content on the net, then he is clearly criminally liable. This liability flows from the general principles of traditional criminal law.[300] It must be noted that this provision provides for a legal privilege for the host- and access provider.

6 2 2 Access Provider

In terms of section 9 of the E-TDG, providers are not criminally liable under certain circumstances for foreign content that they transmit or to which

[300] See chapter 5 1 ff..

they offer access. These circumstances include the situations where the provider has not initiated the transmission, the provider does not select the addressee of the information and the provider has not selected or altered the transmitted information.

The provider is privileged because he does not influence the information in any way. An automatic and brief caching of third party content due to a user query (in particular in so-called proxy-cache servers) therefore also enjoys this liability privilege by being classified as access provision from a functional viewpoint.

The above does not apply in terms of section 9 (1) of the E-TDG where the provider works together with one of his users with the intention of committing a crime. This provision corresponds to the former section 5 (3) TDG. Besides the provision of access, the sending of email and the routing thereof are also privileged. This does not apply where a provider stores an email for a longer period, for example in his archives. In this case, he becomes a host-provider in terms of section 11 E-TDG.

6 2 3 Cache

Section 10 of the E-TDG regulates the temporary storage of information. This kind of storage is necessary for the communication between the network users, particularly in the case of caching of information. Under section 10 of the E-TDG, providers are not liable for foreign information, which they store for a user if they have no knowledge of the unlawful activity or content. Alternatively, providers become active as soon as they obtain actual

knowledge of the information and erase it or prevent access to it. This rule is not applicable if the user is subordinated to the provider or is supervised by him.

6 2 4 Host or Service Provider

Section 11 does not list liability criteria but enumerates the preconditions for the limitation for service providers. The provider shall not be liable for the simple transmission and automatic short-term storage of foreign contents. A service provider stores foreign information on his computers and offers access to information to a third party. The extensive provision of section 11 E-TDG states that providers who store data only for the purpose of enabling the efficient transmission of foreign information are not liable if they do not alter the information or immediately take steps to erase illegal information or block the access to the information.[301] Only if the provider gains actual knowledge that he stores illegal contents is he required to erase or to block the access to them. Under this provision a service provider could never be liable if he has absolutely no knowledge about illegal contents on his server. If he knows about the content of certain data on his server, the provider can only be held liable if he knows that the content contravenes the law.[302]

6 2 5 (Hyper-) Links, peer-to-peer systems and search engines remain

[301] Eck & Ruess "Haftungsprivilegierung der Provider nach der E-Commerce-Richtlinie" 2003 *MMR* 363-366.
[302] ibid.

unregulated by law

In 1996 when the TDG was enacted the German legislature did not take note of the problem relating to links. This non-regulation was based on the ignorance at the time regarding the technical (and criminal) possibilities on the net.[303] Since then the legislature has recognised the problem and is in the process of creating a statutory provision for links. The European member states are allowed to regulate link-liability themselves.[304] A direct application of the liability privileges does not come into play, since the statutory provisions of the E-TDG do not apply to links.

The same applies for peer-to-peer systems (P2P). One can further distinguish between centralised and decentralised peer-to-peer systems. Centralised P2P systems like *Naptster* place all information on a central server. The registered users receive the file information at the server's disposal. There is in principle no difference to the query of a search engine.[305]

Centralised non-genuine P2P systems like Napster are bare search engines, however one can take this example to highlight a special characteristic of this form of search engine: Napster for example never examines contents of the averaged files. Liability for adopted content or intellectual liability could merely occur on the basis of the file name. As there is no real intellectual connection to the file name or to the provided content,

---

[303] www.bundesregierung.de/Gesetzgebung.
[304] See chapter 6 1 1.
[305] The only genuine P2P system is the decentralised P2P. Queries by users are answered by a third party computer, which is registered with the P2P and contains the actual information. Decentralised P2P systems can be technically qualified as a kind of closed network, although it is publicly accessible. The approved files of all computers, which receive the retrieval query, are also evaluated. Providers like Gnutella or Morpheus are therefore not information intermediaries; they only deal with a program, which allows locating information on computer networks.

the only possible form of liability would be a liability as a technical distributor. The users of decentralised genuine P2P systems are undoubtedly responsible for contents stored on their computers. However, there can be no liability of the provider for results of his information-averaging program as these search results are, as those of Napster and other search engines, an accumulation of IP addresses. Neither is liability possible for the users of this software, as the results of the search engines are not made available to other users.

Liability for links and search engines can only be determined by applying traditional criminal law. Similar rules will have to be applied to those techniques, which have been developed in the last few years. No liability exists for linked contents, if the link provider is unaware of the linked content. If he however installs the information himself, he can be held criminally liable.

The ongoing discussion surrounding liability for links in Germany and the European Union shows that the legislation could be desirable to clarify this legal question. An example of such legislation can be found in South Africa.[306]

6 2 6 Conclusion

In principle, the degree of liability fixed in section 5 TDG and its subparagraphs has been retained. The liability privileges set out in sections 8-11 E-TDG are applicable for commercial and non-commercial providers alike. Like the "old" TDG, the sections of the E-TDG have a filter-function and partly exempt providers from the liability relating to illegal activities and information of third parties. The German legislature also intended to privilege

[306] Section 76 ECTA (only for civil liability (see: chapter 7 1 3).

infringements of copyrights to make them also the object of the new TDG.

7 Internet law and its regulation in the world

The liability of Internet providers is a novel problem just like the Internet itself is a new medium. Conclusions can therefore only be drawn from legal systems in which these questions have been determined by special laws. It is important to compare the different laws and create international harmony between the laws to prevent the distortion of competition and "criminal law liability dumping" (judicial units countries, states, cities seeking to attract business at the expense of other, competing, units by offering a less rigorous legal code). Fortunately, in the European Community, Internet law has been standardized since January 2002.

Since this thesis focuses primarily on German criminal law, the comparative analysis is intended to only give a short overview of various jurisdictions and regulations in the American legal system. Considering the criticism of earlier legal practice it is important to examine the treatment of these new legal phenomena in other countries. A common ground must be found in order to regulate Internet liability internationally, which is desirable, and to create uniform control methods to combat crime online. A common ground is also needed for all legal systems with regard to cyber offences that will be prosecuted worldwide.

7 1 Liability of Service providers in South Africa

The Electronic Communications and Transactions Act (ECTA) came into force on August 30, 2002, as per Regulation 68 of 2002.[307] The Act is a very broad piece of legislation, reflecting the previous lack of legislative direction on many of the important and pressing e-commerce issues including the validity of electronically concluded agreements, the legal validity of electronic data, the admissibility of electronic documents in courts of law and the legal status given to electronic signatures. It also deals with issues which are either unique to an electronic environment or which are needed to provide legal certainty. The sections of the law, which are most interesting for the purposes of this thesis, will be pointed out in chapter XI (Limitation of liability of service providers)[308] and chapter XIII (Cybercrime) of the ECTA. As in German law, the ECTA does not affect criminal or civil liability in terms of traditional law - respectively in the case of South Africa, the common law.[309]

7 1 1 Chapter XIII of the ECTA

Chapter XIII of the Act contains the first statutory provisions on cybercrime in South African law. The chapter establishes several computer-related offences like unauthorised access[310] to data, interception[311] of or interference[312] with data, computer-related extortion, fraud and forgery (apparently aimed at preventing interference with commercial activities

---

[307] See the ECTA under www.acts.co.za/documents.
[308] In this chapter, "service provider" means "any person providing an information system service" (section 70 ECTA).
[309] About the background of common law liability see Prof. Coenraad Visser "South Africa: New Liability Regime for ISPs" 2003 *Computer Law Review International* issue 3, 94.
[310] Section 86 ECTA ,for example "hacking" and trading in passwords used to commit an offence (see: Guide to the ECTA www.michlsons.com).
[311] ibid, or example denial of service attacks or tapping into data flows.
[312] ibid, for example computer viruses.

conducted under the ambit of the Act).

The term "unauthorised access to data" (section 86 (1) ECTA), which seeks to outlaw, the "hacking" of databases is of particular interest. The person who is "hacking" has to act intentionally. The Act for the first time makes hacking itself a criminal offence, whether or not data is interfered with in the process.

The Act also states that the unlawful production, distribution and use of devices and applications designed primarily for the purpose of overcoming data protection security measures are punishable offences. Who performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene section 86 is punishable (section 86 (3) ECTA). While the wording of the Act suggests that such actions must be done with intent, this is not expressly stipulated.

The penalties are fixed in Section 89 ECTA. The Act punishes less serious offences[313] with a fine and/or imprisonment of up to 1 year and more serious offences[314], with a fine and/or imprisonment of up to 5 years. Attempting, aiding and abetting the commission of an offence under the Act is of course itself a punishable offence (Section 88 ECTA).

7 1 2 Service provider liability

Chapter XI deals with the limitation of the liability of persons providing information system services. As described earlier in the thesis concerning the liability of providers in Germany and the European Union, the liability for

[313] For example section 86 (1), (2), (3) ECTA (unauthorised access to, interception or interference with data).
[314] Section 87 ECTA (computer-related fraud extortion, fraud and forgery).

service providers basically depends on the role a provider plays in a particular transaction. The Act sets out to limit such liability, drawing extensively on the European E-Commerce Directive[315] and the American Digital Millennium Copyright Act[316].

In the ECTA the definitions of the terms, information system" and, information system services" are broad and could extend protection to telecommunication service providers, corporate entities and persons, involved in the activities of information system services. This does not encompass everyone who uses the Internet but those who perform the functions, which make the Internet available to users.[317]

Chapter XI deals with the limitations of the liability of service providers in general. Firstly, only those service providers can be subject to the privileges and limitations in question who are members of an industry representative body, approved by the South African Minister of Communications, by notice in the Government Gazette, and who are subject to and who implement that body's code of conduct. Secondly, only certain types of activities are protected in terms of Chapter XI.

7 1 3 Limitation of liability for Internet providers

Section 73 ECTA[318] establishes that no liability exists for the mere

---

[315] See chapter 6.
[316] USA Digital Millenium Copyright Act (DMCA) Pub. L. NO. 105-304, 112 Stat. 2860 (October 28, 1998).
[317] Prof. Visser "South Africa: New Liability Regime for ISPs" 2003 *Computer Law Review*, issue 3, 94.
[318] Section 73 Mere conduit
(1) A service provider is not liable for providing access to or for operating facilities for information systems or transmitting, routing or storage of data messages via an information system under its control, as long as the service provider—

transmission of data messages in information systems if the service provider plays a passive role as a conduit of information for third parties. A service provider, who provides information system services and who merely acts as a conduit in the transmission of data, will not be liable for any unlawful activity associated with its information system services, as long as it does not initiate the transmission, does not select the addressee and the data and does not modify the data contained in the transmission.[319] Section 73 ECTA affords protection to service providers in case such providers have little or no control of the content of the data transmitted.

Caching, section 74 ECTA[320], is the process by which information is temporarily stored by the service provider, in order to make the information more readily available if the end user should require that information at some

---

(a) does not initiate the transmission;
(b) does not select the addressee;
(c) performs the functions in an automatic, technical manner without selection of the data; and
(d) does not modify the data contained in the transmission.
(2) The acts of transmission, routing and of provision of access referred to in subsection (1) include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place—
(a) for the sole purpose of carrying out the transmission in the information system;
(b) in a manner that makes it ordinarily inaccessible to anyone other than anticipated recipients; and
(c) for a period no longer than is reasonably necessary for the transmission.
(3) Notwithstanding this section, a competent court may order a service provider to terminate or prevent unlawful activity in terms of any other law.

[319] Section 73 ECTA.

[320] Section 74 Caching
(1) A service provider that transmits data provided by a recipient of the service via an information system under its control is not liable for the automatic, intermediate and temporary storage of that data, where the purpose of storing such data is to make the onward transmission of the data more efficient to other recipients of the service upon their request, as long as the service provider—
(a) does not modify the data;
(b) complies with conditions on access to the data;
(c) complies with rules regarding the updating of the data, specified in a manner widely recognised and used by industry;
(d) does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain information on the use of the data; and
(e) removes or disables access to the data it has stored upon receiving a take-down notice referred to in section 77.
(2) Notwithstanding this section, a competent court may order a service provider to terminate or prevent unlawful activity in terms of any other law.

point in the near future. The limitation of liability given to service providers who cache data for recipients is subject to certain prerequisites, as for example the fact that the service provider removes or disables access to data in a reasonable time upon receipt of a take-down notification (section 77 ECTA)[321].

Section 75 ECTA[322] lays down under which conditions a service provider is not liable for the information stored at the request of a recipient of the service.[323] Section 75 ECTA refers to damages only and only defines if and when civil liability is excluded. In order to avoid liability in the case of hosting, the service provider is required to appoint an agent for the receipt of a take-

---

[321] Section 77 Take-down notification
(1) For the purposes of this Chapter, a notification of unlawful activity must be in writing, must be addressed by the complainant to the service provider or its designated agent and must include—
(a) the full names and address of the complainant;
(b) the written or electronic signature of the complainant;
(c) identification of the right that has allegedly been infringed;
(d) identification of the material or activity that is claimed to be the subject of unlawful activity;
(e) the remedial action required to be taken by the service provider in respect of the complaint;
(f) telephonic and electronic contact details, if any, of the complainant;
(g) a statement that the complainant is acting in good faith;
(h) a statement by the complainant that the information in the take-down notification is to his or her knowledge true and correct; and
(2) Any person who lodges a notification of unlawful activity with a service provider knowing that it materially misrepresents the facts is liable for damages for wrongful take-down.
(3) (...)

[322] Section 75 Hosting
1) A service provider that provides a service that consists of the storage of data provided by a recipient of the service, is not liable for damages arising from data stored at the request of the recipient of the service, as long as the service provider—
(a) does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of a third party; or
(b) is not aware of facts or circumstances from which the infringing activity(or the infringing nature of the data message is apparent; and
(c) upon receipt of a take-down notification referred to in section 77, acts expeditiously to remove or to disable access to the data.
(2) The limitations on liability established by this section do not apply to a service provider unless it has designated an agent to receive notifications of infringement and has provided through its services, including on its web sites in locations accessible to the public, the name, address, phone number and e-mail address of the agent.
(3) Notwithstanding this section, a competent court may order a service provider to terminate or prevent unlawful activity in terms of any other law.
(4) Subsection (1) does not apply when the recipient of the service is acting under the authority or the control of the service provider.

[323] Hosting.

down notification. A service provider is not liable for wrongful take-down in response to a notification, and he is exempted from liability for any damages caused by a wrongful take-down.[324] Any person who lodges a notification knowing that it materially misrepresents the facts is liable for damages for wrongful take-down.[325] The requirement that such misrepresentation must be "knowingly" excludes strict liability.

South Africa's representation of justice has taken the view against privileging criminal liability for hosting, but on the other hand - and in contrast to European[326] and German[327] guiding principles - it has decided in favour of privileging information location tools (section 76 ECTA)[328] if and when the service provider does not have actual knowledge that the data message or an activity relating to the data message will infringe the rights of a person or is not aware of facts or circumstances which reveal the infringing activity of the data message. This exception of liability however, is according to the wording of the regulations only applicable to civil and not to criminal liability. So in South Africa as well as in Germany there is still a juridical uncertainty about the service providers´ duties and how to get away from criminal liability when applying information location tools.

The ECTA also establishes in section 78 ECTA[329], corresponding to

---

[324] Visser "South Africa" 2003 *Computer Law Review International* 95.
[325] Section 77 (2) ECTA.
[326] See chapter 6 1 1.
[327] See chapter 5 4 and chapter 6 2 5.
[328] Section 76 Information location tools
A service provider is not liable for damages incurred by a person if the service provider refers or links users to a web page containing an infringing data message or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hyperlink (...).
[329] Section 78 ECTA No general obligation to monitor
1) When providing the services contemplated in this Chapter there is no general obligation on a service provider to-
a) monitor the data which it transmits or stores; or

Article 15 E-Commerce Directive, that there is no general obligation (FN: Text) for Internet service provider to monitor the information, which they transmit or store. This means that neither in European countries nor in South Africa the provider is obliged to actively seek for facts or circumstances indicating an unlawful activity.

Besides the ECTA, specific provisions for Internet service provider can be found in the Films and Publications Act.[330] The Act became operational on November 8, 1996 and represents the primary source of legislation regarding the classification of films and publications in South Africa. It was amended by the Films and Publications Amendment Act, No, 34 of 1999 and led to important innovations concerning the Internet industry perspective.[331]

The term of "publication",[332] according to this Act, is defined very broadly and was amended by the 1999 Act as "any message or communication, including a visual presentation, placed on any distributed network including, but not confined to the Internet". "Visual presentation" means "a drawing, picture, an illustration, a painting or an image, or (...) any combination thereof, produced through or by means of computer software on a screen or a computer printout". Thus Internet has become an issue for the investigative jurisdiction of the Film and Publication Board.[333]

In terms of section 27 of the Films and Publications Act 65 of 1996, it is an offence to produce, import and possess publications that contain child

---

b) actively seek facts or circumstances indicating an unlawful activity.
2) (...)

[330] The Films and Publications Act 65 of 1996, www.polity.org.za/govdocs/legislation/1996/act96-065.html.

[331] The Film and Publications Act, No. 65 of 1996 and the Film and Publications Amendment Act, No. 34 of 1999 (see: www.gov.polity.org.za).

[332] Chapter 1 ECTA.

[333] Chapter 2 ECTA (Establishment of Film and Publication Board and Film and Publication Review Board).

pornography. The distribution of hate speech is a criminal offence in terms of section 29 (1).[334] In the near future, Internet service providers[335] will be brought within the jurisdiction of the Act in so far as child pornography is concerned. It is therefore necessary to include definitions of "Internet address"[336] and "Internet service providers". The meaning of "possession" will thereupon include the downloading on computers. Section 1 of the Films and Publications Act will then be amended by substituting the definition of "distribute".[337]

According to section 27A, the service provider, among other things, has to take reasonable steps to prevent access to child pornography after he has obtained knowledge.[338]

The main objective of the Films and Publications Amendment Bill is to define provisions for the prohibition of child pornography and for matters incidental to the more effective investigation and prosecution of child pornography offenders. The significant readjustments of the Films and Publications Act do not include a tightening up regarding the hate speech on Internet respectively corresponding regulations for Internet service providers.

---

[334] "Any person who knowingly distributes a publication which, judged within context - (c) advocates hatred that is based on race, ethnicity, gender or religion, and which constitutes incitement to cause harm, shall be guilty of an offence".

[335] Amendment of section 1 of Act 65 of 1996, as amended by section 1 of Act 34 of 1999 1. (d) 'Internet service provider' means any person who provides access to the Internet by any means)

[336] Means a website, a bulletin board service, an Internet chat-room or newsgroup or any other Internet or shared network protocol address.

[337] "Distribute", in relation to a film or a publication, without derogating from the ordinary sense of the word, includes " to sell, hire out" or "offer" or "keep for sale or hire" and, to the purpose of sections 25 (a), (b) and (c), 26 (1) 8 (a) and (b) and 28 (1) and (2), it will include "to hand or exhibit a film or a publication to a person under the age of 18 years", and also "the failure to take reasonable steps to prevent access thereto by such person".

[338] See chapter 7 1 4.

7 1 4 Conclusion

To sum up, the Electronic Communications and Transactions Act of 2002 defines certain categories of service providers who do not incur liability for information carried via those providers. The aim of these provisions is to not hold service providers liable for the illegal dissemination of information, when the service provider itself did not positively commit an illegal transaction.

Section 73 ECTA establishes that no liability exists for the mere transmission of data messages in information systems wherein the service provider plays a passive role as a conduit of information for third parties. Section 73 ECTA is very similar to Article 12 of the E-Commerce Directive[339], the former section 5 (3) TDG[340] and section 9 E-TDG[341]. The provisions of Article 73 and Article 12 are almost identical in excluding liability for service providers who offer mere conduit. Both provisions presuppose that service providers have neither knowledge of nor control over information, which is transmitted or stored by them.

In South Africa and Europe the regulations of privileging liability as for caching resemble each other closely, in particular Article 13 (1) (a) - (d) E-Commerce Directive and section 74 (1) (a) -(d) ECTA. Section 74 ECTA in (1) (e) however, establishes that the service provider is not liable for caching as long as he removes or disables the access to the data he has stored upon receiving a take-down notice.

Neither the Directive nor the E-TDG proposed statutory "notice and take-down"- procedures concerning the disabling or removal of access to

[339] See chapter 6.
[340] See chapter 5 3 1 3.
[341] 6 2 2.

information. According to Article 13 (1) (e) of the Directive instead, an exception of liability presupposes that the provider will act expeditiously to remove or to disable access to the information he has stored as soon as he obtains actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or the access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

The knowledge requirements in section 75 ECTA correspond literally with those fixed in Article 14 E-Commerce Directive ("actual knowledge" / "not aware of facts or circumstances"). But section 75 (1) ECTA only states the conditions and circumstances, under which the service provider is not liable for damages.

Article 14 of the E-Commerce Directive instead applies to criminal liability as well. The provider in Europe is only criminal liable, if he gets actual knowledge of the illegality and - upon obtaining knowledge of illegal activity - acts expeditiously to remove or disable access to the information. Consequently, the E-Commerce Directive provides for a privileging of liability not only for mere conduit and caching, but also for hosting. The ECTA however, does not define provisions for hosting as far as criminal liability is concerned.

Besides the ECTA, specific provisions for Internet service providers can also be found in the Films and Publications Act.[342] Internet service provider must take into account some important judicial changes, in case the Films and Publications Amendment Bill will be legally passed.

---

[342] www.polity.org.za/govdocs/legislation/1996/act96-065.html.

The definition of "distribute" including "the failure to take reasonable steps to prevent access thereto by such a person" seems to be ambiguous because it is questionable if it only refers to privately held collections on a personal computer or if it will regard Internet service provider as well.

The term "reasonable steps" Films and Publications Amendment Bill can be interpreted differently. Section 27 of the Films and Publications Act simply provides the terms "creates", "in any way contributes to", "imports", or "obtain or access", which do not seem very clear. Thus an Internet service provider who gives mere access to the Internet could be considered a distributor within the meaning of the Act. This may cause juridical uncertainties among South African Internet providers.

The ECTA states very distinctly that a service provider is not liable for providing access to or for operating facilities for information systems or transmitting, routing, or the storage of data messages via an information system under its control in certain cases.[343] There is a contradiction proposed in the Films and Publications Amendment Bill. The ECTA excludes strict liability for Internet service providers whilst the Bill confirms - according to the wording - a strict liability. Consequently the Films and Publications Act defines the duties for service providers and the ECTA provides for possible justifications. So as for a consistency, the provisions of the ECT Act and the Bill leave much to be desired.

Opposed to German law[344], the Act has made service providers subject to the injunctive procedure commonly known as "notice and take-down" to avoid liability. Because take-down notices have a chilling effect on freedom of

[343] See chapter 7 1 3.
[344] The E-Commerce Directive suggested in Article 15 (2) that a "notice and take-down" procedure could be established in a form of self-regulation in the member states.

expression and can be compared to prior restraints, they apparently contradict the constitutional guarantee of freedom of expression as determined by previous rulings of South Africa courts.

This take-down requirement coupled with the right accorded to the Minister to approve the code of conduct for the industry representative body for service providers may have serious repercussions with respect to the unique opportunities offered by the Internet and other new media for freedom of expression. Notice and take-down-procedures can lead to a kind of self-justice and should be allowed to be carried out only by prosecution authorities or in response to a judicial order.

7 2 American law

Similar principles for the liability of Internet providers to those found in Germany can also be found in the USA. The legal position in America, however, is characterised by numerous individual regulations.

7 2 1 Liability for harmful content

States are particularly concerned about the control of pornography and obscenity on the Internet, also the United States. Finding that minors have access to harmful materials through the availability of the Internet, the Congress in 1998 enacted the Child Online Protection Act (COPA)[345] to restrict access by minors. This section was carefully drafted to respond to a 1997 U.S. Supreme Court decision, *Reno v. American Civil Liberties Union*

[345] 47 U.S.C. § 231 (2000).

(*ACLU*) 521 U.S. 844 (1997), that struck down as unconstitutional provisions of the Communications Decency Act (CDA)[346], which was enacted by Congress in 1996 to limit the exposure of children to sexually explicit materials online. The CDA stated that anyone who, "by means of a telecommunications device, knowingly makes, creates, or solicits, and initiates the transmission of any comment, request, suggestion, proposal, image, or other communication which is obscene (...) or indecent, knowing that the recipient of the communication is younger than the age of eighteen, is subject of criminal penalties of imprisonment of no more than two years, or a fine, or both".[347] § 223 (d) of the CDA criminalized using knowingly an interactive computer service to send, or display in a manner available to others, any image or "communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activity or organs". 47 U.S.C. § 223 (a) and (d) found to be unconstitutional by the Supreme Court.[348] The *ACLU* decision also challenged the provisions of sections 223 (a) (2) and 223 (d) (2) which made it a crime for anyone to "knowingly permit any telecommunications facility under his control to be used for any activity prohibited" in sections 223 (a) (b) and 223 (d) (1).

Still of relevance is § 223 (e). According to 47 U.S.C. § 223 (e) (1),[349] an

---

[346] Title V, § 502, 110 Stat. 133 (1996) (current version at 47 U.S.C. § 223 (2000)).
[347] 47 U.S.C. § 223 (a).
[348] In its June 26, 1997 decision, the Supreme Court held that the CDA' s "indecent transmission" and "patently offensive display" provisions violated the First Amendment's protection of free speech (see: *Reno v. ACLU*, 929 F.Supp. at 879).
[349] 47 U.S.C. section 223 (e) Defences
In addition to any other defences available by law:
(1) No person shall be held to have violated subsection (a) or (d) of this section solely for providing access or connection to or from a facility, system, or network not under that person's control, including transmission, downloading, intermediate storage, access software,

access provider is not liable, if he merely offers access to an open computer network. The provision protects Internet service provider who has taken, "in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors to forbidden communications". This also includes the disposal of the necessary access software or the operating of a Proxy-Cache-Server. Under 47 U.S.C, section 223 (e) (2) (3),[350] there is no exemption from liability if and when the Internet provider works together with the author of illegal content or advertises illegal content or offers access to the computer system used to distribute the content, which is under his control. Other federal laws remain unchanged.

A further approach in the USA can also be seen in 47 U.S.C. § 231, introduced by the "Child Online Protection Act".[351] This provision[352] makes those liable, who knowingly and for commercial purposes make any communication by means of the WWW which is available to any minor and includes any material that is harmful to minors.[353] The liability provision however, does not apply to network and access providers or search engines

---

or other related capabilities that are incidental to providing such access or connection that does not include the creation or the content of the communication.

[350] 47 U.S.C. section 223 (e) Defences
In addition to any other defences available by law:
(2) The defences provided by paragraph (1) of this subsection shall not be applicable to a person who is a conspirator with an entity actively involved in the creation or knowing distribution of communications that violate this section, or who knowingly advertises the availability of such communications.
(3) The defences provided in paragraph (1) of this subsection shall not be applicable to a person who provides access or connection to a facility, system, or network engaged in the violation of this section that is owned or controlled by such person.

[351] www.cdt.org/speech/constitutional.html.

[352] On May 13, 2002, in *Ashcroft v. ACLU* - 122 S. Ct. 1700 (2002) , the U.S. Supreme Court upheld sections of COPA as not unconstitutionally overbroad, but the Court expressed no viewpoint as to whether COPA surveys strict scrutiny.

[353] 47 U.S.C. § 231 (a) Whoever knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the WWW, makes any communications for commercial purpose that is available to any minor and that includes any material (...) is harmful to minors shall be fined no more than $ 50,000, imprisoned no more than 6 month, or both.

or similar functional carriers. All Internet providers can provide an affirmative defence in the case of prosecution by showing they have taken control measures restricting access by minors to material harmful to minors.[354] This includes, for example, requiring the use of a credit card or adult personal identification number.

Several single states like Pennsylvania enacted a net blocking law that enables the state Attorney General to order the blocking of web sites by Internet service providers.[355] Similar measures will be taken in Maryland, Oklahoma and New Jersey. Internet providers are required to block sites even if they do not host the content and have no relationship whatsoever with the publishers of the content. The law provides that the state Attorney General or any county district attorney can unilaterally apply to a local judge for an order declaring that certain Internet content may be child pornography, and requiring any Internet service provider serving Pennsylvania citizens to block the Internet content. Net blocking law like Pennsylvania's child porn law led to a massive over blocking of websites, because the technical design of the Internet dictates that most Internet service providers can only comply with the blocking orders by also blocking a significant amount of innocent web site content as well. The court proceeding occurs with only government participation and no prior notice to the Internet Service Provider. One Internet Protocol number may be in use for hundreds of legal sites as well as one illegal. A blocking order concerning one incriminated website of the international Internet provider MCI in Pennsylvania demanded the blocking of *terra.es*, the biggest hoster in Spain although American MCI customers would

[354] 47 U.S.C. § 231 (b) (1) .
[355] 18 Pa. C.S. § 7626.

hardly have been able to access thousands of Spanish websites.[356]

7 2 2 Liability for copyright infringement

Violators of intellectual property rights have long been subject to criminal prosecution in the United States. The State of New York enacted criminal sanctions against trademark counterfeiting in 1847, and 39 other states followed suit by 1899.[357] Copyright infringement has been considered a federal crime since 1909. The statutes governing criminal copyright infringement were substantially amended in 1997.[358] These amendments modified the requisite elements of crime.

Copyright infringement is a crime if and when it is done wilfully and either for commercial advantage or private financial gain;[359] or by reproduction or distribution on a large scale - even if not committed for commercial gain.[360] Service provider liability was taken into consideration in light of Congress' reaction to the issue, i.e. the enactment of the Online Copyright Infringement Liability Limitation Act[361], which significantly circumscribes the conditions under which online service providers might incur liability.[362] This section provides limitation for infringement in the following cases:

(i) automatically transmitted communications (such as electronic mail

---

[356] "Pennsylvania child porn law causes massive over blocking off sites", www.theregister.co.uk /2004/01/13/pennsylvania_child_porn_law_causes/print.html). The constitutionality of the Pennsylvania statute is under challenge (See Centre for Democracy and Technology v. Fisher, E.D. Pa. No. 03-5051).
[357] www.aippi.orrg/reports/q169/q169usae.html.
[358] No Electronic Theft Act (NET), Pub. L. No. 105-147, 111 Stat. 2678 (1997).
[359] 17 U.S.C. § 506 (a) (1) in concert with 18 U.S.C. § 2319.
[360] 17 U.S.C. § 506 (a) (2).
[361] Online Copyright Infringement Liability Limitation Act, Pub. L. No. 105-304, 112 Stat. 2877 (1998).
[362] 17 U.S.C. § 512.

messages) which are not modified or edited by the service provider and are not maintained any longer than reasonably necessary,[363]

(ii) system caching of materials requested by users (such as popular websites) on behalf of subsequent users[364]

and

(iii) information residing on systems at the direction of users[365].

The United States also regulated the limitation of liability for information location tools in the case of copyright infringements. Information location tools referring or linking users to an online location containing infringing material or infringing activity are not liable as long as the service provider does not have knowledge of the infringement or financial benefit directly attributable to the infringing activity, if and when the service provider, upon notification, removes the infringing materials or the access to them.[366] Section 512 also provides a process, by which copyright holders may notify service providers of allegedly infringing activities, and service providers have certain duties to respond and by which injunctive or other relief may be sought.[367]

In order to address online service provider liability and to remove it under certain circumstances, in 1998, the Online Copyright Infringement Liability Limitation Act was signed into law. As outlined above, it limits, in a number of online contexts, liability of service providers.[368]

---

[363] 17 U.S. C. § 512 (a).
[364] (17 U.S.C. § 512 (b).
[365] Such as a hosted Web site as long as the service provider does not have knowledge of the infringement or financial benefit directly attributable to the infringing activity, if and when the service provider, upon notification, removes the infringing content, (17 U.S.C. § 512 (c)).
[366] (17 U.S.C. § 512 (d)).
[367] (17 U.S.C. § 512 (g)-(j)). See also A&M Records, Inc. v. Napster, Inc., No. C99-05183 MHP, 2000 WL 573136, at *10 (N.D. Cal. May 12, 2000).
[368] Pub. L. No. 105-304, 112 Stat. 2877 (codified at 17 U.S.C. § 512).

7 2 3 Conclusion

It is quite impossible for network and access providers, to control and block content sent over the Internet, which is why they are on the whole exempt from criminal liability under the E-Commerce Directive of the European Union, the German E-TDG and 47 U.S.C. § 223 (e) (1). According to 47 U.S.C. § 223 (e) (1) an access provider is not liable, if he merely offers access to the Internet. This provision is similar to section 73 ECTA, which establishes that no liability exists for the mere transmission of data messages in information systems wherein the service provider plays a passive role as a conduit of information for third parties and to Article 12 of the E-Commerce Directive[369], the former section 5 (3) TDG[370] and section 9 E-TDG[371].

The Online Copyright Liability Limitation Act limits in a number of Internet contexts the liability of Internet service providers. Like in South Africa's ECTA, opposed to German law[372], 17 U.S.C. § 512 has made service providers subject to the injunctive procedure commonly known as "notice and take-down" to avoid liability for copyright infringements.

The Pennsylvania Law imposes potential liability on Internet service providers for child pornography, even if the providers are not hosting the offending content and have no reference to the author and publisher of the content. The Act restricts Internet content and sets a precedent on regulating

---

[369] See chapter 6.
[370] See chapter 5 3 1 3.
[371] See chapter 6 2 2.
[372] The E-Commerce Directive suggested in Article 15 (2) that a "notice and take-down" procedure could be established in a form of self-regulation in the member states.

Internet providers without notice.[373]

7 3 Convention on Cybercrime

Cybercrime is transnational and requires a transnational response. For that reason, the Council of Europe adopted the Convention on Cybercrime.[374] The Convention on Cyber-crime is the first international treaty on crimes committed via Internet and other computer networks, dealing particularly with computer-related fraud, infringements of copyright, child pornography and violations of network security.[375] The Convention is the product of four years of work by the Council of Europe (including Germany) and by the United States, Canada and other countries (like South Africa), which are not members of the organisation. The Convention and its Explanatory Report[376] were adopted by the Committee of Ministers of the Council of Europe on November 8, 2001 and the Convention was opened for signature in Budapest, on 23 November 2001, at the conclusion of the International Conference on Cybercrime during which the doubts of human rights activists and data protectors were expressed.[377] To date 31 states have signed the Convention, including Germany and South Africa.[378] The Cybercrime Convention entered into force on 1st July 2004 following its ratification by Lithuania, Albania,

---

[373] On September 9, 2003, the American Civil Liberties Union (ACLU) of Pennsylvania filed in a constitutional challenge to the "net blocking law". The challenge, filed in the U.S. District Court of the Eastern District of Pennsylvania, argues that the "net blocking law" is a prior restraint on speech that violates the First and Fourteenth Amendments, see: www.theregister.co.uk /2004/01/13/ pennsylvania_child_porn_law_causes/print.html).

[374] Convention on Cybercrime under www.conventions.coe.int/Treaty.

[375] Substantive criminal law in chapter II, section 1 of the Convention.

[376] The text of the Explanatory Report does not constitute an instrument providing an authoritative interpretation of the Convention, although it might be of such a nature as to facilitate the application of the provisions.

[377] See the initiative of the Global Internet Liberty Campaign (www.gilc.com) and their members like the American Civil Liberties Union, Canadian Journalists for Free Expression or Cyber-Rights & Cyber-Liberties (UK).

[378] www.conventions.coe.int/Treaty/EN/searchings.asp?NT=185&CM=1&DF=16/04/04.

Croatia, Estonia and Hungary. Ratified conventions are binding for a state. Nearly three years after the treaty was open for signature by the member states and the non-member states, which have participated in, its elaboration only five countries have ratified the convention. This shows that harmonisation of law is often not easy to achieve.

During the drafting of the convention some states wanted to act internationally against racist and discriminating contents; for example Germany wanted to be able to take legal action against Nazi websites in the USA. But such limitations on the freedom of speech and expression in the Convention were rejected, particularly by the USA.[379] In response, an Additional Protocol to the Convention on Cybercrime Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature committed through Computer Systems was drawn up. The protocol can be ratified independently from the "main" convention.[380] Through the Additional Protocol the members of the Council of Europe aim to achieve greater unity over the question of how to define and combat racist and xenophobic material.

This convention supplements other conventions like the European Convention on Mutual Assistance in Criminal Matters from 1959. Article 45 of the Convention on Cybercrime regulates how interpretation problems can be solved.[381]

---

[379] www.krefeldercomputerclub.de/Computer/cybercrime.htm.
[380] www.conventions.coe.int; www.heise.de/newsticker/data/anw.
[381] Settlement of disputes (Article 45)
Article 45 (1) provides that the European Committee on Crime Problems (CDPC) should be kept informed about the interpretation and application of the provisions of the Convention. There is an obligation on the Parties to seek a peaceful settlement of any dispute concerning the interpretation or the application of the Convention. Any procedure for solving disputes should be agreed upon by the Parties concerned. Three possible mechanisms for dispute-resolution are suggested by this provision: the European Committee on Crime Problems itself, an arbitral tribunal or the International Court of Justice.

7 3 1 Content and implications of the Convention and the Additional Protocol

The Convention represents a substantial revision of the provisions contained in an earlier version released on April 25, 2000 and provides in chapter I (Use of terms) definitions of critical terms. "Service provider"[382] means "any public or private entity that provides to users of its service the ability to communicate by means of a computer system; any other entity that processes or stores computer data on behalf of such communication service or users of such service".

The definitions are overly broad and unclear about what conduct falls within the definitions. For example, the Convention defines a computer as "any device or a group of interconnected or related devices one or more of which, pursuant to a program, performs automatic processing of data"[383]. This definition is problematic because it does not define or limit what constitutes a device, thus, potentially including Palm Pilots or cable TV boxes. The broad definition of a service provider in the Convention could conceivably encompass any Internet user who maintains a website. Furthermore, it is not

[382] Explanatory Report about service provider: "The term "service provider" encompasses a broad category of persons that play a particular role with regard to communication or processing of data on computer (...) it is made clear that both public and private entities which provide users the ability to communicate with one another are covered. Therefore, it is irrelevant whether the users form a closed group or whether the provider offers its services to the public, whether free of charge or for a fee. The closed group can be e.g. the employees of a private enterprise to whom the service is offered by a corporate network (...)." For example, under this definition, a service provider includes both services that provide hosting and caching services as well as services that provide a connection to a network. However, a mere provider of content (such as a person who contracts with a web hosting company to host his web site) is not intended to be covered by this definition if such content provider does not also offer communication or related data processing services (www.conventions.coe.int/protocol).
[383] Article 1 (b) of the Cybercrime Convention.

clear whether the ambiguous definition of "traffic data"[384] includes for example hyperlinks[385]. If the definition of "traffic data" does include hyperlinks, the definition may be more invasive on communication than the drafters of the Convention intended.

Chapter II of the Cybercrime convention describes measures to be taken at the national level. In section 1, the substantive criminal law is described. The Convention encompasses a list of crimes, some of which currently are crimes in one signatory country but are not in another.

The measures relate to specific fields where each party to the treaty shall adopt legislative measures to provide for offences against the confidentiality, availability and integrity of computer data and systems; computer-related offences, content related offences, offences related to infringements of copyrights and related rights; ancillary liability and sanctions. The Convention does not, however, include guidance detailing the elements required for those offences. For example, the USA may want to prosecute a citizen form France for the crime of illegal access. France's criminal cyber law may not include access to a computer system connected to another computer system within the definition of illegal access. Thus, the USA could not prosecute a French citizen who accessed a computer connected to another computer. In contrast, if the USA and France were both signatories to a Convention codifying the elements of the crime, US prosecutors could prosecute a French citizen because both countries would recognise the same

[384] Article 1 (d) "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.
[385] Defining hyperlinks as an element in an electronic document that links to another place in the same document or to an entirely differently document.

criminal elements. If signatories do not agree upon the elements of a crime, we could face a similar problem as was confronted in *Yahoo! Inc. v. La Ligue Contre Le Racism Et L' Antisemitisme*[386]. Crime standardization could pose some difficulties for regulators because countries may be reluctant to sign the Convention if it infringes upon domestic legal regimes and cultures. Especially when we compare Germany and the USA there are radically different fundamental rights and freedoms between the two countries. As shown, what is hate speech in Germany[387] is freedom of speech, protected by the First Amendment in the United States.

The Convention drafters empowered signatories to enact crime legislation out of concern that if the Convention retained too much power, members would be unwilling to ratify it.[388]

Chapter II, section 2 of the Convention describes procedural measures to be taken at national level by nation states that proceed to ratify the treaty. The measures relate to: specific fields where each party to the treaty shall adopt legislative measures to establish criminal procedures ensuring the empowerment of competent authorities to search and seize stored computer data, make production orders, request the expedited preservation of data stored in a computer system, request the expedited preservation and disclosure of traffic data, intercept electronic communications, and order real-time collection of traffic data.

---

[386] See chapter 3 1 2 ; LICRA & UEJF v. Yahoo! Inc., Tribunal de Grande Instance Paris; www.juriscom.net/txt/jurisfr/cti/tgiparis2000011200.
[387] See chapter 3 1 3 3 (*Töben* case and *Zündel* case).
[388] See Explanatory Memorandum, supra note 1, at 145 (articulating the Convention's purpose is to strike a balance between harmonizing international law and the sanctity of the sovereign.

The provisions of the Convention addressing jurisdiction[389] and international cooperation are intriguing. In particular, each nation state shall enact laws enabling the exercise of jurisdiction over offences committed in its territory. It is apparent that extra-territorial jurisdiction to be exercised by the signatories to the Convention can only be realised through international cooperation. Thus, in addition to asserting general principles concerning the widest possible international cooperation, the Convention details international procedures applicable in various cases. Among the items covered by the Convention are extradition, mutual assistance requests in the absence of applicable international agreements, mutual assistance regarding provisional measures, transborder access to stored computer data not requiring mutual legal assistance, mutual legal assistance regarding interception of data, and real-time collection of traffic data.

The Convention drafters included broad jurisdictional provisions to provide flexibility for states to decide jurisdictional issues in the event of a dispute. Article 22 (1) states, that "each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction (...) when the offence is committed in its territory; or on board a ship flying the flag of the Party; or on board on aircraft registered under the laws of that Party; or by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State". This provision corresponds to sections 3, 4 and 7 (2), no. 1 of the German Criminal Code (StGB)[390].

Article 22 (5) of the Convention allows the parties to determine the most

[389] Chapter II section (3) of the Cybercrime Convention.
[390] See chapter 3 1 3.

appropriate forum to prosecute a claim. But the Convention does not contain a mechanism to deal with conflicts in jurisdiction, further supporting the necessity of clear jurisdictional guidelines. Where crimes involve multinational contact, conflicts of jurisdiction are sure to arise. For example, jurisdiction issues existed where a company incorporated in Vanuatu, operated its business from Australia, maintained its computer server in Denmark, maintained its source code in Estonia and the original developers resided in the Netherlands.[391] The court had to determine whether jurisdiction was in the home state, in each state through which the data traffic travelled or where the harm occurred.

In spite of the Convention, and considering the lack of clear jurisdictional guidelines in place, juridical problems as shown in the Frederic *Töben´s* case[392] do not seem to be fully avoidable either.

The Convention may yield unwieldy conflicts and inconsistent decisions as long as a priority of jurisdiction is not established between the states. Jurisdictional priority should be given to the institutions of a country where the harm incurred and not to the country where the crime was initiated.

Moreover, a detailed guidance should be determined as to what types of political offences or prejudices will legitimately justify a refusal to cooperate by competent authorities.

The section on "attempt and aiding or abetting" (Article 11) in Title 5 of Chapter II[393] is of particular interest to Internet providers. According to the explanatory report of the convention, the purpose of this article is to establish additional offences related to attempting and aiding or abetting the

[391] *Leiber v. Consumer Empowerment* BV, No. 01-09923-SVW (C.D. Cal. 2003).
[392] See chapter 3 1 3 3.
[393] Ancillary liability and sanctions.

commission of the offences defined in the Convention.

Although the transmission of harmful content data or malicious code through the Internet requires the assistance of service providers as a conduit, the Convention provides that a service provider that does not have criminal intent cannot incur liability under this section. Thus, no duty is imposed on a service provider to actively monitor content to avoid criminal liability under this provision. As with all the offences established in accordance with the Convention, attempt and aiding or abetting must be committed intentionally.

Article 27 of the Convention specifically allows a party to refuse extradition under certain circumstances, such as crimes constituting political offences or those that may prejudice a nations interests.[394]

The provision does not clarify what types of offences qualify as "political" in nature or which they will consider prejudicial. As seen in the *Yahoo*! case,[395] this provision will quickly run afoul simply from different interpretations of what constitutes a political offence.

7 3 2 Additional Protocol to the Convention on Cybercrime

The Protocol addresses the definition of "racist and xenophobic material"

[394] Article 27 (4) (a)), allowing parties to refuse to extradite nationals if "the request concerns an offence, which the requested party considers a political offence or an offence connected with a political offence, or it considers that execution of the request is likely to prejudice its sovereignty, security order public or other essential interests".

[395] See chapter 3 1 2 ; LICRA & UEJF v. Yahoo! Inc., Tribunal de Grande Instance Paris; www.juriscom.net/txt/jurisfr/cti/tgiparis2000011200.

and how the members of the Council of Europe could act against such material through criminal law and criminal procedure. The Protocol first links to the Convention the critical terms like "computer system" and "service provider" and defines "racist and xenophobic material".[396] One should note that "dissemination" of such material in a computer system (Article 3) includes exchanging such material in chat rooms, posting similar messages in newsgroups or discussion fora, because such material is thereby made available to the public.[397] The term "to the public" used in Article 3 makes it clear that private communications or expressions via email communicated through the Internet fall outside the scope of this provision. The distributing or otherwise making available through a computer system to the public of material, which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity (Article 4) shall be criminally punishable under the domestic law of each nation. This provision would not lead to change of German criminal law because Germany has a very strict law against genocide as described in chapter 4 above. As in the Convention itself all offences contained in the Protocol must be committed "intentionally" in order for criminal liability to apply. The drafters of the Protocol like those of the Cybercrime Convention agreed that the exact meaning of "intentionally" should be left to national interpretation. In the case of Internet service providers it is, for example, not sufficient for a finding of liability, that the provider served solely as a conduit for, or hosted a website or newsroom,

---

[396] "Racist and xenophobic material" means "any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence against any individual group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors" (Explanatory Report on Article 2 of the Protocol).

[397] See the commentatory on the articles of the Protocol under www.conventions.coe.int /Protocol/comments.

containing racist and/or xenophobic material, unless there was intent, as required by the applicable domestic law. Moreover, Internet providers are not required to monitor conduct to avoid criminal liability. This liability regulation for Internet providers conforms to the European E-Commerce Directive. It is incorporated in German law in terms of the E-TDG.

7 3 4 Conclusion

The Convention attracted widespread attention and sometimes critical comments from various interest groups like privacy activists questioning the access provisions; security professionals querying the restriction on tools; and the International Working Group on Data Protection in Telecommunications disagreeing with the requirement of maintaining traffic data.

Domestic laws are generally confined to a specific territory. As cybercrime is not limited to national boundaries, it can only be properly and efficiently addressed by having some international understanding as to what it is and how it should be fought. As the above discussion shows, achieving a global consensus is always difficult. Differences in the participating states over cultural and national security issues have made the attempt to establish common standards a daunting task. Solutions to the problems posed in the thesis should be addressed by international law, necessitating the adoption of adequate international legal instruments. The Convention aims to meet this challenge. But the criticism of activists like the Global Internet Liberty Campaign, an international Internet association of different groups like data protectors, journalists and human rights activists should also to be taken into

account.[398] The Convention could contravene the norms for the protection of the individual like freedom of speech and expression, and it would expand the police authority of national governments. The Convention will probably reduce government accountability in future law enforcement conduct.

The provisions[399] that will require Internet service providers to retain records regarding the activities of their customers are problematic. These provisions pose a risk to the privacy and human rights of Internet users and contravene principles of data protection. The Convention does not provide a stricter liability for access, content, and service providers[400] than does German criminal law.

The purpose of the Additional Protocol is twofold: firstly harmonising criminal law in the fight against racism end xenophobia on the Internet and secondly improving international cooperation in this area. The Additional Protocol offers a great opportunity to continue international harmonisation in combating cybercrime dealing with racist and xenophobic material. While the Convention covers various harmonisation strategies about many, diverse topics, the Protocol deals with a more restricted area. It tries to harmonise the understanding of what is, for example, "racist" or "denial of genocide and crimes against humanity". From this shared understanding the Protocol then promotes coordinated action against racist and xenophobic material on the Internet.

The Cybercrime Convention is a long-overdue start towards addressing the exigent circumstances evolving from the Internet. Its success will hinge

---

[398] www.gilc.com.
[399] Articles 17, 18, 24, 25 of the Cybercrime Convention.
[400] On the Convention they fall all under the term "service provider", see chapter I Article 1 © of the Convention.

upon the cooperation of all countries, both parties to the Convention and those that are not.

8 Excursion: Possibilities for preventing criminally intended contents

8 1 Measures of self-censorship

Most legal systems are aware that child pornography and other illegal contents in computer networks cannot be combated through criminal prosecution alone. This has led to the formation of pressure groups of Internet providers, for example in Germany, France, Belgium, Canada, Austria, the United Kingdom and Spain.[401] These countries have developed organisations, in which authorities, Internet providers and users work together, collaborating in two fields: self-censorship and codes of conduct.

8 1 1 Codes of conduct

Self-censorship of Internet providers is often called "codes of conduct".[402] Committees or national associations of Internet service providers lay down these codes. They are developed partially from contractual provisions among Internet providers and their subscribers, and partially through governmentally set-up working groups (particularly in France and Japan). In Italy, the codes of conduct are only binding after endorsement by state authorities.[403] Regarding the commitment to codes of conduct, international Internet providers are

---

[401] For Spain: the AUI-Associacion des Usuarios de Internet; for France: Association des utilisateurs de l'Internet.
[402] For Germany see: www.fsm.de/webvk1.html
[403] www.echo.lu/legal/de/internet7wp2de-chap.html.

obliged to turn their attention in particular to the legal use of the Internet in order to prevent the presence of unlawful contents on the Internet. They are obliged to create registration offices, make an effort in identifying their subscribers or to inform prosecution authorities about certain offences and infringements.

The codes of conduct provide special sanctions[404] for any infringements of these duties. These sanctions vary from disapproval to public rebukes. In some countries, governmental registration offices exist. The "Meldepunt Kinderporno" was developed in the Netherlands by providers, users and the police. It opened in June 1996 and was the first its kind in Europe.[405] This Meldepunt informs providers about illegal contents on their servers. A similar organisation exists in Germany, the "Netz gegen Kinderporno" that searches the Internet for child pornography.[406]

Problems arise for the laying down of codes of conduct for internationally active online providers. They are operating in different legal systems, in which varying penal provisions apply. Special problems arise if certain behaviour, for example the dissemination of Nazi propaganda, is illegal in a particular country (for example Austria and Germany), but lawful or acceptable as a result of the freedom of expression in other countries. For example, in Denmark, the dissemination of Nazi symbols, such as swastikas, is legal and can be disseminated on the Internet without any legal consequences.[407] It will therefore be interesting to see to which codes of conduct these internationally active online providers will be subjected. These codes are likely to be "soft

---

[404] An exception is the code of conduct of the Canadian Association of Internet Provider (CAIP) - it does not provide consequences in cases where the code is disregarded.
[405] Www.meldepunt.de.
[406] www.heise.de/Netz_gegen_Kinderporno.
[407] Sieber "Verantwortlichkeit von Internetprovidern im Rechtsvergleich" 1999 *ZUM* 209.

law", which however have the potential to serve as precursors for a more harmonised world-wide criminal law.

8 1 2 Self-censorship of online providers in Germany

In Germany, the *Freiwillige Selbstkontrolle Multimedia Dienstanbieter e.V.*[408] (FSM)[409] assists actively in reducing punishable online contents. An advantage of being a member of the FSM is that professional providers who offer contents, which may be harmful to young people, are as members of FSM exempt from the duty to have a youth protection commissioner[410] The aim of the FSM is to ensure youth protection and to prevent the presence of illegal content on the Internet and to remove any such contents, which may be present. Individual communications, such as email, are excluded from this form of control. The *Freiwillige Selbstkontrolle Multimedia Dienstanbieter e.V.* is also not competent to check data-rights, copyright or competition law infringements[411].

The members of the FSM obligate themselves to contribute to the prevention of illegal contents. This obligation is however limited to statutory liability and it

---

[408] www.fsm.de.
[409] Self-censorship of Multimedia Service provider –incorporated association.
[410] § 7a s.4 GjSM, 8 IV s.1 MdStV.
[411] Rath-Glawatz & Müller-Using "Rechte in der freiwilligen Selbstkontrolle" 1997*JMS-Report* (5) 53.

applies only if the prevention of illegal contents is actually possible and can reasonably be expected of the member. Content that should not be offered or made accessible is content that is punishable in terms of section 130 StGB[412], section 130 (a) StGB[413], section 131 StGB[414], section 86 StGB[415] and section 184 (3) StGB[416].

The code of conduct of the FSM provides that its members have a duty to ensure that children and young people do not have access to illegal content, which is punishable under section 184 (1) StGB (dissemination of pornographic writings. In terms of the latter section, such content includes offers, which are obviously harmful to children and young people. If an infringement of the code of conduct occurs, anyone may file a complaint. The complaints have to be sent to the FSM via email.[417] Once the appointed committee of the FSM investigates the complaint and discovers that an infringement of the code of conduct has taken place, it can sanction the wrongdoer. The sanction can take the form of a request to put things right, a display of its disapproval or a rebuke.

The request to put things right and the disapproval of infringements against the code of conduct remain unpublished and are made only to the provider, serving merely as an appeal to the provider's conscience. Only the rebuke is published. The online provider has the duty to ensure the publication of the rebuke on the Internet for one month, so that every user can determine which providers do not adhere to the code of conduct.

---

[412] (Genocide).
[413] Instruction for crimes.
[414] Racial hatred.
[415] Dissemination of propaganda material of unconstitutional organisations.
[416] Dissemination of pornography.
[417] hotline@fsm.de.

Where a foreign provider offers illegal content and so infringes codes of conduct, an equivalent to the FSM may exist in its country of origin. In this case, the FSM passes on its complaint to the self-censorship controlling body in the provider's country. This self-censorship controlling body can then decide whether it wants to sanction the provider in question.

A provider-independent initiative also exists: "Netz gegen Kinderporno"[418] (Network against child pornography), which was established by the German Child Welfare Organisation in conjunction with some German newspapers. The widespread willingness of users to co-operate with this initiative came as a huge surprise to the initiators and the prosecution. Three months after the founding of the registration office, 450 announcements about child pornography on the Internet were made. As a result of this, 300 investigations into child pornography were commenced.[419]

8 2 Special obligations of providers and their capabilities and possibilities for exercising control

Some legal systems do not limit the liability of Internet providers. They however burden the providers with special duties to control unlawful and harmful contents on the Internet. The main duty of online providers is to install filter software. American reform proposals include the duty to install filter software, bring charges against criminal users and to expel certain persons from the Internet.

---

[418] www.heise.de/ct/Netz_gegen_Kinderporno.
[419] ibid.

8 2 1 What is filter software?

In the past couple of years, the software industry developed various filter software with different functions. The Criminal investigation Department of the German state Hesse (*Hessisches Landeskriminalamt*) has developed software that makes use of the data bank of the Federal Criminal Investigation Department (*Bundeskriminalamt*). This software makes it possible to find child pornography on hard discs.[420] New software has been developed particularly in the area of youth protection software. These technical systems allow for the blocking of various content, so that aspects of various moral and legal opinions of different legal systems are addressed. In addition, parents are enabled to decide what kind of content their children may be exposed to on the Internet.

The blocking of the contents does not take place on the "source" of contents, as the publication of the content itself is not prevented. The blocking takes place because the user cannot call up the contents. The filter software operates by means of so-called negative lists. All web sites, which are noted on these lists, are blocked, while a content not listed is allowed to pass. The best-known programs are Cyber-Patrol and Surfwatch[421]. These programs can be downloaded from the Internet and are useful in protecting children from exposure to harmful contents. Sometimes however, even these programs need protection. In May 2001, Cyber Nanny, the developer of filtering protection software, was hacked and defaced[422].

---

[420] *Die Zeit* March 26, 1998, 69.
[421] www.cyberpatrol.com; www.surfwatch.com.
[422] www.theregister.co.uk/content/6/18412.html.

Negative lists must be contrasted with positive lists that block all Internet contents except these which are marked as permissible. This procedure is used mostly in schools.[423].The third method is the neutral mark. Web sites are marked free of any value and can be rated according to the opinion of the user. The World Wide Web Consortium[424] has developed PiCS (Platform for Internet Content Selection), which is the most significant neutral software and rating system. PiCS is widely supported by various governments and industry-based organisations, such as the Internet Watch Foundation in the UK. PiCS works by embedding electronic labels in the text or image documents to vet their content before the computer displays them or passes them to another computer.[425]

The vetting system of PiCS can be applied to political, religious, advertising or commercial topics. The most common scheme is that developed by the Recreational Software Advisory Council on the Internet (RSACi). This was originally a scheme for rating computer games[426]. It rates material according to the degree of violence, sex, nudity and obscene or profane language. PiCS can read other negative and positive lists (for example Cyber-Patrol), but also uses the ratings systems of publishing houses, religious organisations and online providers.[427] A lot of online providers offer several filter software to their users. Parents, teachers and companies can choose which filter software best serves their needs.

---

[423] Ritz *Inhalteverantwortlichkeit von Online-Diensten* (1998) 43.
[424] www.w3org; Union of more than 100 international companies, among them hard-and software industry, telecommunication businesses and media firms (AT&T, AOL, Apple, CompuServe, IBM, Microsoft, Time Warner).
[425] www.julius.co.uk/censorship/faq.html.
[426] www.rsaci.org.
[427] Ritz *Inhalteverantwortlichkeit von Online-Diensten* 44.

8 2 2 Duty to offer filter software

In recent years, reform proposals in the USA have demanded that Internet providers should be obliged by law to offer filter software free of charge to their users.[428] Furthermore, certain end users, like schools or public libraries, should be obliged to use filter software by law. Laws such as the Communications Privacy and Consumer Empowerment Act of 1997[429], Family-Friendly Internet Access Act of 1997[430] or Who is E-Mailing our Kids Act of 2001[431] force the blocking of contents, which are harmful to children. To block the contents, Internet providers will have to offer their subscribers filter software free of charge or at cost price. The model for the reform proposals was the Internet provider CompuServe, who has been providing filter software free of charge to their subscribers since 1996. [432]

The reform proposals of Safe Schools Internet Act of 1999[433] and the Children's Internet Protection Act[434] want schools and public libraries, which offer Internet access, to bear the duty of using filter software to prevent the access to harmful Internet content for children and young people.

8 2 3 The duty of Internet providers to inform the Criminal Prosecutor

Through the insertion of 27A in Act 65 of 1996 (The Films and

---

[428] Sieber "Verantwortlichkeit von Internetprovidern im Rechtsvergleich" 1999 *ZUM* 205.
[429] H.R. 1964 of the 105th congress, introduced June 19, 1998, www.thomas.loc/gov/home/c105query.html
[430] H.R. 1180 of the 105th congress, ibid.
[431] H.R. 1846: To amend section 254 of the Communications Act of 1934 to require schools and libraries receiving universal service assistance to block access to Internet services that enable users to access the www; ibid.
[432] Sieber "Verantwortlichkeit von Internetprovidern im Rechtsvergleich" 1999 *ZUM* 205.
[433] www.thomas.loc.gov/home.
[434] Pub.L. 106 - 554, titel XVIII; www.tcc.gov/wch/universal_service/chipact.de.

Publications Act),[435] South African Internet service provider shall register with the Board and have to fulfil several obligations. The obligations for Internet service providers are only concerning child pornography. Under section 27A, Internet provider "shall take all reasonable steps to prevent the use of their services for the hosting or distribution of child pornography" (27A (1) (b)). The section provides the legal obligation on Internet service providers who have knowledge that their service is used for the hosting or distribution of such material to report the presence of child pornography to the South African Police Service. The Internet service provider has also report the police particulars of the person "behind" the child pornography on the Internet.[436] The providers are obliged to preserve evidence of child pornography for purposes of investigation and prosecution and shall, upon request by the South African Police Service, furnish the particulars of users "who gained or attempted to gain access to an Internet address that contains child pornography". The provision statutes in paragraph (4) that "any person who fails to comply with the provisions of this section shall be guilty of an offence".

In the United States, another possible way of imposing obligations on Internet providers is the Protection of Children from Sexual Predators Act of 1998. This law, 42 U.S.C. § 227, obliges every provider of telecommunication and data communication services to inform criminal prosecution authorities about the production, dissemination or possession of child pornography in

---

[435] Film and Publications Amendment Bill (explanatory summary of the Bill published in Government Gazette No 25421 of September 1, 2003).

[436] "Registration and other obligations of Internet service providers" 27A. (2) If an Internet service provider has knowledge that its services are being used for the hosting or distribution of child pornography, such internet provider shall – (b) report the presence thereof, as well as the particulars of the person maintaining or hosting or distributing or in any manner contributing to such Internet address, to a police official of the South African Police Service; (...).

terms of 18 U.S.C. §§ 2251, 2251(a), 2252, 2252(a), 260. If an Internet provider knowingly omits this notification, he may be fined for up to US$50,000; if the omission occurs again, the second fine can be up to US$100,000. The Internet providers must inform the criminal prosecution authorities about child pornography. They do not however have to control their subscribers or the contents (42 U.S.C. § 227 (3)). With this rule in place, the regulations of 42 U.S.C. § 227 go beyond the regulations that exist in most of the European legal systems.

8 3 Conclusion

Technical solutions and codes of conduct can act as supplements preventing criminal liability. The protection of children against harmful content will be supported by the use of filter software like PiCS, but without safeguarding complete protection. It can nevertheless assist in avoiding conflicts between different legal systems and the problem of distinguishing which content is to be considered pornographic or harmful in different countries. It must be applied cautiously and be carefully balanced with the right of freedom of expression - a basic right in every democracy. Codes of conduct as well as registration offices can help to prevent Internet crime and to support the enactment of legal liability provisions for Internet providers.

The US-legislation as well as the obligations drafted by the South African Film and Publications Bill and the development of codes of conducts will also be supported by the European Union within Article 16 of the E-Commerce

Directive[437].

9 Concluding remarks

The above-mentioned discourses have shown that the Internet is a space where criminal law does indeed apply. Providers and users are exposed to many risks of criminal prosecution.

However, the difficulties which multimedia data transfers open for legislatures are so plentiful and novel that they require an entire set of new rules in many areas of criminal law. Since nations differ in their regulatory commitments, many Internet transmissions and transactions will be subject to inconsistent regulations. And most unilateral national regulations - especially the most demanding and restrictive ones - will affect the regulatory efforts of other nations. These problems will only be solved by the introduction of unambiguous international regulations. The establishment of such rules seems unlikely in the near future, due to the existence of divergent opinions and cultural differences. The European Directive and the Convention on Cybercrime does however seem to be a first step into the right direction.

The norms of criminal liability of Internet providers show different regulatory models in various countries. There are regulations, which overlap. In some legal systems, for example the German legal system, the liability of Internet providers depends on the legal provisions relating to the Internet, combined with general criminal law principles concerning the differentiation

---

[437] Codes of conduct (article 16): Member States and the Commission shall encourage the drawing up of codes of conduct by professional and consumers associations.

between commissions and omissions and guarantors' positions. Generally these regulations often lead to an exclusion of liability for network and access providers, and to a limited liability for service providers if and when they have knowledge of certain unlawful contents. In some countries, stricter liability regulations are in place, for example in the United States.

German law has been developed quite extensively in this regard. In concluding this analysis as far as the liability of Internet providers is concerned, the main rules can be summarised as follows: Firstly, German criminal law is applicable to offences on the Internet, even if they are *abstrakte Gefährdungsdelikte* (abstract strict liability torts), which are typical in the area of the Internet. The *abstrakten Gefährdungsdelikte* do not require that there is harm or a concrete danger to an object for the offence to apply, as the simple act is seen as such a danger that there is no need for a consequence.[438] It is however necessary for the prosecution authorities to show evidence that there is a certain link between the offence and Germany. In addition, the perpetrator must have wanted his act (committed on the Internet) to have an effect on the German public.

Secondly, the service provider cannot be held liable for the commission of an illegal act when he acts as a conduit for the transmittal of data, even if such data is illegal or contains illegal elements. Liability can only be found in the omission of an act, if and when the provider fails to remove or block the illegal content.

Thirdly, the guarantor's duty to prevent the access to data that is punishable under criminal law is only breached if he has actual knowledge of

[438] See chapter 3 1 4 1 and 3 1 4 2.

the data, by controlling his server for example. A guarantor's obligation to prevent the access to such contents can be fulfilled by the refusal to transfer the data.

The service provider is not liable for data, which he transmits or makes accessible if he does not know that the data's content is illegal. When the service provider puts his own illegal contents on the Internet, he is liable on the basis of the same principles, which apply to the content provider.

The content provider of illegal content is liable because of an active commission. This does not differ from offences, which are not committed on the Internet. When the service provider does not place his own contents on the Internet, but transports only foreign data to a third party, an offence, i.e. an omission, can be taken into consideration concerning his criminal liability. Thus the offence is based on the fact that the provider did not prevent the access of a third party to the data.

The privilege offered to service providers in relation to foreign content in terms of section 8 E-TDG[439] must be interpreted restrictively, because it is not intended to benefit the service provider who enables access to foreign contents to the users, if he knows that the content is illegal.

Because of the inherent complications, which arise from the entire theory of provider liability, it would appear advisable to focus on the prosecution of offences committed by content providers (operators of websites) rather than hosts, and on the prosecution of those who knowingly receive or transmit such illegal content.

South Africa's administration of justice also restricts the criminal liability

[439] See chapter 6 2 1.

of Internet service providers. In pursuance of the Electronic Communications and Transactions Act of 2002 Internet service are not held liable for the illegal dissemination of information, if and when the service provider himself did not positively commit an illegal transaction.

Section 73 ECTA is very similar to Article 12 of the E-Commerce Directive[440]. Both provisions exclude liability for service providers who offer mere conduit presupposing that service providers have neither knowledge of nor control over information, which is transmitted or stored by them. Regarding mere conduit, South Africa and Europe's statute laws accordingly are correspondent. According to 47 U.S.C. § 223 (e) (1) an access provider is not liable, if he merely offers access to the Internet. This provision is similar to the sectiond in South African law, the E-Commerce Directive and the E-TDG.

The conditions of privileging the liability for caching in South Africa and in Europe resemble each other to begin with, in particular concerning Article 13 (1) (a) -(d) and 74 (1) (a)-(d). 74 ECTA in (1) (e) lays down however that the service provider is not liable for caching as long as he removes or disables the access to the data he has stored upon receiving a take-down notice. Neither the Directive nor the E-TDG proposed statutory "notice and take-down"- procedures concerning the disabling or removal of access to information. Article 13 (1) (e) of the Directive instead claims for an exclusion of the service provider's liability that he shall act expeditiously to remove or to disable access to the information he has stored as soon as he obtains actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or the access to it has

[440] In Germany section 9 E-TDG (see chapter 6 2 2).

been disabled, or that a court or an administrative authority has ordered such removal or disablement. So basically the facilities for privileging liabilities of Internet service providers regarding their caching are very extensive both in South Africa and in Germany.

However, South Africa's ECTA and Europe's E-Commerce Directive (inclusive of Germany's E-TDG) totally differ as far as the Internet providers´ privileging of criminal liability is concerned. The knowledge requirements in section 75 and in Article 14 E-Commerce Directive are literally identical ("actual knowledge" / "not aware of facts or circumstances"). But section 75 (1) states only the conditions and circumstances under which the service provider is not liable for damages. Article 14 instead also applies to criminal liability. The European provider is only considered criminal liable, if and when he has actual knowledge of the illegality. Thus, the E-Commerce Directive privileges the liability of Internet service provider not only referring to mere conduit and caching, but also to hosting. So Internet service providers are not considered criminal liable as long as they do not obtain actual knowledge or information of illegal activity. The ECTA instead does not provide a privileging of liability of this sort for hosting as regards criminal liability. Hence, South Africa's Internet service provider receive less legal protection than those in Europe.

As shown above, there is a contradiction proposed in the Films and Publications Amendment Bill. The ECT Act excludes strict liability for Internet service provider whilst the Bill establishes - according to the wording just the opposite - a strict liability. Consequently, achieving a consensus of rights turns out to be difficult not only between different nations, but even in one and

the same country.

Besides the illustrated specific statutory solutions, more technical measures have to be taken to prevent a misuse of the Internet. This can be achieved by increasing international co-operation. Furthermore, an international consensus about liability on the Internet and the duty of providers to delete unlawful contents (if they know about it) has to be established. The Pennsylvania Law imposes liability on Internet service providers for child pornography even if the Internet providers are not hosting the offending content. This statute restricts Internet content and sets a dangerous precedent of regulating Internet providers without notice. Directly contacting of the hosting Internet provider about the alleged child pornography would be a less constitutionally damaging alternative.

The Internet provider, in its own interest, must exhaust all possibilities in preventing an abuse of its technical equipment. This way he protects himself from eventual criminal liability and ensures a good reputation. To secure this, voluntary self-censorship or pedagogic measures could be employed, but with care. An extreme censorship is not the answer for a medium such as the Internet. The Internet interprets censorship as a disturbance - and goes around it, says Internet guru John Gilmore.[441] This is not entirely true because governments are not powerless, as this thesis has illustrated.

Access providers of a state, for instance, can be ordered to ensure that certain content does not become accessible. This is possible, for example, by introducing so-called negative lists. Saudi Arabia and China store every single Internet content, control it by means of a negative list and then, finally, decide

[441] Eck & Ruess "Haftungspriviligierung der Provider nach der E-Commerce-Richtlinie" 2003 *MMR* 363-365.

whether or not it may be made accessible to its citizens or not. But such filter software can fail. Another example are web sites with medical content that cannot be written without the use of certain terminology, which can be filtered out as "sexually explicit".

Besides the two incidents described above, the question of who defines what pornographic or violent data mean must be posed. The decision of the German Federal Court of Justice BGH (*Bundesgerichtshof*) of December 2000[442] has led to worldwide outrage and provoked a discussion about who is ruling whom. As the court sentenced the Australian citizen Frederic Töben, who published his contents of hate from Australia around the world in order to infringe German criminal law, the court has, in practical terms, extended German jurisdiction to the whole Internet. Some German web sites surely infringe on Chinese, Saudi-Arabian and Afghani law or morals and Germany would defend them as falling under the right of "freedom of expression" and therefore being not punishable under German law. If every country would attempt to prosecute the owners of websites of other countries it would lead to mere chaos.

It seems to be highly advisable to find common standards of values between as many countries as possible and not to immediately ask for censorship and punishment. The United States for example vehemently opposed the hate speech provision in the Additional Protocol to the Convention on Cybercrime[443], because it abridges the First Amendment[444]. The Amendment protects hate speech, notwithstanding a few narrow

[442] See chapter 3 1 3 3 (*Töben* -case).
[443] See chapter 7 3 2.
[444] Declan McCullagh, U.S. Won't Support Net "Hate Speech" Ban, CNET News.com, Nov. 15, 2002; at www.news.com/2100-1023-965983.html (declaring that the United States cannot be party to any treaty that abridges the U.S. constitution).

exceptions that allow the Government to ban speech which would constitute a breach of the peace or speech directed at an individual intended to "provoke imminent lawless conduct"). It is interesting that the American Jewish Committee has taken the view against censorship of hatred web sites on the Internet because thus certain activities can be monitored more closely. The gap between the freedom of Internet communication and the difficulties in censoring certain data can provide a chance. It will create open-minded discussions and protects one of mankind's most important basic rights: freedom of expression. And it should not be forgotten that free communication is the enemy of any undemocratic ideology.

Another problem, which must be combated by worldwide consensus, is child pornography. It is suggested that a universal child pornography law should be developed.

Legislators and governments worldwide must be careful not to become the "Big Brother" predicted by George Orwell in his anti-utopia of 1984. In particular the terrorist attacks of September 11, 2001 may lead to the creation of a "Big Brother" on the Internet by the enactment of various new acts and provisions which set up a "transparent user" and make Internet providers the "sleuths" of governmental authorities. The journalist organization reporters without frontiers (*Reporter ohne Grenzen*) criticized an increasing worldwide control of the rights of Internet users, website providers and online journalists on the Internet since September 11, 2001, even in democracies.[445] The situation in many underdeveloped countries, however, is by far worse. In China and Vietnam certain Internet data are being filtered out as

[445] www.internet.rsf.org, June 23, 2004.

"disagreeable" information. In China more than 60 persons have been arrested because of distributing "subversive contents" on the Internet, thus "undermining the supreme power".[446]

The development of a more satisfactory method of fighting cybercrime will take a long time, and Internet providers will have to play a key role in fighting computer-related crime. The Cybercrime Convention with its 45 member states agreed after all on a minimum of standards for fighting against criminal Internet activities. Time will tell if it turns out to be "a ground-breaking agreement".[447]

When we consider the laborious attempts to establish common regulations for, say, environmental protection at an international level, it becomes clear just how tedious a similar process will be in the area of the Internet. Nevertheless, law and jurisdiction will expand as the Internet expands. The above statements show that despite the multitude of unresolved points at issue, the Internet is not an unprotected area. Looking at the past it becomes clear how the law has had to evolve while technology was developing. The technological progress of the 19th and 20th centuries led to new challenges for the jurisprudence of all time. Technical innovations offer an opportunity for the individual and for society as a whole. Simultaneously however, it is in the nature of such innovations that the risks for the individual and his protected interests increase.

---

[446] www.ifex.org; ww.heise.de/newsticker/meldung.
[447] Walter Schwimmer, Secretary General of the Council of Europe, dpa March 18, 2004.

References

Books

Barton, Prof. Dr. Dirk *Multimedia-Strafrecht* 2001 Neuwied.

Bleisteiner, Stephan *Rechtliche Verantwortung im Internet* Köln-Berlin-Bonn-München 1999.

Börner, Fritjof *Der Internet Rechtsberater* Köln 1999.

Bremer, Karsten *Strafbare Internet-Inhalte in internationaler Hinsicht* Frankfurt/Main 2001.

Brießmann, Erwin *Strafrecht und Strafprozeßrecht* 6th edition 1991.

Burkert, Herbert "Privacy-Data Protection" in Engel, Christoph & Keller, Kenneth H. (editors) *Governance of Global Networks in the Light of Differing Local Values* Christoph Baden-Baden 2000.

Dreher, Eduard & Tröndle, Herbert *Strafgesetzbuch und Nebengesetze Kommentar* 47th edition München 1995.

Dreher, Eduard & Fischer, Thomas *Strafgesetzbuch und Nebengesetze Kommentar* 50th edition München 2001.

Duden, Konrad *Das große Wörterbuch der deutschen Sprache* Mannheim 1978.

Edwards, Lilian & Waelde, Charlotte *Law and the Internet-Regulating Cyberspace* Oxford 1997.

Finke, Thorsten *Die strafrechtliche Verantwortung von Internet-Providern* Tübingen 1998.

Foster, Nigel *German legal system & laws* 2nd edition London 1996.

Haft, Fritjof *Strafrecht Allgemeiner Teil* 2nd edition München 1984.

Harris, David J *Cases and Material on International law* 5th edition London 1998.

Hailsham, Lord *Halsbury's Law of England*, 4th ed., Vol. 11 (1) London 1990.

Härting, Nico *Internetrecht* Köln 1999.

Hofman, Julien *Cyberlaw* Cape Town 1999.

Hohloch, Gerhard *Recht und Internet* Baden-Baden 2001.

Hoofacker, Gabriele *Online und Telekommunikation von A-Z* Reinbek bei Hamburg 1995.

Jarass, Hans & Pieroth, Bodo *Grundgesetz für die Bundesrepublik Deutschland Kommentar* 5th edition München 2000.

Kalmring, Dirk *Internet für Wirtschaftswissenschaftler* 2nd edition Köln 1996.

Kaufmann, Hans *Creifelds Rechtswörterbuch* 14th edition München 1997.

Kleinknecht, Theodor & Meyer-Goßner, Lutz *Strafprozeßordnung Kommentar* 45th edition München 2001.

Koch, Frank *Internetrecht* München-Wien 1998.

Kröger, Detlef & Gimmy, Marc A. *Handbuch zum Internetrecht* Berlin-Heidelberg-New York 2000.

Kuner, Christopher *Internet für Juristen* München 1999.

Lackner, Karl & Kühl, Kristian *Strafgesetzbuch Kommentar mit Erläuterungen 23th edition* München 1999.

Lohse, Wolfram *Verantwortlichkeit im Internet* Münster-Hamburg-London 2000.

Lloyd, Jan J. *Information Technology Law* 2nd edition London 1997.

Miesbach, Dr. Klaus & Sander, Dr. Günther *Münchner Kommentar zum Strafgesetzbuch* München 2003.

Oehler, Dietrich *Internationales Strafrecht* 2nd edition Köln 1987.

Orwell, George *Nineteen Eighty-Four* London 1949.

Oxman, Bernhard *Jurisdiction of States* in Bernhard, Rudolf (ed) *Encyclopeadia of Public International Law* London 1987 277 (282).

Piette-Coudol, Thierry & Bertrand, Andre *Internet et la Loi* Dalloz Paris 1997.

Rehmann, Wolfgang *Arzneimittelgesetz Kommentar* 2nd edition München 2003.

Ritz, Dorothee *Inhalteverantwortlichkeit von Online-Diensten* Frankfurt am Main 1998.

Rockey, Nick *The e-Commerce Handbook 2000* Cape Town 2000.

Rowland, Diane & MacDonald, Elizabeth *Information and Technology law* London 1997.

Scheffler, Heuke in Kilian, Wolfgang & Heussen, Benno (ed.) *Computerrechtshandbuch* München 2002.
Schönke, Adolf & Schröder, Horst *Strafgesetzbuch Kommentar* 26th edition München 2001.

Schönke, Adolf & Schröder, Horst *Strafgesetzbuch Kommentar* 28th edition München 2002.

Schwarz, Mathias *Merkmale, Entwicklungstendenzen und Problemstellungen des Internet* in: Prinz, Matthias & Peters, Butz: *Medienrecht im Wandel* Festschrift für Manfred Engelschall Baden-Baden 1996.

Smith, Graham *Internet law and regulation* 2nd edition London 1999.

Spindler, Gerald *Vertragsrecht der Internet-Provider* Köln 2000.

Strömer, Tobias *Online-Recht* Heidelberg 1997; 2nd edition Heidelberg 2002.

Wandtke, Arthur-Axel & Bullinger, Winfried *Ergänzungsband zum Praxiskommentar Urheberrecht* München 2003.

Wessels, Johannes *Strafrecht Allgemeiner Teil* 30th edition Heidelberg 2001; *Strafrecht Besonderer Teil 2*, 22th edition Heidelberg 1999.

Wong, Christoffer *Criminal Jurisdiction over Internet Crimes* in Holoch, Gerhard (editor) *Recht und Internet* Baden Baden 2001.

Articles/Journals:

Altenhain, Karsten "Die strafrechtliche Verantwortung für die Verbreitung mißbilligter Inhalte in Computernetze" 1997 *Computerrecht* 487.

Beisel, Daniel & Heinrich, Bernd "Die Zulässigkeit der Indizierung von Internet-Angeboten und ihre strafrechtliche Bedeutung" 1997 *Computerrecht* 360-362.

Bortloff, Niels "Die Verantwortlichkeit von Online-Diensten" 1997 *Gewerblicher Rechtsschutz und Urheberrecht* 387; "Neue Urteile in Europa betreffend die Frage der Verantwortlichkeit von Online-Diensten" 1997 *Zeitschrift für Urheber und Medienrecht* 167 (170).

Breuer, Barbara "Anwendbarkeit des deutschen Strafrechts auf exterritoriale Internet-Benutzer" 1999 *MultiMedia und Recht* 141.

Collardin, Marcus "Straftaten im Internet" 1995 *Computerrecht* 621.

Conradi, Ulrich & Schlömer, Uwe "Die Strafbarkeit der Internetprovider" 1996 *Neue Zeitschrift für Strafrecht* 1996, 368-369.

Cornils, Karin "Der Begehungsort von Äußerungsdelikten im Internet" 1999 *Juristenzeitung* 394-397.

Dannecker, Gerhard "Neuere Entwicklungen im Bereich der Computerkriminalität" 1996 *Betriebs-Berater* 1285-1288.

Decker, Ute "Haftung für Urheberrechtsverletzungen im Internet" 1999 *MultiMedia und Recht* 7.

Derksen, Roland "Strafrechtliche Verantwortung für die in internationalen Computernetzen verbreiteten Daten mit strafbarem Inhalt" 1997 *Neue Juristische Wochenschrift* 1878 (1881).

Eck, Stefan & Ruess, Peter "Haftungspriviligierung der Provider nach der E-Commerce-Richtline" 2003 *MMR* 363-366.

Flechsig, Norbert "Haftung von Online-Dienstanbietern im Internet" 1996 *Zeitschrift für Medien-und Kommunikationsrecht* 333-335.

Freytag, Stefan "Providerhaftung im Binnenmarkt" 2000 *Computer und Recht* 602.

Geis, Ivo "Die Europäische Perspektive der Haftung von Informationsanbietern und Zertifizierungsstellen" 1999 *Computerrecht* 772-774.

Gewessler, Roland "Das neue US-Telekommmunikationsgesetz" 1986 *CR* 626-632.

Haft, Dr. Fritjof "Rechtsfragen des Datenverkehrs im Internet" 2001 *Juristische Schulung* 115.

Hilgendorf, Eric "Grundfälle zum Computerstrafrecht" 1996 *Juristische Schulung* 511; 1997 *Juristische Schulung* 323 (327); "Überlegungen zur strafrechtlichen Interpretation des Ubiquitätsprinzips" 1997 *Neue Juristische Wochenschrift* 1876-1877.

Hoeren, Thomas "Das Internet für Juristen - eine Einführung" 2000 *Neue Juristische Wochenschrift* 3295.

Jäger, Ulrike & Colardin, Marcus "Die Inhalteverantwortlichkeit von Online-Diensten" 1996 *Computerrecht* 238.

Koch, Frank "Zivilrechtliche Anbieterhaftung für Inhalte in Kommunikationsnetzen" 1997 *Computerrecht* 193.

Kohl, Uta "Eggs, Jurisdiction and the Internet" 2002 *International & Comparative Law Quarterly* 579.

Kreutzer, Till "Filesharing von Musik-Stücken und deutsches Urheberrecht" 2001 *Der iT-Rechtsberater)* 136.
Kuner, Christopher "Internationale Zuständigkeitskonflikte im Internet" 1995 *Computerrecht* 453-455.

Kuning, Prof. Dr. Philipp "Die Lotus-Entscheidung" *Jura* 1994, 186 (187).

Ladeur, Karl-Heinz "Regulierung des Information Superhighway" 1996 *Computerrecht* 614.

Landfermann, Hans-Georg "Der Richtlinienvorschlag Elektronischer Geschäftsverkehr - Ziele und Probleme" 1999 Zeitschrift für Urheber und Medienrecht 795.

Leupold, Andreas, Bachmann, Peter & Pelz, Christian "Zulässigkeit von Glücksspielen im Internet" 2000 *Zeitschrift für Urheber und Medienrecht* 648-651.

Liesching, Marc "Verantwortlichkeit von Internet-Cafe-Betreibern-Besonderheiten bei pornographischen oder sonstigen jugendgefährdenden Inhalten" 2000 *MultiMedia und Recht* 261-263.

Maiwald, Manfred "Grundlagenprobleme der Unterlassungsdelikte" 1981 *Juristische Schulung* 473-476.

Mayer, Franz C. "Recht und Cyberspace" 1996 *Neue Juristische Wochenschrift* 1782.

Mayer-Schönberger, Viktor & Schmölzer, Gabriele "Das Telekommunikationsgesetz 1997-ausgewählte rechtliche Probleme" 1998 *Österreichische Juristen Zeitung* 378.

Pelz, Christian "Die strafrechtliche Verantwortlichkeit von Internet-Providern" 1998 *Zeitschrift für Urheber und Medienrecht* 530-533.

Pichler, Rufus "Haftung des Host Providers für Persönlichkeitsrechtsverletzungen vor und nach dem Teledienstgesetz" 1998 *MultiMedia und Recht* 79-80.

Ringel, Kurt "Rechtsextremistische Propaganda aus dem Internet" 1997 *Computerrecht* 302-303.

Schmitz. Dr. Peter "Datenschutz in der Informationsgesellschaft - gelten die Grundrechte, das Volkszählungsurteil und die Datenschutzgesetze noch?" 2003 *MultiMedia und Recht* editorial.

Sieber, Ulrich "Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Computernetzen" 1996 *Juristen Zeitung* 494-496.; "Zur Umsetzung von 5 TDG am Beispiel der Newsgroups im Internet" 1997 *Computer und Recht* 669; "Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen" 1997 *Computerrecht* 581 (598); "Verantwortlichkeit von Internetprovidern im Rechtsvergleich" 1999 *Zeitschrift*

für Urheber und Medienrecht 198.

Spindler, Gerald "Deliktsrechtliche Haftung im Internet - nationale und internationale Rechtsprobleme" 1996 *Zeitschrift für Urheber und Medienrecht* 541; "Haftungsrechtliche Grundprobleme der neuen Medien" 1997 *Neue Juristische Wochenschrift* 3193; "Verantwortlichkeit von Dienstanbietern nach dem Vorschlag einer E-Commerce-Richtlinie" 1999 *MultiMedia und Recht* 199-203.

Vassilaki, Irini E. "Strafrechtliche Verantwortlichkeit der Dienstanbieter nach dem Teledienstgesetz" 1998 *MultiMedia und Recht* 630.

Visser, Prof. Coenraad "South Africa:New Liability Regime for ISPs" 2003 *Computer Law Review International* issue 3, 94.

Waldenberg, Arthur "Teledienste, Mediendienste und die Verantwortlichkeit ihrer Anbieter" 1998 *MultiMedia und Recht* 124.

Weides, Peter "Der Jugendschutz im Filmbereich" 1987 *Neue Juristische Wochenschrift* 224-226.

Winkelbauer, Wolfgang "Computerkriminalität und Strafrecht" 1985 *Computerrecht* 40-45.

Wöbke, Jörn "Meinungsfreiheit im Internet" 1997 *Computerrecht* 313-315.

Newspaper Articles

ComputerBild Hamburg/Germany 1998, 34-40.

Der Spiegel Hamburg/Germany 23.9.1996, 124.

Der Tagesspiegel Berlin/Germany 27.6.2003, 29.

Frankfurter Allgemeine Zeitung Frankfurt/Germany 30.12.1995, 14.

Stern Hamburg/Germany 20.9.2001, 60.

Süddeutsche Zeitung München/Germany 20.5.2000, 6.

Zeit Hamburg/Germany 26.3.1998.

Table of Cases

AG München 8340 Ds 465 Js 173158/95.

AG Berlin Tiergarten 260 Ds 857/96.

BayObLG - 5 StR 122/00.

BayObLG – 5 4 StR 232/97.

BGH – StR – 1 StR 184/00.

BGH - 1 StR 181/00.

BGH – 1 StR 66/01.

BGH – 1 ZR 118/96.

BGHSt 3, 203.

BGHSt 11, 282, 284.

BGHSt 18, 63.

BGHSt 27, 30.

BGHSt 34, 98, 219.

BGHSt 13, 57.

BVerfGE 71, 108, 115.

BVerfGE 83, 130, 138f.

LG München 312 O 85/98.

Ashcroft v. ACLU – 122 S. Ct. 1700 (2000).

CompuServe, Inc. v. Patterson, Case no. C2/94/91 v. 11.8.1994 (S.D.Ohio).

France v. Turkey (1927) PCIJ Reports Series A No. 10.

Gerwhwin Publishing Corp. V. Columbia Artist Management 443 F. 2d 1159, 1162, 1163 (2d Cir. 1971).

Kenneth M. Zeran v. American Online, Inc., 958 F.Supp. 1124 (E.D. Va. 1997) aff'd. U.S. Ct. of Appeals 4th Circuit, No. 97-1523 of November 12, 1997.

Leiber v. Consumer Empowerment BV, No. 01-09923-SVW (C.D. Cal. 2003).

Metro-Goldwyn-Mayer Studios, Inc., v. Grokster Ltd., 2003 U.S.Dist. 6994 (C.D. Cal. 2003).

North Central Local Council and South Central Local Council v. Roundabout Outdoor (Pty) Ltd and Others 2002 (2) SA 645 (D).

Pres-Kap, Inc. v. System One Direct Access, Inc., 636 so. 2d 1351 (Fla. App. Ct. 1994).

Religious Technology Center, et a. v. Netcom On-Line Communications services, Inc, et al., 907 F. Supp. 1361 (N.D.Cal. 1995).

Sega Enterprises Ltd., et al. v. Maphia, et al., 857 F.Supp. 679 (ND.Cal. 1994).

Sony Corp. Of America v. Universal City Studios, Inc., 4 64 U.S. 417 , 104 S.Ct. 774 C (1984).

Stratton Oakmont, Inc., et al. v. Prodigy Services Co, et al., 1995 WL 323710 (Trial/IASs pt.34 Nassau County, N.Y. Sup. Ct. 1995) (No. 31063/94).

United States of America v. Robert Allen Thomas and Carleen Thomas, 74 F. 3d 701 (6Th Cir. 1996).

Yahoo!, Inc. v. La Ligue Contre Le Racisme at L'Antisemitisme, 169 F.Supp. 2d 1181 (ND Cal. 2001)