THE CRIMINAL RESPONSIBILITY OF INTERNET SERVICE PROVIDERS IN GERMANY

Dr. Dieter Dörr[*] *& Steffen Janich*

INTRODUCTION

In the area of cyber crime we are often confronted with the problem that an effective prosecution of the actual offender is difficult, if not impossible. This problem is mostly connected to the anonymity and globality of communication on the internet. Not only in the case of public internet terminals or the use of unprotected wireless networks is the tracing of delinquents problematic, but anonymization services such as AnOn severely increase the difficulty as well. Even the use of e-mail addresses, where no registration is required or the provider does not verify the registration data, can prevent the prosecution of offenses committed while using the e-mail address.

These difficulties have raised the question: to what extent is the information and communication industry responsible for offenses committed by third persons abusing the infrastructure of the internet? This question is of utmost importance for the internet economy. A responsibility for criminal content on the internet would bring about severe punishment for internet providers. A few years ago, the actions of the German judiciary against several internet providers—mainly against CompuServe Germany[1]—caused a worldwide disturbance[2] and the removal of servers from Germany to other countries. The CompuServe proceedings will be discussed later in more detail.

---

[*] Chair in Public Law, International and European Law, Media Law, Director of the Mainz Media Institute.

[1] Amtsgericht München, Multimedia und Recht [Local Court of Munich] 1998, 429.

[2] *See* Seiber, Multimedia und Recht 1998, 429 (438) (concerning the criticism by the German and the international press).

This question about the responsibility of the information and communication industry for offenses committed by third parties raises numerous legal problems, which are closely connected to the complex technical architecture of the internet. Several persons, or rather companies, are involved when someone is accessing criminally relevant content. For instance, the download of child pornography from an internet page not only involves the actual provider of the content and the user, but also the host provider, who supplies the webspace for the content, and the access provider of the user. Without the participation of these providers, most of the offenses could not be committed. On the other hand, these providers are often not capable of preventing criminal activity. And even if prevention would be theoretically possible, we would have to ask whether an intervention of the providers would be reasonable, considering the immense amount of data. Regarding this, the ongoing development in the area of technical controlling possiblities, which enables providers to monitor and trace activities on the internet without requiring massive amounts of human resources, leads to a strong dynamic in the legal policy discussion. Currently in Germany there is a debate mostly about an obligation to prevent access to child pornographic[3] and terrorist[4] content by blocking or deleting the pages.

But before this article covers these concrete responsibility questions, the next section discusses a few general aspects of German internet regulation.

TELEMEDIA REGULATION IN GERMANY: A MIXED SYSTEM

First, it is important to know that the German legislature uses the term telemedia for all electronic information and communication services.[5] Thus, most of the offers on the

---

[3] *See* Von Christian Stöcker, *Von der Leyen lässt Kinderpornographie aus dem Netz filtern*, SPIEGEL ONLINE, Jan. 15, 2009, http://www.spiegel.de/netzwelt/web/0,1518,601517,00.html (discussing the plans of the Federal Ministry for Family, Seniors, Women and Youth to prevent access to child pornographic content).

[4] *See* Ingrid Melander, *Web Search for Bomb Recipes Should be Blocked: EU*, REUTERS, Sept. 10, 2007, http://www.reuters.com/article/2007/09/10/us-eu-bombs-internet-idUSL1055133420070910.

[5] *Compare* § 1 Abs. 1, 1 Telemediengesetz, *with* § 2 Abs. 1, 3 Rundfunkstaatsvertrag.

internet, such as webshops, online auction services, search engines, podcasts, chatrooms and web portals, are included in this definition. Even private websites or blogs are considered telemedia. Only selected telecommunication services and radio broadcasting are an exception to this. For example, internet telephone and internet radio are not considered telemedia.[6]

Telemedia in Germany is not regulated by a single law, but through a mixed system of regulations.[7] This mixed regulation is mostly a result of a dispute between the federal government and the federal state governments about regulation competence regarding telemedia. Thus, today we find legal specifications in the "Rundfunkstaatsvertrag" ("RStV") and in the Federal Telemedia Act ("TMG"). There has been a compromise, according to which the federal government is responsible for the economic part of telemedia, while the federal states cover all aspects regarding the content in a special section of the RStV, namely the paragraphs following paragraph 54.[8] These regulations also address such telemedia services which are concerned with journalistic and editorial work and specify restrictions for the content of these services. At the core of this are regulations concerning compliance with journalistic principles, certain information responsibilities, and a demand for counterstatements, as well as specific data protection regulations and instructions for advertisement. On the other hand, the federal government set down regulations when it issued the "German Telemedia Act" on March 1, 2007. The Telemedia Act replaced the "Teledienstegesetz" ("Teleservice Law") and the "Teledienstedatenschutzgesetz" ("Teleservice Data Protection Law"), thus unifying these separate regulations. Central to the Telemedia Act are, along with a universal right of access and the country of origin principle, instructions for transparency, as well as area-specific data protection rules. But most of all, the Telemedia Act

---

[6] *See* MARCO GERCKE & PHILLIP W. BRUNST, PRAXISHANDBUCH INTERNETSTRAFRECHT [PRACTICE MANUAL OF INTERNET CRIMINAL LAW] pt. 565 (2009); PETER SCHMITZ, § 1 Telemediengesetz 8, *in* GERALD SPINDLER & FABIAN SCHUSTER, RECHT DER ELEKTRONISCHEN MEDIEN (2008).

[7] DIETER DOERR & ROLF SCHWARTMANN, MEDIENRECHT pt. 271 (2008).

[8] *See id.* at 272; GERCKE & BRUNST, *supra* note 6, at 566; PETER SCHMITZ, § 1 Telemediengesetz 3, *in* SPINDLER & SCHUSTER, *supra* note 6.

regulates, in the paragraphs 7 to 10, the responsibilities of telemedia providers for their content, which is the topic of this article. First, this article will discuss the origin of these responsibility regulations.

DEVELOPMENT OF REGULATIONS FOR RESPONSIBILITY

In the course of the rising importance of the internet in regards to daily communication in the middle of the 1990s, criminal prosecution authorities were increasingly faced with the phenomenon of data network criminality.[9] In particular, this involved the exchange of pornographic and child pornographic pictures via the internet. Due to the lack of specialized legal regulations, the investigation authorities and especially the courts, were in charge of developing limiting criteria to prevent penal responsibilities from escalating out of control.

As I mentioned at the beginning of this article, the fact that the Munich prosecutors' office commenced a preliminary investigation against the director of the access provider CompuServe in 1996 for assisting in the spread of pornographic material, led to worldwide criticism and caused the legislature to create specialized regulations for the responsibilities of service providers in 1997.[10] The teleservice law and the media services state contract were thus rather early in comparison to an international level. In doing so, the German legislature was guided by the results of a commission of experts, which was working on the basic principles of a standardized responsibility regulation on an EU-level. These propositions were planning a graded responsibility, which the German legislature adopted, anticipating the EU-regulation.

---

[9] *See* STEPHAN ACKERMANN, AUSGEWÄHLTE PROBLEME DER MAILBOX-KOMMUNIKATION (1994); ULRICH SIEBER, THE INTERNATIONAL EMERGENCE OF CRIMINAL INFORMATION LAW (1992); Tonio Walter, NSTZ 1990, 523.

[10] *See* The Elucidation in the Bill, Bundestag Drucksache. 13/7385, p.16 (Printed Matter of the Federal Parliament) (concerning the history of the TDG 1997).

Then, in 2000, the directive on electronic commerce[11] was passed. And despite the economic focus of the directive, the responsibility regulations also contained penal issues.

In regards to the development of media regulation, the federal government and the federal states agreed on a restructuring of the legal principles. The split codification of the responsibility regulations was supposed to be resolved with the aforementioned German Telemedia Act. Ignoring claims for amendment and specification,[12] regulations regarding responsibility were transferred from the teleservices law without any changes.[13]

AIM AND CLASSIFICATION OF RESPONSIBILITY REGULATIONS

The aim of the regulations derives itself from the field of problems mentioned at the beginning of this article. If the providers of online services are held responsible, we face the danger of escalating liability. Contrary to that, the operation and use of modern communication media should not lead to unforeseeable legal risks. That would be detrimental not only to the individual person, but also to the international competitiveness of Germany. Thus, the legislature has stated liability priviliges for service providers.

In doing so, a distinction between civil law, public law, and penal law was omitted. Paragraphs 7 to 10 of the Telemedia Act apply to all fields of law. This led to an extensive debate in jurisdiction and science as to how these limitations of liability are to be dogmatically classified.[14] The dominant opinion in science is that the privilege has to be seen as a sort of filter

---

[11] Directive of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, 2000, 2000/31.

[12] *See, e.g.*, the statement of *BITKOM e.V.* on the bill for unification of rules on certain electronic information and communication services (Elektronischer-Geschäftsverkehr-Vereinheitlichkeitsgesetz [EIGVG], Aug. 18, 2006, p. 7); the statement of *eco – Verband der Deutschen Internetwirtschaft e.V.* on the questionnaire of the Federal Ministry of Economics and Technology on the regulation of the provider's responsibility ([TMG], Dec. 10, 2007, p. 2).

[13] *See* BT-Drs. 16/3078, p. 15 (Printed Matter of the Federal Parliament).

[14] *See generally* ULRICH SIEBER, VERANTWORTLICHKEIT IM INTERNET [ACCOUNTABILITY ON THE INTERNET] 114 (C.H. Beck Verlag ed. 1999).

encompassing all fields of law, which has to be considered before either the civil law basis of claim, the public law basis of intervention, or even before the examination of a criminal offense.[15] This is what the legislature had in mind when introducing the liability privilege.[16]

Now that we have covered the basic information about German provider responsibility, let us consider the actual liability privileges in detail.

THE GRADED LIABILITY SYSTEM

The Telemedia Act separates between the functions of service providers and supplies a graded system of responsibility. Without using the now familiar English terms, it distinguishes between content providers, access providers, proxy-cache providers, and hosting providers.

Hosting providers provide storage and access to third party content through their own computer system—the so-called server. For the user to access the internet, he requires an access provider, which transfers the information to the user. Given that the transmission distance to the user is often very long, the proxy-cache provider supplies intermediate storage in order to speed up the transmission of frequently accessed content. Those at last who offer their own data via their own computer or the server of the hosting provider, are called the content provider.[17]

Regarding the question of responsibility, the Telemedia Act makes a basic distinction between providing one's own content or the content of someone else.

LIABILITY FOR ONE'S OWN CONTENT

There are no exceptions for the liability of persons who provide their own content, be it on their own computer or the

---

[15] Bundesgerichtshof [BGH] [Federal Court of Justice], 2004, 166 [MMR]; Gustav Altenhain, Archiv für Presserecht [AfP] [Archive for Press Law] 1998, 457; Stefan Engel-Flechsig, Frithjof A. Maenne & Alexander Tettenborn, NJW 1997, 2981 (2984); Moritz, CR 1998, 500; Sieber, CR 1997, 581.

[16] *See* BT-Drs. 14/6098, p. 23 (Printed Matter of the Federal Parliament).

[17] *See generally* SIEBER, *supra* note 14, at 10 (regarding the function-specific differentiation and the basics of network technology).

server of someone else. The content provider is thus completely liable according to the general rules. Whether he has copy or utilization rights is irrelevant.[18] As an example, someone who provides pornographic material without access control, and thus enables minors to access it, makes himself liable to prosecution.[19]

A liability privilege in the sense of the Telemedia Act therefore always requires external content. But this raises the question: how do we define one's own and someone else's content? Connected to this, the CompuServe decisions in 1999 and 2000[20] attracted a lot of attention in Germany. The question there was, whether the director of a German company (CompuServe GmbH Deutschland), which provided access to the internet and child pornography forums through the network of the U.S. parent company (CompuServe USA), could be penally charged or not. The responsible district court of Munich was apparently motivated by the hope of creating a penal internet control on an international level, based on the German penal law.[21] The result was a severe prison sentence for the director of CompuServe Deutschland, even though there had been no possibility for him to influence the content of the service provided by the parent company. The subsidiary company in Germany only granted access to data available through the service of CompuServe USA. Yet the district court held the opinion that one could not talk about external content, seeing how CompuServe Deutschland is completely controlled by the American parent company. Therefore the liability privilege, which was still placed in paragraph 5, clause 3 of the Tele Services Act back then, was not applied to the case. What the district court did not acknowledge was the fact that when answering the question about the origin of content provided, one cannot rely on the organizational structure of a company. If a provider simply connects to an external network, the

---

[18] Koch, CR 1997, 193 (197); Spindler, NJW 1997, 3193 (3196); Pelz, ZUM 98, 530 (532).

[19] Bundesgerichtshof [BGH] [Federal Court of Justice], 2001, 596 [NStZ]; TATJANA HÖRNLE, § 184, pt. 45, *in* MÜNCHENER KOMMENTAR ZUM STRAFGESETZBUCH [MUNICH COMMENTARY ON THE CRIMINAL CODE] (2005).

[20] *See supra* note 9.

[21] *See* Kühne, NJW 2000, 1003 (1004).

information available there is external content, even if the connection is established by a subsidiary company.[22] A similar point of view was adopted by the regional court of Munich, which cleared the director of all charges.

As shown by this case, the separation between one's own content and external content is frequently causing problems. These difficulties are enhanced when one turns external content into one's own content.[23] How this happens is a point of debate as well. Usually this has been tied to the press law liability, making use of the externally visible attitude of the service provider regarding the content.[24] But this transfer from the press law is not correct in its generality. A provider of child pornographic material cannot free himself from penal liability by stating his disapproval and refusing to take responsibility for the pictures. Externally visible attitudes toward the content are thus only exclusively relevant as criteria of classification in regards to a statement of fact or opinion, but not in regards to child pornography or copyright infringement. To determine whether a provider has adopted content as his own requires a general examination of the individual case. One can assume internal content if the data has been knowingly selected or transferred, or if someone identifies with the content in a way which an objective observer would assume that the provider wishes to take responsibility for the content.[25] Thus, a service provider adopts unchanged external content if he examines the content in an editorial process—for example, moderation in a news group—or if he issues a universal acceptance of responsibility. But the knowledge that a certain file is on one's server is not sufficient.[26]

Whether providing a link constitutes one's own content is a heavily debated question as well. To some extent, links are

---

[22] *See* Kühne, NJW 1999, 188 (189); Sieber, MMR 1998, 429 (439).

[23] *See* BT-Drs. 13/7385, p. 19 n.23 (Printed Matter of the Federal Parliament).

[24] *See, e.g.,* Eichler, K&R 1998, 412 (414); Koch, CR 1997, 193 (197); Pelz, ZUM 1998, 530 (532); Pilcher, MMR 1998, 79 (86); Spinler, NJW 1997, 3193 (3196); Vassilaki, MMR 1998, 630 (633).

[25] *See* SIEBER, *supra* note 14, at pt. 294.

[26] THEODOR LENCKNER ET AL., § 184 pt. 58, *in* ADOLPH SCHÖNKE & HORST SCHRÖDER, KOMMENTAR ZUM STRAFGESETZBUCH [COMMENT ON THE PENAL CODE] (2006); HÖRNLE, *supra* note 19, at pt. 47.

only considered a mediation of access to external content.[27] Other authors propose an unlimited liability.[28] But in this case as well, a distinguishing solution on an indivual basis is most convincing.[29] Someone who agrees to the provided content in his own words adopts it as his or her own.[30] Incidentally, the number of links and the amount of data they relate to are relevant as well. Universal references to a large amount of data or documents can hardly be seen as an adoption of content. A different point of view is required for links to clearly arranged summaries, or so-called jump labels, automatically linking to a certain part of a larger page.[31] If there are further links on the referenced page, the liability never extends to this second level.[32] Also, the referenced page is only examined at the moment the link has been placed, and there is no obligation to recheck already placed links.[33] If the person who placed the link has to accept the content as his own, he is—most of the time—not to be considered the offender; rather he should be punished for assistance, as he does not control the content or continuance of the referenced page.[34]

---

[27] Koch, *supra* note 24, at 198; LENCKNER ET AL., *supra* note 26, at pt. 66.

[28] DIRK-MICHAEL BARTON, MULTIMEDIA-STRAFRECHT 357 [MULTIMEDIA-CRIMINAL] (1999); LACKNER ET AL., KOMMENTAR ZUM STRAFGESETZBUCH § 184 pt. 7b (2007).

[29] Engel-Flechsig, Maennel & Tettenborn, *supra* note 15, at 2985; Engels & Köster, MMR 1999, 522 (523); Gehrke, ZUM 2001, 34 (39); Haft & Eisele, JuS 2001, 112 (117); HÖRNLE, *supra* note 19, at pt. 47; Kloos, CR 1999, 46 (47); Köster & v. Bonin, ZUM 1997, 821 (824); SIEBER, *supra* note 14, at pt. 307; Spindler, NJW 1997, 3193 (3198); Spindler, CR 1998, 745 (752); Vassilaki, MMR 1998, 630 (636); Vassilaki, CR 1999, 85; Gehrke, ZUM 2001, 34 (39).

[30] Engel-Flechsig, Maennel & Tettenborn, *supra* note 15, at 2985; OLIVER BOESE, STRAFRECHTLICHE VERANTWORTLICHKEIT FÜR VERWEISUNGEN DURCH LINKS IM INTERNET [CRIMINAL RESPONSIBILITY FOR BEING MADE THROUGH LINKS ON THE INTERNET] 88 (2000); SIEBER, *supra* note 14, at pt. 309.

[31] SIEBER, *supra* note 14, at pt. 308.

[32] Flechsig & Gabel, CR 1998, 351 (356); Löhnig, JR 1997, 496 (498); Park, GA 2001, 23 (32); Gehrke, ZUM 2001, 34 (39); Spindler, MMR 2002, 495 (503); SIEBER, *supra* note 14, at pt. 308. *Contra* Lackner & Kühl, pt. 7b.

[33] Berlin-Tiergarten [AG Berlin] [Criminal Court of First Instance in Berlin] June 30, 1997, 260 DS 857/96, CR 1998, 111; Lübeck, Nov. 24, 1998, 11 S 4/98, CR 1999, 650; Haft & Eisele, JuS 2001, 112 (117); Gehrke, ZUM 2001, 34 (39); SIEBER, *supra* note 14, at pt. 313. *Contra* Löhnig, JR 1997, 496 (498); Müglich, CR 2002, 583 (591).

[34] Löhnig, JR 1997, 496 (497); Vassilaki, MMR 1998, 630 (636); Vassilaki, CR 1999, 85 (87); Flechsig & Gabel, CR 1998, 351 (356). *Contra* Koch, MMR 1999, 704 (708); BOESE, *supra* note 30, at 127.

Thus, as an intermediate result, the question of whether it is one's own content, or external content, is relevant for a service provider's penal liability, even if it is not always easy to answer. Only in the latter case can we consider a liability privilege.

LIABILITY FOR EXTERNAL CONTENT

Between the providers of external content then, the German legislator provides us with further categories.

Access Provider

One who limits himself to transmit information or provide access to the usage of information will not be followed up by prosecution.[35] Thus, the Telemedia Act excludes access providers from any kind of liability. An example of an access provider would be telecommunication companies who provide internet access via telephone lines to their customers. But the exemption from liability is only valid, if (1) the access provider does not initiate the transmission in question, (2) does not pick the address of the transferred information, and (3) does not select or change the transmitted information.

This privilege gives credit to the enormous importance of access providers for the information society, which should not be burdened with incalculable liability risks.[36] There would be no plausible reason to charge a provider with assistance to the spread of pornographic material just because the pornographic content was transmitted through the provider's infrastructure.

At the same time, the legislature supports this privilege with the knowledge that a control of the data stream by the access provider would—in most cases—be technically impossible.[37] The legislature, however, consciously refrained

---

[35] Telemediengesetz [Telemedia Act], Jan. 18, 2007, ¶ 8, clause 1.

[36] BT-Drs. 14/6098, p. 24 (Printed Matter of the Federal Parliament); GERCKE & BRUNST, *supra* note 6, at pt. 608; TOBIAS PAUL, PRIMÄRRECHTLICHE REGELUNGEN ZUR VERANTWORTLICHKEIT VON INTERNETPROVIDERN AUS STRAFRECHTLICHER SICHT [PRIMARY LEGAL RULES ON THE LIABILITY OF INTERNET PROVIDERS FROM CRIMINAL LAW] 126 (2005).

[37] *See* SIEBER, *supra* note 14, at pt. 88 (concerning the technical control possibilities).

from connecting liability privileges to technical incapability. Therefore, the access provider never has the obligation to guarantee an investigation or surveillance of content transmitted by him, whether it is technically possible or not. This is especially important because the current assessment of control possibilities can only be seen as a snapshot in time due to rapid technical development. When looking at the controversial yet successful filter attempts in China, a review of the technical influence that access providers are capable of is necessary.[38]

It is also important to mention that even if the access provider is aware of transmitting penally relevant material, he is still not held responsible.[39] Even though the legislature explicitly included knowledge of penal content as a restriction for the other privileges (which is discussed later), this is not the case for access providers.

Yet the German legislature does restrict the privilege for access providers. According to the second sentence of paragraph 8, clause 1 of the Telemedia Act, the privilege is not applicable if the service provider deliberately cooperated with a user of his service to commit illegal activities. For this cooperation, it is not necessary for provider and user, who can himself be a provider again, to act as joint offenders.[40] It is sufficient if the provider gives assistance to commit a criminal offense—for example—through the provision of necessary links. But of course this raises the question of whether this collusive behavior does not constitute internal content according to paragraph 7, clause 1 of the Telemedia Act.

Finally, in regards to access providers, it should be mentioned that the liability privilege is also effective if content is shortly and automatically cached on a server, as long as it is not saved longer than necessary for the transmission.[41]

---

[38] *See also* SIEBER & NOLDE, SPERRVERFÜGUNGEN IM INTERNET: NATIONALE RECHTSDURCHSETZUNG IM GLOBALEN CYBERSPACE? [BLOCKING ORDERS ON THE INTERNET: NATIONAL LAW ENFORCEMENT IN THE GLOBAL CYBERSPACE?] (2008).

[39] BT-Drs. 14/6098, p. 24 (Printed Matter of the Federal Parliament).

[40] LENCKNER ET AL., *supra* note 26, at pt. 59.

[41] Telemediengesetz [Telemedia Act], Jan. 18, 2007, ¶ 8, clause 2.

Proxy-cache Provider

Separated from the short-term caching of access providers is the "cache-privilege" included in paragraph 9 of the Telemedia Act. As mentioned at the beginning of this article, proxy-cache providers cache commonly demanded content, so it does not have to be transmitted by the content-provider repeatedly. This leads to popular content being cached on various servers. Due to the economic importance of these cachings, the legislature decided to include it in a special privilege. Even though the caching is usually done by access providers, the legislature rightly decided to split the liability for caching from the responsibilities of access providers and created a special regulation.[42]

According to paragraph 9 of the Telemedia Act, operators of such proxy-cache servers are not liable for automatic, temporally limited cachings, which serve the purpose to efficiently transmit external content to users on their demand. But to qualify for this liability privilege, proxy-cache providers need to fulfill a complex system of cumulative requirements.

First, the content must not be altered. This is meant to ensure that the copy on the proxy-server resembles the initial version on the original server.[43]

Second, the requirements for accessing the information must not be disregarded. Thus, the provider of the proxy-server may not alter the access requirements set forth by the owner of the original server.[44] If, for example, the operator of a website installed a password protection to meet youth protection standards, this password protection would need to be guaranteed when accessing the content through the proxy-server. Any kind of access control or restriction must be maintained.

Third, the provider must follow the widely accepted rules for updating content. By this, the provider is bound to regularly compare the cached information to the initial source, verify

---

[42] BT-Drs. 14/6098, p. 24 (Printed Matter of the Federal Parliament).

[43] *Id.* at p. 25.

[44] *See supra* note 41.

whether the original has been changed, and update his cached version if necessary.[45]

Fourth, the proxy-cache provider is not allowed to interfere with data collection technologies. Therefore, he has to ascertain that a website access though his proxy-server is correctly transmitted to the access statistic of the original website.[46]

Finally, the provider is bound to delete the caching if at any time he is made aware of the original source being removed or blocked. This is especially related to cases where the removal or blocking has been judicially or officially ordered. In this way, the legislature accounts to a general problem when issuing removal or blocking decrees. Due to caching, illegal content remains widely accessible even after the removal of the original source. If the proxy-cache provider does not delete penally relevant content, even though he is aware that it has been removed from the original server or the removal has been ordered, he can be prosecuted.

Of course, in a case of collusion, the liability privilege is void as well.

Host Provider

Finally the matter of host provider liability needs to be answered. As a reminder, a host provider enables users to save content on his computer. The classic example for such a service would be the provision of servers, where private persons as well as companies can host their websites.

The legislature assumed that a systematic content control is not possible for the host provider due to the sheer amount and rapid change of data saved on his servers. But what I said about access providers applies here as well: whether a monitoring of content is not possible must be critically reexamined due to technical development. The legislature, however, refrained from a universal control duty in this case as well, as not to unnecessarily burden the providers. Thus, service providers are—according to the first sentence of

---

[45] *Id.*

[46] BT-Drs. 14/6098, p. 25 (Printed Matter of the Federal Parliament).

paragraph 10 of the Telemedia Act—not responsible for the external content they save for a user. Yet this only applies if the provider has no knowledge of the criminal activity or information. If he becomes aware of the content, the provider must take action immediately to remove it or block access to it. Otherwise, he is again fully liable for the content. Knowledge implies that the provider at least knows the exact place of discovery of the illegal information.[47] Whether this knowledge is based on the provider's research or external sources is irrelevant.[48] But due to the penal principle of guilt, it has to be available to the responsible person itself and cannot be attributed as external knowledge according to paragraph 14 or paragraph 166 of the German Civil Code.[49] If, for instance, the youth protection commissary of a company has gained this knowledge but did not pass it on to the director, the existence of knowledge will have to be declined.[50] A further requirement is that the technical possibilities to remove the content are there, and that it is appropriate to demand the removal, even though the law does not state so explicitly. In the legislature's view, this follows the basic principle that law cannot demand technically impossible or inappropriate actions.[51] Inappropriate, however, does not necessarily equate to economic reasons.[52] The point where it becomes inappropriate must be determined on a case-by-case basis, and is also connected to the value of the object of legal interest.[53] Usually this is rather unproblematic. If the host provider knows the concrete address the illegal content is affiliated with, a removal

---

[47] LENCKNER ET AL., *supra* note 26, at pt. 60; Pelz, wistra 1999, 53 (59); *see* SIEBER, *supra* note 14, at pt. 338.

[48] BT-Drs. 14/6098, p. 23 (Printed Matter of the Federal Parliament); Holznage & Kussel, MMR 2001, 347 (349); LENCKNER ET AL., *supra* note 26, at pt. 60; SIEBER, *supra* note 14, at pt. 345.

[49] STEPHAN BLEISTEINER, RECHTLICHE VERANTWORTLICHKEIT IM INTERNET [LEGAL RESPONSIBILITY ON THE INTERNET] 186 (1999); LENCKNER ET AL., *supra* note 26, at pt. 60; SIEBER, *supra* note 14, at pt. 346.

[50] LENCKNER ET AL., *supra* note 26, at pt. 60.

[51] BT-Drs. 14/6098, p. 25 (Printed Matter of the Federal Parliament).

[52] DIRK BARTON, MULTIMEDIA-STRAFRECHT [MULTIMEDIA CRIMINAL LAW] pt. 350 (1999); HÖRNLE, *supra* note 19, at 52.

[53] BT-Drs. 14/6098 pp. 23, 25 (Printed Matter of the Federal Parliament); LENCKNER ET AL., *supra* note 26, at pt. 60.

or blocking should be easily possible without further drawbacks to the provider.[54]

CONCLUSION

When analyzing the respective regulations of the German Telemedia Act, it shows that even though they are briefly formulated, they are absolutely capable of handling the problems of liability arising on the internet. Of course, the regulations do not provide us with rules for every detail, but in light of the rapid technological development, this seems more of an advantage than a disadvantage. When measured according to legal security and flexibility, these regulations are a generally successful solution. Full liability for one's own content, limited liability for external content if one is aware of it, as well as the extensive exclusion from liability for the transmission and mediation of external content, is a proper approach to face the difficulties.

---

[54] *See* Altenhain, AfP 1998, 457 (463); SIEBER, *supra* note 14, at pt. 359.