Institut suisse de droit comparé
Schweizerisches Institut für Rechtsvergleichung
Istituto svizzero di diritto comparato
Swiss Institute of Comparative Law

COMPARATIVE STUDY

ON

BLOCKING, FILTERING AND TAKE-DOWN OF ILLEGAL INTERNET CONTENT

Excerpt, pages 261-289

This document is part of the Comparative Study on blocking, filtering and take-down of illegal Internet content in the 47 member States of the Council of Europe, which was prepared by the Swiss Institute of Comparative Law upon an invitation by the Secretary General. The opinions expressed in this document do not engage the responsibility of the Council of Europe. They should not be regarded as placing upon the legal instruments mentioned in it any official interpretation capable of binding the governments of Council of Europe member States, the Council of Europe's statutory organs or the European Court of Human Rights.

Avis 14-067

Lausanne, 20 December 2015
National reports current at the date indicated at the end of each report.

Dorigny – CH – 1015 Lausanne - Tel : +41 (0)21 692 49 11 - Fax : +41 (0)21 692 4949 –
www.isdc.ch – info@isdc.ch

I. INTRODUCTION

On 24th November 2014, the Council of Europe formally mandated the Swiss Institute of Comparative Law ("SICL") to provide a comparative study on the laws and practice in respect of filtering, blocking and takedown of illegal content on the internet in the 47 Council of Europe member States.

As agreed between the SICL and the Council of Europe, the study presents the laws and, in so far as information is easily available, the practices concerning the filtering, blocking and takedown of illegal content on the internet in several contexts. It considers the possibility of such action in cases where public order or internal security concerns are at stake as well as in cases of violation of personality rights and intellectual property rights. In each case, the study will examine the legal framework underpinning decisions to filter, block and takedown illegal content on the internet, the competent authority to take such decisions and the conditions of their enforcement. The scope of the study also includes consideration of the potential for existing extra-judicial scrutiny of online content as well as a brief description of relevant and important case law.

The study consists, essentially, of two main parts. The first part represents a compilation of country reports for each of the Council of Europe Member States. It presents a more detailed analysis of the laws and practices in respect of filtering, blocking and takedown of illegal content on the internet in each Member State. For ease of reading and comparison, each country report follows a similar structure (see below, questions). The second part contains comparative considerations on the laws and practices in the member States in respect of filtering, blocking and takedown of illegal online content. The purpose is to identify and to attempt to explain possible convergences and divergences between the Member States' approaches to the issues included in the scope of the study.

II. METHODOLOGY AND QUESTIONS

1. Methodology

The present study was developed in three main stages. In the first, preliminary phase, the SICL formulated a detailed questionnaire, in cooperation with the Council of Europe. After approval by the Council of Europe, this questionnaire (see below, 2.) represented the basis for the country reports.

The second phase consisted of the production of country reports for each Member State of the Council of Europe. Country reports were drafted by staff members of SICL, or external correspondents for those member States that could not be covered internally. The principal sources underpinning the country reports are the relevant legislation as well as, where available, academic writing on the relevant issues. In addition, in some cases, depending on the situation, interviews were conducted with stakeholders in order to get a clearer picture of the situation. However, the reports are not based on empirical and statistical data, as their main aim consists of an analysis of the legal framework in place.

In a subsequent phase, the SICL and the Council of Europe reviewed all country reports and provided feedback to the different authors of the country reports. In conjunction with this, SICL drafted the comparative reflections on the basis of the different country reports as well as on the basis of academic writing and other available material, especially within the Council of Europe. This phase was finalized in December 2015.

The Council of Europe subsequently sent the finalised national reports to the representatives of the respective Member States for comment. Comments on some of the national reports were received back from some Member States and submitted to the respective national reporters. The national reports were amended as a result only where the national reporters deemed it appropriate to make amendments. Furthermore, no attempt was made to generally incorporate new developments occurring after the effective date of the study.

All through the process, SICL coordinated its activities closely with the Council of Europe. However, the contents of the study are the exclusive responsibility of the authors and SICL. SICL can however not assume responsibility for the completeness, correctness and exhaustiveness of the information submitted in all country reports.

2. Questions

In agreement with the Council of Europe, all country reports are as far as possible structured around the following lines:

1. What are the legal sources for measures of blocking, filtering and take-down of illegal internet content?

Indicative list of what this section should address:

- Is the area regulated?

- Have international standards, notably conventions related to illegal internet content (such as child protection, cybercrime and fight against terrorism) been transposed into the domestic regulatory framework?
- Is such regulation fragmented over various areas of law, or, rather, governed by specific legislation on the internet?
- Provide a short overview of the legal sources in which the activities of blocking, filtering and take-down of illegal internet content are regulated (more detailed analysis will be included under question 2).

2. What is the legal framework regulating:

2.1. Blocking and/or filtering of illegal internet content?

Indicative list of what this section should address:

- On which grounds is internet content blocked or filtered? This part should cover all the following grounds, wherever applicable:
  - the protection of national security, territorial integrity or public safety (e.g. terrorism),
  - the prevention of disorder or crime (e.g. child pornography),
  - the protection of health or morals,
  - the protection of the reputation or rights of others (e.g. defamation, invasion of privacy, intellectual property rights),
  - preventing the disclosure of information received in confidence.
- What requirements and safeguards does the legal framework set for such blocking or filtering?
- What is the role of Internet **Access** Providers to implement these blocking and filtering measures?
- Are there soft law instruments (best practices, codes of conduct, guidelines, etc.) in this field?
- A brief description of relevant case-law.

2.2. Take-down/removal of illegal internet content?

Indicative list of what this section should address:

- On which grounds is internet content taken-down/ removed? This part should cover all the following grounds, wherever applicable:
  - the protection of national security, territorial integrity or public safety (e.g. terrorism),
  - the prevention of disorder or crime (e.g. child pornography),
  - the protection of health or morals,
  - the protection of the reputation or rights of others (e.g. defamation, invasion of privacy, intellectual property rights),
  - preventing the disclosure of information received in confidence.

- What is the role of Internet Host Providers and Social Media and other Platforms (social networks, search engines, forums, blogs, etc.) to implement these content take down/removal measures?
- What requirements and safeguards does the legal framework set for such removal?
- Are there soft law instruments (best practices, code of conduct, guidelines, etc.) in this field?
- A brief description of relevant case-law.

3. Procedural Aspects: What bodies are competent to decide to block, filter and take down internet content? How is the implementation of such decisions organized? Are there possibilities for review?

Indicative list of what this section should address:

- What are the competent bodies for deciding on blocking, filtering and take-down of illegal internet content (judiciary or administrative)?
- How is such decision implemented? Describe the procedural steps up to the actual blocking, filtering or take-down of internet content.
- What are the notification requirements of the decision to concerned individuals or parties?
- Which possibilities do the concerned parties have to request and obtain a review of such a decision by an independent body?

4. General monitoring of internet: Does your country have an entity in charge of monitoring internet content? If yes, on what basis is this monitoring activity exercised?

Indicative list of what this section should address:

- The entities referred to are entities in charge of reviewing internet content and assessing the compliance with legal requirements, including human rights – they can be specific entities in charge of such review as well as Internet Service Providers. Do such entities exist?
- What are the criteria of their assessment of internet content?
- What are their competencies to tackle illegal internet content?

5. Assessment as to the case law of the European Court of Human Rights

Indicative list of what this section should address:

- Does the law (or laws) to block, filter and take down content of the internet meet the requirements of quality (foreseeability, accessibility, clarity and precision) as developed by the European Court of Human Rights? Are there any safeguards for the protection of human rights (notably freedom of expression)?
- Does the law provide for the necessary safeguards to prevent abuse of power and arbitrariness in line with the principles established in the case-law of the European Court of Human Rights (for example in respect of ensuring that a blocking or filtering decision is as targeted as possible and is not used as a means of wholesale blocking)?

- Are the legal requirements implemented in practice, notably with regard to the assessment of necessity and proportionality of the interference with Freedom of Expression?
- In the case of the existence of self-regulatory frameworks in the field, are there any safeguards for the protection of freedom of expression in place?
- Is the relevant case-law in line with the pertinent case-law of the European Court of Human Rights?

For some country reports, this section mainly reflects national or international academic writing on these issues in a given State. In other reports, authors carry out a more independent assessment.

GERMANY

1. Legal sources

Under German federal law, there is **no specific law** for measures of blocking, filtering and taking down illegal Internet content. Whereas the German legislator implemented[1] the European Directive 2000/31/EC on electronic commerce (E-Commerce-Directive),[2] which concerns inter alia the civil liability of different types of Internet Service Providers, no specific regulations for blocking, filtering and taking down of illegal Internet content exist.

There are several general regulations in the areas of **copyright, trademark and unfair competition law**, which grant general injunctive relief and which are also now being used to order host providers to take down and filter illegal Internet content. In addition, German jurisprudence has developed the notion of so-called **disturbance liability**, which makes it possible to hold host providers (and, to a very limited extent, access providers) responsible for blocking illegal content.

At the same time, the **sixteen federal states** of Germany (*Bundesländer*) have agreed upon two Interstate Treaties: the **Interstate Treaty on Broadcasting and Telemedia** (*Staatsvertrag für Rundfunk und Telemedien*, RStV)[3] as well as the **Interstate Treaty on the Protection of Minors in the Media** (*Jugendmedienschutzstaatsvertrag*, JMStV)[4]. All German federal states have enacted laws ratified these Interstate Treaties and thus turning the provisions of these treaties into law of the respective federal state.

1.1. Host Providers

As concerns the **filtering and taking down of Internet content by host providers at the federal level**, the jurisprudence applies (by analogy) the general rules on injunctive relief against infringements of corporeal property, which are part of German property law and can hence be found in § 1004 German Civil Code (*Bürgerliches Gesetzbuch*, BGB).[5] This rule must be applied in an analogous way since it technically targets only infringements of corporeal property and not of intellectual property. As a result, in order to apply this rule to Internet Service Providers through indirect liability,[6] German jurisprudence has developed the notion of so-called **disturbance liability (*Störerhaftung*)** in its **case law**. As a consequence, extent, limits and preconditions for filtering and taking down of illegal Internet content are governed by case law and not by specific laws.

At the same time, for violations of copyright or trademark law as well as for acts of unfair competition, special regulations exist allowing general injunctive relief. **§ 97 German Copyright Act**

---

1 §§ 7-10 German Telemedia Act (*Telemediengesetz*, TMG), available at http://www.gesetze-im-Internet.de/tmg/index.html (20.04.2015).

2 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

3 Available in both German and English at http://www.kjm-online.de/recht/gesetze-und-staatsvertraege/rundfunkstaatsvertrag-rstv.html (26.05.2016).

4 Available in both German and English at http://www.kjm-online.de/recht/gesetze-und-staatsvertraege/jugendmedienschutz-staatsvertrag-jmstv.html (26.05.2016).

5 Available at http://www.gesetze-im-Internet.de/bgb/index.html (20.04.2015).

6 C. Busch, Secondary Liability of Service Providers, in M. Schmidt-Kessel (ed.), German National Reports on the 19th International Congress of Comparative Law, Tübingen: Mohr Siebeck 2014, p. 765 *et seq*, p. 767.

(*Urhebergesetz*, UrhG),[7] **§§ 14 *et seq.* German Trademark Act (*Markengesetz*, MarkenG)**[8] and **§ 8 German Unfair Competition Act (*Gesetz gegen den unlauteren Wettbewerb*, UWG)**[9] all grant **injunctive relief** against copyright or trademark infringements or measures of unfair competition. Nonetheless, these laws are **not specifically designed for matters of illegal Internet content**.[10]

Based not on federal law but on the **law of the different federal states**, orders to take down illegal Internet content by host providers can be given within the scope of § 59 of the Interstate Treaty on Broadcasting and Telemedia as well as § 20 of the Interstate Treaty on the Protection of Minors in the Media. The former Interstate Treaty includes a legal basis for the respective supervisory authorities of each federal state to **prohibit illegal offers** and to **orderi the blocking thereof**.[11] In the first place, any measures must be directed against the **content provider**. Only if such an order against the content provider proves to be impracticable or unlikely to be successful, can the blocking measure be taken against **host or access providers**. The latter Interstate Treaty regulates the protection of minors in the media in general and also on the Internet. Its **§ 20** refers to the aforementioned § 59 of the Interstate Treaty on Broadcasting and Telemedia[12] and thus provides the legal basis for **prohibiting content providers** from offering illegal Internet content and **ordering host providers to block** illegal offers with regard to the **protection of minors**.[13]

1.2. Access Providers

With regard to **blocking illegal Internet content by access providers**, only the **laws of the sixteen federal states** provide a legal basis. It is the same basis as for ordering host providers to take down illegal Internet content, namely **§ 59 of the Interstate Treaty on Broadcasting and Telemedia** as well as, by referring to this § 59, **§ 20 of the Interstate Treaty on the Protection of Minors on the Media**. For further information see above, under point 1.1.

At the **federal level** however, **German statutory law** provides **no legal basis** for blocking illegal Internet content by access providers. For a period of about two years, the German Access Impeding

---

7 § 97 para. 1 German Copyright Act (*Urhebergesetz*, UrhG); available at http://www.gesetze-im-Internet.de/urhg/index.html (20.04.2015).

8 § 14 para. 4 ss. 1, 2, § 15 para. 4 ss. 1, 2 German Trademark Act (*Markengesetz*, MarkenG); available at http://www.gesetze-im-Internet.de/markeng/index.html (20.04.2015).

9 § 8 para. 1 ss. 1, 2 German Unfair Competition Act (*Gesetz gegen den unlauteren Wettbewerb*, UWG), available at http://www.gesetze-im-Internet.de/uwg_2004/index.html (20.04.2015).

10 They already existed prior to the European Directive 2001/29/EC on copyright (Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, Copyright-Directive), but have been slightly rephrased as part of the implementation process of this directive as well as of Directive 2004/48/EC on the enforcement of intellectual property rights (Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, Enforcement-Directive); Arts. 4, 6 German Act for Improving Enforcement of Intellectual Property Rights (*Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums*).

11 § 59 para. 3 ss. 1, 2, para. 4 Interstate Treaty on Broadcasting and Telemedia (*Staatsvertrag für Rundfunk und Telemedien*, RStV).

12 § 20 para. 4 Interstate Treaty on the Protection of Minors in the Media (*Jugendmedienschutzstaatsvertrag*, JMStV).

13 German Commission for the Protection of Minors in the Media (*Kommission für Jugendmedienschutz*, KJM), Control procedures, available at http://www.kjm-online.de/en/telemedia/control-procedures.html (26.05.2016).

Act (*Zugangserschwerungsgesetz*, ZugErschwG)[14] existed and allowed access to websites with child pornography to be blocked. However, no blocking order had actually ever been made based on this law and it was subsequently abolished. In January 2015, parts of the criminal law regulations on child pornography were amended, *inter alia* in order to implement the European Directive 2011/93/EC on sexual abuse and child pornography (Child Pornography-Directive)[15].[16] Yet, these amendments do not address measures for blocking or taking-down child pornography on the Internet as regulated in Article 25 of the Directive.

Nonetheless, access providers can be held responsible based on the notion of **disturbance liability** mentioned above. Two Higher Regional Courts have addressed this issue recently, and both **denied the respective access provider's responsibility**. As appeals have been lodged against both decisions, the German Federal Court of Justice will also soon deal with this question.[17]

In the context of access providers' responsibility based on disturbance liability, the role of operators of wireless local area networks (**WLAN**) is noteworthy. There are several court decisions dating from the last five or so years, in which the courts have applied the aforementioned notion of **disturbance liability** to WLAN-operators, particularly with regard to WLAN in hotels, cafés or Internet-cafés, i.e. places where the operators offer their WLAN-access to a wide number of people. In these decisions, the courts have treated **WLAN-operators as access providers**, based on the argument that they were granting their guests access to the Internet via their WLAN and were thus giving them the opportunity to up- or download illegal content.[18] The European Court of Justice has also been called upon to decide the question of whether WLAN-operators qualify as access providers with regard to article 12 E-Commerce-Directive.[19] In an attempt to remedy this unclear situation and in order to guarantee broad coverage of WLAN in Germany, an amendment of the German Telemedia Act has been drafted. This proposed amendment explicitly categorises WLAN-operators as access providers, on the one hand, but, on the other hand, it also excludes these operators from responsibility for both damages and blocking illegal content under certain conditions.[20]

---

14 The text of the German Access Impeding Act (*Zugangserschwerungsgesetz*, ZugErschwG) is available in Bundesgesetzblatt (BGBl.) Part I 2010, p. 78 *et seq*, http://www.bgbl.de/banzxaver/bgbl/text.xav?SID=&tf=xaver.component.Text_0&tocf=&qmf=&hlf=xaver.component.Hitlist_0&bk=bgbl&start=%2F%2F*%5B%40node_id%3D'254310'%5D&skin=pdf&tlevel=-2&nohist=1 (11.03.2015).

15 Directive 2011/93/EC of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.

16 Bundesgesetzblatt (BGBl.) Part I 2015, p. 10 *et seq*.

17 Higher Regional Court (*Oberlandesgericht*, OLG) Hamburg, judgement of 21.11.2013 – 5 U 68/10; OLG Köln, judgement of 18.07.2014 – 6 U 192/11 (*Goldesel*).

18 German Federal Court of Justice (*Bundesgerichtshof*, BGH), judgement of 12.05.2010 – I ZR 121/08 (*Sommer unseres Lebens*); Regional Court (*Landgericht*, LG) Frankfurt a.M., judgement of 18.08.2010 – 2-06 S 19/09; LG Hamburg, judgement of 25.11.2010 – 310 O 433/10.

19 Regional Court (*Landgericht*, LG) München I, decision of 18.09.2014 – 7 O 14719/12.

20 Federal Ministry for Economic Affairs and Energy, *Referentenentwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes (Zweites Telemedienänderungsgesetz – 2. TMGÄndG)* vom 15.06.2015, available at http://www.bmwi.de/BMWi/Redaktion/PDF/S-T/telemedienaenderungsgesetz-aenderung,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf (15.07.2015).

1.3. Implementation of International Conventions

Germany has implemented the **Convention on Cybercrime**[21] in the 41st Criminal Law Amendatory Act,[22] as well as in the Revision Act on Telecommunications Surveillance and Other Undercover Investigation Measures as well as for the Implementation of Directive 2006/24/EC.[23] The **Additional Protocol to this Convention**[24] has been implemented in an act implementing the Framework decision 2008/913/JI of the Council of the European Union.[25] The German parliament (*Bundestag*) accepted **the Convention on the Prevention of Terrorism**[26] by law.[27] **The Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse**[28] has been signed and also recently ratified; it entered into force at the beginning of March 2016.[29] As regards **Directive 95/46/EC on data protection** (Data Protection-Directive),[30] Germany has implemented this Directive by the Federal Data Protection Law Amendatory Act.[31]

2. Legal Framework

In German Telemedia Act § 7,[32] the German legislator made use of the option given in the E-Commerce-Directive[33] to **allow injunctive relief outside of a provider's limited civil responsibility**. This law thus permits regulations on injunctive relief against Internet Service Providers. Yet, the two basic principles set out in German Telemedia Act § 7 remain applicable: while paragraph 2, sentence

---

21 Council of Europe Convention on Cybercrime, Budapest, dated 23.11.2001.

22 *41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität* (41. StrÄndG), dated 07.08.2007, Bundesgesetzblatt (BGBl.) Part I 2007, p. 1786 *et seq*.

23 *Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmassnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG*, dated 21.12.2007, Bundesgesetzblatt (BGBl.) Part I 2007, p. 3198 *et seq*.

24 Council of Europe Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, dated 28.01.2003.

25 *Gesetz zur Umsetzung des Rahmenbeschlusses 2008/913/JI des Rates vom 28. November 2008 zur strafrechtlichen Bekämpfung bestimmter Formen und Ausdrucksweisen von Rassismus und Fremdenfeindlichkeit und zur Umsetzung des Zusatzprotokolls vom 28. Januar 2003 zum Übereinkommen des Europarats vom 23. November 2001 über Computerkriminalität betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art*, dated 16.03.2011, Bundesgesetzblatt (BGBl.) Part I, p. 418 *et seq*.

26 Council of Europe Convention on the Prevention of Terrorism, Warsaw, dated 16.05.2005.

27 *Gesetz zu dem Übereinkommen des Europarats vom 16. Mai 2005 zur Verhütung des Terrorismus*, dated 16.03.2011, Bundesgesetzblatt (BGBl.) Part II 2011, p. 300 *et seq*.

28 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Lanzarote, 25.10.2007.

29 Council of Europe, *Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Status as of 20/4/2015*, available at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=201&CM=8&DF=20/04/2015&CL=ENG (20.04.2015).

30 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

31 *Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze*, dated 18.05.2001, Bundesgesetzblatt (BGBl.) Part I 2001, p. 904 *et seq*.

32 § 7 para. 2 s. 2 German Telemedia Act (*Telemediengesetz*, TMG).

33 Last paragraph of articles 12 to 14 E-Commerce-Directive respectively.

1 states that **Internet Service Providers do not have a duty to permanently check Internet content**,[34] paragraph 1 clarifies that all Internet Service Providers are **responsible for their own content**. Moreover, § 59 of the Interstate Treaty on Broadcasting and Telemedia refers to German Telemedia Act §§ 7-10, stating that § 7 paragraph 2, sentence 1 of this law shall remain unaffected by the legal basis for taking down and blocking illegal Internet content in the Interstate Treaty. Content providers, i.e. providers offering their own content such as information or comments, are thus ever responsible for their own content in its entirety. The former of these two basic principles implies, however, that an Internet Service Provider becomes responsible only in the particular moment in which it notices the infringement, or in which someone else points out to it the infringement. The Internet Service Provider must have **knowledge of the relevant infringement** in order to be responsible for it. In case the provider is responsible, it has a **duty to take down or remove** the illegal Internet content and to take adequate and appropriate measures in order to **prevent similar infringements** in the future.

In relation to **host providers**, one can say that they become responsible as soon as they **adopt the content contributed by users as their own**. After they have adopted the foreign content as their own, they can be treated as content providers. Yet, it is **difficult to define** at which point a host provider adopts this foreign and illegal content.[35] The German Federal Court of Justice has developed different criteria to determine this, although these **criteria are not absolute and depend upon the circumstances of the individual case**. According to the criteria, it can generally be considered such an adoption if the host provider reviews new content before uploading it.[36] On the other hand, this alone is not sufficient if users can clearly see that a third person authored the respective content. A strong indication of relevant adoption is the provider integrating the foreign content into its own layout as well as if the provider benefits economically from this contribution.[37] The jurisprudence sometimes elaborated further on these criteria, concluding that an overall view by an objective observer shall be decisive.[38]

The Internet Service Provider can be asked to fulfil its duty to take down and filter illegal content by way of injunctive relief.[39] In most cases, this claim is based on the so-called **disturbance liability**,

---

34 The Federal Court of Justice (*Bundesgerichtshof*, BGH) elaborated in this context also that operators of an Internet auction website are not obliged to manually control whether any picture on the website differs from the original, BGH, judgement of 22.07.2010 – I ZR 139/08 (*Kinderhochstühle im Internet*); see also J. Ensthaler & M. Heinemann, Die Fortentwicklung der Providerhaftung durch die Rechtsprechung, in Gewerblicher Rechtsschutz und Urheberrecht (GRUR) 2012, p. 433 *et seq*, p. 437.

35 B. Nordemann, Haftung von Providern im Urheberrecht: Der aktuelle Stand nach dem EuGH-Urteil vom 12.7.2011 – EUGH 12.07.2011 Aktenzeichen C-324/09 – L'Oréal/eBay, in Gewerblicher Rechtsschutz und Urheberrecht (GRUR) 2011, p. 977 *et seq*, p. 977 *et seq*; H. Hören & S. Yankova, The Liability of Internet Intermediaries – The German Perspective, in International Review of Intellectual Property and Competition Law (IIC) 2012, p. 501 *et seq*, p. 510.

36 The Higher Regional Court (*Oberlandesgericht*, OLG) Hamburg has considered the lack of such preliminary check as sufficient reason to reject the provider's responsibility, OLG Hamburg, judgement of 29.09.2010 – 5 U 9/09 (*Sevenload*).

37 German Federal Court of Justice (*Bundesgerichtshof*, BGH), judgement of 12.11.2009 – I ZR 166/07 (*marions-kochbuch.de*).

38 "Gesamtschau […] aus der Perspektive eines objektiven Beobachters", Higher Regional Court Berlin (*Kammergericht*, KG), decision of 10.07.2009 – 9 W 119/08.

39 However, a legal dispute is not always necessary, as for example in 2012 when Twitter suspended account privileges for a German neo-Nazi group after a request from the police, W. Benedek & M. Kettemann, Freedom of expression and the Internet, Strasbourg 2013; see also the corresponding

created by the courts in their case law. This notion of disturbance liability as developed by the jurisprudence is not based on responsibility for unlawful acts, but rather on responsibility for nuisance; it is only directed at injunctive relief, not at damages. The central regulation for this general injunctive relief due to nuisance is § 1004 German Civil Code. According to that section, a person disturbing someone else's property in an "adequate and causal way" owes injunctive relief irrespective of her/his fault.[40] By analogy, this is also applied in practice to disturbance of intellectual property rights. However, the norm's distinct wording[41] does not allow a claim for damages based on this concept of disturbance liability.

In German case law, claims for taking down or removing illegal Internet content by host providers, as well as for blocking or filtering such content by access providers, generally concerns **private law issues**. This is due to the fact that one of the elements of disturbance liability is that someone's (intellectual) property is being disturbed. Most of these cases deal with copyright, trademark or unfair competition disputes; some also deal with aspects of the general personal right. Additionally, cases concerning the law of the different federal states, i.e. the Interstate Treaties on Broadcasting and Telemedia as well as on the Protection of Minors in the Media, are dealt with by the administrative courts. Competent to give orders to block or take down illegal Internet content based on these Treaties are the State Media Authorities of the different federal states and, as regards the protection of minors, the German Commission on the Protection of Minors in the Media acting as an organ of the State Media Authorities.[42] The **very few cases on criminal content** date from a short period during which the courts neglected to consider the constitutional right to privacy of telecommunication. Until a legal basis for removing or blocking criminal content, as for example child pornography or extreme right wing statements, has been enacted, authorities can only order the content providers themselves, *i.e*. the authors, to remove the content. As a result, no relevant case law exists on these issues.

2.1. Blocking and/or filtering of illegal Internet content

Blocking and/or filtering of illegal Internet content is particularly relevant to access providers, since they have the technical ability to block access to a website in its entirety.

Based on the Interstate Treaties on Broadcasting and Telemedia as well as on the Protection of Minors in the Media and with that on the law of the different federal states, access providers can be ordered to block illegal Internet content.

---

letter published by Lumen Database, a project of the Berkman Center for Internet & Society at Harvard University, available at https://www.lumendatabase.org/notices/1799690 (09.12.2015).

40 § 1004 para. 1 s. 1 German Civil Code (*Bürgerliches Gesetzbuch*, BGB).

41 "§ 1004 Bürgerliches Gesetzbuch: Beseitigungs- und Unterlassungsanspruch:
(1) Wird das Eigentum in anderer Weise als durch Entziehung oder Vorenthaltung des Besitzes beeinträchtigt, so kann der Eigentümer von dem Störer die Beseitigung der Beeinträchtigung verlangen. Sind weitere Beeinträchtigungen zu besorgen, so kann der Eigentümer auf Unterlassung klagen.
(2) Der Anspruch ist ausgeschlossen, wenn der Eigentümer zur Duldung verpflichtet ist."

42 German Commission for the Protection of Minors in the Media (*Kommission für Jugendmedienschutz*, KJM), Organisation, available at http://www.kjm-online.de/en/the-kjm/organisation.html (27.05.2016).

However, there is currently no statutory legal basis at federal level for ordering an access provider to block or filter illegal Internet content. In absence of a statutory legal basis, such an order would infringe the constitutional right to privacy of telecommunications.

Access providers (in the common sense) also cannot be ordered to block or filter illegal Internet content on the basis of the notion of disturbance liability, as this is not technically possible for them to do.

Nevertheless, there is case law based on disturbance liability in which WLAN-operators have been considered as access providers and have been found responsible for illegal Internet content up- or downloaded by third persons using their WLAN. At the moment, it is unclear whether this trend will continue, as the European Court of Justice has been called upon in this matter and also because a draft for amending the German Telemedia Act has been developed.

2.1.1. Statutory legal basis for a claim

Currently, **only the law of the various federal states provides a statutory legal basis for blocking illegal Internet content by access providers**. This legal basis can be found in **§ 59 of the Interstate Treaty on Broadcasting and Teleme**dia as well as in **§ 20 of the Interstate Treaty on the Protection of Minors in the Media**, which refers to §59 of the aforementioned treaty.

According to § **59 of the Interstate Treaty on Broadcasting and Telemedia**, the **State Media Authority** of the respective state must take appropriate measures if it becomes aware of **violations of certain provisions for telemedia**.[43] These provisions regard the duty to supply information on the provider[44], the duty to separate advertising from other content[45], the duty to supply information regarding commercial communication[46] as well as the prohibition of subliminal advertising and requirements concerning audiovisual offers and gambling[47].[48] In addition, the State Media Authorities must also take appropriate measures when they detect violations of "**general law**" as well as legal provisions **protecting personal honour**. These include criminal law, civil law provisions in private law, unfair competition law, copyright law and trademark law as well as §§ 823 *et seq.* German Civil Code and §§ 185 *et seq.* German Criminal Code which protect the personal honour.[49]

Through **§ 20 of the Interstate Treaty on the Protection of Minors in the Media**, the **German Commission for the Protection of Minors in the Media, acting as an organ of the State Media Authorities,** takes the appropriate measures if it becomes aware of violations of the said treaty. The treaty enumerates certain **illegal contents** in its § 4 and furthermore prohibits **content impairing development** in § 5 and specific forms of **advertising and teleshopping** in § 6.

---

43 § 59 para. 3 s. 1, para. 2 Interstate Treaty on Broadcasting and Telemedia (*Staatsvertrag für Rundfunk und Telemedien*, RStV).

44 As set out in § 55 para. 1, § 5 German Telemedia Act (*Telemediengesetz*, TMG).

45 As set out in § 58 para. 1 German Telemedia Act (*Telemediengesetz*, TMG).

46 As set out in § 6 German Telemedia Act (*Telemediengesetz*, TMG).

47 As set out in § 58 para. 1 German Telemedia Act (*Telemediengesetz*, TMG).

48 C. Fiedler, in H. Gersdorf/B.P. Paal (eds.), Beck'scher Online-Kommentar Informations- und Medienrecht, 11th ed., Munich 2016, § 59 RStV, para. 13.

49 C. Fiedler, in H. Gersdorf/B.P. Paal (eds.), Beck'scher Online-Kommentar Informations- und Medienrecht, 11th ed., Munich 2016, § 59 RStV, para. 15.

However, §59 of the Interstate Treaty on Broadcasting and Telemedia also provides for certain **conditions** that must be fulfilled for taking measures based on either this norm or on § 20 of the Interstate Treaty on the Protection of Minors in the Media. First, measures must be **directed at the content provider in the first instance**. Only if measures against the content provider are not practicable or unlikely to prove successful can measures be directed against the access provider.[50] Second, blocking the illegal Internet content must be **technically possible and reasonable**.[51] The latter leads to the condition that blocking Internet content must be a last resort and can only be ordered if milder means are not possible. As a consequence, most case law concerns official complaints made by the State Media Authority or the German Commission for the Protection of Minors in the Media against access providers and not blocking orders.[52] Third, the supervisory authorities are not allowed to take any measures if the illegal Internet content affects the **rights of a third party** and legal action is possible for this third party. In this case, the authority merely acts, if this is in public interest.[53] This condition does not apply to matters of protection of minors on the media.[54] And, finally, specific rules apply for **journalistic edited content**, which is protected to a higher extent from prohibition or blocking.[55]

At the federal level, however, there is currently **no statutory legal basis for blocking or filtering illegal Internet content by access providers**.

Some **older case law** states that the respective access providers were obliged to block access to illegal Internet content.[56] These orders were based on the Interstate Agreement on Media Services (*Mediendienste-Staatsvertrag*, MDStV),[57] which ceased operation in 2007. According to its § 22,[58] the respective surveillance authority took the necessary measures to remove violations of the

---

50 § 59 para. 4 s. 1 Interstate Treaty on Broadcasting and Telemedia (*Staatsvertrag für Rundfunk und Telemedien*, RStV).

51 § 59 para. 4 s. 1 Interstate Treaty on Broadcasting and Telemedia (*Staatsvertrag für Rundfunk und Telemedien*, RStV); see also § 59 para 3 ss. 3, 4 RStV, which states that prohibition orders directed at the content provider must be proportionate and may only be given if the objective can be achieved by other means. If the latter is the case, the prohibition must be restricted to specific types and parts of the Internet content or it must be limited in time.

52 See for example these decisions, regarding the different Internet Service Providers: Federal Administrative Court (Bundesverwaltungsgericht, BVerwG), decision of 23.7.2014 – 6 B 1/14; Higher Administrative Court (Oberverwaltungsgericht, OVG) Münster, judgement of 17.06.2015 – 13 A 1072/12; Administrative Court (Verwaltungsgericht, VG) Hamburg, judgement of 29.02.2012 – 9 K 139/09; VG Karlsruhe, decision of 25.7.2012 – 5 K 3496/10; VG Hamburg, judgement of 21.08.2013 – 9 K 1879/12; VG Düsseldorf, judgement of 24.06.2014 – 27 K 7499/13 (this decision refuses a claim for ordering to block a website).

53 § 59 para. 5 Interstate Treaty on Broadcasting and Telemedia (*Staatsvertrag für Rundfunk und Telemedien*, RStV).

54 § 20 para. 4 Interstate Treaty on the Protection of Minors in the Media (*Jugendmedienschutzstaatsvertrag*, JMStV).

55 According to § 59 para. 3 s. 6 Interstate Treaty on Broadcasting and Telemedia (*Staatsvertrag für Rundfunk und Telemedien*, RStV), „journalistic edited offers which, in particular, reproduce completely or partially the texts or visual contents of periodical print media may be blocked only pursuant to the provisions detailed in § 97 para. 5 s. 2 and § 98 of the German Code of Criminal Procedure."

56 Higher Regional Administrative Court (*Oberverwaltungsgericht*, OVG) Münster, decision of 19.03.2003 – 8 B 2567/02; Administrative Court (*Verwaltungsgericht*, VG) Arnsberg, judgement of 26.11.2004 – 13 K 3173/02; VG Gelsenkirchen, decision of 28.07.2006 – 15 K 2170/03.

57 Still available at http://www.recht-niedersachsen.de/22620/mdstv1.htm (20.04.2015).

58 Para. 3 in conjunction with para. 2.

Agreement. In case measures against the responsible person, namely the content provider, were not possible or not promising, the authority could direct its measures against an access provider. In the cases that the courts dealt with, the content providers had uploaded extreme right wing content that constituted criminal offences. Since the content providers were based abroad, orders to take down the illegal content had proven unfruitful. Hence, the authority asked the access providers to block access to the respective websites and the courts then found these orders to be legitimate.

Conversely, **current jurisprudence forbids blocking by access providers without a legal basis**. The courts argue that such a violation of the **constitutional right to privacy of telecommunications**[59] may only happen with an explicit legal basis.[60] The courts that dealt with the aforementioned blocking orders had neglected this notion of the right to privacy of telecommunications and did not discuss it at all. Although the **German Access Impeding Act**[61] of February 2010 allowed access to websites with child pornography to be blocked, this act was **abolished** just two years later.[62] Also during this time, an internal document advised the respective authorities not to enforce this law and it has indeed never been enforced.[63] It is probably due to this questionable instruction not to apply the law that the much-criticised act[64] was ultimately abolished.[65] Following the abolishment of the German Access Impeding Act, **no such legal basis exists** under German law. Blocking orders against access providers are thus currently impossible (and will remain impossible for as long as there is no explicit legal basis for such an order) as they would infringe the right to privacy of telecommunications.

2.1.2. Disturbance Liability

As a general rule, blocking of illegal Internet content by access providers is only rarely possible in Germany at the moment and even then only as part of the so-called **disturbance liability**. This notably applies to WLAN-operators, who are typically being considered as access providers.

---

59 Art. 10 German Constitution (*Grundgesetz*, GG), available at http://www.gesetze-im-Internet.de/gg/index.html (20.04.2015).

60 Higher Regional Court (*Oberlandesgericht*, OLG) Hamburg, judgement of 22.12.2010 – 5 U 36/09; Regional Court (*Landgericht*, LG) Hamburg, judgement of 12.03.2010 – 308 O 640/08; LG Köln, judgement of 31.08.2011 – 28 O 362/10; see also W. Durner, Fernmeldegeheimnis und informationelle Selbstbestimmung als Schranken urheberrechtlicher Sperrverfügungen im Internet?, in Zeitschrift für Urheber- und Medienrecht (ZUM) 2010, p. 833 *et seq*; D. Gesmann-Nuissl & K. Wünsche, Neue Ansätze zur Bekämpfung der Internetpiraterie – ein Blick über die Grenzen, in Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil (GRUR Int) 2012, p. 225, p. 228 *et seq*.

61 The text of the German Access Impeding Act (*Zugangserschwerungsgesetz*, ZugErschwG) is available at Bundesgesetzblatt (BGBl.) Part I 2010, p. 78 *et seq*, http://www.bgbl.de/banzxaver/bgbl/text.xav?SID=&tf=xaver.component.Text_0&tocf=&qmf=&hlf=xaver.component.Hitlist_0&bk=bgbl&start=%2F%2F*%5B%40node_id%3D'254310'%5D&skin=pdf&tlevel=-2&nohist=1 (20.04.2015).

62 Bundesgesetzblatt (BGBl.) Part I 2011, p. 2958.

63 D. Frey *et al.*, Internetsperren und der Schutz der Kommunikation im Internet: Am Beispiel behördlicher und gerichtlicher Sperrungsverfügungen im Bereich des Glücksspiel- und Urheberrechts, in: MultiMedia und Recht Beilage 2012, p. 1, p. 4.

64 See for example D. Heckmann, Stellungnahme von Prof. Dr. Dirk Heckmann zur Sachverständigenanhörung des Deutschen Bundestages in Sachen Zugangserschwerungsgesetz. Zur Verfassungswidrigkeit von Netzsperren, 2010, available at http://fr.scribd.com/doc/101855879/Stellungnahme-ZugErschwG-Heckmann (15.07.2015).

65 M. Gercke, Die Entwicklung des Internetstrafrechts 2010/2011, in: Zeitschrift für Urheber- und Medienrecht (ZUM) 2011, p. 609, p. 609 *et seq*.

In 2013 and 2014, two Higher Regional Courts addressed the question of access providers' responsibility based on disturbance liability in detail and both **denied the respective access providers' responsibility**. The courts pointed out that protective measures were technically not effective enough and also had the effect of blocking access to legal content,[66] which constituted a violation of the freedom of opinion.[67] Furthermore, there lacked an explicit legal basis for lawfully intervening in the constitutional right to privacy of telecommunication[68].[69] Appeals have been lodged and accepted against both judgements, meaning that the **German Federal Court of Justice will soon deal with this question**.[70]

2.1.2.1. WLAN-operators

The current notion of disturbance liability seems to apply only to access providers in the context of **WLAN-operators**. These have been held responsible in cases in which they allowed or tolerated the use of their respective **WLAN**, or if they did not sufficiently protect their WLAN against use by third parties. This mainly applies to natural persons or operators of, for example, Internet-cafés, hotels or holiday flats.[71] By letting someone else use their WLAN, they become **access providers that are then responsible as a disturber for rights violations committed through their WLAN, even if committed by a third party**.[72] According to these court decisions,[73] and in contrast to access providers in the

---

66 So-called "overblocking".

67 Art. 5 para. 1 s. 1 German Constitution (*Grundgesetz*, GG).

68 Art. 10 German Constitution (*Grundgesetz*, GG).

69 Higher Regional Court (*Oberlandesgericht*, OLG) Hamburg, judgement of 21.11.2013 – 5 U 68/10; OLG Köln, judgement of 18.07.2014 – 6 U 192/11 (*Goldesel*).

70 On 26.11.2015, the Federal Court of Justice (*Bundesgerichtshof*, BGH) rejected both appeals on the grounds that the provision of access to websites with content that violates copyright law was indeed a causal contribution to the corresponding infringement. Yet, the access provider can only be deemed as the disturber, if the copyright holder has taken reasonable measures in order to take action against the content and the host provider, see the corresponding press release of the Federal Court of Justice on the judgements of 26.11.2015, available at http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2015&Sort=3&nr=72928&pos=0&anz=195 (09.12.2015).

71 German Federal Court of Justice (*Bundesgerichtshof*, BGH), judgement of 12.05.2010 – I ZR 121/08 (*Sommer unseres Lebens*); Regional Court (*Landgericht*, LG) Frankfurt a.M., judgement of 18.08.2010 – 2-06 S 19/09; LG Hamburg, judgement of 25.11.2010 – 310 O 433/10.

72 K. Nenninger, Anmerkung zu Bundesgerichtshof (BGH), Urteil vom 12.5.2010 – I ZR 121/08 *(Sommer unseres Lebens)*, in: Neue Juristische Wochenschrift (NJW) 2010, p. 2064, p. 2064; S. Leible/D. Jahn, Anmerkung zu Bundesgerichtshof (BGH), Urteil vom 12.5.2010 – I ZR 121/08 (Sommer unseres Lebens), in Kommentierte BGH-Rechtsprechung Lindenmaier-Möhring (LMK) 2010, 306719; R. Mantz, Die Haftung des Betreibers eines gewerblich betriebenen WLANs und die Haftungsprivilegierung des § 8 TMG: Zugleich Besprechung von LG Frankfurt a.M., Urt. V. 28.6.2013 – 2-06 O 304/12 – *Ferienwohnung*, in Gewerblicher Rechtsschutz und Urheberrecht Rechtsprechungs-Report (GRUR-RR) 2013, p. 497, p. 499; C. Busch, Secondary Liability of Service Providers, in M. Schmidt-Kessel (ed.), German National Reports on the 19th International Congress of Comparative Law, Tübingen: Mohr Siebeck 2014, p. 765 *et seq*, p. 774; R. Mantz & T. Sassenberg, Rechtsfragen beim Betrieb von öffentlichen WLAN-Hotspots, in NJW 2014, p. 3537, p. 3540 *et seq*.

73 The five cases cited in the German Lawyer Association's (*Deutscher Anwaltverein*, DAV) statement on the draft for amending the German Telemedia Act (*Telemediengesetz*, TMG) are not of relevance here, as they only regard damages and not blocking or removing illegal Internet content; DAV, Stellungnahme des Deutschen Anwaltvereins durch den Ausschuss Informationsrecht zum Entwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetz (Zweites Telemedienänderungsgesetz – 2. TMGÄndG) vom 11.03.2015, 2015, available at http://anwaltverein.de/de/newsroom/sn-17-15-

narrower sense, which offer access to the Internet to an unmanageable multitude of people, it was considered reasonable for the named access providers in the broader sense to be required to take protective measures. For example, it was considered possible and reasonable for an operator of an Internet-café to block the ports necessary for file sharing.[74] By the same token, hotel operators could protect themselves against any responsibility as a disturber by advising their hotel guests to respect the laws while using the hotel's WLAN.[75]

In order to substantiate this reasoning and in parts also as a reaction to the decision on UPC Telekabel Wien by the European Court of Justice,[76] the Regional Court Munich I stayed proceedings end of 2014 in a case in which the WLAN operator knowingly did not protect his WLAN by a password, in order to make the Internet access available to third parties. **The court submitted the question of whether WLAN-operators are access providers with regard to article 12 E-Commerce-Directive to the European Court of Justice**.[77] The regional court's questions to the European Court of Justice concern the following wordings and ambiguities:

- "normally provided for remuneration" (art. 12 para. 1 in conjunction with art. 2 lit. b) E-Commerce-Directive in conjunction with art. 1 n° 2 Directive 98/34/EC as amended by Directive 98/48/EC)
- "transmission in a communication network" (art. 12 para. 1 E-Commerce-Directive)
- "providing" (art. 12 para. 1 in conjunction with art. 2 lit. b) E-Commerce-Directive)
- "not liable for the information transmitted" (art. 12 para. 1 E-Commerce-Directive)
- Competence of national judges to order access provider to in the future refrain from providing third persons a concrete copyrighted work through Internet sharing networks via a concrete Internet connection (art. 12 para. 1 in conjunction with art. 3 E-Commerce-Directive)
- Application by analogy of art. 14 para. 1 lit. b) E-Commerce-Directive on injunctive relief (art. 12 para. 1 E-Commerce-Directive)
- Requirements for a service provider (art. 12 para. 1 in conjunction with art. 2 lit. b) E-Commerce-Directive)
- Opposition of art. 12 para. 1 E-Commerce-Directive against decisions by national judges ordering access providers with costs to in the future refrain from providing third persons a concrete copyrighted work through Internet sharing networks via a concrete Internet connection, whereat the access provider can choose the technical measure freely (art. 12 para. 1 E-Commerce-Directive)
- Opposition of art. 12 para. 1 E-Commerce-Directive against decisions by national judges ordering access providers with costs to in the future refrain from providing third persons a concrete

---

entwurf-eines-zweiten-gesetzes-zur-aenderung-des-telemediengesetz-zweites-telemedienaenderungsgesetz-2-tmgaendg-vom-11- (15.07.2015).

74 Regional Court (*Landgericht*, LG) Hamburg, judgement of 25.11.2010 – 310 O 433/10.

75 Regional Court (*Landgericht*, LG) Frankfurt a.M., judgement of 18.08.2010 – 2-06 S 19/09.

76 European Court of Justice, judgement of 27.03.2014 – C-314/12 (*UPC Telekabel Wien GmbH*); see on this decision also G. Spindler, Zivilrechtliche Sperrverfügungen gegen Access Provider nach dem EuGH-Urteil „UPC Telekabel", in Gewerblicher Rechtsschutz und Urheberrecht (GRUR) 2014, p. 826 *et seq*; A. Nazari-Khanachayi, Access-Provider als urheberrechtliche Schnittstelle im Internet: Europarechtliche Vorgaben im Hinblick auf Zugangserschwerungsverfügungen und Lösungsansätze für das deutsche Recht de lege ferenda, in GRUR 2015, p. 115 *et seq*.

77 Regional Court (*Landgericht*, LG) München I, decision of 18.09.2014 – 7 O 14719/12; see also R. Mantz & T. Sassenberg, Verantwortlichkeit des Access-Providers auf dem europäischen Prüfstand: Neun Fragen an den EuGH zu Haftungsprivilegierung, Unterlassungsanspruch und Prüfpflichten des WLAN-Betreibers, in MultiMedia und Recht (MMR) 2015, p. 85 *et seq*.

copyrighted work through Internet sharing networks via a concrete Internet connection, whereat the access provider can choose the technical measure freely, but in practice the choice is reduced to shutting down the Internet connection, introducing a password or checking every communication (art. 12 para. 1 E-Commerce-Directive).[78]

Furthermore, a **new draft for amending the German Telemedia Act** seeks to **explicitly categorise WLAN operators as access providers and thus exclude them from responsibility for both damages and blocking illegal content**.[79] Through this reduced responsibility, private and public institutions shall feel more at ease to provide Internet access through their WLANs for the public in order to obtain broader coverage. At the moment, an amended[80] first draft of the Federal Ministry for Economic Affairs and Energy exists, which has not yet been approved by the government. Only after the latter's approval will the draft start going through the legislative process and be discussed in the Federal Parliament (*Bundestag*) as well as in the Federal Assembly (*Bundesrat*). As of 15 June 2015, this draft has been notified to the European Commission and can now be commented on by the Commission as well as by the member states of the European Union until 16 September 2015.[81]

As regards access providers, the draft plans to add to the already existing § 8 German Telemedia Act inter alia a third paragraph, stating that the reduced civil responsibility of access providers as delineated by Article 12 E-Commerce-Directive and implemented in § 8 paragraphs 1, 2 German Telemedia Act also applies to WLAN-operators.[82] The new paragraph 4 then specifies under which conditions WLAN-operators have fulfilled their due diligence and thus cannot be held liable on the basis of disturbance liability: according to this new paragraph, WLAN-operators[83] providing Internet access have to take reasonable precautionary measures in order to prevent and remove law violations through WLAN-users. The operator has to install reasonable protective measures to stop

---

78 Regional Court (*Landgericht*, LG) München I, decision of 18.09.2014 – 7 O 14719/12.

79 Federal Ministry for Economic Affairs and Energy, Referentenentwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes (Zweites Telemedienänderungsgesetz – 2. TMGÄndG) dated 11.03.2015, not available online anymore.

80 The first draft dates from 11.03.2015. As a reaction to statements from different actors, this draft has been amended by 15.06.2015.

81 Meanwhile, the draft has been approved by the Federal Cabinet, see Federal Ministry for Economic Affairs and Energy, Mehr Rechtssicherheit bei WLAN: Geänderter Gesetzentwurf bringt erhebliche Vereinfachungen, available at http://www.bmwi.de/DE/Themen/Digitale-Welt/Netzpolitik/rechtssicherheit-wlan,did=695334.html (15.07.2015); regarding the procedure of notification see also European Commission, The notification procedure in brief, available at http://ec.europa.eu/growth/tools-databases/tris/en/about-the-9834/the-notification-procedure-in-brief1/ (15.07.2015).

82 "(3) Die vorstehenden Absätze gelten auch für Diensteanbieter nach Absatz 1, die Nutzern einen Internetzugang über ein drahtloses lokales Netzwerk zur Verfügung stellen.", Federal Ministry for Economic Affairs and Energy, Referentenentwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes (Zweites Telemedienänderungsgesetz – 2. TMGÄndG) dated 15.06.2015, available at http://www.bmwi.de/BMWi/Redaktion/PDF/S-T/telemedienaenderungsgesetz-aenderung,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf (16.07.2015), p. 6.

83 In its first version, the draft stated that this only applied to WLAN-operators that were doing this as part of their business (both with and without intention to make profit, such as hotels, Internet-cafés, doctor's offices or sports clubs) or to public institutions (such as libraries, schools, universities, citizen centres recreational facilities). Private WLAN-operators' due diligence was said to consist of the same requirements as business or public operators, but with the additional requirement that they also had to know the person using their WLAN by name; Federal Ministry for Economic Affairs and Energy, Referentenentwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes (Zweites Telemedienänderungsgesetz – 2. TMGÄndG) dated 11.3.2015, not available online anymore, p. 4, 5, 6, 11, 12.

unauthorised persons from using the WLAN and Internet access must only be given to those customers that declare that they will only use the Internet in a lawful way.[84] With a view to remaining neutral to different technologies, the second version of the draft does not specify which protective measure shall be used. The comment to the draft states, however, that specially encrypted routers may be used, such as WPA2-standards.[85]

2.1.2.2. Copyright violations

In the context of claims for injunctive relief for **copyright violations**, various case law exists, stating that **access providers have no duty to block access to these types of infringement**. Since they do not have direct control over the illegal contents, it follows that access providers cannot be treated as offenders or participants of the rights violations. The cases also considered that a requirement that access providers install preventive control measures was unreasonable for technical reasons.[86]

2.2. Take-down/removal of illegal Internet content

An order to take down or remove illegal Internet content generally applies to host providers, since they have the technical possibility to change the content of their specific website.

Orders to take down illegal Internet content are possible based on the law of the different federal states, namely the Interstate Treaties on Broadcasting and Telemedia as well as on the Protection of Minors in the Media.

Under federal law, there are several statutory legal bases for injunctive relief, namely in the fields of copyright, trademark and unfair competition law. Nevertheless, it is important to note that these regulations regard injunctive relief in general and were not designed to specifically deal with Internet content.

As regards orders to take down or remove illegal Internet content on the basis of disturbance liability, there is a range of case law. Although a few general conclusions can be drawn from this case law, the decisions relate to many different aspects and criteria, which vary on a case by case basis. It is thus not possible to present all the existing case law in detail, but only to show the general conclusions and trends.

Conversely, there is almost no case law or commentary dealing with the removal of illegal Internet content in criminal law matters.

2.2.1. Statutory legal basis for a claim

---

84 Federal Ministry for Economic Affairs and Energy, Referentenentwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes (Zweites Telemedienänderungsgesetz – 2. TMGÄndG) dated 15.06.2015, available at http://www.bmwi.de/BMWi/Redaktion/PDF/S-T/telemedienaenderungsgesetz-aenderung,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf (16.07.2015), p. 7.

85 Federal Ministry for Economic Affairs and Energy, Referentenentwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes (*Zweites Telemedienänderungsgesetz* – 2. TMGÄndG) dated 15.06.2015, available at http://www.bmwi.de/BMWi/Redaktion/PDF/S-T/telemedienaenderungsgesetz-aenderung,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf, p. 15.

86 Higher Regional Court (*Oberlandesgericht*, OLG) Frankfurt a.M., decision of 22.01.2008 – 6 W 10/08; Regional Court (*Landgericht*, LG) Düsseldorf, judgement of 13.12.2007 – 12 O 550/07; LG Hamburg, judgement of 12.03.2010 – 308 O 640/08; LG Kiel, judgement of 23.11.2007 – 14 O 125/07.

Currently, **only the law of the different federal states provides a statutory legal basis for blocking illegal Internet content by access providers**. This legal basis can be found in **§ 59 of the Interstate Treaty on Broadcasting and Teleme**dia as well as in **§ 20 of the Interstate Treaty on the Protection of Minors in the Media**, which refers to §59 of the aforementioned treaty. These regulations apply to both host and access providers and have thus already been presented above, under point 2.1.1.

The relevant **legal bases for injunctive relief** against Internet Service Providers are § 97 paragraph 1 German Copyright Act, §§ 14 paragraph 5, 15 paragraph 4 German Trademark Act and § 8 German Unfair Competition Act. In addition to that, the general clause for unlawful acts in § 823 paragraph 1 German Civil Code may be important, especially in conjunction with the general personal right.[87] Judging from the existing case law, copyright infringements seem to be most common.

2.2.1.1. Copyright violations

According to § 97 paragraph 1 German Copyright Act, the only requirement for **injunctive relief due to a copyright violation** is that a person infringes a copyright or any other right protected under the German Copyright Act. These rights have in common that they are all absolute rights and thus enforceable against anyone and everyone.[88] As defined by law, the "[c]opyright protects the author in his intellectual and personal relationships to the work and in respect of the use of the work. It shall also serve to ensure equitable remuneration for the exploitation of the work."[89]
The copyright comprises the right of publication, the recognition of authorship and the distortion of the work as moral rights[90] as well as a range of exploitation rights,[91] namely reproduction, distribution, exhibition, recitation, performance and presentation, making the work available to the public, broadcasting, communication by video or audio recordings and communication of broadcasts and of works made available to the public. In addition to the copyright and the rights it comprehends, the German Copyright Act also protects the authors' access to copies of works, their right to resale as well as their right to remuneration for rental and lending.[92]

A person infringes one of these rights, if (s)he assumes it or exercises it without the author's approval or any other legitimation.[93] The author can seek both removal of an existing violation and restraint from any further infringements if there is shown to be a risk of repetition.[94]

2.2.1.2. Trademark violations

---

87 The general personal right is not expressly regulated, but derives from Art. 1 para. 1 in conjunction with Art. 2 para. 1 German Constitution (*Grundgesetz*, GG).

88 T. Dreier & G. Schulze, Urheberrechtsgesetz, Urheberrechtswahrnehmungsgesetz, Kunsturhebergesetz: Kommentar, 4th ed., München: C.H. Beck 2013, § 97 UrhG, para. 3.

89 § 11 ss. 1, 2 German Copyright Act (*Urhebergesetz*, UrhG).

90 §§ 12-14 German Copyright Act (*Urhebergesetz*, UrhG).

91 § 15 para. 1 N° 1-3, para. 2 ss. 1, 2 N° 1-5 in conjunction with §§ 19-22 German Copyright Act (*Urhebergesetz*, UrhG).

92 §§ 25-27 German Copyright Act (*Urhebergesetz*, UrhG).

93 T. Dreier & G. Schulze, Urheberrechtsgesetz, Urheberrechtswahrnehmungsgesetz, Kunsturhebergesetz: Kommentar, 4th ed., München: C.H. Beck 2013, § 97 UrhG, para. 3.

94 § 97 para. 1 s. 1 German Copyright Act (*Urhebergesetz*, UrhG).

As to **injunctive relief due to a trademark violation**, this can only be claimed for suspected infringements in the future, irrespective whether this will be the first infringement of this kind or a repetitive one.[95] Both trademarks[96] and commercial designations[97] are protected.[98]

Regarding trademarks, the German Trademark Act generally prohibits the unauthorised use within business operations of the following signs: identical signs for goods or services that are for their part identical to those for which the trademark enjoys protection; signs that might, due to their identity or similarity to the trademark and the goods or services covered, confuse the public or lead to an association with the trademark; or identical or similar signs for goods or services that are not identical to those for which the trademark enjoys protection, if the trademark has a reputation in this country and if using this sign without due cause takes unfair advantage of or is detrimental to the character or the esteem of the trademark.[99] The law also names a range of particular acts that shall be prohibited, if one of the named signs is concerned.[100]
Commercial designations are protected in a comparable way by the German Trademark Act: It is thus prohibited to use a commercial designation or a similar sign within business operations without approval in a way that can cause confusion with the protected designation. Furthermore, and if the commercial designation has a reputation in the country, it is also prohibited to use it or a similar sign within business operations insofar as its use without due cause takes unfair advantage of, or is detrimental to, the character or the esteem of the commercial designation.[101]

2.2.1.3. Unfair competition

§ 8 German Unfair Competition Act simply states that **injunctive relief against unfair commercial practices** is possible regarding both removing the violation and refraining from recurring or imminent violations in the future. Generally speaking, unfair commercial practices are illegal, if they can distinctly affect the interests of competitors, consumers or other market actors. Commercial practices by an entrepreneur towards a consumer are also illegal, if the entrepreneur: acted negligently; if the practices can distinctly affect the consumer's ability to take her/his decision based

---

95 § 14 para. 5 ss. 1, 2, § 15 para. 4 ss. 1, 2 German Trademark Act (*Markengesetz*, MarkenG).

96 § 14 German Trademark Act (*Markengesetz*, MarkenG).

97 § 15 German Trademark Act (*Markengesetz*, MarkenG).

98 The German Trademark Act (*Markengesetz*, MarkenG) also protects indications of geographical origin, which are however not relevant in the context of this report.

99 § 14 para. 2 N° 1-3 German Trademark Act (*Markengesetz*, MarkenG).

100 "(1) [A]ffix[ing] the sign to goods or their wrappings or packaging; offering goods under the sign, to put them on the market or to stock them for the above purposes; (2) […] offer[ing] or provid[ing] services under the sign; […] import[ing] or export[ing] goods under the sign; (3) us[ing] the sign in business papers or in advertising", § 14 para. 3 N° 1-5 German Trademark Act (*Markengesetz*, MarkenG). Additionally, it is also prohibited, without the rights holder's authorization and within business operations, "if the danger exists that the wrappings or packaging are used to wrap or package or that the means of identification are used to identify goods or services with regard to which third parties would be prohibited from using the sign in accordance with paras. 2 and 3, (1) to affix a sign that is identical to the trademark or a similar sign on wrappings or packaging or on means of identification such as labels, tags, badges or the like; (2) to offer, put on the market or stock for the listed purposes wrappings, packaging or means of identification which bear a sign that is identical to the trademark or to a similar sign; or (3) to import or export wrappings, packaging or means of identification which bear a sign that is identical to the trademark or to a similar sign", § 14 para. 4 N° 1-3 German Trademark Act (*Markengesetz*, MarkenG).

101 § 15 paras. 2, 3 German Trademark Act (*Markengesetz*, MarkenG).

on information; and, if the practice can lead the consumer to a business decision (s)he would not have taken without this commercial practice.[102] The act lists a broad range of examples of unfair commercial practices,[103] which also constitute misleading commercial practices,[104] comparative advertising[105] and unacceptable nuisance.[106]

However, with regard to a host provider's responsibility, German **competition law provides of a particularity**. According to the jurisprudence, the Internet Service Provider acts as an offender of an anticompetitive practice and not merely as a participant to it. The courts have argued that it constitutes an infringement of the Unfair Competition Act if a person neglects her/his due diligence. This due diligence is defined in § 3 Unfair Competition Act, namely that every party creating an economic source of danger has to take every adequate and appropriate precautionary measures in order to protect their competitor's economic interests as much as possible.[107] As a consequence, host providers are directly liable if they do not remove anticompetitive content despite having knowledge of such infringements.[108]

2.2.2. Disturbance Liability

In order to limit the rather broad liability granted by **disturbance liability,**[109] the jurisprudence tries to develop certain **criteria, although these vary significantly from case to case**.[110] Generally speaking, these criteria can be summarised as follows: the host provider has to have a **duty of care to check the contents** and this **duty has to be defined in each particular case**.[111] This duty must be one that can **reasonably be expected of the respective provider**.[112] As a general rule one can say that the standard of how a host provider muat check the allegedly illegal content increases with the amount of concrete information it has, indicating that a right is being violated.[113] As already mentioned, there

---

102 § 3 paras. 1, 2 German Unfair Competition Act (*Gesetz gegen den unlauteren Wettbewerb*, UWG).

103 § 4 German Unfair Competition Act (*Gesetz gegen den unlauteren Wettbewerb*, UWG).

104 §§ 5, 5a German Unfair Competition Act (*Gesetz gegen den unlauteren Wettbewerb*, UWG).

105 § 6 German Unfair Competition Act (*Gesetz gegen den unlauteren Wettbewerb*, UWG).

106 § 7 German Unfair Competition Act (*Gesetz gegen den unlauteren Wettbewerb*, UWG).

107 German Federal Court of Justice (*Bundesgerichtshof*, BGH), judgement of 12.07.2007 – I ZR 18/04 (*jugendgefährdende Medien bei eBay*).

108 H. Hören & S. Yankova, The Liability of Internet Intermediaries – The German Perspective, in International Review of Intellectual Property and Competition Law (IIC) 2012, p. 501 *et seq*, p. 523 *et seq*.

109 See point 2. of this report on German law.

110 A. Ohly, Die Verantwortlichkeit von Intermediären, in Zeitschrift für Urheber- und Medienrecht (ZUM) 2015, p. 308, p. 312.

111 German Federal Court of Justice (*Bundesgerichtshof*, BGH), judgement of 17.05.2001 – I ZR 251/99; BGH, judgement of 22.07.2010 – I ZR 139/08; BGH, judgement of 25.10.2011 – VI ZR 93/10.

112 See also J. Ensthaler & M. Heinemann, Die Fortentwicklung der Providerhaftung durch die Rechtsprechung, in Gewerblicher Rechtsschutz und Urheberrecht (GRUR) 2012, p. 433, p. 436 *et seq*.

113 H. Hören & S. Yankova, The Liability of Internet Intermediaries – The German Perspective, in International Review of Intellectual Property and Competition Law (IIC) 2012, p. 501 *et seq*, p. 504 *et seq*. See also German Federal Court of Justice (*Bundesgerichtshof*, BGH), judgement of 12.07.2012 – I ZR 18/11 (*Alone in the Dark*) and BGH, judgement of 15.08.2013 – I ZR 80/12 (*RapidShare*) as well as Freedom House, Freedom on the Net 2014: Germany, available at https://freedomhouse.org/sites/default/files/resources/Germany.pdf (21.07.2015), p. 10. Based on case law available until 2008, Wilmer has developed a matrix with different levels of the duty of care: T. Wilmer, Überspannte Prüfpflichten für Host-Provider? Vorschlag für eine Haftungsmatrix, in Neue Juristische Wochenschrift

is no general duty for Internet Service Providers to check all content.[114] However, there can be a duty to prevent easily detectable infringements in the future.[115]

2.2.2.1. Hyperlinks

Regarding responsibility in connection with **hyperlinks**, the German Federal Court of Justice has ruled that hyperlinks to copyrighted works do not constitute an infringement of copyright. According to the court, the rights holder has implied her/his consent to using her/his works by not taking any precautionary technical measures against this use.[116] In contrast to this, the Higher Regional Court Munich considered it an infringement that an article on new software for copying DVDs also included a direct hyperlink to the producer of this software. In the context of this article, the court found that the link considerably facilitated the search for this illegal content and that as a consequence, disturbance liability applied.[117] Nevertheless, the German Federal Court of Justice disagreed and argued that the article's content was protected by the freedom of the press[118].[119]

2.2.2.2. Search engines

As regards the responsibility of **search engines**, a change in the German jurisprudence seems to be taking place. Since the European Court of Justice's *Google France*-decision, neutral search engines that have no knowledge of, or no control over, the stored data will probably be treated as host providers in the future and will thus be responsible in only a limited way.[120] There is, however, a particularity concerning the **autocomplete-function**. If the search engine uses a specific algorithm to suggest other keywords when typing in a search item, then this creates a duty for the search engine's operator to check these suggested keywords. The German Federal Court of Justice argues that the algorithm represents a content owned or at least adopted by the search engine's operator. Yet, this duty to check the keywords only applies as soon as the operator has knowledge of the illegality of the suggested keywords.[121] This duty is particularly relevant in cases where the infringement regards a person's personal right.[122]

(NJW) 2008, p. 1845, p. 1850.

114 § 7 para. 2 s. 1 German Telemedia Act (*Telemediengesetz*, TMG); Higher Regional Court (*Oberlandesgericht*, OLG) Hamburg, judgement of 01.07.2015 – 5 U 87/12 and 5 U 175/10.

115 German Federal Court of Justice (*Bundesgerichtshof*, BGH), judgement of 15.10.1998 – I ZR 120/96.

116 German Federal Court of Justice (*Bundesgerichtshof*, BGH), judgement of 17.07.2003 – I ZR 259/00 (*Paperboy*).

117 Higher Regional Court (*Oberlandesgericht*, OLG) München, judgement of 28.07.2005 – 29 U 2887/05 (*AnyDVD*).

118 Art. 5 para. 1 s. 2 German Constitution (*Grundgesetz*, GG).

119 German Federal Court of Justice (*Bundesgerichtshof*, BGH), judgement of 20.10.2010 – I ZR 191/08 (*AnyDVD*).

120 German Federal Court (*Bundesgerichtshof*, BGH), judgement of 29.04.2010 – I ZR 69/08 (*Vorschaubilder I*); BGH, judgement of 19.10.2011 – I ZR 140/10 (*Vorschaubilder II*); H. Hören & S. Yankova, The Liability of Internet Intermediaries – The German Perspective, in International Review of Intellectual Property and Competition Law (IIC) 2012, p. 501 *et seq*, p. 515.

121 German Federal Court of Justice (*Bundesgerichtshof*, BGH), judgement of 14.05.2013 – VI ZR 269/12 (*Autocomplete*).

122 H. Hören, in: W. Kilian & B. Heussen (eds.), Computerrechts-Handbuch: Informationstechnologie in der Rechts- und Wirtschaftspraxis, 32. ed., München: C.H. Beck 2013, part 14, Vertragsrechtliche Fragen, para. 30.

2.2.2.3. Unfair competition

In **competition law, it is not clear whether disturbance liability is applicable at all**, since competition law itself is part of the law of unlawful acts. Hence, specific rules of conduct apply within the scope of acts relating to business. Consequently, the jurisprudence seems to avoid applying the rules of disturbance liability in cases with regard to competition law. In lieu thereof, it increasingly treats the provider as a direct offender.[123] Still, there is not yet an explicit decision stating that disturbance liability shall not be applicable in competition law cases.

2.2.3. Criminal law

As regards criminal law, it is not quite clear how a **court can proceed after having convicted a person for a criminal offense committed through illegal Internet content,** such as dissemination of pornography to minors,[124] depictions of violence[125] or propaganda material of unconstitutional organisations.[126] The law is not clear on this matter and both case law and comments on this aspects are scarce. According to § 74d German Criminal Code,[127] unlawful written materials including the equipment to produce them shall be subject of deprivation. The norm also refers to § 11 German Criminal Code, according to which "[a]udiovisual media, data storage media, illustrations and other depictions shall be equivalent to written material".[128] The question is whether Internet content can be classified as any of these terms. In its introductory statement to the respective amendment of § 11 German Criminal Code, the parliament (*Bundestag*) states with regard to the term "data storage media" (*Datenspeicher*) that also electronic, electromagnetic, optic, chemical or other data storage media embodying notional contents, which are only perceivable with the help of technical instruments such as a screen, shall be equivalent to written material. As a consequence, the parliament goes on, contents of both data carriers like magnetic tape, hard drive or CD-ROMS and electronic working storage shall be data storage media within the scope of § 11 paragraph 3 German Criminal Code.[129] The German Federal Court of Justice interpreted this explanation such that digitalised photographs uploaded on the Internet are data storage media within this scope. The court

---

123 See point 2.2.1. of this report on German law.

124 § 184 German Criminal Code (*Strafgesetzbuch*, StGB), available at http://www.gesetze-im-Internet.de/stgb/index.html (20.04.2015).

125 § 131 German Criminal Code (*Strafgesetzbuch*, StGB).

126 § 86 German Criminal Code (*Strafgesetzbuch*, StGB).

127 § 74d para. 1 ss. 1, 2 German Criminal Code (*Strafgesetzbuch*, StGB).

128 § 11 German Criminal Code (Strafgesetzbuch, StGB):
"(3) Den Schriften stehen Ton- und Bildträger, Datenspeicher, Abbildungen und andere Darstellungen in denjenigen Vorschriften gleich, die auf diesen Absatz verweisen."

129 "[Es] ist klarzustellen, dass auch elektronische, elektromagnetische, optische, chemische oder sonstige Datenspeicher, die gedankliche Inhalte verkörpern, die nur unter Zuhilfenahme technischer Geräte wahrnehmbar werden, den Schriften gleichstehen. Sie können in vergleichbarer Weise zur Wiedergabe rechtswidriger Inhalte verwendet werden und sind daher in das strafrechtliche System einzubeziehen. Gleichgültig ist dabei, welcher Art das zur Wahrnehmbarmachung eingesetzte Gerät ist; in Betracht kommt insbesondere die Anzeige auf einem Bildschirm. Die Klarstellung erfasst damit sowohl Inhalte in Datenträgern (Magnetbänder, Festplatten, CD-ROMs u.a.) als auch in elektronischen Arbeitsspeichern, welche die Inhalte nur vorübergehend bereithalten.", Deutscher Bundestag, printed paper (*Drucksache*) 13/7385 of 09.04.1997, *Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienstegesetz, IuKDG)*, p. 36.

clarifies that these photographs are "data stored on a storage medium – mostly the hard drive of a server."[130]

Yet, comments and case law on the definition of the term "data storage media" in § 11 German Criminal Code generally discuss the topic with regard to elements of a crime as for example dissemination of pornography to minors,[131] as was the case in the German Federal Court of Justice's decision just mentioned. Our research revealed only one case in which deprivation of illegal Internet content according to § 74d German Criminal Code, or any other norm, is concerned. In this decision, the Regional Court Hamburg cites the German Court of Justice's clarification and applies it to scans of documents that were made available online and thus digitalised.[132] However, even if illegal content whose dissemination on the Internet constitutes a crime is considered data storage media within the scope of § 11[133] and thus also § 74d German Criminal Code,[134] only those pieces in the perpetrator's possession or in the possession of a person whose business it is to take part in the dissemination can be subject to deprivation.[135] This can for example be the author, a print office, the publisher or a bookseller.[136] There is no case law or literature available to us discussing the question of whether Internet Service Providers of any kind should be part of this exception. The previously mentioned decision by the Regional Court of Hamburg does not deal with exactly this paragraph of § 74d German Criminal Code and is not readily comparable with cases of illegal Internet content.[137] Additionally, another paragraph of § 74d German Criminal Code provides that "[d]issemination […] shall also mean providing access […] or at least one copy of it to the public by putting it on display, putting up posters, performances or other means."[138] Dissemination of the content itselfis the relevant issue.[139] Under specific circumstances, Internet Service Providers may thus be deemed to be involved in the dissemination of the illegal content with the consequence that § 74d German Criminal Code on deprivation of publication media applies.

---

130 "Digitalisierte Fotos, die ins Internet gestellt werden, sind Datenspeicher i[m Sinne des § 11 Abs. 3 StGB); genauer: auf einem Speichermedium – in der Regel der Festplatte des Servers – gespeicherte Daten", German Federal Court of Justice (*Bundesgerichtshof*, BGH), judgement of 27.06.2001 – 1 StR 66/01.

131 § 184 German Criminal Code (*Strafgesetzbuch*, StGB).

132 Regional Court (*Landgericht*, LG) Hamburg, decision of 02.09.2013 – 629 Qs 34/13 (*Fall Mollath*).

133 § 11 para. 3 German Criminal Code (*Strafgesetzbuch*, StGB).

134 § 74d para 1 German Criminal Code (*Strafgesetzbuch*, StGB).

135 § 74d para. 2 German Criminal Code (*Strafgesetzbuch*, StGB).

136 The law only states that the person has to be "involved" in the dissemination. Yet, the commentary on this norm specifies that it has to be part of the business of this person to take part in the dissemination, as for example the case for the author, a print office, the publisher or a bookseller, F. Herzog & F. Saliger, in U. Kindhäuser *et al.* (eds.), Strafgesetzbuch, 4th ed., Baden-Baden: Nomos 2013, § 74d, para. 10; W. Joecks, in: W. Joecks & K. Miebach (eds.), Münchener Kommentar zum StGB: Band 2 §§ 38-79b StGB, 2nd ed., München: C.H. Beck 2012, § 74d, para. 16; A. Eser, in: A. Schönke & H. Schröder (eds.), *Strafgesetzbuch: Kommentar*, 29th ed., München: C.H. Beck 2014, § 74d, para. 9.

137 In the case decided by the court, not § 74d para. 2 German Criminal Code is relevant, but, rather, para. 3 s. 2 N° 1, according to which only those pieces which are in the possession of a perpetrator or participant of the actual offence can be the subject of deprivation ("Die Einziehung oder Unbrauchbarmachung werden jedoch nur angeordnet, wenn 1. die Stücke und die in Absatz 1 Satz 2 bezeichneten Gegenstände sich im Besitz des Täters, des Teilnehmers oder eines anderen befinden, für den der Täter oder Teilnehmer gehandelt hat, oder von diesen Personen zur Verbreitung bestimmt sind […].")

138 § 74d para. 4 German Criminal Code (*Strafgesetzbuch*, StGB).

139 W. Joecks, in: W. Joecks & K. Miebach (eds.), Münchener Kommentar zum StGB: Band 2 §§ 38-79b StGB, 2nd ed., München: C.H. Beck 2012, § 74d, para. 10.

3. Procedural Aspects

3.1. Court order

In Germany, there is **no specific law on blocking, filtering or taking down illegal Internet content at the federal level**. Currently, the only way to order a host provider to take down/remove, or to order an access provider to filter/block illegal Internet content at the federal level is a **court decision on injunctive relief**. These cases concern **private law disputes**, mostly regarding trademark law, copyright law, unfair competition law or the general private right.[140] Since there are no special laws on the responsibility of Internet Service Providers, the **general rules apply**. In this context, these are the regulations in the German Civil Procedure Code (*Zivilprozessordnung*, ZPO).[141]

As soon as the judge or the tribunal's chairman has **rendered the decision** that the Internet provider as the losing party must take down or block illegal Internet content, the respective provider is obliged to do so.[142] The court's decision will be served to the parties; if it is a judgement in absence, only the losing party will be served.[143] If the matter in dispute is worth more than 600 EUR or if the court of first instance has accepted this,[144] the losing party can **appeal (*Berufung*)** a final judgement (*Endurteil*)[145] on questions of fact or of law.[146] The party filing the appeal must do so within one month counting from service of the complete judgement including its reasons, or at the latest five months after rendition of judgement.[147] If the Internet Service Provider also loses in this second instance, it can appeal this second decision, but only on questions of law **(*Revision*)**[148] and only if the court of second instance[149] accepts this appeal.[150] This will be the case if the respective question of law is of general importance or if a decision by a higher instance is necessary in order to establish a stable jurisprudence.[151] Again, the party filing the appeal must do so within one month counting from service of the complete judgement in the second instance, or at the latest five months after rendition of this second judgement.[152] In specific circumstances, the party losing in the first instance can also skip the appeal to the second instance (*Berufung*) and appeal directly on questions of law only (*Revision*).[153]

---

140 See point 2. and especially point 2.2. of this report on German law.

141 Available at http://www.gesetze-im-Internet.de/zpo/index.html (20.04.2015).

142 § 311 para. 2 S. 1 in conjunction with § 300 para. 1, § 325 para. 1 and § 136 para. 4 German Civil Procedure Code (*Zivilprozessordnung*, ZPO).

143 § 317 para. 1 s. 1 German Civil Procedure Code (*Zivilprozessordnung*, ZPO).

144 § 511 para. 2 N° 1, 2 German Civil Procedure Code (*Zivilprozessordnung*, ZPO).

145 § 300 German Civil Procedure Code (*Zivilprozessordnung*, ZPO).

146 § 513 para. 1 in conjunction with § 529 and/or § 546 German Civil Procedure Code (*Zivilprozessordnung*, ZPO).

147 § 517 German Civil Procedure Code (*Zivilprozessordnung*, ZPO).

148 § 545 para. 1 German Civil Procedure Code (*Zivilprozessordnung*, ZPO).

149 Or the court of third instance upon appeal against the court of second instance's decision, not to accept the new appeal, § 543 para. 1 N° 2 German Civil Procedure Code (*Zivilprozessordnung*, ZPO).

150 § 543 para. 1 N° 1 German Civil Procedure Code (*Zivilprozessordnung*, ZPO).

151 § 543 para. 2 s. 1 N° 1, 2 German Civil Procedure Code (*Zivilprozessordnung*, ZPO).

152 § 548 German Civil Procedure Code (*Zivilprozessordnung*, ZPO).

153 See for details § 566 German Civil Procedure Code (*Zivilprozessordnung*, ZPO).

In the event that the Internet Service Provider as the losing party **does not comply with the court order** to remove or block illegal Internet content and to filter similar infringements in the future, it will be required to pay an administrative fine for each violation of this order, generally with a maximum total of 250'000 EUR. As an alternative to this administrative fine, the Internet Service Provider can also be arrested for contempt of court, for up to six months for each violation, with a total maximum of two years.[154] It will also be convicted of contempt of court if an administrative fine was imposed on the provider, but the latter did not pay.[155]

3.2. State Media Authorities

Orders to block or take down illegal Internet content based on the Interstate Treaties on Broadcasting and Telemedia as well as on the Protection of Minors in the Media are given by the **State Media Authority of the respective country**. If the order regards matters of **protection of minors** in the media, the order is given by the State Media Authority, but it is the **German Commission for the Protection of Minors in the Media that takes the decision**. Neither of the two Interstate Treaties regulates the decision-making or review procedure. The aforesaid Commission however explains its decision-making process on its website. According to this information, **examining boards** investigate every individual case for potential violations of the Interstate Treaty on the Protection of Minors in the Media. Each board consists of a director of a State Media Authority, a delegate of the Supreme Youth Authorities of the federal states as well as a representative of the Federal Supreme Youth Authority. In case of breach of the provisions of the treaty, the boards decide how to prosecute and how to impose fines for administrative offences. Which measure the board will decide to take depends upon the severity of the violation. The following **sanctions** are possible:

- Complaint against the content provider
- Prohibition against the content provider
- Blocking requirement against the host or access provider
- Blocking against the host or access provider
- Administrative offence: Fining
- Criminal offence: issue is handed over to the State Prosecutor.

The Commission's examining board will then give its decision to the competent **State Media Authority who will implement the decision**. These measures are **administrative acts** as defined by § 35 Administrative Procedures Act.[156] As a consequence, the addressee can file an **objection** in writing within one month.[157] In case the authority refuses to change its decision, the addressee can, again in writing and within one month, file **action for rescission at the administrative court**, claiming that the administrative act is unlawful and that the addressee's rights have thereby been violated.[158]

---

154 Regional Court (*Landgericht*, LG) Hamburg, judgement of 31.07.2009 – 325 O 85/09; LG Hamburg, decision of 25.11.2010 – 310 O 433/10; with a maximum of 250'000 EUR for each violation and without any total maximum for the administrative fine or for the arrest LG Düsseldorf, judgment of 23.05.2007 – 12 O 151/07.

155 See § 888 para. 1 s. 1 German Civil Procedure Code (*Zivilprozessordnung*, ZPO).

156 § 35 s. 1 Administrative Procedures Act.

157 § 79 para. 1 s. 1 Administrative Court Procedure Code (*Verwaltungsgerichtsordnung*, VwGO).

158 § 80 para. 1 s. 1 in conjunction with § 113 para. 1 s. 1 Administrative Court Procedure Code (*Verwaltungsgerichtsordnung*, VwGO).

The same administrative procedure applies to decisions by the different State Media Authorities based on the Interstate Treaty on Broadcasting and Telemedia, as these decisions also constitute administrative acts.

4. General monitoring of Internet

In Germany, the **Federal Criminal Police Office (*Bundeskriminalamt*, BKA)** acting as a **Central Authority for Event-unrelated Research in Data Networks (*Zentralstelle für anlassunabhängige Recherchen in Datennetzen*, ZaRD)** is the competent authority for monitoring Internet content.[159]

However, the aim of this monitoring is **not to block illegal Internet content, but to detect criminal offences** and refer the information to the respective police station for further investigation. This is based on its general competence and task to support the local and regional police in interregional, international or particularly important matters.[160] The Central Authority does not have the right to conduct research related to specific information or hints, since this would violate the constitutionally protected freedom of expression.[161] As a result, it is only permitted to search publicly accessible data without relation to any specific event.[162] It is therefore not possible to contact the Central Authority in case a person becomes aware of illegal Internet content. For example, regarding child pornography, the Federal Criminal Police Office instead advises people to contact the local police office, prosecution or Criminal Police Office of the respective *Bundesland*.[163] The Central Authority is neither competent to conduct undercover investigation or comparable measures nor to circumvent access restrictions through specific technical measures. Yet, it has the right to obtain personal data from Internet Service Providers on the basis of a general right to ask public and other actors for information, if it needs this information for its research as the Central Authority[164].[165] In order to obtain inventory data such as name, address or bank details as well as connection data recorded by Internet Service Providers, the Central Authority can act on the basis of the German Telecommunication Act (*Telekommunikationsgesetz*, TKG)[166].[167] This act obliges telecommunication

---

159 Bundeskriminalamt, ZaRD - Instrument zur Bekämpfung der IuK-Kriminalität (IuK = Informations- und Kommunikationstechnik), available at http://www.bka.de/nn_205994/DE/ThemenABisZ/Deliktsbereiche/InternetKriminalitaet/InternetrechercheZaRD/zard__node.html?__nnn=true (16.04.2015).

160 § 2 para. 1 German Federal Criminal Police Office Act (*Bundeskriminalamtgesetz*, BKAG).

161 Art. 5 para. 1 s. 1 German Constitution (*Grundgesetz*, GG).

162 Bundeskriminalamt, Die Rechtsgrundlagen, available at http://www.bka.de/nn_205188/DE/ThemenABisZ/Deliktsbereiche/InternetKriminalitaet/InternetrechercheZaRD/zard__node.html?__nnn=true#doc204436bodyText2 (16.04.2015).

163 Bundeskriminalamt, Was mache ich, wenn ich Kinder-/Jugend-/Tierpornographie auf einer Internetseite entdeckt habe?, available at http://www.bka.de/nn_204512/DE/ThemenABisZ/HaeufigGestellteFragenFAQ/Kinderpornographie/kinderpornographieFrage09.html (16.04.2015).

164 § 7 para. 2 German Federal Criminal Police Office Act (*Bundeskriminalamtgesetz*, BKAG).

165 Bundeskriminalamt, Die Rechtsgrundlagen, available at http://www.bka.de/nn_205188/DE/ThemenABisZ/Deliktsbereiche/InternetKriminalitaet/InternetrechercheZaRD/zard__node.html?__nnn=true#doc204436bodyText2 (16.04.2015).

166 Available at http://www.gesetze-im-Internet.de/tkg_2004/index.html (20.04.2015).

167 Bundeskriminalamt, Die Beweiserhebung, available at http://www.bka.de/nn_205188/DE/ThemenABisZ/Deliktsbereiche/InternetKriminalitaet/InternetrechercheZaRD/zard__node.html?__nnn=true#doc204436bodyText4 (16.04.2015).

services and thus also Internet Service Providers[168] to provide law enforcement agencies with the relevant information in order to prosecute a criminal offence or to prevent unlawful acts.[169]

In addition, and with regard to removing or blocking illegal Internet content, a privately run but subsidised **Internet Complaint Office (*Internet-Beschwerdestelle*)** exists. This is a single non-governmental contact point for Internet users to report illegal and harmful content and activities online (particularly content related to youth media protection). It is run by two private initiatives, namely the Voluntary Self-Monitoring of Multimedia Service Providers (*Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V.*, FSM),[170] dealing with content that is illegal and harmful to young people, and the eco Association of the German Internet Industry (*eco Verband der deutschen Internetwirtschaft e.V.*),[171] handling any other illegal Internet content. The Internet Complaint Office is part of the Safer Internet Programme initiated by the European Union in 1999 and of the respective network of so-called Safer Internet Centres in 26 European countries.[172] Any person can file a complaint with the Internet Complaint Office, which will be dealt with by one of the two participating organisations according to their respective areas of expertise.[173] The respective organisation will then investigate and verify whether the reported content is actually illegal. If this is the case, the organisation will inform the content or host provider, who then generally will remove the illegal content on its own initiative, normally at the latest within a week and often as soon as the next working day.[174] The Voluntary Self-Monitoring of Multimedia Service Providers will publish some of those decisions taken not directly by the hotline, but by the board of complaint in an anonymised form on its website.[175] In case the content is not only illegal, but constitutes a criminal law offense, the two organisations will inform the Federal Criminal Police Office[176] or any other competent authority.[177] Illegal Internet content by Internet Service Providers from abroad will be forwarded to a

---

168 If they provide their service for remuneration, § 3 N° 24 German Telecommunication Act (*Telekommunikationsgesetz*, TKG).

169 § 113 para. 1 s. 1, para. 2 s. 1, para. 3 N° 1 German Telecommunication Act (*Telekommunikationsgesetz*, TKG).

170 Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V., FSM welcome, available at http://www.fsm.de/en?set_language=en (17.07.2015).

171 eco Verband der deutschen Internetwirtschaft e.V., About eco, available at https://international.eco.de/about.html (17.07.2015).

172 Internet-Beschwerdestelle, The "Safer Internet Program" of the EU, available at http://www.Internet-beschwerdestelle.de/en/international/siap/index.htm (17.07.2015).

173 Internet-Beschwerdestelle, How to submit your complaint, available at http://www.Internet-beschwerdestelle.de/en/complaint/submit/index.htm and Complaints Procedure, available at http://www.Internet-beschwerdestelle.de/en/complaint/procedure/index.htm (both 17.07.2015).

174 eco Verband der deutschen Internetwirtschaft e.V., Statistik, available at https://www.eco.de/services/Internet-beschwerdestelle/statistik.html (17.07.2015).

175 § 12 s. 1 Complaint Rules for the Association Freiwillige Selbstkontrolle Multimedia e.V., available at http://www.fsm.de/about-us/FSM-Complaint_Rules.pdf (20.07.2015); for a list of some of these decisions see Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V., Beschwerdestelle: Entscheidungen aus der Praxis, available at http://www.fsm.de/beschwerdestelle/praxisentscheidungen (20.07.2015).

176 Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V., Beschwerdestelle: Was passiert mit meiner Beschwerde?, available at http://www.fsm.de/hotline/complaints-procedure?set_language=en (20.07.2015).

177 eco Verband der deutschen Internetwirtschaft e.V., eco Internet-Beschwerdestelle, available at https://www.eco.de/services/Internet-beschwerdestelle.html (20.07.2015).

partner organisation through the umbrella organisation INHOPE, comprising 51 hotlines in 45 countries worldwide[178].[179]

The Voluntary Self-Monitoring of Multimedia Service Providers also provides a Code of Conduct, to which there are currently 35 members[180] plus four associated members[181] and three sponsoring members[182].[183] Regarding the members of this Code of Conduct, the organisation provides for a complaint procedure in different, escalating, steps: once the organisation has checked the content and found it to be illegal, it will, depending on the gravity of the infringement, (1) request the member to remove the illegal Internet content, (2) reprimand the member, (3) impose an association penalty on the member, or (4) exclude the member from the association. In case of non-observance of the respective measure, the organisation will take the next measure in this list.[184] Out of the decisions published on the website of the Voluntary Self-Monitoring of Multimedia Service Providers, for three of them it is not clear whether the Internet Service Providers were signatories of the Code of Conduct,[185] all other decisions state explicitly that they do not concern a signatories of the Code of Conduct.

5. Assessment as to the case law of the European Court of Human Rights

Under German law, no specific law on blocking, filtering or removing illegal Internet content exists at the federal level. As a consequence, it is not possible to assess whether the safeguards for freedom of expression are respected in this regard. At the moment, it is only possible to take action against illegal Internet content on the basis of disturbance liability. This is based on the concept of nuisance to corporeal property, or on the basis of the general regulations on injunctive relief in copyright law, trademark law and unfair competition law. **These legal bases were not designed for matters of**

178 INHOPE, at a glance, available at http://www.inhope.org/gns/who-we-are/at-a-glance.aspx (17.07.2015).

179 Internet-Beschwerdestelle, Content from abroad, available at http://www.Internet-beschwerdestelle.de/en/complaint/abroad/index.htm (17.07.2015).

180 Autentic GmbH, Cybits AG, Deutsche Telekom AG, Deutsche Telekom Medien GmbH, Discovery Communications Deutschland GmbH & Co. KG, Edict GmbH, E-Plus Mobilfunk GmbH & Co.KG, Google Inc., IAC Search & Media Europe Ltd., Inter Publish GmbH, Kabel Deutschland Vertrieb und Service GmbH, Knuddels GmbH & Co. KG, Lokalisten media GmbH, Lotto24 AG, maxdome GmbH & Co. KG, MovieStarPlanet ApS, MSN/Microsoft Deutschland GmbH, PMS Interactive GmbH, ProSiebenSat.1 Digital GmbH, RTL 2 Fernsehen GmbH & Co. KG, RTL Disney Fernsehen GmbH & Co. KG, RTL interactive GmbH, Scoyo GmbH, Searchteq GmbH, Sky Deutschland Fernsehen GmbH & Co. KG, SPORT1 GmbH, Tele 5 TM-TV GmbH, Telefónica Germany GmbH & Co. OHG, Telekom Deutschland GmbH, The Walt Disney Company (Germany) GmbH, VIMN Germany GmbH, Vodafone D2 GmbH, wer-kennt-wen.de GmbH, Yahoo! Deutschland GmbH, ZEAL NETWORK SE.

181 Antenne Thüringen GmbH & Co. KG, Bettermarks GmbH, Sofort AG, vebidoo GmbH.

182 Bundesverband Digitale Wirtschaft e.V., Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien e.V., Verband Privater Rundfunk und Telemedien e.V.

183 Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V., About us: Members, available at http://www.fsm.de/about-us/membership/members (20.07.2015).

184 § 11 paras. 4 *et seq* Complaint Rules for the Association Freiwillige Selbstkontrolle Multimedia e.V., available at http://www.fsm.de/about-us/FSM-Complaint_Rules.pdf (20.07.2015).

185 Decision 02205, available at http://www.fsm.de/beschwerdestelle/praxisentscheidungen/Entscheidung_Prostitutionsangebot.pdf, decision 355-2003, available at http://www.fsm.de/beschwerdestelle/praxisentscheidungen/Entscheidung_FKKBilder.pdf, decision 763-2003, available at http://www.fsm.de/beschwerdestelle/praxisentscheidungen/Entscheidung_Abtreibungsgegner.pdf (all 20.07.2015).

freedom of expression on the Internet. Although host providers can be ordered to filter or take down illegal Internet content if the preconditions of the aforementioned bases are fulfilled, access providers cannot generally be ordered to block illegal Internet content. This is only possible regarding access providers in the broader sense, namely WLAN operators.

However, the sixteen **federal states** have adopted the **Interstate Treaties on Broadcasting and Telemedia as well as on the Protection of Minors in the Media**. The former treaty **explicitly allows for blocking orders against host and access provider** and the latter treaty refers to this provision.

As a signatory of the **European Convention on Human Rights**, general safeguards on freedom of expression apply, including in the field of Internet. The European Convention on Human Rights names different preconditions under which the **freedom of expression can be restricted**[186] and the European Court of Human Rights has elaborated on these preconditions. According to Article 10 of the Convention, restricting the freedom of expression is only possible on a legal basis that has to pursue a legitimate goal. In addition to that, the restriction has to be necessary in a democratic society.

5.1. Legal basis

Article 10 paragraph 2 European Convention on Human Rights states that any restriction must be "prescribed by law". In general, this means that a **written law, enacted by the parliament** must exist in order to guarantee the regulation's **accessibility** to the public.[187] The question is, whether this is the case for German orders to block, filter or remove illegal Internet content. The regulations on injunctive relief in copyright law, trademark law and unfair competition law are laws enacted by the German parliament (*Bundestag*)[188] and hence fulfil this criteria. The same is true for the provisions of the Interstate Treaties on Broadcasting and Telemedia as well as on the Protection of Minors in the Media, which have both been ratified by law and thus enacted by the respective states parliaments (*Landtag*) in all sixteen federal states. The notion of disturbance liability however has been developed by the jurisprudence in its case law. Disturbance liability is based on § 1004 German Civil Code and the European Court of Human Rights has repeatedly confirmed that the "impugned measure should have a basis in domestic law".[189] Yet, it is necessary to apply § 1004 of the German Civil Code by analogy, since the norm itself only refers to corporeal property and not intellectual property.[190] In addition, the courts have had to develop certain criteria in order to apply the notion of

---

186 Art. 10 para. 2 European Convention on Human Rights (ECHR).

187 M. Macovei, Freedom of expression: A guide to the implementation of Article 10 of the European Convention on Human Rights, Council of Europe 2001, 2004, p. 32.

188 Gesetz über das Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz), Bundesgesetzblatt (BGBl.) Part I 1965, p. 1273 *et seq*; Gesetz zur Reform des Markenrechts und zur Umsetzung der Ersten Richtlinie 89/104/EWG des Rates vom 21. Dezember 1988 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über die Marken (Markenrechtsreformgesetz), BGBl. Part I 1994, p. 3082 *et seq*; Bekanntmachung der Neufassung des Gesetzes gegen den unlauteren Wettbewerb, BGBl. Part I 2010, p. 254 *et seq*.

189 See for example European Court of Human Rights, Leyla Şahin v. Turkey, judgement of 10.11.2005, application N° 44774/98.

190 P. Bassenge, in: O. Palandt (ed.), Bürgerliches Gesetzbuch, 74th ed., München: C.H. Beck 2015, § 1004, para. 4.

this claim for injunctive relief due to nuisance to illegal Internet content.[191] Although the European Court of Human Rights has, in particular cases, considered common-law rules to be sufficient as legal basis within the scope of Article 10 of the Convention,[192] this exceptional rule is probably not applicable to German case law. In general, jurisprudence is not considered a source of law in Germany; due to its factual binding effect the status of especially settled case law in Germany is, however, debatable. Nonetheless, it is rather unlikely that the European Court of Human Rights would consider German case law comparable to Common Law rules in this regard, especially since also the Common Law rules will only be sufficient in very rare cases.[193] As a result, it is doubtful whether disturbance liability fulfils the Convention's criteria of being an exception "prescribed by law". Yet, many court decisions dealing with disturbance liability are published and thus accessible to the public.

Another question is whether these legal bases are **predictable**, which is another reason why restrictions to freedom of expression are "prescribed by law".[194] The courts have developed a general rule as to the preconditions for disturbance liability. In accordance with this rule, the host provider has a duty of care to check the contents and this duty must be defined in each particular case. Furthermore, this duty must be one that can reasonably be expected of the respective provider.[195] If copyright, trademark or unfair competition issues are concerned, this duty of care is defined by the respective laws. In other matters, as for example defamation or other infringements of the general personal right[196], however, the court will define this duty of care based on the facts and circumstances of the individual case. As German law is designed in a comparably abstract way in order to be applicable to many different cases, the law often does not specify the kind of duty of care to be applied.[197] Consequently, one could argue that this general rule applied by the courts within the scope of disturbance liability was sufficiently predictable.

5.2. Legitimate goal

As a second precondition, restrictions of freedom of expression must pursue a **legitimate goal**. Article 10 paragraph 2 European Convention on Human Rights exhaustively[198] enumerates all legitimate goals, i.e. "interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence or for maintaining the authority and impartiality of the judiciary." The claims regarding injunctive relief based on competition law, trademark law and unfair competition law as well as those based on

---

191 C. Busch, Secondary Liability of Service Providers, in M. Schmidt-Kessel (ed.), German National Reports on the 19th International Congress of Comparative Law, Tübingen: Mohr Siebeck 2014, p. 765 *et seq*, p. 767.

192 European Court of Human Rights, *Sunday Times v. The United Kingdom*, judgement of 26.04.1979, application N° 6538/74.

193 M. Macovei, Freedom of expression: A guide to the implementation of Article 10 of the European Convention on Human Rights, Council of Europe 2001, 2004, p. 33.

194 M. Macovei, Freedom of expression: A guide to the implementation of Article 10 of the European Convention on Human Rights, Council of Europe 2001, 2004, p. 31.

195 German Federal Court of Justice (*Bundesgerichtshof*, BGH), judgement of 17.05.2001 – I ZR 251/99; BGH, judgement of 10.10.1996 – I ZR 129/94; BGH, judgement of 15.10.1998 – I ZR 120/96.

196 Art. 2 para. 1 in conjunction with Art. 1 para. 1 German Constitution (*Grundgesetz*, GG).

197 See for example § 280 para. 1 s. 1, § 823 paras. 1, 2 German Civil Code (*Bürgerliches Gesetzbuch*, BGB).

198 M. Macovei, Freedom of expression: A guide to the implementation of Article 10 of the European Convention on Human Rights, Council of Europe 2001, 2004, p. 34.

disturbance liability all aim at **protecting the rights or reputation of others**. They all protect infringements of another person's **intellectual property or other rights** and thus pursue a legitimate goal. The provisions of the Interstate Treaties on Broadcasting and Telemedia aim to **protect morals** and **the reputation and rights of others** as well as the **prevention of disorder or crime**. The Interstate Treaty on the Protection of Minors in the Media is directed at the **protection of minors** and thus mainly at the **prevention of disorder and crime** as well as the **protection of health and morals**. As a consequence, both treaties pursue legitimate goals.

5.3. Necessary for a democratic society

Finally, in order to be necessary for a democratic society, the restriction of freedom of expression must also be **proportionate**.[199]

Section 59 of the Interstate Treaty on Broadcasting and Telemedia states that blocking orders directed at other persons than the content provider, i.e. at host or access providers, must be **reasonable**.[200] In addition, even measures directed at content providers must be **proportionate with respect to the relevance of the illegal Internet content to the provider and to the general public**. Prohibition orders are only allowed if **no less severe means** can be chosen. If less severe means are possible, the prohibition must be **restricted to specific types or parts of the content** or it must be **limited in time**.[201] By referring to these provisions, § 59 also applies to blocking measures based on § 20 of the Interstate Treaty on the Protection of Minors in the Media.

Part of the general rule concerning when someone is liable under a theory of disturbance liability is also that the **duty of care of the** perpetrator, i.e. the **host provider, can reasonably be expected of her/him**.[202] This precondition is probably taken from § 1004 paragraph 2 German Civil Code, according to which "[t]he claim is excluded if the owner is obliged to tolerate the interference." Through this, in each individual case the courts weigh the host provider's freedom of expression against the claimant's violated right.[203] Furthermore, and also applicable to claims based on copyright law, trademark law or unfair competition law, the host provider need filter or remove illegal Internet content only if it has **knowledge of such infringements**. Section 7, paragraph 2, sentence 1 of the German Telemedia Act explicitly states that Internet Service Providers have **no general duty to control** all information provided by them on the Internet. Finally, the courts **do not allow so-called overblocking**, through which legal Internet content is also blocked, filtered or removed.[204] These different measures ensure that the restriction put on freedom of expression through orders to filter, take down or, in rare cases, block illegal Internet content remains proportionate.

---

199 M. Macovei, Freedom of expression: A guide to the implementation of Article 10 of the European Convention on Human Rights, Council of Europe 2001, 2004, p. 35.

200 § 59 para. 4 s. 1 Interstate Treaty on Broadcasting and Telemedia (*Staatsvertrag für Rundfunk und Telemedien*, RStV).

201 § 59 para. 3 ss. 3, 4 Interstate Treaty on Broadcasting and Telemedia (*Staatsvertrag für Rundfunk und Telemedien*, RStV).

202 See also J. Ensthaler & M. Heinemann, Die Fortentwicklung der Providerhaftung durch die Rechtsprechung, in Gewerblicher Rechtsschutz und Urheberrecht (GRUR) 2012, p. 433, p. 436 *et seq*.

203 See for example German Federal Court of Justice (*Bundesgerichtshof*, BGH), judgement of 17.05.2001 – I ZR 251/99; BGH, judgement of 22.07.2010 – I ZR 139/08; BGH, judgement of 25.10.2011 – VI ZR 93/10.

204 Higher Regional Court (*Oberlandesgericht*, OLG) Hamburg, judgement of 21.11.2013 – 5 U 68/10; OLG Köln, judgement of 18.7.2014 – 6 U 192/11 (*Goldesel*).

There is very little case law in which **access providers** have been ordered to filter illegal Internet content. This case law typically concerns WLAN-operators, whose WLAN has been used by a third person to up- or download illegal Internet content. In the most important case in this context, the **German Federal Court of Justice considered which duty of care can reasonably be expected of the WLAN-operator**. As the latter was a private person, the court found it disproportionate that the WLAN-operator be required to keep her/his WLAN up-to-date with the actual security measures. As a consequence, the WLAN-operator was only ordered to take the security measures against illegal use of their WLAN that were common and appropriate at the time when installing the WLAN and not to also keep it up-to-date.[205] In another case, the Regional Court of Frankfurt am Main found it proportionate that the WLAN-operator, namely the operator of a hotel, informed her/his guests of their duty to respect the existing laws when using the Internet through the WLAN. According to the court, it would have been disproportionate to burden the WLAN-operator with a duty of preventive control, as the operator already used cryptographic techniques.[206] In the third case dealing with WLAN-operators as access providers in this context, the Regional Court of Hamburg considered it proportionate to order an operator of an Internet-café and thus of a WLAN to block ports necessary for file sharing.[207]

5.4. Internet Complaint Office

As to the Internet Complaint Office described above,[208] the two private organisations running it provide model**by-laws** regulating scope, aim and procedure of the Internet Complaint Office.[209] These by-laws are binding to the respective organisation, namely the Voluntary Self-Monitoring of Multimedia Service Providers (*Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V.*, FSM) and the eco Association of the German Internet Industry (*eco Verband der deutschen Internetwirtschaft e.V.*), but not to anyone else. This however is different for the former's **Code of Conduct**, as the **members** of the Voluntary Self-Monitoring of Multimedia Service Providers voluntarily bound themselves to comply with the Code of Conduct. These members can be sanctioned by the organisation in case they violate the Code of Conduct.[210]

As both by-laws and the Code of Conduct as well as the Voluntary Self-Monitoring of Multimedia Service Providers' by-law explaining the criteria of their assessment in more detail[211] are written down and publicly available on the Internet, they are both **accessible and predictable**. The Internet Complaint Office also strives toward a **legitimate goal**, i.e. **protecting the rights or reputation of others** by using a range of criminal offences as criteria, which protect a person's rights or reputation: sexual criminal offences, dissemination of Nazi propaganda, incitement of the people, support of

---

205 German Federal Court of Justice (*Bundesgerichtshof*, BGH), judgement of 12.05.2010 – I ZR 121/08 (*Sommer unseres Lebens*).

206 Regional Court (*Landgericht*, LG) Frankfurt a.M., judgement of 18.08.2010 – 2-06 S 19/09.

207 Regional Court (*Landgericht*, LG) Hamburg, judgement of 25.11.2010 – 310 O 433/10.

208 See point 4. of this report on German law.

209 Internet-Beschwerdestelle, Complaints Procedure, available at http://www.Internet-beschwerdestelle.de/en/complaint/procedure/index.htm (20.07.2015).

210 Para. II Code of Conduct for the Association Freiwillige Selbstkontrolle Multimedia- Diensteanbieter e.V., available at http://www.fsm.de/about-us/FSM-Code_of_Conduct.pdf (20.07.2015).

211 Prüfrichtlinie der Freiwilligen Selbstkontrolle Multimedia-Diensteanbieter (FSM e.V.), available at http://www.fsm.de/ueber-uns/FSM-Pruefrichtlinie.pdf (20.07.2015).

criminal or terrorist groups or dissemination of youth-inappropriate content.[212] As already explained, the Internet Complaint Office will inform the respective content or host provider in case it considers Internet content as illegal and will ask them to take this illegal content down. Since it is not the Internet Complaint Office itself which removes the content, but the content or host provider, these Internet Service Providers can decide themselves whether they will follow this request and to what extent. The Office's request will therefore **not be disproportionate**, as it does not touch the content itself. Regarding violations of the Code of Conduct by its members, sanctions by the Voluntary Self-Monitoring of Multimedia Service Providers are possible. There seem to be no cases in which measures more severe than the mere request to take down the illegal Internet content have been taken. This conclusion can be drawn from the fact that no such decision is published on the organisation's website, although its by-laws state that decisions against signatories of the Code of Conduct for sanctions more serious than the mentioned request will be published on the website in a not-anonymised form.[213]

Dr. Johanna Fournier
21.07.2015

Revised on 30.05.2016 taking into consideration comments from Germany on this report

212 § 2 Complaint Rules for the eco Verband der deutschen Internetwirtschaft e.V., available at https://www.eco.de/wp-content/blogs.dir/beschwerdeordnung_Internet-beschwerdestelle.pdf (21.07.2015).

213 § 12 s. 2 Complaint Rules for the Association Freiwillige Selbstkontrolle Multimedia e.V., available at http://www.fsm.de/about-us/FSM-Complaint_Rules.pdf (20.07.2015) in conjunction with the cases published on Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V., Beschwerdestelle: Entscheidungen aus der Praxis, available at http://www.fsm.de/beschwerdestelle/praxisentscheidungen (20.07.2015).