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 39-61

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.

AUSTRIA

1. Legal Sources and overview

Austria is a legal system with comparably unconstrained freedom of expression on the Internet. There is no specific general legislation concerning **blocking** of internet sites.

For the time being, the only real legal (hard law) measure to block sites seems to exist in the field of **intellectual property rights** and here based on EU-Law (directive and respective national Austrian law). In this field**,** there is (in the aftermath of the famous UPC Cablecom Case of the ECJ[1]), a recent judgment (2014) of the Austrian Highest Court[2] (OGH) on **blocking of sites by ISPs**. In such cases the ISP can be obliged to block sites by an injunction. Which exact measures are to be taken is at the discretion of the ISP. The Austrian Highest Court tried hard to integrate such blocking measures (and including **human rights safeguards** for the domain-owners and customers) within the existing Austrian legal system of the law of civil enforcement. One may doubt if this endeavor can be regarded as successful. But in the absence of any other legal basis, there seems to have been no alternative options open to the Austrian court. The reaction of the ISPs was that they see themselves as being pushed into the role of a judge when it comes to making blocking decisions; the ISP's objections to this development were formulated in a rather strong way.[3] Austrian ISPs have a strong preference for a law-based procedure and a decision by a (civil, penal or administrative) judge, in each case before an act of blocking takes place. They also demanded that costs be covered for the blocking measures in the claimant's interest. In a very recent judgement, the Austria's Highest Court[4] (for civil cases) saw no reason to ask the ECJ or the Austrian Constitutional Court again to test the constitutionality of the relevant rules under intellectual property law. ISPs have to block and bear the costs in such civil law cases.

In all other fields of law (including general penal and administrative law), there seems to be no hard law blocking possible against an ISP (no matter how illegal the content of a third person may be). However, the ISPs announced that they would block sites, but only if a (civil, administrative or penal) court order or decision would require them to do so. The Austrian ISPs would not block on a non-legal basis if the government or any authority or private organization or person would simply "ask" or recommend them to do so (i.e., there is no non-transparent, non-law based blocking). From the perspective of freedom of expression, this makes a big difference.

Only for **child pornography** and **nazi-propaganda**, there exists in Austria a so-called stopline.at. It seems, ISPs do only **monitor** (and not block) such pages. The "legal basis" of this measure is a non-binding **resolution** of the Austrian Parliament. In other words, such (user driven) monitoring is done on the basis of a sort of voluntary self-regulation of the ISPs. The goal is to remove such material, if hosted in Austria, or to inform international partners (like INHOPE). In the case of child pornography there will hardly ever be an objection claiming freedom of expression against such removal. In the case of nazi-propaganda, the ECtHR confirmed the special sensitivity that exists in Austria in light of the terrible Nazi regime which ruled Austria from 1938 to 1945. Such restrictions of freedom of expression in Austria (as in Germany) are reconcilable with the ECHR according to the ECtHR.

---

1 ECJ, 27 March 2014, Rs C-314/12. Kino.to-case.

2 OGH 24 June 2014, 4Ob71/14s.

3 E.g. http://orf.at/stories/2287588/.

4 OGH 19 May 2015, 4Ob22/15m, MR 2015, 201.

In the field of **removal** of illegal content against a host (in Austria), the European rules on the Host provider privilege on the basis of the E-Commerce Directive apply on the basis of the Austrian E-Commerce Act (transposing the abovementioned directive). The term of a host is understood in a rather extensive way in Austria. All sorts of web sites are regarded as hosts, no matter how active or passive they are.

If the host is a "media company", the **Austrian Media Act** applies. The Media Act contains special provisions where a media company is acting as a website-host. It is important to note that also a physical person offering a commentary function on his (private) Facebook site is regarded as a media company according to the Austrian Media Act.[5] The media company is in principle liable (e.g. for libel and slander according to the criminal and private law offences of the Media Act). Although however, the media-host of a website may prove that he acted with due care. For the time being (end November 2015), this duty of care is interpreted by the Austrian courts in conformity with the host provider privilege of the Austrian E-Commerce Act and does, consequently, not contain any proactive duty of care to remove online-content (in other words notice-and-take-down also applies in this field). In addition the Austrian Media Act contains a special and very interesting penal law provision on confiscation of websites (and penalties) against the media company/host.

There are however some legal writers who strongly advocate that for media companies, the host provider privilege shall not apply and refer therefore explicitly to the *Delfi* case of the ECtHR. If that would be the case, the media hosts would probably have proactive duties to check content before it goes online in order to avoid liability if damage is objectively foreseeable (given the particular subject). Such a development would constitute a more narrow approach of freedom of expression than is the current practice today in Austria. However, such narrow approach of freedom to impart information would be possible according to the *Delfi* case. So even if such development would take place, the Austrian legal system would be in line with the ECHR.

There is also a sort of (very) soft law measure for removal of certain internet content. For **radical Islamic videos**, there exists a special e-mail-hotline of a Federal Agency to which anybody may send notices. The Federal Agency for State Protection and Counter Terrorism informs the **host** (e.g. youtube or facebook) of the relevant video. A host decides itself if it proceeds to delete the content. This very soft measure falls within the normal duties of an agency and should not be in conflict with the ECHR. Similar measures exist at the same agency for nacist material.[6]

As a short summary, one can say that blocking measures are very limited in scope and the host provider privilege is, for the time being, understood in a rather extensive way in Austria. That is to say that freedom of expression on the internet is largely unconstrained in Austria (compared to other states).

There seems to be no court decisions in Austria that specifically state that **access to the internet** is a human right. However, according to the Austrian Act on Provision of Goods and Services to Customers,[7] a company rendering a necessary good or service may be obliged in civil law to conclude a contract with a consumer. This rule applies to the provision of, e.g., energy or water. It should also apply to access to the internet. That is to say, the Access Provider may only refuse to conclude a contract for very good reasons.

---

5 In a penal case: OGH 29 April 2015, 15 Os 14/15w, 15 Os 15/15t.

6 http://www.bmi.gv.at/cms/bmi_verfassungsschutz/meldestelle/.

7 So called Nahversorgungsgesetz (29 June 1977, BGBl. Nr. 392/1977).

International sources (racist, terrorist material and child pornography)

Austria has ratified the Convention on Cybercrime (CETS No.185, Budapest Convention) and it entered into force on 1 October 2012.[8] However, there seems to be no indication whatsoever that this convention (or the relevant Austrian Acts) would contain any measures on blocking or removal.

Austria has indeed signed the "Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a **racist** and **xenophobic** nature committed through computer systems" (CETS No. 189), but it has not ratified it. However, as the Protocol only extends the measures from the Budapest Convention to racist crimes, it should not contain any blocking or removal measures. Racist or xenophobic content **cannot be blocked** in Austria (but stays illegal from the perspective of penal law, and against the content provider). The relevant rules of penal law will not be applied against an ISP (or, at least, will only be applied if the ISP intentionally fails to block in order to support the material itself). For Nazi propaganda, there is particular self-regulation.

Austria has ratified the Council of Europe Convention on the Prevention of **Terrorism** (CETS No. 196, Warsaw Convention).[9] The Convention itself does not contain measures on blocking or removal. It contains material penal law. In this respect it has indirect effects on soft law blocking and removal. An act of blocking depends on whether the ISP qualifies as a co-perpetrator in penal law. There is a particular rule in Austrian penal law, on the making available of terrorist material on the Internet.[10] Indeed, the activity of a host (or ISP) would (directly) qualify as the "making available" of such material. To prevent such penal liability, the ISPs might block out of cautiousness. However, such an omission to act becomes punishable only after active knowledge of the ISP (namely to prove criminal intention of the ISP itself).[11] That will hardly ever be the case; even omission of the ISP will regularly be without such intention. Mere laziness is not enough.[12] This is also in line with the provider privileges of the E-Commerce Directive (and even goes beyond these privileges). As a consequence, Austrian ISPs are **not generally obliged** to block such content. This is a very broad approach to freedom of expression. In the field of terrorism, there is a soft law removal measure.

Austria has ratified (and brought into force) the Council of Europe Convention on the Protection of **Children** against Sexual Exploitation and **Sexual Abuse** (CETS No. 201, Lanzarote Convention).[13] The convention does not seem to contain any measures on blocking or removal. However, there might be European Union instruments that could foresee blocking in this respective field.[14] For child

---

8 Übereinkommen über Computerkriminalität, BGBl. III Nr. 140/2012 (NR: GP XXIV RV 1645 AB 1697 S. 150. BR: AB 8707 S. 807.)

9 Übereinkommen des Europarats zur Verhütung des Terrorismus, BGBl. III Nr. 34/2010 (NR: GP XXIV RV 95 AB 357 S. 40. BR: AB 8190 S. 777.).

10 § 278 f Austrian Penal Code.

11 See especially Plöchl, Wiener Kommentar zum StGB, January 2014, § 278 f, no. 15 and esp. 19: "Committance as a co-perpetrator by a mere conduit of a provider can be relevant, if the provider is obliged to act and with criminal intention does not do so". However, there is still a doubt as to where the duty to act shall come from. The Austrian E-Commerce Act does not contain such a duty. There are no court cases and in a case of doubt there would be no conviction of an ISP.

12 Brenn, E-Commerce-Gesetz, 2002, § 13, p. 266, 268: access providers are not co-perpetrators, even if they know about the illegal content. A duty to act only exists for the informed host (§ 16 sect. 1 no. 2 ECG).

13 Übereinkommen des Europarats zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch, BGBl. III Nr. 96/2011 (NR: GP XXIV RV 881 AB 1017 S. 86. BR: AB 8435 S. 791.).

14 See the Austrian Regierungsvorlage (RV) mentioned above and Fritz/Zeder, Neue Vorschläge zur Bekämpfung von Menschenhandel und sexueller Ausbeutung von Kindern, JSt 2009, 126, 129 (referring to a proposal for a framework decision; later on the framework decision became directive 2011/93/EU). It can be left open here if the proposal was finally decided or not.

pornography, it is said in Austria, that an ISP does not "make available" such material. So the relevant rule is not (even indirectly) applicable to ISPs. It is discussed if an ISP is a co-perpetrator with the content provider. In literature the answer is indeed affirmative, if there is a duty to act for the ISP. Such a duty could be based, say legal writers, on the Austrian E-Commerce Act.[15] However, it is not so clear if such a duty for an ISP is indeed contained in the Austrian E-Commerce Act.[16] As a consequence, Austrian ISPs are **not legally obliged to block** such content. However, they do so (voluntarily) on the basis of self-regulation.

2. Legal Framework

In Austria, the EU's E-Commerce Directive was transposed into national law by the **E-Commerce Act** (ECG).[17]

Certain service providers and host liability provisions exist under sections 13 to 19 of the ECG. These rules are based on the **safe harbor provisions** of the EU E-Commerce Directive. Sect. 13 ECG contains an exclusion of liability provision for transmission (ISP). Similar exclusions of liability exist for search engines (sect. 14) and caching (sect. 15). The exclusion of liability of host providers is regulated in a different way (sect. 16).[18] Sect. 17 excludes liability for links, sect. 18 contains mainly information duties of access and host service providers. According to sect. 19 ECG, sects. 13 to 18 shall not prejudice any legal provisions in accordance with which a **court** or **administrative authority** may **order** a service provider (ISP or host) to desist from, remedy or prevent any legal violation. This applies also to providers which provide electronic services free of charge.

The question is then which specific legal provisions according to Austrian law can serve as a basis for a court or administrative authority for such an order directed against an ISP or host to "desist, remedy or prevent" any legal violation. The Austrian legislative material to sect. 19 ECG contains some advice on the matter:[19]

Art. 12 to 14 of the EC-Directive preclude the responsibility of providers for the mentioned information society services (provision of access, automatic caching and storage of external content) under certain conditions. Thus both the **criminal** responsibility of the provider, its officers and employees as well as the **compensation** liability are excluded. However, the directive does not affect the legal systems of the Member States insofar as the competent authorities or courts are entitled and have the ability to require a provider to block or prevent an infringement. **The competent authority or court may order the blocking of access or order the removal of content.** The Directive

---

15 Philipp, Wiener Kommentar zum StGB, 2014, § 207a, no. 18.

16 It is very interesting that the legal writers to the Austrian E-Commerce Act do refer in the relevant rule (mere conduit) to the penal law rule (§ 207a StGB), as a basis for blocking (e.g. Laga, Sehrschön, Ciresa, E-Commerce-Gesetz, 2. Ed. 2007, § 13, p. 65, 66). So the one refers to the other and vice versa. These legal writers say that the administration could make an injunction for a blocking in child porn cases. It is however left totally open, where the legal basis for such an administrative injunction should come from.

17 Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden (E-Commerce-Gesetz - ECG), BGBl. I Nr. 152/2001.

18 See below to Austria 2.2.

19 ECG, 817 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXI. GP, Nachdruck vom 19. 11. 2001, Regierungsvorlage, Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt (E-Commerce-Gesetz – ECG) und das Signaturgesetz sowie die Zivilprozessordnung geändert werden.

itself does not prevent Member States from establishing procedures governing the removal or disabling of access to it (see Art. 14, para. 3).
§ 19 Abs. 1 Austrian ECG contains these exceptions foreseen by the Directive. The provision presupposes that a court or authority shall be entitled to order a provider on the basis of a statutory provision under the conditions mentioned therein, the omission, removal or prevention of any infringement. However, such a **power cannot be inferred** from the proposed § 19 **ECG** on its own.

The preparatory documents[20] of the legislator mention that such a power to block or remove content could derive from the **Security Police Act (SPG) and/or Criminal Procedure Law (StPO)**.[21] However, the legislator did not specify which provisions it had in mind. Also commentators do not mention any specific sources in the SPG or or StPO.[22] There is, as far as we can see, no evidence that provisions of a more general nature in these **public law Acts** would be applied to access blocking against ISPs or removal of content against hosts.[23]

§ 19 paragraph 1 ECG also applies to the **civil courts**. It is possible to make an order against a provider - at the request of a claimant or a vulnerable party - to adopt an injunction (by interlocutory order or judgment), provided that the substantive conditions of injunctive relief exist. As an example, the legislator refers to: general civil law regulations such as § 16 (General Right to **Privacy**), § 43 (Right of the use of its own name) and § 1330 Austrian Civil Code (tort claim in case of **defamation**). One can also think of the Act on Unfair Competition.[24] Also mentioned in this context is a special provision such as the § 81 of the Copyright Act and other "similar" provisions. It does not matter if the service provider has actual knowledge of the retrieved, transferred or hosted information.

Some of these legal grounds are more related to blocking against an ISP (e.g. the Copyright Act), others more to removal against a host (e.g. defamation).

2.1. Blocking and/or filtering of illegal Internet content

In Austria, the legal consequences of violations of copyright are regulated through the Copyright Act.[25] In principle, it does not matter whether a violation of copyright is committed through the Internet or not. The legal basis for blocking against an ISP is found in paragraphs 81(1) and (1a) of the Austrian Copyright Act. These provisions state (quote):

"(1) A person who has suffered an infringement of any exclusive rights conferred by this Law, or who fears such an infringement, shall be entitled to bring proceedings for a restraining injunction. Legal proceedings may also be brought against the proprietor of a business if the infringement is committed in the course of the activities of his business by one of his employees or by a person acting under his control, or if there is a danger that such an infringement will be committed; paragraph 81(1a) shall apply mutatis mutandis.

---

20 For the source see footnote above.

21 What is meant is the Security Police Act (Sicherheitspolizei-Gesetz, SPG) and the Criminal Procedural Code (Strafprozessordnung, StPO).

22 E.g. Zankl, E-Commerce-Gesetz, Kommentar und Handbuch, Verlag Österreich 2002, § 19, p. 217.

23 However, there are provisions that oblige the providers to render information, e.g. in the StPO (§ 135 sect. 2) or the SPG (§ 53 Abs. 3a). But such an obligation to inform cannot be equated with an obligation to block against an ISP or to remove against a host.

24 E.g. by Brenn, ECG, E-Commerce-Gesetz, Commentary, Manz 2002, Vienna, § 19, p. 307.

25 Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte (Urheberrechtsgesetz, UrhG), BGBl. Nr. 111/1936.

(1a) If the person who has committed such an infringement, or by whom there is a danger of such an infringement being committed, uses the services of an **intermediary** for that purpose, the intermediary shall also be liable to an injunction under subparagraph (1). …"[26]

In the aftermath of the ECJ decision C-314/12 (**UPC Telekabel Wien** /Constantin Film, "kino.to"[27]) on **24 June 2014,** the **Austrian Highest Court** decided a case on internet-blocking [28]. The focus of this Austrian decision was if and how the Austrian legal system corresponds to the framework established by the ECJ in terms of a check on fundamental rights and Austrian procedural and enforcement law.

The Austrian Highest Court found that in the respective case the internet site contained only illegal contents. Therefore, the **fundamental right to information** of the other users (as mentioned by the ECJ: access to information) was not concerned (Yildirim-case of the ECtHR).

However, the rights of the rights holder (property rights) against the ISP are rights that are based on a prohibition against interference. There is no right to any positive action or behavior. The defendant (ISP) is given considerable flexibility as to the means by which it removes the interference. This also serves to secure the **professional freedom** of the ISP (as another fundamental right concerned).

Such an order for prohibition – or, an injunction, - against interference (so called *Erfolgsverbot*) is, according to the view of the ECJ, only admissible, if the provider can **object** (before a valid sanction is applied) that he has done everything possible to prevent the infringement. This element of participation of the obliged party (ISP) seems to be problematic under Austrian law of enforcement of judgements[29]. According to the view of the Austrian Highest Court, these **procedural aspects** of the ECJ can be **safeguarded** by an adapted application of the Austrian rules on suspension of enforcement. This happens in the form of a counter claim of the obliged party (so called *Impugnationsklage*). Such a counter claim would also be a reason for a suspension of penalties. However, there would be other obstacles according to Austrian law (e.g. the enforcement procedure may only be interrupted if the obliged party would suffer a detriment that is not reparable for the case in which the enforcement was not allowed). Nevertheless, the Austrian Highest court proceeds with a sort of **special adaptation of Austrian law** for such cases, simply to secure that the obliged party is heard before the enforcement of such penalties takes place (safeguards). From a more practical perspective, it is only important that the obliged party can defend himself or herself before a fine has to be paid (enforced). That a fine is first applied (by a decision) does no harm to the ISP's procedural rights, according to the Austrian Highest Court.

A further condition of such an injunction is, according to the ECJ, that the clients of the ISPs have a possibility to claim their right of **access to information** in front of a court as soon as the **blocking measures** of the ISP are made known to them or made **public**. According to the Austrian Highest Court, any client could bring a claim, on a contractual basis, against an ISP to remove excessive blocking which violates the fundamental right of access to information. The contract between the ISP

---

26 The provision aims to transpose Article 8 of Directive 2001/29, headed "Sanctions and remedies", which states in paragraph 3: 'Member States shall ensure that rights holders are in a position to apply for an injunction against **intermediaries** whose services are used by a third party to infringe a copyright or related right.'

27 Judgment of 27 March 2014, UPC Telekabel Wien (C-314/12) ECLI:EU:C:2014:192.

28 4Ob71/14s, published in numerous Austrian legal journals, e.g. ecolex 2014/375. And in a German journal: GRUR Int 2014, 1074.

29 Enforcement Act, Gesetz vom 27. Mai 1896, über das Exekutions- und Sicherungsverfahren (Exekutionsordnung, EO, RGBl. Nr. 79/1896).

and any client will have to be interpreted in a way that only blockings according to the guidelines of the ECJ are admissible, according to the Austrian Highest Court.
In such a dispute between any client and the ISP for **access to information**, the ISP may call the rights holder for help in the dispute according to the Austrian Civil Procedure Act (ZPO). However, it would also be possible for the client to bring a direct claim against the rights holder for access to information if the latter has caused excessive blocking as a result of his or her demand for a blocking order. According to the views of the ECJ, such a right to information is an **absolute right that can be enforced against every ISP**. Such an absolute right to information would also be protected within the law of enforcement. However, in practice, there would probably be very few clients (users) who would claim their right to access of information. Nevertheless, the ECJ only claims that it must be legally possible. Already the existence of such a possibility will, says the Austrian Highest Court, convince the rights holder and the ISP to take care when blocking sites.

There is already considerable commentary in Austria[30] on this relatively recent decision, reflecting the great impact of the case. In the Austrian legal system, such a blocking order and the reasoning on freedom of information (access) amounts to what is really a small revolution.

First of all, the ISPs are directly affected. The association ISPA (Internet Service Providers Austria[31]) stated that the decision puts Austrian **ISPs in a very difficult position**. Either the ISP has to examine every demand for a blocking request (which would be too cumbersome, in practice) or the ISP would simply block after each demand (which would probably violate fundamental rights). The legitimacy of the blocking demand would be determined by a court only after the ISP has let itself be exposed to a fine. The ISPA suggests that the ISP shall not take such a role of a judge deciding what to block; furthermore, the decision about blocking shall be taken by a state judge; all blockings shall be reported for purposes of **transparency**; all blockings shall be examined by a judge periodically. For Austria, a situation like in the UK (where allegedly 20 % of the sites are blocked) has to be prevented. The Austrian ISP will provide clear online information regarding who has demanded the blocking and will try to refer the customers directly to the requesting party.[32]

A legal advisor to the film industry commented on the judgment and recommended that the relevant departments of the Austrian Business chamber prepare a sort of practical **standard approach** for blocking requests.[33]

Another comment states that the decision of the Austrian Highest Court is positive because the ISP has in fact the possibility to **challenge** the blocking. In order to do so, the ISP has, under the Austrian law of enforcement, all the remedies and instruments of an ordinary procedure according to the Austrian Code of Civil Procedure.[34] The right to information of the users shall be regulated in standard contract terms between the user and the ISP.[35] Such standard terms will be controlled by the authorities and under the rather strict Austrian Consumer Protection Law.

An open question remains (according to Prof. Otenhajmer) if a page can be blocked that contains legal and illegal content at the same time, e.g. like YouTube. The case in front of the Austrian Courts

---

30 Kraft, MR 2014,171, Walter, MR 2014,201, jusIT 2014/80 S 169 (Beimrohr), ÖBl 2014/50 S 237 (Anzenberger), EvBl 2015,27 (Otenhajmer), ecolex 2014/375 S 887 (Zemann).

31 www.ispa.at.

32 https://www.ispa.at/presse/presseaussendungen/2014/ogh-urteil-draengt-provider-in-richterrolle/ (as for June 2015).

33 Kraft, Zugangssperren zu Webseiten als Mittel der Rechtsdurchsetzung, MR 2014, 171, 174.

34 Zivilprozessordnung, ZPO, Gesetz vom 1. August 1895, über das gerichtliche Verfahren in bürgerlichen Rechtsstreitigkeiten, RGBl. Nr. 113/1895.

35 Walter, Rechtsverletzende Website – Sperranordnung gegen Access-Provider, MR 2014, 201.

only concerned pages with exclusively illegal content. In particular it is unclear, who should decide on such blocking: the ISP or a judge in a procedure according to enforcement law.[36] From the practices witnessed in Austria it can be said, that in such cases of mixed content, there is no blocking.

From a more technical perspective, Mr. Bogendorfer refers to a German judgement ("*Goldesel*"[37]) and states that the judgement of the Austrian Highest Court might be wrong. He argues that the claim against the ISP should be **subsidiary** to the claim against the **host provider** and that it would be very difficult to find the right blocking method.[38] This view would mean that removal would have a sort of priority before blocking. However, it is clear that this was not the opinion of the Austrian Highest Court and the ECJ.

Mrs. Beimrohr argues that there are considerable risks for ISPs with regard to the possibility of users to rely on their fundamental rights of **access to information**. Since the basis for such claims is, according to the Austrian Highest Court, a contractual claim, every client could claim individually and at different times. And it seems unclear how the users should be informed about a blocking measure. She argues that it would be more than desirable if the **legislator** developed a **particular procedure for blocking measures**.[39] Also Anzenberger thinks that the legislator will have to become active in the medium term[40] and Bogendorfer sees further problems until such time as the legislator sets a clear frame.[41] Prof. Wilhelm expects further developments of the Austrian law in this field.[42]

No other hard law blocking

As shown above, there are no other bases in hard law for blocking according to Austrian law, not even in severe cases such as terrorist or racist propaganda or child pornography. (However, this sentence only refers to blocking. For the latter material, there are some other measures against the content provider or a host; but no blocking against Austrian IAP).

In the field of **competition law**, it is possible to obtain an injunction against the authority (company) administrating Domain-names, e.g. in case of a danger of confusion. However, that seems not to be classical blocking against an ISP but an order against the domain name authority.

In the field of **gambling law**, the Austrian government currently verifies if it makes sense to block illegal foreign online-gambling offers. It seems that no decisions or legal measures have been taken so far (November 2015). The government is currently considering whether to follow the gambling blocking rules in place in certainly countries, such as Hungary[43] or the law proposal in Switzerland.

In other fields (e.g. medical products or data protection) it seems that there are no possibilities for obtaining an order against an ISP. No such measures seem to be being discussed in Austrian legal literature. Nor would ISPs block out of their own initiative.

---

36 Otenhajmer, Access-Provider muss Zugang zu unrechtmäßigen Inhalten verhindern, EvBl 2015/2, p. 30.

37 OLG Köln 18. 7. 2014, 6 U 192/11.

38 Bogendorfer, Sperren illegaler Inhalte auf kino.to & Co, ipCompetence 2014 H 12, 28, p. 35.

39 Beimrohr, OGH: Zur Wperre einer Website nach § 81 Abs 1a UrhG, jusIT 2014/80, p. 171.

40 Anzenberger, Sperrverfügungen gegen Access-Provider, ÖBl 2014/50, p. 242.

41 Bogendorfer, Sperren illegaler Inhalte auf kino.to & Co, ipCompetence 2014 H 12, 28, p. 36.

42 Wilhelm, Ausgerechnet: Die EO als Schnittstelle von Gemeinschafts- und Heimat-Recht, EuGH UPC Telekabel und die Folgen, ecolex 2014, 669.

43 E.g. press release of 10 June 2015: http://diepresse.com/home/wirtschaft/economist/4751659/Gluecksspiel_Stopp-fur-illegales-OnlineZocken or http://derstandard.at/2000013340524/Online-Gluecksspiel-Finanzministerium-erwaegt-Internetsperren (November 2015).

2.2. Take-down/removal of illegal Internet content

Introduction

Section 16 of the ECG covers host providers. However, it exempts host providers from being liable for the information stored on behalf of a user where the provider immediately takes action to remove illegal information or block access to it once made aware of it (notice and take down). This places a legal duty on the host to act or to be deemed as a co-perpetrator in circumstances where there is a failure to act. For practical reasons, this is of particular interest where the host has its place of business or residence in Austria. The main court cases on removal of content concern the violation of property rights and defamation.

Violation of Intellectual Property Rights

Illegal content can occur where it violates another's intellectual property rights.

In a recent case (October 2014) of the Austrian Highest court, an Austrian online-media platform (in terms of Austrian law, a host-provider, but also a media company) invited the public (readers) to post **pictures of the football players** of a traditional football club based in Vienna. In the general terms and conditions for the public, the online-media platform stated that intellectual property rights should not be violated by the posted pictures. Nevertheless, some contributions of readers violated rights of the claimant, which might not have come as a big surprise for the host. The Austrian Highest Court held that the media platform was a host provider, and as such it was liable as a **co-perpetrator** (so called ***Gehilfe***) for a failure to remove the relevant content. The co-perpetrator has to be judged according to its own contribution, not for the violation of the rights of the third party as such. It must **know** about the violation of the (third) perpetrator or has to have violated its duty to **examine** the online-platform (in particular cases). The duty to examine is, however, limited to material which amounts to a gross violation of rights. These principles are, according to the Austrian Highest Court, "explained in more detail," in the host provider privilege of the Austrian Act on E-Commerce (ECG, § 16) and in § 81 sect. 1a of the Austrian Act on Copyright. The subject matter was (only) claims on injunctive relief (not damages), that is to say removal and take down. It is a material precondition for such an action to remove content that the offence must be **obvious** to the defendant, e.g. by a clear, informative and transparent **warning** or **notice**. The claimant has to give **reasons** and proof to the defendant. It must be possible for the defendant to evaluate his legal position at least vaguely in an amateur way (which is to say he does not have to verify all details in depth from the legal perspective; only clear violations are covered). The host provider must be able to examine the claimant's legal title in the particular IP-matter. Only clear cases are covered by this obligation to remove content.[44]

A commentator on this decision notes that this legal evaluation is not only important for host providers but also for access providers in connection to all possible violation of IP rights.[45] We would add, that it is also important outside the field of IP violations in all civil cases. Another comment is that the requirements for such a warning or notice are quite demanding,[46] respectively correct and adequate.[47]

---

44 OGH 21 October 2014, 4 Ob 140/14p, published in jusIT 2015/5 p. 17 (note Staudegger), wbl 2015,113/39, ecolex 2015/86 p. 222 (Tonninger), RdW 2015/107 p. 102, EvBl 2015/69 p, 472, GRUR Int 2015,497 - Fußballerfotos, and in MR 2015, 31, note Walter, Uhl, Pateter. In the particular case the claimant was not successful because he formulated his claim against the defendant as a direct tortfeasor not as a "Gehilfe". This seams a rather formalistic reason (so Uhl and Pateter, loc.cit., pt. 3.5.).

45 Walter, loc.cit.

46 Uhl and Prateter, loc.cit.

47 Staudegger in jusIT 2015, 17.

Violation of the General Right to Privacy

In principle, there is also no doubt that the general right to privacy (§ 16, Austrian Civil Code) permits claims for injunctive relief[48] and that such a right is relevant in connection with arts. 16 and 19 Act on Electronic commerce (ECG).[49] However, there seems to be no court decision that would positively and explicitly confirm such an assumption. In many cases, the host provider will have already removed the content himself and the claim in question is "only" one on giving information on the identity of the posting person.[50] The cases might have a closer link to copyright legislation (e.g. post mortal protection of images[51]). However, in legal writing it is said that § 16 of the Austrian Civil Code could possibly be used in cases where someone posts pictures of other persons (without clothes) on social networks. A claim based on § 16 ACC on deletion of the pictures or removal of relevant sites could be directed against a host provider.[52]

Defamation-Cases according to the "Guest-Book"-judgment

Privacy and **defamation** cases present more of a problem for **host**-providers, although they could, in principle[53], also pose a problem for access providers.[54]

In 2006, the Austrian Highest Court[55] decided a leading case where a tourism association displayed a guest book on the homepage of their website. The terms of use noted that the association reserved the right to remove content. An anonymous user wrote, in a rather impolite way, some criticisms concerning a particular restaurant within the territorial sphere of the association. The claimant would, it said, be the "worst innkeeper" of Austria, he would commit tax fraud, would invite the guests to illegally use others' parking places and would lie about his brother. The claimant demanded that the host provider remove these comments. The host provider did so immediately after receiving this notice. However, there were further postings that confirmed and supported the allegations as true. These other posts were only removed about two weeks later, again after notice from the claimant. The Austrian Highest court referred to the rules on host providers in the Act on Electronic Commerce (sect. 16). According to this rule, the host provider must, after knowledge of illegal acts or information, remove the information or block access to it. But it is not liable for damages. However,

---

48 Even if such claims on injunctive relief are not explicitly mentioned in the text of the law (see e.g. Egger in Schwimann-ABGB, Taschenkommentar, 2010, § 16 nr. 18).

49 The preparing documents of the legislator to the Act on Electronic Commerce mention § 16 of the Austrian Civil Code explicitly. See e.g. Brenn, ECG, 2002, p. 305. Also mentioned is § 43 Austrian Civil Code (right on use of its own name, and to exclude everybody else from such use).

50 E.g. OGH 22 June 2012, 6Ob119/11k: A female military officer was insulted (by a third party) in the online discussion forum of the defendant.

51 OGH, 17.02.2014, 4Ob203/13a, published e.g. in jusIT 2014/47 S 92 (note Thiele): The picture of a dead lawyer was used in a way to express his (alleged) connection to the red-light society. Injunctive relief against an online journal. However, this was a case against a content provider, not a host provider.

52 Thiele, Unbefugte Bildaufnahme und ihre Verbreitung im Internet – Braucht Österreich einen eigenen Paparazzi-Paragrafen?, RZ 2007, 2, p. 6. Zöchbauer, Schutz vor Lichtbildaufnahmen und deren Veröffentlichung - Persönlichkeitsschutz an der Schnittstelle der § 16 ABGB, § 78 UrhG und auch des DSG, Medien und Recht 2013, 255, 258: „Als normative Basis für ein allfälliges "Fotografierverbot" eignet sich – im Gegensatz zum Recht am eigenen Bild nach § 78 Abs 1 UrhG – die Bestimmung des § 16 ABGB".

53 However, there seem to be no cases on privacy and defamation for blocking against access providers. In these cases removal seems the better remedy from a practical perspective.

54 Injunctive relief against an access provider might be linked to more requirements than against host providers. Such remedies against host providers were recognized quite some time ago in Austria (for a discussion see M. Neubauer, Zur Haftung und Auskunftsverpflichtung von Providern, MR-Int 2008, 25, 27).

55 21 December 2006, 6Ob178/04a, published e.g. in MR 2007, 79 (note Thiele).

this rule does not concern the wrongfulness of the acts of the host providers which is something which has to be examined according to the Austrian Civil Code, the Act on Unfair Competition or the Act on Copyright. The Austrian Highest Court explained the difference between claims for damages and injunctive relief; only the former would be covered by the liability privileges according to the Act on Electronic Commerce. An action for injunctive relief can be based on the rule of defamation in the Austrian Civil Code (§ 1330 sect. 1, libel, and sect. 2, damage to the reputation). These rules contain a very far reaching definition of dissemination; also simple posting of others statements on its own homepage is covered. If a violation has become known to the host provider, it also has an **obligation to control and examine** similar contents for further violations. Such an obligation is adequate since the claimant is subjected to severe violations; it is, according to the Austrian Highest Court, also adequate in the light of the **freedom of expression according to Art. 10 ECHR**. In the abovementioned case, this obligation was violated since the defendant did not immediately remove all (other) postings that confirmed or supported the removed statement. The removal only took place two weeks later, and was too late. Hence, there was a right to an injunctive relief.

One commentary on this decision states that things would be different if the platform was a live chat platform. Live statements could not be controlled.[56] Other commentaries say that the obligation to observe and remove content would cover all forms of online-chats, platforms and published letters to the editor (hosts). A host provider can, where the wrongfulness is obvious and can also be understood by a legal amateur, be obliged to **post-control** and remove offending contents. . A generally accepted **reaction time would be three days**. There would be no general difference between commercial and non-commercial platforms; however, non-commercial platforms should be given more leeway.[57] Such guidelines seem to be in conformity with the ECtHR judgement in the Delfi case.

Excursus: Claims for damages or identification of users against a host

A different question would be if the platform operator (media companies, chat-rooms, blogs, etc.) was regarded as a **host provider** and can profit from the liability privileges concerning financial reparation (damages) contained in the Austrian Act on E-Commerce[58]. This question becomes more important after the recently rendered Delfi-decision of the ECtHR.[59]

According to the Austrian view, e.g. any **internet-media** is clearly regarded as a **host-provider**[60] with the consequence that there are no damages to be paid. However, there are (as a sort of counter balance) rules on **information obligations** of the host provider[61] which take a central role in current discussions in Austria. The host is, according to the Austrian Highest Court, denied the right to plead editorial secrecy[62] for (moderated[63]) postings. However, in the absence of the registration of the

---

56 Pichler, Besondere Kontrollpflicht für Host-Provider, ecolex 2007, 189.

57 Thiele, note to OGH 21.12.2006, 6 Ob 178/04a, MR 2007, 79.

58 § 16 sect. 1 ECG.

59 Delfi AS v. Estonia, 16 June 2015, Appl. No. 64569/09. Also the Papasavvas case of the ECJ (11 September 2014, C-291/13) seems of little relevance for this study since it only concerned the payment of damages, not the removal (see e.g. Staudegger, EuGH: Providerhaftungsprivilegien bei Verleumdungsklage gegen Presseunternehmen, jusIT 2015/4).

60 So clearly the materials of the legislator (RV 817, 21. GP) and, e.g. Zankl, ECG, 2002, § 16 no. 222, host providers are: Chat-Forum, E-mail or sms services, someone opening his site for postings and comments, electronic editorial letters in media or a journal's web pages, internet auctions, etc.). Host provider is understood to be a wide term. Unlike in Estonia according to the Delfi case (loc. Cit.), where a media web pages was not regarded as a host for postings.

61 § 18 sect. 4 ECG.

62 E.g. OGH 23.1.2014, 6 Ob 133/13x. Published, e.g. in jusIT 2014, 91, note Mader. The editorial secrecy (Art. 31 Media Act) did not apply because the information (e-mail-adress of the offender) was not

offender, anonymous registration and posting or data protection rules[64] may prevent or hinder a successful pursuit of the claim against the offender by the insulted person (victim).

This rather odd legal situation is regarded as detrimental to the media landscape as such because there are many insulting comments in web-postings in Austria.[65] To improve the legal situation, it is suggested that the categorization as a website-media-provider (according to the Austrian Media Act[66]) and the quality as a host provider (according to the E-Commerce Act) should exclude each other.[67] This view would probably mean that those responsible for a media enterprise (including its webpages), should no longer qualify as a host provider.[68] The responsibility provisions of the **Media Act** would instead apply (see below).

Special rules according to the Austrian Media Act

As already mentioned in the introduction, recent case law[69] applies the Austrian Media Act (*Mediengesetz*) provisions on websites. The Media Act provides for a compensation in cases of defamation, slander, mockery and libel, violation of the most private areas of life, for revealing identities in certain cases as well as violation of the presumption of innocence in the media.[70] The Media Act stipulates also a sort of special procedure for the **deletion of websites** (or part of it), if the website is under the control of a media-editor (*Medieninhaber*).

In principle, almost all regular Internet websites with at least some publicist function fall under the term "media" according to the Austrian Media Act.[71] Also, websites which serve purely commercial

---

collected in the course of some journalistic activity. Symptomatically, the removal of the insulting material was done immediately after the notice of the insulted ex-politician (who was convicted by a criminal court for corruption) and was not a matter of the dispute. The Austrian Court explicitly denied the opposite position of the Swiss Federal Court (MMR-Aktuell 2010, 311076, 10.11.2010, Az. 1B – 44/2010).

63 OGH 15 December 2014, 6 Ob 188/14m. Before publication, the host controlled the postings by a computer program ("Foromat") and by staff members.

64 OGH, 22 June 2012, 6 Ob 119/11k, jusIT 2012/61 S 134 (Mader), ecolex 2012/367 S 904 (Anderl), ZIR 2013,56 (Briem): The claimant (an offended female military officer) would have had no possibility to use the dynamic IP-address in a legal way, since the telecom company was not allowed to inform about the client to the specific IP-address. Therefor the IP-address was regarded as not necessary to pursue her rights.

65 Austria has been called the "Country of shitstorms" (https://dnp14.unwatched.org/content/land-der-shitstorms-%C3%BCber-hasspostings-und-welche-rolle-die-anonymit%C3%A4t-beim-digitalen-wutausb). It has been suggested that anonymous posting be stopped in order to impose responsibility.

66 Including a liability for carelessness (§ 6-7 Media Act).

67 Staudegger, Medieninhaber als Hostprovider? jusIT 2015/34, p. 86, 93.

68 Staudegger, Haftungsprivilegierung des Hostproviders oder Medieninhaberschaft – tertium non datur, ALJ 1/2015, 42–66 (http://alj.uni-graz.at/index.php/alj/article/view/36).

69 In a penal case: OGH 29 April 2015, 15 Os 14/15w, 15 Os 15/15t: The case concerned anonymous third party comments on the Facebook page of a politician. The comments insulted another (third) politician. The host did remove the comments a few days after notice following receipt of legal advice. The principle question was if a few days are still in good time or if the removal should have taken place immediately. The answer was that legal advice and a few days of time for such device is still in conformity with the Media Act and the host provider privilege.

70 § 6 – 7 c Media Act.

71 § 1 sect. 1 nr. 5a Media Act: A "periodical electronic medium" is a medium which is electronically a) broadcast (broadcast programme) or b) to be downloaded (website) or c) disseminated in comparable makeup at least four times each year (recurrent electronic medium).

or private purposes are "media" in the sense of the Media Act.[72] One main objective of the Media Act was (and is) to safeguard the freedom of speech according to the ECHR.

The relevant rules (e.g. on defamation or slander) contain rules on damages to be paid.[73] Regularly, there are adaptations of the rules in the Media Act for websites. E.g., no claims may be raised, if they concern download availability on a **website**, provided that the media owner or one of his employees or agents has not failed to use **due care**.[74]

A person affected can file his or her claim for an indemnity in the course of the **criminal proceedings** in which the media owner is involved as defendant. If no criminal proceedings are initiated, the claim can be submitted in a separate civil law filing. With regard to the proceedings on a separate filing, the provisions for criminal proceedings instituted on the basis of a private prosecution shall apply.[75]

What is of interest for this study is that the Media Act introduced some **special provisions for web-sites** in 2005.[76] According to section 33 sect. 1 of the Austrian Media Act, a **sentence** handed down in connection with a media contents offence shall, on the request of the prosecution, include the **deletion** of the parts of the **website** constituting the penal act (withdrawal from circulation).

The removal or deletion of parts of a website can also be ordered as an **interim measure** of protection:
the court may order the **deletion** of the parts of the website constituting the penal act (confiscation) if the negative consequences of the confiscation will not **unreasonably outweigh** the interests of protection of the right which provides the reason for the confiscation. The confiscation is in any case inadmissible if the interest of protection of the respective right can also be satisfied by publication of a notice on the proceedings instituted.[77]

It is a condition of an order for deletion that criminal proceedings or separate proceedings are being conducted on account of the trial of a media contents offence (or separate proceedings have been applied for), and that the prosecution or the applicant have expressly **requested** the deletion as part of those separate proceedings.[78]

The decision ordering the deletion shall state which passage or presentation of the media product and which suspected offence has been the reason for ordering the deletion.[79]

---

72 However, if a site is purely private, there are adaptations to the remedies available under the Media Act: § 21 (Restriction of the application to particular websites): "§ 9 through § 20 shall apply only to **websites containing information beyond the presentation of the personal sphere** of life or the presentation of the media owner, suitable to influence public opinion". The particular rules on Media offences are to be found in §§ 6 to 7c Media Act, which means that they are also applicable for "purely private" websites.

73 § 6. (1) Media Act: If an offence is committed via the media, such as defamation, libel, slander, insult or ridicule, the person affected is entitled to claim from the media owner an indemnity for the injury suffered. The amount of the indemnity depends on the scope and the effects of the publication, in particular on the type and circulation of the medium; the preservation of the economic basis of the media owner is to be respected. The indemnity must not exceed 20,000 euros, in the case of slander or for particularly serious effects of libel or slander, the maximum is 50,000 euros.

74 § 6 sect. 2 lit. 3a Media Act.

75 §§ 8 and 8a Media Act.

76 So called MedienG-Novelle 2005, BGBl. I 2005/49. That is to say after the E-Commerce Act in 2001.

77 § 36 sect. 1 MedienG.

78 § 36 sect. 2 MedienG.

79 § 36 sect. 3 MedienG.

A decision on an order for deletion may be appealed against to the court of the next highest instance. The **appeal** has no suspending effect.[80]

There is even a particular rule which has been put in place for the **enforcement** of the withdrawal and confiscation of websites.[81] In cases where a **sentence** imposing deletion of the parts of the website constituting the penal act (confiscation, *Einziehung*) or the deletion of the parts of the website constituting the penal act is **ordered** (confiscation, according to Austrian terminology: *Beschlagnahme*), the media owner shall be ordered to comply with the order of the court within an adequate timeframe to be set for such compliance on his or her part. The media owner shall inform the prosecutor or the applicant without delay that the parts of the website constituting the penal act have been deleted.

If such court order has **not being complied** with in due time or has not being complied with adequately, a **fine** shall be imposed on the media owner to be paid to the prosecutor or to the **applicant** upon the prosecutor's or applicant's motion in the independent proceedings, after the media owner has been heard. A fine of up to **2000 euros** shall be due **for each day** on which the parts of the website constituting the penal act continue to be available for download after expiry of the term set by the court. The amount of the fine shall be determined in accordance with the weight of the penal or the independent proceedings, the significance of the publication constituting the penal act and the personal and financial circumstances of the media owner.[82]

A **complaint** against a court decision regarding a fine imposed or waived may be lodged with the court of the next highest instance. If a fine has been imposed because the deletion has not been duly effected and an appeal has, in the meantime, been filed against the decision on the fine, no further fines shall be imposed for the duration of the appeals proceedings, if the deletion in dispute has been effected in a way which broadly respects the order for deletion.[83]

If the defendant (media owner) wins the case, he or she may apply to be authorized to publish a short respective message in a form complying with particular rules.[84] Such application shall be filed within six weeks after termination of the legal proceedings. The media owner is entitled to claim from the private prosecutor, or from the applicant, **compensation for the cost of such publication** as well as for the cost of the publication of the message under special provisions. The claim for compensation for cost for a publication shall be filed within six weeks after termination of the legal proceedings, for a publication, the claim for publication under sentence 1 within six weeks after publication of the notice on the outcome of the proceedings. If the termination of the proceedings is based on a mutual agreement, the private prosecutor or the applicant shall bear the cost of publication only to the extent this has been mutually agreed upon. If a notice has been published and **a decision for withdrawal** has been made or the decision has been **rendered**, and availability has been given on a **website**, the media owner may ask for authorization to publish a brief notice to this effect. Such application shall be filed within six weeks after termination of the legal proceedings. The media owner is entitled to claim compensation against the **author of the media contents offence** for the cost of such publication. Such compensation shall be claimed under civil law proceedings.

---

80 § 36 sect. 4 Media Act.

81 § 36a Media Act.

82 § 36a sect. 2 Media Act refers to § 20 paras 2 through 4 Media Act (procedure), which shall apply accordingly.

83 § 20 sect. 4 Media Act.

84 § 39 Media Act.

At this point, it should be mentioned that it is rather sure that the abovementioned provisions of the Media Act on the deletion of websites can be applied to **two-party relationships**, i.e. if the content has been produced by the Media organization itself. In legal literature, as already mentioned above, it is strongly advocated that the rules on the Media Act shall also be applied to three-party relationships: something which has been confirmed by recent case law in 2015. The latter view might mean, that a media-editor would no longer qualify as a host provider, i.e. postings would be produced under his or her control and would therefore be his or her own content.[85] However, in latest jurisprudence it seems that the Media Act provisions were interpreted in line with the host provider privilege.[86] That would mean that there would be no difference between two or three party relationships.

Therefore, for the objectives of this study, we would say that these different views are of **minor importance**. This study does not directly address the question of liability for the payment of **damages**, but, rather, the **removal** of the content (injunctive relief). As was seen above, the Media Act provides a rather specific procedure for the removal of pages with specific fines to support enforcement. However, a host, also, as is seen above, can be forced to delete content according to the Austrian E-Commerce Act in connection with other rules (e.g. § 1330 ACC on defamation). Hence, for the particular remedy of removal there is not much of a difference between provisions of the Media Act and those of the E-Commerce Act. It would only be different if one would understand the Media Act provisions as independent of the host privilege, but this does not presently seem to be the case.

One might think that the Austrian jurisprudence will develop in the direction that a media editor can no longer plead the privileges of a host if it allows postings on their sites that constitute the specific types of **media offences** according to the Media Act (defamation, etc.). Such a solution seems also to be viable in the aftermath of the *Delfi* decision of the ECtHR (where online-media did not qualify as a host according to Estonian Law) and the *Papasavvas* case of the ECJ (where a media editor could not plead – in relation to his own journalistic content and not, of course, reader comments - according to Cyprus-law, host-privileges). Such a step could considerably reduce, also in Austria, the amount of hate speech and inadequate, anonymous postings.

However, in **all other types of case** (violation of intellectual property rights or where there is no publicist content, as e.g. mots likely in the guest-book decision), the above mentioned decisions of the Austrian Highest court will probably continue to be the leading cases.

Planned legal measure: Act on Protection of Justice

In the recent past, there have been more and more defamation attacks against judges or prosecutors on the internet. Such attacks could be pursued by such individuals individually on the basis of a right to privacy or defamation. However, judges and prosecutors often do not want to take civil action against such offenders. They regard this more as a problem for these professions in general and for public law. Hence, the Austrian legislator is currently considering a so-called Act on the Protection of Justice. Such an Act could include measures on removal against a host. However, for the time being, no draft text has been put forward for such legislation.[87]

Soft law removal: Radical Islamic Propaganda-videos

---

85 Staudegger, Haftungsprivilegierung des Hostproviders oder Medieninhaberschaft – tertium non datur, ALJ 1/2015, 42–66 (http://alj.uni-graz.at/index.php/alj/article/view/36).

86 See Fötschl, Das Haftungsprivileg des Host-Providers auf dem Prüfstand, MR-Int 2015, 47.

87 See e.g. http://diepresse.com/home/politik/innenpolitik/4726532/Justizschutz_Wenn-Richter-zu-Opfern-werden (November 2015).

For radical-Islamic propaganda videos, the Austrian Ministry of Internal affairs has launched an e-mail reporting system in March 2015. It is based on a "cooperation" with Google and YouTube. It covers only videos which include a reference to Austria.[88] Video-links can be sent to: stopextremists@bmi.gv.at. The link is transferred to Google/YouTube who will (themselves) decide in an accelerated procedure if the video will be removed or not.[89] Such removal would be done abroad, not in Austria. Such videos would not be blocked by Austrian ISPs.

Such form of "cooperation" seems to be the weakest form of action or measure. As much as the SICL can see, there is no explicit basis in Austrian law for such measures. However, there are more general rules and it is not clear if an explicit legal basis would be needed for such a very weak measure of transfer of information to Google/YouTube.

Appendix: Content control for online Audio-Visual Media

Some videos online, e.g. racial discrimination or terrorist videos, can have negative effects but under the Austrian system it can be difficult to get them taken down or blocked. This would seem to provide the background to attempts by Austrian authorities to apply the Audio-Visual Media Act to such online videos. The consequence of such application would not be removal (against a host) or blocking (against an ISP). It is more a sort of ex-post content control (in purely two-party situations: authority and content provider). So it is, in a narrow sense, outside the scope of this study. Nevertheless its basics shall be addressed here.

As a member country of the European Union, Austria had to transpose the Audiovisual Media Services Directive (AVMSD[90]). The Directive seems to be aimed overwhelmingly at television and video on-demand services. However, the Austrian legislator seems to have a rather broad understanding of "Audiovisual Media". In particular, the Austrian Audio-Visual Media Services Act (AMD-G[91]) defines on-demand audio-visual media services as follows: an audio-visual media service provided by a media service provider for the viewing of programs at the moment chosen by the user and at the user's individual request on the basis of a catalogue of programs selected by the media service provider (on-demand service).

This also covers internet videos of Austrian companies and Austrian citizens. The Austrian regulatory authority provides an online **public registry**. Amongst the announced and registered on-demand videos are critical information groups, citizen movements and, e.g. YouTube-channels.[92]

The line between purely private purposes and those not purely private seems to be difficult to assess. However, it appears that the Act (as with the Directive) is rather aimed at commercial activities. Audio-visual media service is defined as a service as defined by Articles 56 and 57 of the Treaty on the Functioning of the European Union. That is to say services for remuneration in the

---

88 http://www.bmi.gv.at/cms/BMI_Verfassungsschutz/stopextremists/start.aspx.

89 Zusammenarbeit mit Google/Youtube im Kampf gegen Terrororganisationen, see http://www.bmi.gv.at/cms/bmi/_news/bmi.aspx?id=3370504A447741744647553D&page=0&view=1 (June 2015).

90 Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive).

91 Federal Act on Audio-visual Media Services (Audio-visual Media Services Act – AMD-G), Original version: Federal Law Gazette I No. 84/2001, as amended by: Federal Law Gazette I No. 84/2013.

92 E.g. https://www.youtube.com/user/Schrauberitsch, of Mr. Joachim Held (seems to be a private person acting for rather private purposes). There are many other private video channels in the registry. However, the majority are commercial video sites of companies or online tv channels. For the online registry see https://www.rtr.at/de/m/Abrufdienste (site of the regulatory authority with a list of the registrations).

broadest sense. The principal purpose of the service is the provision of programs, in order to inform, entertain or educate, the general public by electronic communications networks.[93]

In Austrian legal literature it has been suggested that the AMD-G should **in fact not be applied** to e.g. self-presentation-TV for gardening or boat-repair, motoring-TV, events-TV, tourism-TV and "leisure-TV" (e.g. cooking-TV). These internet platforms would not try to compete in the process of the creation of opinions.[94] However, already the statement shows that the line of delimitation is hard to find.

The application of the media rules was expanded on web-TV and video-on-demand in an amendment of 2010. For this reason, the title of the Act was also changed from Private-TV-Act to Act on Audiovisual-Media. The legislator explained that purely private websites or video-portals should not be covered by the Act. They would not be services in the sense of the Treaty of the EU. For such pure private sites and portals, only the minimal requirements of the Act on Media (Mediengesetz) would apply.[95]

According to the Austrian AMD-G, Austrian providers of on-demand media services shall report to the regulatory authority their activity no later than two weeks before commencement of the activity.[96] The report obligation is connected with the obligation to pay certain fees.[97] If the regulatory authority finds, on the basis of a report, that a media service reported would obviously violate certain **minimal content requirements**, the regulatory authority has to take action.

The **minimal content requirements** are the following:

Audio-visual media services shall respect the **human dignity** and **fundamental rights** of others with regard to the presentation and content of those services.[98] Audio-visual media services shall not incite others to hatred on grounds of **race**, **sex**, **religion**, disability, and nationality.[99]

A further minimal content refers to protection of **minors**: In the case of audio-visual media services whose content might seriously impair the physical, mental or moral development of minors, the media service provider shall ensure by appropriate measures of conditional access that minors will not normally perceive such on-demand audio-visual media services.[100] Television channels must not contain programmes that may seriously impair the physical, mental or moral development of minors, in particular, programmes that involve **pornography** or gratuitous violence.[101]

---

93 § 2 nr. 3 AMD-G.

94 So Kogler, Fernsehänliches TV-On Demand. Was ist (k)ein „Audiovisueller Mediendienst auf Abruf"? MR 2011, 228, 229.

95 See the explanatory report for the proposal to the Act: Nr. 611 der Beilagen XXIV. GP - Regierungsvorlage - Vorblatt und Erläuterungen, p. 8.

96 § 9 sect. 1 AMD-G.

97 So called *Finanzierungsbeitrag* according to § 35 sect. 2 KOG (KommAustria-Gesetz, Act on the establishment of a regulatory authority).

98 § 30 sect. 1 AMD-G.

99 § 30 sect. 2 AMD-G.

100 § 39 AMD-G.

101 § 42 sect. 1 AMD-G.

The legal consequences against the content provider are: **monetary fines** and **prohibition** (take down) of the audio-visual media service. Every prohibition decision has to be examined according to the test of proportionality stipulated by Art. 10 of the **ECHR**.[102]

Until recently, there was a **procedure pending** in front of the **ECJ** (*New Media Online*[103]). The Austrian Highest Administrative Court has asked the ECJ if an audiovisual medium service has to be "TV-like". In this particular case, the Austrian regulatory authority decided that an internet site (including videos) of a daily newspaper (*Tiroler Tageszeitung*[104]) would be such a service and would have to respect the obligations in the AMD-G. The site contained some parts with a catalogue of short-videos showing local news. In Austrian legal writings it was said, that the pending decision of the ECJ would have a big impact on e.g. **YouTube**.[105].

The **Opinion** of the **Advocate General** Szpunar was delivered on 1 July 2015. According to the opinion, an internet portal of this kind, such as the *Tiroler Tageszeitung Online website*, does **not meet the requirements for being regarded as an audiovisual media** service within the meaning of the Directive.[106]

However, the ECJ decided[107] that the concept of 'programme' must be interpreted as including, under the subdomain of a website of a newspaper, the provision of videos of short duration consisting of local news bulletins, sports and entertainment clips. Assessment of the principal purpose of a service making videos available offered in the electronic version of a newspaper must focus on whether that service as such has content and form which is independent of that of the journalistic activity of the operator of the website at issue, and is not merely an indistinguishable complement to that activity, in particular as a result of the links between the audiovisual offer and the offer in text form. That assessment is a matter for the referring court.

We will probably see a stronger content control of this kind within the EU. That should reduce the need for removal or blocking, but only within the EU. It is rather clear that the more problematic material comes from outside the EU.

---

102 See the explanatory report for the proposal to the Act: Nr. 611 der Beilagen XXIV. GP - Regierungsvorlage - Vorblatt und Erläuterungen, p. 70 to § 9 sect. 7 AMDG: Im Lichte des Art. 10 EMRK ist eine Untersagung stets auf ihre Verhältnismäßigkeit zu prüfen.

103 C-347/14.

104 www.tt.com. For the time being (June 2015), the part on videos is not online, probably due to the pending procedure.

105 Thiele, VwGH : Vorabentscheidungsersuchen zur Qualifizierung der Videoplattform einer Online-Zeitung als audivisueller Mediendienst (auf Abruf) iSd RL 2010/13/EU, jusIT 2014/82.

106 Nr. 55 of the opinion: "Firstly, the emergence of multimedia internet portals containing audio and audiovisual material in addition to written content and photographs is not the result of the technological development of television, but an entirely new phenomenon linked primarily with the increase in the bandwidth of telecommunication networks. Secondly, the multimedia nature of portals such as the Tiroler Tageszeitung Online website does not permit the audiovisual content placed on it to be analysed separately from the rest of the portal, even if those audiovisual materials are collected in a separate section of the portal. The essence of a multimedia service is the combination of different forms of communication — word, image and sound — and the specific architecture of the portal is merely a secondary technical aspect. Thirdly and finally, such a multimedia internet portal is the current form of what the legislature, when working on the Audiovisual Media Services Directive, could still describe as the 'electronic version of newspapers or magazines'".

107 21 October 2015, Case C‑347/14.

3. Procedural Aspects

For **legal blocking**, the most important procedural guidelines are found above under 2.1. in a decision of the OGH (24 June 2014[108], as explained above in 2.1. for violations of intellectual property rights). In this decision, the different procedural positions of all parties and concerned persons are explained extensively. This decision attempts to expressly safeguard all involved fundamental rights. Since this is the only hard law blocking measure in Austria, this decision is the only relevant factor. The main problem is that there is no specific legislation. The Austrian Highest court tries hard to bring the blocking measures and procedural safeguards under the umbrella of the Austrian Act on Civil Enforcement. There remain however considerable problems (see the discussion of the decision under 2.1).

For **soft law blocking**: The internet page of the stopline.at (for blocking of child pornography and Nazi propaganda) refers to a broad procedure for blocking on a voluntary basis**.** Of course, complaints against such blocking are probably relatively infrequent. However, if one is not satisfied with the activity of Stopline for any reason, one may send a detailed objection to the email address *beschwerde@stopline.at*. A complaint will be forwarded to the **Stopline advisory board** for further processing. The Stopline Board is a communication platform between the business community, the internet industry and the public authorities. Specialists like lawyers and university professors contribute additional know-how expertise. The Stopline board has 3 - 4 meetings per year. This board supports the general cooperation of the different organizations in their fight against illegal content on the internet, provides the exchange of knowledge, and enables mutual assistance. Additionally, the Stopline board is responsible for the operation of Stopline itself. It discusses the internal procedures and competences, and defines key aspects of its activity.

For legal removal, see the judgments referred to in 2.2. above on intellectual property and defamation cases. The main problem here is to identify procedures regarding when and how the host is being informed and has actual knowledge. If the host has knowledge, the next problem is how obvious a legal violation has to be. The next question is if the host may consult a lawyer for his opinion: this is answered in the affirmative by Austrian courts. This non-law based procedure can become rather complex and it can be difficult to convince a host to take down material.

For soft law removal, procedural problems do not matter since such removal is done by the hosts (mainly abroad) on a voluntary basis. One might refer in particular to the guidelines of Facebook and YouTube.

4. General Monitoring of Internet

According to § 18 sect. 1 ECG, the service providers mentioned in §§ 13 to 17 (access and host providers) shall not be required to monitor in a general fashion the information stored, transmitted or made available by them or to actively research circumstances indicating illegal activity. To our knowledge, there is no general monitoring of the internet in Austria. However, there could be legal developments in this direction (see below on developments).

---

[108] 4Ob71/14s, published in numerous Austrian legal journals, e.g. ecolex 2014/375. And in a German journal: GRUR Int 2014, 1074.

Soft law monitoring and removal in case of child pornography and Nazi propaganda

With regard to the soft law removal of child pornography and Nazi propaganda and other extremist material, there are some special forces within the Ministry of the Interior (Criminal Intelligence Service).[109] The reports to the so called "Meldestelle" can be done by everybody and anonymously.

The so called "www.stopline.at" is a public online-hotline to report child pornography and Nazi propaganda. The Criminal Intelligence Service is responsible for child pornography, the Federal Agency for State Protection and Counter Terrorism is responsible for national socialist offences. Stopline.at can be contacted by everybody to report **child pornography offences**[110] as well as "**national socialist offences"**[111]. The ISPs do participate in this cooperation and will remove such sites, if hosted in Austria. The "legal" basis for this removal cooperation of the authorities and the ISPs is a **resolution** of the Austrian Parliament. [112]

For the time being, when reports are submitted to Stopline.at, the hotline operators check whether the material is actually illegal according to Austrian legislation. If the reported content is deemed illegal, Stopline.at immediately contacts the responsible public authorities, the affected Austrian ISPs, and, where applicable, foreign partner hotlines within the INHOPE network. The Stopline.at has been incorporated within the ISPA (the Internet Service Providers Austria, the umbrella organization of the Internet economy) as an institution of **voluntary self-control** of the Austrian ISPs, and it is subject to the Code of Conduct of the ISPA members. If the child pornography or Nazi material is illegal according to Austrian Law, the ISP will **remove** (block) the site.[113]

Stopline only takes action if the relevant content contains child pornography or national socialist propaganda. However, if any other possibly illegal contents are reported to the Stopline, the Stopline agents will also try to provide assistance in these cases. Further sources of information and contact points will be forwarded if needed.[114]

For the specific crime of pornographic depiction of minors (§ 207a Austrian Penal Code) it is also explicitly said that a host provider may be penalised according to this rule if he does not remove the content after having been informed of the pictures or movies (notice and take down). Hosts can be regarded as **co-perpetrators** who commit the criminal act by omission if they fail to block or remove the content. Under Austrian penal law however, an omission is only punishable if there is a legal duty to act. Such duty to act can be determined, for a host, from the Austrian Act on Electronic Commerce (according to § 16 sect 1 no 2 ECG).[115] However, such a duty applies only to hosts (removal), and not

---

109 http://www.bmi.gv.at/cms/BMI_Verfassungsschutz/ .

110 § 207a StGB (Criminal Code) - Pornografische Darstellungen Minderjähriger.

111 Verbotsgesetz (national socialist prohibition law), Verfassungsgesetz vom 8.5.1945 über das Verbot der NSDAP. In Austria, the denial of national socialist crimes as well as the propagation and glorification of national socialist ideas is liable to prosecution. In contrast to this, countries like England or USA protect such activities by the right of freedom of opinion and speech. There is no legal basis for counteractive measures in these countries.

112 Entschließung des Nationalrates vom 19.9.1996 (21/E XX.GP, 165/UEA) betreffend die „Verhinderung des Missbrauchs des Internet, insbesondere im Zusammenhang mit Kinderpornographie und NS-Wiederbetätigung" (Resolution on the prevention of the abuse of the internet in connection with child pornography and Nazi Propaganda). A resolution is a political declaration and not legally binding. The report hotline for child pornography on the internet was launched in March 1997. See: http://www.parlament.gv.at/PAKT/VHG/XX/UEA/UEA_00165/index.shtml (November 2015).

113 Austrian Report Centre against Child Pornography and National Socialism on the Internet, ISPA report: http://www.stopline.at/fileadmin/stopline.at/content/dateien/Folder_Stopline-engl.pdf, p. 4.

114 http://www.stopline.at/en/meldung/report-processing/.

115 Philipp, in Wiener-Kommentar zum StGB, 2. Ed., March 2014, § 207a para. 18.

to ISPs (blocking).[116] This means that an Austrian host faces serious consequences if it fails to remove after notice. However, hosts of such criminal material are hardly ever placed in Austria. The same is true for terrorist material. Therefore, the SICL would think that it makes sense that the Austrian authorities rather try to convince foreign hosts by conviction and soft means to remove material (placed abroad).

However, from the perspective of human rights law, such a resolution of Parliament might be sufficient for such "voluntary" removal indicated by authorities. Such removal of illegal material hosted in Austria or taking contact with foreign partners should be in line with human rights standards. To our knowledge the stopline.at does not block any content but only removes content.

Legal developments in the field of monitoring

The legal framework does not seem to be satisfactory for state authorities. Hence, for the time being (as at the end of November 2015), the Austrian government has sent a draft to Parliament, on a so-called Act on the Protection of a State. The main purpose is protection against spying activities, terrorism and extremist activities. This draft contains the authorization for the new central authority to search on the net and to work with the data gained in this way. Discussions are very vivid and there has been considerable protest from civil society.[117] It cannot presently be foreseen (as at the end of November 2015) if the draft legislation will be accepted.[118] An important vote is foreseen for 1st December 2015. The prospective entry into force would be the middle of 2016. As much as we can see at the moment, there are no measures on blocking or removal in the proposed draft legislation.

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

The ECHR has traditionally had a very strong influence in Austria. As such, it forms part of Austrian constitutional law.

With regard to the legal blocking measures in the field of intellectual property law, the Austrian Highest court closely follows the position of the ECJ on human rights. We consider that such blocking is also in conformity with the ECHR. The law is foreseeable and proportionate and provides legal remedies. However, there are also many legal writers who criticize the blocking measure and associated procedures. The main argument is that such blocking measures are not very efficient and are technically easy to circumvent (see above at 2.1). The ISPA has said that the legal ruling of the Austrian court is difficult (if not impossible) to follow since it leaves the concrete decisions to the ISPA. The ISPs have to arrive at the outcome that there are no infringements. But that seems technically impossible. However, the Austrian courts have insisted on their approach (see above at 2.1).

As to soft law removal (only for child pornography and Nazi propaganda, stopline.at), we also consider that such removal (if hosted in Austria) is in line with the ECHR. There are procedural measures in place for complaining about such measures. However, given the heavy illegal nature of such material, there will hardly ever be complaints. There seems to be no blocking measures by

---

116 Brenn, E-Commerce-Gesetz, 2002, § 13, p. 266, 268: access providers are regularly not deemed to be co-perpetrators, even if they know about the illegal content. A duty to act only exist for the informed host (§ 16 sect. 1 no. 2 ECG).

117 E.g. the platform https://www.staatsschutz.at/.

118 For the draft and the discussion : https://www.parlament.gv.at/PAKT/VHG/XXV/ME/ME_00110/. (It was accepted on 27 January 2016, i.e. after the termination of this study (State Protection Act).

stopline.at. If the illegal material is hosted abroad, the only measure is co-operation with foreign partners. We would not think that such soft cooperation would need a particular legal basis, according to the jurisprudence of the ECtHR.

For hosts, the situation is a bit different, because they may be characterized as co-perpetrators. The Austrian E-Commerce Act contains a special duty for the host to act, in circumstances where he gets active knowledge. That can constitute a **legal basis** for being a co-perpetrator under penal and in civil law. Such a thread for legal liability (under penal or civil) law, constitutes also a legal authorization to remove content. It is, according to our view, also a sufficient legal basis for the removal of the material in perspective of Art. 10 ECHR.

With regard to the legal removal of content by hosts, we estimate that the **host provider privilege** is, for the time being, respected to a rather large extent in Austria. However, there are tendencies to reduce the application of the privilege; such reduction should nevertheless be in line with the *Delfi* decision of the ECtHR.

An overall assessment is as follows: For the time being (end November 2015), Austria offers comparably very unconstrained freedom of expression on the net. Future developments, however, have the potential to restrict such freedom, for blocking of internet content, as well as for its removal.

Andreas Fötschl
14.12.2015

Revised on 03.05.2016 taking into consideration comments from Austria on this report.