

XI. REGULATORY ISSUES OF HATE SPEECH IN AUSTRIA – AN EXEMPLARY REGULATORY MODEL IN EUROPE

DE NEGRI LAURA

1. Hate speech and constitutional background – fundamental rights and cyberbullying in Austria

In Austria, the legal framework surrounding fundamental rights and cyberbullying is shaped by both national laws and international human rights standards. The relationship between these two areas is complex, as it involves balancing the protection of individual rights with the need to address the harms caused by cyberbullying. Fundamental rights in Austria are enshrined in the Austrian Constitution¹ and have their foundations in the European Convention on Human Rights² (ECHR), to which Austria is a signatory. These rights include, but are not limited to, the right to freedom of expression, the right to privacy, and the right to personal dignity. These rights are considered the cornerstone of democratic societies and are protected by the judiciary. The right to freedom of expression is particularly relevant in the context of cyberbullying. While this right allows individuals to express their opinions and ideas freely, it is not absolute. Restrictions on freedom of expression are permissible under certain conditions, such as when it is necessary to protect the rights and reputations of others, national security, public

1 Constitution of Austria (*Bundes-Verfassungsgesetz*), BGBl 1930/1, <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10000138>

2 European Convention on Human Rights https://www.echr.coe.int/documents/d/echr/convention_ENG

order, or public health and morals. The right to privacy and the right to personal dignity are also central when considering cyberbullying. Individuals have the right to have their personal data protected and their personal integrity respected. Cyberbullying often involves violations of these rights through the unauthorized sharing of personal information, harassment, or other forms of online abuse.

Having regard to the constitutional protection of fundamental rights Austria has taken steps to regulate cyberbullying through various legal measures. The areas where the regulation is applied include: criminal law, civil law, media law. Austrian criminal law addresses cyberbullying through provisions that criminalize stalking, defamation, and insult. These laws are applied to acts committed via digital platforms, thus encompassing cyberbullying. Victims of cyberbullying may also seek remedies under civil law, including injunctions and claims for damages. Civil law can be used to protect the rights to privacy and personal dignity. Concerning media law, specific regulations apply to media content, including content published online. These laws aim to prevent the dissemination of harmful content and can be used to combat certain forms of cyberbullying.

The challenge in regulating cyberbullying lies in balancing the protection of fundamental rights with the need to prevent and remedy the harm caused by such behavior. Austrian law seeks to achieve this balance by allowing for certain restrictions on rights like freedom of expression when necessary to protect individuals from harm. However, any restrictions must be proportionate, necessary in a democratic society, and not exceed what is required to address the specific issue of cyberbullying. In conclusion, the relationship between fundamental rights and cyberbullying regulation in Austria is characterized by the need to protect individuals from harm while respecting the freedoms that are essential to democracy. Austrian law, in alignment with international human rights standards, provides a framework for addressing cyberbullying that respects fundamental rights and offers avenues for victims to seek protection and redress.

2. The regulation method of cyberbullying in Austria

Even if considerable evidence suggests that cyberbullying and traditional bullying cooccur, as do cybervictimization and traditional victimization,³ it is still appropriate to deal separately with offline and online bullying.

³ Gradingner, Stroheimer, Spiel: A Study on Bullies and Bully-Victims in Austria In. Qing Li, Donna Cross, Peter K. Smith, 2012, p. 267.

2.1. Hate speech in the offline space

The issue of hate crime has received a lot of international attention in recent years and Austrian legislation has reacted to this phenomenon, which requires a social response with reason. In recent years, Austria has amended its legal framework on hate speech in several steps, with the first comprehensive change in 2015, while the latest amendment is quite recent, from 2021. On 1 January 2021, the ‘Hate on the Internet’ (*Hass im Netz*) package of legislation entered into force, providing more effective protection against hate speech on the internet than before. After examining the current legal framework on hate speech, it is no exaggeration to say that Austria has a complex and exemplary legal framework to combat hate speech and online harassment.

The term ‘bias crime’, which is more criminologically accurate than the more commonly used ‘hate crime’, has not frequently been used in German and English legal literature,⁴ nevertheless, it covers not only situations where the perpetrators act on the basis of strong hostile feelings, but also motivations based on pejorative prejudice and discrimination. These motivations are linked to social structures of power and oppression⁵ that make members of certain social groups particularly vulnerable to attacks targeting core identity traits or immutable characteristics.

In a study⁶ published in 2021, the Austrian Institute for Legal and Criminal Sociology (Institut für Rechts- und Kriminalsoziologie) comprehensively examined the question of what makes certain crimes hate/prejudice crimes. The project came up with the following complex definition of hate crimes: prejudice crimes are punishable acts committed because the victims actually or presumably belong to groups that the perpetrators reject. They may be directed against life and limb, property, honour or other legal interests. In the case of such offences, it is of crucial importance that the victim or the object of the offence is selected precisely because the perpetrators consider it to represent a group against which they harbour derogatory prejudices. The perpetrators’ derogatory behaviour may also consist of perceiving a group as unduly privileged. The groups typically rejected by the perpetrator and typically deserving of special protection are defined by characteristics of identity (in particular gender, ethnic/racial origin, religion, sexual orientation, and ideology), physical characteristics (in particular age, disability, colour, illness) or social standing (in particular social status, homelessness).⁷

⁴ See Wickes et al., 2016.

⁵ See Perry, 2001.

⁶ Fuchs, 2021.

⁷ Fuchs, 2021, p. 12-13.

The above definition is based on the interpretation of hate crimes by the Organisation for Security and Cooperation in Europe's Office for Democratic Institutions and Human Rights (ODIHR) and, as a result, the Austrian civil society network Hate Crime Kontern.⁸ The phenomenon can be succinctly and catchily described as hate crimes are crimes motivated by prejudice against certain collectivities.

Austria has an obligation under international and EU law to prosecute and sanction such bias-based crimes adequately and to provide and evaluate data and statistics on prosecutions. The most important international legal bases include the EU Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law,⁹ the prohibition of discrimination in the Charter of Fundamental Rights of the European Union, which has been binding since 2009,¹⁰ the OSCE Resolution 9/0, Athens Ministerial Council Decision No 9.9.2009,¹¹ Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 on minimum standards on the rights of persons with disabilities,¹² the European Convention on Human Rights¹³ and, last but not least, the relevant case law of the European Court of Human Rights (hereinafter: ECHR) since 2003.

In 2015, the Austrian legislator, inter alia, in order to implement the above-mentioned international obligations, reformed the legal framework on hate speech, broadened the scope of protected groups and reduced the requirements of dangerousness and public danger. The current Criminal Code¹⁴ (hereinafter: StGB) specifically regulates hate speech. According to Article 283(1)(2)

8 OSZE-Büro für demokratische Institutionen und Menschenrechte: Gesetze gegen „Hate Crime“. Ein praktischer Leitfaden. (2011) <https://www.osce.org/files/f/documents/c/7/36431.pdf>

9 Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008F0913>

10 Charter of Fundamental Rights of the European Union Art. 21.

11 See the Document of the Seventeenth Meeting of the Ministerial Council, “Ministerial Declaration on the Occasion of the 25th Anniversary of the Adoption of the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment”, sections 8. and 9. <https://www.osce.org/files/f/documents/e/3/40697.pdf>

12 Directive 2012/29/EU of the European Parliament and of the Council of October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:315:0057:0073:EN:PDF>.

13 European Convention on Human Rights https://www.echr.coe.int/documents/d/echr/convention_ENG.

14 Austrian Criminal Code – *Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch – StGB)*, BGBl 1974/60.

StGB, not only the insulting of certain protected collectives (namely churches, religious assemblies or other groups of persons defined on the basis of race, colour, language, religion or belief, nationality, descent, national or ethnic origin, sex, disability, age or sexual orientation) but also the insulting of individuals on the basis of their membership of such groups is punishable as hate speech. This presupposes that the insult is intended to offend the human dignity of the members of the group or of the person and is likely to discredit or denigrate that group or person in the public eye.¹⁵

Austrian legislation contains two laws criminalising the most serious forms of hate speech: the Prohibition Act 1947¹⁶, which includes a ban on the use of National Socialist symbols and the dissemination of Nazi propaganda, and the StGB.

Article 3d of the Prohibition Act states that anyone who, in public or in the presence of several persons, in publications, in disseminated papers or illustrations, prompts, incites or attempts to incite a prohibited act as defined by § 1 or § 3 of the Prohibition Act, with the aim of glorifying the aims, institutions or measures of the National Socialist German Workers' Party, shall be punished with imprisonment for a term of five to ten years.¹⁷ If the offender or the activity is particularly dangerous, the offender shall be punished by imprisonment for a term of up to twenty years.¹⁸ Article 3h of the same Act punishes anyone who attempts to deny, grossly belittle, condone or justify the National Socialist genocide or other crimes against humanity committed by National Socialists in publications, on the radio, in another medium or otherwise in such a way that it becomes accessible to many people.¹⁹ The provisions of the Prohibition Act therefore prohibit not only denial, but also the denigration or justification of the crimes of the Nazi regime.²⁰

In addition to the Prohibition Act, the Austrian StGB contains a number of provisions directly restricting certain forms of hate speech. According to the law, hate speech is committed by anyone who publicly in such a way that it becomes accessible to many people prompts violence or incites hatred against a church or religious community or any other group of persons defined by the existing or absent criteria of race, colour, language, religious belief,

15 Fuchs, 2021, p. 18-19.

16 Prohibition Act (*Verbotsgesetz*) https://www.ris.bka.gv.at/Dokumente/ErV/ERV_1945_13/ERV_1945_13.pdf

17 Prohibition Act, Art. 3 d.

18 Prohibition Act, Art. 3 g.

19 Prohibition Act, Art. 3 h.

20 Austria: Responding to 'hate speech' 2018 Country Report, p. 18. <https://www.article19.org/wp-content/uploads/2018/09/Austria-Responding-to-Hate-Speech-.pdf>

nationality, descent, national or ethnic origin, sex, disability or age, or against a member of such a group expressly because of his/her membership of that group; anyone who insults one of these groups or a person because of his/her membership of such a group with the intention of violating the human dignity of the members of the group or the person in a way that is likely to disparage or degrade the group or person in the public opinion; and anyone who condones, denies, grossly trivializes or justifies war crimes and crimes against humanity that have been legally established by a domestic or international court, where the act is directed against one of these groups or against a member of such a group expressly because of membership of that group and is committed in a manner that is likely to incite violence or hatred against such a group or against a member of such a group. Hate speech is punishable by up to two years' imprisonment.²¹

The offender is also liable to prosecution if he commits the offence in a printed work, on the radio or by other means.²² The offender is also deemed to have committed the offence if he or she incites others to act violently against the groups listed above. In such a case, a custodial sentence of a minimum of 6 months and a maximum of 5 years may be imposed.²³

Any person who produces, promotes or makes available to the general public material, pictures or other representations of ideas or theories which incite hatred or violence against the above-mentioned groups, or their members shall also be considered committing this offence.²⁴

In addition to the relevant provisions of the Prohibition Act and Article 283 of the StGB, the provision on sentencing in Article 33(1)(5) of the StGB is the main legal basis for punishing bias crimes in Austria. According to this provision it constitutes an aggravating circumstance if the perpetrator has acted out of racist, xenophobic or other particularly reprehensible motives, in particular those directed against one of the groups of persons named in Section 283(1)(1) StGB or a member of such a group expressly because of their membership of this group.²⁵

In principle, hate/prejudice crimes can be committed by a wide range of intentional offences – the only requirement is that the offence is committed because the victim belongs to a group that the offender rejects.²⁶

²¹ StGB Art. 283. (1).

²² StGB Art. 283. (2).

²³ StGB Art. 283. (3).

²⁴ StGB Art. 283. (4).

²⁵ Fuchs, 2021, p. 22.

²⁶ Fuchs, 2021, p. 28.

2.2. Hate speech in the online space

Austria had a population of 9 million, with 8 million internet users and 7.2 million active social media users in January 2021, when the ‘Hate on the Internet’ package of legislation entered into force. 89.0% of the population use the internet and 79.9% use social media.²⁷ In addition to the positive effects of technological progress, hateful and offensive messages have also come to the fore at an alarming rate. In response to this problem, the Austrian legislator has recently adopted two laws to sanction action against content on the internet that is of criminal relevance and against hate speech on the internet: measures to combat hate speech on the internet²⁸ and measures to protect users of communication platforms.²⁹

The Act on Measures to Combat Online Hate (hereinafter referred to as the HiNBG) contains mainly private law and civil procedural provisions necessary to combat hate speech on the Internet, as well as criminal and media law sanctions.

As a result of the HiNBG, the provisions of the Austrian Civil Code³⁰ (ABGB) on personality law have been amended and the rules on the protection of the personality rights of deceased persons by their relatives have been made more precise.³¹ The law also allows for the so-called “blocking of the network” in cases where the infringement of personality rights is committed through an internet service provider. The liability of intermediary platform providers in cases of infringement of personality rights remains, but in certain cases internet service providers may be exempted from this liability.³²

The law also introduces a new civil procedural institution in this regard: the so-called Mandate Procedure (*Mandatsverfahren*).³³ This can be used in cases of significant violations of personality rights committed via electronic communications networks. If the action is for a serious violation of human dignity, the court may, on the basis of the plaintiff’s mandate, order the defendant to refrain

²⁷ Simsa, 2021, p. 18.

²⁸ The Federal Act on Measures to Combat Online Hate, Bundesgesetz, mit dem Maßnahmen zur Bekämpfung von Hass im Netz getroffen werden (Hass-im-Netz-Bekämpfungsgesetz, HinBG), BGBl I 2020/148.

²⁹ Communication Platforms Act, Kommunikationsplattformen-Gesetz (KoPI-G).

³⁰ Civil Code of Austria – Allgemeines Bürgerliches Gesetzbuch (ABGB), JGS 1811/946, <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001622>

³¹ Austrian Civil Code (ABGB) Art. 17. a.

³² Austrian Civil Code (ABGB) Art. 20.

³³ Bodzási, 2021; <https://jogaszegylet.hu/jogelet/uj-osztrak-torvenyek-az-interneten-megjeleno-jogserto-tartalmakkal-szembeni-fellepes-eszkozeirol/>

from further violations, even without a prior hearing and without the other party having been heard, and may also order interim measures. This is subject to the condition that the action must be based on clear and convincing evidence of the serious infringement alleged by the applicant.³⁴

Among the criminal law provisions of the Act, it is important to highlight the offence of harassment by means of telecommunication or computer systems, which is punishable by up to one year's imprisonment. A further offence is the production of unauthorized images, for which the law provides for a sentence of six months' imprisonment.³⁵

Media law provisions are contained in the Austrian Press and Other Published Media Act. Notable among these is a provision aimed at increasing the amounts of compensation. In the most serious cases, internet service providers can be ordered to pay damages of up to €100,000.³⁶

The other new Austrian law, the Act on Measures for the Protection of Users of Communication Platforms³⁷ (hereafter KoPI-G) – which has in the meantime lost its effect due to EU legislation –, aimed to ensure that internet service providers and communication platforms (such as Facebook, Twitter) have transparent and effective review and reporting systems in place to detect criminal content. The law also required service providers to report to the Austrian Communications Authority (*Kommunikationsbehörde Austria*)³⁸, the state supervisory body. Violations of this obligation were punishable by heavy fines according to the mentioned act.

It should be stressed that the provisions of the KoPI-G were not only applicable to undertakings established in Austria, but were also binding on undertakings established outside Austria. For the personal scope of the Act, it was relevant whether the undertakings operating communication platforms are profit-oriented. On this basis, the provisions of the new Austrian law were applicable to all undertakings operating a communication platform with at least 100,000 users and an annual turnover of at least €500,000.³⁹ The law was not applicable to training and educational platforms, nor to platforms directly linked to the journalistic offer of a media company.⁴⁰

A special situation was applied to so-called video-sharing platforms (e.g. Youtube), which were in principle not covered by the law. However, textual

34 Civil Procedure Code of Austria (ZPO) Art. 549.

35 Austrian Criminal Code (StGB) Art. 107.c.; Art. 120.a.

36 Austrian Media Act, (MedienG) Art. 8.

37 Communication Platforms Act.

38 Austrian Communications Authority.

39 Communication Platforms Act, Art. 1.

40 Communication Platforms Act, Art. 1.

commentaries on such video-sharing platforms are already covered by Austrian law.⁴¹

The question of what is understood by infringing content was of crucial importance for the practical application of the KoPI-G. Indeed, the review and notification procedures provided for by the law relate to infringing content. Austrian law did not extend the concept of infringing content to all possible unlawful content. For the purposes of the application of the KoPI-G, content which was in breach of the Austrian StGB and the National Socialist Prohibition Act of 1947 was considered to be of criminal relevance.⁴²

2.3. *Hate speech in judicial practice*

The case of the Green politician Sigrid Maurer in Austria has attracted more media attention than any other hate crime in recent years. Among other things, this case was one of the motives behind the ‘hate on the net’ package of laws, which was motivated by the need to effectively prosecute hate crimes. On the facts of the case Sigrid Maurer was accused of insulting a beer shop owner after he had ‘verbally raped’ her. An Austrian court ruled that Sigrid Maurer, who leads the Greens’ parliamentary group in the Austrian parliament, had the right to insult a man who had sent her obscene messages.⁴³

The ‘FPÖ MP’ case⁴⁴ concerned an FPÖ MP who, along with others, was accused of running a national socialist forum between 2009 and 2010. Posts on the forum incited violence and promoted right-wing, racist and extremist ideas. The accused had editorial and administrative functions on the website: he could block certain users, moderate posts, set rules for the forum and impose sanctions for non-compliance. The accused allegedly used a burning Star of David as a profile picture on his user profile and over the years posted messages such as “Jews should be gassed”, “Jews and Gypsies should be put in camps”, “Jews are biological carriers of crime” and “Jews are half human”. He was indicted under several provisions of the StGB and in May 2017 was found guilty under Article 283(2) of the StGB by the first instance court, the Vienna Provincial Criminal Court.⁴⁵ The defendant

⁴¹ Bodzási, 2021.

⁴² Bodzási, 2021.

⁴³ Politico: Austrian MP allowed to call beer shop owner ‘asshole’, court rules, <https://www.politico.eu/article/austrian-mp-sigrid-maurer-allowed-to-call-beer-salesman-asshole-court-rules/>

⁴⁴ *Freiheitlichen Partei Österreich* – a radical right-wing or far-right Austrian Party.

⁴⁵ Provincial Court for Criminal Cases Vienna, AZ 606 Hv 2/11h.

appealed to the Supreme Court⁴⁶, also arguing that it had not been proven that he had actually published these messages. The Supreme Court referred the case back to the first instance.⁴⁷ The Court found that the first instance court had not sufficiently proven the required level of intent on the part of the accused – as required by Article 283(2) StGB.⁴⁸

Another well-known case is the ‘Danish Student Facebook’ case, in which the defendant posted a link on Facebook to a national socialist website (nasjonalsamling.blogspot.de), accompanied by a flyer with national socialist content. In his Facebook posts, he called Muslims a ‘carcinoma’, claimed that “the Turkish and Negro races are primitive” and that “people of the Negro race are less intelligent”. The court of first instance, the Regional Court of Vienna, found him guilty under, inter alia, Article 283(2) StGB.⁴⁹ The defendant invoked his right to freedom of expression under Article 10 of the European Convention. He argued that he was not an Austrian citizen (he was a Danish student) and was not familiar with the relevant law. The Supreme Court confirmed the decision of the first instance court.⁵⁰ In the decision, the court concluded, inter alia, that the relevant law was generally known in Austria and that the defendant should have been aware of this legislation.⁵¹

3. Regulation of cyberbullying

3.1. Implementation of cyberbullying into the Austrian StGB

Today, privacy concerns are increasingly shifting to the Internet, and one of the consequences of this is that cybersecurity is also under increased threat and attention. The Internet provides a new medium for various forms of aggression, which necessitates the creation of new criminal offences and provides a medium for new crimes. The Austrian legislator has been monitoring

46 The defendant argued that the court did not make a reasonable decision and did not specify on what material the decision was based.

47 Decision of the Supreme Court of 30 May 2017, OGH 11 Os 20/17a.

48 Austria: Responding to ‘hate speech’ 2018 Country Report, p. 22. <https://www.article19.org/wp-content/uploads/2018/09/Austria-Responding-to-Hate-Speech-.pdf>

49 Decision of the Provincial Court in Vienna (*Landesgericht Wien*) of 19 January 2015, Z 608 Hv 3/14z.

50 Decision of the Supreme Court of 10 June 2015, 15 Os 40/15v.

51 Austria: Responding to „hate speech” 2018 Country Report, p. 22. <https://www.article19.org/wp-content/uploads/2018/09/Austria-Responding-to-Hate-Speech-.pdf>

developments in cyberspace for years and the 2015 Austrian criminal law reform, which was necessitated by circumstances, included a demand for cyberbullying to be included as a separate criminal offence.⁵² Technological developments, and in particular the continuing presence of new social media platforms, made it necessary to counterbalance the negative side effects of this with legislation.

In its explanatory memorandum for the legislative amendment, the relevant working group pointed out that the legal framework prior to 2015 did not provide adequate protection against cyberbullying, since, unlike ‘classic’ bullying, which is usually confined to a specific area or environment (school, workplace), acts committed on the internet are accompanied by widespread publicity. In the case of traditional harassment committed in offline spaces, it is easier for the victim to escape from the harassment by moving away from the place where the harassment took place, by leaving the environment in which he or she was harassed or by changing jobs. This is not possible in the case of cyberbullying and is the factor that distinguishes cyberbullying from ‘traditional’ bullying. On this basis, the Austrian legislator has taken the view that it seems justified to introduce a specific criminal law provision for cyberbullying. As regards the conceptual distinction, the legislator’s aim was to make a clear distinction between harassment and cyberbullying in the wording of the legislation, and as a result it was considered necessary to add the phrase “by means of telecommunication or computer systems” to the definition of cyberbullying.⁵³

The creation of cyberbullying as a separate criminal offence is a product of the 2015 criminal law reform. Prior to the introduction of Article 107c of the Austrian Criminal Code, cyberbullying was only punishable if it could be subsumed under other offences.⁵⁴ Certain acts of bullying, such as the dissemination of hateful posts or compromising images, could fall under the definition of defamation in some cases⁵⁵ or the offence of misuse of data under Article 63 of the Data Protection Act.⁵⁶ Other acts, although already covered by the definition

52 Justification for the StGB amendment (689 der Beilagen XXV. GP – Regierungsvorlage – Erläuterungen) p. 1. https://www.parlament.gv.at/PAKT/VHG/XXV/I/I_00689/index.shtml

53 “StGB 2015 Bericht der Arbeitsgruppe” p. 46. https://www.parlament.gv.at/PAKT/VHG/XXV/III/III_00104/imfname_366604.pdf

54 Justification for the StGB amendment (689 der Beilagen XXV. GP – Regierungsvorlage – Erläuterungen) p. 1. https://www.parlament.gv.at/PAKT/VHG/XXV/I/I_00689/index.shtml

55 StGB Art. 115.

56 Data Protection Act, Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), BGBl I 1999/165.

of cyberbullying, were not criminalised, although they had the same negative consequences for the victim. One could think of the dissemination of a purely embarrassing image that portrays a person in a bad light.⁵⁷

However, the whole phenomenon of cyberbullying was not covered by criminal law before 2015.⁵⁸ This shortcoming was noticed by the legislator prior to the 2015 criminal law reform, who concluded that the introduction of cyberbullying as a separate offence was the only logical way to address this complex problem. In 2013, the Minister of Justice at the time set up a working group called 'StGB 2015', whose task was to examine the law in force at the time and to draft the necessary changes to update the StGB.⁵⁹ Above all, the aim was to ensure that the law could cope with changes in society in a way that was in line with the modernisation of technology.⁶⁰

In counteracting the negative side effects of technological progress, in particular cyberbullying, by means of criminal law, the Austrian legislator paid particular attention to the tragic case of Amanda Todd.⁶¹ Amanda Todd was one of the victims of cyberbullying of teenagers who received the most attention and media coverage. In the autumn of 2009, the young girl wanted to make new friends, so she started chatting to strangers via webcam. She met a man who was older than her, seduced her and persuaded her to undress for him with nice words. Amanda stripped down to her underwear, not thinking anything bad would happen. He posted the photo online and forwarded it to her classmates. Amanda Todd was then harassed on a massive scale, particularly over the internet. The girl even changed schools, but soon her new schoolmates found out about the photo posted online and Amanda Todd was again bullied. In 2012, the then 15-year-old Canadian girl committed suicide because she could no longer stand the mass bullying she was receiving from her classmates, especially online. But before she committed suicide, she drew attention to herself and her fate with a YouTube video. In the black-and-white video, she holds handwritten messages in front of the camera and explains how he forced her to reveal herself to him.⁶²

57 Reindl-Krauskopf, 2015, p. 19.

58 Reindl-Krauskopf, 2015, p. 19.

59 Tipold, 2017, p. 31.

60 Report of the working group charged with drafting the proposals for the 2015 amendments to the StGB. (Bericht der Arbeitsgruppe StGB 2015 III-104 BlgNR XXV GP.) p. 3. https://www.parlament.gv.at/PAKT/VHG/XXV/III/III_00104/imfname_366604.pdf

61 Report of the working group charged with drafting the proposals for the 2015 amendments to the StGB, p. 46.

62 Hatheuer (2021) p. 9.

The ‘StGB working group’ proposed that the crime of cyberbullying should be included in the provisions on invasion of privacy.⁶³ However, the offence does not only show the characteristics of offences of invasion of privacy, but also elements of offences of violation of liberties and crimes against honour.

The concept of ‘cyberbullying’, proposed in the first round, has not been included in the law either – this offence is covered by the StGB under the heading “continuous harassment by means of telecommunication or computer systems”. The concept of harassment goes much further than criminal defence. To avoid misleading conclusions arising from a general interpretation of the term mobbing, it was finally decided to use the more difficult criminal heading.⁶⁴ By retaining the German criminal offence term, the legislator remained true to itself, since the term was not deliberately used for other offences, such as stalking or harassment, which is not a common term.

3.2. Analysis of the facts

Austria is now one of the states which treats cyberbullying as a specific offence in the Criminal Code. Cyberbullying has been a criminal offence in Austria since 1 January 2016. The term used in the StGB is “continuous harassment by means of telecommunication or computer systems”.⁶⁵ Anyone who, by using a telecommunication device or computer system in such a way that is likely to unreasonably interfere with the victim’s way of life, commits an offence against the honour of a person in a way that is perceptible to a large number of people for a longer period of time or makes facts or images of a person’s highly personal sphere of life perceptible to a large number of people for a prolonged period of time without their consent is punishable by imprisonment for up to one year or a fine of up to 720 daily allowances.⁶⁶

The classic phenomenon of bullying basically takes three forms – verbal bullying, physical bullying and psychological bullying. Cyberbullying usually takes the form of verbal or psychological harassment, but can also sometimes

63 Report of the working group charged with drafting the proposals for the 2015 amendments to the StGB, p. 10.

64 Report of the working group charged with drafting the proposals for the 2015 amendments to the StGB, p. 45.

65 StGB Art. 107c.

66 StGB Art. 107c. (1)

involve physical harassment, a typical form of which is the so called ‘happy slapping’.⁶⁷

In the case of verbal cyberbullying, the victim is insulted, hurt or teased in text messages, emails, chat rooms or other forums and blogs. When the authors talk about psychological cyberbullying, they refer to defamation through digital networks, the spreading of rumours and falsehoods, unconfirmed acquaintance marking on various social platforms and the like. This includes the posting of private photos, intimate films, etc. on Facebook, etc., where a few clicks will attract the attention of thousands of people who will become spectators within a short time.⁶⁸

3.3. Specific characteristics of the offence

3.3.1. Harassment by means of telecommunications or computer systems

As the name of the offence suggests, cyberbullying takes place in cyberspace. The use of digital media devices, such as a smartphone or a computer, therefore falls under this criminal offence⁶⁹ and is a mandatory element of the offence.

3.3.2. Ability to interfere to an intolerable degree with a person’s normal way of life

Whether an offence is capable of having an intolerable effect on a person’s way of life⁷⁰ is a matter for prior assessment. The offence must be serious enough in the individual case for the average person to feel compelled to change his or her way of life. A prerequisite for the commission of an offence under Article 107c StGB is that the offence must be capable of interfering to an intolerable extent with the way of life of a person. With regard to suitability, an objective-subjective test must be applied, i.e. the question must be asked whether an ordinary person in the given situation might have changed his or her lifestyle as a result of the acts.⁷¹ This should be interpreted broadly. If the victim withdraws from

67 “Happy slapping” refers to the phenomenon where fights are filmed with a mobile phone camera and then distributed as a video. https://www.oesterreich.gv.at/themen/bildung_und_neue_medien/internet_und_handy___sicher_durch_die_digitale_welt/3/1/Seite.1720710.html

68 Official website of the Austrian government: Was ist Cyber-Mobbing, Cyber-Bullying, Cyber-Stalking? https://www.oesterreich.gv.at/themen/bildung_und_neue_medien/internet_und_handy___sicher_durch_die_digitale_welt/3/1/Seite.1720710.html

69 Schwaighofer in Höpfel/Ratz, WK StGB § 107c Rz 5.

70 StGB Art. 107 c.

71 Schwaighofer in Höpfel/Ratz, WK StGB § 107 a Rz. 18.

the online presence or even deletes his or her profile from social networks, this is already an unreasonable restriction of daily life. These channels are now indispensable means of communication for most people, both in business and in private life.⁷² However, the victim does not have to actually change his or her lifestyle; the perpetrator's acts must merely be capable of unreasonably impairing the victim's lifestyle.⁷³

There is one more crucial element to cyberbullying, and that is that the victim must be aware of the perpetrator's behaviour. Naturally, the victim cannot be affected in his or her lifestyle to an intolerable extent if he or she is not aware of the offence.⁷⁴

3.3.3. *Continuous harassment that is felt over a long period of time*

According to Article 107c (1) StGB anyone who, by means of telecommunication or using a computer system, in a way that is likely to unreasonably impair a person's way of life,

- a) commits a criminal offence against the honour of a person in a way that is perceptible to a large number of people over a longer period of time, or
- b) makes a fact or image of a person's highly personal sphere of life perceptible to a large number of people for a longer period of time without their consent,

shall be liable to a custodial sentence not exceeding one year or a monetary penalty not exceeding 720 daily penalty units.

The wording 'continuous harassment', which constitutes the offence, was in the StGB until the end of 2020, and was replaced by 'continuous' with the introduction of the HiNBG. The primary consequence of this amendment is, that a single offence should also be sufficient for the state of affairs to be fulfilled. Also, if the perpetrator's act occurs over a prolonged period of time and is likely to unduly influence the person concerned in his or her way of life, an element of the offence is met. Therefore, it is possible that an offender may commit an offence under Article 107c by uploading an image to a digital network only once, provided that the image is visible/available for a longer period of time.⁷⁵ Since one of the characteristics of the offence is continuity, the context in which it is

⁷² Salimi, 2015, p. 191.

⁷³ Mitgutsch, 2020, p. 13.

⁷⁴ L. M. Hatheuer, 2021, p. 29.

⁷⁵ Schwaighofer in Höpfel/Ratz, WK StGB § 107 a Rz. 18.

carried out may also lead to the offence being committed by a single act or even omission.⁷⁶

3.3.4. *A qualified case of cyberbullying*

The law provides for a more severe punishment in cases where the offender's act results in the suicide or attempted suicide of the victim, the offender continues the act beyond one year. In this case, the offender is punishable by imprisonment for up to three years.⁷⁷

3.3.5. *Distinguishing cyberbullying from classic bullying*

Cyberbullying has been defined as a specific form of harassment which, although it shares some similarities with traditional harassment, has important differences when comparing the two offences. In the literature, it has been very aptly put that cyberbullying is in fact a very serious extension of face-to-face harassment: it is nothing more than "new wine in an old bottle".⁷⁸

The first and most striking difference is that cyberbullying, unlike traditional bullying, takes place in the digital world.

Another defining characteristic of cyberbullying is that the degree of anonymity in this crime is extremely high. This is because the perpetrators are often unidentifiable or very difficult to identify, as they hide behind virtual identities and fake profiles. In addition, most victims only know the perpetrator from the internet, i.e. they have no connection to the real bullying environment. This leads to a feeling of helplessness on the part of the victim, given that they do not have the necessary evidence to reveal the identity of the perpetrator. Another important difference is that the level of public access to cyberbullying is very high, and the number of people who have access to the various cyberbullying crimes is often in the millions. Lies and slander are no longer known only to a narrow, manageable circle, such as classmates or a parallel class, but to a huge audience. This makes cyberbullying particularly painful for victims.

Compared to victims of traditional bullying, victims of cyberbullying lack a safe haven where they can retreat and process their grievances after painful attacks. Cyberbullying is online 24 hours a day, accessible to anyone, anywhere,

⁷⁶ Salimi, 2015, p. 191.

⁷⁷ StGB Art. 107c. (2).

⁷⁸ Marzano, Lizut, 2019, p. 22.

and the perpetrator can even be in the child's room via a smartphone, tablet or computer.⁷⁹

3.3.6. *Further examples of cyberbullying*

In addition to the Art 107c StGB, cyberbullying can also be punishable by further offences – regulated by the StGB – which are:

- (a) coercion;⁸⁰
- (b) defamation;⁸¹
- (c) slander;⁸²
- (d) data breach;⁸³
- (e) damage to credit;⁸⁴
- (f) pornographic depiction of minors.⁸⁵

In addition to the StGB, several other Austrian laws contain provisions that may be applicable in cases of cyberbullying. According to the Copyright Act,⁸⁶ the public distribution of confidential recordings is prohibited if it infringes the legitimate interests of the author, and the publication of photographs that expose the persons in them is also prohibited under the right to one's own picture.

Under the Austrian Media Act,⁸⁷ which also applies to public websites, damages can be claimed by victims of defamation, libel or mockery, and by persons whose privacy has been violated. In Austria, youth protection laws prohibit, for example, the transmission of pornographic or violent content to young people and prohibit young people from possessing such content.⁸⁸

⁷⁹ Katzer, 2014, p. 61.

⁸⁰ StGB Art. 105.

⁸¹ StGB Art. 111.

⁸² StGB Art. 115.

⁸³ StGB Art. 126 a.

⁸⁴ StGB Art. 152.

⁸⁵ StGB Art. 207a.

⁸⁶ Copyright Act- Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte (Urheberrechtsgesetz) <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001848>

⁸⁷ Media Act – Gesamte Rechtsvorschrift für Mediengesetz –<https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10000719>

⁸⁸ See Youth Protection Act – Jugendschutzgesetz (JuSchG) <https://www.gesetze-im-internet.de/juschg/BJNR273000002.htm>

4. Enforceability of official action against online crime, cyberbullying and hate speech

Recognising the seriousness of crime in online spaces, the Austrian government adopted a legislative package⁸⁹ to combat online hate speech on 3 September 2020. In addition to a comprehensive judicial reform, the package included a bill imposing new obligations on online platforms to remove illegal user-generated content. Although this law is no longer in force at the time of publication of this volume, in order to get a full picture of the context and legal development concerning the Austrian legislation on communication platforms and as a result, cyberbullying, it is essential to also present the main features of the previous regulation.

The legislation listed, in the definitions section, the acts that constitute illegal content and to which the provisions of the legislation applied:

- (a) coercion;
- (b) dangerous threats;
- (c) persistent persecution;
- (d) persistent harassment by means of telecommunications;
- (e) defamation;
- (f) unauthorised taking of photographs;
- (g) extortion;
- (h) denigration of religious doctrine;
- (i) pornographic depiction of minors;
- (j) initiating sexual contact with minors;
- (k) terrorist organisation;
- (l) instruction on how to commit a terrorist offence;
- (m) incitement to commit terrorist offences and approval of terrorist offences;
- (n) hate speech.

The Act aimed to promote responsible and transparent measures regarding user reports of specific content on communication platforms and the prompt handling of such reports.⁹⁰

The Act applied to domestic and foreign service providers offering communication platforms for profit, unless:

⁸⁹ Communications-Platform-Act, (Kommunikationsplattformen-Gesetz – KoPI-G), BGBl I 2020/151.

⁹⁰ Communications-Platform-Act, Art. 1. (1).

- (a) the average number of users entitled to access the communication platform by registration has not reached 100 000 in Austria in the previous calendar year;
- (b) the revenue generated by the operation of the communication platform in Austria in the previous calendar year is less than EUR 500 000.⁹¹

Providers of communication platforms which are exclusively used for the brokerage or sale of goods or services, for real estate or job advertisements, or for non-profit activities (e.g. making available online encyclopedias or educational and learning platforms for the transfer of knowledge) were in any case exempted from the above obligations.⁹² At the request of the provider, the supervisory authority had to determine whether the provider is subject to federal law.⁹³

The supervisory authority had to keep a register of providers covered by the Act and publish it in an appropriate manner. The register, which had to be updated annually, had to be declarative. If, in the course of its duties, the supervisory authority concluded that the information in the register is no longer correct, it had to make the appropriate corrections.⁹⁴

4.1. The monitoring procedure

The Austrian Media Authority (*Kommunikationsbehörde Austria*) supervised the service providers covered by the Act.⁹⁵ The law described in detail the supervisory procedure for service providers. As a general rule, if more than five substantiated complaints were received by the regulatory body within a month about the inadequacy of the measures taken by a particular service provider, the supervisory authority had to check whether the measures taken to meet the requirements of the Act were appropriate.⁹⁶

If the supervisory authority concluded, on the basis of the frequency and nature of the complaints, the results of previous supervisory procedures, the remedy body's notification or its own preliminary assessment, that there has been a breach of the obligations laid down in the Act, it had to initiate a supervisory procedure,⁹⁷ which could normally have two consequences:

⁹¹ Communications-Platform-Act, Art. 1. (2).

⁹² Communications-Platform-Act, Art. 1. (2).

⁹³ Communications-Platform-Act, Art. 1. (5).

⁹⁴ Communications-Platform-Act, Art. 1. (6).

⁹⁵ Communications-Platform-Act, Art. 8. (1).

⁹⁶ Communications-Platform-Act, Art. 9. (1).

⁹⁷ Communications-Platform-Act, Art. 9. (2).

- (a) ordering the provider by decision to restore the lawful situation and to take appropriate measures to prevent future infringements; the provider must have complied with this decision within a time limit set by the supervisory authority, which may not exceed four weeks, and must have been reported to the supervisory authority through the responsible delegate;
- (b) in cases where such a decision has already been taken against the provider on several occasions, a financial penalty had to be imposed if the provider did not comply with the decision.⁹⁸

The supervisory authority had, when assessing compliance and imposing appropriate precautionary measures, to take into account that the measures required of the provider under the Act may not result in a general prior check of the content. The precautionary measures ordered, and the measures required in this context had to be appropriate and proportionate to the objectives pursued, in particular those relating to increasing the effectiveness of mechanisms for protecting users, protecting the public against illegal content and protecting the interests of individuals affected by such content, taking into account the legitimate interests of service providers.⁹⁹

4.2. Cases of fines

Service providers might have been subject to significant fines for infringements in the following cases:

- (a) any person who, individually or as a member of a body, as a person authorised to represent the provider externally or as a person empowered to take decisions on behalf of the provider, in a managerial position, despite having been requested to do so by the supervisory authority) failed to comply with the obligation to appoint a responsible agent or a person authorised to act as a service agent, might have been fined up to one million euros. The supervisory authority had to waive the penalty if a fine has already been imposed on the legal person for the same infringement and there were no special circumstances that would preclude the waiver of the penalty;¹⁰⁰
- (b) the supervisory authority imposed a fine of up to EUR 10 million on the provider, depending on the gravity of the infringement.¹⁰¹

⁹⁸ Communications-Platform-Act, Art. 9. (2).

⁹⁹ Communications-Platform-Act, Art. 9. (3) .

¹⁰⁰ Communications-Platform-Act, Art. 10. (1).

¹⁰¹ Communications-Platform-Act, Art. 10. (2).

In determining the amount of the fine, the following circumstances in particular had to be taken into account:

- (a) the financial strength of the provider, as demonstrated, for example, by its total turnover;
- (b) the number of registered users of the platform;
- (c) previous infringements;
- (d) the extent and duration of the provider's negligence in fulfilling the obligation imposed;
- (e) the contribution to the establishment of the facts; and
- (f) the extent to which precautions have been taken to prevent the infringement and the extent to which employees have been instructed to comply with the rules.¹⁰²

In the context of enforceability of the laws against online crime, cyberbullying and hate speech it is inevitable to mention, that on 8th June 2023 the ECJ's Advocate General, delivered his opinion in the Case C-376/22, concerning the conformity of the so-called Austrian Communications-Platforms-Act with EU-law. As it appeared, according to the Advocate General, the Austrian provisions were indeed likely to be contrary to EU-law. According to the E-Commerce Directive¹⁰³ information society services shall be subject to the legal system of the country on the territory of which they are established ('country-of-origin principle') and other Member States may not, in principle, provide for stricter requirements. Although Art. 3 (4) of the E-Commerce Directive provides for an exception to this principle under certain conditions "with regard to a specific information society service", from the Advocate General's point of view general-abstract legal measures – as also provided for by the Austrian KoPl-G – restricted the free movement of information society services from a Member State without constituting a permissible exception to the country-of-origin principle.¹⁰⁴

The EU Digital Services Act is applicable directly in every member state of the Union as of February 17, 2024. Consequently, after the E-Commerce Directive

¹⁰² Communications-Platform-Act, Art. 10. (3).

¹⁰³ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031>

¹⁰⁴ International Network of Privacy Law Professionals: Is the Austrian Communications-Platform-Act Contrary to EU law? <https://inplp.com/latest-news/article/austria-is-the-austrian-communication-platforms-act-contrary-to-eu-law/>

entered into force in 2024, the earlier existing Communications-Platforms-Act was repealed.¹⁰⁵

4.3. Preventive legislation and practice

In Austria, just like in other countries, the prevention of violence and the safe use of the Internet are in the public interest.¹⁰⁶ The Austrian government not only regulates hate speech by law, but also carries out specific preventive measures and campaigns to minimise hate crimes.

At federal and provincial level, there are several bodies that have a potential role in dealing with hate crime or that can help to address the causes of hate crime. These institutions include the Equal Treatment Commission (*Gleichbehandlungskommission*), the National Equal Treatment Board (*Anwaltschaft für Gleichbehandlungsfragen*), the National Commission against Discrimination (*Antidiskriminierungsstelle*), or the National Advisory Councils for Small Minorities (*Volksgruppenbeiräte*).¹⁰⁷

The best-known platforms for prevention and assistance to victims are described below.

4.4. No hate speech movement

It is important to underline that Austria has joined the Council of Europe's No hate speech movement,¹⁰⁸ launched in 2013, which aims to combat hate speech. In order to make this work effective, Austria also has a National Commission composed of experts on hate speech. The Commission aims to raise awareness of online hate speech, to fight online hate speech and to encourage and support action against hate speech.

ZARA (*Zivilcourage und Anti-Rassismus-Arbeit*) is the advisory centre against hate crime in the online space¹⁰⁹, which aims to contribute, with the help of

105 Parlamentskorrespondenz Nr. 1322 vom 30. 11. 2023., Hass im Netz: Europäischer Digital Service Act löst Kommunikationsplattformengesetz ab, https://www.parlament.gv.at/aktuelles/pk/jahr_2023/pk1322

106 Q. Li, D. Cross, P. K. Smith, 2012, p. 280.

107 Austria: Responding to „hate speech“ Country Report, 2018, p. 32-33. <https://www.article19.org/wp-content/uploads/2018/09/Austria-Responding-to-Hate-Speech-.pdf>

108 See the website of the portal: https://www-coe-int.translate.google/en/web/no-hate-campaign?_x_tr_sl=de&_x_tr_tl=hu&_x_tr_hl=hu&_x_tr_pto=nui,sc

109 See: *Beratung gegen Hass im Netz* https://www.oesterreich.gv.at/themen/bildung_und_neue_medien/internet_und_handy___sicher_durch_die_digitale_welt/3/3/Seite.1720230.html

theoretical and practical experts, to the development of a society that takes a critical view of exclusion and thus combats discrimination, racism and hatred online.

The Anti-Hate Advice Centre (*#GegenHassimNetz*) provides support and advice to victims and witnesses of hate speech, cyberbullying and other forms of verbal and psychological violence on the internet. This service is free of charge for everyone. After an initial assessment of the facts that led to the offence, people who come to the centre are advised by a trained and experienced team of counsellors on the steps to take and possible counterstrategies. They will also receive support for possible legal action and be put in touch with other institutions from which they can get help. The advice centre will also report relevant content to the IT companies concerned. The advice can be provided via chat, messenger, e-mail or telephone. Personal advice is available by appointment. The helpdesk is not only for victims of online hate crime and those affected by cyberbullying, but also for organisations working with these groups and users who want to know how to respond to hate crime in the online space. The Advisory Centre aims to share with all members of society the dangers of online hate crime and to provide support to those who have been victims of online hate crime. The counselling centre is run by staff members of the non-profit organisation ZARA (*Zivilcourage und Anti-Rassismus-Arbeit*), who have received legal and psychosocial training.

4.4.1. Saferinternet.at portal

Saferinternet.at promotes the safe, competent and responsible use of digital media, mainly by providing advice, educational brochures and workshops for specific target groups, such as children, young people, parents and teachers. The initiative is implemented by the European Union under the Digital Europe Programme (DEP).

4.4.2. Rat auf Draht¹¹⁰ or telephone advice

‘Rat auf Draht’, which translates as ‘Advice on wire’ is an emergency telephone assistance specifically for children, available 24 hours a day, anonymously and free of charge.

¹¹⁰ See the web-page of the portal: <https://www.rataufdraht.at/telefonberatung>

5. Responsibilities of service providers and institutions

Until 2024 in Austria, the liability of service providers and institutions was regulated by the Communications Platforms Act. The Act came into force on 1 January 2021 and was prompted by the increasing number of online infringements, as new technologies and communication channels on the internet have negative side effects¹¹¹ in the form of misleading information, offensive language and threats of violence. Experience has shown that the providers of the various Internet platforms have failed in their obligation to delete or block access to offensive content. The content subject to complaint has been handled by service providers largely based on their own guidelines, often forcing victims to take legal action to enforce their rights.¹¹²

The Communication Platforms Act provided guidance to service providers on exactly what obligations they must fulfil in the chapter on requirements for communication platforms.

On the one hand, service providers had to put in place an effective and transparent procedure for handling and dealing with notifications of allegedly illegal content available on the communication platform.¹¹³ Such a procedure should have been designed in such a way that users have easy-to-find, permanently accessible and easy-to-use functionalities on the communication platform, allowing them to notify the service provider of the content and the data necessary for its assessment; to be informed of the way in which their notification is being handled and the outcome of the procedure concerned; and to be informed without delay of the main reasons for the decision to assess the notification concerned, including the possible date of removal or blocking.¹¹⁴

Service providers were also required to ensure, through the internal organization of the notification procedure, that the content reported, where its illegality is obvious to lay persons who do not have the necessary knowledge of the law without further investigation, was removed or access to it was blocked without delay and at the latest within 24 hours of receipt of the notification. If their illegality became apparent only after a detailed investigation, they had to be removed or access to them had to be disabled immediately after the completion of that investigation and at the latest within seven days of receipt of the notification.¹¹⁵

111 Folk, 2021, p. 6.

112 Simsa, 2021, p. 19.

113 Communications-Platform-Act, Art. 3. (1).

114 Communications-Platform-Act, Art. 3. (2).

115 Communications-Platform-Act, Art. 3. (3) 1.

In the event of blocking or deletion, the service provider were obliged to provide the content concerned, the date of production of the content and the data necessary to identify the user for whom the content concerned was stored on the communication platform and already held by the service provider, for the purposes of evidence, including criminal proceedings, and to store them for a maximum period of ten weeks. This period might have been exceeded in individual cases, at the express request of a law enforcement authority, if the provision of evidence would otherwise fail; the data had to be deleted when the purpose for which they were processed has ceased to exist.¹¹⁶

Service providers should have also ensured that an effective and transparent procedure was in place to review their decision to block or delete notified content.¹¹⁷ A review had to be carried out where

- (a) in the case of a decision not to block or remove content, the notifying user submitted a request for a review of that decision within two weeks of receipt of the decision;
- (b) in the case of blocking or deletion of the content, the user for whom the content was hosted on the communication platform submitted a request for a review of that decision within two weeks of receipt of the decision.

The service provider had to inform the users of the outcome of the review without delay. The review procedure had to be concluded within two weeks of the request.

The provider was not obliged to carry out the notification or review procedure if, in particular on the basis of the nature or frequency of the notifications received, it could have been assumed with a probability approaching certainty that the notifications have been either automated or otherwise initiated in an abusive manner.¹¹⁸ The supervisory authority might have adopted, by means of a regulation, detailed rules for the design of the notification process, in particular minimum standards for the notification forms to be used.¹¹⁹

5.1. Reporting obligations for service providers

Service providers were required to report annually, or every six months for communication platforms with more than one million registered users, on the handling of notifications of allegedly illegal content. The report must have been

¹¹⁶ Communications-Platform-Act, 3. (3) 2.

¹¹⁷ Communications-Platform-Act, 3. (4).

¹¹⁸ Communications-Platform-Act, 3. (6).

¹¹⁹ Communications-Platform-Act, Art. 3. (7).

submitted to the supervisory authority at the latest one month after the end of the period covered by the report and must have been made available on the website in a permanent and easily accessible way at the same time.¹²⁰

The report had to contain at least the following information:

- (a) general information on the efforts made by the service provider to restrict illegal content on the platform;
- (b) a description of the design and user-friendliness of the notification procedure and the criteria for deciding whether to delete or block illegal content, including the verification steps to be taken to determine whether illegal content has been posted or whether contractual provisions between the service provider and the user have been breached;
- (c) a description of the number of notifications of alleged illegal content received during the reporting period;
- (d) an overview of the number of notifications of allegedly illegal content received during the reporting period that led to the deletion or blocking of the content in question, including information on which step of the monitoring process led to the deletion or blocking, and a summary description of the nature of the content;
- (e) an overview of the number, content and outcome of the review procedures;
- (f) a description of the organisation, staffing and technical resources, the expertise of the personnel responsible for processing notifications and review procedures, and the education, training and support of the personnel responsible for processing notifications and review procedures;
- (g) an overview of the time periods between the receipt of the notification by the service provider, the initiation of the monitoring and the deletion or blocking of the illegal content, broken down into the following time periods: 'within 24 hours', 'within 72 hours', 'within seven days' and 'at a later date';
- (h) an overview of the number and type of cases where the service provider has waived the notification and review procedures.¹²¹

In order to ensure the information content and comparability of the reports, the supervisory authority had to, by means of a regulation, lay down detailed rules on the structure of the reports and the scope of the reporting obligation.¹²²

¹²⁰ Communications-Platform-Act, 4. (1).

¹²¹ Communications-Platform-Act, Art. 4. (2).

¹²² Communications-Platform-Act, Art. 4. (3).

5.2. Responsible agent and authorised agent for notification

Service providers had to appoint a person who fulfils the conditions laid down in § 9(4) of the Administrative Penalties Act 1991 (*Verwaltungsstrafgesetz 1991 – VStG, BGBl. 52/1991*).¹²³

This person:

- (a) ensured compliance with the provisions of the Act;
- (b) had the necessary powers of disposal to ensure compliance with the provisions of the Act,
- (c) had the necessary German language skills to cooperate with the authorities and the courts; and
- (d) had the necessary resources to perform these duties.

5.3 Enforcement

If the service provider failed to comply with the obligation to appoint a responsible agent or an authorized recipient, the authority had to issue a written request for the appointment, setting a deadline of seven days. If the service provider did not have a registered office, branch or other permanent establishment in the territory of the Member State and it is established that it is not possible or practicable to effect service of this notice abroad within a reasonable period of time, the notice had to be notified by publication on the supervisory authority's website. The notice had to be deemed to have been served on the provider from the date of publication. The publication must also have indicated that further orders of the authority shall be deemed to be served if they are deposited with the authority and must have been made available for inspection¹²⁴

If the provider did not comply with the supervisory authority's request to appoint a responsible agent or authorized recipient, the supervisory authority had to impose a financial penalty on the provider. If the provider did not have a registered office, branch or other permanent establishment in the territory of the Member State and had not appointed a responsible agent or authorized recipient who can be served with legal effect, the decisions or other orders of the authority had to be deposited with the authority. The provider had to be informed of the deposit on the supervisory authority's website. The notification had to state the starting date and duration of the period of receipt and had to draw attention to the effect of the deposit.¹²⁵

¹²³ Communications-Platform-Act, Art. 5. (1).

¹²⁴ Communications-Platform-Act, Art. 6. (1).

¹²⁵ Communications-Platform-Act, Art. 6. (2).

At the end of this chapter, it is once again emphasised that the Communications-Platform-Act was repealed after the entry into force of the EU Digital Services Act (E-Commerce Directive) on 17 February 2024, consequently the presented provisions of the Austrian Communications-Platform-Act are no longer in force.

Summary

Today, there is no universally accepted definition of cyberbullying and most countries treat cyberbullying as a form of violence (insult, defamation, unauthorised filming and photographing, stalking) perpetrated on the Internet.¹²⁶ Austria is one of the European legal systems, which has specific laws criminalising cyberbullying.¹²⁷ The issue of responding to hate crime has become increasingly prominent in Austria over the last few years and has become a much debated topic at various levels of society. The Austrian legislation deals with both hate speech and cyberbullying in great detail, including specific obligations for individual service providers and their accountability. In Austria, cyberbullying is combated through a combination of criminal and civil law provisions.

Over the past decade, Austria has incorporated a number of amendments to the StGB to prevent hate speech and has also introduced new legislation specifically to combat hate crimes committed in the online space, with regard to the liability of online platform providers. In this respect, the transparency obligations are very impressive. The legislation imposes annual reporting obligations on internet service providers (quarterly reports for large platforms), which must explain exactly how the content moderation process works, how many cases of alleged illegal content have been reported, how long they have been checked and after how many hours a decision was made. In addition to statistics, the training of content moderators and the technical systems used should be described. However, this legislative solution has been criticised, alongside praise, by EDRI, one of Europe's largest civil society organisations defending rights and freedoms, which argues that the Austrian legal framework, by imposing very strict rules on large and dominant operators, disproportionately hampers the activities of smaller operators, which are very important for the internet world.

¹²⁶ Janković, Stošić, 2022, p. 98.

¹²⁷ Gottschalk, 2022, p. 34.

The relatively new criminal law provisions, which entered into force at the beginning of 2021, are allowing cyberbullying to be punishable after the first offence – and not only if it is repeated. The StGB reform also makes it a criminal offence to bully someone because they belong to a certain religion or ethnicity or because they have a disability. Previously, this protection applied only to groups of persons.

As to whether the newly introduced legislation will live up to the expectations in combating hate crime and reducing harassment in the online space in the future, it is too early to say. However, it is clear that in recent years, measures to combat hate crime and harassment via telecommunications or computer systems in Austria have become ‘the pace-setter’ in Europe, as Federal Minister Karoline Edstadler aptly put it in 2020.¹²⁸

128 Bundeskanzleramt, Edstadler: Österreich ist Tempomacher im Kampf gegen Hass im Netz <https://www.bundeskanzleramt.gv.at/bundeskanzleramt/nachrichten-der-bundesregierung/2020/edstadler-oesterreich-ist-tempomacher-im-kampf-gegen-hass-im-netz.html>

Bibliography

- Bodzási, B. (2021) *Új osztrák törvények az Interneten megjelenő jogsértő tartalmakkal szembeni fellépés eszközeiről*. [Online] <https://jogaszegylet.hu/jogelet/uj-osztrak-torvenyek-az-interneten-megjeleno-jogserto-tartalmakkal-szembeni-fellepes-eszkozeirol/>
- Brad, P. (2015) 'A gyűlölet-bűncselekmények büntetőjogi üldözésének jogszabályi és társadalmi feltételrendszere', *Kriminológiai Közlemények* 75, pp. 93-154
- Folk, P. (2021) *Zur strafrechtlichen Sanktionierung von Hass im Netz*, Institut für Strafrechtswissenschaften, Johannes Kepler Universität Linz (thesis)
- Gottschalk, F. (2022) *Cyberbullying: An overview of research and policy in OECD countries*, OECD Education Working Papers No. 270 [Online] [https://one.oecd.org/document/EDU/WKP\(2022\)8/en/pdf](https://one.oecd.org/document/EDU/WKP(2022)8/en/pdf)
- Fuchs, W. (2021) *Projekt HC-POL-DATA, Pilotbericht, Hate Crime in Österreich*, Institut für Rechts- und Kriminalsoziologie. [Online] https://www.bmi.gv.at/408/Projekt/files/hc_pilotbericht_final_druck.pdf
- Hatheuer L. M. (2021) *Cybermobbing – Zentrale Probleme des § 107c StGB*, Institut für Strafrechtswissenschaften, Johannes Kepler Universität Linz (thesis)
- Höpfel F., Ratz E. (2016) *Wiener Kommentar zum Strafgesetzbuch*. Manz Verlag Wien
- Janković, A., Stošić, Lazar: *Cyberbullying legislation: the role of cyberbullying law*. Law- theory and practice No. 4/2022
- Katzer, C. (2014) *Cybermobbing Wenn das Internet zur Waffe wird*. Springer Verlag: Berlin Heidelberg
- Li Q., Cross D., Smith P. K. (2012) *Cyberbullying in the Global Playground: Research from International Perspectives*. Blackwell Publishing Ltd.
- Marzano G., Lizut J. (2019) *Cyberbullying and the Critical Importance of Educational Resources for Prevention and Intervention*. IGI Global
- Mitgutsch, I. (2020) 'Stalking und Cybermobbing – Gemeinsamkeiten und Unterschiede der §§ 107a und 107c StGB', *Journal für Strafrecht* pp. 13-25.
- Perry, B. (2001) *In the Name of Hate: Understanding Hate Crimes*. New York/London: Routledge
- Reindl-Krauskopf, S. (2015) *Cyberstrafrecht im Wandel*, ÖJZ, Manz Verlag Wien
- Reindl-Krauskopf, S., Salimi, F., Stricker, M. (2018) *IT-Strafrecht Cyberdelikte und Ermittlungsbefugnisse*. Manz Verlag
- Salimi, F. (2015) 'Auf dem Weg zu einem neuen Strafbestand', *Journal für Strafrecht* pp. 191-197.
- Simsa, T. (2021) *A közösségi média és az online platformok szabályozása az Európai Unióban*. Országgyűlés Hivatala, Közgyűteményi és Közművelődési Igazgatóság

- Tipold, A. (2017) 'Das Strafrechtsänderungsgesetz 2015', *SIAK-Journal, Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis*, pp. 31-41.
- Wickes, R., Pickering S., Gail, M., Maher, J. M., McCulloch, J. (2016) 'From Hate to Prejudice: Does the New Terminology of Prejudice Motivated Crime Change Perceptions and Reporting Actions?', *The British Journal of Criminology* 56(2), pp. 239-255.