

V. PROGRESS REPORT 2024 ON THE NEVER-ENDING WAR – AN OVERVIEW OF EU LAW AGAINST DEVIANCES INDUCED BY HATRED IN THE ONLINE SPACE

———— ROLAND LINDT – GYÖRGY MARINKÁS ————

1. Introductory Thoughts on the Beginnings of the Fight Against Hatred

Nowadays the European Union (hereinafter: EU) is usually interpreted as an international ‘entity’¹ that aims at deepening the economic integration in the European continent. On the one hand, this statement clearly describes today’s reality, however, one must not forget that the original motivation of the ‘founding fathers’ was to create long-term peace after the horrors of the World War II. To this end, the victorious states decided to develop an international platform, thus preventing the re-radicalisation of the German society.² On the other hand, we could state that the first steps of the European integration were realised as part of the fight against hatred among European nations. As the flow of history has demonstrated, the initiative was successful, since not only World War III has been avoided until now, but through economic integration the EU has become a major operator of global economy and can stand up to other super-powers like China and the USA – although nowadays this statement has become rather questionable.

1 For an analysis on the debated legal status of the EU, see: von Bogdandy, 2012; cf. Kiljunen, 2004, pp. 19–20.

2 Cf. Kiljunen, 2004, pp. 12–14; Berend, 2021, pp. 71–92.

During the 1980s, the original content of action against hatred within the EU has been expanded: the European Parliament, the Council and the Commission issued a joint declaration³ in 1986, '[r]ecognizing the existence and growth of xenophobic attitudes [...] which are often directed against immigrants'. In this document, EU decision-makers emphasised the importance of tolerance towards each person and group of persons regardless of their racial, religious, cultural, social or national characteristics and declared the aim of protecting the individuality and dignity of every member of the European society, rejecting any form of segregation. Nevertheless, the process started to accelerate only a few years later, a period during which several political documents⁴ were adopted, although major progress was yet to come. In 1994, the European Council decided on the establishment of the Consultative Commission on Racism and Xenophobia (hereinafter: CCRX). Analysing the two-year-period of its operation, two phases can be distinguished: the one before and the one after June 1995. In the first period, the CCRX had the 'overall task' of making recommendations in order to encourage tolerance, understanding and harmony with foreigners in the EU. Thus, three subcommittees and the so-called ad hoc Working Party were established with a view to scrutinising different aspects of the question. After June 1995, the CCRX was given a precise task, the examination of the feasibility of establishing an observatory monitoring racism and xenophobia in the Member States, an idea first presented by the Subcommittee on Information, Communications and Media.⁵

Without the intention of further analysing the impact of the CCRX, we must highlight two major aspects with high relevance of its work:

The observatory, of which the establishment was planned by the CCRX, was created as the European Monitoring Centre on Racism and Xenophobia.⁶ This institution is in fact the legal predecessor of the European Agency for Fundamental Rights, usually referred to as FRA.⁷

The ad hoc Working Party underlined the importance of the inclusion of the fight against racism and xenophobia in the EU's primary law through the wording of certain competences.

3 Declaration against racism and xenophobia, OJ C 158, 25.6.1986, p. 1–3.

4 For an overview of the most important ones, see: Costa-Lascoux, 1995, pp. 215–216; Leman, 1996, pp. 602–603; Szajbély, 2018, p. 289.

5 For more details on the history and achievements of the CCRX, see: Costa-Lascoux, 1995, pp. 217–218; Leman, 1996, pp. 605–611.

6 Council Regulation (EC) No 1035/97 of 2 June 1997 establishing a European Monitoring Centre on Racism and Xenophobia, OJ L 151, 10.6.1997, p. 1–7. See also: Ligeti, 2008b, pp. 668–669.

7 See: Council Regulation (EC) No 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights, OJ L 53, 22.2.2007, p. 1–14, Art. 23.

Not long after the termination of the CCRX's work, a joint action concerning action to combat racism and xenophobia (hereinafter: Joint Action)⁸ was adopted by the EU legislator.⁹ This occasion was the first step of criminal law harmonisation in the discussed area.

As a result of the revision of the Founding Treaties in 1997, fight against hatred became an explicit objective of the EU in the framework of the Third Pillar: '[...] the Union's objective shall be to provide citizens with a high level of safety within an area of freedom, security and justice by developing common action among the Member States [...] and by preventing and combating racism and xenophobia.'¹⁰ Three years later, in December 2000, the Charter of Fundamental Rights of the European Union (hereinafter: Charter)¹¹ was proclaimed, although its legal status was not precisely defined then. Part II of the Treaty establishing a Constitution for Europe would have adopted the content of the Charter, with important modifications regarding the provisions on the field of application and the scope and interpretation of the rights therein,¹² interpreting human rights as fundamental values of the EU, however this document never entered into force because of the failure of the ratification process in the Netherlands and France.¹³ Its legal status as part of the EU's primary law was only acquired through the entry into force of the Treaty of Lisbon in 2009.

These days, both the EU as a whole and the Member States must face the challenges posed by mass migration, thus tolerance may be a more essential treat than ever. As it appears, EU's primary law provides an adequate basis for acceptance and the integration of the newcomers:¹⁴

The Treaty on the European Union (hereinafter: TEU),¹⁵ discussing fundamental principles and values, displays the problem of discrimination. In Art. 2 the document declares that the 'Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities.'

8 96/443/JHA: Joint Action of 15 July 1996 adopted by the Council on the basis of Art. K.3 of the Treaty on European Union, concerning action to combat racism and xenophobia, OJ L 185, 24.7.1996, p. 5–7.

9 For its content, see subchapter 2.

10 Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts, OJ C 340, 10.11.1997, p. 1–144, Art. K.1.

11 For the consolidated text, see: Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–407.

12 Kiljunen, 2004, p. 59.

13 Friedery and Horváthy, 2018, p. 249.

14 For an overview, see also: Kalaitzaki, 2022, pp. 12–14.

15 Consolidated version of the Treaty on European Union, OJ C 326, 26.10.2012, p. 13–45.

As it follows, '[t]hese values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail.' It must be emphasised that, according to the TEU, equality and respect for human rights are fundamental values of the EU and it also suggests that principles of non-discrimination and tolerance are realised in Member States, as it was the *status quo*. However, Art. 3(3) adds that [the EU] 'shall combat social exclusion and discrimination and shall promote social justice and protection [...]'. The need for such actions slightly contradicts the solemn declaration of Art. 2 that the so-called 'common values' prevail.

The Treaty on the Functioning of the European Union (hereinafter: TFEU),¹⁶ among the 'provisions having general application' states that '[i]n defining and implementing its policies and activities, the Union shall aim to combat discrimination based on sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation.'¹⁷ In other words, the principle of non-discrimination must be taken into account in connection with all kinds of actions performed by the EU. Furthermore, the TFEU declares that no discrimination on the grounds of nationality shall happen and provides a legislative competence in order to 'take appropriate action to combat' different forms of discrimination.¹⁸ The discussed principle appears among the provisions regarding the humanitarian aid provisions too.¹⁹ From the point of view of criminal law harmonisation, general rules of the policy titled 'area of freedom, security and justice' must also be underlined. If it is deemed necessary, the EU can take measures to combat crime, racism and xenophobia approximating the criminal laws of the Member States.²⁰ Although hate crime does not appear in the list of the so-called 'euro-crimes',²¹ criminal law harmonisation has already taken place concerning the minimum standards of related criminal offences.

According to the TEU, the Charter has the same legal value as the Founding Treaties themselves,²² thus the term EU's primary law encompasses it. Title III named 'Equality' contains the most relevant declarations concerning the

16 Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, p. 47–390.

17 TFEU, Art. 10.

18 TFEU, Arts. 18–19.

19 TFEU, Art. 214(2).

20 TFEU, Art. 67(3).

21 Pursuant to Art. 83(1) of the TFEU, euro-crimes are 'terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime'.

22 TEU, Art. 6(1).

prohibition of discrimination. Art. 21 provides the most detailed enumeration of the characteristics based on which any kind of discrimination is prohibited.²³ Moreover, it should be noted that the wording, intentionally, does not create to a taxation, it is to say, discrimination on the grounds of features not mentioned is also forbidden. The rule is complemented by a declaration with less normative value: ‘The Union shall respect cultural, religious and linguistic diversity.’²⁴ Further provisions address equality between men and women, the rights of the child, the rights of the elderly and integration of persons with disabilities.²⁵ Art. 52(3) states that the scope and meaning of fundamental rights that appeared beforehand in the Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter: Convention) ‘shall be the same as those laid down by the said Convention’. Halász then argues that the Charter emphasises the reaffirmation of the rights enshrined in the Convention by the EU.²⁶ On the other hand, EU law may provide a more extensive protection in connection with these rights, i.e. the content of the Convention can be interpreted as minimum standard.²⁷ Any limitation exercised shall undertake the test of proportionality and necessity described by Art. 52 para 1. Finally, we must accentuate the field of application of the Charter: its provisions are ‘addressed to the institutions, bodies, offices and agencies of the Union [...] and to the Member States only when they are implementing Union law.’²⁸ It is also underlined that the Charter neither extends or modifies the existing powers of the EU, nor creates new ones.²⁹

One may argue that EU’s primary law, rooted in the constitutional traditions of the Member States and drawing on the human rights standards established within the framework of the Council of Europe, constitutes a proper framework for anti-discrimination regulation and the fight against racism and xenophobia. Nonetheless, the ever-accelerating process of digitisation brings new difficulties

23 ‘Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.’ – Charter, Art. 21(1). Para. 2 of the same article also adds nationality to this catalogue.

24 Charter, Art. 22.

25 Charter, Arts. 23–26. See also: Friedery and Horváthy, 2018, pp. 252–253.

26 Halász, 2023, p. 77.

27 Furthermore, Art. 52 paras. 2 and 4 also highlight the importance of the Founding Treaties and the constitutional traditions of the Member States. Cf. Kokott and Sobotta, 2010, pp. 2–3; Friedery and Horváthy, 2018, p. 256.

28 For the problems regarding the interpretation of this norm, see: Kokott and Sobotta, 2010, pp. 6–8; Friedery and Horváthy, 2018, pp. 254–255.

29 Charter, Art. 51.

with which the EU legislator must cope, since the existing regulation designed for problems in ‘real-life’ space does not guarantee sufficient protection.³⁰

This chapter seeks to summarise the current answers of the EU to the challenges arisen because of technological development, including tools against hate crime in the cyberspace, the issue of cyberbullying, child protection in the digital age and liability framework regarding digital platforms.

2. Harmonisation of Hate Crime in the EU

As we have introduced above in a nutshell, first political, then legal steps were taken to combat intolerance in Europe. Logically, hate crime is the most severe form of manifestation of racism and xenophobia, but other forms also had to be repressed. At the beginning of the new millennium, the EU legislator adopted the directive on the rules of equal treatment which describes violations of the principle in question that are considered acts of discrimination³¹ and another directive specifying the conditions thereof in the field of employment and occupation.³² As our analysis focuses on criminal law harmonisation, we refrain from presenting the main elements of these instruments. In this subchapter, rules of the aforementioned Joint Action and the framework decision that later repealed it will be presented.

2.1. Legal Basis of Criminal Law Harmonisation in EU's Primary Law

Ius puniendi, in other words, the competence of states to define criminal policy and criminal law within their territory has always been a sensitive question when it comes to sharing competences with other members of the European community. According to the quote well-known among Hungarian scholars, criminal law is the last ‘protective bastion’ of state sovereignty;³³ seemingly the Member States agree with the statement, since cooperation in criminal matters

³⁰ For the major issues highlighted by experts, see: Nagy, 2023, pp. 28–29.

³¹ Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, OJ L 180, 19.7.2000, p. 22–26; cf. Szajbély, 2018, p. 289.

³² Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation, OJ L 303, 2.12.2000, p. 16–22.

³³ In Hungary, the first use of the term is usually attributed to *Ákos Farkas*, professor in criminal sciences. For an overview of the first decade of the development of European criminal law, see his work: Farkas, 2001.

is one of the most slowly growing areas of EU competences. In this regard, the Maastricht Treaty meant a real breakthrough, creating the possibility of criminal law harmonisation in the Third Pillar, characterised by intergovernmental decision-making, through three types of legal instruments: joint position, joint action and (EU) convention.³⁴ Joint action could be adopted by the Council if ‘the objectives of the Union can be attained better by joint action than by the Member States acting individually on account of the scale or effects of the action envisaged’. The wording had two major problems:

- the scope of applicability is defined too wildly; and
- the text remains silent regarding legal binding force.

Nevertheless, the first instrument of substantial criminal law harmonisation concerning hate crime was adopted based on the cited provision.

The Treaty of Amsterdam revised the catalogue of legal instruments within the framework of ‘police and judicial cooperation in criminal matters’, eliminating joint action and introducing decision and framework decision, i.e. four types of instruments could be adopted after the reform.³⁵

The Treaty of Lisbon completely changed the system of cooperation in criminal matters in a positive way; today, instead of intergovernmental decision-making, substantive criminal law standards can be prescribed using the ordinary legislative procedure in connection with euro-crimes and if ‘the approximation of criminal laws and regulations of the Member States proves essential to ensure the effective implementation of a Union policy in an area which has been subject to harmonisation measures’³⁶ – in the latter case, special legislative procedure shall be applied if it is prescribed in connection with the relevant policy. The minimum rules can be issued exclusively through directives.³⁷

³⁴ Treaty on European Union, OJ C 191, 29.7.1992, p. 1–112, Art. K.3. See also: Ligeti, 2008a, pp. 41–42.

³⁵ See: Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts, Art. K.6. For the detailed description of the four instruments, see: Ligeti, 2008a, pp. 43–45; Udvarhelyi, 2019, pp. 38–39.

³⁶ TFEU, Art. 83(1)–(2). The cited part of Art. 83(2) is the *ratio decidendi* of the case of the Council Framework Decision on the protection of environment through criminal law. Case C-176/03, *Commission v Council*, judgment of 13 September 2005. For the details of the case, see: Karsai, 2006, pp. 2–5; Udvarhelyi, 2015, pp. 50–51; Udvarhelyi, 2019, pp. 109–112.

³⁷ For the evaluation of the development of cooperation in criminal matters, see: Udvarhelyi, 2019, pp. 49–51. Cf. Lehotay, 2019, pp. 175–176.

2.2. *The Joint Action Concerning Action to Combat Racism and Xenophobia*

In July 1996, criminal law harmonisation in the field of hate crime commenced, partly due to the work of the CCRX, partly with a view to complying with the rules on the limitation of the freedom of expression as provided by the Convention of 1950 (Arts. 10–11) and the International Covenant on Civil and Political Rights (Art. 19(3)).³⁸

The Joint Action contained five offences in total:³⁹

- ‘public incitement to discrimination, violence or racial hatred in respect of a group of persons or a member of such a group defined by reference to colour, race, religion or national or ethnic origin;
- public condoning, for a racist or xenophobic purpose, of crimes against humanity and human rights violations;
- public denial of the crimes defined in Article 6 of the Charter of the International Military Tribunal [...] [crimes against peace, war crimes and crimes against humanity committed by the European Axis countries in World War II] insofar as it includes behaviour, which is contemptuous of, or degrading to, a group of persons defined by reference to colour, race, religion or national or ethnic origin;
- public dissemination or distribution of tracts, pictures or other material containing expressions of racism and xenophobia;
- participation in the activities of groups, organizations or associations, which involve discrimination, violence, or racial, ethnic or religious hatred.’

Member States could decide either they implemented the definitions as criminal offences or derogated from the principle of double criminality.

It must be highlighted as a positive aspect, that none of these definitions includes outcome, i.e. the sole performance of one of the listed activities realises the violation of the Joint Action. As for the discriminative element, its role varies in each description. In case (a) it appears as a distinctive characteristic of the passive subject(s); in case (b) it is a purpose, meaning that the act can be perpetrated only intentionally (*dolus directus*); in case (c) it is a *modus operandi*; in case (d) it is the distinctive characteristic of the object of perpetration; and in case (e) it is a definitional element of a special type of criminal organisation. A major negative aspect is the fact that the definitions use taxations of distinctive

³⁸ Joint Action, Preambular.

³⁹ Joint Action, Title I A. (a)–(e).

characteristics, unable to provide protection for every kind of minorities. The absence of interpretative provisions can be evaluated as another deficiency. In our opinion, ‘crimes against humanity and human right violations’ in case (b) and the constitutive elements of groups, organisations and associations in case (e) (e.g. at least how many members are required or at least for how much time does it have to work, etc.) should have been produced.⁴⁰

Other important provisions oblige the authorities of the Member States to seize and confiscate objects destined for dissemination with a discriminative purpose and to remove potential obstacles of transboundary criminal cooperation.⁴¹

Looking back, now it is evident that the Joint Action was never able to fill its purpose, since the type of the legal instrument itself was poorly structured. As the issue of binding force was not determined by the Maastricht Treaty, a conflict emerged among Member States, resulting in the elimination of joint actions from the revised text of the Founding Treaties.⁴² The Joint Action of 1996 was only repealed in 2008.

2.3. Criminal Law Harmonisation of Our Days: Main Provisions of the Council Framework Decision

In November 2008⁴³ the new legal instrument, in the form of framework decision (hereinafter: Framework Decision),⁴⁴ was adopted, delivering a significantly more detailed regulation than its predecessor. The Framework Decision describes four offences:⁴⁵

- ‘publicly inciting to violence or hatred directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin;
- the commission of an act referred to in point (a) by public dissemination or distribution of tracts, pictures or other material;

⁴⁰ Furthermore, *Ligeti* considers that even the concept of racist and xenophobic acts lacks a proper definition. Ligeti, 2008b, p. 668.

⁴¹ Joint Action, Title I B. (a)–(d).

⁴² Although the adopted joint actions were not repealed automatically. Ligeti, 2008a, p. 45.

⁴³ The first proposal was presented in 2002 to the Council. The legislative procedure was prolonged because of the sensitivity of the regulatory subject matter. Cf. Turner, 2012, pp. 566–567.

⁴⁴ 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, OJ L 328, 6.12.2008, p. 55–58.

⁴⁵ Framework Decision, Art. 1(1). See also: Lehotay, 2019, p. 178.

- publicly condoning, denying or grossly trivialising crimes of genocide, crimes against humanity and war crimes as defined in Articles 6, 7 and 8 of the Statute of the International Criminal Court [genocide, crimes against humanity and war crimes], directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin when the conduct is carried out in a manner likely to incite to violence or hatred against such a group or a member of such a group;
- publicly condoning, denying or grossly trivialising the crimes defined in Article 6 of the Charter of the International Military Tribunal appended to the London Agreement of 8 August 1945, directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin when the conduct is carried out in a manner likely to incite to violence or hatred against such a group or a member of such a group.’

Comparing to the Joint Action, one must underline the following novelties. Participation in groups which involve discrimination, violence or hatred is no longer included. In our opinion, it is rather an unlucky outcome of the legislative procedure that this offence was omitted, since such an ensemble of persons regularly poses a greater threat to society than lonely perpetrators. The wording of Art. 1(1)(a) of the Framework Decision can be considered a major change: incitement to *discrimination* has been eliminated from the text, meaning that in the new concept ‘simple’ discrimination does not need to be criminalised, i.e. the limitation of the freedom of speech has been narrowed. Title I A.(b) of the Joint Action also went through a major change. Relevant international crimes are now defined with a reference to the Rome Statute, thus better complying with the requirement of *lex certa*. In Art. 1(1)(c)–(d) of the Framework Decision, criminal conducts were also revised and unified (‘condoning, denying or grossly trivialising’). More importantly, it must be emphasised that these definitions, instead of an outcome, contain the method of operation (‘in a manner likely to incite [...]’), i.e. the creation of the abstract possibility of such an outcome already carries out the discussed offences. Art. 1(2) adds disjunctive definitional criteria to the described offences that, in our opinion, further narrows criminal law limitation of the relevant fundamental rights.

The provision regarding the criminal liability of accessories⁴⁶ is also an improvement of the instrument in power. It should be noted that Member States

⁴⁶ Framework Decision, Art. 2.

are not compelled to punish the instigators of the offences described in Art. 1(1) (a) and (b). The reason behind this seemingly illogical provision is that these provisions are usually implemented as *sui generis* inciting conducts, i.e. the incitement itself constitutes the offence. Measures on the sanctioning of perpetrators and regarding the liability and sanctions of legal persons are also novelties of the Framework Decision.⁴⁷

Apart from the discussed liability rules, three major improvements must be emphasised. Most importantly, racist and xenophobic motivation in general must be considered an aggravating circumstance or at least taken into account by the courts in the determination of the penalties.⁴⁸ Through this provision even all the offences that do not fall under the term hate crime may be sanctioned more severely when the discriminative element is a dominant circumstance of the case. Another, semi-successful, development is that certain terms, such as ‘descent’, ‘hatred’ and ‘religion’ are granted legal definitions.⁴⁹ Although it is not clear why such definitions were placed in the preambular instead of the normative part. Moreover, the first proposal of the Framework Decision (hereinafter: Proposal)⁵⁰ contained essential definitions (‘racism and xenophobia’⁵¹ and ‘racist and xenophobic group’⁵²) that would have been necessary tools of an effective harmonisation but were finally omitted.⁵³ Finally, the provisions concerning jurisdiction shall be accentuated, since their content already reacted to the challenges of digitisation more than fifteen years ago. As it follows, a Member State has jurisdiction regarding cases in which the conduct is committed through an information system if either the offender or the information system in question was present in its territory during the perpetration.⁵⁴

47 Framework Decision, Arts. 3, 5–6. Due to space constraints, we just refer to the involvement of these norms without further analysing them.

48 Framework Decision, Art. 4.

49 Framework Decision, Recitals (7)–(9). Although it can be disturbing that religion has another meaning applicable in the context of Art. (1)1. See: Framework Decision, Art. 1(3).

50 European Commission, Proposal for a Council Framework Decision on combating racism and xenophobia [(COM(2001) 664 final – 2001/0270(CNS)], OJ C 75E, 26.3.2002, p. 269–273.

51 ‘[T]he belief in race, colour, descent, religion or belief, national or ethnic origin as a factor determining aversion to individuals or groups’. – Proposal, Art. 3(a).

52 ‘[S]tructured organisation established over a period of time, of more than two persons, acting in concert to commit offences referred to in Article [...]’. – Proposal, Art. 3(b).

53 For the potential difficulties that may have arisen in connection with these terms, see: Ligeti, 2008b, pp. 669–670.

54 Framework Decision, Art. 9(2). See also: Kalaitzaki, 2022, p. 16.

2.4. Evaluation of the Situation of Hate Crime in the EU – Challenges of the Near Future

It is indisputable that the adoption of the Framework Decision was a significant progress compared to the Joint Action, even though some Member States have not yet implemented properly – or implemented at all – its provisions.⁵⁵ On the other hand, the progress of digital technology rendered it necessary to renew criminal law harmonisation in this field, not to mention the increasing prevalence of relevant cases.⁵⁶ EU legislator has two options at this point: either it does not take any serious action and observe whether the existing national liability regimes are able to handle and evaluate the new unlawful phenomena or begins to prepare an improved regulation designed for hate crimes in cyberspace. It appears that the second option has been chosen, although the proper legal basis in EU's primary law is not provided currently.⁵⁷ In 2012, *Turner* saw four alternatives in the framework of the TFEU to solve this deficiency:⁵⁸

- insertion of hate crime into Art. 83(1) as a new euro-crime;
- application of Art. 83(2), i.e. criminal law harmonisation in order to 'ensure effective implementation of EU policy';
- application of Art. 67(3), a general provision of the area of freedom, security and justice;
- usage of the EU's implied powers through Art. 352 known as the implied powers provision.

In the 2020s, it seems that EU institutions prefer alternative (a): the European Commission adopted a communication in 2021, aiming at the extension of the catalogue of euro-crimes,⁵⁹ an initiative welcomed by the European Parliament.⁶⁰

Until now no official decision in connection with the inclusion of hate crime among euro-crimes has been made; such a decision requires the fulfilment of

55 European Parliament resolution of 10 November 2022 on racial justice, non-discrimination and anti-racism in the EU, 2022/2005(INI), point 7.

56 For recent statistics, see: Peršak, 2022, pp. 92–95.

57 On this issue, see: Udvarhelyi, 2016, p. 128.

58 Turner, 2012, pp. 575–577.

59 European Commission, Communication from the Commission to the European Parliament and the Council – A more inclusive and protective Europe: extending the list of EU crimes to hate speech and hate crime, COM(2021) 777 final, Brussels, 9.12.2021.

60 European Parliament resolution of 10 November 2022 on racial justice, non-discrimination and anti-racism in the EU, 2022/2005(INI), point 9.

certain criteria that hate crime does not meet without a doubt.⁶¹ In summary, we can declare that the in-depth revision of the discussed field is becoming more and more urgent these days due to mass migration and technological development, yet it is clear that not even EU's primary law is prepared for a harmonisation effort of this magnitude.

3. Cyberbullying – Tackling the Issue of Cyberbully with 'Non-Cyberbully Specific' EU Legal Framework and Some Related Policies

3.1. EU Legal Frameworks and Policies

The issue of cyberbully, which based on scientific analyses is a serious problem in all Member States,⁶² has long been in the sight of the EU institutions. The European Commission already in its 2001 cyber security communiqué⁶³ examined the regulations of the Member States on cyberbullying and concluded that it was punishable as cybercrime⁶⁴ in the then 15 Member States. Cyberbully constitutes a separate offence only recently and only in a few Member States:⁶⁵

61 For an overview of these criteria in the light of hate crime, see: Peršak, 2022, pp. 109–116.

62 Henares-Montiel et al., 2022.

63 European Commission, Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM(2000) 890 final, Brussels, 26.1.2001.

64 Based on a 2013 Communication from the European Commission: Cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware). – European Commission, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final, Brussels, 7.2.2013.

65 Ćmiela, 2014, pp. 29–34.

Ireland's Coco's Law,⁶⁶ the French⁶⁷ and Italian⁶⁸ regulations worth mentioning in this regards. In 2009, the European Commission defined cyberbullying as follows: 'Cyberbullying is repeated verbal or psychological harassment carried out by an individual or group against others'.⁶⁹ However, it is important to clarify at the outset that despite this awareness, for the time being⁷⁰ there is no legally binding EU act directly addressing cyberbullying as *sui generis* criminal offence.⁷¹ In May 2023 the *European People's Party Group* (EPP) called for an EU-wide criminalisation of cyberbullying citing the Irish regulation as an example. The EPP reiterated its point of view in September 2023.⁷² However, there is no legislative procedure in progress at the moment based on the European Parliament's website. It is worth mentioning that Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) already in 2016 recommended that the European Commission should consider the possibility of initiating EU legislation and establish minimum rules by means of a directive, as the cross-border element makes it necessary to approximate national rules.⁷³ However, taking into account the answer of *Didier Reynders*, the European Commissioner for Justice, on the EPP's proposal during an EP debate on 10 May 2023 it seems less likely that in the near future these initiations will result in legislation. As *Reynders* emphasized, the European Commission is of the view that the current legislative framework and policies are sufficient to deal with the issue.⁷⁴

66 The law was enacted after the tragic suicide of Nicole Fox nicknamed 'Coco', who was a victim of bully both in person and online for three years. Her mother led a national campaign to raise attention to online harassment and abuse with success: in 2021, Ireland adopted 'Coco's Law' according to which the perpetrator could be incarcerated up to seven years if found guilty of distributing or publishing intimate images of a person without consent. – See: Collins, 2023.

67 LOI n° 2022-299 du 2 mars 2022 visant à combattre le harcèlement scolaire.

68 Legge 29 maggio 2017, n. 71 Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo.

69 European Commission, Safer Internet Day 2009: Commission starts campaign against cyber-bullying, MEMO/09/58.

70 5 January 2024.

71 Dalla Pozza et al., 2016, p. 9.

72 *Criminalise cyber-bullying*, 2023; *Criminalise cyberbullying across the EU*, 2023.

73 As the LIBE argued in its report in the absence of approximation, diverging offences and penalties renders the protection of victims insufficient and make it difficult to implement EU-wide policies on cyberbullying and other related issues, like data protection. The LIBE also suggested the creation of a specific criminal law offence for cyberbullying. Dalla Pozza et al., 2016, p. 15.

74 In a wider context he said: 'While we acknowledge that the issue of cyberbullying raises concerns at Member State and at EU level, we are convinced that the EU's legislative and policy framework is fit for purpose. With the entry into application of the Digital Services Act (DSA), the European Union now has powerful new tools to tackle mental health risks

The currently applicable legislative framework is constituted by:

- the Digital Services Act (hereinafter: DSA);⁷⁵
- the Audiovisual Media Services Directive (hereinafter: AVMSD);⁷⁶
- the European Electronic Communications Code;⁷⁷
- The applicable policy framework is:
- the 2022 Better Internet for Children Strategy (hereinafter: BIK+);⁷⁸
- the EU Comprehensive Strategy on the Rights of the Child;⁷⁹
- the Commission's proposal combating violence against women and domestic violence and;⁸⁰
- The Declaration on European Digital Rights and Principles.⁸¹

As Reynders explained, the DSA, in force since August 2023, creates a wide set of due diligence obligations applicable to intermediaries of digital services in connection with the specific risks related to serious negative effects on a person's physical and mental well-being. The consequences on physical and mental development of children is also taken into account.⁸² Under Art. 34(1) of the DSA, platform providers shall assess the actual and foreseeable effects of their services on mental health. They should also implement solutions that remedy

online, in particular for minors and young people. The Commission will work in close cooperation with the National Digital Services Coordinators in the supervisory framework established by the DSA.' – European Parliament, 2023.

75 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), Text with EEA relevance, OJ L 277, 27.10.2022, p. 1–102.

76 Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU 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) in view of changing market realities, OJ L 303, 28.11.2018, p. 69–92

77 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast), Text with EEA relevance, OJ L 321, 17.12.2018, p. 36–214.

78 European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+), COM(2022) 212 final, Brussels, 11.5.2022.

79 European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – EU Strategy on the Rights of the Child, COM(2021) 142 final, Brussels, 24.3.2021.

80 European Commission, 2024.

81 *European Digital Rights and Principles* [Online]. Available at: <https://digital-strategy.ec.europa.eu/en/policies/digital-principles>.

82 DSA, Recitals (81), (83) and (89).

the negative effects under Art. 35. Arts. 6a, 9 and 28b of AVMSD⁸³ obliges the Member States and the platform operators to take specific measures on the protection of minors for audiovisual content which may impair their physical, mental or moral development.⁸⁴ Under Art. 96 of the Electronic Communications Code, phone number ‘116 111’ addresses cyberbullying EU-wide in cooperation with the EU co-funded safer internet helplines by providing a permanent helpline for the victims.

As for the policies, taken into account the provisions of Art. 24 of the Charter, with special regard to Paragraph 2 which states that: ‘[...] the child’s best interests must be a primary consideration [...]’, the Union has launched a number of programmes aimed at protecting children in the online space and thus, even if mostly indirectly, providing protection against cyberbullying,⁸⁵ through *mainstreaming* children’s rights at EU policy level. The EU’s child protection programmes pay particular attention to the protection of children in the online space. This focus on the virtual space is important because, since while social networks offer the opportunity to build a digital society in Europe,⁸⁶ they also present a myriad of risks for children. The so-called ‘online exposure’ carries the risk of harmful and unlawful contact, such as online grooming and cyber-pandering to the detriment of children, cyberbullying, online abuse and harassment. Nearly a third of girls and a fifth of boys have experienced disturbing content on a monthly basis in the past year. Minority children are more likely to witness disturbing incidents online.⁸⁷ One of the side effects of the COVID-19 pandemic is that it has significantly increased the amount of time children spend online due to the fact that school, cultural and social life moved to the online space. This has led to increased online risks and digital inequalities.⁸⁸

83 Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU 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) in view of changing market realities OJ L 303, 28.11.2018, p. 69–92

84 For details on the scope of application of AVMSD, see: Specht-Riemenschneider, Marko and Wette, 2023, pp. 230–231.

85 Rizza and Guimarães Pereira, 2013, p. 7.

86 As stated in the European Commission’s ‘EU Strategy on the Rights of the Child: ‘Children play, create, learn, communicate and express themselves from a very young age through online and connected environments. Digital technologies enable children to participate in global movements and to play an active role in citizenship. Their innate digital literacy can help them to thrive in an increasingly digital and networked education and later in the labour market systems’, see: European Commission, COM (2021) 142 final, p. 18.

87 European Commission, COM(2021) 142 final, p. 18.

88 Lobe et al., 2021, pp. 21–25.

The European Commission's Strategy on the Rights of the Child 2021-2024⁸⁹ strives to answer these issues. Based on the strategy: 'all children in Europe and worldwide should enjoy the same rights and live free from discrimination, retaliation and intimidation.'⁹⁰ The Commission's detailed action plan is set out in point No. 5 of the Strategy. In the Action Plan, the Commission undertook, inter alia, to (i) adopt a Better Internet for Kids Strategy in 2022, (ii) take fight against all forms of abusing the children sexually online. The Commission invites Member States and companies in the information and communication technology (ICT) sector to take these actions.⁹¹ One of the objectives of this Strategy for a child-friendly internet is to raise awareness of the phenomenon of cyberbullying.⁹² The Commission communicated BIK+ in May 2022.⁹³ According to the Commission, the updated BIK+ strategy is the digital arm of the rights of the child strategy and reflects the recently proposed digital principle that 'Children and young people should be protected and empowered online.' The strategy highlights the importance of protection of children from:

- abusive marketing strategies;
- the harms of online gaming (including the financial harms);
- the harms of media illiteracy; and
- the harms of 'digital divide'.⁹⁴

The *Pathways to Success in School* initiative⁹⁵ also worth mentioning, which aims at developing or, where appropriate, further strengthening an integrated, comprehensive strategy towards school success by 2025.

Last but not least, according to the Commission: 'The Declaration on Digital Rights and Principles presents the EU's commitment to a secure, safe and sustainable digital transformation that puts people at the centre, in line with EU core values and fundamental rights.'⁹⁶ – Cyberbullying is not mentioned in the document, however.

89 European Commission, COM(2021) 142 final. For an analysis of the Commission's strategy on the rights of the child, see: Benyusz, 2021, p. 149

90 European Commission, COM(2021) 142 final, p. 1.

91 European Commission, COM(2021) 142 final, pp. 17–21.

92 ILGA-Europe, 2021.

93 European Commission, COM(2022) 212 final.

94 For an analysis on the indigenous peoples and the digital divide, see: Marinkás, 2018, pp. 313–314.

95 Announced in the Communication on achieving the European Education Area by 2025. See: European Commission, COM(2020) 625 final, Brussels, 30.9.2020.

96 European Commission, 2022.

3.2. Other Approaches

If the EU legislator would decide to regulate the issue at EU level this could only take place on the basis of the powers conferred on the Union under Art. 83 of the TFEU,⁹⁷ that is ‘setting minimum regulatory standards in a directive’.

However, in the absence of specific EU legislation aimed at cyberbullying it is worth considering, which other EU legislative acts or principles elaborated by the Court of Justice of the European Union may be applied to cyberbullying.

According to the document ‘Social Networks and Cyberbullying among Teenagers: EU Scientific e political report’,⁹⁸ efforts to regulate the social media platforms used by teenagers are an important element of EU level policies and actions in the context of the Charter. The theoretical bases developed in the document to address cyberbullying are that

Cyberbullying is about challenging the integrity, dignity and personality of the person, therefore it violates Arts. 1 and 3 of the Charter, namely the right to Human dignity and the right to integrity.

Cyberbullying may be considered as a form of torture, in this case Art. 4 on prohibition of torture and inhuman or degrading treatment or punishment would also be called up.

Cyberbullying is simultaneously the cause and outcome of damage to an individual’s reputation; protecting one’s privacy cannot be the main focus of strategies to cope with cyberbullying since that does not prevent reputations from being damaged online. One’s reputation online is sometimes challenged by the right to freedom of expression and information, set out in Art. 11 of the Charter.⁹⁹

Others argue that data protection is a promising approach,¹⁰⁰ thus the General Data Protection Regulation, the ‘GDPR’¹⁰¹ should be applied. The main point of this argument is that the right to erasure, also known as the ‘right to be forgotten’,¹⁰² guaranteed by the GDPR in Art. 17 could be an effective tool to combat

97 Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, p. 47–390.

98 Rizza and Guimarães Pereira, 2013, p. 49.

99 Rizza and Guimarães Pereira, 2013, p. 23.

100 As an excursion outside the EU, the 2021 ‘Cyber and Data Protection Act’ of Zimbabwe follows this approach. See: *Preventing cyberbullying under the Data Protection Act*, 2022.

101 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Text with EEA relevance, OJ L 119, 4.5.2016, p. 1–88.

102 Hulkó and Marinkás, 2023.

cyberbullying.¹⁰³ Indeed cyberbullying is characterised on the *one hand by the fact that it takes place on online platforms accessible to a large public*, i.e. the victim is bullied in front of a significantly larger audience than in case ‘traditional bullying’, and *on the other hand by the fact that the bullying content remains accessible for a long period of time*. However, at the time of writing,¹⁰⁴ the Court of Justice of the European Union (hereinafter: CJEU) has not yet handed down any judgments in which cyberbullying has been the subject of proceedings, although it has dealt with the right to be forgotten, on several occasions, and some trends can be discerned in relation to this right. According to the *Google Spain case*,¹⁰⁵ an individual has the right to request the removal of his or her personal data from the search engine results of the internet, but this right is not absolute: each request must be examined on a case-by-case basis, striking the right balance between the fundamental rights to the protection of personal data and privacy of the data subject and the legitimate interests of internet users, including freedom of expression and opinion. The rights to data protection and privacy prevail over the right to information where information on the individual’s private life is sensitive and knowing the information at hand is not a public interest. The latter two conditions clearly apply to data made public as part of cyberbullying. In the *Google LLC case*,¹⁰⁶ the CJEU clarified the above ruling by stating that the search engine operator, when executing a request for deletion of a link, is not obliged to carry out the deletion on all versions of its search engine, but only on the Member State specific versions of the search engine, that is to say the GDPR does not have *extra territorial effect* in this respect.¹⁰⁷ In a case initiated by a Hungarian domestic court, namely, the *C-46/23 Budapest Főváros IV. Kerület Újpest Önkormányzat Polgármesteri Hivatala v Nemzeti Adatvédelmi és Információszabadság Hatóság* judgment, ruled that that the national supervisory authority may order the erasure of data processed unlawfully, even in the absence of a prior request by the data subject, and that such erasure may also cover data collected from that person and from other sources.¹⁰⁸

¹⁰³ Cook, 2015.

¹⁰⁴ 10 January 2024.

¹⁰⁵ Case C-131/12, *Google Spain*, judgment of 13 May 2014.

¹⁰⁶ Case C-507/17, *Google LLC, successor in title to Google Inc. v Commission nationale de l’informatique et des libertés (CNIL)*, judgment of 24 September 2019.

¹⁰⁷ Bourne et al., 2020.

¹⁰⁸ ‘Article 58(2)(d) and (g) of [the GDPR] must be interpreted as meaning that the supervisory authority of a Member State is entitled, in the exercise of its corrective powers foreseen under those provisions, to order the controller or processor to erase unlawfully processed personal data, even though no request to that end has been made by the data subject with a view to exercising his or her rights pursuant to Article 17(1) of that regulation.’ – For a detailed analysis of the case, please see: Angyal, 2024, pp. 4-12.

Last but not least some independent initiatives also worth mentioning like the Youth Pledge for a *Child-Friendly Internet*,¹⁰⁹ the *Youth Call for Action*,¹¹⁰ aimed at preventing bullying online by creating a school climate free from bullying, and the opportunities to use artificial intelligence tackling the issue of cyberbully.¹¹¹ – The latter idea is articulated in a 2021 proposal for legislation of the European Commission as well.¹¹²

4. Child Protection in the Digital Age ‘from the Digital Age’ – EU Perspective

The ever-increasing use of digital space poses unknown threats to each consumer; naturally, children are more endangered than average users. When it comes to the analysis of EU’s primary law, it must be stated that the legal basis of an effective child protection system is not laid down in details, at least explicitly. The TEU declares that the protection of the rights of the child is one of the EU’s core values regarding the realisation of both its inner policies and external activities.¹¹³ According to the TFEU, ‘trafficking in human beings and sexual exploitation of women and children’ belongs to the category of euro-crimes.¹¹⁴ Title III of the Charter encompasses the rights of the child; in this provision ‘the right to such protection and care as is necessary for their well-being’ and the child’s best interest as a primary consideration must be accentuated.¹¹⁵ Therefore, it can be deduced that EU’s child protection system stands on the grounds of several competences that do not refer to the issues of children explicitly in the Founding Treaties.

109 *Youth Pledge for Better Internet* [Online]. Available at: <https://www.betterinternetforkids.eu/en/policy/youth-pledge-for-a-better-internet>

110 *1st European Youth Day at Europol, 20 November 2018* [Online]. Available at: https://www.europol.europa.eu/sites/default/files/documents/call_for_action-european-youth-day.pdf

111 Rakhmatov, 2022.

112 European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (artificial intelligence act) and Amending Certain Union Legislative Acts, COM(2021) 206 final, Brussels, 21.4.2021.

113 TEU, Art. 3(3) and (5).

114 TFEU, Art. 83(1). In the field of common immigration policy, the basis of harmonisation can also be the aim of combatting trafficking in persons, in particular women and children. See: TFEU, Art. 79(2)(d).

115 Charter, Art. 24. Of course, other articles also influence indirectly the status of children. For a brief overview, see: Kaesling, 2023, pp. 79–80.

The enumeration of the relevant EU (secondary) legislation influencing child protection is almost impossible, since a huge number of legal instruments encompasses provisions sporadically. The sources concerned can be divided into two pairs of categories: firstly, soft law and hard law instruments can be distinguished through the examination of their legal binding force; secondly, analysing the core content of the pieces of legislation, we may differentiate instruments on child protection (direct instruments) and instruments regulating other kinds of social relations with specific provisions applicable to children (indirect instruments).¹¹⁶ Therefore, we find reasonable the division of these sources into four subcategories based on their relation to child protection:

- indirect soft law;
- direct soft law;
- indirect hard law; and
- direct hard law.

Various documents could be discussed in the category of indirect soft law tools of child protection; therefore, introduce only a few pieces of paramount importance here. The 2030 Digital Compass¹¹⁷ mentions among the so-called ‘digital principles’ the protection and empowerment of children in the online space. In 2023, the European Parliament adopted a resolution concerning consumer protection in connection with the online video games. In addition to other important principals, this document states that children, ‘when playing online video games, should benefit from an equal level of protection to that provided by the DSA’.¹¹⁸ As a third example, the European Commission’s recommendation¹¹⁹ on principles for the protection of players of online gambling deserves to be emphasised, since this document encompasses a series of child protection measures,

¹¹⁶ Naturally, EU sources of child protection are complete with the respective case law of the CJEU. However here, due to space constraints, we only focus on pieces of legislation.

¹¹⁷ European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – 2030 Digital Compass: the European way for the Digital Decade, COM(2021) 118 final, Brussel, 9.3.2021, point 15.

¹¹⁸ European Parliament resolution of 18 January 2023 on consumer protection in online video games: a European single market approach, 2022/2014(INI).

¹¹⁹ As we all know, recommendations are considered legal instruments of the EU, however they do not possess binding force like regulations, directives and resolutions do, that is why we decided to introduce the mentioned document as an example of relevant soft law sources.

including suggestions regarding the content and broadcast of commercial communications concerned.¹²⁰

Among direct soft law instruments, the EU Strategy on the Rights of the Child and BIK+,¹²¹ already discussed in subchapter 3, stand out from the past few years. Besides, The EU's Strategy for a more effective fight against child sexual abuse¹²² may be classified here, an instrument with the finality of providing a comprehensive response to the threat of child sexual abuse, both on- and offline; to achieve this, it envisages the full implementation by Member States alongside with the revision of the existing framework of protection, and the strengthening of law enforcement in the area, enhancing 'cooperation among all stakeholders'.

In subchapter 3, a number of indirect hard law instruments has been introduced like DSA, AVMSD and the European Electronic Communications Code, their most significant rules concerning child protection have been briefly summarised.¹²³ Instead of an attempt to create a taxonomy about this subcategory, we just refer to the criminal procedure related EU harmonisation activity and to some of its special minimum standards. According to EU law, persons under the age of 18 has special rights both as suspects or accused ones and as victims in criminal procedures. In the group of indirect hard law instruments, we shall place the directive on the protection of victims of crime,¹²⁴ which has a general focus in the sense that it provides rights to victims of each age group, but specific child protection elements also appear: (i) child's best interest as primary consideration and the promotion of child-sensitive approach appear among the objectives in Art. 1(2); (ii) the rules on the right to protection of privacy (Art. 21) contain an obligation for Member States to 'ensure that competent authorities may take all lawful measures to prevent public dissemination of any information that could lead to the identification of a child victim'; (iii) pursuant to Art.

120 For all the measures related to minors in the cited document, see: 2014/478/EU: Commission Recommendation of 14 July 2014 on principles for the protection of consumers and players of online gambling services and for the prevention of minors from gambling online, Text with EEA Relevance, OJ L 214, 19.7.2014, p. 38–46, points 8–14.

121 See: footnotes 77 and 78.

122 European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – EU Strategy for a more effective fight against child sexual abuse, COM(2020) 607 final, Brussels, 24.7.2020.

123 See: footnotes 74–76. Major provisions of DSA are discussed in subchapter 5.

124 Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA, OJ L 315, 14.11.2012, p. 57–73.

24 on the right to protection of child victims, it is stated that, in criminal investigations, interviews with the child shall be recorded, thus the records can be used as evidence in order to avoid unnecessary repetition of such actions.¹²⁵

Finally, we chose to emphasise the role of two direct hard law instruments. The first source serves substantial criminal law harmonisation concerning sexual abuse and sexual exploitation of the children and child pornography.¹²⁶ Art. 5, that describes minimum standards of the offence of child pornography, reacts to certain typical online phenomena like *sexting* that may be considered deviances.¹²⁷ Returning to the issue of the rights of the child in criminal procedures, there is a separate directive that recollects special requirements in favour of the protection of juvenile offenders.¹²⁸ Related to technological solutions and challenges, two provisions must be highlighted: (i) the requirement of providing the opportunity of making an audiovisual record of questioning, if it is proportionate in the circumstances of the case (Art. 9); (ii) and the right to privacy, meaning that the previously mentioned records cannot be distributed and that court hearings shall be held in the absence of the public (Art. 14).¹²⁹

We can conclude that the protection of children against online (and offline) threats has a fragmented, yet detailed legal regime on EU level, nonetheless it does not guarantee a sufficient level of defence, since today, although their ideas may prevail in practice, Member States are not bound by the many soft law sources presented above and in the cases where implementation is mandatory, transposition is usually incomplete or incorrect. From another point of view, child protection can never be only an area of (harmonised) legal safeguards.

125 The proposal regarding the amendment of the directive concerned was adopted on 12 July 2023, also affecting children's accessibility to special assistance. For a summary on the content of the amendment, see: Görgényi, 2023, pp. 250–252.

126 Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, OJ L 335, 17.12.2011, p. 1–14.

127 On the other hand, the transposition of this provision created further problems in practice. Namely, it renders Member States to criminalise the act of interchanging indecent photos between two minors, which clearly could not be the purpose of the legislator. In Hungary, scholars argue that criminal courts shall solve such cases by declaring that the criminal offence in question is not committed due to the lack of danger to society. See: Ambrus, 2021, pp. 105–106; Mezei, 2021, pp. 27–28. In contrast, recordings not originally obtained by unlawful means may later be used for unlawful purposes like revenge porn. See: Sorbán, 2023, pp. 180–181.

128 Directive (EU) 2016/800 of the European Parliament and of the Council of 11 May 2016 on procedural safeguards for children who are suspects or accused persons in criminal proceedings, OJ L 132, 21.5.2016, p. 1–20.

129 For more details on the content of the directive concerned, see: Róth, 2018, pp. 834–839.

In our opinion, EU initiatives should rather focus on the effectiveness of programmes and other actions raising user awareness, thus teaching children how to handle the risks of cyberspace.

5. The Beginning of a New Age of platform liability (?): Main Rules of DSA

In an effort to provide a holistic picture of our main issue, in addition to the liability rules on perpetrators, we considered necessary to give a brief introduction on the EU regulation affecting the ‘third parties’ concerned in such unlawful situations, i.e. those persons who operate online platforms.

Because of the expansion of online platforms, and the online sphere in general, new dilemmas frequently emerge, affecting different branches of law and leading to the accelerated development of relatively new areas of regulation; this is the case of consumer protection law too. As new forms of violations appear, issues regarding the right to privacy¹³⁰ or rather, the concept of private sphere needs to be reinterpreted.¹³¹ In our opinion, these arguments prove that digital platforms need a *sui generis* legal regulation to ensure security for users. Moreover, as physical frontiers do not limit the harmful activities realised in the online space, the creation of a supranational legal framework is desirable. We can state that in Europe, a major development has taken place in this regard.

In autumn 2022, two legal instruments of fundamental importance were adopted by the EU legislator, delivering a new framework applicable to activities in the digital sphere: the regulation mentioned several times throughout this chapter, the DSA and the Digital Markets Act (hereinafter: DMA¹³²).¹³³ In simple

¹³⁰ For different scientific approaches on the concept of the right to privacy, see: Halász, 2023, pp. 59–74.

¹³¹ For example, Barzó and Halász analysed the discussed issue in connection with the protection of personal rights in Hungary. They identified several new problematic areas, e.g. related to biometric identification and the so-called ‘cookies’. Barzó and Halász, 2020, pp. 46–47.

¹³² Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), Text with EEA relevance, OJ L 265, 12.10.2022, p. 1–66.

¹³³ The two regulations are part of a strategy of five major projects with the aim of the ‘European re-sovereignisation’. In this context, according to Bendiek, the notion ‘sovereignty’ has a new meaning, as it refers to ‘a multi-level political practice’ (*eine politische Mehrebenenpraxis*) in Europe. Bendiek, 2021, pp. 6–8.

terms, we can state that the provisions of DSA mainly focus on consumer protection, while DMA sets standards that fall within the scope of competition law. As the whole chapter analyses the pieces of EU's legal framework that provide protection for individuals, we have decided to omit the examination of competition law regulation, so subchapter 5 concentrates on the concept represented by DSA. Additionally, as DSA is a new piece of legislation, we feel obliged to summarise the main rules of this area on EU level before 2022.

5.1. The 'Ante DSA Era' – Relevant Provisions of the E-Commerce Directive

As legal challenges in connection with online platforms have showed up relatively recently, legislative bodies, both on supranational and intra-national level, took their time to outline the foundations of the respective regulation. Moreover, since in this area European legal culture has no well-established legal traditions, the regulatory concepts applied by Member States logically diverge from each other, at least to some extent. Therefore, the adoption of instruments with the aim of a comprehensive harmonisation envisages the need for creating a European concept of platform law, which is a major task in itself. Hence, self-regulation of digital platforms has been playing a key role in the area.

As a relatively important piece of legislation concerning digital services from the 'ante DSA era', we chose to briefly introduce relevant rules of the E-Commerce Directive (hereinafter: ECD).¹³⁴ Its main objective is to 'contribute to the proper functioning of the internal market by ensuring the free movement of information society services'¹³⁵ between the Member States.¹³⁶ To this end, it determines provisions in several fields; hereby we highlight rules on commercial communications,¹³⁷ the liability of intermediaries and codes of conduct.

Section 2 of ECD encompasses requirements of commercial communications. Pursuant to Art. 6, in addition to other information requirements prescribed by EU law, Member States shall guarantee that commercial communications that

¹³⁴ 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'), OJ L 178, 17.7.2000, p. 1–16.

¹³⁵ As for the legal definition of 'information society services', ECD makes a reference to Art. 1(2) of Directive 98/34/EC, which was repealed in 2015. See: Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations, OJ L 204, 21.7.1998, p. 37–48.

¹³⁶ ECD, Art. 1(1).

¹³⁷ For the definition of commercial communication, see: ECD, Art. 2(f).

are part of, or constitute, an information service also comply with the following criteria: (i) ‘the commercial communication shall be clearly identifiable as such; (ii) the natural or legal person on whose behalf the commercial communication is made shall be clearly identifiable; (iii) promotional offers [...], where permitted in the Member State where the service provider is established, shall be clearly identifiable as such, and the conditions which are to be met to qualify for them shall be easily accessible and be presented clearly and unambiguously; (iv) promotional competitions or games, where permitted in the Member State where the service provider is established, shall be clearly identifiable as such, and the conditions for participation shall be easily accessible and be presented clearly and unambiguously.’ In summary, commercial communications are required to be easily identifiable, accessible, clearly comprehensible and transparent. Art. 7 discusses the issue of unsolicited commercial communications, better known as spams. Such communications shall also be clearly identifiable when received by the recipient. It also states that service providers who use such instruments shall regularly consult opt-out registers, where natural persons can indicate that they do not wish to receive any.¹³⁸ Art. 8 adds an extra condition to commercial communications when ‘provided by a member of a regulated profession (such as lawyers or medics), namely that these instruments shall comply with the rules of the profession concerned, ‘in particular, the independence, dignity and honour of the profession, professional secrecy and fairness towards clients and other members of the profession.’ The same article also encourages the establishment of codes of conduct by professional bodies.

As for the liability of providers of intermediary services (hereinafter: providers), the ECD differentiates explicitly between three types of such services, also establishing the respective liability rules and grounds of exemption: (i) mere conduit (Art. 12); (ii) caching (Art. 13); and (iii) hosting (Art 14.).¹³⁹ In this regard, it is a crucial provision that, pursuant to Art. 15, Member States cannot impose on providers ‘to monitor the information which they transmit or store,

¹³⁸ Although, this provision became obsolete not long after its entry into force, since Art. 13 of the so-called ePrivacy Directive introduced an opt-in system of direct marketing, when the recipient is considered a consumer. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47. See also: Lodder, 2017, pp. 39–40.

¹³⁹ For a detailed description of these terms, see: Lodder, 2017, pp. 48–52. For a brief explanation of the liability rules concerned, see: Gosztönyi, 2022, pp. 20–22.

nor a general obligation actively to seek facts or circumstances indicating illegal activity.¹⁴⁰

ECD also encourages self-regulation of the operators concerned: both Member States and the European Commission shall promote ‘the drawing up of codes of conduct [...], designed to contribute to the proper implementation of [the main provisions of ECD]’ and codes promoting ‘the protection of minors and human dignity’. EU also encourages the participation of associations or organisations representing consumers in the drafting process of such documents. Moreover, the idea of interchanging best practices based on information granted by professional and consumer associations with practical experience.¹⁴¹

5.2. The structure and the main novelties of DSA

DSA, which consists of 93 articles in total, is a codex-like piece of EU legislation on intermediary services. Here, our purpose is to summarise the structure and the main novelties, thus we refrained from giving a comprehensive presentation on each norm.

5.2.1. Objective, Scope and Selected Basic Notions

Art. 1(1) of DSA clarifies the main objective of the regulation, namely ‘to contribute to [...] the internal market for intermediary services by setting out harmonised rules for a *safe, predictable and trusted online environment that facilitates innovation and in which fundamental rights* enshrined in the Charter, including the principle of consumer protection,¹⁴² *are effectively protected.*’ Then Art. 1(2) states the three main fields of harmonised rules:

- ‘a framework for the conditional exemption from liability of providers of intermediary services;
- rules on specific due diligence obligations tailored to certain specific categories of providers of intermediary services;
- rules on the implementation and enforcement of this Regulation, including as regards the cooperation of and coordination between the competent authorities.’

¹⁴⁰ To complete the picture, it must be noted that the second paragraph of the same article allows Member States to establish obligations for providers to inform public authorities *whenever they become aware* of alleged criminality. It must be emphasised that this measure does not constitute the obligation of active monitoring either.

¹⁴¹ ECD, Art. 16.

¹⁴² ‘Union policies shall ensure a high level of consumer protection.’ – Charter, Art. 38.

Nonetheless, regarding the scope of DSA, Art. 2(1) states that it ‘shall apply to intermediary services offered to recipients of the service that have their place of establishment or are located in the Union, irrespective of where the providers of those intermediary services have their place of establishment.’ In short, whether DSA is applicable depends on the physical location of the recipient; from another point of view, providers established outside of the EU will also fall under the scope of DSA, whenever their service is used by someone located in the EU.

DSA operates with several *sui generis* notions, of which we must underline some. One key term, intermediary service is a subcategory of information society services of which the definition is described by a reference to Directive 2015/1535.¹⁴³ DSA then uses the same terms as ECD did concerning intermediary services, i.e. the three types are distinguished: (i) mere conduit; (ii) caching; and (iii) hosting.¹⁴⁴ Other two important notions are ‘online platform’¹⁴⁵ and online search engine’.¹⁴⁶ Although it is not placed among definitions, we must emphasise the terms ‘very large online platform’ (hereinafter: VLOP) and ‘very large online search engine’ (hereinafter: VLOSE). These are intermediary services that ‘have a number of average monthly active recipients of the service in the Union equal to or higher than 45 million’ and which appear in the designation decision of the European Commission.¹⁴⁷

5.2.2. *The Structure of the Framework Obliging Providers of Intermediary Services*

After the general provisions, Chapter II summarises liability rules applicable to providers. Similarly to ECD, DSA treats separately the three types of intermediary services (Art. 4–6), but then adds on Voluntary own-initiative investigations and legal compliance (Art. 7), declaring that such initiatives do not affect the

143 ‘[A]ny Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.’ Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, Text with EEA relevance, OJ L 241, 17.9.2015, p. 1–15, Art. 1(1)(b).

144 For the respective definition on each type, see: DSA, Art. 3(g).

145 DSA, Art. 3(i). As an essential definitional element, it must be underlined that online platforms form a subcategory of hosting services. This notion has a different a focus and a narrower scope compared to the one in the original proposal of the European Commission and to the approach of the OECD. For more details, see: Sorbán, 2022, pp. 71–72.

146 DSA, Art. 3(j).

147 DSA, Art. 33(1). Cf. Zódi, 2022, pp. 73–74.

eligibility for the exemptions from liability. More importantly, neither ECD did, nor DSA does constitute the obligation of general monitoring for providers (Art. 8). On the other hand, DSA grants the right for national judicial and administrative authorities to issue orders to act against illegal contents and to provide information towards providers (Art. 9–10).¹⁴⁸

Chapter III prescribes obligations for different categories of providers. Here, DSA presents a layered regulation framework as indicated in the figure below.

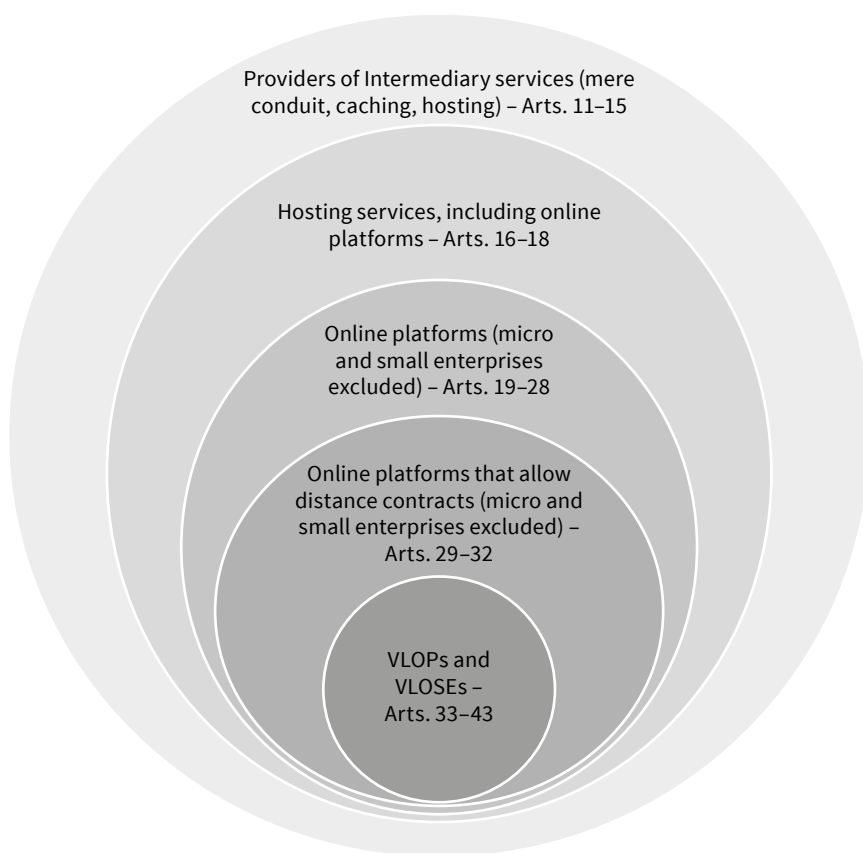


Figure 1. Layers of DSA Chapter III regulation framework¹⁴⁹

¹⁴⁸ See also: Chiarella, 2023, p. 45.

¹⁴⁹ Source: edited by the authors based on DSA.

As it can be seen, five layers can be distinguished. Each layer must comply with the rules prescribed for the more outer layers, i.e. VLOPs and VLOSEs¹⁵⁰ are obliged by rules of Arts. 11–43; providers of online platforms that allow distance contracts are obliged by rules of Arts. 11–32; and so on. Chapter III Section 6 on due diligence obligations are also common standards for each category. One aspect worth highlighting is that hosting services, including online platforms has the duty to ‘put [easy to access and user-friendly] mechanisms in place to allow any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content.’¹⁵¹

5.2.3. National and EU Authorities

As part of the implementation, DSA obliges Member States to designate one or more competent authorities to be responsible for the supervision of providers and the enforcement of itself. One of these authorities must be chosen as the ‘Digital Services Coordinator’ (hereinafter: DSC) that holds responsibility in the Member State concerned. DSCs must cooperate with each other and competent EU actors, i.e. the European Commission and the European Board for Digital Services (hereinafter: Board).¹⁵² Furthermore, DSCs function as fora of complaints; a complaint can be lodged by the recipients of the service and by ‘anybody, organisation or association mandated to exercise the rights conferred by this Regulation on their behalf’.¹⁵³ Then DSCs draw up annual reports, including the number of received complaints and an overview of their follow-up, which must be available publicly and also sent to the European Commission and the Board.¹⁵⁴ Finally, a special competence worth mentioning is that, if certain criteria are met, DSCs have the possibility to lead joint investigations, of which the duration is three months unless otherwise agreed amongst the participants.¹⁵⁵

In addition to the European Commission, a *sui generis* body of DSA is the Board, an organ that consists of delegated members of DSCs, chaired by the

150 For the complete list of VLOPs and VLOSEs, see: *Supervision of the designated very large online platforms and search engines under DSA* [Online]. Available at: <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses> (). For a brief summary on the duties of VLOPs and VLOSEs, see: Chiarella, 2023, pp. 47–49.

151 DSA, Art. 16(1). For more information regarding the lawful treatment of illegal content, see: Bendiek, 2021, pp. 9–11.

152 DSA, Art. 49. The exact powers of DSCs provided by EU measures are listed in Art. 51.

153 DSA, Art. 53.

154 DSA, Art. 55.

155 DSA, Art. 60.

European Commission. The Board mainly has advisory consultative and supportive powers and can adopt opinions and recommendations.¹⁵⁶ A specific information sharing system has been established that national and EU bodies concerned shall use for all communications related to their competences prescribed by DSA.¹⁵⁷

5.2.4. Financial Sanctions in DSA

DSA introduces two types of financial sanctions: (i) fine; and (ii) periodic penalty payment. A fine is a one-time sanction that shall be imposed in case of the violation of certain rules of DSA, while periodic penalty payment is applied periodically when a provider fails to fulfil a decision of the competent authority. Both types are maximised based on the worldwide turnover of the provider concerned in the preceding financial year. Member States have the right to formulate their own measures complying with these provisions. In connection with VLOPs and VLOSEs, the European Commission has the right to impose the sanctions.

5.3. Expectations and Misgivings

From the European perspective, it is indisputable that DSA has brought the new age of platform regulation with an unprecedented complexity. Nevertheless, it is worth noticing that the regulation in question does not create a completely new framework but improves the one based on ECD.¹⁵⁸ Some scholars argue that these improvements will strengthen the enforceability of both consumer rights and fundamental rights.¹⁵⁹ Others state that the introduction of new categories (VLOPs and VLOSEs) and the mandatory designation of national authorities (DSCs) supplemented by the Board will eventually result in the development of a consistent, ‘European practice’ in the area.¹⁶⁰ In this regard, crucial questions like jurisdictional issues, the protection of vulnerable consumers and the interpretation of new notions provided by DSA must be discussed.¹⁶¹ In principle, these improvements will have an overwhelmingly positive impact. On the other hand, experts have already expressed their concern regarding the fact that tightening liability rules could lead to the deficit of certain fundamental

¹⁵⁶ DSA, Arts. 61–63.

¹⁵⁷ DSA, Art. 85.

¹⁵⁸ Zankova and Gosztonyi, 2022, p. 74.

¹⁵⁹ Halász, 2023, p. 222.

¹⁶⁰ Zankova and Gosztonyi, 2022, p. 77. Cf. Gombos, 2023, pp. 115–116.

¹⁶¹ Gombos, 2023, pp. 114–115.

rights. Specifically, the obligation to remove illegal content, including content that constitutes hate speech, is likely to result in excessive removal practices, thereby limiting unnecessarily the freedom of expression.¹⁶²

At this point, all the opinions mentioned are hypothetical statements, only radical change is certain. The success of European legislation was just the first essential step towards a reliable and secure digital sphere. Both jurisprudence and legal practice will play prominent roles in realising the potential of DSA and avoiding pitfalls in the coming years.

Summary

Final Thoughts on the Status Quo of EU Legislation vs. Deviances Induced by Hatred

Legal regulation, especially criminal law regulation, is reactive in nature, i.e. it evolves by solving new problems arising from the development of social and economic relations. From the 1990s onwards, computers began to slowly become part of everyday life, thus we entered the digital age. These days our smartphones are capable of performing more different functions than those computers thirty years ago and no man can foresee the new directions for future development – today, it is more than likely that computers will eventually become part of the human body as implants.¹⁶³ This ever-accelerating technological process causes accelerated pace of change in social and economic relations too. Consequently, it is becoming increasingly difficult for intra-national legislations to improve their legal regimes accordingly. Furthermore, online crime and new forms of cyber-deviance know no national borders; a change of (physical) location is no longer necessary to commit an offence with an international component. Therefore, international cooperation has become a cornerstone of effective law enforcement, requiring the (at least partial) harmonisation of the respective national regulations. In Europe, it is evident that the driving force behind such a cooperation shall be the EU.

In this chapter, we strived to summarise the most important tools provided by EU legislation to date. Assessing the progress as it stands today, we must declare that the reactivity of the supranational legislator is far from optimal.

¹⁶² Zankova and Gosztanyi, 2022, pp. 78–79; Turillazzi et al., 2023, pp. 93–94.

¹⁶³ This prediction is no longer part of science fiction. In early 2024, it was officially announced that Neuralink had placed its first chip in a human brain. See: Guarino, 2024.

The legal instrument currently harmonising hate speech and hate crime was adopted in the form of a framework decision, i.e. a *sui generis* source of law of the late Third Pillar. More than fifteen years passed since its entry into force, but today not even the legal basis of the adoption of a new directive in the area is laid down properly in the Founding Treaties, although the first steps have been taken in this regard. The concept of cyberbullying as a new criminal law minimum standard towards Member States has not been developed yet.¹⁶⁴ It can be stated that many national legal systems in Europe are more advanced from this point of view. The ‘applicable legal framework’ enumerated in subchapter 3 does not provide the sufficient level of protection against such criminal activities. The use of analogy may be a beneficial way of treating the problem, nevertheless the majority of criminal law theorists argue that its use would violate the principle of legality, thus cannot be applied.¹⁶⁵ The child protection system consists of numerous instruments, both soft law and hard law; the regulation is fragmented. In our opinion, apart from certain types of criminal offences which are usually perpetrated online and the rights of the children in criminal procedures, EU should rather promote the interchange of national best practices on a regular basis, since child protection is a far too complex issue; a comprehensive (hard law) harmonisation is hardly achievable. In the field of platform law, DSA and DMA can both be considered significant results of EU legislation. In subchapter 5, we focused on the main rules of DSA which are quite promising theoretically. Nonetheless, several innovative solutions shall be applied from 17 February 2024, thus we still do not know precisely what kind of new, unforeseen practical problems may emerge.

As a final conclusion, we must declare that the current EU framework does not give the impression of an up-to-date system of legal norms in the discussed areas. On the other hand, it can be noticed that relevant initiatives are in progress, however the applicable legislative procedures, when the European society faces such urgent issues, are too time-consuming. The way we see it, in order to achieve effective harmonisation, and through harmonisation, effective cooperation in practice, Member States might create other fora to facilitate the approximation of different national concepts in the field of these common problems.

¹⁶⁴ At this point, it is worthy of note that a potential theoretical basis for the future EU concept of cyberbullying could be derived from the *ratio decidendi* of the relevant case law of the European Court of Human Rights. For its most relevant decisions, see: Béres, 2023, pp. 89–93.

¹⁶⁵ Although, the total ban of the use of analogy in criminal law is rather debated in some cases. On this question, see: Horváth and Sántha, 2019, pp. 70–71; Belovics, 2020, pp. 624–625; Myftari and Guço, 2021, pp. 20–22, 25.

Bibliography

- Ambrus, I. (2021) *Digitalizáció és büntetőjog*. Budapest: Wolters Kluwer.
- Angyal Z. (2024) 'A tagállami felügyeleti hatóságok és a jogellenesen kezelt adatok törlése Az Európai Bíróság legújabb ítélkezési gyakorlatában', *Advocat*, 27(1), pp. 4–12.
- Barzó, T., Halász, Cs. (2020) 'Elmosódott magánélet? A privátszféra érvényesülése és határai az online közösségi térben', *Miskolci Jogi Szemle*, 15(1), pp. 33–47.
- Belovics, E. (2020) 'A büntetőjog jogállami követelményei', *Magyar Tudomány*, 181(5), pp. 614–629; <https://doi.org/10.1556/2065.181.2020.5.5>.
- Bendiek, A. (2021) *Integrationspolitische Bedeutung des Digital Service Act (DSA) und Digital Markets Act (DMA) – Digitalmarktregulierung als eines von fünf digitalpolitischen Großprojekten der EU*. Berlin: Stiftung Wissenschaft und Politik; <https://doi.org/10.18449/2021AP01>.
- Benyusz, M. (2021) 'A gyermekek jövője az Európai Unióban – Mit ígér a Bizottság 2021-2024-es stratégiája?', *Jog – Állam – Politika*, 13(3), pp. 149–162.
- Berend, T. I. (2021) *Az Európai Unió története – Integráció, populizmus, nacionalizmus*. Budapest: Kossuth.
- Béres, N. (2023) 'Strasbourgi tükrök: az online gyűlöletbeszéd és a kibermegfélemlítés az Emberi Jogok Európai Bírósága esetjogában' in Nagy, Z. (ed.) *Az összehasonlító jog eszközével a gyűlölet ellen – Az online gyűlöletbeszéd, zaklatás és megfélemlítés nemzetközi szabályozása*. Budapest: Mádl Ferenc Intézet, pp. 73–97; https://doi.org/10.47079/2023.nz.gyuloletbeszed.10_4.
- von Bogdandy, A. (2012) 'Neither an International Organization Nor A Nation State: The EU as a Supranational Federation' in Jones, E., Menon, A., Weatherill, S. (eds.) *The Oxford Handbook of the European Union*. Oxford: Oxford University Press, pp. 761–776; <https://doi.org/10.1093/oxfordhb/9780199546282.013.0053>.
- Bourne, H., Moran, J., Corbett-Wilkins, R., McDevitt, J. (2020) 'Reflecting on the Google LLC v CNIL (Case C-507/17) ECJ Judgment: A UK and Australian Perspective', *Clyde & Co LLP*, 29 January. [Online]. Available at: <https://www.mondaq.com/uk/privacy-protection/888242/reflecting-on-the-google-llc-v-cnll-case-c-50717-ecj-judgment-a-uk-and-australian-perspective>
- Chiarella, M. L. (2023) 'Digital Markets Act (DMA) and Digital Services Act (DSA): New Rules for the EU Digital Environment', *Athens Journal of Law*, 9(1), pp. 33–58; <https://doi.org/10.30958/ajl.9-1-2>.
- Ćmiela, S. (2014) 'Cyberbullying Legislation in Poland and Selected EU Countries', *Procedia – Social and Behavioral Sciences*, 109(1), pp. 29–34; <https://doi.org/10.1016/j.sbspro.2013.12.416>.
- Collins, A. (2023) 'Coco's Law – Harassment, Harmful Communications and Related Offences Act', *Wolfe & Co. LLP*, 23 August. [Online]. Available at:

- <https://www.wolfe.ie/cocos-law-harassment-harmful-communications-and-related-offences-act/>
- Cook, L. (2015) 'The Right to Be Forgotten: A Step in the Right Direction for Cyberspace Law and Policy', *Case Western Reserve Journal of Law, Technology & the Internet*, (6)1, pp. 121-132.
- Costa-Lascoux, J. (1995) 'La lutte contre le racisme en Europe. Les instruments internationaux', *Revue Européenne des Migrations Internationales*, 11(3), pp. 205-219; <https://doi.org/10.3406/remi.1995.1487>.
- European Commission (2022) 'Digital Rights and Principles: Presidents of the Commission, the European Parliament and the Council sign European Declaration' *European Commission – Press release*, 15 December. [Online]. Available at: <https://digital-strategy.ec.europa.eu/en/news/digital-rights-and-principles-presidents-commission-european-parliament-and-council-sign-european>
- European Commission (2024) 'Commission welcomes political agreement on new rules to combat violence against women and domestic violence' *European Commission – Press release*, 6 February. [Online]. Available at: https://ec.europa.eu/commission/presscorner/api/files/document/print/es/ip_24_649/IP_24_649_EN.pdf
- European Parliament (2023) *Verbatim report of proceedings: 16. Fighting cyberbullying of young people across the EU (debate) (Strasbourg, 10 May 2023)* [Online]. Available: https://www.europarl.europa.eu/doceo/document/CRE-9-2023-05-10-ITM-016_EN.html
- Farkas, Á. (2001) *Büntetőjogi együttműködés az Európai Unióban*. Budapest: Osiris.
- Friedery, R., Horváthy, B. (2018) 'Európai Unió Alapjogi Chartája' in Lamm, V. (ed.) *Emberi jogi enciklopédia*. Budapest: HVG-ORAC, pp. 248-257.
- Gombos, K. (2023) 'A Digital Services Act és a Digital Markets Act várható kihívásai a jogalkalmazásban', *In Medias Res*, 12(2), pp. 92-119; <https://doi.org/10.59851/imr.12.2.5>.
- Gosztonyi G. (2022) 'Az internetes tartalomszabályozás európai típusú szabályozásának kezdetei, avagy irányelvektől a rendeletekig (TWF, AVMS, E-Comm, DSA, DMA)', *Jog – Állam – Politika*, 13(4), pp. 17-32.
- Görgényi, I. (2023) 'Áldozatvédelem az Európai Unióban a Stratégia előtt és után', *Miskolci Jogi Szemle*, 18(2), pp. 239-254; <https://doi.org/10.32980/MJSz.2023.2.239>.
- Guarino, B. (2024) 'Elon Musk's Neuralink Has Implanted Its First Chip in a Human Brain. What's Next?', *Scientific American*, 30 January. [Online]. Available at: <https://www.scientificamerican.com/article/elon-musks-neuralink-has-implanted-its-first-chip-in-a-human-brain-whats-next/>
- Halász, Cs. (2023) *A magánélethez való jog*. Miskolc: Bíbor.

- Henares-Montiel, J., Benítez-Hidalgo, V., Ruiz-Pérez, I., Pastor-Moreno, G., Rodríguez-Barranco, M. (2022) 'Cyberbullying and Associated Factors in Member Countries of the European Union: A Systematic Review and Meta-Analysis of Studies with Representative Population Samples', *International Journal of Environmental Research and Public Health*, 19(12), 7364, pp. 1–13; <https://doi.org/10.3390/ijerph19127364>.
- Horváth, T., Sántha, F. (2019) 'A jogállami büntetőjog alapelvei' in Görgényi, I., Gula, J., Horváth, T., Jacsó, J. Lévy, M., Sántha, F., Váradi, E.: *Magyar büntetőjog – Általános rész*. Budapest: Wolters Kluwer, pp. 68–75.
- Hulkó, G., Marinkás, Gy. (2023) 'A személyes adatok kezelése és a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog összehasonlító elemzése az Egyesült Királyság, Olaszország és Németország szabályozási rendszereiben', *Közigazgatás Tudomány*, 3(2), pp. 57–70; <https://doi.org/10.54200/kt.v3i2.57>.
- ILGA-Europe (2021) 'How the EU Strategy on the Rights of the Child will protect LGBTI kids' *ilga-europe*, 26 March. [Online]. Available at: <https://www.ilga-europe.org/blog/how-the-eu-strategy-on-the-rights-of-the-child-will-protect-lgbti-kids/>
- Kaesling, K. (2023) 'A Rights-Based Approach to Children's Digital Participation in the Multi-Level System of the European Union' in Dethloff, N., Kaesling, K., Specht-Riemenschneider, L. (eds.) *Families and New Media – Comparative Perspectives on Digital Transformations in Law and Society*. Wiesbaden: Springer, pp. 73–110; https://doi.org/10.1007/978-3-658-39664-0_4.
- Kalaitzaki, K. (2022) 'An Overview and Critical Analysis of the EU Anti-Racism Legal Framework' in Hadjigeorgiou, N. (ed.) *The implementation of the EU anti-racism legal framework in 6 European States: Bulgaria, Cyprus, Greece, Malta, Italy and the Netherlands*. Preserve Project, pp. 10–31. [Online]. Available at: https://www.cecl.gr/wp-content/uploads/2022/11/Preserve_FULL_E-book1-compressed.pdf
- Karsai, K. (2006) 'Az európai büntetőjog röögös útján', *Magyar Jog*, 53(1), pp. 1–10.
- Kiljunen, K. (2004) *The European Constitution in the Making*. Brussels: Centre for European Policy Studies.
- Kokott, J., Sobotta, K. (2010) 'The Charter of Fundamental Rights of the European Union after Lisbon', *European University Institute Working Papers – Academy of European Law*, 2010/6, pp. 1–15.
- Lehotay, V. (2019) 'Az antiszemitizmus, az idegengyűlölet és a rasszizmus elleni küzdelem az Európai Unióban', *Publicationes Universitatis Miskolcensis. Sectio Juridica et Politica*, 37(1), pp. 170–186.

- Leman, J. (1996) 'Europe's Consultative Commission on Racism and Xenophobia and the Slow Progress towards a European Antiracism Observatory', *Loyola of Los Angeles International and Comparative Law Review*, 18(3), pp. 603–612.
- Ligeti, K. (2008a) 'A nemzetközi bűnügyi együttműködés intézményi keretei Európában' in Kondorosi, F., Ligeti, K. (eds.) *Az Európai büntetőjog kézikönyve*. Budapest: Magyar Közlöny Lap- és Könyvkiadó, pp. 35–58.
- Ligeti, M. (2008b) 'A rasszizmus és az idegengyűlölet elleni büntetőjogi fellépés' in Kondorosi, F., Ligeti, K. (eds.) *Az Európai büntetőjog kézikönyve*. Budapest: Magyar Közlöny Lap- és Könyvkiadó, pp. 666–678.
- Lobe, B., Velicu, A., Staksrud, E., Chaudron, S., Di Gioia, R. (2021) *How children (10-18) experienced online risks during the Covid-19 lockdown – Spring 2020 – Key findings from surveying families in 11 European countries*. Luxembourg: Publications Office of the European Union; <https://doi.org/10.2760/562534>.
- Lodder, A. R. (2017) 'Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market' in Lodder, A. R., Murray, A. D. (eds.) *EU regulation of e-commerce: A Commentary*. Cheltenham: Edward Elgar, pp. 15–58; <https://doi.org/10.4337/9781785369346.00010>.
- Marinkás, Gy. (2018) *Az őslakos népek védelmének aktuális jogi kihívásai*. Miskolc: Private publication.
- Mezei, K. (2021) 'Az online gyermekpornográfia és a büntetőjog', *Ügyészek Lapja*, 28(4), pp. 19–30.
- Myftari, K., Guço, S. (2021) 'Prohibition of the application of criminal law by analogy within the principle of legal certainty', *Journal of Research in Humanities and Social Science*, 9(5), pp. 20–28.
- Nagy, Z. (2023) 'Modern technológiák és jogi szabályozásukkal kapcsolatos elméleti kérdések' in Nagy, Z. (ed.) *Az összehasonlító jog eszközével a gyűlölet ellen. Az online gyűlöletbeszéd, zaklatás és megfélemlítés nemzetközi szabályozása*. Budapest: Mádl Ferenc Összehasonlító Jogi Intézet, pp. 21–32; https://doi.org/10.47079/2023.nz.gyuloletbeszed.10_1.
- Peršak, N. (2022) 'Criminalising Hate Crime and Hate Speech at EU Level: Extending the List of Eurocrimes Under Article 83(1) TFEU', *Criminal Law Forum*, 33(1), pp. 85–119; <https://doi.org/10.1007/s10609-022-09440-w>.
- Dalla Pozza, V., Di Pietro, A., Morel, S., Psaila, E. (2016) *Cyberbullying Among Young People – Study for the LIBE Committee*. Brussels: European Parliament; <https://doi.org/10.2861/748350>.
- Rizza, C., Guimarães Pereira, Â. (2013) *Social Networks and Cyber-bullying among Teenagers: EU Scientific e policy report*. Luxembourg: Publications Office of the European Union; <https://doi.org/10.2788/41784>.

- Rakhmatov, D. (2022) 'Methods and Effectiveness of the Use of Artificial Intelligence in the Fight against Cyberbullying', *Journal of Academic Research and Trends in Educational Sciences*, 1(4), pp. 122–129.
- Róth, E. (2018) 'A kiszolgáltatott és a gyermek gyanúsítottak, valamint vádlottak uniós védelme', *Acta Universitatis Szegedinensis: Acta Juridica et Politica*, 2018/81, pp. 829–841.
- Sorbán, K. (2022) 'Merre tovább az online gyermekvédelemben? A kiskorúak védelme az új médiakörnyezetben megjelenő káros tartalmaktól', *Glossa Iuridica*, 9(1–2), pp. 65–88.
- Sorbán, K. (2023) 'An elephant in the room – EU policy gaps in the regulation of moderating illegal sexual content on video-sharing platforms', *International Journal of Law and Information Technology*, 31(3), pp. 71–85; <https://doi.org/10.1093/ijlit/eaad024>.
- Specht-Riemenschneider, L., Marko, A., Wette, Sascha (2023) 'Protection of Minors on Video Sharing Platforms' in Dethloff, N., Kaesling, K., Specht-Riemenschneider, L. (eds.) *Families and New Media – Comparative Perspectives on Digital Transformations in Law and Society*. Wiesbaden: Springer, pp. 227–257; https://doi.org/10.1007/978-3-658-39664-0_11.
- Szajbély, K. (2018) 'Faji alapú diszkrimináció tilalma' in Lamm, V. (ed.) *Emberi jogi enciklopédia*. Budapest: HVG-ORAC, pp. 286–293.
- Turilazzi, A., Taddeo, M., Floridi, L., Casolari, F. (2023) 'The digital services act: an analysis of its ethical, legal, and social implications', *Law, Innovation and Technology*, 15(1), 83–106; <https://doi.org/10.1080/17579961.2023.2184136>.
- Turner, J. I. (2012) 'The Expressive Dimension of EU Criminal Law', *The American Journal of Comparative Law*, 60(2), pp. 555–583; <https://doi.org/10.5131/AJCL.2011.0012>.
- Udvarhelyi, B. (2015) 'Criminal law competences of the European Union before and after the Treaty of Lisbon', *European Integration Studies*, 11(1), pp. 46–59.
- Udvarhelyi, B. (2016) 'A Lisszaboni Szerződés és a büntetőjog – gondolatok az Európai Unió megújult büntetőjogi jogharmonizációs hatásköréről', *Állam- és Jogtudomány*, 57(3), pp. 123–142.
- Udvarhelyi, B. (2019) *Az Európai Unió anyagi büntetőjoga a Lisszaboni Szerződés után*. Budapest: Patrocinium.
- Zankova, B., Gosztonyi, G. (2022) 'Quo vadis, European's Union New Digital Regulation Package?', *Business and Law*, 2021/2, pp. 67–90; <http://doi.org/10.370.75/BAL.2021.2.03>.
- Zöldi, Zs. (2022) 'Az európai platformszabályozás jellegzetességei – Platformjog és felhasználóvédelem', *In Medias Res*, 11(1), pp. 66–82.
- Criminalise cyber-bullying* (2023) *eppgroup*, 10 May [Online]. Available at: <https://www.eppgroup.eu/newsroom/criminalise-cyber-bullying>

Criminalise cyberbullying across the EU (2023) *eppgroup*, 20 September [Online]. Available at: <https://www.eppgroup.eu/what-we-do/with-eu-countries/ireland/criminalise-cyberbullying-across-the-eu>

Preventing cyberbullying under the Data Protection Act (2022) *The Sunday Mail*, 26 June [Online]. Available at: https://www.sundaymail.co.zw/preventing-cyberbullying-under-the-data-protection-act#google_vignette